****

# 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** | **4/21/2024** | **Jacob Burchett** |  |

## 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

Jacob Burchett

## Algorithm Cipher

The customer, Artemis Financial, is requesting security measures for their web services for secure communication. Due to the nature of the work done at Artemis Financial, encryption utilizing the SHA-256 cipher algorithm would be the best course of action as it would provide the highest level of security in order to protect personal financial information. This is due to the way in which a hashing algorithm works. Hashing refers to the scrambling of secure information to make it unreadable without an encryption key. SHA-256 is one of the strongest hashing means, utilizing a 256-bit key (32 characters). In addition, utilizing asymmetric encryption, meaning encryption in which the encryption key and decryption key are different, adds a much higher level of security than utilizing symmetric encryption, which uses the same key for both.

## Certificate Generation

Insert a screenshot below of the CER file.

A computer screen with white 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.

A screenshot of a computer

Description automatically generated

## Secondary Testing

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

A screen shot 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 screen shot of a computer program

Description automatically generated

## Summary

In refactoring code for this assignment, adding the RestController was step one. This ensured that secure communication via the RESTful service could be accomplished. Utilizing SHA-256 was used utilized to increase security to the best of my capabilities. When specifically looking at the vulnerability assessment flow chart, addressing cryptography and code quality was essential to ensure that the refactored code not only met the minimum requirements but was done so in a way that would instill confidence in the customer.

## Industry Standard Best Practices

With industry-standard best practices, the first time that comes to mind is structure. Utilizing comments and organization not only makes code easier to maintain in the future but also leads to improved code quality, referring back to the vulnerability assessment chart. In addition, moving into this assignment, I was aware of the general work of Artemis Financial. With that knowledge, I was able to ensure the best security possible by utilizing SHA-256, as they are a financial institution and personal security needs to be the highest priority.