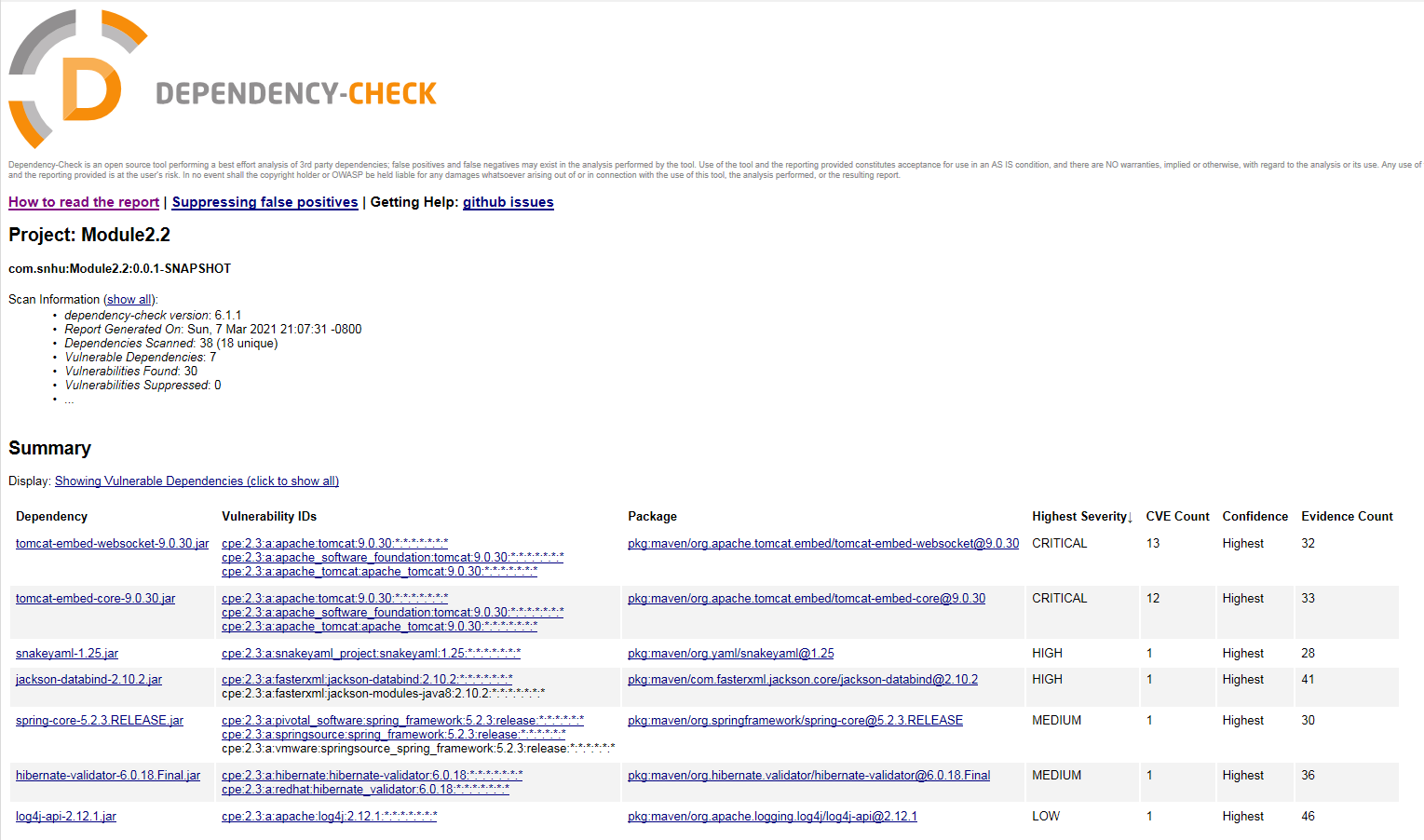
# CS 305 Module Two Static Testing Summary Template

## 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

* [Document the results from the dependency check here. Be sure to identify the codes and descriptions of the dependencies found by including these details for each dependency.]

Vulnerable dependencies:

* [tomcat-embed-websocket-9.0.30.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l18_33157f6bc5bfd03380ebb5ac476db0600a04168d)
  + Package: [pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=6.1.1)
  + CVE / Evidence Count: 13 / 32
  + Severity: Critical
  + Description: Core Tomcat implementation
  + Vulnerability IDs: [cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Atomcat&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A9.0.30)  
    [cpe:2.3:a:apache\_software\_foundation:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_software_foundation&cpe_product=cpe%3A%2F%3Aapache_software_foundation%3Atomcat&cpe_version=cpe%3A%2F%3Aapache_software_foundation%3Atomcat%3A9.0.30)  
    [cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_tomcat&cpe_product=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat&cpe_version=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat%3A9.0.30)
* [tomcat-embed-core-9.0.30.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l16_ad32909314fe2ba02cec036434c0addd19bcc580)
  + Package: [pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=6.1.1)
  + CVE / Evidence Count: 12 / 33
  + Severity: Critical
  + Description: Core Tomcat implementation
  + Vulnerability IDs: [cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Atomcat&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A9.0.30)  
    [cpe:2.3:a:apache\_software\_foundation:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_software_foundation&cpe_product=cpe%3A%2F%3Aapache_software_foundation%3Atomcat&cpe_version=cpe%3A%2F%3Aapache_software_foundation%3Atomcat%3A9.0.30)  
    [cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_tomcat&cpe_product=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat&cpe_version=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat%3A9.0.30)
* [snakeyaml-1.25.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l13_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421)
  + Package: [pkg:maven/org.yaml/snakeyaml@1.25](https://ossindex.sonatype.org/component/pkg:maven/org.yaml/snakeyaml@1.25?utm_source=dependency-check&utm_medium=integration&utm_content=6.1.1)
  + CVE / Evidence Count: 1 / 28
  + Severity: High
  + Description: YAML 1.1 parser and emitter for Java
  + Vulnerability IDs:  [cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Asnakeyaml_project&cpe_product=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml&cpe_version=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml%3A1.25)
* [jackson-databind-2.10.2.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l4_0528de95f198afafbcfb0c09d2e43b6e0ea663ec)
  + Package: [pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=6.1.1)
  + CVE / Evidence Count: 1 / 41
  + Severity: High
  + Description: General data-binding functionality for Jackson: works on core streaming API
  + Vulnerability IDs: [cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Afasterxml&cpe_product=cpe%3A%2F%3Afasterxml%3Ajackson-databind&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson-databind%3A2.10.2)  
    cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\*
* [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l15_3734223040040e8c3fecd5faa3ae8a1ed6da146b)
  + Package: [pkg:maven/org.springframework/spring-core@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-core@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=6.1.1)
  + CVE / Evidence Count: 1 / 30
  + Severity: Medium
  + Description: Spring Core
  + Vulnerability IDs:  [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3)  
    [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3)  
    cpe:2.3:a:vmware:springsource\_spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*
* [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l2_7fd00bcd87e14b6ba66279282ef15efa30dd2492)
  + Package:  [pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final](https://ossindex.sonatype.org/component/pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final?utm_source=dependency-check&utm_medium=integration&utm_content=6.1.1)
  + CVE / Evidence Count: 1 / 36
  + Severity: Medium
  + Description: Hibernate's Bean Validation (JSR-380) reference implementation.
  + Vulnerability IDs: [cpe:2.3:a:hibernate:hibernate-validator:6.0.18:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Ahibernate&cpe_product=cpe%3A%2F%3Ahibernate%3Ahibernate-validator&cpe_version=cpe%3A%2F%3Ahibernate%3Ahibernate-validator%3A6.0.18)  
    [cpe:2.3:a:redhat:hibernate\_validator:6.0.18:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aredhat&cpe_product=cpe%3A%2F%3Aredhat%3Ahibernate_validator&cpe_version=cpe%3A%2F%3Aredhat%3Ahibernate_validator%3A6.0.18)
* [log4j-api-2.12.1.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l9_a55e6d987f50a515c9260b0451b4fa217dc539cb)
  + Package:  [pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1](https://ossindex.sonatype.org/component/pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1?utm_source=dependency-check&utm_medium=integration&utm_content=6.1.1)
  + CVE / Evidence Count: 1 / 46
  + Severity: Low
  + Description: The Apache Log4j API
  + Vulnerability IDs: [cpe:2.3:a:apache:log4j:2.12.1:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Alog4j&cpe_version=cpe%3A%2F%3Aapache%3Alog4j%3A2.12.1)

### Interpret Results

* Due to the way dependency-check collects information about the files it scans (using Analyzers), there can be false positives (primarily on the CPE, Common Platform Enumeration, values). These incorrect CPE values should be obvious; a suppression feature can be used in the report to filter false positives out from future scans.

[tomcat-embed-websocket-9.0.30.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l18_33157f6bc5bfd03380ebb5ac476db0600a04168d)

[**CVE-2019-17569**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569)

Refactoring present in Apache Tomcat 9.0.28 to 9.0.30 introduced a regression, resulting in invalid Transfer-Encoding headers being incorrectly processed. This lead to HTTP Request smuggling possibility. Solution is to upgrade apache tomcat to 9.0.31+.

[**CVE-2020-13934**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13934)

An h2c direct connection to ApacheTomcat 9.0.0.M5 to 9.0.36 did not release the HTTP/1.1 processor, after upgrading to HTTP/2. This could lead to Denial of Service and OutOfMemoryException. Solution is to upgrade apache tomcat to 9.0.37.

[tomcat-embed-core-9.0.30.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l16_ad32909314fe2ba02cec036434c0addd19bcc580)

[**CVE-2020-11996**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11996)

A sequence of specially crafted HTTP/2 requests sent to Apache Tomcat 9.0.0.M1 to 9.0.35 could trigger high CPU for several seconds, causing the server to become unresponsive. Solution: Apache-tomcat upgrade to 9.0.36.

[**CVE-2020-1938**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1938)

A critical Apache Tomcat vulnerability: “When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection.” These connections can be exploited by an attacker.

A workaround: Opening "server.xml" in a text editor and commenting out "protocol="AJP/1.3"" connector. Restart SVF services.

If AJP protocol used: Specify IP to allow access from secure server only (loop-back 127.0.0.1)

[snakeyaml-1.25.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l13_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421)

[**CVE-2017-18640**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640)

“The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564.”

Fix: Developer has fixed this in version 1.26+. Please update to that version.

[jackson-databind-2.10.2.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l4_0528de95f198afafbcfb0c09d2e43b6e0ea663ec)

[**CVE-2020-25649**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25649)

A flaw found in FasterXML Jackson Databind – entity expansion not secured properly, leaving vulnerability to XML entity attacks, risking data integrity.

Fix: Upgrading to 2.10.5.1 will solve the problem.

[spring-core-5.2.3.RELEASE.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l15_3734223040040e8c3fecd5faa3ae8a1ed6da146b)

[**CVE-2020-5421**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421)

According to NVD, CVE-2020-5421 details: “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 is to update Spring Framework to 5.2.9 or the following:

5.1.18

5.0.19

4.3.29

[hibernate-validator-6.0.18.Final.jar](file:///C:\Users\Vic\eclipse-workspace\Module2.1_Test\target\dependency-check-report.html#l2_7fd00bcd87e14b6ba66279282ef15efa30dd2492)

[**CVE-2020-10693**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-10693)

CVE-2020-10693: A flaw found in Hibernate Validator ; “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.”

Only known solution is to upgrade affected systems libhibernate-validator-java package in distro.