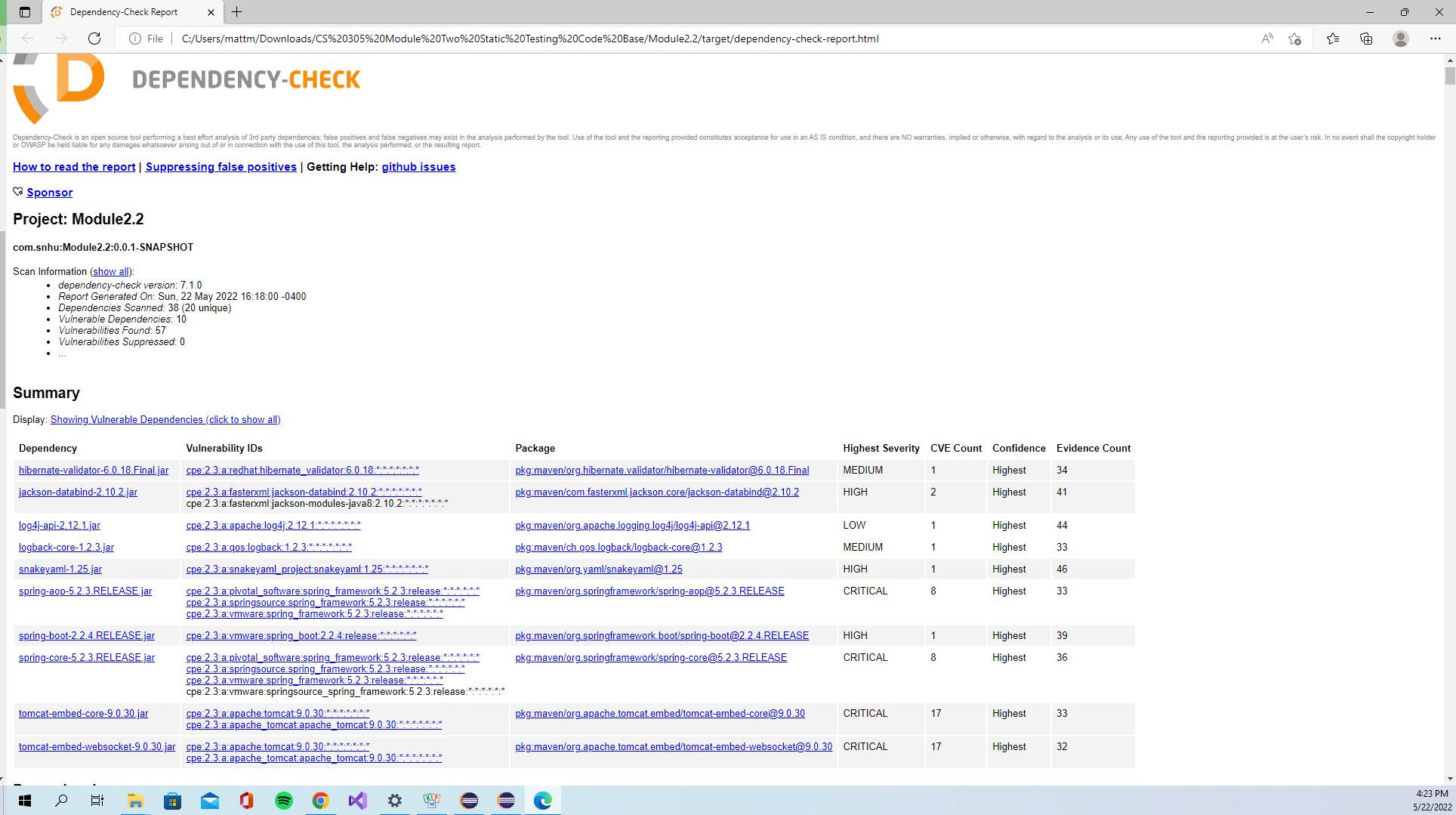
# CS 305 Module Two Static Testing Summary Template

## Instructions

Replace the bracketed text with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

### Run Dependency Check



### Document Results

* hibernate-validator-6.0.18.Final.jar
  + Hibernate's Bean Validation (JSR-380) reference implementation
  + A flaw was found in hibernate-validator 6.1.2.Final. A bug in the interpolation of constraint error messages code enables invalid EL expressions to be evaluated as if they were valid. This bug enables attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.
* jackson-databind-2.10.2.jar
  + General data-binding functionality for Jackson: works on core streaming API
  + jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.
* log4j-api-2.12.1.jar
  + The Apache Log4j API
  + Apache Log4j2, a Java Logging Framework, is vulnerable to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code.
* logback-core-1.2.3.jar
  + logback-core module
  + 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.
* snakeyaml-1.25.jar
  + YAML 1.1 parser and emitter for Java
  + The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564.
* spring-aop-5.2.3.RELEASE.jar
  + Spring AOP
  + In Spring Framework versions 5.3.0 - 5.3.16, 5.2.0 - 5.2.19, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.
* spring-boot-2.2.4.RELEASE.jar
  + Spring Boot
  + In Spring Framework versions 5.3.0 - 5.3.16, 5.2.0 - 5.2.19, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.
* spring-core-5.2.3.RELEASE.jar
  + Spring Core
  + In Spring Framework versions 5.3.0 - 5.3.16, 5.2.0 - 5.2.19, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.
* tomcat-embed-core-9.0.30.jar
  + Core Tomcat implementation
  + The documentation for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.
* tomcat-embed-websocket-9.0.30.jar
  + Core Tomcat implementation
  + The documentation for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.

### Interpret Results

* hibernate-validator-6.0.18.Final.jar
  + This flaw is fixed in versions of hibernate-validator 6.0.20.Final and newer.
* jackson-databind-2.10.2.jar
  + The recommended mitigation for this vulnerability is to upgrade the jackson-databind package being used.
* log4j-api-2.12.1.jar
  + This issue is fixed by limiting JNDI data source names to the java protocol. It is also recommended to upgrade the apache-log4j2 package being used.
* logback-core-1.2.3.jar
  + This vulnerability can be mitigated by upgrading to a version of logback newer than 1.2.7
* snakeyaml-1.25.jar
  + This vulnerability can be mitigated by upgrading snakeyaml to 1.26 in order to mitigate CVE-2017-18640
* spring-aop-5.2.3.RELEASE.jar
  + This issue can be mitigated accordingly: 5.3.x users should upgrade to 5.3.17+. 5.2.x users should upgrade to 5.2.20+
* spring-boot-2.2.4.RELEASE.jar
  + This vulnerability is patched in versions v2.2.11.RELEASE or later.
* spring-core-5.2.3.RELEASE.jar
  + This issue can be mitigated accordingly: 5.3.x users should upgrade to 5.3.17+. 5.2.x users should upgrade to 5.2.20+
* tomcat-embed-core-9.0.30.jar
  + Users running clustering over an untrusted network who require full protection should switch to an alternative solution such as running the clustering communication over a VPN.
* tomcat-embed-websocket-9.0.30.jar
  + Users running clustering over an untrusted network who require full protection should switch to an alternative solution such as running the clustering communication over a VPN.

It is important to filter false positives from the dependency check because a high false positive rate can lead to legitimate findings being hidden by irrelevant ones. This can lead to delays in software development or worse yet, having legitimate vulnerabilities slip through the analysis of the dependency check.