GLOBALRAIN

Practices for Secure Software Report

Table of Contents

Document Revision History

Version	Date	Author	Comments
1.0	02/23/2025	Tony A	

Client

ARTEMIS
FINANCIAL

Instructions

Submit this completed practices for secure software report. 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 outlined below and include your findings.
- Respond 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
Tony Aguilar

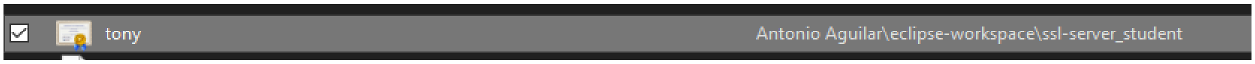
1. **Algorithm Cipher**
2. Provide a brief, high-level overview of the encryption algorithm cipher.
    a. The SHA-256 was developed in 2001 by the NIST, it is deterministic and collision resistant.
3. Discuss the hash functions and bit levels of the cipher.
    a. The SHA-256 uses 256-bit hash value that converts any input into a fixed hash value length.
4. Explain the use of random numbers, symmetric versus non-symmetric keys, and so on.
    a. Random numbers allow for the security of a hash function as it would take an unrealistic amount of time to "guess" the right key by a computer program in order to decode a system. This is accomplished either symmetrically or asymmetrically. The former being that the input and output are both decoded with the same key and the latter having a public key for decoding but a private for encoding.
5. Describe the history and current state of encryption algorithms.
    a. Currently there are many great algorithms in place for both cryptography and signing but there have been shifts in the sector that were previously thought of as impossible so I am sure that it will continue to evolve and change, hopefully for the better.

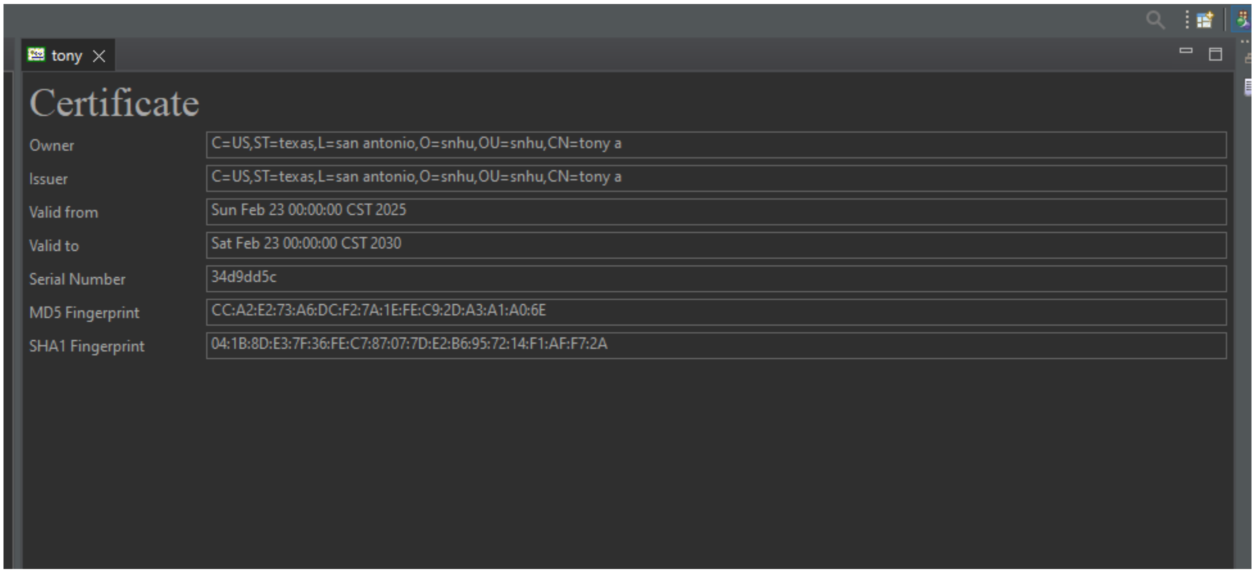
6.

SHA-256

7. Certificate Generation

8.


☑ tony Antonio Aguilar\eclipse-workspace\ssl-server_student



Certificate

Owner C=US,ST=texas,L=san antonio,O=snhu,OU=snhu,CN=tony a

Issuer C=US,ST=texas,L=san antonio,O=snhu,OU=snhu,CN=tony a

Valid from Sun Feb 23 00:00:00 CST 2025

Valid to Sat Feb 23 00:00:00 CST 2030

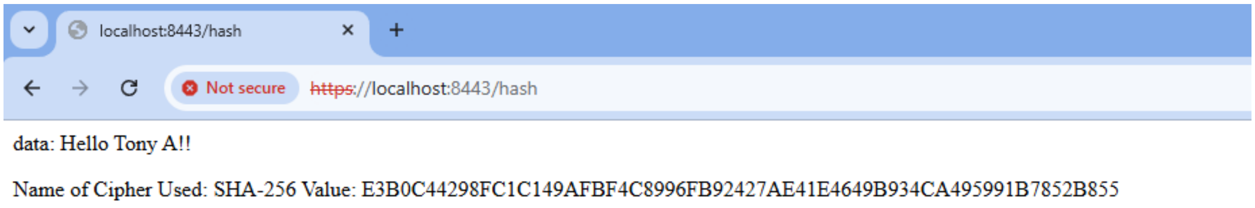
Serial Number 34d9dd5c

MD5 Fingerprint CC:A2:E2:73:A6:DC:F2:7A:1E:FE:C9:2D:A3:A1:A0:6E

SHA1 Fingerprint 04:1B:8D:E3:7F:36:FE:C7:87:07:7D:E2:B6:95:72:14:F1:AF:F7:2A

9. Deploy Cipher

Insert a screenshot below of the checksum verification.



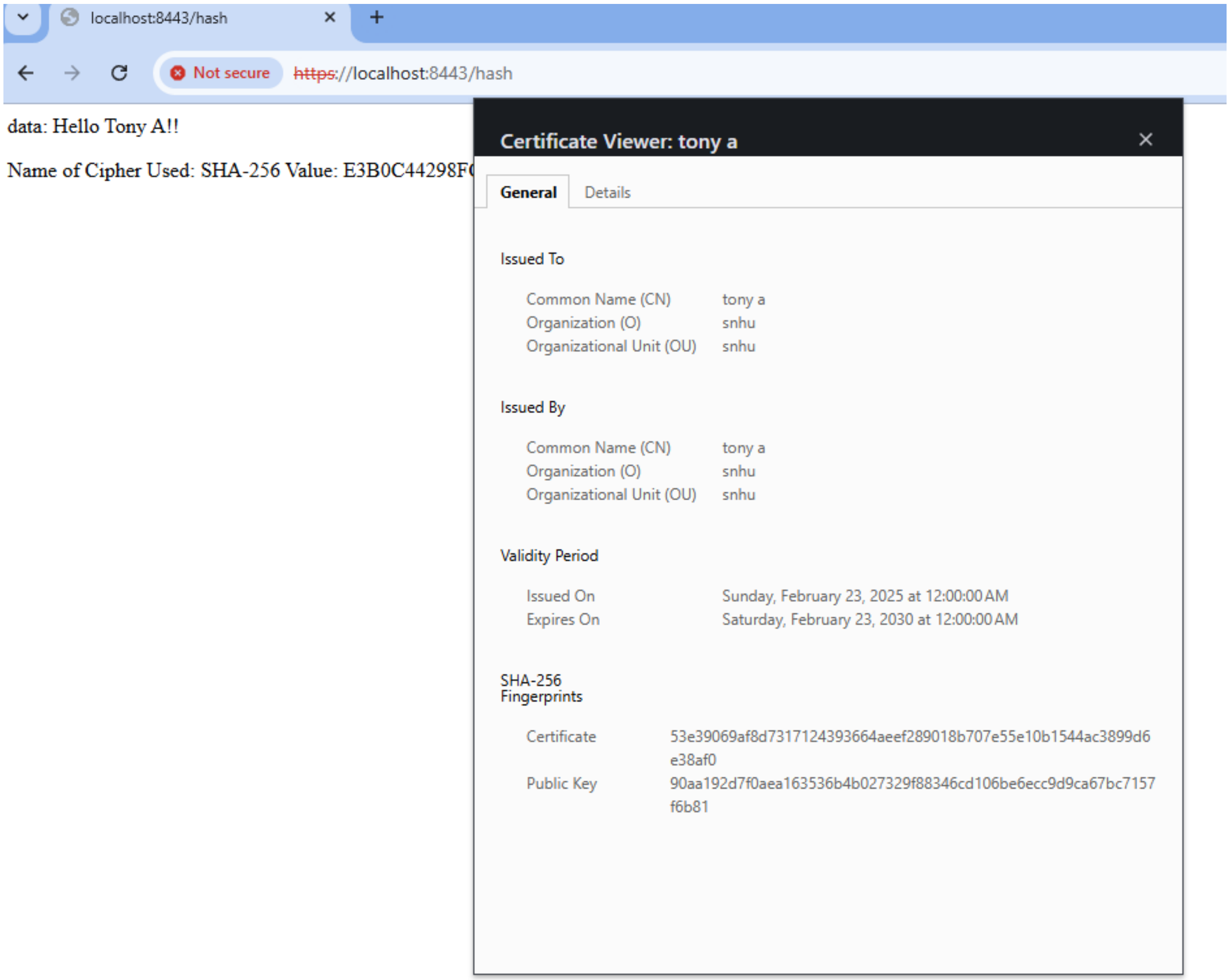
~~https~~://localhost:8443/hash

data: Hello Tony A!!

Name of Cipher Used: SHA-256 Value: E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855

10. Secure Communications

Insert a screenshot below of the web browser that shows a secure webpage.



data: Hello Tony A!!

Name of Cipher Used: SHA-256 Value: E3B0C44298F(

Certificate Viewer: tony a

Issued To

Common Name (CN)	tony a
Organization (O)	snhu
Organizational Unit (OU)	snhu

Issued By

Common Name (CN)	tony a
Organization (O)	snhu
Organizational Unit (OU)	snhu

Validity Period

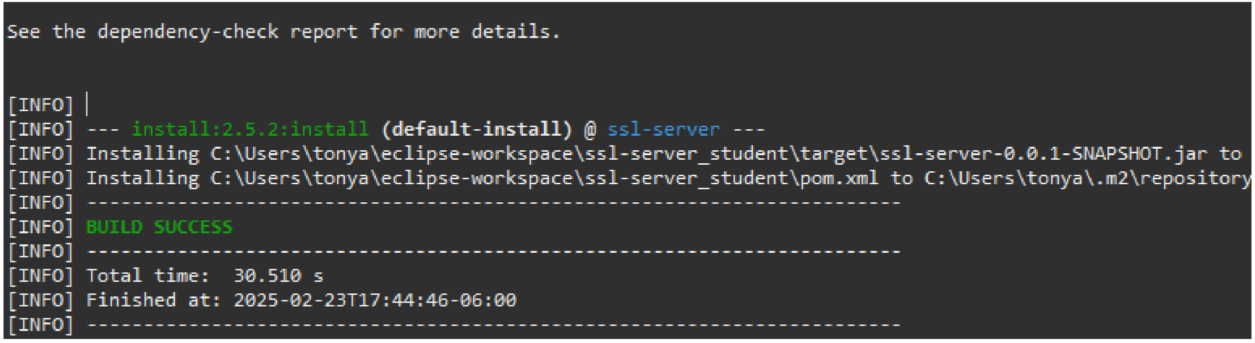
Issued On	Sunday, February 23, 2025 at 12:00:00 AM
Expires On	Saturday, February 23, 2030 at 12:00:00 AM

SHA-256 Fingerprints

Certificate	53e39069af8d7317124393664aeef289018b707e55e10b1544ac3899d6e38af0
Public Key	90aa192d7f0aea163536b4b027329f88346cd106be6ecc9d9ca67bc7157f6b81

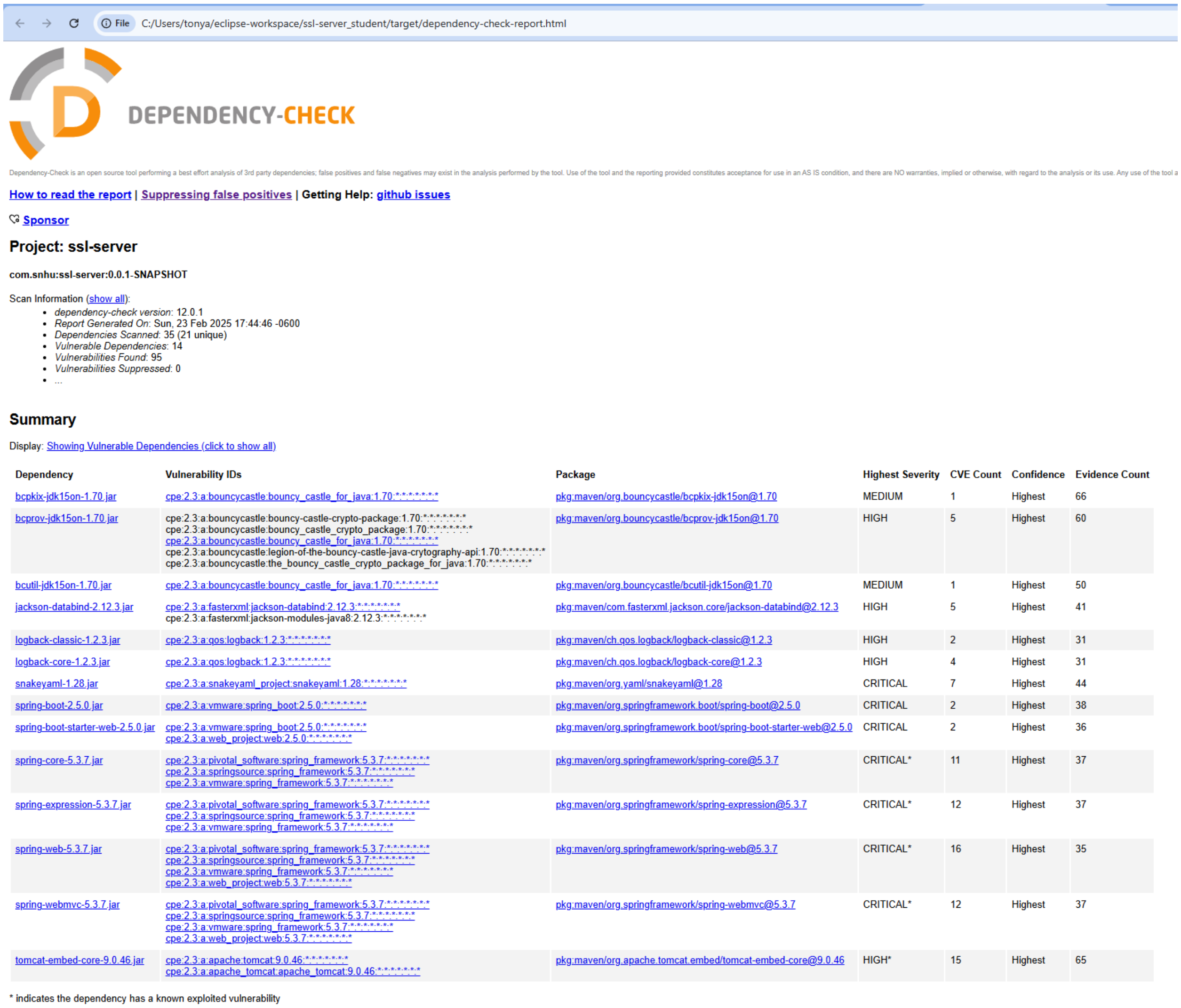
11. Secondary Testing

Insert screenshots below of the refactored code executed without errors and the dependency-check report.



```
See the dependency-check report for more details.

[INFO] |
[INFO] --- install:2.5.2:install (default-install) @ ssl-server ---
[INFO] Installing C:\Users\tonya\eclipse-workspace\ssl-server_student\target\ssl-server-0.0.1-SNAPSHOT.jar to
[INFO] Installing C:\Users\tonya\eclipse-workspace\ssl-server_student\pom.xml to C:\Users\tonya\.m2\repository
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  30.510 s
[INFO] Finished at: 2025-02-23T17:44:46-06:00
[INFO] ------------------------------------------------------------------------
```



File C:/Users/tonya/eclipse-workspace/ssl-server_student/target/dependency-check-report.html

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 a

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

Sponsor

Project: ssl-server

com.snhu:ssl-server:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 12.0.1
- *Report Generated On*: Sun, 23 Feb 2025 17:44:46 -0600
- *Dependencies Scanned*: 35 (21 unique)
- *Vulnerable Dependencies*: 14
- *Vulnerabilities Found*: 95
- *Vulnerabilities Suppressed*: 0
- ...

Summary

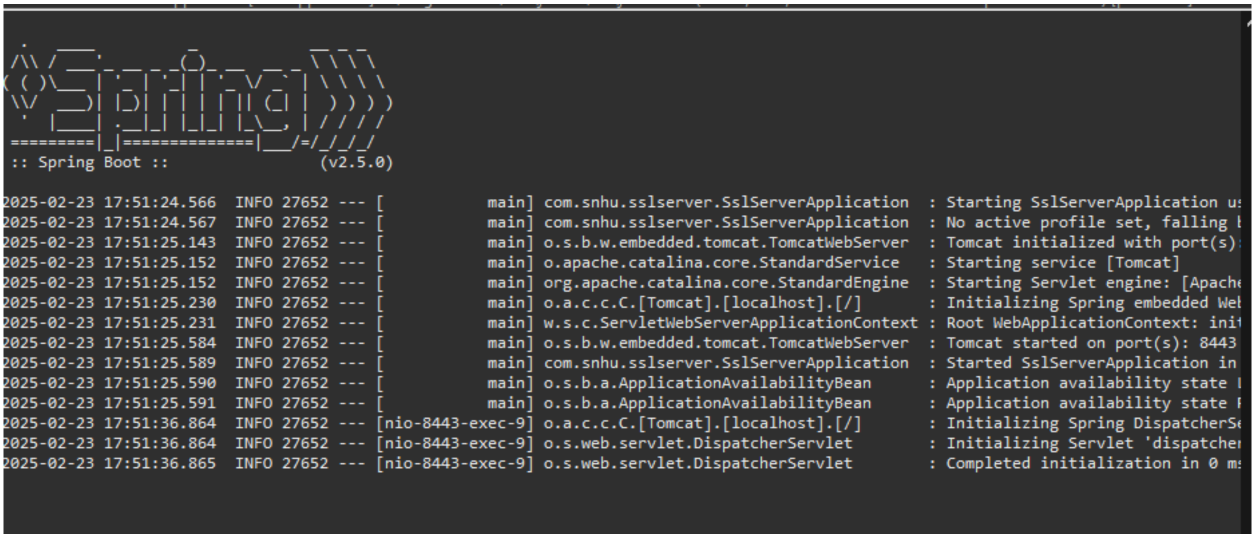
Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
bcpkix-jdk15on-1.70.jar	cpe:2.3:a:bouncycastle:bouncy_castle_for_java:1.70:*:*:*:*:*:*:*	pkg:maven/org.bouncycastle/bcpkix-jdk15on@1.70	MEDIUM	1	Highest	66
bcprov-jdk15on-1.70.jar	cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.70:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.70:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:bouncy_castle_for_java:1.70:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.70:*:*:*:*:*:*:* cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.70:*:*:*:*:*:*:*	pkg:maven/org.bouncycastle/bcprov-jdk15on@1.70	HIGH	5	Highest	60
bcutil-jdk15on-1.70.jar	cpe:2.3:a:bouncycastle:bouncy_castle_for_java:1.70:*:*:*:*:*:*:*	pkg:maven/org.bouncycastle/bcutil-jdk15on@1.70	MEDIUM	1	Highest	50
jackson-databind-2.12.3.jar	cpe:2.3:a:fasterxml:jackson-databind:2.12.3:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-modules-java8:2.12.3:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.12.3	HIGH	5	Highest	41
logback-classic-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-classic@1.2.3	HIGH	2	Highest	31
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	4	Highest	31
snakeyaml-1.28.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.28:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.28	CRITICAL	7	Highest	44
spring-boot-2.5.0.jar	cpe:2.3:a:vmware:spring_boot:2.5.0:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot@2.5.0	CRITICAL	2	Highest	38
spring-boot-starter-web-2.5.0.jar	cpe:2.3:a:vmware:spring_boot:2.5.0:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:2.5.0:*:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-web@2.5.0	CRITICAL	2	Highest	36
spring-core-5.3.7.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.7:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-core@5.3.7	CRITICAL*	11	Highest	37
spring-expression-5.3.7.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.7:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-expression@5.3.7	CRITICAL*	12	Highest	37
spring-web-5.3.7.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.3.7:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.3.7	CRITICAL*	16	Highest	35
spring-webmvc-5.3.7.jar	cpe:2.3:a:pivotal_software:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:vmware:spring_framework:5.3.7:*:*:*:*:*:*:* cpe:2.3:a:web_project:web:5.3.7:*:*:*:*:*:*:*	pkg:maven/org.springframework/spring-webmvc@5.3.7	CRITICAL*	12	Highest	37
tomcat-embed-core-9.0.46.jar	cpe:2.3:a:apache:tomcat:9.0.46:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.46:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.46	HIGH*	15	Highest	65

* indicates the dependency has a known exploited vulnerability

12. Functional Testing

Insert a screenshot below of the refactored code executed without errors.



```
  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::                (v2.5.0)

2025-02-23 17:51:24.566  INFO 27652 --- [           main] com.snhu.sslserver.SslServerApplication  : Starting SslServerApplication u
2025-02-23 17:51:24.567  INFO 27652 --- [           main] com.snhu.sslserver.SslServerApplication  : No active profile set, falling
2025-02-23 17:51:25.143  INFO 27652 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s)
2025-02-23 17:51:25.152  INFO 27652 --- [           main] o.apache.catalina.core.StandardService   : Starting service [Tomcat]
2025-02-23 17:51:25.152  INFO 27652 --- [           main] org.apache.catalina.core.StandardEngine  : Starting Servlet engine: [Apache
2025-02-23 17:51:25.230  INFO 27652 --- [           main] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring embedded We
2025-02-23 17:51:25.231  INFO 27652 --- [           main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: ini
2025-02-23 17:51:25.584  INFO 27652 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8443
2025-02-23 17:51:25.589  INFO 27652 --- [           main] com.snhu.sslserver.SslServerApplication  : Started SslServerApplication in
2025-02-23 17:51:25.590  INFO 27652 --- [           main] o.s.b.a.ApplicationAvailabilityBean      : Application availability state
2025-02-23 17:51:25.591  INFO 27652 --- [           main] o.s.b.a.ApplicationAvailabilityBean      : Application availability state
2025-02-23 17:51:36.864  INFO 27652 --- [nio-8443-exec-9] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring DispatcherS
2025-02-23 17:51:36.864  INFO 27652 --- [nio-8443-exec-9] o.s.web.servlet.DispatcherServlet        : Initializing Servlet 'dispatche
2025-02-23 17:51:36.865  INFO 27652 --- [nio-8443-exec-9] o.s.web.servlet.DispatcherServlet        : Completed initialization in 0 m
```

The digest method was updated, error handling was added, as well as added html output.

13. Summary

We added hashing functionality, secure hosting as well as certificate signing. Lastly, we also added layers of security for the traffic and visitors to the website we are hosting.

14. Industry Standard Best Practices

The industry's best standards used were avoiding hardcoded secrets, using modular and reusable code, clear method naming, using a hash algorithm to secure our data, the addition of error handling as well as restful Api design and testability.

As a whole, cryptography is vital to our society. We not only use these functions on our everyday lives, but some of us depend on them to stay alive. Take for example, when we are driving our cars, how can we avoid a third party from being able to cleverly inject a sophisticated attack to cause a crash or worse. Likewise the financial sector from collapsing. Crypto currency now makes a bit more sense with the terms de-centralized given the context of the security sector.