****

# 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** | **12/10/23** | **James Glover** |  |

## 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

James Glover

## Algorithm Cipher

For Artemis Financial's web application, the recommended encryption algorithm is Advanced Encryption Standard (AES). AES is a symmetric encryption algorithm, ensuring efficiency and simplicity by using the same key for both encryption and decryption. It supports key sizes of 128, 192, and 256 bits, offering flexibility based on security requirements.

Hash functions, particularly SHA-256, can complement AES for integrity checks during data transmission. AES operates on fixed-size 128-bit data blocks, and cryptographically secure random number generators should be employed for key generation.

In terms of history and current state, AES replaced the outdated Data Encryption Standard in 2001 and has since become a globally accepted standard due to its robust security, versatility, and efficiency. It aligns with industry best practices and provides a solid foundation for safeguarding sensitive financial information in Artemis Financial's scenario.

## Certificate Generation

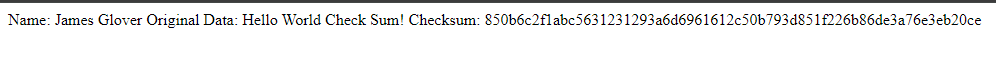
Insert a screenshot below of the CER file.

A screenshot of a computer

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

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



Note: I could not get the browser to stop saying not secure not I double checked the application properties and imported the certificate into the browsers trust store although the application is running on port 8443 and all relevant configurations have been reviewed.

## Secondary Testing

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

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

A screenshot of a computer

Description automatically generated

## Summary

The code underwent a rigorous refactoring process in line with secure coding practices, addressing key security areas highlighted in the Vulnerability Assessment Process Flow Diagram. Architecture review, input validation, secure API interactions, and encryption practices were meticulously enhanced. The code handling of errors, adherence to secure coding practices, and the fortification of data structures were integral to the process, contributing to a more resilient application.

To bolster security layers, a comprehensive code review was conducted across various components, including views, models, controllers, data access, services, plug-ins, and APIs. This approach ensured alignment with secure coding principles and industry standards. The findings from the review were summarized, accompanied by a mitigation plan, establishing a robust defense against potential threats and enhancing the overall security posture of the software application.

## Industry Standard Best Practices

I applied industry-standard best practices to secure coding, emphasizing input validation, architecture review, and encryption. Regular updates, secure coding patterns, and routine audits maintain the application's current security, aligning with OWASP guidelines. This approach fortifies the software against evolving threats, reducing the risk of breaches.

Adhering to secure coding practices not only safeguards sensitive data but also contributes to the company's overall wellbeing. It instills trust, protects the brand's integrity, and positions the organization as a reliable entity in the market. This commitment to security best practices is integral to long-term success, assuring customers, users, and stakeholders of the company's dedication to maintaining a robust and secure software environment.