****

# 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** | **06/25/2024** | **Courtney Warner** |  |

## 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

Courtney Warner

## Algorithm Cipher

For Artemis Financial the selected encryption cipher is SHA-256. This is a cryptographic hash function designed to ensure the integrity of data. It provides a fixed-size 256-bit hash value from input data making it the best choice for securing financial information, and everything Artemis will need to protect. Bit levels determine the length of the hash, ensuring strong security properties and collision resistance. SHA-256 was developed by the NSA and published by the NIST in 2001. It remains a cornerstone of modern cryptographic security due to its robustness against attacks.

## Certificate Generation

Insert a screenshot below of the CER file.

A screenshot of a certificate

Description automatically generated  
A computer screen with white text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated

## Secure Communications

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

A screenshot of a computer

Description automatically generated

## Secondary Testing

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

A screenshot of a computer error

Description automatically generated

## Functional Testing

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

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

## Summary

I generated and exported a self-signed certificate using keytool. The chosen algorithm cipher SHA-256 was implemented by refactoring the code to the “SslServerApplication.java” file to serve as the secure controller for the hash RESTful endpoint. Then I refactored the “application.properties” file to convert the code from HTTP to HTTPS. I then checked that the server was running type <https://localhost:8443/hash> to ensure a secure communication. Next, I conducted a dependency check to ensure that the code is compiled with the software security enhancements made. All of this concurs with the Vulnerabilities Assessment Diagram.

## Industry Standard Best Practices

To ensure secure coding, the following industry best practices were applied to the application:

* Use of SHA-256 to ensure data integrity
* Implementation of HTTPS to protect data in transit
* Generation of self-signed certificate to enable secure communications
* Conducting static code analysis and functional testing to identify and mitigate vulnerabilities

By implementing these best practices helps safeguard sensitive information, ensures compliance with regulatory requirements, and reduces costs associated with security incidents and breaches. Additionally, these practices build trust with customers and partners by demonstrating a commitment to security and data protection. This helps contribute to a positive brand image and strengthens the company's reputation in the market.