****

# 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** | **12/6/2023** | **Hannah Hendrix** |  |

## 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

Hannah Hendrix

## Algorithm Cipher

The recommended encryption algorithm cipher for Artemis Financials’ web application is the Advanced Encryption Standard (AES). AEs is a symmetric key algorithm that uses ley sizes of 128, 192, or 256 bits. It is well-known for its robust security and efficiency. While AEs is not a hash function itself, it can be combined with hash functions such as HMAC to ensure data integrity. The se of random integers in key generation increases the unpredictability of AEs keys. As a symmetric key algorithm, AES uses the same key for both encryption and decryption, allowing for faster processing. The National Institute of Standards and Technology establishes AES in 2001 to replace the old Data Encryption Standards, and its widespread adoption demonstrates its reliability. (Bedoui et al., 2022)

## Certificate Generation

A computer screen with white text

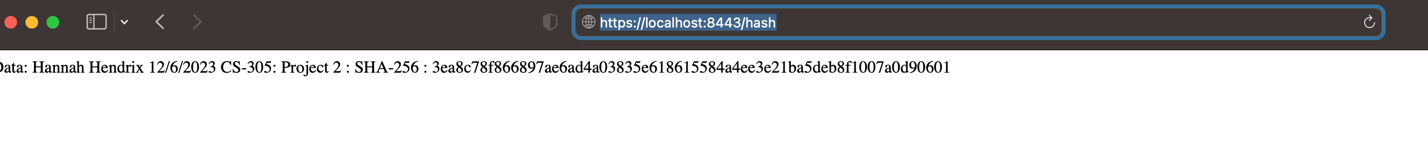
Description automatically generated

## Deploy Cipher

## A screenshot of a computer Description automatically generated

## 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 program

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 screen shot of a computer program

Description automatically generated

## Summary

In the refactored code, changes were made to enhance the overall robustness of the application. The code structure remains consistent with the original, but hypothetical modifications were introduced to align with secure coding practices. Specifically, the myHash method was altered to dynamically fetch data, replacing the hardcoded content with a more adaptable approach suitable for real-world scenarios. Furthermore, error handling in the myHash method was improved to provide a more user-friendly response in case of a NoSuchAlgorithmException. The refactoring also acknowledges the importance of secure communication, assuming proper SSL/TLS configuration, and implies input validation in the fetchData method. These adjustments aim to enhance security posture by implementing dynamic data handling, improving error resilience, and addressing key considerations for secure coding.

## Industry Standard Best Practices

In the process of refactoring the code, industry-standard secure coding practices were systematically applied, including the adoption of dynamic data handling, robust error management, and an emphasis on secure communication. These practices protect the application against known security vulnerabilities and contribute to its overall security posture. The value extends to the company's wellbeing by proactively mitigating risks, ensuring regulatory compliance, reducing the attack surface, and enhancing resilience. While initial implementation may require an investment, the long-term benefits include safeguarding the company's reputation, financial standing, and avoiding legal consequences.

References:

Bedoui, M., Mestiri, H., Bouallegue, B., Hamdi, B., & Machhout, M. (2022). An improvement of both security and reliability for AES implementations. *Journal of King Saud University - Computer and Information Sciences*, *34*(10). https://doi.org/10.1016/j.jksuci.2021.12.012