****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_heading=h.2dj8z09oo0hk)

[**Client 3**](#_heading=h.guxqgnqfawc1)

[**Instructions 3**](#_heading=h.oz9g41k04uv9)

[**Developer 4**](#_heading=h.iqzoz5c3wdpx)

[**1. Algorithm Cipher 4**](#_heading=h.qyxfazg947jx)

[**2. Certificate Generation 4**](#_heading=h.8xvh02fw8nod)

[**3. Deploy Cipher 4**](#_heading=h.easm9v77510d)

[**4. Secure Communications 4**](#_heading=h.3cwo59gzwpti)

[**5. Secondary Testing 4**](#_heading=h.4lqyleu3ogw6)

[**6. Functional Testing 4**](#_heading=h.mqhy9cl4m4ci)

[**7. Summary 4**](#_heading=h.dnag76qxuhdi)

[**8. Industry Standard Best Practices 4**](#_heading=h.fw85w0xcvndh)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **04/20/2025** | **Jerry Vasquez** |  |

## Client



## 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

Jerry Vasquez

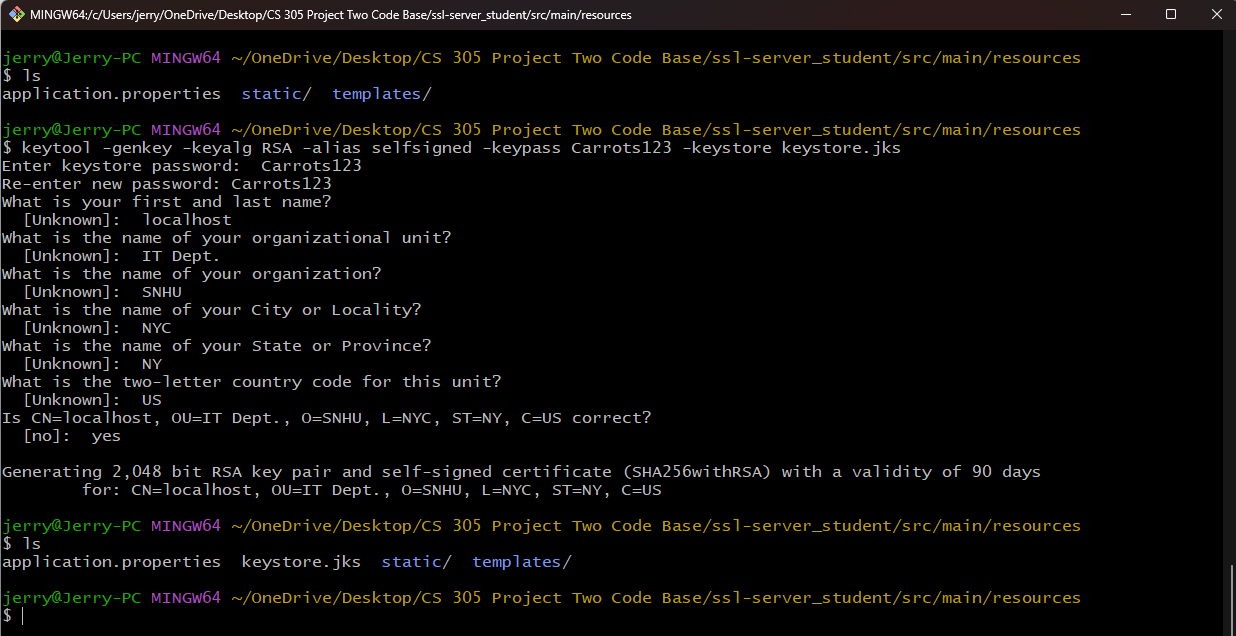
## Algorithm Cipher

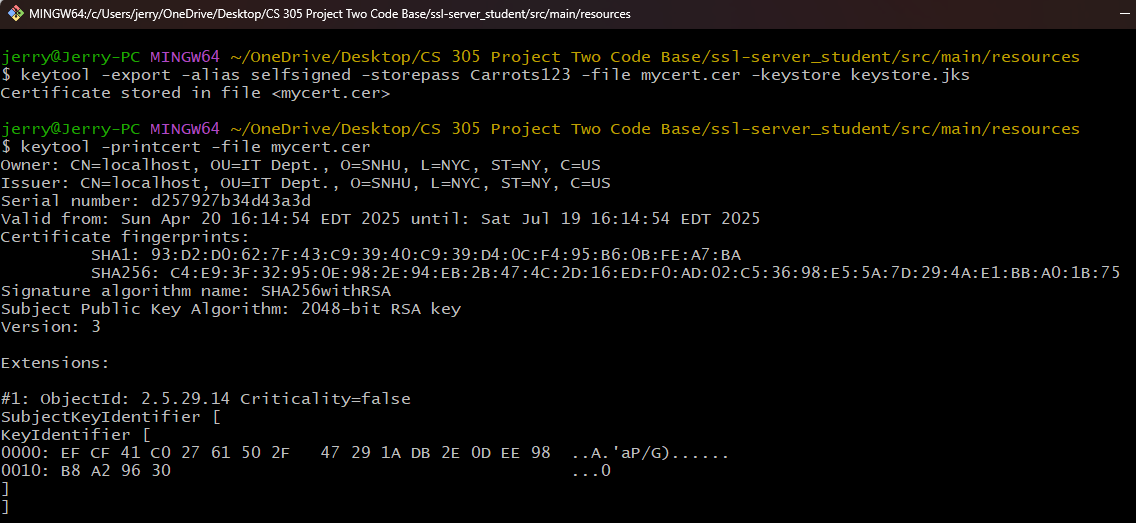
Artemis Financial is responsible for the security of its organizational and client information which can include financial documents, business transactions, and client PII (personally identifiable information). As a security measure, file encryption is a method used to prevent unauthorized access or unwanted modifications of information during data transmission or at rest. There are different cipher algorithms that implement file encryption and decryption using keys. One such algorithm that stands out and is recommended for Artemis Financial’s system is the Advanced Encryption Standard (AES) 256.

AES-256 is a symmetric block cipher algorithm that uses a 256-bit length key for encrypting and decrypting data (Kiteworks, 2022). It is known as the most effective encryption algorithm, often described as impenetrable, that is used by many organizations including the U.S. government to protect confidential information (Kananda, 2022).

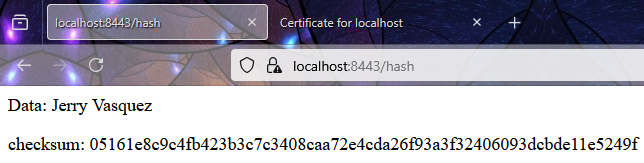
With a symmetric key encryption, the same secret key is used to convert plaintext to ciphertext or ciphertext to plaintext (Loshin, 2021.). This differs from asymmetric encryption that employs a public and private key, where one is used for encryption and the other for decryption (Loshin, 2021). According to an article by Kananda, some of the benefits for using a symmetric key encryption are that they are fast at encrypting data, good for internal or organizational data, great for encrypting large volumes of data, and require less computation to run (Kananda, 2022). With these benefits, Artemis Financial’s system can safeguard the large volumes of sensitive company and client data without sacrificing performance of the system.

## Certificate Generation





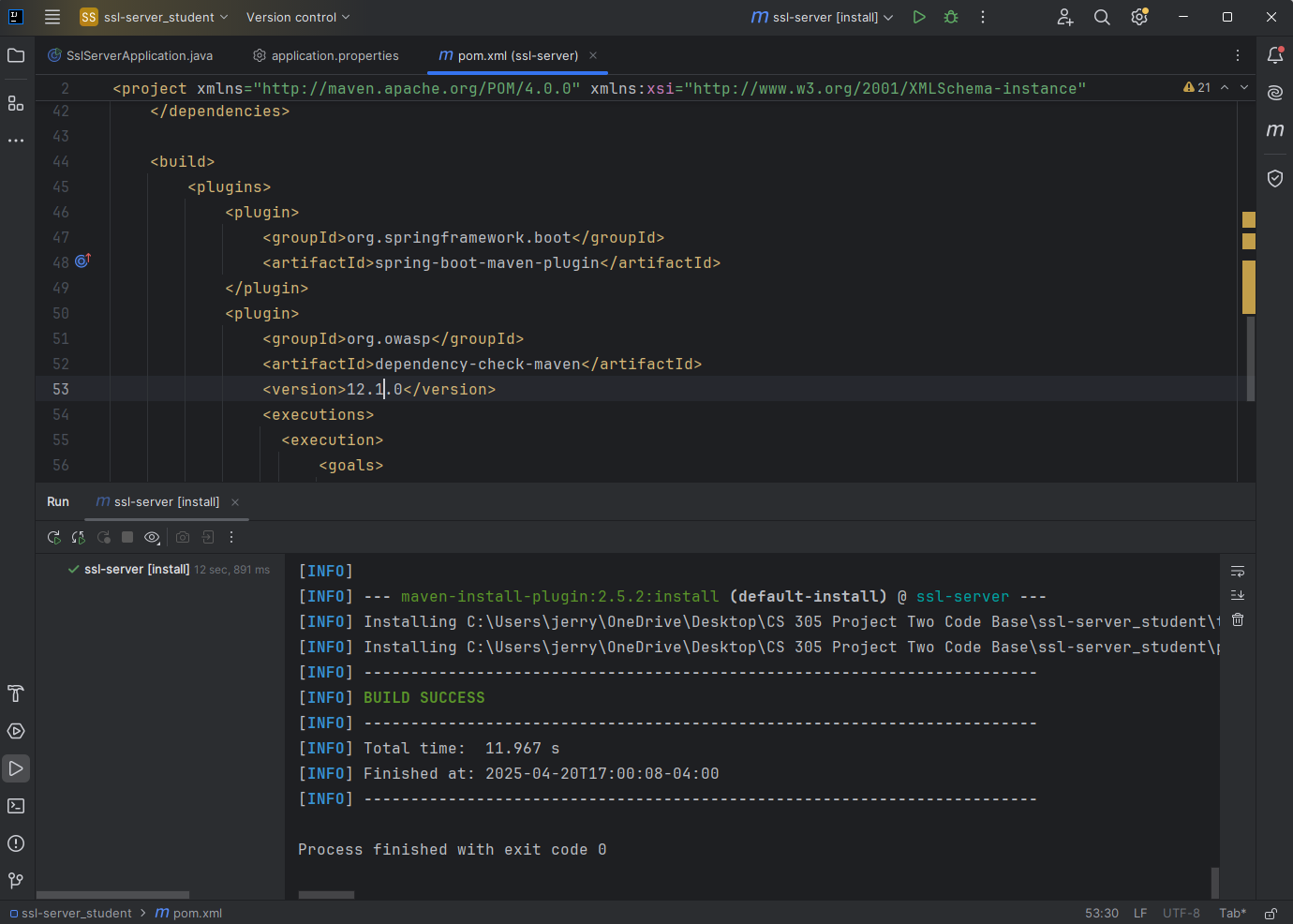
## Deploy Cipher

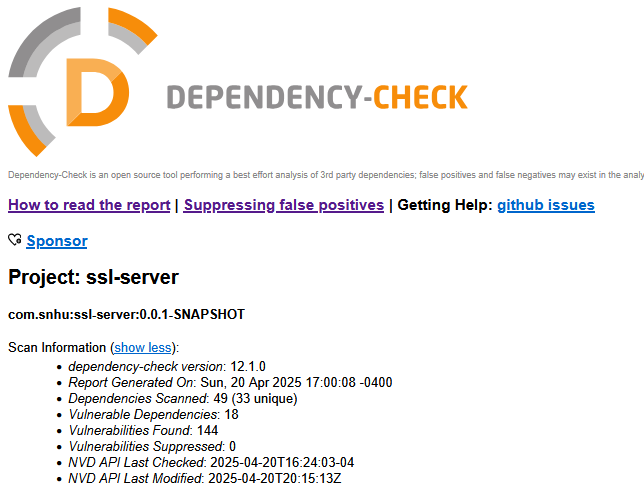


## Secure Communications

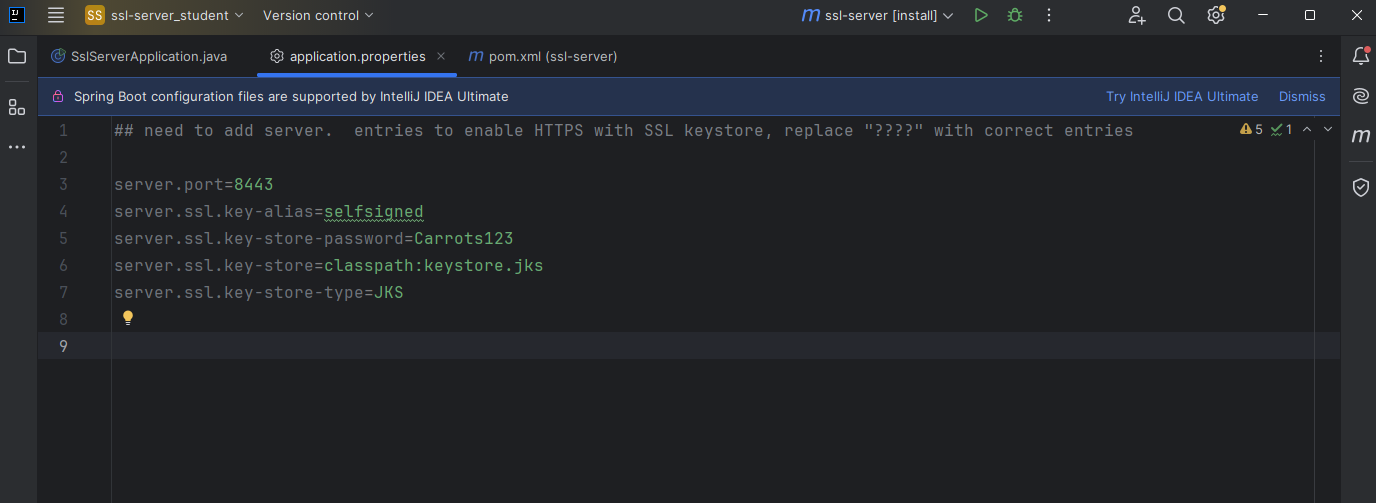
## 

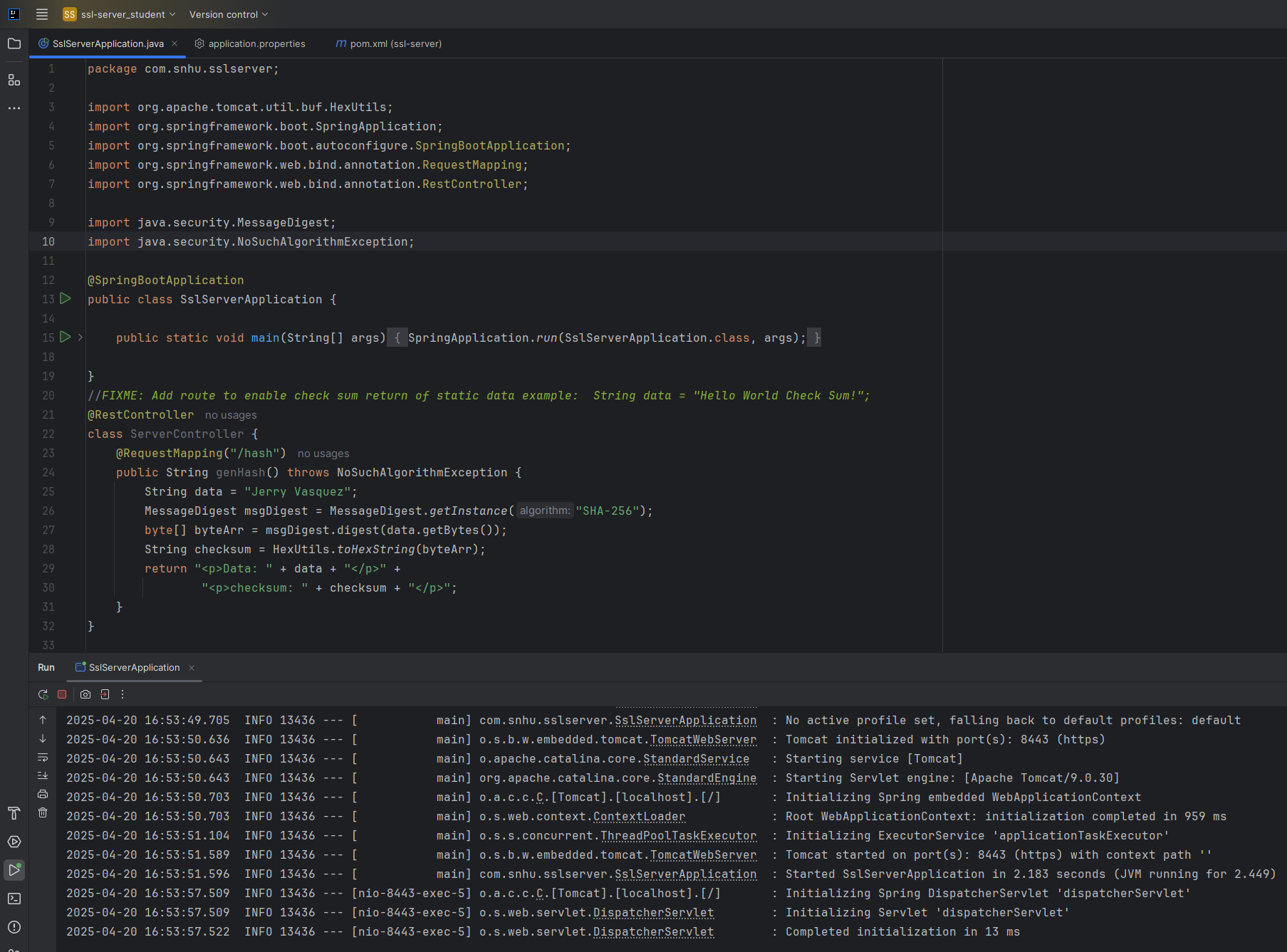
## Secondary Testing





## Functional Testing





## Summary

The code base has been refactored to run on HTTPS protocol to enable secure communication between the client and the server. The communication between the client and server employs SSL/TLS to encrypt data both at rest and during transit.

## Industry Standard Best Practices

The value of applying industry standard best practices for secure coding is that we are able to promote data protection and integrity and minimize the risk of security breaches. Maintaining secure coding practices can also help to save time and money by reducing the need to patch vulnerabilities found after release (Ghalleb, 2024). Secure coding can also help us maintain trust with our users by ensuring that their personal information is protected (Ghalleb, 2024).

**References**

* Kiteworks. (2022, September 6). *AES 256 Encryption: What Is AES 256 Encryption?.* Kiteworks. [https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/](https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/#:~:text=AES%2D256%20encryption%20is%20extremely,operating%20in%20highly%20regulated%20industries)
* Loshin, P. (2021, October). *What is a cryptographic cipher?.* TechTarget. <https://www.techtarget.com/searchsecurity/definition/cipher>
* Kananda, V. (2022, June 22). *What Is AES 256 Encryption & How Does it Work?.* Progress. <https://www.progress.com/blogs/use-aes-256-encryption-secure-data>
* Ghalleb, Z. (2024, November 26). *What is Secure Coding? Overview and Best Practices*. Wiz. <https://www.wiz.io/academy/secure-coding-best-practices>