# 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

I ran the code after installing the plugin and and some difficulty figuring it out and having patientce for the database to download, but afterwhile I was successful.

A screenshot of a computer

Description automatically generated

## Document Results

Here is a copy of the successful results from running Maven.

A screenshot of a computer

Description automatically generated

## Analyze Results

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The OWASP Dependency-Check scan identified several critical and high-severity vulnerabilities across core libraries used in the project. These include:

Spring Boot 2.2.4 / Spring Framework 5.2.3CVEs: *CVE-2022-22965 (Spring4Shell)*, *CVE-2023-20873*, and moreThese are remote code execution and expression injection vulnerabilities.

Jackson Databind 2.10. CVEs: *CVE-2020-25649*, *CVE-2022-42003*, *CVE-2023-35116* Known for deserialization vulnerabilities that can allow attackers to execute arbitrary code if untrusted data is processed.

Hibernate Validator, Logback, Log4j, MongoDB Driver, and SnakeYAML. Each had multiple vulnerabilities related to unsafe input handling, logging exposure, or deserialization issues.

To address the vulnerabilities identified in the dependency check, the most effective strategy is to upgrade the outdated libraries to their latest secure versions. The Spring Boot and Spring Framework components should be updated to at least version. The Jackson Databind library should be upgraded to a higher version to mitigate multiple vulnerabilities. Similarly, the logback logging libraries should be updated to patched versions to prevent information leakage and code injection risks. Lastly, the MongoDB Java Driver should be replaced with a modern and secure version.