

**ATTACK**

**DEFENSE**

by PentesterAcademy

|             |   |
|-------------|---|
| <b>Name</b> | OWASP Dependency-Check  |
| <b>URL</b>  | <a href="https://www.attackdefense.com/challengedetails?cid=2062">https://www.attackdefense.com/challengedetails?cid=2062</a> |
| <b>Type</b> | DevSecOps Basics: Software Component Analysis   |

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

## Challenge Description

[Dependency-Check](#) tool is used to scan the dependencies(libraries, packages) of a project to detect the components with known vulnerabilities.

A Kali GUI machine (kali-gui) is provided to the user with Dependency-Check installed on it. The source code for three sample web applications is provided in the home directory of the root user.

**Objective:** Use OWASP Dependency-Check to detect vulnerable code dependencies!

### Instructions:

- The source code of web applications is provided at /root/github-repos

## Solution

**Step 1:** Check the available options of dependency check.

**Command:** dependency-check.sh --help

```

root@attackdefense:~# dependency-check.sh --help
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
usage: Dependency-Check Core [--advancedHelp] [--enableExperimental]
      [--exclude <pattern>] [-f <format>] [--failOnCVSS <score>] [-h]
      [--junitFailOnCVSS <score>] [-l <file>] [-n] [-o <path>]
      [--prettyPrint] [--project <name>] [-s <path>] [--suppression
      <file>] [-v]

```

Dependency-Check Core can be used to identify if there are any known CVE vulnerabilities in libraries utilized by an application. Dependency-Check Core will automatically update required data from the Internet, such as the CVE and CPE data files from [nvd.nist.gov](http://nvd.nist.gov).

|                      |  |
|----------------------|--|
| --advancedHelp       | Print the advanced help message.   |
| --enableExperimental | Enables the experimental analyzers.  |
| --exclude <pattern>  | Specify an exclusion pattern. This option can be specified multiple times and it accepts Ant style exclusions.   |
| -f,--format <format> | The report format (HTML, XML, CSV, JSON, JUNIT, or ALL). The default is HTML. Multiple format parameters can be  |
| --prettyPrint        | When specified the JSON and XML report formats will be pretty printed.   |
| --project <name>     | The name of the project being scanned.   |
| -s,--scan <path>     | The path to scan - this option can be specified multiple times. Ant style paths are supported (e.g. 'path/**/*.jar'); if using Ant style paths it is highly recommended to quote the argument value. |
| --suppression <file> | The file path to the suppression XML file. This can be specified more than once to utilize multiple suppression files  |
| -v,--version         | Print the version information.   |

```

root@attackdefense:~#

```

**Step 2:** Check the provided web applications.

**Command:** `ls -l github-repos`

```

root@attackdefense:~# ls -l github-repos/
total 12
drwxr-xr-x 3 root root 4096 Sep 15 15:25 java-mvn-hello-world-web-app
drwxr-xr-x 3 root root 4096 Sep 15 15:25 javaee7-essentials-archetype
drwxr-xr-x 3 root root 4096 Sep 15 15:25 wifi-password-cli
root@attackdefense:~#

```

We will take one example at a time and run the tool on that.

### Example 1: wifi-password-cli

**Step 1:** Change to the wifi-password-cli directory and check its contents.

#### Commands:

```
cd ~/github-repos/wifi-password-cli/  
ls
```

```
root@attackdefense:~# cd github-repos/wifi-password-cli/  
root@attackdefense:~/github-repos/wifi-password-cli#  
root@attackdefense:~/github-repos/wifi-password-cli# ls  
cli.js  license  node_modules  package-lock.json  package.json  readme.md  test.js  
root@attackdefense:~/github-repos/wifi-password-cli#
```

**Step 2:** Run the dependency-check.sh while passing the project directory and flag to not to check for updates.

**Command:** dependency-check.sh -n -s .

#### Command Explanation:

- -n = Scan without checking for updates
- -s = Scan the passed directory

```
root@attackdefense:~/github-repos/wifi-password-cli# dependency-check.sh -n -s .  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
[INFO]  
  
Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false p  
ositives and false negatives may exist in the analysis performed by the tool. Use of the tool and the report  
ing provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or o  
therwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the u  
ser's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arisin  
g out of or in connection with the use of this tool, the analysis performed, or the resulting report.  
  
[INFO] Analysis Started  
[INFO] Finished File Name Analyzer (0 seconds)  
[ERROR] -----  
[ERROR] .NET Assembly Analyzer could not be initialized and at least one 'exe' or 'dll' was scanned. The 'do  
tnet' executable could not be found on the path; either disable the Assembly Analyzer or add the path to dot  
net core in the configuration.  
[ERROR]
```



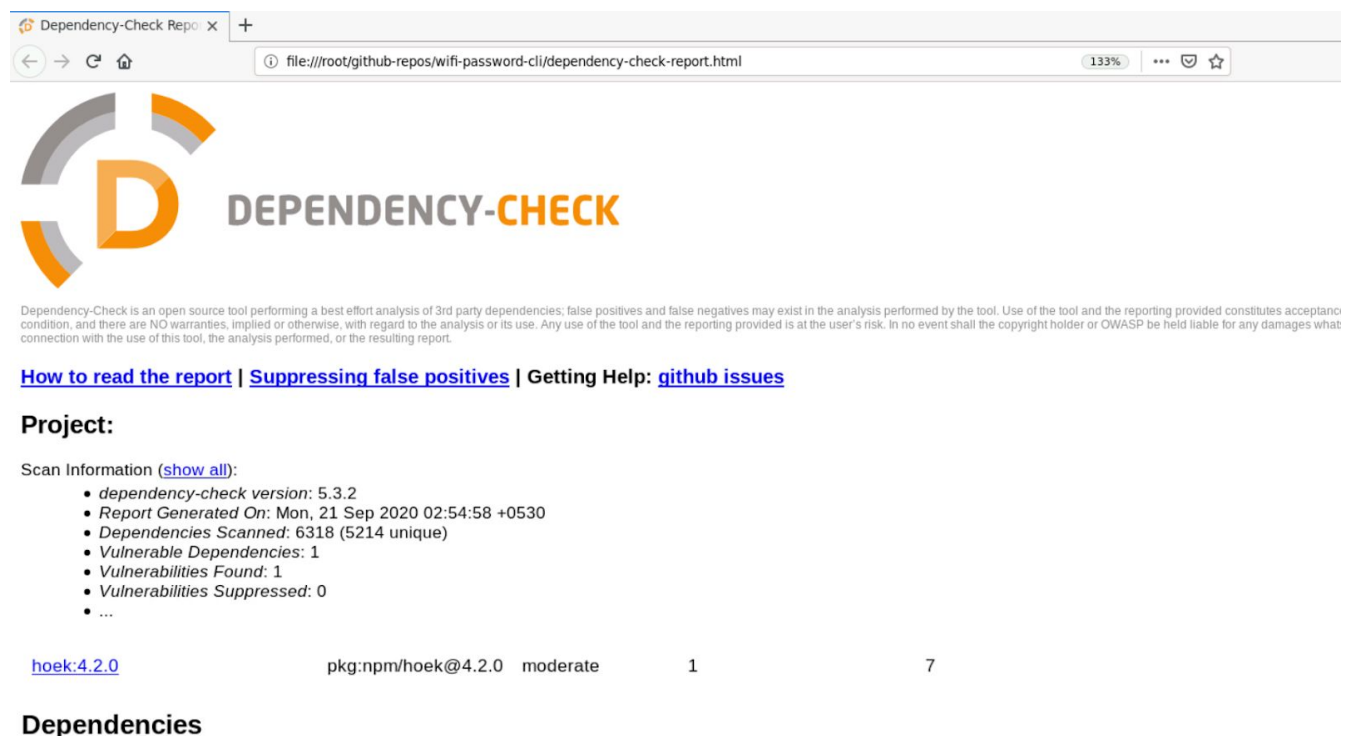
```
[INFO] Finished Dependency Merging Analyzer (3 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
[INFO] Finished Hint Analyzer (1 seconds)
[INFO] Created CPE Index (5 seconds)
[INFO] Finished CPE Analyzer (6 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[INFO] Finished Node Audit Analyzer (0 seconds)
[INFO] Finished RetireJS Analyzer (74 seconds)
[WARN] An error occurred while analyzing '/root/github-repos/wifi-password-cli/node_modules/@typescript-eslint/eslint-plugin/dist/rules/prefer-readonly-parameter-types.js' (Sonatype OSS Index Analyzer).
[INFO] Finished Sonatype OSS Index Analyzer (20 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (2 seconds)
[INFO] Finished Dependency Bundling Analyzer (7 seconds)
[INFO] Analysis Complete (117 seconds)
```

The dependency-check.sh file has scanned the application for possible security threats and generated an HTML report.

**Note:** Ignore the Failed to request component-reports message.

**Step 3:** Open the HTML report in firefox, The report is stored inside the project directory

**Command:** firefox dependency-check-report.html



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance of the tool's output as is, with no warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

**Project:**

Scan Information ([show all](#)):

- dependency-check version: 5.3.2
- Report Generated On: Mon, 21 Sep 2020 02:54:58 +0530
- Dependencies Scanned: 6318 (5214 unique)
- Vulnerable Dependencies: 1
- Vulnerabilities Found: 1
- Vulnerabilities Suppressed: 0
- ...

| Package Name | Version            | Severity | Count |
|--------------|--------------------|----------|-------|
| hoek:4.2.0   | pkg:npm/hoek@4.2.0 | moderate | 1     |

**Dependencies**

#### hoek:4.2.0

**Description:**

General purpose node utilities

**License:**

BSD-3-Clause

**File Path:** /root/github-repos/wifi-password-cli/node\_modules/hoek/package.json

**MD5:** edb8d502978e4cb012ca8890c201a038

**SHA1:** ef079cc1155f9d8db7f98448a70f48d7274ea3e7

**SHA256:** e91a8b3cbb1f174ed0bc875def306a55199f868dbaf26ee55bbbf39fd17e6cae

**Referenced In Project/Scope:** wifi-password-cli:1.0.0

#### Issues Detected

- hoek 4.2.0 is vulnerable to prototype pollution.

#### Example 2: javaee7-essentials-archetype

**Step 1:** Change to the javaee7-essentials-archetype directory and check its contents.

**Commands:**

```
cd ~/github-repos/javaee7-essentials-archetype
ls
```

```
root@attackdefense:~/github-repos# cd javaee7-essentials-archetype
root@attackdefense:~/github-repos/javaee7-essentials-archetype#
root@attackdefense:~/github-repos/javaee7-essentials-archetype# ls
LICENSE  README.md  pom.xml  snapshot.sh  src
root@attackdefense:~/github-repos/javaee7-essentials-archetype#
```

**Step 2:** Run the dependency-check.sh while passing the project directory and flag to not to check for updates.

**Command:** dependency-check.sh -n -s .

```
root@attackdefense:~/github-repos/javaee7-essentials-archetype# dependency-check.sh -n -s .
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[INFO]
```

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

```
[INFO] Analysis Started
[INFO] Finished Archive Analyzer (0 seconds)
[INFO] Finished File Name Analyzer (0 seconds)
[INFO] Finished Jar Analyzer (0 seconds)
[INFO] Finished Central Analyzer (0 seconds)
[INFO] Finished Dependency Merging Analyzer (0 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
[INFO] Finished Hint Analyzer (0 seconds)
[INFO] Created CPE Index (4 seconds)
```

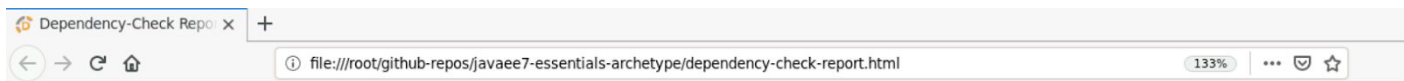
```
[INFO] Finished Hint Analyzer (0 seconds)
[INFO] Created CPE Index (4 seconds)
[INFO] Finished CPE Analyzer (5 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[WARN] An error occurred while analyzing '/root/github-repos/javaee7-essentials-archetype/src/commons-collections-3.2.1-1.0.0.jar' (Sonatype OSS Index Analyzer).
[INFO] Finished Sonatype OSS Index Analyzer (20 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
[INFO] Finished Dependency Bundling Analyzer (0 seconds)
[INFO] Analysis Complete (27 seconds)
[ERROR] Failed to request component-reports
root@attackdefense:~/github-repos/javaee7-essentials-archetype#
```

The dependency-check.sh file has scanned the application for possible security threats and generated an HTML report.

**Step 3:** Open the HTML report in firefox, The report is stored inside the project directory

**Command:** firefox dependency-check-report.html





Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damage or connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

## Project:

Scan Information ([show all](#)):

- *dependency-check version*: 5.3.2
- *Report Generated On*: Mon, 21 Sep 2020 03:02:50 +0530
- *Dependencies Scanned*: 2 (2 unique)
- *Vulnerable Dependencies*: 2
- *Vulnerabilities Found*: 3
- *Vulnerabilities Suppressed*: 0

## Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

| Dependency  | Vulnerability IDs  | Package  | Highest Severity | CVE Count | Confidence | Evidence Count |
|---|--|--|------------------|-----------|------------|----------------|
| <a href="#">commons-collections-3.2.1-1.0.0.jar</a> | <a href="#">cpe:2.3:a:apache:commons-collections:3.2.1-1.0.0:*</a> | pkg:maven/commons-collections/commons-collections@3.2.1<br>pkg:maven/org.ow2.util.bundles/commons-collections-%24%7Bcommons-collections.version%7D@1.0.0 | CRITICAL         | 2         | Highest    | 37             |
| <a href="#">httpclient-4.0.3.jar</a>                | <a href="#">cpe:2.3:a:apache:httpclient:4.0.3:*</a>                | pkg:maven/org.apache.httpcomponents/httpclient@4.0.3   | MEDIUM           | 1         | Highest    | 31             |

## Issues Detected

- Common Collections: Deserialization of Untrusted Data (CVE-2015-6420,CVE-2017-15708)
- HttpClientComponents Client: Man in the Middle attacks (CVE-2014-3577)

## Example 3: Java Maven Hello World Web App

**Step 1:** Change to the cloned directory and check its contents.



### Commands:

```
cd ~/github-repos/java-mvn-hello-world-web-app
```

```
ls
```

```
root@attackdefense:~/github-repos# cd java-mvn-hello-world-web-app/
root@attackdefense:~/github-repos/java-mvn-hello-world-web-app#
root@attackdefense:~/github-repos/java-mvn-hello-world-web-app# ls
ApplicationManifest.yml  SecurityManifest.yml      src
Jenkinsfile             pom.xml                   struts-tiles-1.3.8.jar
LICENSE                 sample_jenkins_file
README.md               sonar-project.properties
root@attackdefense:~/github-repos/java-mvn-hello-world-web-app#
```

**Step 2:** Run the dependency-check.sh while passing the project directory and flag to not to check for updates.

**Command:** dependency-check.sh -n -s .

```
root@attackdefense:~/github-repos/java-mvn-hello-world-web-app# dependency-check.sh -n -s .
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[INFO]

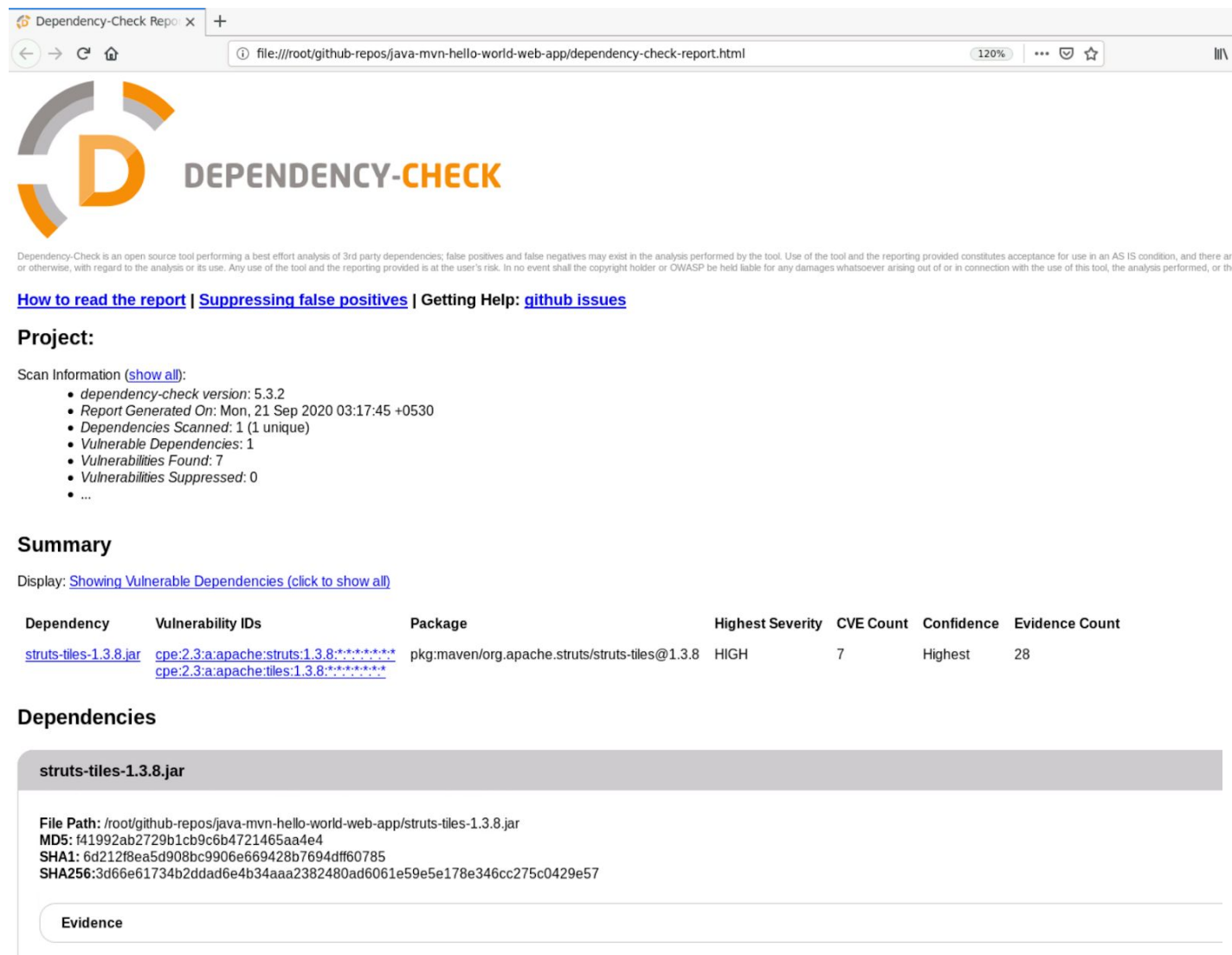
Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[INFO] Analysis Started
[INFO] Finished Archive Analyzer (0 seconds)
[INFO] Finished File Name Analyzer (0 seconds)
[INFO] Finished Jar Analyzer (0 seconds)
[INFO] Finished Central Analyzer (0 seconds)
[INFO] Finished Dependency Merging Analyzer (0 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
[INFO] Finished Hint Analyzer (0 seconds)
[INFO] Created CPE Index (4 seconds)

[INFO] Created CPE Index (4 seconds)
[INFO] Finished CPE Analyzer (5 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[WARN] An error occurred while analyzing '/root/github-repos/java-mvn-hello-world-web-app/struts-tiles-1.3.8.jar' (Sonatype OSS Index Analyzer).
[INFO] Finished Sonatype OSS Index Analyzer (20 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
[INFO] Finished Dependency Bundling Analyzer (0 seconds)
[INFO] Analysis Complete (26 seconds)
[ERROR] Failed to request component-reports
root@attackdefense:~/github-repos/java-mvn-hello-world-web-app#
```

The dependency-check.sh file has scanned the application for possible security threats and generated an HTML report.

**Command:** firefox dependency-check-report.html



The screenshot shows a web browser window displaying the Dependency-Check report. The browser's address bar shows the file path: `file:///root/github-repos/java-mvn-hello-world-web-app/dependency-check-report.html`. The report header features the "DEPENDENCY-CHECK" logo and a disclaimer. Below the header, there are links for "How to read the report", "Suppressing false positives", and "Getting Help: github issues". The "Project:" section is followed by "Scan Information (show all):" which lists details such as the tool version (5.3.2), the report generation date (Mon, 21 Sep 2020 03:17:45 +0530), the number of dependencies scanned (1), and the number of vulnerabilities found (7). A "Summary" section includes a link to "Showing Vulnerable Dependencies (click to show all)". Below this is a table with columns: Dependency, Vulnerability IDs, Package, Highest Severity, CVE Count, Confidence, and Evidence Count. The table lists one entry for "struts-tiles-1.3.8.jar" with a "HIGH" severity and 7 CVEs. The "Dependencies" section is expanded, showing details for "struts-tiles-1.3.8.jar", including its file path, MD5, SHA1, and SHA256 hashes. An "Evidence" section is also present but empty.

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are no warranties, expressed or implied, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the reporting provided.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

**Project:**

Scan Information ([show all](#)):

- dependency-check version: 5.3.2
- Report Generated On: Mon, 21 Sep 2020 03:17:45 +0530
- Dependencies Scanned: 1 (1 unique)
- Vulnerable Dependencies: 1
- Vulnerabilities Found: 7
- Vulnerabilities Suppressed: 0
- ...

**Summary**

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

| Dependency                             | Vulnerability IDs   | Package  | Highest Severity | CVE Count | Confidence | Evidence Count |
|--|---|--|------------------|-----------|------------|----------------|
| <a href="#">struts-tiles-1.3.8.jar</a> | <a href="#">cpe:2.3:a:apache:struts:1.3.8:*:*:*:*:*</a><br><a href="#">cpe:2.3:a:apache:tiles:1.3.8:*:*:*:*</a> | pkg:maven/org.apache.struts/struts-tiles@1.3.8 | HIGH             | 7         | Highest    | 28             |

**Dependencies**

**struts-tiles-1.3.8.jar**

File Path: /root/github-repos/java-mvn-hello-world-web-app/struts-tiles-1.3.8.jar  
MD5: f41992ab2729b1cb9c6b4721465aa4e4  
SHA1: 6d212f8ea5d908bc9906e669428b7694dfff60785  
SHA256: 3d66e61734b2ddad6e4b34aaa2382480ad6061e59e5e178e346cc275c0429e57

**Evidence**

## Issues Detected

- Execute Arbitrary commands via unspecified vectors (CVE-2012-0394)
- Execute Arbitrary OGNL code (CVE-2013-2115)
- Allows remote attackers to manipulate class loader to execute arbitrary code (CVE-2014-0114)

- Bypass intended restrictions via modified page parameter (CVE-2015-0899)
- Cross-Site Scripting (CVE-2015-2992)
- Arbitrary Code Execution via multipart request (CVE-2016-1181)
- Cross-Site Scripting via unrestricted validator configuration (CVE-2016-1182)

## Learnings

Detecting known vulnerable components in project's dependencies. .