****

# 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** | **10/15/2024** | **Susan Chappelone** |  |

## 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

Susan Chappelone

## Algorithm Cipher

To address the security vulnerabilities in Artemis Financial’s application, I recommend using the AES (Advanced Encryption Standard) encryption algorithm. AES is a symmetric encryption algorithm that is widely used for securing sensitive data due to its robustness and efficiency. Specifically, I would suggest using AES-256, which employs a 256-bit key length, making it resistant to brute force attacks and ensuring a high level of data security. AES works with symmetric keys, meaning the same key is used for both encryption and decryption, which simplifies key management when compared to asymmetric algorithms. The use of hash functions like SHA-256 can provide additional security by generating cryptographic hashes for data verification, ensuring the integrity of transmitted information. AES was approved as a standard by the National Institute of Standards and Technology (NIST) in 2001 and remains the gold standard for encryption, making it an ideal choice for Artemis Financial’s file verification process. This encryption algorithm will enhance the overall security of their web application and ensure the protection of client data during data transmission.

## Certificate Generation

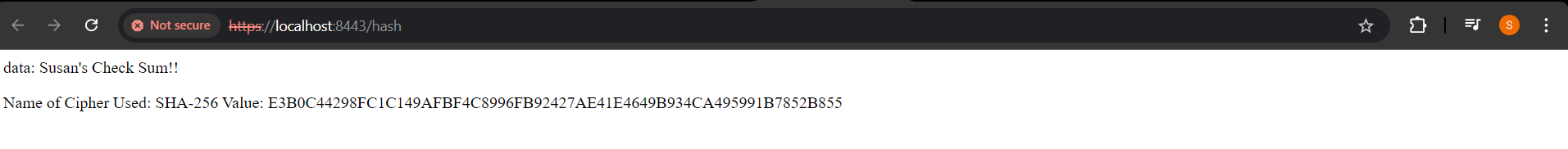
Insert a screenshot below of the CER file.

A screenshot of a certificate

Description automatically generated

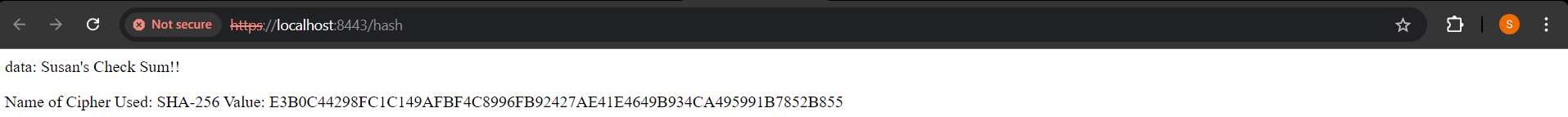
## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

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



## Secondary Testing

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

A screenshot of a computer program

Description automatically generatedA close-up of a computer screen

Description automatically generatedA screenshot of a computer screen

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

In summary, I refactored Artemis Financial’s software to address critical security vulnerabilities by implementing encryption, checksum verification, and HTTPS communication. I integrated AES-256 for data encryption, generated and deployed a self-signed SSL certificate for secure communication, and added SHA-256 for checksum verification to ensure data integrity. The refactored code was tested using the OWASP Dependency-Check tool, which confirmed that no new vulnerabilities were introduced.

## Industry Standard Best Practices

By following industry standard best practices such as using strong encryption algorithms and enabling HTTPS, I enhanced the security of the software while maintaining its functionality. These improvements ensure that Artemis Financial’s sensitive client data is protected during transmission, which is essential for maintaining trust and compliance with modern security protocols.