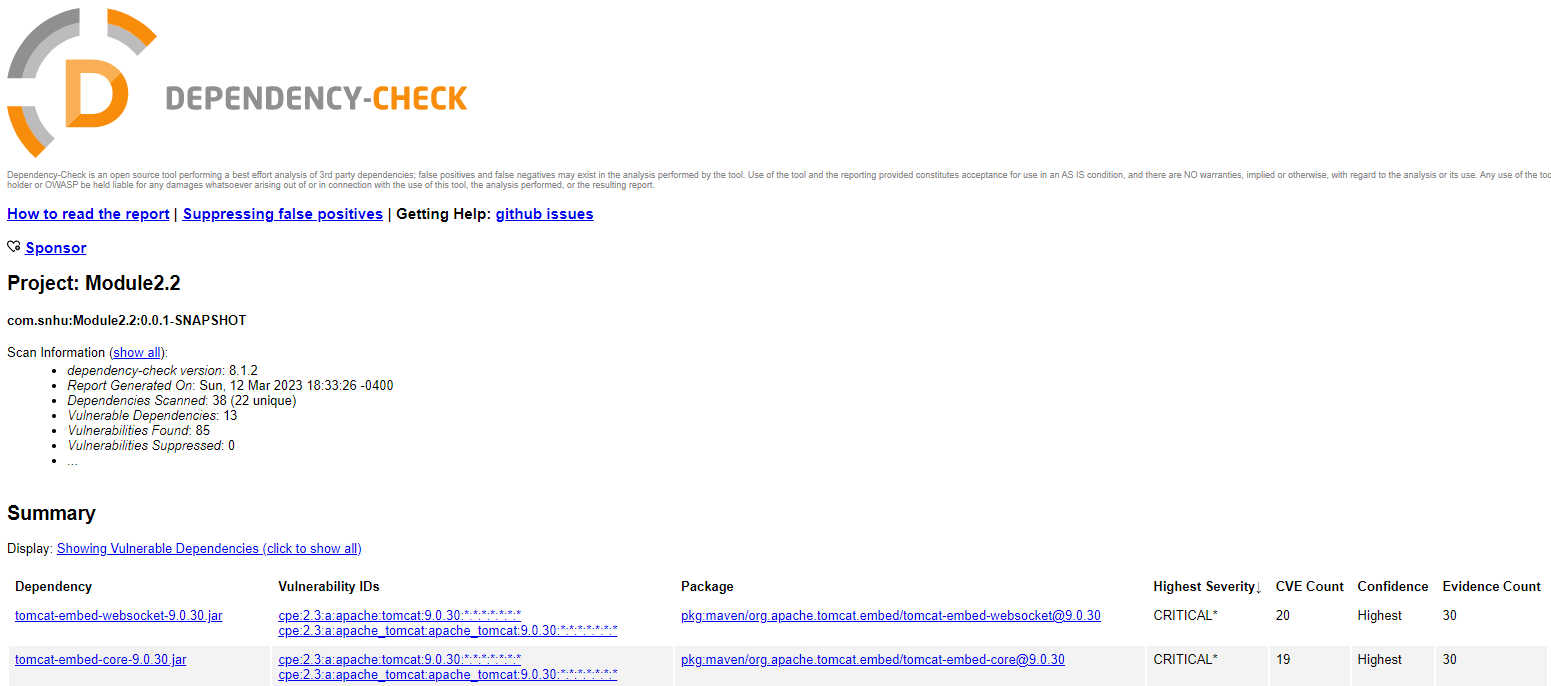
|  |
| --- |
| CS 305 Software Security |
| 2-2 Coding Assignment: Static Testing |
| Emily Wood |

|  |
| --- |
| emily.wood7@snhu.edu  3-12-2023 |

# CS 305 Module Two Coding Assignment Template

## Run Dependency Check



## Document Results

* Dependency: tomcat-embed-websocket-9.0.30.jar  
  Severity: Critical  
  CVE Count: 20  
  Description: Core Tomcat implementation
* Dependency: tomcat-embed-core-9.0.30.jar  
  Severity: Critical  
  CVE Count: 19  
  Description: Core Tomcat implementation
* Dependency: spring-webmvc-5.2.3.RELEASE.jar  
  Severity: Critical  
  CVE Count: 9  
  Description: Spring Web MVC
* Dependency: spring-web-5.2.3.RELEASE.jar  
  Severity: Critical  
  CVE Count: 10  
  Description: Spring Web
* Dependency: spring-core-5.2.3.RELEASE.jar  
  Severity: Critical  
  CVE Count: 9  
  Description: Spring Core
* Dependency: snakeyaml-1.25.jar  
  Severity: High  
  CVE Count: 8  
  Description: YAML 1.1 parser and emitter for Java
* Dependency: spring-boot-starter-web-2.2.4.RELEASE.jar  
  Severity: High  
  CVE Count: 1  
  Description: Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container
* Dependency: spring-boot-2.2.4.RELEASE.jar  
  Severity: High  
  CVE Count: 1  
  Description: Spring Boot
* Dependency: jackson-databind-2.10.2.jar  
  Severity: High  
  CVE Count: 4  
  Description: General data-binding functionality for Jackson: works on core streaming API
* Dependency: mongo-java-driver-2.4.jar  
  Severity: Medium  
  CVE Count: 1  
  Description: Java Driver for MongoDB
* Dependency: logback-core-1.2.3.jar  
  Severity: Medium  
  CVE Count: 1  
  Description: logback-core module
* Dependency: hibernate-validator-6.0.18.Final.jar  
  Severity: Medium  
  CVE Count: 1  
  Description: Hibernate's Bean Validation (JSR-380) reference implementation.
* Dependency: log4j-api-2.12.1.jar  
  Severity: Low  
  CVE Count: 1  
  Description: The Apache Log4j API

## Analyze Results

Many of these vulnerabilities were found to exist with earlier and unsupported versions. Using the latest version dependencies should eliminate the vulnerabilities.

False positives can show up based on old databases. They also may not be exploitable based on the environment used. The software we are creating may be using the latest version of dependencies, but because the name is still connected to an old vulnerability, it will show up. This a good reason to suppress any false positives.