****

# 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** | **2/13/25** | **Drina Baptiste** |  |

## 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

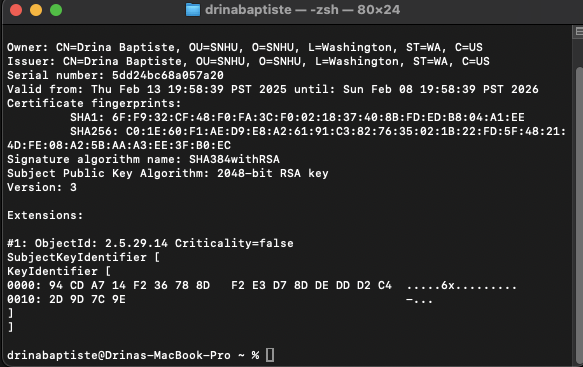
Drina Baptiste

## Algorithm Cipher

Artemis Financial should implement SHA-256 as a secure hashing algorithm to ensure data integrity and protect client information. SHA-256 is a part of the SHA-2 family, developed as an improvement over older, vulnerable hashing methods. It generates a fixed 256-bit hash value that uniquely represents any given input, making it nearly impossible to alter data without detection. Unlike encryption, which uses keys to encode and decode data, SHA-256 is a one-way function used to verify data authenticity. This ensures that any file transferred within the web application remains intact and unchanged. As cybersecurity threats evolve, businesses must adopt reliable security measures to prevent unauthorized data modifications. SHA-256 is widely used in secure communication protocols, digital signatures, and financial transactions because it resists collision attacks and ensures trust in transmitted data. Its use in Artemis Financials web application would provide a robust verification step, guaranteeing that financial data remains secure and unaltered throughout transmission. Implementing SHA-256 aligns with industry best practices and strengthens the company’s commitment to client security.

## Certificate Generation

Insert a screenshot below of the CER file.



## 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.



Shows the same information for #3.

## Secondary Testing

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

A screenshot of a computer error

AI-generated content may be incorrect.

## Functional Testing

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

A screen shot of a computer program

AI-generated content may be incorrect.

## Summary

I specifically focused on code quality. Some of the versions used in the pom.xml file above was outdated and therefore had to be updated to reduce the risk of vulnerabilities.

## Industry Standard Best Practices

To maintain the software application’s security, we applied industry-standard best practices by ensuring secure coding principles were followed throughout the development process. This included updating critical components to eliminate vulnerabilities, enforcing encryption for secure data transmission, and implementing proper error handling to prevent information leaks. These practices help mitigate security risks while maintaining the application's integrity and reliability.

Applying these best practices is essential for Artemis financials overall well-being, as it protects sensitive financial data, builds client trust, and ensures compliance with security regulations. Secure coding reduces the risk of data breaches, financial fraud, and operational disruptions, ultimately safeguarding the company’s reputation. By prioritizing security, Artemis Financial enhances the reliability of its software and strengthens its position as a trusted financial services provider.