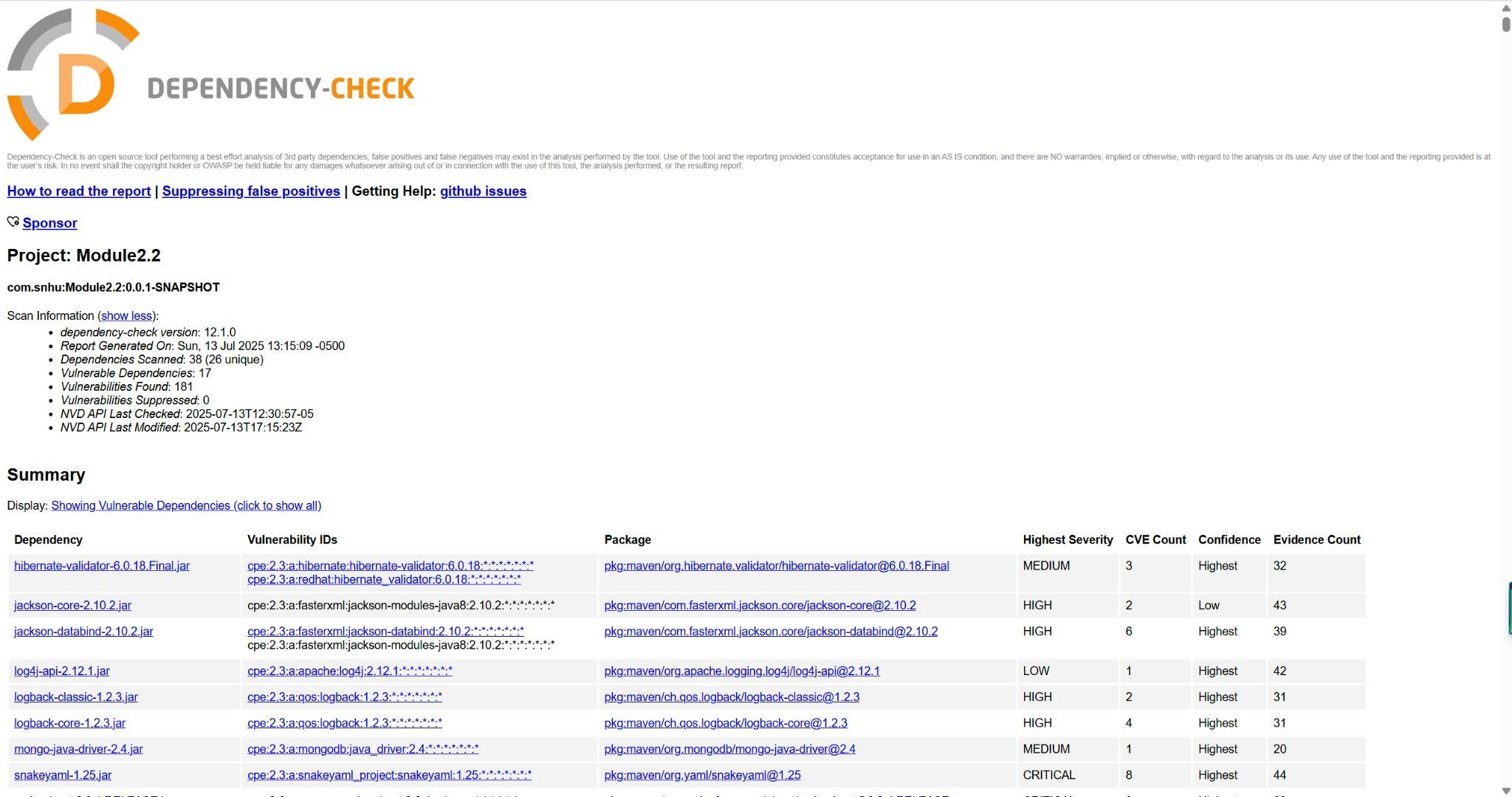
# CS 305 Module Two Coding Assignment Template

## 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

* hibernate-validator-6.0.18.Final.jar

Description: Hibernate's Bean Validation (JSR-380) reference implementation.

* Jackson-core-2.10.2.jar

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

* Jackson-databind-2.10.2.jar

Description: General data-binding functionality for Jackson: works on core streaming API

* Log4j-api-2.12.1.jar

Description: The Apache Log4j API

* Logback-classic-1.2.3.jar

Description: logback-classic module

* Logback-core-1.2.3.jar

Description: logback-core module

* Mongo-java-driver-2.4.jar

Description: Java Driver for MongoDB

* Snakeyaml-1.25.jar

Description: YAML 1.1 parser and emitter for Java

* spring-boot-2.2.4.RELEASE.jar

Description: Spring Boot

* 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

* spring-context-5.2.3.RELEASE.jar

Description: Spring Context

* spring-core-5.2.3.RELEASE.jar

Description: Spring Core

* spring-expression-5.2.3.RELEASE.jar

Description: Spring Expression Language (SpEL)

* spring-web-5.2.3.RELEASE.jar

Description: Spring Web

* spring-webmvc-5.2.3.RELEASE.jar

Description: Spring Web MVC

* Tomcat-embed-core-9.0.30.jar

Description: Core Tomcat implementation

* tomcat-embed-websocket-9.0.30.jar

Description: Core Tomcat implementation

## Analyze Results

* hibernate-validator-6.0.18.Final.jar

Summary: A flaw was found in hibernate-validator's 'isValid' method in the org.hibernate.validator.internal.constraintvalidators.hv.SafeHtmlValidator class, which can be bypassed by omitting the tag ending in a less-than character. Browsers may render an invalid html, allowing HTML injection or Cross-Site-Scripting (XSS) attacks.

A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.

Solution: Upgrade to Latest Version.

* Jackson-core-2.10.2.jar

Summary: Deserialization of malicious input with extremely large values in the nanoseconds field of a time value.

Solution: Upgrade to Latest Version

* Jackson-databind-2.10.2.jar

Summary: A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.

Solution: Upgrade to latest version

* Log4j-api-2.12.1.jar

Summary: Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender. Fixed in Apache Log4j 2.12.3 and 2.13.1

Solution: upgrade to latest version

* Logback-classic-1.2.3.jar

Summary: In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.

Solution: upgrade to latest version

* Logback-core-1.2.3.jar

Summary: A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.

Solution: upgrade to latest version

* Mongo-java-driver-2.4.jar

Summary: Lack of TLS/SSL support: Early versions had limited or no support for secure connections. No hostname verification: Vulnerable to man-in-the-middle (MITM) attacks.Java Driver for MongoDB

Solution: upgrade to latest version

* Snakeyaml-1.25.jar

Summary: The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, a related issue to CVE-2003-1564.

Solution: Upgrade to latest version

* spring-boot-2.2.4.RELEASE.jar

Summary: spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer

Solution: upgrade to latest version

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

Summary: spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer

Solution: upgrade to latest version

* spring-context-5.2.3.RELEASE.jar

Summary: In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

Solution: upgrade to latest version

* spring-core-5.2.3.RELEASE.jar

Summary: In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

Solution: upgrade to latest version

* spring-expression-5.2.3.RELEASE.jar

Summary: In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

Solution: upgrade to latest version

* spring-web-5.2.3.RELEASE.jar

Summary: In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

Solution: upgrade to latest version

* spring-webmvc-5.2.3.RELEASE.jar

Summary: In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

Solution: upgrade to latest version

* Tomcat-embed-core-9.0.30.jar

Summary: Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.

Solution: upgrade to latest version

* tomcat-embed-websocket-9.0.30.jar

Summary: Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.

Solution: upgrade to latest version

* Also consider why you should filter false positives from the dependency-check tool: Filtering false positives from OWASP Dependency-Check is crucial for efficient and effective security analysis. False positives, vulnerabilities flagged by the tool that don't actually exist in the specific project's usage of a library, lead to wasted time and resources, potentially delaying or even preventing the resolution of real security issues. By filtering these out, teams can focus on genuine vulnerabilities and improve the overall security posture of their projects.