# CS 305 Module Two Coding Assignment

Christopher Gauthier

## 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

In the dependency review, 20 dependencies were identified as vulnerable, with 10 being critical. Though upon further review 12 are likely false positives based on the false positive guide outlined in the dependency-check article: ”How to Read the Report” (Long, 2025)

I will focus on the 12 dependencies within the flagged report.

Tomcat-embed-websocket-9.0.30.jar

CVE 2020-1938, CVE 2025-48988

Summary: Tomcat websocket had issues with AJP and potential RCE

Tomcat-embed-core-9.0.30.jar

CVE 2023-42795

Summary: incomplete cleanup could cause information leakage between requests

Spring-webmvc-5.2.3.RELEASE.jar

CVE 2022-22965

Summary: if running on JDK9+ may be vulnerable to RCE via data binding.

Spring-web-5.2.3.RELEASE.jar

Multiple – see Spring Framework

Summary: inherits CVE through Spring Framework components

Spring-expression-5.2.3.RELEASE.jar

CVE 2023-20861, CVE 2022-22950, CVE 2023-20863

Summary: DoS and SpEL injection issues in expression handling

Spring-core-5.2.3.RELEASE.jar

See Spring Framework

Spring-context-5.2.3.RELEASE.jar

See Spring Framework

Snakeyaml-1.25.jar

Past versions CVE 2022-25857

Sumamry: pre 1.31 are vulnerable to DoS due to missing nested depth limitations.

## Analyze Results

After reviewing the results, the following actions should be taken. First, remove explicit child dependency version declarations in the pom.xml file. This ensures that when the parent dependency is updated, all child dependencies are updated and compatible as well. Of the flagged dependencies, upgrading Spring Framework to 5.2.24 or 5.3.x would ensure updated fixes and practices are implemented. Second, updating Tomcat to 9.0.81 or later will resolve the CVE’s mentioned above. Finally, updating Snakeyami to 2.0 or later will ensure previously mentioned issues and exploits are patched.

References:

Long, J. (2025, February 16). *How to read the report*. OWASP Dependency-Check. <https://jeremylong.github.io/DependencyCheck/general/thereport.html>