****

# 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** | **8/16/2025** | **Joshua Dewess** | **Project Submission** |

## 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

Joshua Dewess

## Algorithm Cipher

* **Overview:** Advanced Encryption Standard (AES) was chosen due to its strong industry adoption, efficiency, and security.
* **Hash Functions & Bit Levels:** SHA-256 was implemented for checksums, offering 256-bit security strength.
* **Random Numbers & Keys:** Symmetric AES keys with secure random number generation were utilized. Asymmetric methods (RSA) were also explored for certificate management.
* **History & State:** AES, standardized in 2001, remains the most widely used cipher in secure communications, trusted by governments and financial institutions.

## Certificate Generation

Insert a screenshot below of the CER file.

A screenshot of a computer

AI-generated content may be incorrect.

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

AI-generated content may be incorrect.

## Secure Communications

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

A screenshot of a computer

AI-generated content may be incorrect.

## Secondary Testing

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

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Functional Testing

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

A screenshot of a computer

AI-generated content may be incorrect.

## Summary

* The codebase was refactored to strengthen secure communications.
* Vulnerabilities addressed:
  + Encryption of sensitive data.
  + HTTPS protocol enforcement.
  + Secure checksum validation.
* Layers of security were added following the **Vulnerability Assessment Process Flow Diagram**, addressing encryption, certificate management, and dependency validation.

## Industry Standard Best Practices

* **Maintaining Security:** Applied AES encryption, SHA-256 hashing, and HTTPS enforcement in line with OWASP recommendations.
* **Best Practices Value:** Ensures Artemis Financial protects client data, prevents interception, and strengthens trust with customers.