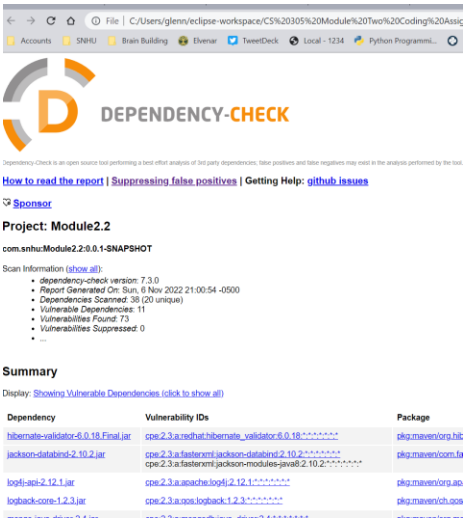
CS 305 Module Two Coding Assignment

1. Run Dependency Check



2. Document Results

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
classmate-1.5.1.jar		pkg:maven/com.fasterxml/classmate@1.5.1		0		57
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:redhat:hibernate_validator:6.0.18:*:*:*:*:*:*:*	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	1	Highest	34
jackson-core-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-core@2.10.2		0	Low	47
jackson-databind-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	4	Highest	41

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
jakarta.annotation-api-1.3.5.jar	cpe:2.3:a:oracle:java_se:1.3.5:*:*:*:*:*:*:* cpe:2.3:a:oracle:projects:1.3.5:*:*:*:*:*:*:*	pkg:maven/jakarta.annotation/jakarta.annotation-api@1.3.5		0	Low	37
jakarta.validation-api-2.0.2.jar		pkg:maven/jakarta.validation/jakarta.validation-api@2.0.2		0		58
jboss-logging-3.4.1.Final.jar		pkg:maven/org.jboss.logging/jboss-logging@3.4.1.Final		0		44
jul-to-slf4j-1.7.30.jar		pkg:maven/org.slf4j/jul-to-slf4j@1.7.30		0		26
log4j-api-2.12.1.jar	cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:*	pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1	LOW	1	Highest	44
log4j-to-slf4j-2.12.1.jar		pkg:maven/org.apache.logging.log4j/log4j-to-slf4j@2.12.1		0		42
logback-core-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-core@1.2.3	MEDIUM	1	Highest	33
mongo-java-driver-2.4.jar	cpe:2.3:a:mongodb:java_driver:2.4:*:*:*:*:*:*:*	pkg:maven/org.mongodb/mongo-java-driver@2.4	MEDIUM	1	Highest	20
slf4j-api-1.7.30.jar		pkg:maven/org.slf4j/slf4j-api@1.7.30		0		27
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:* cpe:2.3:a:yaml_project:yaml:1.25:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.25	HIGH	6	Highest	46
spring-boot-2.2.4.R	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-	HIGH	1	Highest	39

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
ELEASE.jar		boot@2.2.4.RELEASE				
spring-core-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.2.3.RELEASE	CRITICAL	9	Highest	36
spring-web-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.2.3.RELEASE	CRITICAL	10	Highest	34
tomcat-embed-core-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30	CRITICAL	19	Highest	33
tomcat-embed-el-9.0.30.jar		pkg:maven/org.apache.tomcat.embed/tomcat-embed-el@9.0.30		0		30
tomcat-embed-websocket-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30	CRITICAL	20	Highest	32

3. Analyze Results

Within the list of dependencies, there is a shorter list of vulnerabilities. This list should be approached with critical items first to ensure the project is secure. The suppression of false positive items allows developers to focus on actual issues.

Specifically, this project has the following issue:

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:redhat:hibernate_validator:6.0.18:*:*:*:*:*:*:*	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	1	Highest	34
jackson-databind-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	4	Highest	41
log4j-api-2.12.1.jar	cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:*	pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1	LOW	1	Highest	44
logback-core-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-core@1.2.3	MEDIUM	1	Highest	33
mongo-java-driver-2.4.jar	cpe:2.3:a:mongodb:java_driver:2.4:*:*:*:*:*:*:*	pkg:maven/org.mongodb/mongo-java-driver@2.4	MEDIUM	1	Highest	20
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:* cpe:2.3:a:yaml_project:yaml:1.25:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.25	HIGH	6	Highest	46
spring-boot-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE	HIGH	1	Highest	39
spring-core-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.2.3.RELEASE	CRITICAL	9	Highest	36
spring-web-5.2.3.RE	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_	pkg:maven/org.springframework/spring-web@5.2.3.RELEASE	CRITICAL	10	Highest	34

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
LEASE.jar	framework:5.2.3:release:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*:*					
tomcat-embed-core-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30	CRITICAL	19	Highest	33
tomcat-embed-websocket-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30	CRITICAL	20	Highest	32

I would focus on this issue first:

tomcat-embed-websocket-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30	CRITICAL	20	Highest	32

The issue would need to be evaluated based NVD database and the system configuration being run, and then appropriate precautions would be taken.

There is disparate information from the sources, so a deep dive into the issues would need to occur.

pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30 indicates no vulnerabilities.

Back to Component Details

tomcat-embed-websocket

org.apache.tomcat.embed
Version 9.0.30

Vulnerabilities

This version of tomcat-embed-websocket has no known vulnerabilities!

cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* Has a rather long list.

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES | SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Search Type: Search All
- CPE Vendor: cpe:/:apache
- CPE Product: cpe:/:apache:tomcat
- CPE Product Version: cpe:/:apache:tomcat:9.0.30

There are **20** matching records.
Displaying matches **1** through **20**.

Vuln ID	Summary	CVSS Severity
CVE-2022-42252	If Apache Tomcat 8.5.0 to 8.5.52, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header. **Published:** November 01, 2022; 5:15:10 AM -0400	*V3.1:* 7.5 HIGH *V2.0:*(not available)
CVE-2021-43980	The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client. **Published:** September 28, 2022; 10:15:09 AM -0400	*V3.1:* 3.7 LOW *V2.0:*(not available)
CVE-2022-34305	In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability. **Published:** June 23, 2022; 7:15:07 AM -0400	*V3.1:* 6.1 MEDIUM *V2.0:* 4.3 MEDIUM
CVE-2022-29885	The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 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. **Published:** May 12, 2022; 4:15:07 AM -0400	*V3.1:* 7.5 HIGH *V2.0:* 5.0 MEDIUM