****

# 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** | **04/15/2023** | **Ciera Hernandez** |  |

## 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

Ciera Hernandez

## Algorithm Cipher

The goal of Artemis Financial is to provide safe and secure financial plans for their international customers. Because the safety and security of their customers is the main goal, I would advise using the SHA-256 encryption algorithm cipher as it allows for all information to be protected from any outside access. The SHA-256 cipher is considered one of the most secure algorithm ciphers on the market and almost impossible to penetrate or crack. This is why SHA-256 is the number one cipher to be used by financial firms. The hash function and bit levels of SHA-256 are comprised randomness. Hash functions are created by taking the input value and converting it to a compressed value, the compressed value is known as the hash value. The bit levels determine the length of the encryption.

The 256-bit encryption is determined by the number of combinations within the encryption, using random numbers so that it’s harder for hackers to gain unauthorized access to sensitive information. Randomness equals unpredictability. The simplest forms of encryption is symmetric keys, which have the advantage of taking less time to execute and only needs one key. Symmetric keys are usually used in AES-256, which uses an encrypted plain text with a key. Asymmetric keys are considered to be more secure than symmetric keys because it needs two keys. This is why Asymmetric keys are typically used for internet communication.

## Certificate Generation

Insert a screenshot below of the CER file.

Text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Graphical user interface, text, application, email

Description automatically generated

## Secure Communications

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

Graphical user interface, text, application

Description automatically generated

## Secondary Testing

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

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

A computer screen capture

Description automatically generated with medium confidence

## Functional Testing

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

Text

Description automatically generated

## Summary

Using the Vulnerability Assessment Process Flow Diagram, the cryptography area was implemented with the use of the hash function for checksum verification. API was used along with a restfulAPI using the springframework. The client/server area was implemented with the certification generation and keystore use. Next, I used the hash function for data integrity verification, the customer will know if the file they were trying to access had been tampered with and will then know not to trust the data if it had been tampered with. Also, using HTTPS instead of HTTP increases the security. Finally, by updating the dependencies in use, any previous vulnerabilities should be patched and increased software security. All of this will help Artemis Financial and their clients as the less security issues they have the more secure trustworthy Artemis Financial will be.

## Industry Standard Best Practices

In order to maintain the current security of the software application, dependencies should be periodically checked for any patches and updated as needed.