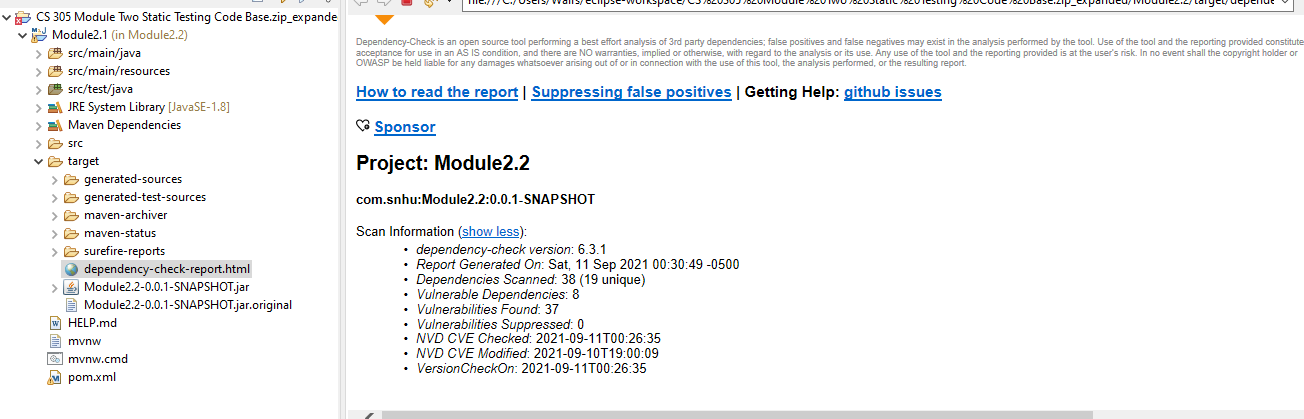
# CS 305 Module Two Static Testing Summary Template

## 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  
  Description: Hibernate's Bean Validation (JSR-380) reference implementation.  
  License: <http://www.apache.org/licenses/LICENSE-2.0.txt>
* 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>
* log4j-api-2.12.1.jar  
  Description: The Apache Log4j API  
  License: <https://www.apache.org/licenses/LICENSE-2.0.txt>
* 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>
* spring-aop-5.2.3.RELEASE.jar  
  Description: Spring AOP  
  License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>
* spring-core-5.2.3.RELEASE.jar  
  Description: Spring Core  
  License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>
* 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>
* 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>

### Interpret Results

* While running a dependency check some false positives may become evident. Though these may provide insight into your programs dependencies and may not indicate an immediate security risk they’re important to explore. Filtering them can help to bring attention to larger more serious security risks within your program. The majority of these security bugs can be corrected to upgrading to the current version of software available.
* hibernate-validator-6.0.18.Final.jar  
  Summary: 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.  
  Remediation: You can pass user input as an expression variable by unwrapping the context to HibernateConstraintValidatorContext. Or upgrade to current 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.  
  Remediation: Upgrade to 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.  
  Remediation: Previous versions can set the system property mail.smtp.ssl.checkserveridentity to true to globally enable hostname verification for SMTPS connections.
* snakeyaml-1.25.jar  
  Summary: The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564.  
  Remediation: update to the latest snakeyaml
* spring-aop-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.  
  Remediation: Updated to latest version.
* spring-core-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.  
  Remediation: Update to latest version.
* tomcat-embed-core-9.0.30.jar  
  Summary: Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.  
  Remediation: Update to current version.
* tomcat-embed-websocket-9.0.30.jar
* Summary: Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.  
  Remediation: Upgrade to current version.