# CS 305 Module Two Coding Assignment Template

Winnie Kwong

Southern New Hampshire University

CS-305 Software Security

Professor Foultz

September 9th, 2023

## 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

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Document Results

* hibernate-validator-6.0.18.Final.jar

Description: Hibernate's Bean Validation (JSR-380) reference implementation.

License: <http://www.apache.org/licenses/LICENSE-2.0.txt>

CVE-2020-10693

* jackson-databind-2.10.2.jar  
  Description: General data-binding functionality for Jackson: works on core streaming API

License: <http://www.apache.org/licenses/LICENSE-2.0.txt>

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

* log4j-api-2.12.1.jar

Description: The Apache Log4j API

License: <https://www.apache.org/licenses/LICENSE-2.0.txt>

CVE-2020-9488

* logback-core-1.2.3.jar

Description: logback-core module

License: <http://www.eclipse.org/legal/epl-v10.htm>

<http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html>

CVE-2021-42550

* mongo-java-driver-2.4.jar

Description: Java Driver for MongoDB

License: The Apache Software License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

CVE-2021-20328

* snakeyaml-1.25.jar

Description: YAML 1.1 parser and emitter for Java

License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

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

* spring-boot-2.2.4.RELEASE.jar

Description: Spring Boot

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

CVE-2023-20873, CVE-2022-27772, CVE-2023-20883

* spring-boot-starter-web-2.2.4.RELEASE.jar

Description: Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

CVE-2023-20873, CVE-2022-27772, CVE-2023-20883

* spring-core-5.2.3.RELEASE.jar

Description: Spring Core

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

CVE-2022-22965, CVE-2021-22118, CVE-2020-5421, CVE-2022-22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CVE-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096

* spring-web-5.2.3.RELEASE.jar

Description: Spring Web

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

CVE-2016-1000027, CVE-2022-22965, CVE-2021-22118, CVE-2020-5421, CVE-2022-22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CVE-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096

* spring-webmvc-5.2.3.RELEASE.jar

Description: Spring Web MVC

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

CVE-2022-22965, CVE-2021-22118, CVE-2020-5421, CVE-2022-22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CVE-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096

* tomcat-embed-core-9.0.30.jar

Description: Core Tomcat implementation

License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

CVE-2020-1938, CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25122, CVE-2021-41079, CVE-2022-29885, CVE-2022-42252, CVE-2020-9484, CVE-2021-25329, CVE-2021-30640, CVE-2022-34305, CVE-2023-41080, CVE-2021-24122, CVE-2021-33037, CVE-2019-17569, CVE-2020-1935, CVE-2020-13943, CVE-2023-28708, CVE-2021-43980

* tomcat-embed-websocket-9.0.30.jar

Description: Core Tomcat implementation

License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

CVE-2020-1938, CVE-2020-8022, CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25122, CVE-2021-41079, CVE-2022-29885, CVE-2022-42252, CVE-2020-9484, CVE-2021-25329, CVE-2021-30640, CVE-2022-34305, CVE-2023-41080, CVE-2021-24122, CVE-2021-33037, CVE-2019-17569, CVE-2020-1935, CVE-2020-13943, CVE-2023-28708, CVE-2021-43980

## Analyze Results

Repeated vulnerabilities frequently involved access rights, denial-of-service (DoS) attacks, and privileged network positions throughout the documented results. The hibernate validator, which can override and extend through XML, had a vulnerability where hackers could bypass input sanitation controls that developers may have implemented when handling user-controlled data in error messages. Other portions, such as FasterXML Jackson Databind, Snakeyaml, and Spring, had many issues vulnerable to DoS attacks that could damage data integrity. Within snakeYAML, an attack may supply content that could cause the parser to crash by stack overflow. At the same time, Spring Framework was using outdated versions that were no longer supported and more vulnerable to attacks. Furthermore, the documented results exposed vulnerabilities within network connections shown in Java Driver for MongoDB and Core Tomcat implementation. Within the Java Driver for MongoDB, the exposure in combination with a privileged network position active MITM attack could result in interception of traffic between the Java driver and the KMS service, rendering Field Level Encryption ineffective. In the Core Tomcat implementation, attacks would be able to control the web application's content while being accessible to other remote code executions.

Filtering out false positives, also called false alarms, from the dependency-check tool kit should be considered because it provides unnecessary worries and can lead to uncalled-for diagnostic tests. Typically, false positives can disappear during different dependency checks. Still, if the tester continues to resolve false positives, it will consume and waste much of the tester’s time and energy.