****

# 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** | **08/17/2025** | **Danielle Alvis** | **Initial Report** |

## 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

Danielle Alvis

## Algorithm Cipher

For securing Artemis Financial’s web application, I recommend implementing AES (Advanced Encryption Standard) with SHA-256 for hashing. AES is a symmetric-key encryption algorithm that encrypts data in 128-bit blocks and supports key sizes of 128, 192, or 256 bits. In this project, AES-256 provides strong protection for sensitive financial data, ensuring that unauthorized users cannot access or alter the information. SHA-256 is a cryptographic hash function that generates a 256-bit digest, allowing the application to verify the integrity of data with a checksum.

AES uses symmetric keys, meaning the same key encrypts and decrypts data. It is efficient for large volumes of data, such as financial records. Secure random numbers are used to generate encryption keys, which ensures that the encryption cannot be easily predicted. While AES handles the encryption of the data, SHA-256 ensures that even minor changes to the data produce a completely different hash, providing reliable verification during transfers.

Historically, AES replaced DES in 2001 due to DES becoming vulnerable to brute-force attacks. Today, AES is the global standard for symmetric encryption and is widely adopted in financial, government, and commercial applications. SHA-256, part of the SHA-2 family, remains highly secure against collisions or pre-image attacks. Using AES combined with SHA-256 aligns with industry best practices, effectively protects client data, and supports secure communications within the web application.

## Certificate Generation

Insert a screenshot below of the CER file.

A computer screen with white text

AI-generated content may be incorrect.

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A black text on a white background

AI-generated content may be incorrect.

## Secure Communications

Insert a screenshot below of the web browser that shows a secure webpage.



## Secondary Testing

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

A screen shot of a computer

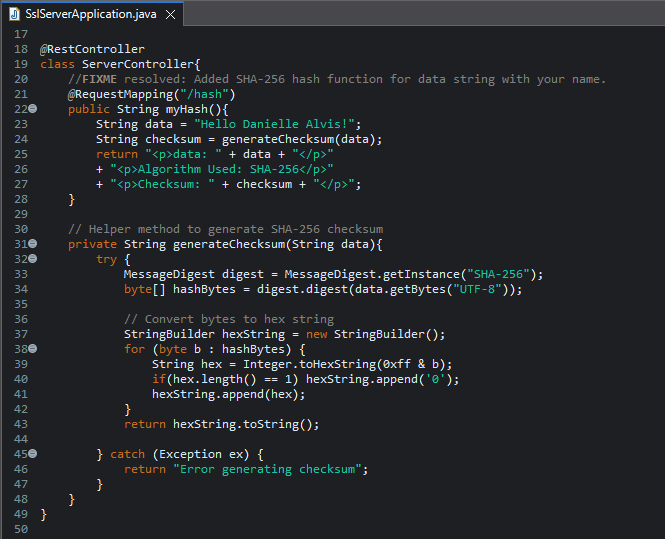
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Functional Testing

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



## Summary

The code for Artemis Financial’s application was refactored to enhance its security in alignment with software security testing protocols. During the refactoring process, I focused on areas highlighted in the Vulnerability Assessment Process Flow Diagram, including secure communications, data integrity, and encryption. Specifically, I implemented a SHA-256 cryptographic hash algorithm to generate checksums for data verification, ensuring that data transmitted via the web interface cannot be tampered with. HTTPS was enabled to encrypt communications between the client and server, preventing unauthorized access and eavesdropping.

Additional layers of security were added by generating a self-signed certificate, configuring the SSL keystore, and verifying secure connections through browser testing. The code was reviewed and tested to ensure compliance with industry-standard secure coding practices, including input validation, proper key management, and adherence to cryptographic protocols. These enhancements collectively strengthen the application’s defenses against common vulnerabilities while maintaining functionality and reliability.

## Industry Standard Best Practices

In refactoring the Artemis Financial application, industry-standard secure coding practices were applied to mitigate known vulnerabilities and maintain the integrity of the software. The use of HTTPS and SSL certificates ensures encrypted communication, protecting sensitive client financial data from interception. Implementing the SHA-256 hash algorithm for checksum verification guarantees data integrity, preventing tampering during transmission.

Key management and proper use of cryptographic algorithms follow recommended standards, and the code was reviewed to avoid common security pitfalls such as hard-coded credentials, weak encryption, and unvalidated inputs. Static analysis with the dependency-check tool helped verify that no additional vulnerabilities were introduced during development.

Applying these best practices not only maintains the application’s existing security but also strengthens the company’s overall trustworthiness and operational stability. By adhering to secure coding standards, Artemis Financial can reduce the risk of data breaches, safeguard client information, and uphold its reputation as a secure and reliable financial services provider.