****

# 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** | **2/20/25** | **Ifeoluwa Adewoyin** | **P2** |

## 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

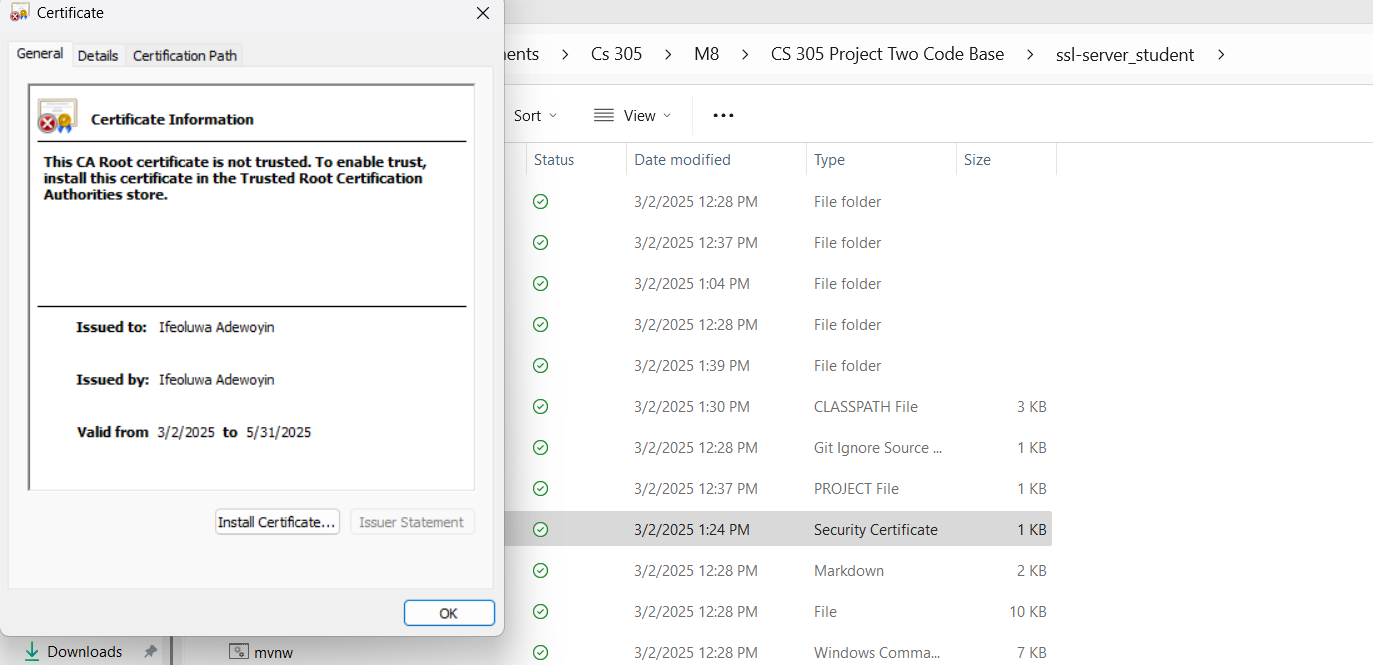
Ifeoluwa Adewoyin

## Algorithm Cipher

SHA-256 was selected as the encryption algorithm cipher for Artemis Financial's application due to its robust security features and industry-wide adoption. This cryptographic hash function belongs to the SHA-2 family developed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST). SHA-256 produces a fixed-size 256-bit (32-byte) hash value, typically rendered as a 64-character hexadecimal string, regardless of the input size. This algorithm employs a one-way function making it computationally infeasible to reverse-engineer the original input from the hash output.

The SHA-256 algorithm processes data in 512-bit blocks and utilizes a series of logical functions, including bitwise operations (AND, OR, XOR, rotations) and modular addition to transform the input data into a hash. Unlike older algorithms such as MD5 and SHA-1, SHA-256 has demonstrated strong resistance against collision attacks, where two different inputs produce the same hash value. For Artemis Financial's financial application, SHA-256 provides an excellent balance between security and performance, ensuring data integrity without excessive computational overhead. The algorithm's widespread implementation in security protocols like TLS/SSL, digital signatures, and blockchain technologies further confirms its reliability for financial applications.

## Certificate Generation



## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer program

AI-generated content may be incorrect.

A white background with black text

AI-generated content may be incorrect.

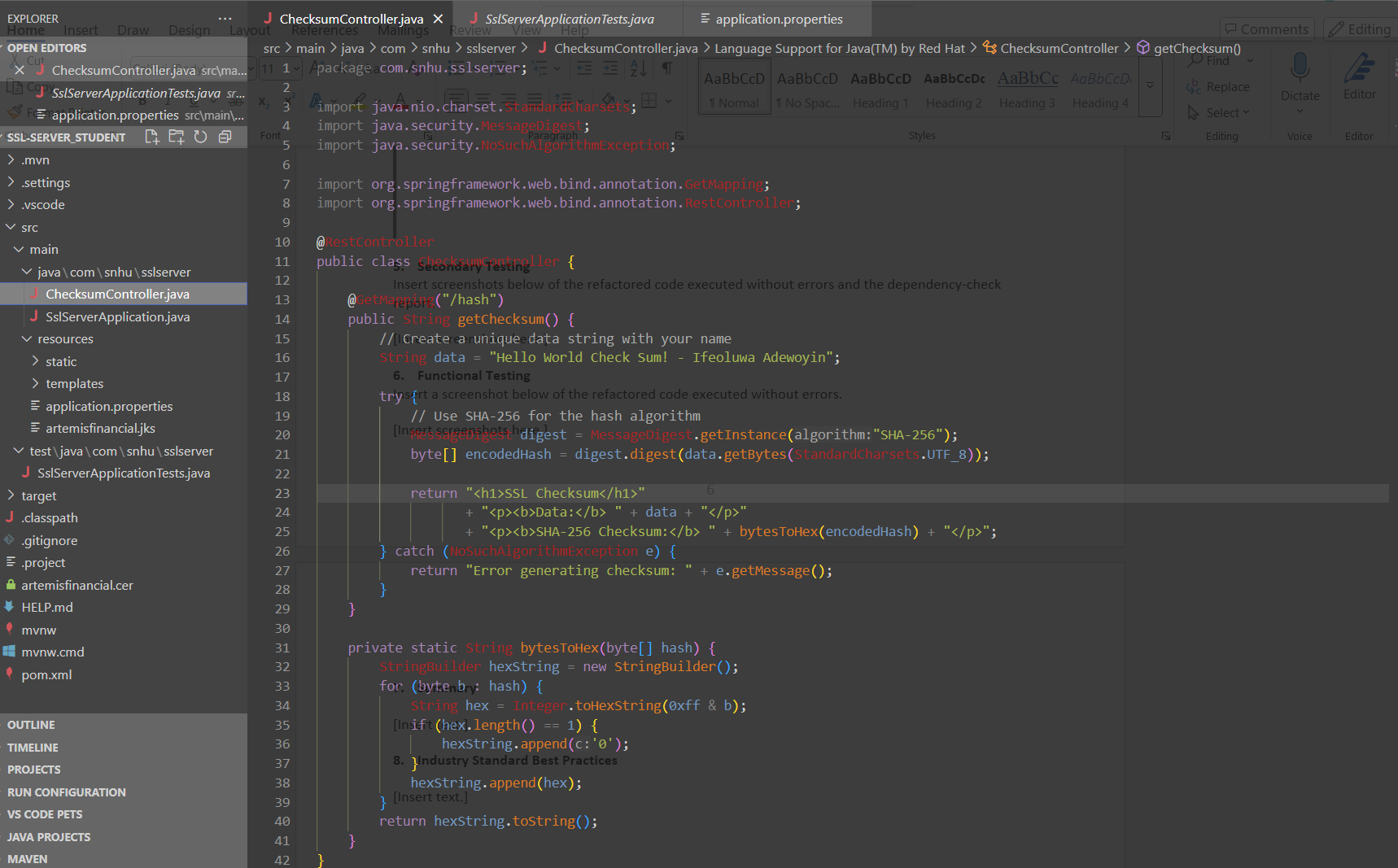
## Secure Communications

A screenshot of a computer

AI-generated content may be incorrect.

## Secondary Testing

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



A screenshot of a computer

AI-generated content may be incorrect.

## Functional Testing

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

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

## Summary

The refactored code for Artemis Financial's application now incorporates multiple layers of security that align with modern cybersecurity best practices. Following the vulnerability assessment process flow, several key areas of security were addressed: cryptography was enhanced by implementing SHA-256 for data integrity verification; client/server security was improved by enabling HTTPS communications with TLS encryption; and code quality was elevated by following secure coding practices and patterns throughout the implementation.

The process of adding security layers to the application involved a systematic approach starting with the implementation of a secure RESTful endpoint for checksum calculation. This was followed by generating a self-signed certificate and configuring the application to use HTTPS for all communications. The implementation was then tested through both automated dependency checking and manual code review to ensure that no vulnerabilities were introduced during the refactoring process. This multi-layered security approach provides Artemis Financial with a robust foundation for protecting their clients' sensitive financial data against various threats while maintaining the application's functionality and performance.

The refactored code for Artemis Financial's application now incorporates multiple layers of security that align with modern cybersecurity best practices. Following the vulnerability assessment process flow, several key areas of security were addressed: cryptography was enhanced by implementing SHA-256 for data integrity verification; client/server security was improved by enabling HTTPS communications with TLS encryption; and code quality was elevated by following secure coding practices and patterns throughout the implementation.

The process of adding security layers to the application involved a systematic approach starting with the implementation of a secure RESTful endpoint for checksum calculation. This was followed by generating a self-signed certificate and configuring the application to use HTTPS for all communications. The implementation was then tested through both automated dependency checking and manual code review to ensure that no vulnerabilities were introduced during the refactoring process. This multi-layered security approach provides Artemis Financial with a robust foundation for protecting their clients' sensitive financial data against various threats while maintaining the application's functionality and performance.

## Industry Standard Best Practices

The security enhancements implemented for Artemis Financial's application adhere to industry standard best practices for secure coding. The OWASP Top Ten security risks were considered throughout the development process, with particular attention to encryption failures, security misconfiguration, and outdated components. The implementation of HTTPS with TLS encryption follows the industry best practice of encrypting all sensitive data during transmission, preventing interception and unauthorized access to financial information.

The application's existing security was maintained and enhanced by carefully integrating new security features without disrupting existing functionality. This approach ensured that security was improved without introducing new vulnerabilities. The value of applying these industry standard practices extends beyond immediate security benefits—it also demonstrates Artemis Financial's commitment to protecting client data, which enhances their reputation and client trust. In the financial industry, where data breaches can have severe financial and reputational consequences, adherence to security best practices is not just a technical requirement but a business imperative. By implementing these security measures, Artemis Financial is better positioned to protect their clients' financial information and maintain their competitive position in the market.