# 

# 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

![Graphical user interface, text, application, email

Description automatically generated]()

![Graphical user interface, text, application, email, website

Description automatically generated]()

![Text

Description automatically generated with medium confidence]()

### Document Results

* log4j-api-2.12.1.jar - *The Apache Log4j API:* 
  + [**CVE-2020-9488**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9488)
* snakeyaml-1.25.jar - *YAML 1.1 parser and emitter for Java*
  + [**CVE-2017-18640**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640)
* jackson-databind-2.10.2.jar - *General data-binding functionality for Jackson:*

*works on core streaming API*

* [**CVE-2020-25649**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25649)
* tomcat-embed-core-9.0.30.jar - *Core Tomcat implementation*
  + [**CVE-2019-17569**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569)
  + [**CVE-2020-11996**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11996)
  + [**CVE-2020-13934**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13934)
  + [**CVE-2020-13935**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13935)
  + [**CVE-2020-13943**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13943)
  + [**CVE-2020-17527**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17527)
  + [**CVE-2020-1935**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1935)
  + [**CVE-2020-1938**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1938)
  + [**CVE-2020-8022**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8022)
  + [**CVE-2020-9484**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9484)
  + [**CVE-2021-24122**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24122)
  + [**CVE-2021-25122**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25122)
  + [**CVE-2021-25329**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25329)
  + [**CVE-2021-30640**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30640)
  + [**CVE-2021-33037**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33037)
  + [**CVE-2021-41079**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41079)
  + [**CVE-2021-42340**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42340)
* hibernate-validator-6.0.18.Final.jar - *Hibernate's Bean Validation (JSR-380)*

*reference implementation.*

* [**CVE-2020-10693**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-10693)
* spring-core-5.2.3.RELEASE.jar - *Spring Core*
  + [**CVE-2020-5421**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421)
  + [**CVE-2021-22096**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096)
  + [**CVE-2021-22118**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118)
* spring-jcl-5.2.3.RELEASE.jar - *Spring Commons Logging Bridge*
  + [**CVE-2020-5421**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421)

### Interpret Results

* log4j-api-2.12.1.jar - *The Apache Log4j API:* “Improper validation of certificate with host mismatch. Would allow connection to be intercepted, leading to leaked log messages”. The above Dependency is the latest version of Log4j. However, there is a minor source incompatibility with prior release due to new methods to the logger interference. Its suitable to review and fix any compiler errors for this vulnerability.
* snakeyaml-1.25.jar - *YAML 1.1 parser and emitter for Java:* “Allows entity expansion during load operation”. Updating to the latest version should eliminate this vulnerability.
* jackson-databind-2.10.2.jar - *General data-binding functionality for Jackson:*

*works on core streaming API:* “Error due to no entity expansion being secured properly. Allows vulnerability to XML external entity attacks. Highest threat could lead to the data integrity”. Updating to latest version, will eliminate most vulnerabilities within this dependency error.

* tomcat-embed-core-9.0.30.jar - *Core Tomcat implementation:*

Multiple vulnerabilities within the Dependency listed above. Such as Memory and data loss. Making clients and users vulnerable to attacks from the forms of Username and passwords being exploited over the web. Should ensure version is updated to latest version and conclude to an HTTPS header.

* hibernate-validator-6.0.18.Final.jar - *Hibernate's Bean Validation (JSR-380)*

*reference implementation.* –

“Flaw found in Hibernate version 6.1.2. Final. Enables invalid EL expressions to be evaluated as they were valid. Allows attackers to bypass input sanitization due to developer error”. Update to Most current version to eliminate both risk and vulnerability

* spring-core-5.2.3.RELEASE.jar - *Spring Core:*

“Older unsupported versions of Spring Framework, protection against RFD attacks remain vulnerable to being bypassed. Update to latest version within Spring framework.

* spring-jcl-5.2.3.RELEASE.jar - *Spring Commons Logging Bridge:*

Vulnerabilities listed for this dependency are occurring due to older unsupported versions in Spring Framework. There is no protection in place and can be easily bypassed. Updating to the latest version within software applications will reduce such risk.

Running dependency check reports within maven, is a vital role in successfully addressing any vulnerabilities to the current application. Continued monitoring of this is crucial toward the development and security of any business. Its highly recommended that each error be carefully evaluated and addressed, as to the resolution of most dependencies above. The overall spring Framework needs to be updated to the latest version, to eliminate risk.

False positives create a false sense of security, leading to unnecessary work or attention in order to fix an error that’s not present. It truly takes skill and knowledge to clearly address and understand this topic. But with careful review, better results for addressing these issues are possible.

**References**

<https://mvnrepository.com/artifact/org.yaml/snakeyaml/1.25>

<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>

<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>

<https://stackoverflow.com/questions/7600028/maven-error-in-opening-zip-file-when-running-maven>

<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>

I also Used google.com/search. To gain more insight and valid information in regard to each dependency error and vulnerability.