****

# 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** | **2/20/2024** | **Jeff Fulfer** |  |

## Client



## Developer

Jeff Fulfer

## Algorithm Cipher

The encryption algorithm I would recommend Artemis Financial to use to secure communications on their website would be the Advanced Encryption Standard (AES) cipher. This encryption standard is widely adopted across the industry and is known for its efficiency, speed, and high level of security.

AES itself is not a hashing function and rather a symmetric block cipher that utilizes a secret key to encrypt and decrypt a block of data. To complement the encryption function of AES, a hashing function such as Secure Hash Algorithm (SHA) should be used to verify the integrity of the data. Both algorithms have different bit levels that can be used when being implemented. AES has three bit levels that can be used: AES-128, AES-192, and AES-256. When implementing the hashing function SHA, there are more options available but the most popular are SHA-256 and SHA-512. When choosing the bit level for either algorithm, the larger the bit level chosen will result in a stronger implementation of the cipher.

AES relies on high-quality random number for key generation and initialization vectors (IV). Using a cryptographically secure random number generator (CSPRNG) ensures the unpredictability of keys and IVs, reducing the risk of cryptographic attacks. Since AES is a symmetric algorithm, this means that a single secret key is used for both the encryption and decryption functions of the cipher. This differs from asymmetric algorithms such as RSA or ECC where separate keys are used for encryption and decryption. Since asymmetric algorithms are slower than symmetric algorithms when being utilized for large volumes of data, they are generally used to exchange the symmetric secret key between parties when initializing a communications channel.

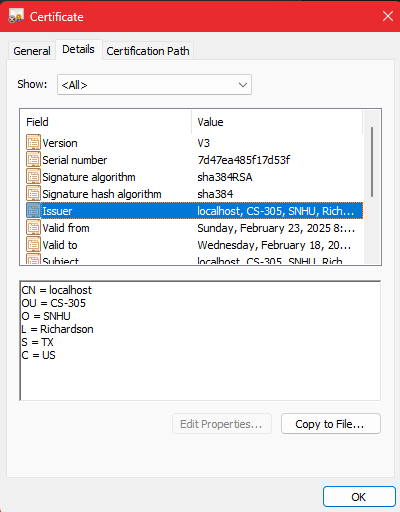
Encryption algorithms have evolved over time to protect sensitive information from unauthorized access. Early methods like DES were eventually deemed insecure due to advances in computing power, leading to the development of stronger algorithms like AES, which is now the global standard for secure data encryption. As technology continues to advance, research is focused on creating new encryption methods to withstand emerging threats like quantum computing.

## Certificate Generation

Insert a screenshot below of the CER file.

A computer screen with text

Description automatically generated



## Deploy Cipher

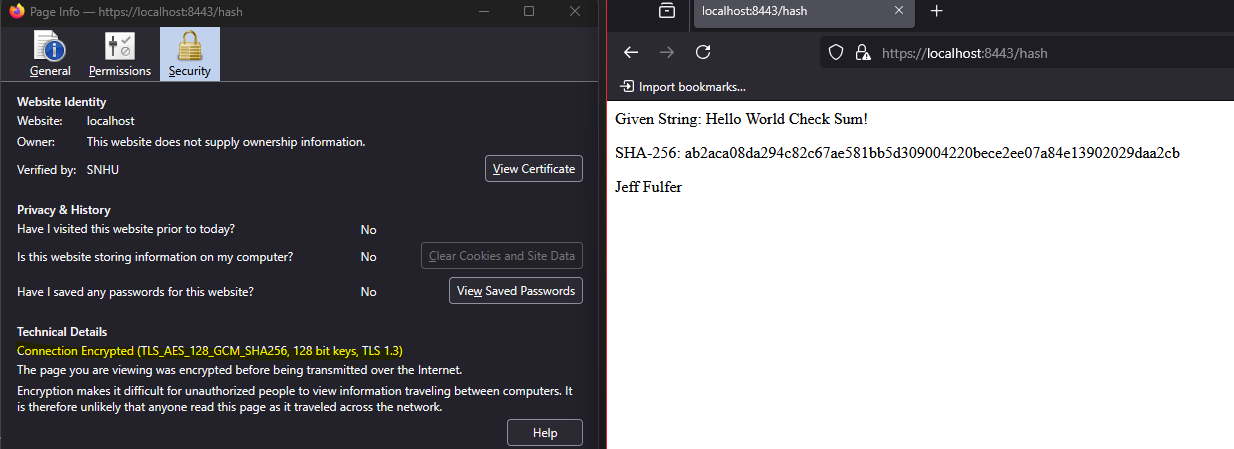
Insert a screenshot below of the checksum verification.

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 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 screen

Description automatically generated

## Summary

To enhance the security of Artemis Financial’s web application, HTTPS encryption and file integrity verification using SHA-256 were implemented. HTTPS was configured to secure data transmitted between the client and server, ensuring data integrity and confidentiality during communication. Additionally, SHA-256 hashing was used to verify the integrity of transferred files, ensuring that no unauthorized modifications occurred during transmission.

These security enhancements addressed the Cryptography and APIs components of the Vulnerability Assessment Process Flow Diagram, focusing on securing API interactions and verifying data integrity. By encrypting communications and validating file integrity, the application now provides robust protection for sensitive financial data while maintaining compliance with industry security standards.

## Industry Standard Best Practices

Artemis Financial improved its web application security by adding SHA-256 checks to verify file integrity and using HTTPS to secure data during online communication. These updates follow widely accepted security guidelines to protect information from unauthorized changes and ensure safe data transmission.

By using these trusted security methods, the company not only protects sensitive customer data but also builds trust and strengthens its reputation. This approach reduces the risk of data breaches, lowers maintenance costs, and helps the company stay ahead of potential security threats, ensuring long-term success and reliability.