# 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

* hibernate-validator-6.0.18.Final.jar
  + Reference implementation of the bean validation specification.
* jackson-databind-2.10.2.jar
  + A library called Jackson that works with JSON data.
* log4j-api-2.12.1.jar
  + Apache log api for the logging framework.
* Logback-classic-1.2.3.jar
  + A module for the logging framework.
* logback-core-1.2.3.jar
  + core module of logback.
* mongo-java-driver-3.11.2.jar

java driver that allows java apps to interact with mongodb databases.

* snakeyaml-1.25.jar
  + A YAML parser and emitter for Java.
* spring-boot-2.2.4.RELEASE.jar
  + Core spring boot framework
* spring-boot-starter-web-2.2.4.RELEASE.jar
  + Starter module for spring boot that builds web apps and includes spring mvc.
* spring-core-5.2.3.RELEASE.jar
  + core module of the spring framework
* Spring-expression-5.2.3.RELEASE.jar
  + Spring expression language that allows querying and the manipulation of object graphs.
* spring-web-5.2.3.RELEASE.jar
  + core web functionality for spring
* spring-webmvc-5.2.3.RELEASE.jar
  + spring web mvc module where mvc is model view controller.
* tomcat-embed-core-9.0.30.jar
  + core part of tomcat web server and servlet container.
* tomcat-embed-websocket-9.0.30.jar
  + websocket support module for tomcat.

## Analyze Results

* hibernate-validator-6.0.18.Final.jar
  + Keep this up to date to avoid bug fixes, update to a newer version.
* jackson-databind-2.10.2.jar
  + Stack overflow can happen when parsing nested XML docs, ensure Jackson is used solely for JSON data binding.
* log4j-api-2.12.1.jar
  + Has vulnerabilities on remote code execution, use a higher version where this issue has been fixed.
* Logback-classic-1.2.3.jar
  + Have a cve that can be exploited if the system uses vulnerable configs, so monitoring updates for logback is critical to avoid this issue.
* logback-core-1.2.3.jar
  + ensure ldap is properly secured.
* mongo-java-driver-3.11.2.jar
  + ensure all mongodb connections are secured with ssl or tls encryption.
* snakeyaml-1.25.jar
  + insecure deseriwalization when parsing yaml input. Ensure that solely authorized users can modify or read these yaml files.
* spring-boot-2.2.4.RELEASE.jar
  + remote code execution can happen, upgrade spring boot and core to a newer version.
* spring-boot-starter-web-2.2.4.RELEASE.jar
  + follow the spring boot upgrade.
* spring-core-5.2.3.RELEASE.jar
  + upgrade to a newer release.
* Spring-expression-5.2.3.RELEASE.jar
  + Nothing to change besides compatibility with new upgrade.
* spring-web-5.2.3.RELEASE.jar
  + needs upgraded.
* spring-webmvc-5.2.3.RELEASE.jar
  + needs upgraded.
* tomcat-embed-core-9.0.30.jar
  + apache jserv protocol can be an issue, either disable ajp or secure the connector using firewalls.
* tomcat-embed-websocket-9.0.30.jar
  + needs more security using firewalls.

1. Dependency-check tools are used to scan a project and use its dependencies against databases with vulnerabilities. These tools are great for identifying potential security risks, but sometimes they report vulnerabilities that do not actually pose a threat (which happens when I am coding allll the time). This is due to non-vulnerable configurations that are linked to optional features or settings that are not turned on in the project, along with mismatches in library usage. A tool may flag a specific version of a library when the project could be using a different version or might not use the feature of the library that is vulnerable. By filtering out these false positives, the vulnerabilities can be reported more accurately, so the dependency reports show real, relevant security issues.