****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc575442617)

[Table of Contents 1](#_Toc2146715)

[Document Revision History 2](#_Toc560396609)

[Client 3](#_Toc1292772914)

[Instructions 3](#_Toc205041299)

[Developer 3](#_Toc228366552)

[1. Algorithm Cipher 4](#_Toc745374613)

[2. Certificate Generation 4](#_Toc362260141)

[3. Deploy Cipher 5](#_Toc1906648847)

[4. Secure Communications 5](#_Toc2107532601)

[5. Secondary Testing 5](#_Toc162602807)

[6. Functional Testing 6](#_Toc1154896542)

[7. Summary 7](#_Toc734815307)

[8. Industry Standard Best Practices 7](#_Toc664287396)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **7/31/25** | **Anthony Wilkinson** |  |

## 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

Anthony Wilkinson

## Algorithm Cipher

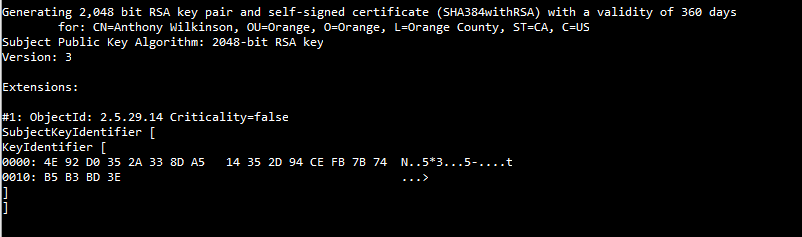
**Recommendation: Implement AES-256 Encryption at Artemis Financial**

To protect sensitive financial data, I recommend implementing the AES-256 encryption algorithm at Artemis Financial. AES is widely recognized as the industry standard for encrypting confidential information. It provides strong resistance to brute force attacks, and to date, has no known vulnerabilities. In addition to its security, AES is also efficient and scalable, making it capable of handling high volumes of encrypted transactions without sacrificing performance.

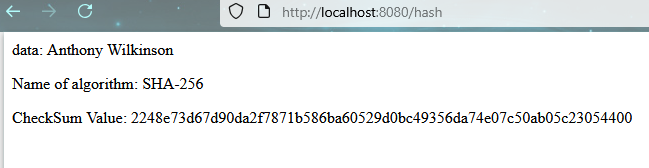
AES encrypts data through multiple rounds of transformation. Each round includes several steps: adding a round key, substituting bytes, row shifting, and column mixing. AES uses a symmetric key, meaning the same key is used for both encryption and decryption. These keys are generated using random numbers and have varying lengths. The length of the key (bit level) determines how many rounds of data transformation the encryption performs. For example, a 128-bit key uses 10 rounds, and a 256-bit key uses 14 rounds. Ultimately the more bits in the key, the more secure the cipher is.

The task performed by AES—encryption—can be traced back thousands of years. For example, Julius Caeser invented the Caeser cipher, a method that shifts letters in the alphabet. Modern computer encryption started in the 1970s with the development of the Data Encryption Standard (DES). DES began to fall out of favor in 1997 when it was cracked. Since then, it has been largely replaced by the AES encryption standard.

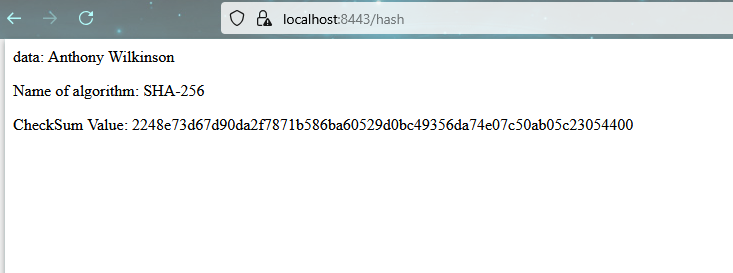
## Certificate Generation



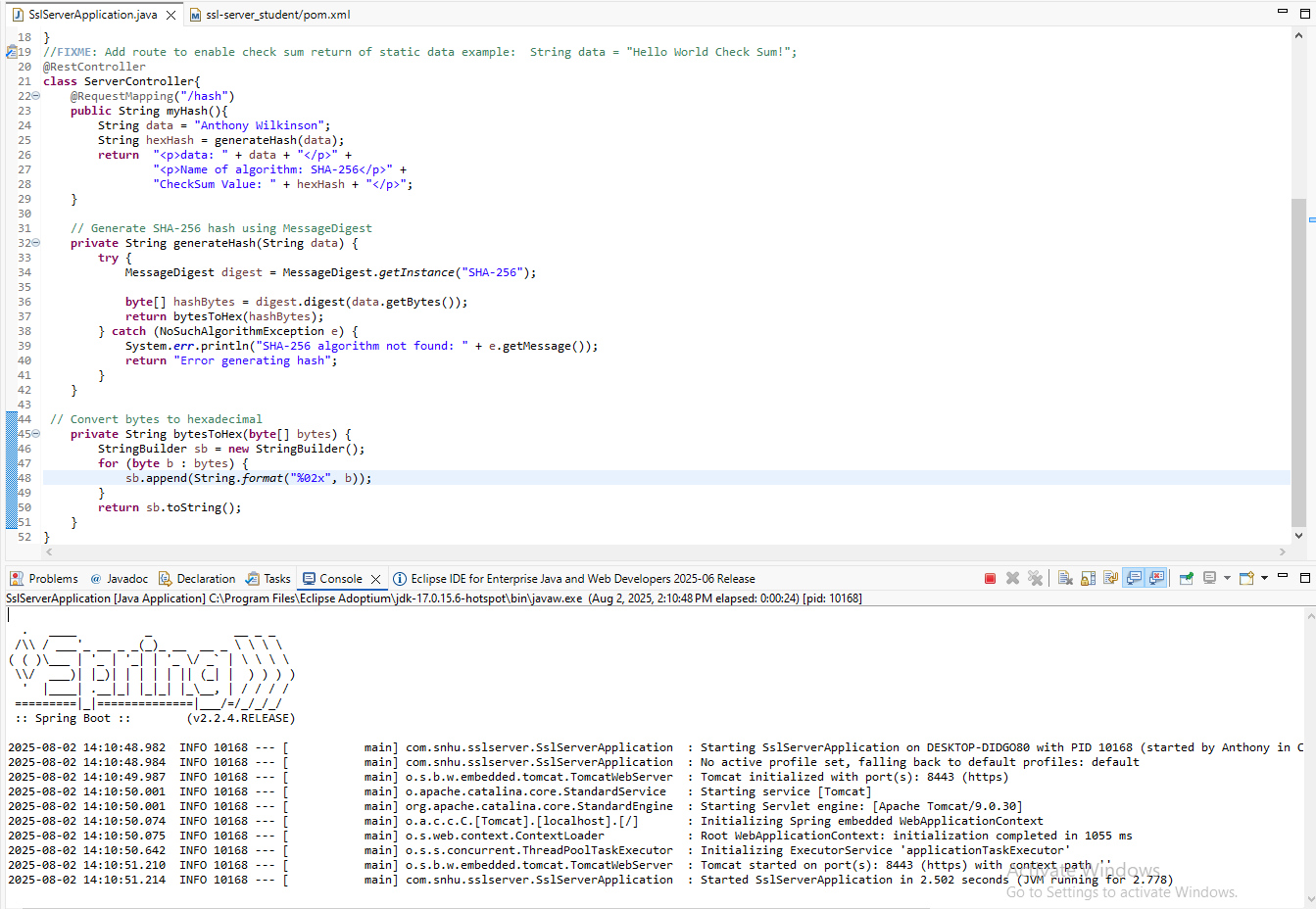
## Deploy Cipher



## Secure Communications

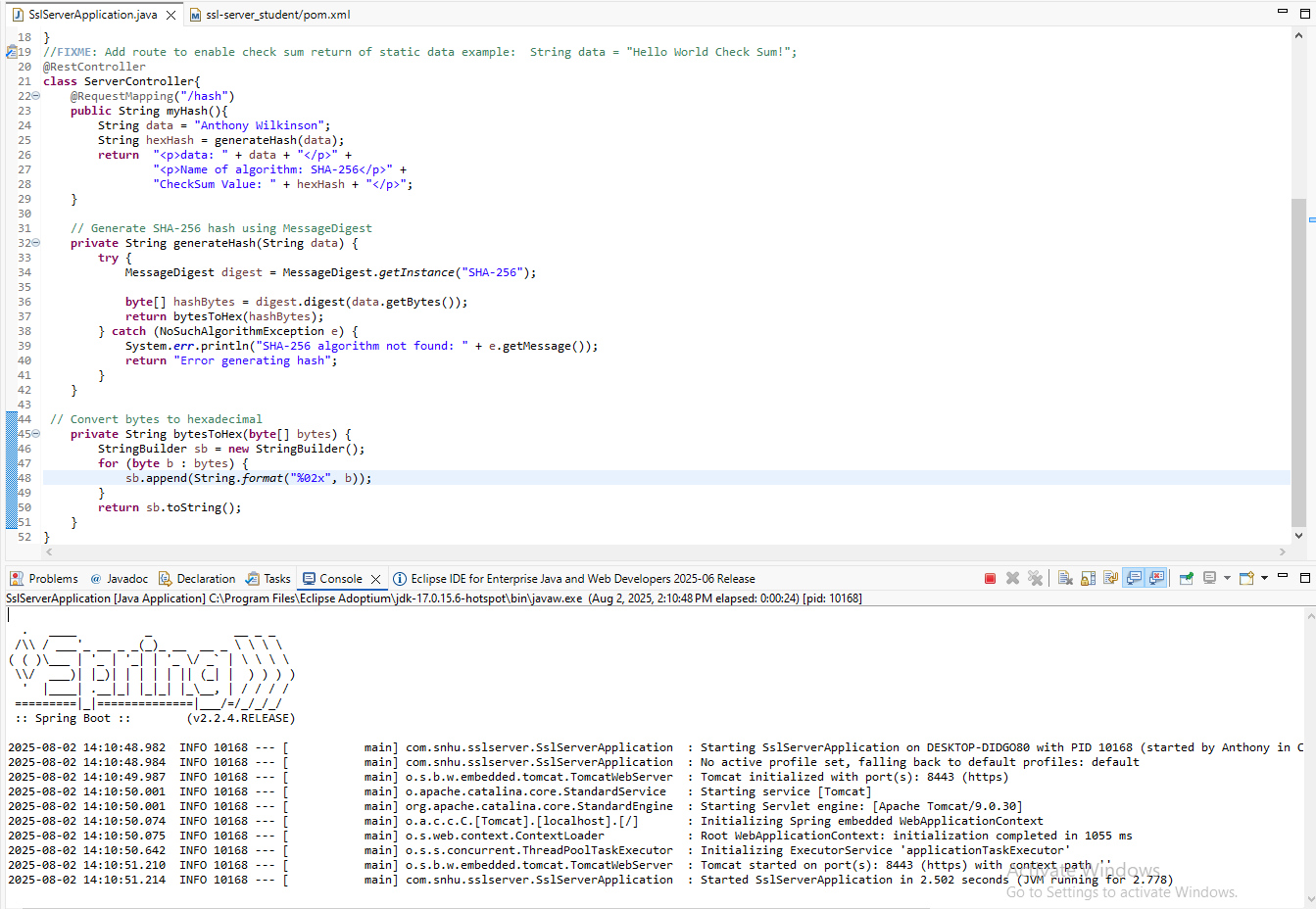


## Secondary Testing





## Functional Testing



## Summary

I refactored the application by addressing several areas in the vulnerability assessment process flow diagram:

* **Cryptography** - I implemented a SHA-256 has function to support file validaton.
* **Client/Server** - I configued the application to use HTTPS with a self-signed certificate and keystore.
* **Code Error** - I used a try-catch block to handle hashing errors.

I added these security layers in two steps: implementing security features and testing them. The testing portion of implemenation included running the program to verify correct behavior, performing a static test using the maven dependency check, and conducting a manual code review.

## Industry Standard Best Practices

Industry standard best practices are essential to a company's overall well-being. Most notably, they can save the company significant cost by preventing security breaches from occurring. These practices also support compliance with government regulations, which is necessary for Artemis Financial. While refactoring the application I applied the following industry standard best practices: Encrypting data, using strong algorithms, performing static analysis, and conducting manual code review.