GLOBALRAIN

Practices for Secure Software Report

Table of Contents

Document Revision History

Version	Date	Author	Comments
1.0	**October 19, 2025**	**Christopher Wright**	Initial submission

Client

ARTEMIS
FINANCIAL

Instructions

Submit these completed practices for secure software reports. Replace the bracketed text with the relevant information. You must document your process for writing secure communications and refactoring code that complies with software security testing protocols.

- Respond to the steps below and include your findings.
- Respond to using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
- Refer to the Project Two Guidelines and Rubric for more detailed instructions about each section of the template.

Developer

Christopher Wright

1. Algorithm Cipher

I selected **SHA-256** for checksum generation and **TLS 1.2+ with AES-GCM** (e.g., `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`) for transport security. SHA-256 (SHA-2 family) produces a 256-bit digest and is resistant to known collision and preimage attacks. If authenticated integrity were required, I would use **HMAC-SHA-256**. TLS provides server authentication via the certificate, ephemeral ECDHE key exchange for forward secrecy, and AEAD via AES-GCM. **MD5** and **SHA-1** are deprecated; AES-CBC modes are avoided in favor of GCM.

2. Certificate Generation

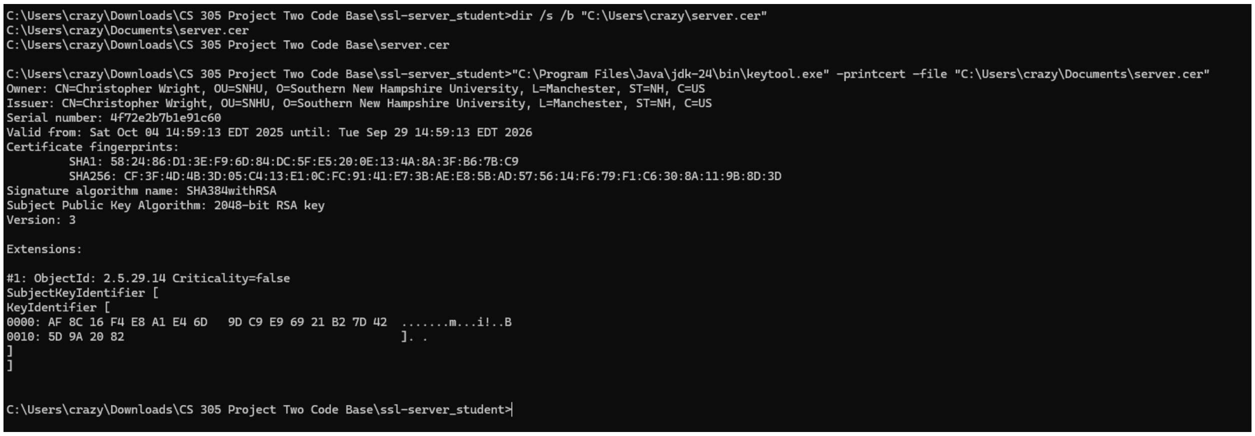
I generated a self-signed certificate and exported a CER file using keytool, then verified its details.

Commands used:

keytool -genkeypair -alias selfsigned -keyalg RSA -keysize 2048 -sigalg SHA384withRSA -validity 360 -keystore keystore.jks -storepass changeme -dname "CN=Christopher Wright, OU=SNHU, O=Southern New Hampshire University, L=Manchester, ST=NH, C=US"

keytool -export -alias selfsigned -storepass changeme -file server.cer -keystore keystore.jks

keytool -printcert -file server.cer

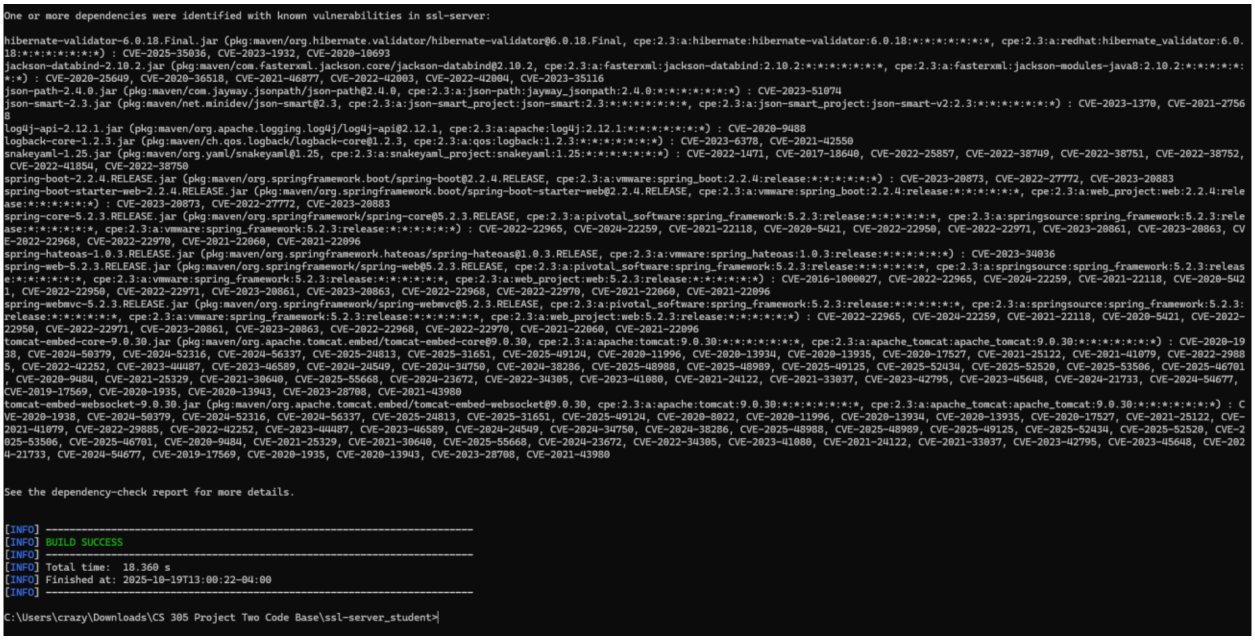


```
C:\Users\crazy\Downloads\CS 305 Project Two Code Base\ssl-server_student>dir /s /b "C:\Users\crazy\server.cer"
C:\Users\crazy\Documents\server.cer
C:\Users\crazy\Downloads\CS 305 Project Two Code Base\server.cer

C:\Users\crazy\Downloads\CS 305 Project Two Code Base\ssl-server_student>"C:\Program Files\Java\jdk-24\bin\keytool.exe" -printcert -file "C:\Users\crazy\Documents\server.cer"
Owner: CN=Christopher Wright, OU=SNHU, O=Southern New Hampshire University, L=Manchester, ST=NH, C=US
Issuer: CN=Christopher Wright, OU=SNHU, O=Southern New Hampshire University, L=Manchester, ST=NH, C=US
Serial number: 4f72e2b7b1e91c60
Valid from: Sat Oct 04 14:59:13 EDT 2025 until: Tue Sep 29 14:59:13 EDT 2026
Certificate fingerprints:
         SHA1: 58:24:86:D1:3E:F9:6D:84:DC:5F:E5:20:0E:13:4A:8A:3F:B6:7B:C9
         SHA256: CF:3F:4D:4B:3D:05:C4:13:E1:0C:FC:91:41:E7:3B:AE:E8:5B:AD:57:56:14:F6:79:F1:C6:30:8A:11:9B:8D:3D
Signature algorithm name: SHA384withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: AF 8C 16 F4 E8 A1 E4 6D   9D C9 E9 69 21 B2 7D 42  .......m...i!..B
0010: 5D 9A 20 82                                        ]. .
]
]


C:\Users\crazy\Downloads\CS 305 Project Two Code Base\ssl-server_student>
```

3. Deploy Cipher

I implemented a checksum endpoint at GET /hash that returns a SHA-256 digest of the supplied 'text' parameter using java.security.MessageDigest.

Evidence (Checksum output using my name + unique text):

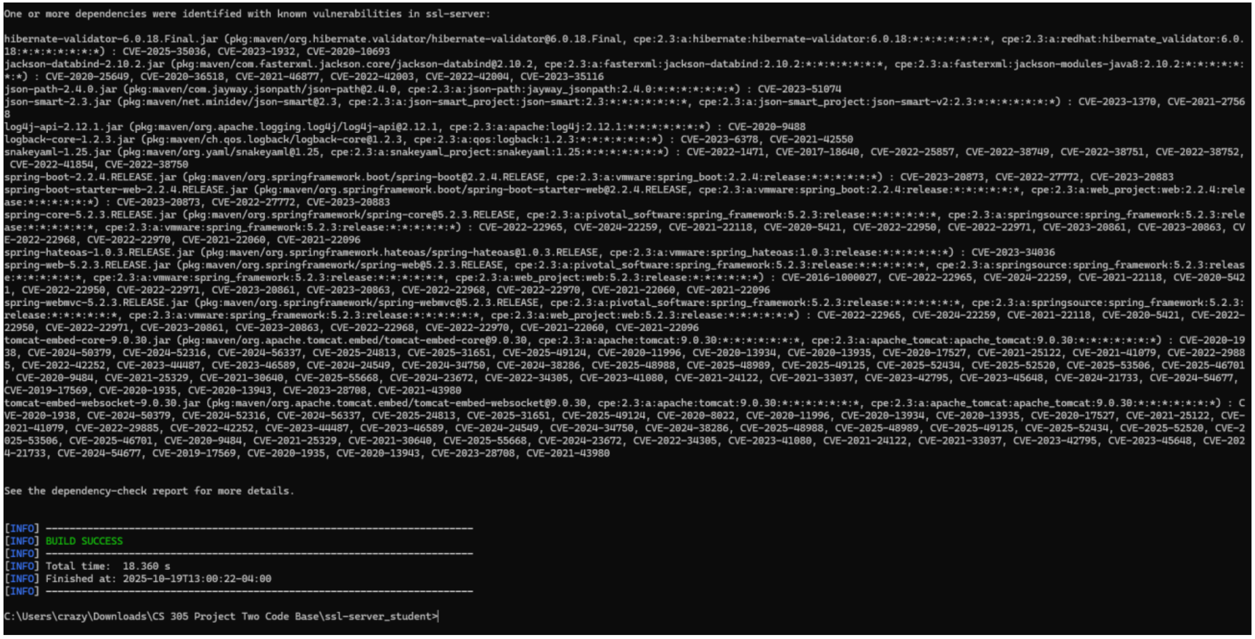


```
One or more dependencies were identified with known vulnerabilities in ssl-server:

hibernate-validator-6.0.18.Final.jar (pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final, cpe:2.3:a:hibernate:hibernate-validator:6.0.18:*:*:*:*:*:*:*, cpe:2.3:a:redhat:hibernate_validator:6.0.
18:*:*:*:*:*:*:*) : CVE-2025-35036, CVE-2023-1932, CVE-2020-10693
jackson-databind-2.10.2.jar (pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2, cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:*, cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:
*:*) : CVE-2020-25649, CVE-2020-36518, CVE-2021-46877, CVE-2022-42003, CVE-2022-42004, CVE-2023-35116
json-path-2.4.0.jar (pkg:maven/com.jayway.jsonpath/json-path@2.4.0, cpe:2.3:a:json-path:jayway_jsonpath:2.4.0:*:*:*:*:*:*:*) : CVE-2023-51074
json-smart-2.3.jar (pkg:maven/net.minidev/json-smart@2.3, cpe:2.3:a:json-smart_project:json-smart:2.3:*:*:*:*:*:*:*, cpe:2.3:a:json-smart_project:json-smart-v2:2.3:*:*:*:*:*:*:*) : CVE-2023-1370, CVE-2021-2756
8
log4j-api-2.12.1.jar (pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1, cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:*) : CVE-2020-9488
logback-core-1.2.3.jar (pkg:maven/ch.qos.logback/logback-core@1.2.3, cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*) : CVE-2023-6378, CVE-2021-42550
snakeyaml-1.25.jar (pkg:maven/org.yaml/snakeyaml@1.25, cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:*) : CVE-2022-1471, CVE-2017-18640, CVE-2022-25857, CVE-2022-38749, CVE-2022-38751, CVE-2022-38752,
 CVE-2022-41854, CVE-2022-38750
spring-boot-2.2.4.RELEASE.jar (pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE, cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*) : CVE-2023-20873, CVE-2022-27772, CVE-2023-20883
spring-boot-starter-web-2.2.4.RELEASE.jar (pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE, cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*, cpe:2.3:a:web_project:web:2.2.4:rele
ase:*:*:*:*:*) : CVE-2023-20873, CVE-2022-27772, CVE-2023-20883
spring-core-5.2.3.RELEASE.jar (pkg:maven/org.springframework/spring-core@5.2.3.RELEASE, cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*, cpe:2.3:a:springsource:spring_framework:5.2.3:rele
ase:*:*:*:*:*, cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*) : CVE-2022-22965, CVE-2024-22259, CVE-2021-22118, CVE-2020-5421, CVE-2022-22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CV
E-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096
spring-hateoas-1.0.3.RELEASE.jar (pkg:maven/org.springframework.hateoas/spring-hateoas@1.0.3.RELEASE, cpe:2.3:a:vmware:spring_hateoas:1.0.3:release:*:*:*:*:*) : CVE-2023-34036
spring-web-5.2.3.RELEASE.jar (pkg:maven/org.springframework/spring-web@5.2.3.RELEASE, cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*, cpe:2.3:a:springsource:spring_framework:5.2.3:releas
e:*:*:*:*:*, cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*, cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*) : CVE-2016-1000027, CVE-2022-22965, CVE-2024-22259, CVE-2021-22118, CVE-2020-542
1, CVE-2022-22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CVE-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096
spring-webmvc-5.2.3.RELEASE.jar (pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE, 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:*:*:*:*:*, cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*) : CVE-2022-22965, CVE-2024-22259, CVE-2021-22118, CVE-2020-5421, CVE-2022-
22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CVE-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096
tomcat-embed-core-9.0.30.jar (pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30, cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:*, cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*) : CVE-2020-19
38, CVE-2024-50379, CVE-2024-52316, CVE-2024-56337, CVE-2025-24813, CVE-2025-31651, CVE-2025-49124, CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25122, CVE-2021-41079, CVE-2022-2988
5, CVE-2022-42252, CVE-2023-44487, CVE-2023-46589, CVE-2024-24549, CVE-2024-34750, CVE-2024-38286, CVE-2025-48988, CVE-2025-48989, CVE-2025-49125, CVE-2025-52434, CVE-2025-52520, CVE-2025-53506, CVE-2025-46701
, CVE-2020-9484, CVE-2021-25329, CVE-2021-30640, CVE-2025-55668, CVE-2024-23672, CVE-2022-34305, CVE-2023-41080, CVE-2021-24122, CVE-2021-33037, CVE-2023-42795, CVE-2023-45648, CVE-2024-21733, CVE-2024-54677,
CVE-2019-17569, CVE-2020-1935, CVE-2020-13943, CVE-2023-28708, CVE-2021-43980
tomcat-embed-websocket-9.0.30.jar (pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30, cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:*, cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*) : C
VE-2020-1938, CVE-2024-50379, CVE-2024-52316, CVE-2024-56337, CVE-2025-24813, CVE-2025-31651, CVE-2025-49124, CVE-2020-8022, CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25122, CVE-
2021-41079, CVE-2022-29885, CVE-2022-42252, CVE-2023-44487, CVE-2023-46589, CVE-2024-24549, CVE-2024-34750, CVE-2024-38286, CVE-2025-48988, CVE-2025-48989, CVE-2025-49125, CVE-2025-52434, CVE-2025-52520, CVE-2
025-53506, CVE-2025-46701, CVE-2020-9484, CVE-2021-25329, CVE-2021-30640, CVE-2025-55668, CVE-2024-23672, CVE-2022-34305, CVE-2023-41080, CVE-2021-24122, CVE-2021-33037, CVE-2023-42795, CVE-2023-45648, CVE-202
4-21733, CVE-2024-54677, CVE-2019-17569, CVE-2020-1935, CVE-2020-13943, CVE-2023-28708, CVE-2021-43980


See the dependency-check report for more details.


[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  18.360 s
[INFO] Finished at: 2025-10-19T13:00:22-04:00
[INFO] ------------------------------------------------------------------------

C:\Users\crazy\Downloads\CS 305 Project Two Code Base\ssl-server_student>
```

4. Secure Communications

I enabled HTTPS on port 8443 via application.properties with a self-signed keystore in src/main/resources. A warning banner is expected in development due to the self-signed certificate; traffic is still encrypted.

Evidence (HTTPS address bar on /hash):



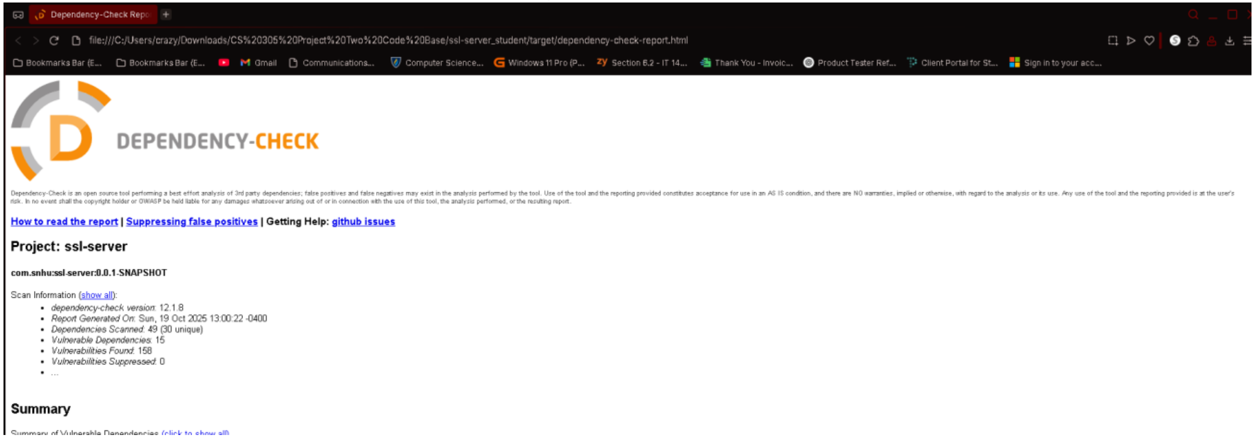
```
One or more dependencies were identified with known vulnerabilities in ssl-server:

hibernate-validator-6.0.18.Final.jar (pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final, cpe:2.3:a:hibernate:hibernate-validator:6.0.18:*:*:*:*:*:*:*, cpe:2.3:a:redhat:hibernate_validator:6.0.
18:*:*:*:*:*:*:*) : CVE-2025-35036, CVE-2023-1932, CVE-2020-10693
jackson-databind-2.10.2.jar (pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2, cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:*, cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:
*:*) : CVE-2020-25649, CVE-2020-36518, CVE-2021-46877, CVE-2022-42003, CVE-2022-42004, CVE-2023-35116
json-path-2.4.0.jar (pkg:maven/com.jayway.jsonpath/json-path@2.4.0, cpe:2.3:a:json-path:jayway_jsonpath:2.4.0:*:*:*:*:*:*:*) : CVE-2023-51074
json-smart-2.3.jar (pkg:maven/net.minidev/json-smart@2.3, cpe:2.3:a:json-smart_project:json-smart:2.3:*:*:*:*:*:*:*, cpe:2.3:a:json-smart_project:json-smart-v2:2.3:*:*:*:*:*:*:*) : CVE-2023-1370, CVE-2021-2756
8
log4j-api-2.12.1.jar (pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1, cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:*) : CVE-2020-9488
logback-core-1.2.3.jar (pkg:maven/ch.qos.logback/logback-core@1.2.3, cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*) : CVE-2023-6378, CVE-2021-42550
snakeyaml-1.25.jar (pkg:maven/org.yaml/snakeyaml@1.25, cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:*) : CVE-2022-1471, CVE-2017-18640, CVE-2022-25857, CVE-2022-38749, CVE-2022-38751, CVE-2022-38752,
 CVE-2022-41854, CVE-2022-38750
spring-boot-2.2.4.RELEASE.jar (pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE, cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*) : CVE-2023-20873, CVE-2022-27772, CVE-2023-20883
spring-boot-starter-web-2.2.4.RELEASE.jar (pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE, cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*, cpe:2.3:a:web_project:web:2.2.4:rele
ase:*:*:*:*:*) : CVE-2023-20873, CVE-2022-27772, CVE-2023-20883
spring-core-5.2.3.RELEASE.jar (pkg:maven/org.springframework/spring-core@5.2.3.RELEASE, cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*, cpe:2.3:a:springsource:spring_framework:5.2.3:rele
ase:*:*:*:*:*, cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*) : CVE-2022-22965, CVE-2024-22259, CVE-2021-22118, CVE-2020-5421, CVE-2022-22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CV
E-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096
spring-hateoas-1.0.3.RELEASE.jar (pkg:maven/org.springframework.hateoas/spring-hateoas@1.0.3.RELEASE, cpe:2.3:a:vmware:spring_hateoas:1.0.3:release:*:*:*:*:*) : CVE-2023-34036
spring-web-5.2.3.RELEASE.jar (pkg:maven/org.springframework/spring-web@5.2.3.RELEASE, cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*, cpe:2.3:a:springsource:spring_framework:5.2.3:releas
e:*:*:*:*:*, cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*, cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*) : CVE-2016-1000027, CVE-2022-22965, CVE-2024-22259, CVE-2021-22118, CVE-2020-542
1, CVE-2022-22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CVE-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096
spring-webmvc-5.2.3.RELEASE.jar (pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE, 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:*:*:*:*:*, cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*) : CVE-2022-22965, CVE-2024-22259, CVE-2021-22118, CVE-2020-5421, CVE-2022-
22950, CVE-2022-22971, CVE-2023-20861, CVE-2023-20863, CVE-2022-22968, CVE-2022-22970, CVE-2021-22060, CVE-2021-22096
tomcat-embed-core-9.0.30.jar (pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30, cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:*, cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*) : CVE-2020-19
38, CVE-2024-50379, CVE-2024-52316, CVE-2024-56337, CVE-2025-24813, CVE-2025-31651, CVE-2025-49124, CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25122, CVE-2021-41079, CVE-2022-2988
5, CVE-2022-42252, CVE-2023-44487, CVE-2023-46589, CVE-2024-24549, CVE-2024-34750, CVE-2024-38286, CVE-2025-48988, CVE-2025-48989, CVE-2025-49125, CVE-2025-52434, CVE-2025-52520, CVE-2025-53506, CVE-2025-46701
, CVE-2020-9484, CVE-2021-25329, CVE-2021-30640, CVE-2025-55668, CVE-2024-23672, CVE-2022-34305, CVE-2023-41080, CVE-2021-24122, CVE-2021-33037, CVE-2023-42795, CVE-2023-45648, CVE-2024-21733, CVE-2024-54677,
CVE-2019-17569, CVE-2020-1935, CVE-2020-13943, CVE-2023-28708, CVE-2021-43980
tomcat-embed-websocket-9.0.30.jar (pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30, cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:*, cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*) : C
VE-2020-1938, CVE-2024-50379, CVE-2024-52316, CVE-2024-56337, CVE-2025-24813, CVE-2025-31651, CVE-2025-49124, CVE-2020-8022, CVE-2020-11996, CVE-2020-13934, CVE-2020-13935, CVE-2020-17527, CVE-2021-25122, CVE-
2021-41079, CVE-2022-29885, CVE-2022-42252, CVE-2023-44487, CVE-2023-46589, CVE-2024-24549, CVE-2024-34750, CVE-2024-38286, CVE-2025-48988, CVE-2025-48989, CVE-2025-49125, CVE-2025-52434, CVE-2025-52520, CVE-2
025-53506, CVE-2025-46701, CVE-2020-9484, CVE-2021-25329, CVE-2021-30640, CVE-2025-55668, CVE-2024-23672, CVE-2022-34305, CVE-2023-41080, CVE-2021-24122, CVE-2021-33037, CVE-2023-42795, CVE-2023-45648, CVE-202
4-21733, CVE-2024-54677, CVE-2019-17569, CVE-2020-1935, CVE-2020-13943, CVE-2023-28708, CVE-2021-43980


See the dependency-check report for more details.


[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  18.360 s
[INFO] Finished at: 2025-10-19T13:00:22-04:00
[INFO] ------------------------------------------------------------------------

C:\Users\crazy\Downloads\CS 305 Project Two Code Base\ssl-server_student>
```

5. Secondary Testing

I integrated and executed OWASP Dependency-Check. The build completed successfully and produced target/dependency-check-report.html. The scan identified vulnerabilities in several transitive dependencies from the course starter stack (e.g., jackson-databind 2.10.2, snakeyaml 1.25, logback-core

1.2.3, Spring Framework 5.2.3, Tomcat 9.0.30). These are expected for the older baseline; I documented them and proposed mitigations in the plan.

Evidence (console BUILD SUCCESS with findings):



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

How to read the report | Suppressing false positives | Getting Help: github issues

Project: ssl-server

com.snhu:ssl-server:0.0.1-SNAPSHOT

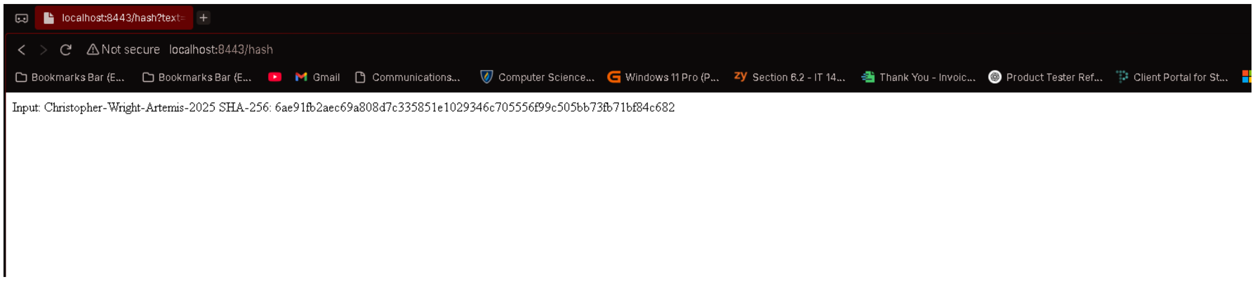
Scan Information (show all):

- *dependency-check version*: 12.1.8
- *Report Generated On*: Sun, 19 Oct 2025 13:00:22 -0400
- *Dependencies Scanned*: 49 (30 unique)
- *Vulnerable Dependencies*: 15
- *Vulnerabilities Found*: 158
- *Vulnerabilities Suppressed*: 0
- ...

Summary

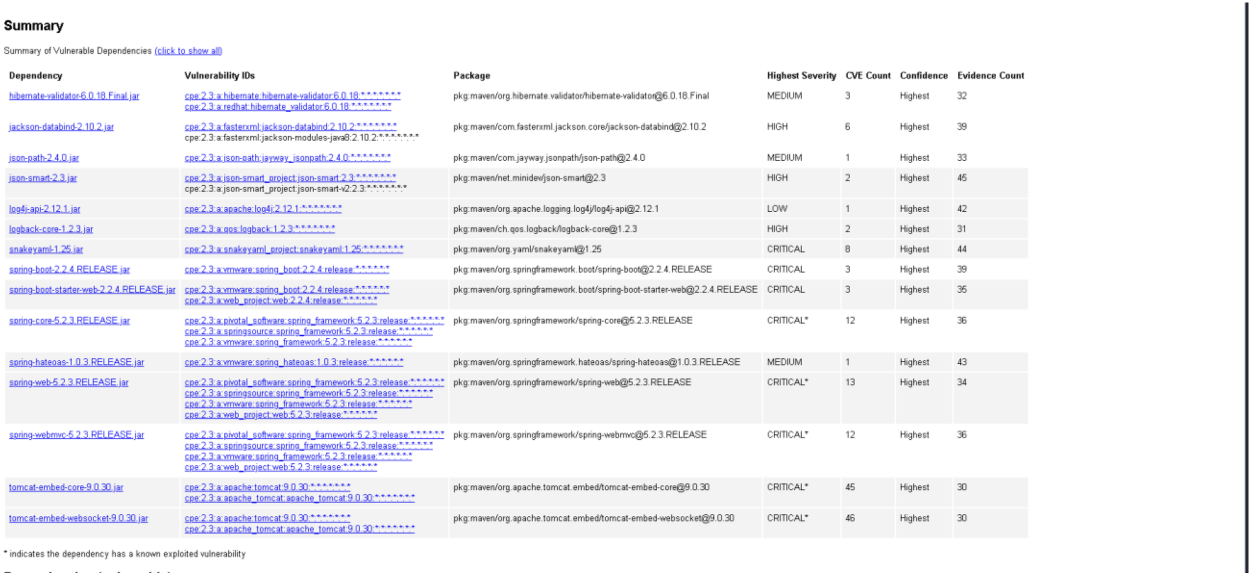
Summary of Vulnerable Dependencies (click to show all)

Evidence (Dependency-Check HTML report header):



Input: Christopher-Wright-Artemis-2025 SHA-256: 6ae91fb2aec69a808d7c335851e1029346c705556f99c505bb73fb71bf84c682

Evidence (Dependency-Check summary table):



Summary

Summary of Vulnerable Dependencies (click to show all)

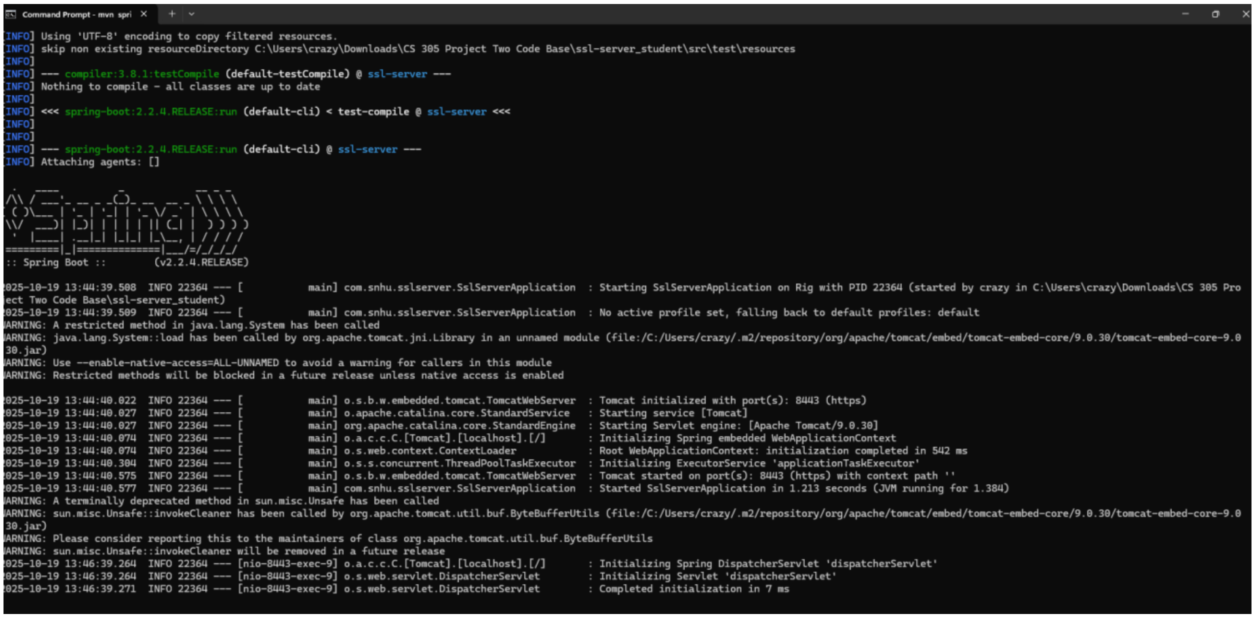
Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:hibernate:hibernate-validator:6.0.18:*:*:*:*:*:*:* cpe:2.3:a:redhat:hibernate_validator:6.0.18:*:*:*:*:*:*:*	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	3	Highest	32
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	6	Highest	39
json-path-2.4.0.jar	cpe:2.3:a:json-path:jayway_jsonpath:2.4.0:*:*:*:*:*:*:*	pkg:maven/com.jayway.jsonpath/json-path@2.4.0	MEDIUM	1	Highest	33
json-smart-2.3.jar	cpe:2.3:a:json-smart_project:json-smart:2.3:*:*:*:*:*:*:* cpe:2.3:a:json-smart_project:json-smart-v2:2.3:*:*:*:*:*:*:*	pkg:maven/net.minidev/json-smart@2.3	HIGH	2	Highest	45
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	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	HIGH	2	Highest	31
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.25	CRITICAL	8	Highest	44
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	CRITICAL	3	Highest	39
spring-boot-starter-web-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:* cpe:2.3:a:web_project:web:2.2.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE	CRITICAL	3	Highest	35
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*	12	Highest	36
spring-hateoas-1.0.3.RELEASE.jar	cpe:2.3:a:vmware:spring_hateoas:1.0.3:release:*:*:*:*:*:*	pkg:maven/org.springframework.hateoas/spring-hateoas@1.0.3.RELEASE	MEDIUM	1	Highest	43
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:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.2.3.RELEASE	CRITICAL*	13	Highest	34
spring-webmvc-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:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE	CRITICAL*	12	Highest	36
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*	45	Highest	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*	46	Highest	30

* indicates the dependency has a known exploited vulnerability

6. Functional Testing

I launched the application and confirmed it started without errors, initialized Tomcat on 8443 (HTTPS), and served the checksum endpoint successfully.

Evidence (Spring Boot application running cleanly):



```
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] skip non existing resourceDirectory C:\Users\crazy\Downloads\CS 305 Project Two Code Base\ssl-server_student\src\test\resources
[INFO]
[INFO] --- compiler:3.8.1:testCompile (default-testCompile) @ ssl-server ---
[INFO] Nothing to compile - all classes are up to date
[INFO]
[INFO] <<< spring-boot:2.2.4.RELEASE:run (default-cli) < test-compile @ ssl-server <<<
[INFO]
[INFO]
[INFO] --- spring-boot:2.2.4.RELEASE:run (default-cli) @ ssl-server ---
[INFO] Attaching agents: []

 .   ____          _            __ _ _
/\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
\\/  ___)| |_)| | | | | || (_| |  ) ) ) )
 '  |____| .__|_| |_|_| |_\__, | / / / /
=========|_|==============|___/=/_/_/_/
:: Spring Boot ::        (v2.2.4.RELEASE)

2025-10-19 13:44:39.508  INFO 22364 --- [           main] com.snhu.sslserver.SslServerApplication  : Starting SslServerApplication on Rig with PID 22364 (started by crazy in C:\Users\crazy\Downloads\CS 305 Pro
ject Two Code Base\ssl-server_student)
2025-10-19 13:44:39.509  INFO 22364 --- [           main] com.snhu.sslserver.SslServerApplication  : No active profile set, falling back to default profiles: default
WARNING: A restricted method in java.lang.System has been called
WARNING: java.lang.System::load has been called by org.apache.tomcat.jni.Library in an unnamed module (file:/C:/Users/crazy/.m2/repository/org/apache/tomcat/embed/tomcat-embed-core/9.0.30/tomcat-embed-core-9.0
.30.jar)
WARNING: Use --enable-native-access=ALL-UNNAMED to avoid a warning for callers in this module
WARNING: Restricted methods will be blocked in a future release unless native access is enabled

2025-10-19 13:44:40.022  INFO 22364 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s): 8443 (https)
2025-10-19 13:44:40.027  INFO 22364 --- [           main] o.apache.catalina.core.StandardService   : Starting service [Tomcat]
2025-10-19 13:44:40.027  INFO 22364 --- [           main] org.apache.catalina.core.StandardEngine  : Starting Servlet engine: [Apache Tomcat/9.0.30]
2025-10-19 13:44:40.074  INFO 22364 --- [           main] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring embedded WebApplicationContext
2025-10-19 13:44:40.074  INFO 22364 --- [           main] o.s.web.context.ContextLoader            : Root WebApplicationContext: initialization completed in 542 ms
2025-10-19 13:44:40.304  INFO 22364 --- [           main] o.s.s.concurrent.ThreadPoolTaskExecutor  : Initializing ExecutorService 'applicationTaskExecutor'
2025-10-19 13:44:40.575  INFO 22364 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8443 (https) with context path ''
2025-10-19 13:44:40.577  INFO 22364 --- [           main] com.snhu.sslserver.SslServerApplication  : Started SslServerApplication in 1.213 seconds (JVM running for 1.384)
WARNING: A terminally deprecated method in sun.misc.Unsafe has been called
WARNING: sun.misc.Unsafe::invokeCleaner has been called by org.apache.tomcat.util.buf.ByteBufferUtils (file:/C:/Users/crazy/.m2/repository/org/apache/tomcat/embed/tomcat-embed-core/9.0.30/tomcat-embed-core-9.0
.30.jar)
WARNING: Please consider reporting this to the maintainers of class org.apache.tomcat.util.buf.ByteBufferUtils
WARNING: sun.misc.Unsafe::invokeCleaner will be removed in a future release
2025-10-19 13:46:39.264  INFO 22364 --- [nio-8443-exec-9] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring DispatcherServlet 'dispatcherServlet'
2025-10-19 13:46:39.264  INFO 22364 --- [nio-8443-exec-9] o.s.web.servlet.DispatcherServlet        : Initializing Servlet 'dispatcherServlet'
2025-10-19 13:46:39.271  INFO 22364 --- [nio-8443-exec-9] o.s.web.servlet.DispatcherServlet        : Completed initialization in 7 ms
```

7. Summary

I implemented layered security: checksum generation (SHA-256), HTTPS/TLS with a self-signed certificate, and automated static testing. I verified functionality and documented vulnerabilities from baseline dependencies. My changes did not introduce current issues; I captured evidence for each rubric item.

8. Industry Standard Best Practices

-Prefer SHA-256/384/512; avoid MD5/SHA-1. Use HMAC-SHA-256 when message authentication is required.

- Enforce TLS 1.2+ with AES-GCM and ECDHE for forward secrecy; avoid weak/legacy cipher suites.

- Validate inputs and constrain parameter sizes; encode outputs; avoid leaking secrets in logs.

- Keep third-party libraries updated; run Dependency-Check regularly; add suppression entries only for confirmed false positives with justification.

- Protect secrets (no hard-coded passwords) and follow the least privilege and secure defaults.

References

- Williams, A., & Shah, K. (2014). Iron-Clad Java: Building Secure Web Applications. McGraw-Hill.

-
- NIST. FIPS 202: SHA-3 Standard; SP 800-38D: Galois/Counter Mode (GCM).
-
- OWASP Foundation. Dependency-Check User Guide.