****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **04/13/2023** | **Philip Trinh** |  |

## Client



## Instructions

Submit these 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

Philip Trinh

## Algorithm Cipher

A cryptographic algorithm cipher is used to encrypt and decrypt data. Using a mathematical function, plaintext is converted into ciphertext, and the process is then reversed to perform decryption.

Hash functions are used to create a fixed-size output known as hash value from a variable-size input. The number of bits in the cipher might range from 128 bits to 256 bits or more, depending on the specific technique utilized.

In encryption, random numbers are employed to introduce unpredictability and so add an additional layer of protection. Non-symmetric keys utilize a distinct key for each procedure while symmetric keys use the same key for both encryption and decryption.

The history of encryption techniques began in ancient civilizations who employed substitution ciphers to encrypt communications. Since the invention of computers, encryption methods have developed into increasingly intricate algorithms like Rivest-Shamir-Adleman (RSA) and the Advanced Encryption Standard (AES). AES, RSA, and Elliptic Curve Cryptography (ECC), among other industry-standard algorithms, are currently employed in many different applications, demonstrating how far encryption methods have come. In sectors including finance, healthcare, and government encryption is widely utilized since it is essential for protecting sensitive data, serving as a deterrence to attackers who want to access data for personal gain. To remain ahead of possible security problems, encryption algorithms must continue to advance with the rise in computing power and the sophistication of assaults.

## Certificate Generation

## Certificate file of server.cer can be found in the project file attached.

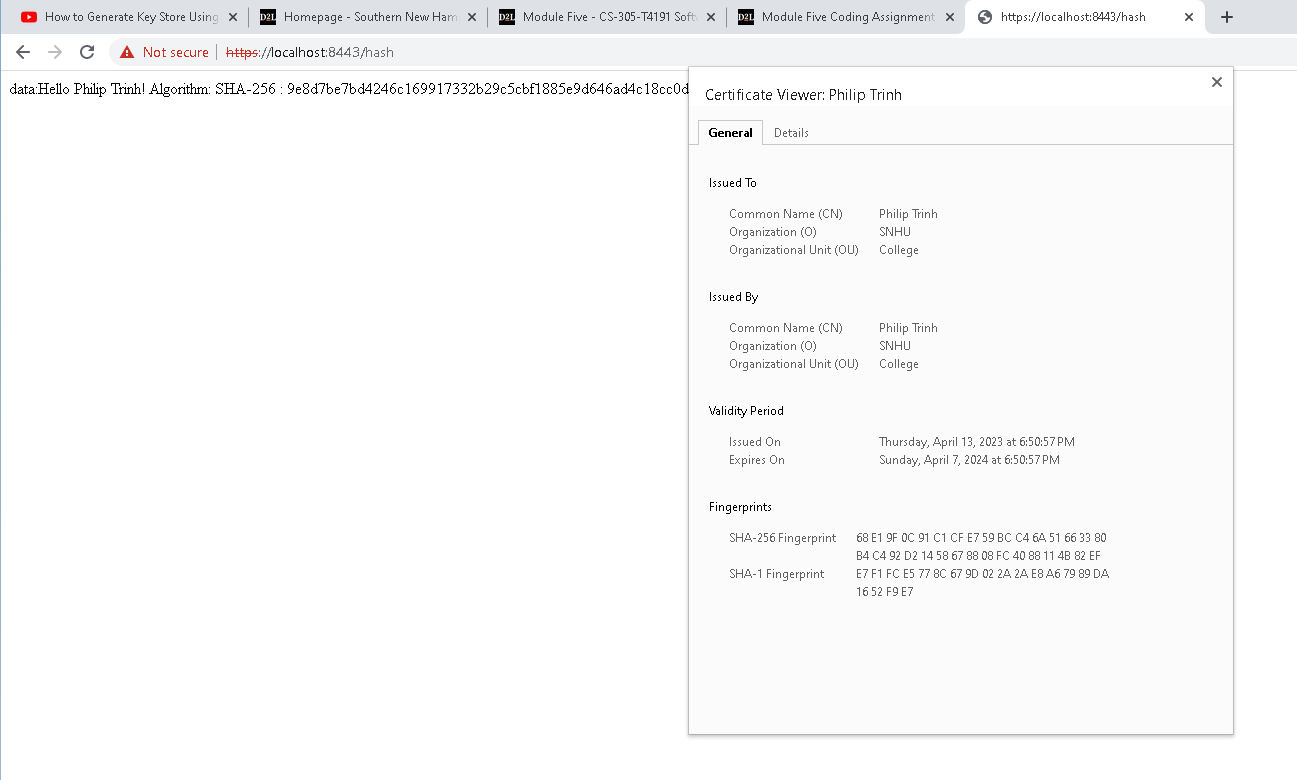
## Deploy Cipher

## Checksum verification

## Secure Communications

web browser that shows a secure webpage HTTPS protocol

Graphical user interface, text, application

Description automatically generated

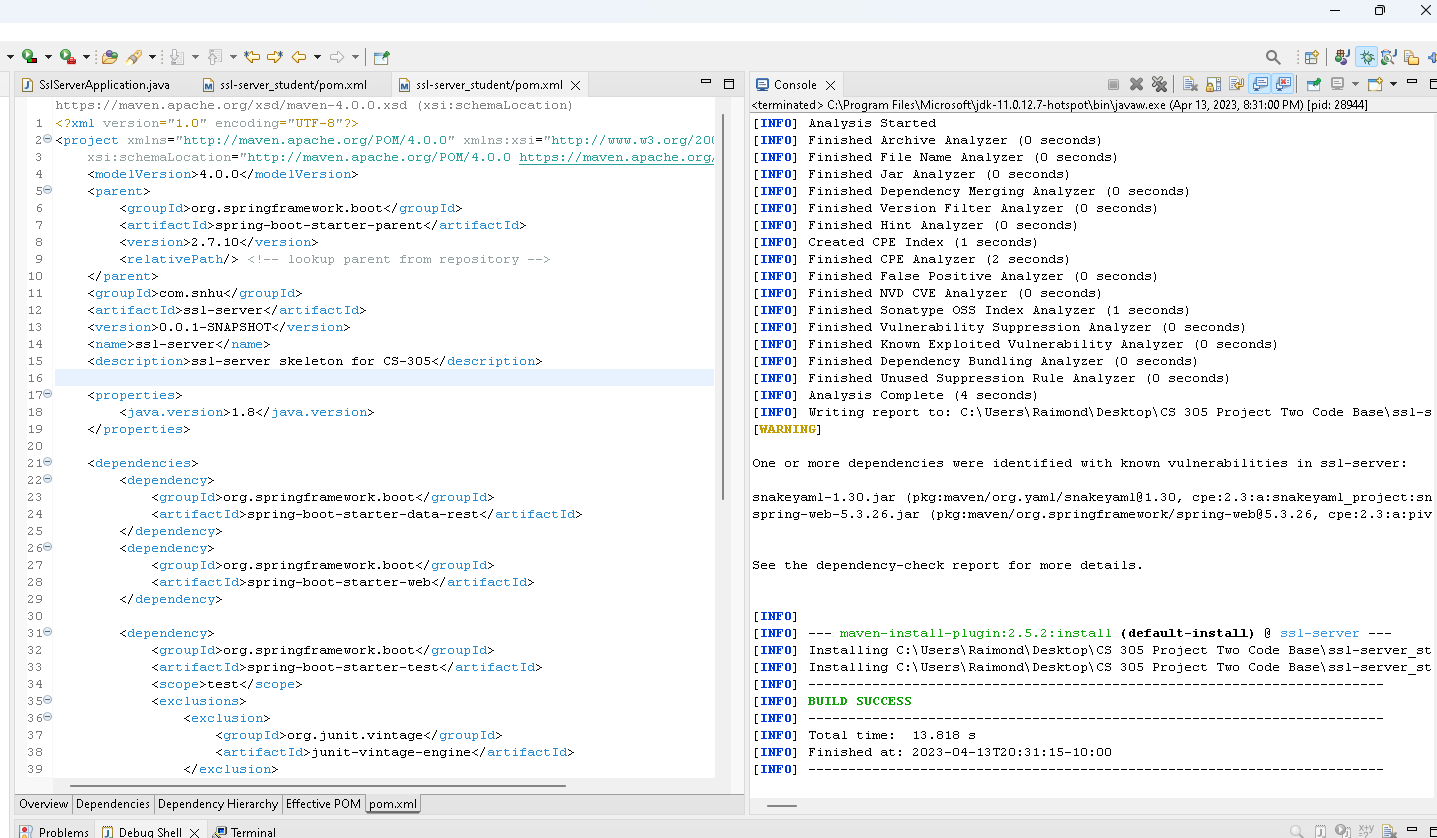
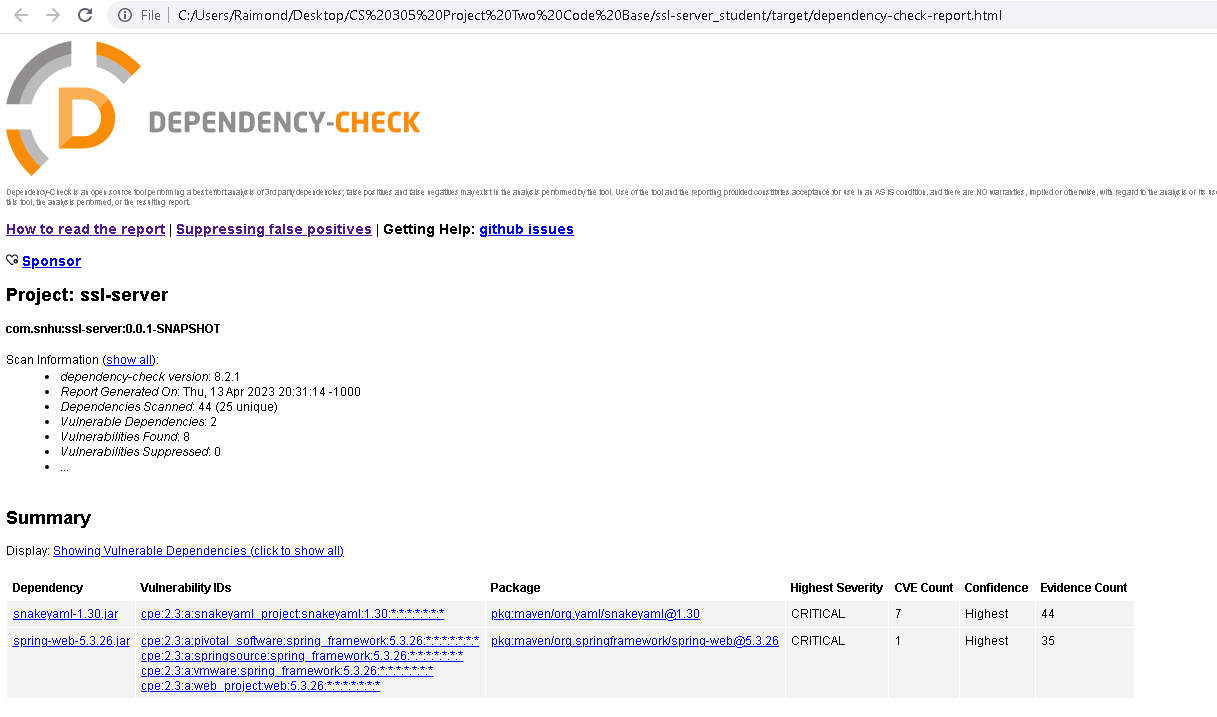
## Secondary Testing

Graphical user interface, text, email

Description automatically generatedGraphical user interface, text, application

Description automatically generatedThe refactored code was executed without errors and the dependency-check report

## Functional Testing

Refactored code executed without errors.

## Summary

1. SECURE CODING: The code complies with the vulnerability assessment's Secure Coding criteria by using the text variable to generate a SHA-256 hash and adding the RESTful API map to the hash.
2. APIs: API issues were addressed by updating dependencies. The spring framework-boot parent was out of date (2.2.4. RELEASE) and updated to the latest version possible (2.7.10) due to not being able to update to the 3X version.
3. Cryptography: the code now includes the SHA-256 hash function and checksum verification. 4)
4. Client/Server: Communication security issues between the client and server were addressed by generating a certificate and implementing the SSL/HTTPS protocol.
5. Code Quality: identify and address errors and improve adherence to security best practices by keeping the code short and concise.

To enhance security, I began to create a self-signed certificate first, which allows SSL/HTTPS protocol-based communication between the client and server. This is essential for a financial institution like Artemis Financial. Getting a trusted CA certificate would be the next step before deployment.

To create checksums that ensure the data's integrity during transmission between the server and clients, a hash creation approach was also used.

By running the dependency-check, 94 vulnerabilities were discovered out of 49 dependencies scanned, and the majority were fixed by simply updating the spring framework-boot package from version 2.2.4 to version 2.7.10. The number essentially lowered to 8 out of 44 scanned. Dependencies are essential for creating modern web applications, but if they are not frequently updated and maintained, they could compromise platform security. It is advised to verify dependencies regularly and update it even after the product passes QA.

## Industry Standard Best Practices

When writing code, industry-recognized secure coding best practices should be used to fix known security flaws. I normally follow these steps:

1. User input validation: This safeguard ensures that the server only takes legitimate data and thwarts any potential attacks that make use of false or malicious data.
2. Using HTTPS encryption: The application had HTTPS encryption set up. Secure connection between the server and clients is ensured by the properties file, preventing the transmission of sensitive data in plaintext.
3. Hashing sensitive data: By rendering sensitive data unreadable, hashing lowers the possibility of data interception and the ability to reverse-engineer data to obtain the original data.
4. Limiting exposure: By restricting exposed routes and data, code was refactored to lower the application's possible attack surface and make it more resistant to attacks.
5. Update regularly: Maintaining the program with the most recent security patches and upgrades fixes will help eliminate known vulnerabilities before attackers may exploit them.

Following these best practices helps to maintain the security of the software program and will help to lower the danger of potential security flaws and vulnerabilities. By doing this, the business is better protected from potential risks such as data breaches, intellectual property theft, brute force attack, ransomware, etc. Additionally, observing pertinent rules, regulations, and industry standards fosters confidence among stakeholders and clients, helping business grow and make customers happy.

REFERENCES

Thales Group. (2016, April 18). A brief history of encryption | Thales Group.

Www.thalesgroup.com. <https://www.thalesgroup.com/en/markets/digital-identity-and->

security/magazine/brief-history-encryption

Scholten (guests), P. S. & U. (n.d.). The Role of Random Number

Generators in HSMs & Key Management. Www.cryptomathic.com. Retrieved March 27,

2023, from <https://www.cryptomathic.com/news-events/blog/the-role-of-random-number-generators-in-relation-to-hsms-key-management#:~:text=The%20role%20of%20RNGs%20in>

Hougen, A. (2021, May 24). What Is AES Encryption & How Does It Work in 2022?

[256-bit vs 128-bit]. Cloudwards. <https://www.cloudwards.net/what-is->

aes/#:~:text=The%20AES%20algorithm%20is%20the

Daniel, B. (2021, May 4). Symmetric vs. Asymmetric Encryption: What’s the Difference?

Www.trentonsystems.com. <https://www.trentonsystems.com/blog/symmetric-vs->

asymmetric-

encryption#:~:text=Unlike%20symmetric%20encryption%2C%20which%20uses

Anusheh, M. What is the AES algorithm? (n.d.). Retrieved 26 March, 2023

Educative: Interactive Courses for Software Developers.

<https://www.educative.io/answers/what-is-the-aes-algorithm>