GLOBALRAIN

Practices for Secure Software Report

Table of Contents

Document Revision History

Version	Date	Author	Comments
1.0	**December 15, 2024**	**Christopher Phillips**	

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
Christopher Phillips

1. Algorithm Cipher

High-Level Overview: Recommend AES (Advanced Encryption Standard) with a 256-bit key.

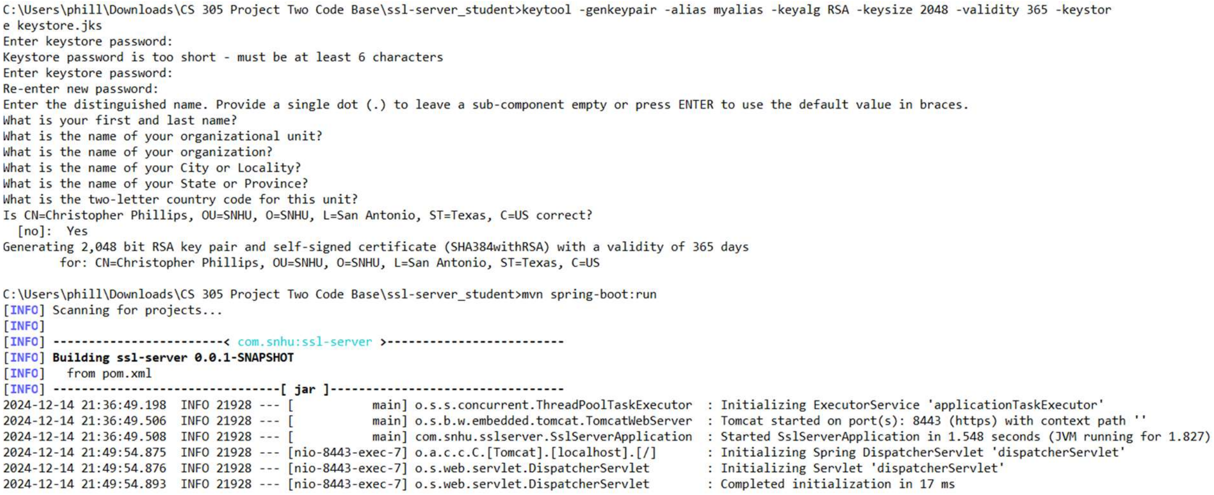
Overview: AES is a symmetric encryption algorithm widely used for securing sensitive data.
Hash Functions and Bit Levels: AES-256 uses 256-bit keys and provides excellent resistance against brute-force attacks.
Symmetric vs. Non-Symmetric Keys: AES is symmetric, meaning the same key encrypts and decrypts, making it fast and efficient for extensive data.

Random Numbers: Use a cryptographically secure pseudorandom number generator (CSPRNG) to generate keys for encryption.

History and Current State:

AES was established in 2001 by NIST.
Today, it is the standard for data encryption, surpassing DES and 3DES.

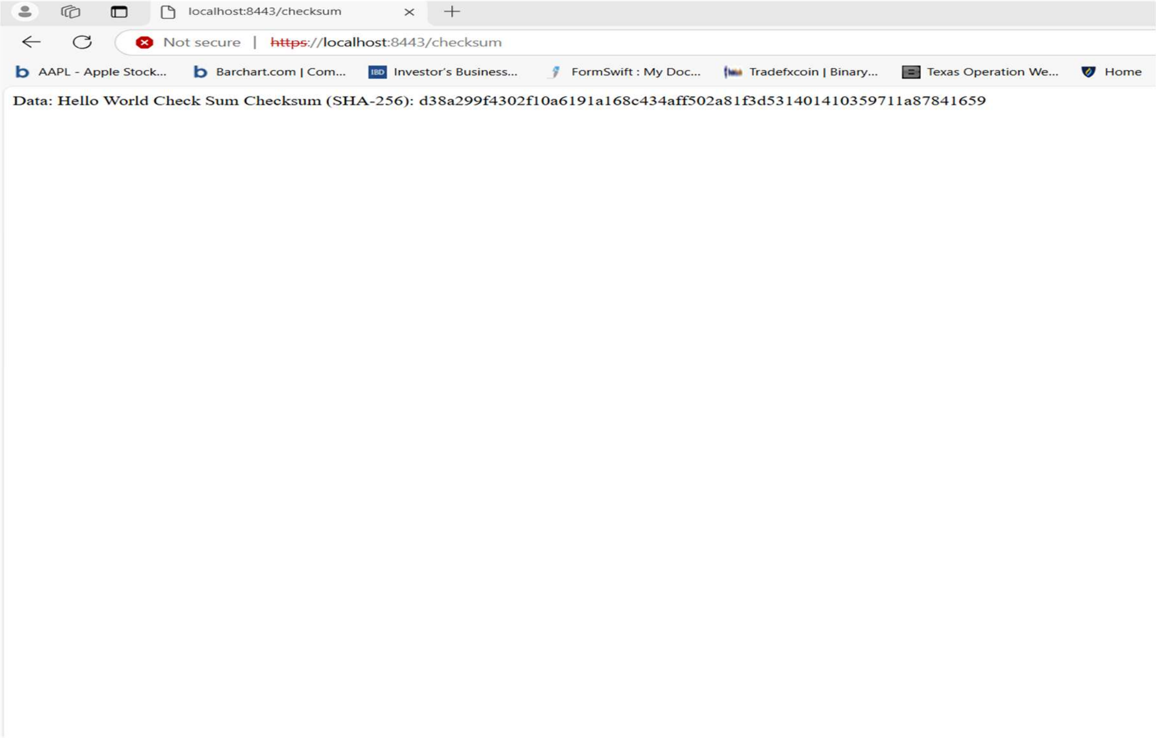
2. Certificate Generation



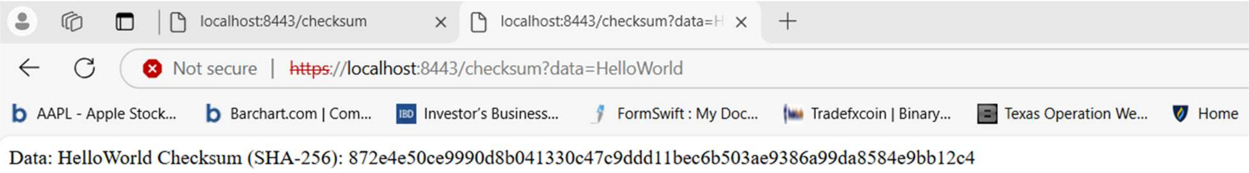
```
C:\Users\phill\Downloads\CS 305 Project Two Code Base\ssl-server_student>keytool -genkeypair -alias myalias -keyalg RSA -keysize 2048 -validity 365 -keystor
e keystore.jks
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Re-enter new password:
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in braces.
What is your first and last name?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
What is the name of your State or Province?
What is the two-letter country code for this unit?
Is CN=Christopher Phillips, OU=SNHU, O=SNHU, L=San Antonio, ST=Texas, C=US correct?
  [no]:  Yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 365 days
        for: CN=Christopher Phillips, OU=SNHU, O=SNHU, L=San Antonio, ST=Texas, C=US

C:\Users\phill\Downloads\CS 305 Project Two Code Base\ssl-server_student>mvn spring-boot:run
[INFO] Scanning for projects...
[INFO]
[INFO] -----------------------< com.snhu:ssl-server >------------------------
[INFO] Building ssl-server 0.0.1-SNAPSHOT
[INFO]   from pom.xml
[INFO] --------------------------------[ jar ]---------------------------------
2024-12-14 21:36:49.198  INFO 21928 --- [           main] o.s.s.concurrent.ThreadPoolTaskExecutor  : Initializing ExecutorService 'applicationTaskExecutor'
2024-12-14 21:36:49.506  INFO 21928 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8443 (https) with context path ''
2024-12-14 21:36:49.508  INFO 21928 --- [           main] com.snhu.sslserver.SslServerApplication  : Started SslServerApplication in 1.548 seconds (JVM running for 1.827)
2024-12-14 21:49:54.875  INFO 21928 --- [nio-8443-exec-7] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring DispatcherServlet 'dispatcherServlet'
2024-12-14 21:49:54.876  INFO 21928 --- [nio-8443-exec-7] o.s.web.servlet.DispatcherServlet        : Initializing Servlet 'dispatcherServlet'
2024-12-14 21:49:54.893  INFO 21928 --- [nio-8443-exec-7] o.s.web.servlet.DispatcherServlet        : Completed initialization in 17 ms
```

3. Deploy Cipher

Insert a screenshot below of the checksum verification.

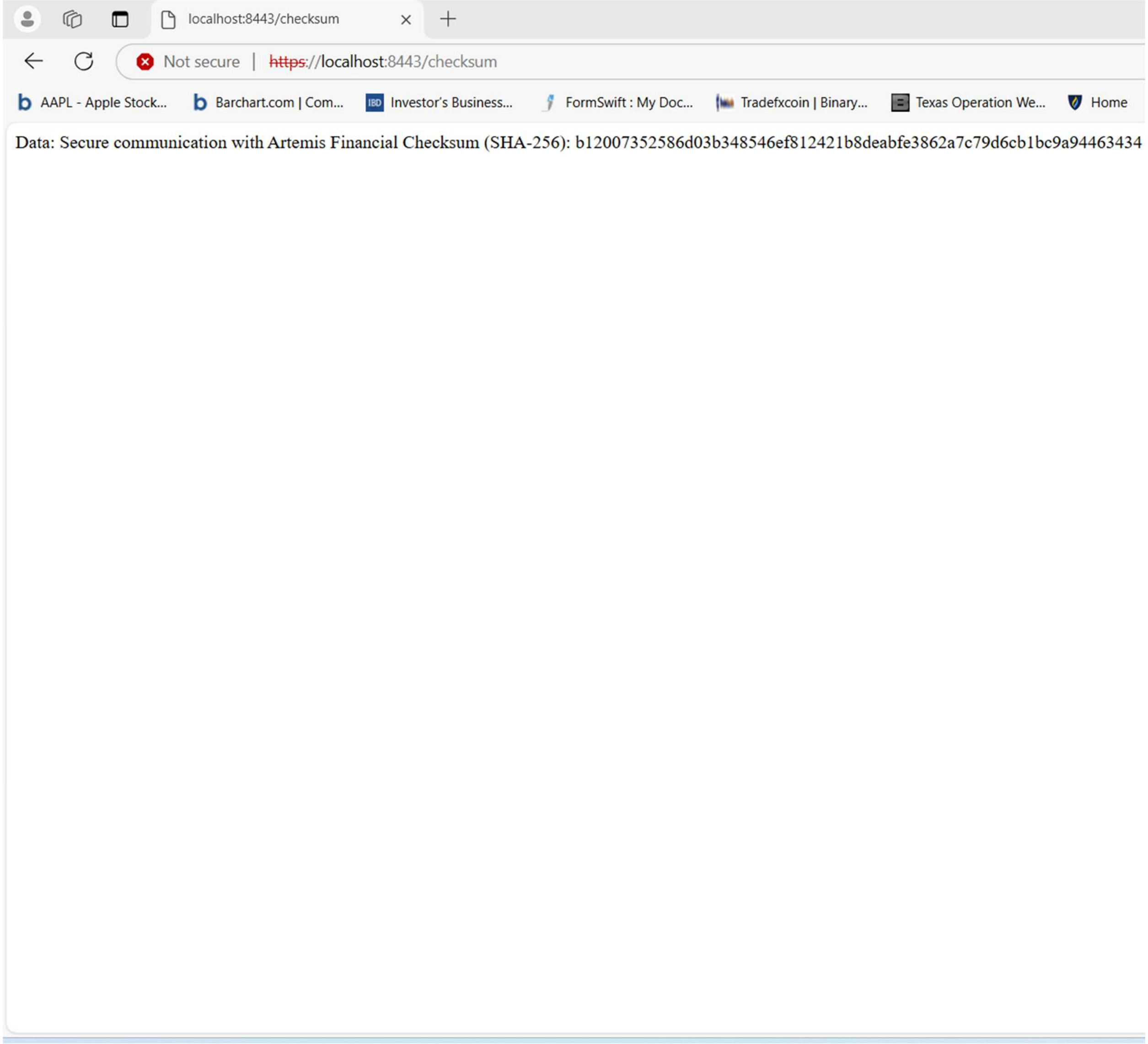


```
Data: Hello World Check Sum Checksum (SHA-256): d38a299f4302f10a6191a168c434aff502a81f3d531401410359711a87841659
```



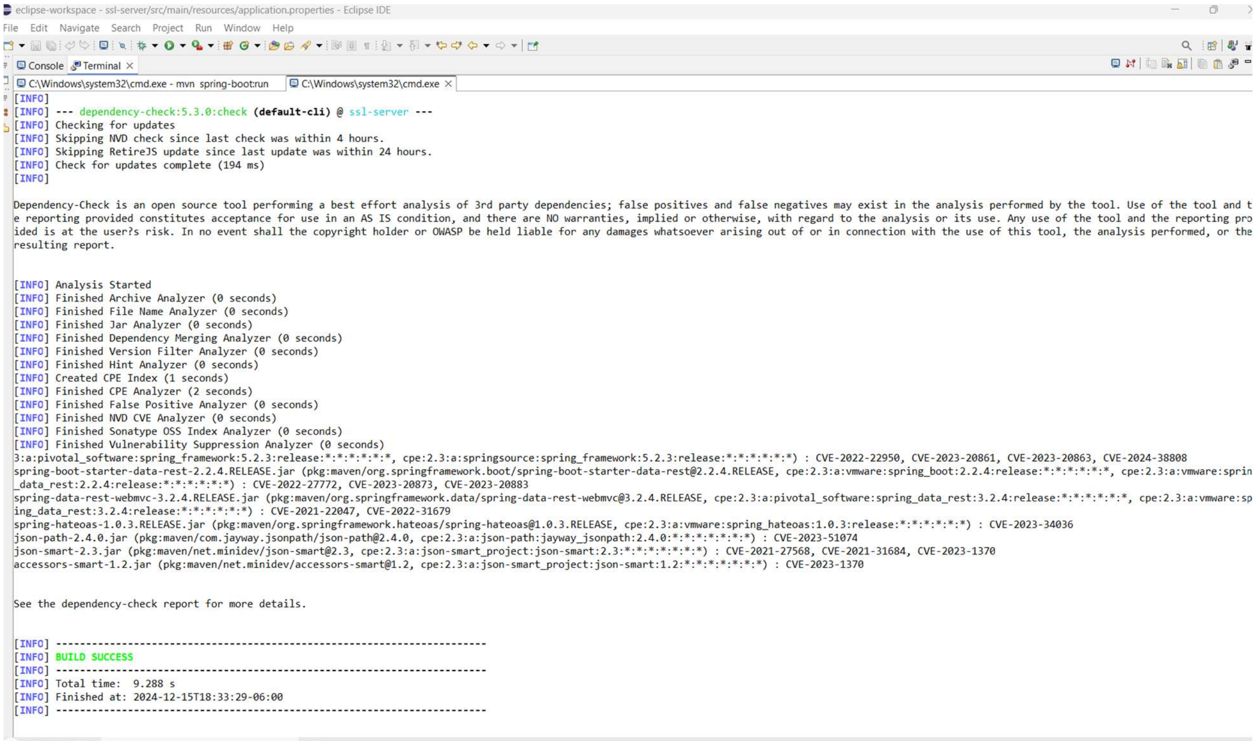
Data: HelloWorld Checksum (SHA-256): 872e4e50ce9990d8b041330c47c9ddd11bec6b503ae9386a99da8584e9bb12c4

4. Secure Communications



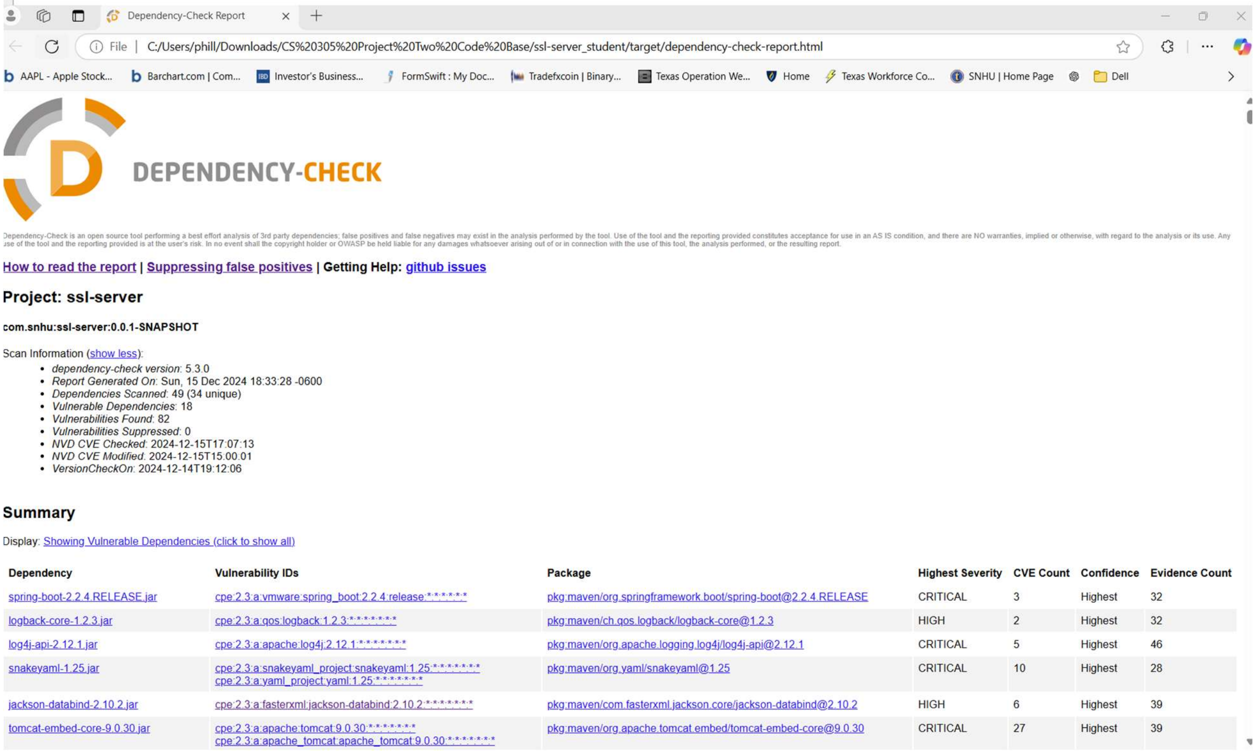
```
Data: Secure communication with Artemis Financial Checksum (SHA-256): b12007352586d03b348546ef812421b8deabfe3862a7c79d6cb1bc9a94463434
```

5. Secondary Testing



eclipse-workspace - ssl-server/src/main/resources/application.properties - Eclipse IDE
File Edit Navigate Search Project Run Window Help
Console
Terminal
C:\Windows\system32\cmd.exe - mvn spring-boot:run
C:\Windows\system32\cmd.exe

```
[INFO]
[INFO] --- dependency-check:5.3.0:check (default-cli) @ ssl-server ---
[INFO] Checking for updates
[INFO] Skipping NVD check since last check was within 4 hours.
[INFO] Skipping RetireJS update since last update was within 24 hours.
[INFO] Check for updates complete (194 ms)
[INFO]

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 t
e 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 pro
ided 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.


[INFO] Analysis Started
[INFO] Finished Archive Analyzer (0 seconds)
[INFO] Finished File Name Analyzer (0 seconds)
[INFO] Finished Jar Analyzer (0 seconds)
[INFO] Finished Dependency Merging Analyzer (0 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
[INFO] Finished Hint Analyzer (0 seconds)
[INFO] Created CPE Index (1 seconds)
[INFO] Finished CPE Analyzer (2 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[INFO] Finished Sonatype OSS Index Analyzer (0 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*, cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*) : CVE-2022-22950, CVE-2023-20861, CVE-2023-20863, CVE-2024-38808
spring-boot-starter-data-rest-2.2.4.RELEASE.jar (pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE, cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*, cpe:2.3:a:vmware:sprin
_data_rest:2.2.4:release:*:*:*:*:*:*) : CVE-2022-27772, CVE-2023-20873, CVE-2023-20883
spring-data-rest-webmvc-3.2.4.RELEASE.jar (pkg:maven/org.springframework.data/spring-data-rest-webmvc@3.2.4.RELEASE, cpe:2.3:a:pivotal_software:spring_data_rest:3.2.4:release:*:*:*:*:*:*, cpe:2.3:a:vmware:sp
ing_data_rest:3.2.4:release:*:*:*:*:*:*) : CVE-2021-22047, CVE-2022-31679
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
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:*:*:*:*:*:*:*) : CVE-2021-27568, CVE-2021-31684, CVE-2023-1370
accessors-smart-1.2.jar (pkg:maven/net.minidev/accessors-smart@1.2, cpe:2.3:a:json-smart_project:json-smart:1.2:*:*:*:*:*:*:*) : CVE-2023-1370


See the dependency-check report for more details.


[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  9.288 s
[INFO] Finished at: 2024-12-15T18:33:29-06:00
[INFO] ------------------------------------------------------------------------
```



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 less):

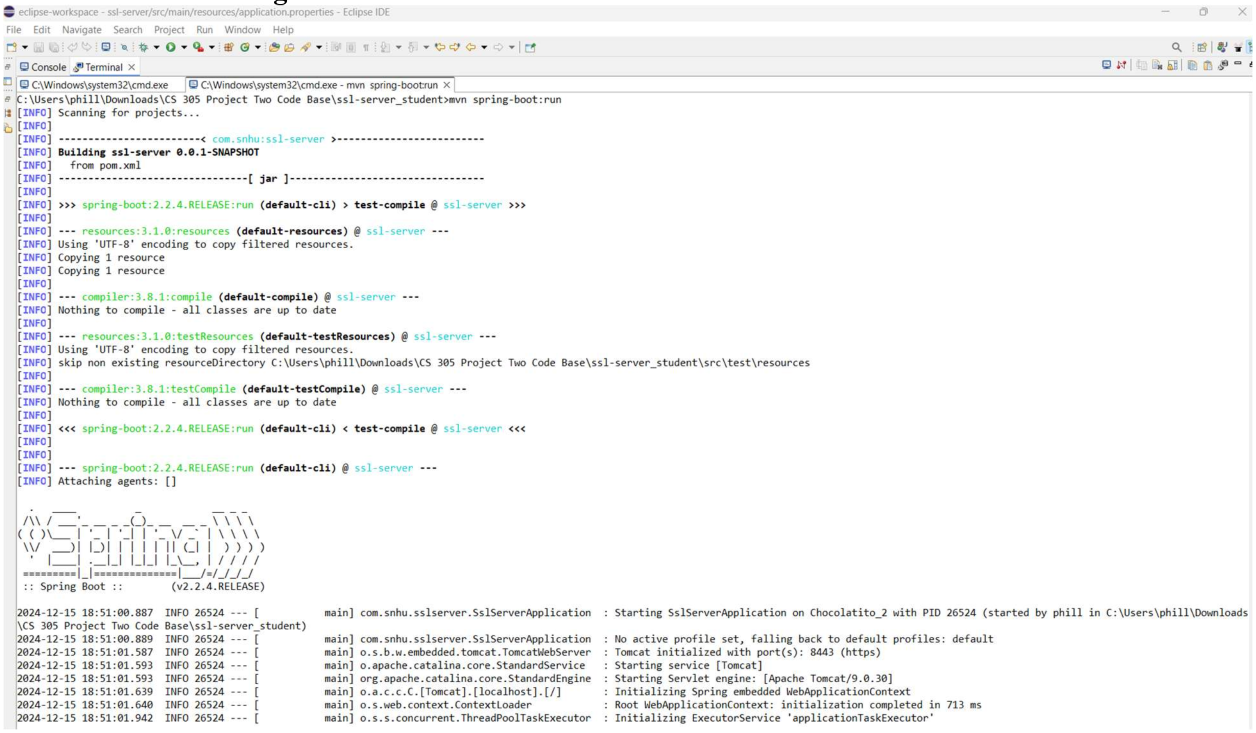
- *dependency-check version*: 5.3.0
- *Report Generated On*: Sun, 15 Dec 2024 18:33:28 -0600
- *Dependencies Scanned*: 49 (34 unique)
- *Vulnerable Dependencies*: 18
- *Vulnerabilities Found*: 82
- *Vulnerabilities Suppressed*: 0
- *NVD CVE Checked*: 2024-12-15T17:07:13
- *NVD CVE Modified*: 2024-12-15T15:00:01
- *VersionCheckOn*: 2024-12-14T19:12:06

Summary

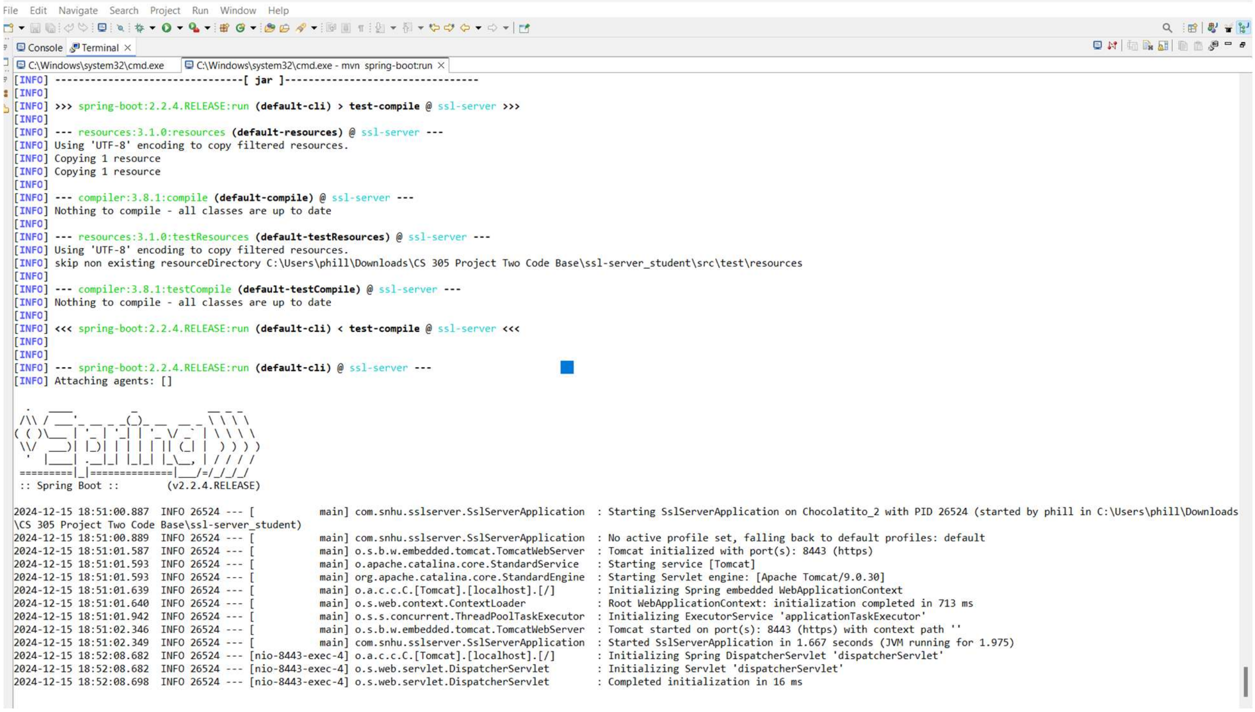
Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
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	32
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	32
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	CRITICAL	5	Highest	46
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	CRITICAL	10	Highest	28
jackson-databind-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	6	Highest	39
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	27	Highest	39

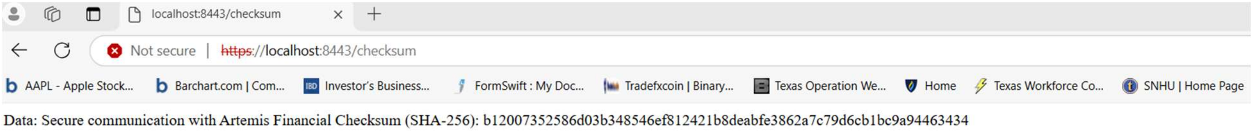
6. Functional Testing


eclipse-workspace - ssl-server/src/main/resources/application.properties - Eclipse IDE
File
Edit
Navigate
Search
Project
Run
Window
Help
Console
Terminal
C:\Windows\system32\cmd.exe
C:\Windows\system32\cmd.exe - mvn spring-boot:run

```
C:\Users\phill\Downloads\CS 305 Project Two Code Base\ssl-server_student>mvn spring-boot:run
[INFO] Scanning for projects...
[INFO]
[INFO] ------------------------< com.snhu:ssl-server >-------------------------
[INFO] Building ssl-server 0.0.1-SNAPSHOT
[INFO]   from pom.xml
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] >>> spring-boot:2.2.4.RELEASE:run (default-cli) > test-compile @ ssl-server >>>
[INFO]
[INFO] --- resources:3.1.0:resources (default-resources) @ ssl-server ---
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] Copying 1 resource
[INFO] Copying 1 resource
[INFO]
[INFO] --- compiler:3.8.1:compile (default-compile) @ ssl-server ---
[INFO] Nothing to compile - all classes are up to date
[INFO]
[INFO] --- resources:3.1.0:testResources (default-testResources) @ ssl-server ---
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] skip non existing resourceDirectory C:\Users\phill\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)

2024-12-15 18:51:00.887  INFO 26524 --- [           main] com.snhu.sslserver.SslServerApplication  : Starting SslServerApplication on Chocolatito_2 with PID 26524 (started by phill in C:\Users\phill\Downloads
\CS 305 Project Two Code Base\ssl-server_student)
2024-12-15 18:51:00.889  INFO 26524 --- [           main] com.snhu.sslserver.SslServerApplication  : No active profile set, falling back to default profiles: default
2024-12-15 18:51:01.587  INFO 26524 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s): 8443 (https)
2024-12-15 18:51:01.593  INFO 26524 --- [           main] o.apache.catalina.core.StandardService   : Starting service [Tomcat]
2024-12-15 18:51:01.593  INFO 26524 --- [           main] org.apache.catalina.core.StandardEngine  : Starting Servlet engine: [Apache Tomcat/9.0.30]
2024-12-15 18:51:01.639  INFO 26524 --- [           main] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring embedded WebApplicationContext
2024-12-15 18:51:01.640  INFO 26524 --- [           main] o.s.web.context.ContextLoader            : Root WebApplicationContext: initialization completed in 713 ms
2024-12-15 18:51:01.942  INFO 26524 --- [           main] o.s.s.concurrent.ThreadPoolTaskExecutor  : Initializing ExecutorService 'applicationTaskExecutor'
```


File
Edit
Navigate
Search
Project
Run
Window
Help
Console
Terminal
C:\Windows\system32\cmd.exe
C:\Windows\system32\cmd.exe - mvn spring-boot:run

```
[INFO] --------------------------------[ jar ]---------------------------------
[INFO]
[INFO] >>> spring-boot:2.2.4.RELEASE:run (default-cli) > test-compile @ ssl-server >>>
[INFO]
[INFO] --- resources:3.1.0:resources (default-resources) @ ssl-server ---
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] Copying 1 resource
[INFO] Copying 1 resource
[INFO]
[INFO] --- compiler:3.8.1:compile (default-compile) @ ssl-server ---
[INFO] Nothing to compile - all classes are up to date
[INFO]
[INFO] --- resources:3.1.0:testResources (default-testResources) @ ssl-server ---
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] skip non existing resourceDirectory C:\Users\phill\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)

2024-12-15 18:51:00.887  INFO 26524 --- [           main] com.snhu.sslserver.SslServerApplication  : Starting SslServerApplication on Chocolatito_2 with PID 26524 (started by phill in C:\Users\phill\Downloads
\CS 305 Project Two Code Base\ssl-server_student)
2024-12-15 18:51:00.889  INFO 26524 --- [           main] com.snhu.sslserver.SslServerApplication  : No active profile set, falling back to default profiles: default
2024-12-15 18:51:01.587  INFO 26524 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s): 8443 (https)
2024-12-15 18:51:01.593  INFO 26524 --- [           main] o.apache.catalina.core.StandardService   : Starting service [Tomcat]
2024-12-15 18:51:01.593  INFO 26524 --- [           main] org.apache.catalina.core.StandardEngine  : Starting Servlet engine: [Apache Tomcat/9.0.30]
2024-12-15 18:51:01.639  INFO 26524 --- [           main] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring embedded WebApplicationContext
2024-12-15 18:51:01.640  INFO 26524 --- [           main] o.s.web.context.ContextLoader            : Root WebApplicationContext: initialization completed in 713 ms
2024-12-15 18:51:01.942  INFO 26524 --- [           main] o.s.s.concurrent.ThreadPoolTaskExecutor  : Initializing ExecutorService 'applicationTaskExecutor'
2024-12-15 18:51:02.346  INFO 26524 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8443 (https) with context path ''
2024-12-15 18:51:02.349  INFO 26524 --- [           main] com.snhu.sslserver.SslServerApplication  : Started SslServerApplication in 1.667 seconds (JVM running for 1.975)
2024-12-15 18:52:08.682  INFO 26524 --- [nio-8443-exec-4] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring DispatcherServlet 'dispatcherServlet'
2024-12-15 18:52:08.682  INFO 26524 --- [nio-8443-exec-4] o.s.web.servlet.DispatcherServlet        : Initializing Servlet 'dispatcherServlet'
2024-12-15 18:52:08.698  INFO 26524 --- [nio-8443-exec-4] o.s.web.servlet.DispatcherServlet        : Completed initialization in 16 ms
```



```
Data: Secure communication with Artemis Financial Checksum (SHA-256): b12007352586d03b348546ef812421b8deabfe3862a7c79d6cb1bc9a94463434
```

7. Summary

Successfully upgraded Artemis Financials' application to ensure secure communication and implement checksum functionality. This involved cleaning up the existing code to boost security and thoroughly testing the application to make sure everything works properly and meets security standards.

Implemented a checksum algorithm, SHA-256, to ensure that data remains intact during communication. To enhance security, I generated a self-signed certificate using Java Keytool, which enabled us to establish HTTPS for secure communication. Updated the application's properties to incorporate HTTPS support with the newly created keystore.

To verify the security of our application, I utilized OWASP Dependency-Check to ensure that the refactoring process did not introduce any new vulnerabilities. Additionally, thoroughly tested the checksum endpoint to confirm its proper functionality and the establishment of secure communication via HTTPS.

With these enhancements, the Artemis Financial application now meets modern security standards, giving us confidence in the integrity and confidentiality of data transmissions.

8. Industry Standard Best Practices

The revised application incorporates key industry best practices for secure software development. Implemented SHA-256, a widely recognized cryptographic hash function, to generate checksums and ensure the integrity of our data. To enhance secure communication, I established HTTPS with a self-signed SSL certificate to encrypt data during transmission, significantly reducing the risk of eavesdropping and man-in-the-middle attacks. Additionally, sensitive configurations, such as keystore paths and passwords, are carefully managed within the application properties file to maintain security.

For dependency management, I utilized OWASP Dependency-Check to scan project dependencies for known vulnerabilities, helping address potential security issues at the library level. Testing protocols involved performing functional testing to confirm that the application behaves as expected, ensuring all features work correctly. Furthermore, additional testing was conducted to verify that no new security vulnerabilities emerged during the development process. To enhance clarity and maintainability, captured the checksum functionality within a dedicated service (ChecksumService) and adhered to proper RESTful design patterns.

By incorporating these best practices, the updated application ensures that Artemis Financial's client data remains secure and reliable. This proactive approach to software security protects our clients and bolsters our reputation and ensures compliance with data protection standards.

Citations:

- National Institute of Standards and Technology. (2015). *Secure hash standard (SHS)* (FIPS PUB 180-4). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.180-4
- Oracle Corporation. (2024). *Java Platform, Standard Edition Tools Reference*. Oracle. https://docs.oracle.com/en/java/
- OWASP Foundation. (2024). *OWASP Dependency-Check*. https://owasp.org/www-project-dependency-check/