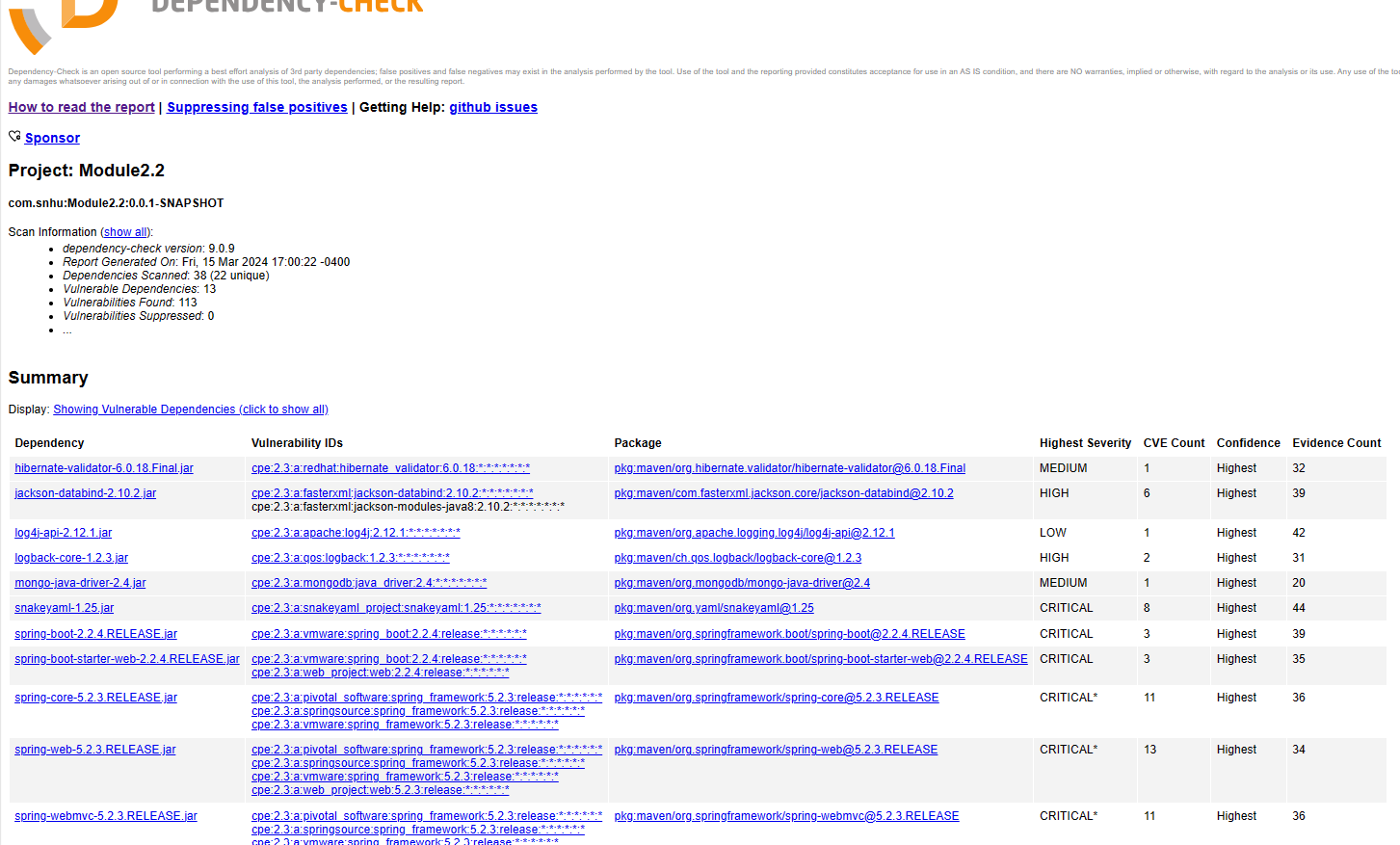
# CS 305 Module Two Coding Assignment Template

## Instructions

Replace the bracketed text with the relevant information in your own words. If you choose to include images or supporting materials, make certain to insert them in all the relevant locations in the document.

## Run Dependency Check



## Document Results

* Hibernate-validator-6.0.18.Final.jar

Vuln ID: CVE-2020-10693

Description: Hibernate Validator version 6.1.2.Final has a flaw that allows attackers to bypass input sanitation controls.

* Jackson-databind-2.10.2.jar

Vuln ID: CVE-2023-35116, CVE-2021-46877, CVE-2022-42004, CVE-2022-42003, CVE-2020-36518, CVE-2020-25649

Description: Outdated Jackson Data Bind

* Log4j-api-2.12.1.jar

Vuln ID: CVE-2021-44832, CVE-2-2021-45105, CVE-2021-45046, CVE-2021-44228, CVE-2020-9488

Description: Outdated version of Apache Log4j2

* Logback-core-1.2.3.jar

Vuln ID: CVE-2023-6378, CVE-2021-4255

Description: A vulnerability in the logback version 1.4.11 allows attackers to use a Denial-of-Service attack.

* Snakeyaml-1.25.jar

Vuln ID: CVE-2022-1471, CVE-2022-41854, CVE-2022-38752, CVE-2022-38751, CVE-2022-38750, CVE-2022-38749, CVE-2022-25857, CVE-2017-18640

Description: Using SnakeYaml’s Constructor () it is recommended to use SnakeYaml’s SafeContructor for parsing untrusted content.

* Spring-boot-2.2.4.RELEASE.jar

Vuln ID: CVE-2023-20883, CVE-2023-20873, CVE-2022-27772

Description: Using outdated version of Spring Boot

* Spring-web-5.2.3.RELEASE.jar

Vuln ID: CVE-2023-20863, CVE-2023-20861, CVE-2022-22971, CVE-2022-22970, CVE-2022-22968, CVE-2022-22965, CVE-2022-22950, CVE-2021-22060, CVE-2021-22118, CVE-2020-5421, CVE-2016-1000027

Description: Using an old version of Spring Framework.

* Tomcat-embed-core-9.0.30.jar

Vuln ID: CVE-2024-21733, CVE-2023-46589, CVE-2023-45648, CVE-2023-42795, CVE-2023-44487, CVE-2023-41080, CVE-2023-28708, CVE-2022-42252, CVE-2021-43980, CVE-2022-34305, CVE-2022-29885, CVE-2021-41079, CVE-2021-33037, CVE-2021-30640, CVE-2021-25329, CVE-2021-25122, CVE-2021-24122, CVE-2020-17527, CVE-2020-13943, CVE-2020-13935

Description: Using outdated version of Apache Tomcat

* Tomcat-embed-websocket-9.0.30.jar

Vuln ID: see IDs above under Tomcat-embed-core-9.0.30.jar.

Description: Using outdated version of Apache Tomcat

## Analyze Results

The dependency-check tool identified many vulnerabilities within the code provided. After reviewing these vulnerabilities provided in the report the best way to address the dependencies is to use the newest versions of Hibernate Validator, Jackson Data Bind, Apache Log4j, logback, Spring Boot, Spring Framework, and Apache Tomcat. Using the newest versions during the coding process will limit vulnerabilities and take advantage of the patches that have been made. Using SnakeYaml’s SafeConstructor instead of SnakeYaml’s Constructor () to better parsing of untrusted content. Filtering false positives from the dependency-check tool will allow you to focus on the true vulnerabilities and issues. False positives are typically CPE values that are incorrect. There is a suppression feature available within the Dependency-Check tool that will filter these values out of the report so the severe issues can be addressed.