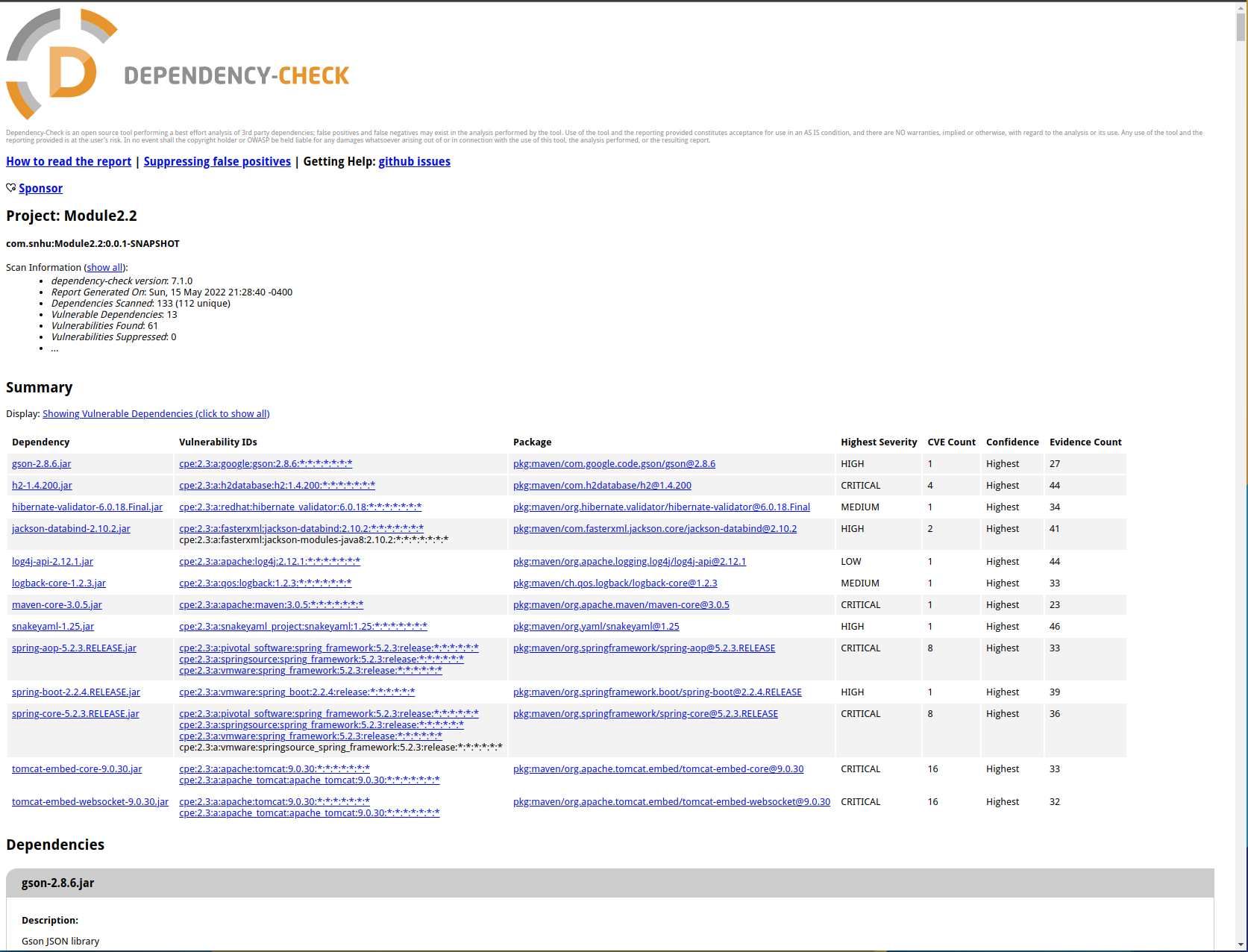
# CS 305 Module Two Static Testing Summary Template

## 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

* gson-2.8.6.jar  
  Description: Gson JSON library  
  CVE-2022-25647, CVE-2022-23221, CVE-2021-23463
* h2-1.4.200.jar  
  Description: H2 Database Engine  
  CVE-2021-42392
* hibernate-validator-6.0.18.Final.jar  
  Description: Hibernate's Bean Validation (JSR-380) reference implementation.  
  CVE-2020-10693
* jackson-databind-2.10.2.jar  
  Description: General data-binding functionality for Jackson: works on core streaming API  
  CVE-2020-25649, CVE-2020-36518
* log4j-api-2.12.1.jar  
  Description: The Apache Log4j API  
  CVE-2020-9488
* logback-core-1.2.3.jar  
  Description: logback-core module  
  CVE-2021-42550
* maven-core-3.0.5.jar  
  Description: Maven Core classes.  
  CVE-2021-26291
* snakeyaml-1.25.jar  
  Description: YAML 1.1 parser and emitter for Java  
  CVE-2017-18640
* spring-aop-5.2.3.RELEASE.jar  
  Description: Spring AOP  
  CVE-2016-1000027, CVE-2022-22965, CVE-2021-22118, CVE-2020-5421, CVE-2022-22950, CVE-2022-22968, CVE-2021-22060, CVE-2021-22096
* spring-boot-2.2.4.RELEASE.jar  
  Description: Spring Boot  
  CVE-2022-27772
* spring-core-5.2.3.RELEASE.jar  
  Description: Spring Core  
  CVE-2016-1000027, CVE-2022-22965, CVE-2021-22118, CVE-2020-5421, CVE-2022-22950, CVE-2022-22968, CVE-2021-22060, CVE-2021-22096
* tomcat-embed-core-9.0.30.jar  
  Description: Core Tomcat implementation  
  CVE-2020-1938, CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25122, CVE-2021-41079, CVE-2020-9484, CVE-2021-25329, CVE-2021-30640, CVE-2021-24122, CVE-2021-33037, CVE-2019-17569, CVE-2020-1935, CVE-2020-13943
* tomcat-embed-websocket-9.0.30.jar  
  Description: Core Tomcat implementation  
  CVE-2020-1938, CVE-2020-8022, CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25122, CVE-2021-41079, CVE-2020-9484 , CVE-2021-25329, CVE-2021-30640, CVE-2021-24122, CVE-2021-33037, CVE-2019-17569, CVE-2020-1935, CVE-2020-13943

### Interpret Results

* The best solution for addressing the vulnerabilities within the dependencies is to update them to the latest version. This will patch most, if not all CVE’s within the Dependency-Check Report.
* False positives happen often, what this means is that the report may have found a CVE that has already been patched. Filtering it from the report will help you focus on the true vulnerabilities, rather than ones already patched.