# 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

A screenshot of a computer

Description automatically generated

## Document Results

There was 13 total dependencies with vulnerabilities and most have critical severity.

**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

**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>

**log4j-api-2.12.1.jar**

Description: The Apache Log4j API

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

**logback-core-1.2.3.jar**

Description of Dependency: Module for logback-core.

License Given: [http://www.eclipse.org/legal/epl-v10.html, http://www.gnu.org/licenses/old-](http://www.eclipse.org/legal/epl-v10.html,%20http:/www.gnu.org/licenses/old-%20%20licenses/lgpl-2.1.html)

[licenses/lgpl-2.1.html](http://www.eclipse.org/legal/epl-v10.html,%20http:/www.gnu.org/licenses/old-%20%20licenses/lgpl-2.1.html)

**mongo-java-driver-2.4.jar**

Description of Dependency: MongoDB JavaDriver.

License Given: The Apache Software License, Version 2.0:

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

**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>

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

Description of Dependency: Spring Boot

License Given: Apache License, Version 2.0: [https://www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt)

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

Description of Dependency: A beginning point for creating web applications with Spring MVC,

including RESTful features, uses the integrated container Tomcat by default.

License Given: Apache License, Version 2.0: [https://www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt)

**spring-core-5.2.3.RELEASE.jar**

Description of Dependency: Spring Core

License Given: Apache License, Version 2.0: [https://www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt)

**spring-web-5.2.3.RELEASE.jar**

Description of Dependency: Spring Web

License Given: Apache License, Version 2.0: [https://www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt)

**spring-webmvc-5.2.3.RELEASE.jar**

Description of Dependency: Spring Web MVC

License Given: Apache License, Version 2.0: [https://www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt)

**tomcat-embed-core-9.0.30.jar**

Description of Dependency: Implementation for Core Tomcat

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

**tomcat-embed-websocket-9.0.30.jar**

Description of Dependency: Implementation for Core Tomcat

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

## Analyze Results

There are numerous vulnerabilities exposed by the dependencies, most of which pose risk for code injection, remote code executions, and data leaks or manipulation. Many of the dependencies are outdated, which is exposing the project to known vulnerabilities that the updated versions have addressed. Making sure the dependencies follow the same, or similar, reccommendations is essential for maintaining a secure environment for the application. The dependencies should be regularly audited as to keep them up-to-date with any new vulnerabilities to ensure the applications security. It is also important to filter out the false positives from the vulnerability reports will help prioritize the real security threats. The false reports can overload dependency reports. This would then make it difficult to identify the true issues. Filtering out these false vulnerabilities can allow for a more focused report. This approach will make it easier for future evaluations will be more efficient and also ensure that all security measures are properly implemented and maintained.