****

# 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** | **10/17** | **Christopher Rossi** |  |

## 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

Christopher Rossi

## Algorithm Cipher

For Artemis Financial's software, I recommend using the Advanced Encryption Standard due to its strong security, efficiency, and wide use in financial sectors. AES is a symmetric key algorithm that operates on 128-bit blocks and supports key sizes of 128, 192, and 256 bits, with the 256-bit option offering protection for sensitive data. It pairs well with hash functions like SHA-256 for data integrity checks.

AES relies on random number generation for key creation ensuring secure and unique encryption processes. Key management is essential so secure channels like HTTPS should be used for distribution and key rotation practices can further enhance security.

AES replaced the older Data Encryption Standard, which became vulnerable to brute-force attacks. AES developed in the early 2000s and is the global standard for secure data transmission. This makes it ideal for protecting client data in Artemis Financial’s web application. Its implementation, along with a checksum for data verification, will ensure both confidentiality and integrity during data transfers.

## Certificate Generation

A screenshot of a computer program

Description automatically generated

## Deploy Cipher

A close-up of a check sum

Description automatically generated

## Secure Communications

A black screen with orange and white text

Description automatically generated

## Secondary Testing

A computer screen shot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

## Functional Testing

A screenshot of a computer

Description automatically generated

## Summary

I focused on enhancing security and meeting testing standards. I implemented a cryptographic hash algorithm to verify that the data we send hasn't been altered. I also switched from HTTP to HTTPS, which helps keep the information exchanged between the client and server safe from unauthorized access. By using SHA-256 for generating checksums, I ensured that the data remains intact while the self-signed SSL certificate encrypts communication, protecting it from potential hackers. I improved input validation to prevent issues like injection attacks, making sure that only valid data gets processed.

## Industry Standard Best Practices

By following best practices for secure coding, I was able to maintain the application’s security while reducing potential risks. I used cryptographic methods and double checked my settings to ensure they were secure. Regularly testing the code for vulnerabilities also helped me catch any issues early on. This approach helps prevent data breaches Overall, applying these best practices is essential for keeping our software secure and ensuring we meet industry standards.