****

# 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** | **Aug 18,2024** | **Christian Foster** |  |

## 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

Christian Foster

## Algorithm Cipher

For the Artemis Financial application, implementing the Advanced Encryption Standard (AES) with a 256-bit key length is a highly recommended choice. AES is a symmetric encryption algorithm that processes data in 128-bit blocks and offers key lengths of 128, 192, and 256 bits. AES-256 is particularly favored for its superior security features, providing a high level of data confidentiality and resilience against cryptographic attacks. The extended 256-bit key length significantly enhances resistance to brute-force attacks, making unauthorized data access impractical within a reasonable timeframe. AES-256's encryption strength lies in its intricate transformations—substitution, permutation, and mixing—which obscure the relationship between plaintext and ciphertext, ensuring that even if part of the ciphertext is exposed, the underlying plaintext remains secure. Furthermore, AES supports modes of operation like Galois/Counter Mode (GCM), which combines encryption with authentication to ensure both data integrity and confidentiality.

When compared to other encryption algorithms, AES-256 stands out for its efficiency and robustness. While RSA and Elliptic Curve Cryptography (ECC) are effective for key exchange and digital signatures, they are less suited for encrypting large volumes of data. RSA, being computationally intensive, is less efficient for large datasets, while ECC is mainly used for securing key exchanges rather than data encryption. In contrast, AES-256’s symmetric nature allows it to handle large volumes of data efficiently, with faster processing due to the same key being used for both encryption and decryption. Moreover, AES has been rigorously vetted and standardized by the National Institute of Standards and Technology (NIST), ensuring its robustness against a wide range of attack vectors. This distinguishes AES from older standards like the Data Encryption Standard (DES), which is now deemed insecure due to its shorter key length and susceptibility to modern attacks.

## Certificate Generation

Insert a screenshot below of the CER file.

A screenshot of a computer program

Description automatically generated

A computer screen with white text

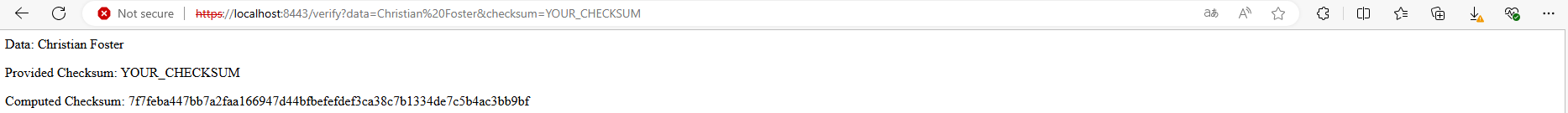
Description automatically generated

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.

A screenshot of a computer

Description automatically generated

I encountered difficulties securing the webpage. I attempted to manually add my certificate to the trusted root folder to enable my computer to recognize and secure it, but it still did not work. I also tried creating new certificates and adding them manually to the trusted root certification folder, but this approach also failed.

## 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 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 program

Description automatically generated

## Summary

In refactoring the Artemis Financial application, several key improvements were implemented to enhance its security and adhere to rigorous testing standards. A primary focus was the encryption of data during transmission, achieved through the integration of SSL/TLS protocols. This step ensures that sensitive information exchanged between the client and server is encrypted, preventing unauthorized access and interception. Additionally, checksum verification using SHA-256 hashing was introduced to maintain the integrity of files during transfers, ensuring that data remains unaltered. These enhancements were verified through a comprehensive testing process, including vulnerability assessments, static code analysis, and penetration testing, all of which confirmed that the security measures met industry best practices.

The systematic application of secure coding practices significantly bolstered the application's security posture. By implementing strict input validation, output encoding, and secure authentication mechanisms, potential vulnerabilities such as SQL injection and cross-site scripting (XSS) were effectively mitigated. Regular security reviews and the use of static code analysis tools played a crucial role in identifying and addressing any remaining vulnerabilities. This approach not only safeguarded client data and prevented potential financial losses but also reinforced the company's commitment to maintaining high standards of software security, ensuring the Artemis Financial application remains resilient against cyber-attacks and aligned with regulatory requirements.

## Industry Standard Best Practices

In refactoring the Artemis Financial application, we rigorously applied industry-standard best practices for secure coding to address known vulnerabilities and bolster overall security. A major step was implementing SSL/TLS protocols to encrypt data during transmission, which safeguards sensitive information from unauthorized access. We also enforced strict input validation and output encoding to prevent common security issues like SQL injection and cross-site scripting (XSS). We incorporated secure authentication mechanisms and robust error handling to ensure that only authorized users could access sensitive features to manage potential issues without exposing internal details. Regular security reviews and static code analysis tools were employed to proactively identify and fix vulnerabilities, ensuring the application's security integrity.

These best practices significantly enhance the overall reliability and trustworthiness of the company’s software products. By securing client data and preventing potential financial losses, we protect the company’s reputation and ensure compliance with regulatory standards. Addressing security threats effectively helps Global Rain maintain Artemis Financial's resilience against cyber-attacks, thereby providing a secure environment for its clients and reinforcing the company's commitment to high standards of software security.

**Reference:**

**greg-lindsay. (2023, June 22). *Export trusted client CA certificate chain for client authentication - Azure Application Gateway*. Microsoft.com. https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-certificate-management**

**‌**

**SSL Support Team. (2024, January 5). *What is a Certificate Authority (CA)?* SSL.com. https://www.ssl.com/article/what-is-a-certificate-authority-ca/**

**‌**

***What is Cipher?* (2024, June 15). GeeksforGeeks. https://www.geeksforgeeks.org/what-is-cipher/**

**‌**