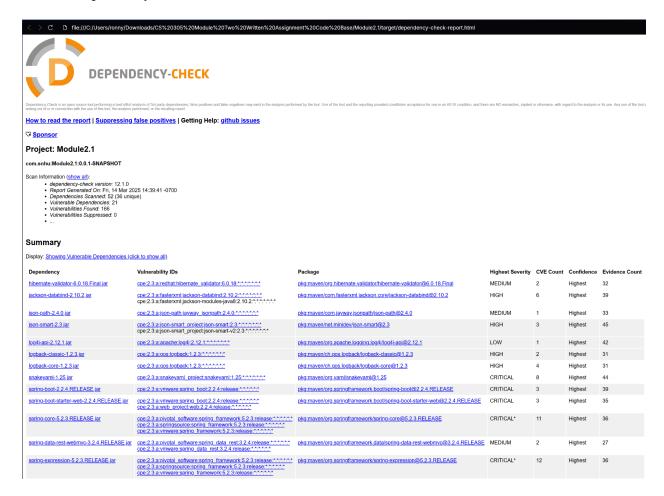


CS 305 Module Two Coding Assignment Template Ronny Z. Valtonen

Version 1.0

1. Run Dependency Check



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

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

Description:



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.