


CS 305 Module Two Coding Assignment Template

Ronny Z. Valtonen

Version 1.0

1. Run Dependency Check


DEPENDENCY-CHECK

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 is arising out of or 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](#)

[Sponsor](#)

Project: Module2.1

com.nhu:Module2.1:0.0.1-SNAPSHOT

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

- dependency-check version: 12.1.0
- Report Generated On: Fri, 14 Mar 2025 14:39:41 -0700
- Dependencies Scanned: 52 (36 unique)
- Vulnerable Dependencies: 21
- Vulnerabilities Found: 166
- Vulnerabilities Suppressed: 0
- ...

Summary

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

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:redhat:hibernate_validator:6.0.18:*****	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	2	Highest	32
jackson-databind-2.10.2.jar	cpe:2.3:a:fastenxml:jackson-databind:2.10.2:***** cpe:2.3:a:fastenxml:jackson-modules-jvab:2.10.2:*****	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	6	Highest	39
json-path-2.4.0.jar	cpe:2.3:a:json-path:json-path:2.4.0:*****	pkg:maven/com.jayway.jsonpath/json-path@2.4.0	MEDIUM	1	Highest	33
json-smart-2.3.jar	cpe:2.3:a:json-smart:project:json-smart:2.3:***** cpe:2.3:a:json-smart:project:json-smart-v2.2.3:*****	pkg:maven/net.minidev/json-smart@2.3	HIGH	3	Highest	45
log4j-api-2.12.1.jar	cpe:2.3:a:apache:log4j:2.12.1:*****	pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1	LOW	1	Highest	42
logback-classic-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*****	pkg:maven/ch.qos.logback/logback-classic@1.2.3	HIGH	2	Highest	31
logback-core-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*****	pkg:maven/ch.qos.logback/logback-core@1.2.3	HIGH	4	Highest	31
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml:project:snakeyaml:1.25:*****	pkg:maven/org.yaml/snakeyaml@1.25	CRITICAL	8	Highest	44
spring-boot-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*****	pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE	CRITICAL	3	Highest	39
spring-boot-starter-web-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:***** cpe:2.3:a:web:project:web:2.2.4:release:*****	pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE	CRITICAL	3	Highest	35
spring-core-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal:software:spring_framework:5.2.3:release:***** cpe:2.3:a:springsource:spring_framework:5.2.3:release:***** cpe:2.3:a:vmware:spring_framework:5.2.3:release:*****	pkg:maven/org.springframework/spring-core@5.2.3.RELEASE	CRITICAL*	11	Highest	36
spring-data-rest-webmvc-3.2.4.RELEASE.jar	cpe:2.3:a:pivotal:software:spring_data_rest:3.2.4:release:***** cpe:2.3:a:vmware:spring_data_rest:3.2.4:release:*****	pkg:maven/org.springframework.data/spring-data-rest-webmvc@3.2.4.RELEASE	MEDIUM	2	Highest	27
spring-expression-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal:software:spring_framework:5.2.3:release:***** cpe:2.3:a:springsource:spring_framework:5.2.3:release:***** cpe:2.3:a:vmware:spring_framework:5.2.3:release:*****	pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE	CRITICAL*	12	Highest	36

2. Document Results

snakeyaml-1.25.jar

Description:

YAML 1.1 parser and emitter for Java

spring-boot-2.2.4.RELEASE.jar

Description:

Spring Boot

spring-expression-5.2.3.RELEASE.jar

Description:

Spring Expression Language (SpEL)

spring-security-config-5.2.1.RELEASE.jar

Description:

spring-security-config

spring-web-5.2.3.RELEASE.jar

Description:

Spring Web

jackson-databind-2.10.2.jar

Description:

General data-binding functionality for Jackson: works on core streaming API

json-smart-2.3.jar

Description:

JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language, Standard ECMA-262 3rd Edition - December 1999. JSON is a text

format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language.

logback-classic-1.2.3.jar

Description:

logback-classic module

logback-core-1.2.3.jar

Description:

logback-core module

3. Analyze Results

The Maven Dependency vulnerability check revealed a total of 21 dependencies. Above, I have only listed the ones marked as CRITICAL and HIGH severity. There were a number of duplicate (non-unique) dependencies that I did not write down, but were reported. One of the most effective ways to mitigate a lot of these vulnerabilities is to update the dependencies to the versions where vulnerabilities have been fixed. For example, the Spring Boot 2.2.4-RELEASE is not the latest and updating this may fix the vulnerabilities involved.

It is important to filter false positives that the dependency-check can sometimes generate because some issues may not be exploitable in this specific environment. Taking the time to solve every single dependency check may not be the proper resource use, which filtering will prevent wasted effort.

Checking some of the dependency vulnerabilities such as ‘tomcat-embed-websocket-9.0.30.jar’ has a reference to CVE-2020 which describes issues like remote code execution risks and DDOS attacks. Similarly, the spring-boot-2.2.4 CVE reference states flaws in the embedded container components and is recommended to use the latest release.