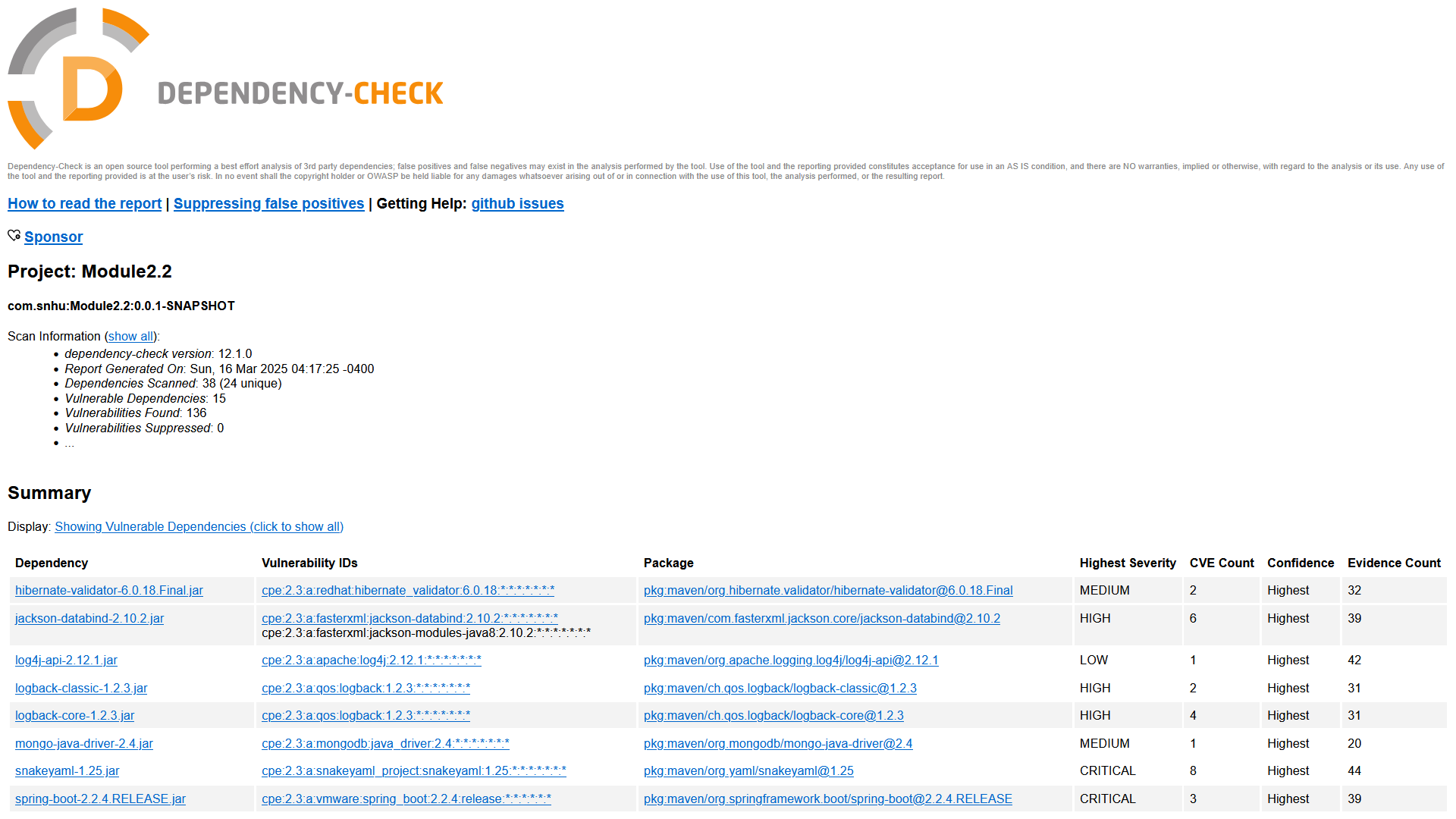
# CS 305 Module Two Coding Assignment Template

## 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

Below is a screenshot of the dependency check. The check scanned 38 dependencies and found 15 vulnerable dependencies.



## Document Results

* Hibernate-validator-6.0.18.final.jar
  + Hibernate's Bean Validation (JSR-380) reference implementation
* Jackson-databind-2.10.2.jar
  + General data-binding functionality for Jackson: works on core streaming API
* Log4j-api-2.12.1.jar
  + The Apache Log4j API
* Logback-classic-1.2.3.jar
  + Logback-classic module
* Logback-core-1.2.3.jar
  + Logback-core module
* Mongo-java-driver-2.4.jar
  + Java Driver for MongoDB
* Snakeyaml-1.25.jar
  + YAML 1.1 parser and emitter for Java
* Spring-boot-2.2.4.RELEASE.jar
  + Spring Boot
* Spring-boot-starter-web-2.2.4.RELEASE.jar
  + Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container.
* Spring-core-5.2.3.RELEASE.jar
  + Spring Core
* Spring-expression-5.2.3.RELEASE.jar
  + Spring Expression Language(SpEL)
* Spring-web-5.2.3.RELEASE.jar
  + Spring Web
* Spring-webmvc-5.2.3.RELEASE.jar
  + Spring Web MVC
* Tomcat-embeded-core-9.0.30.jar
  + Core Tomcat implementation
* Tomcat-embedded-websocket-9.0.39.jar
  + Core Tomcat implementation

## Analyze Results

While running a dependency check, false positives may become apparent. False positives may not pose a security risk, so they should be filtered from results as they can take time and resources away from more serious vulnerabilities.

* Hibernate-validator-6.0.18.Final.jar
  + A flaw was found in the “isValid”method, which could allow HTML injection, or Cross-Site-scripting attacks
* Jackson-databind-2.10.2.jar
  + Allows Java StackOverflow exception and denial of service via large depth of nested objects.
* Log4j-api-2.12.1.jar
  + Improper validation of certificate with host mismatch in Apache Log4j SMTP appender could allow SMTPS connection to be intercepted by man-in-the-middle attack.
* Logback-classic-1.2.3.jar
* Logback-core-1.2.3.jar
  + ACE vulnerability in JaninoEventEvaluator allows attacker to execute arbitrary code by compromising an existing logback configuration file or by injecting an environment variable before program execution
  + Server-side Request Forgery in SaxEventRecorder allows an attacker to forge requests by compromising logback configurations in XML.
* Mongo-java-driver-2.4.jar
  + Specific versions of the Java driver that supports client-side field level encryption fail to perform correct host name verification on the KMS servers certificate. This, in combination with a privileged network position active MITM attack could result in interception of traffic between Java driver and the KMS service, rendering field level encryption ineffective.
* Snakeyaml-1.25.jar
  + SnakeYaml’s Constructor() class does not restrict types which can be instasiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution.
  + Missing depth limitation for collections could lead to denial of service
  + Using snakeyaml to parse untrusted files may lead to denial of service by stackoverflow.
* Spring-boot02.2.4.RELEASE.jar
  + Unsupported versions be susceptible to security bypass, temporary directory hijacking, and denial of service attack
* Spring-boot-starter-web-2.2.4.RELEASE.jar
  + Unsupported versions be susceptible to security bypass, temporary directory hijacking, and denial of service attack
* Spring-core-5.2.3.RELEASE.jar
  + May be vulnerable to remote code execution via data binding.
  + WebFlux application is vulnerable to a privilege escalation
  + Protections against RFD attacks may be bypassed.
  + Vulnerable to Denial of Service attacks by authenticated user.
  + Possible for a user to provide specially crafted SpEL expression that may cause Denial of Service.
* Spring-expression-5.2.3.RELEASE.jar
  + May be vulnerable to remote code execution via data binding
  + WebFlux application is vulnerable to a privilege escalation
  + Protections against RFD attacks may be bypassed.
  + Vulnerable to Denial of Service attacks by authenticated user.
  + Possible for a user to provide specially crafted SpEL expression that may cause Denial of Service.
* Spring-web-5.2.3.RELEASE.jar
  + May be vulnerable to remote code execution via data binding
  + Application that parse ETags from “If-Match” or “If-Non-Match”request headers are vulnerable to denial or service attacks.
  + Vulnerable to privilege escalation
  + Spring MVC controller methods with an @RequestBody byte[] method parameter are vulnerable to a denial of service attack.
  + Protections against RFD attacks may be bypassed.
  + Possible for a user to provide specially crafted SpEL expressions that may cause denial of service
* Spring-webmvc-5.2.3.RELEASE.jar
  + May be vulnerable to remote code execution via data binding
  + Application that parse ETags from “If-Match” or “If-Non-Match”request headers are vulnerable to denial or service attacks.
  + Vulnerable to privilege escalation
  + Spring MVC controller methods with an @RequestBody byte[] method parameter are vulnerable to a denial of service attack.
  + Protections against RFD attacks may be bypassed.
  + Possible for a user to provide specially crafted SpEL expressions that may cause denial of service
  + Application serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks.
* Tomcat-embed-core-9.0.30.jar
  + When using the Apache JServe Protocol, care must be taken when trusting incoming connections to Apache Tomcat.
  + A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrant HTTP/2 connections, the server could become unresponsive.
  + An OutOfMemoryException could be triggered if a sufficient number of requests for upgrade to HTTP/2 due to a missing release of HTTP/1.1 processor. This could lead to a Denial of Service.
  + The payload length in a WebSocket frame was not correctly validated. This could trigger an infinite loop.
  + Apache Tomcat could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. This could lead to an information leak between requests.
  + When responding to new h2c connection requests, request headers could be duplicated and a limited amount of request body from one request to another could expose sensitive information to an unauthorized actor
  + A specially crafted packet could be use to trigger and infinite loop, resulting in a denial of service.
* Tomcat-embed-websocket-9.0.30.jar
  + When using the Apache JServe Protocol, care must be taken when trusting incoming connections to Apache Tomcat.
  + A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrant HTTP/2 connections, the server could become unresponsive.
  + An OutOfMemoryException could be triggered if a sufficient number of requests for upgrade to HTTP/2 due to a missing release of HTTP/1.1 processor. This could lead to a Denial of Service.
  + The payload length in a WebSocket frame was not correctly validated. This could trigger an infinite loop.
  + Apache Tomcat could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. This could lead to an information leak between requests.
  + When responding to new h2c connection requests, request headers could be duplicated and a limited amount of request body from one request to another could expose sensitive information to an unauthorized actor
  + A specially crafted packet could be use to trigger and infinite loop, resulting in a denial of service.