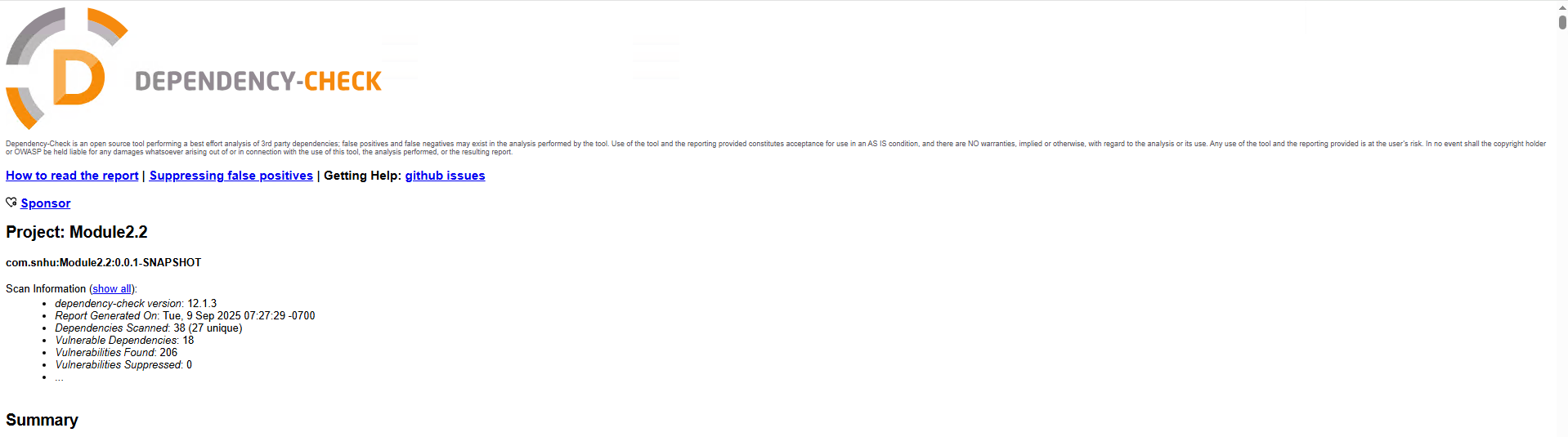
# CS 305 Module Two Coding Assignment Template

## 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



## Document Results

Name: tomcat-embed-websocket-9.0.30.jar

Description: Core Tomcat implementation

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

Name: tomcat-embed-core-9.0.30.jar

Description: Core Tomcat implementation

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

Name: spring-webmvc-5.2.3.RELEASE.jar

Description: Spring Web MVC

License: Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0

Name: spring-web-5.2.3.RELEASE.jar

Description: Spring Web

License: Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0

Name: spring-expression-5.2.3.RELEASE.jar

Description: Spring Expression Language (SpEL)

License: Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0

Name: spring-core-5.2.3.RELEASE.jar

Description: Spring Core

License: Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0

Name: spring-context-5.2.3.RELEASE.jar

Description: Spring Context

License: Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0

Name: spring-boot-starter-web-2.2.4.RELEASE.jar

Description: Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container

License: Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0

Name: spring-boot-2.2.4.RELEASE.jar

Description: Spring Boot

License: Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0

Name: spring-aop-5.2.3.RELEASE.jar

Description: Spring AOP

License: Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0

Name: 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

Name: jackson-core-2.10.2.jar

Description: Core Jackson processing abstractions (aka Streaming API), implementation for JSON

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

Name: logback-core-1.2.3.jar

Description: logback-core module

License: http://www.eclipse.org/legal/epl-v10.html, http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html

Name: logback-classic-1.2.3.jar

Description: logback-classic module

License: http://www.eclipse.org/legal/epl-v10.html, http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html

Name: 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

Name: 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

Name: mongo-java-driver-2.4.jar

Description: Java Driver for MongoDB

License: The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt

Name: log4j-api-2.12.1.jar

Description: The Apache Log4j API

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

## Analyze Results

Filtering false positives is important as dependency check tools often flag vulnerabilities based only on version numbers without confirming if the affected code is actually used. If every alert is treated as critical, development teams would waste time patching issues that may not pose real risk to the application. This can introduce unnecessary change risk, since upgrading libraries that are not truly vulnerable may break functionality. Reducing false positives help teams prioritize real, exploitable vulnerabilities, making sure that resources are focused where they have the greatest impact. By filtering out false positives, organizations maintain accuracy in their security posture and can focus on genuine threats. Below is the details on the vulnerabilities that were detected and the best course of action to address them.

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

This version is vulnerable to HTTP/2 denial-of-service flaws in older Tomcat releases. The best remediation is to upgrade to a newer version and to disable the AJP connector if it is not required.

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

The Tomcat core module is vulnerable to HTTP/2 vulnerabilities. Remediation requires upgrading to a newer version and applying AJP restrictions.

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

This outdated Spring MVC version is exposed to critical remote code execution vulnerabilities. The remediation is to upgrade to Spring Framework 6.x or higher.

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

The Spring Web module in this version is unsupported. The solution is to upgrade to Spring Framework 6.x bundled with Spring Boot 3.x.

**spring-expression-5.2.3.RELEASE.jar**

This version of Spring Expression Language has known security flaws tied to the outdated Spring Framework. Remediation is achieved by upgrading to Spring Framework 6.x.

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

The Spring Core library is outdated and unsupported, making it susceptible to vulnerabilities. The recommended remediation is to upgrade to Spring 6.x through Spring Boot 3.x.

**spring-context-5.2.3.RELEASE.jar**

This version of Spring Context is no longer supported and may be affected by vulnerabilities like Spring4Shell. Remediation involves upgrading to Spring Framework 6.x.

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

The starter inherits vulnerabilities from Spring and Tomcat. The remediation is to upgrade to Spring Boot 3.x, which includes fixes for all critical components.

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

This core Spring Boot version is end-of-life and exposed to multiple CVEs. The recommendation is upgrading to Spring Boot 3.x.

**spring-aop-5.2.3.RELEASE.jar**

This version is outdated and is vulnerable in this release set. The remediation is to upgrade to Spring Framework 6.x.

**snakeyaml-1.25.jar**

This version contains remote code execution vulnerabilities such as CVE-2017-18640 and CVE-2022-1471. The remediation is to upgrade to SnakeYAML 2.x.

**jackson-core-2.10.2.jar**

The Jackson Core library is vulnerable to deserialization issues, including CVE-2020-36518. The remediation is to upgrade to Jackson 2.17.x or later.

**jackson-databind-2.10.2.jar**

Jackson Databind is known for many deserialization-based flaws, such as CVE-2022-42003. The recommended remediation is to upgrade to Jackson 2.17.x or later.

**logback-core-1.2.3.jar**

This version is affected by CVE-2021-42550, which allows malicious configuration loading that could lead to code execution. The remediation is to upgrade to Logback 1.4.14 or newer and make logging configuration files read-only.

**logback-classic-1.2.3.jar**

The Logback Classic module inherits the same flaws as logback-core, including denial-of-service issues such as CVE-2023-6378. The remediation is to upgrade to Logback 1.4.14 or later.

**hibernate-validator-6.0.18.Final.jar**

This outdated version of Hibernate Validator may be vulnerable to denial-of-service and is no longer maintained. The remediation is to upgrade to a later version, which requires Java 11 or later.

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

This very old MongoDB Java driver lacks TLS, authentication, and cluster support found in modern versions, creating both security and performance risks. The remediation is to upgrade to MongoDB Java Driver 5.x or the latest version.

**log4j-api-2.12.1.jar**

This version is is obsolete and may cause security or compatibility issues. The remediation is to upgrade to Log4j API 2.23.x.