****

# 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** | **10/20/2024** | **NayQuan Christopher** |  |

## Client



## Instructions

Submit these 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.

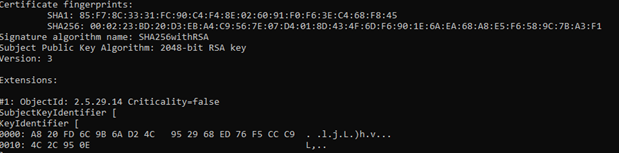
## Developer

[Insert your name here.]

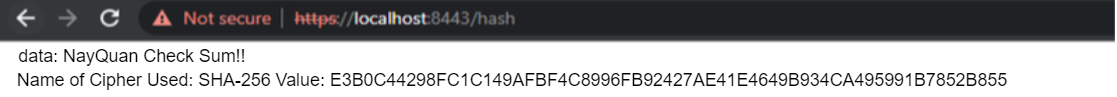
## Algorithm Cipher

## Artemis Financial is an international financial services company that offers a wide range of financial programs to its clients. To ensure the security of its clients' financial information, Artemis Financial recommends the use of the SHA-256 cipher algorithm with 256-bit keys. The SHA-256 algorithm is a member of the SHA-2 family of hash functions, which are designed to provide an important level of security. The hash values are generated by a mathematical algorithm that is designed to be resistant to collision attacks.

## Certificate Generation

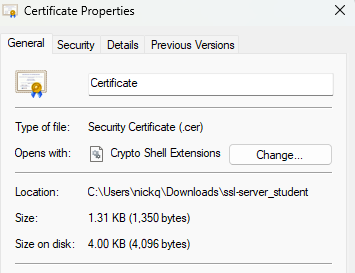


## Deploy Cipher



## 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 screenshot of a computer program

Description automatically generated



## Functional Testing

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

A screenshot of a computer code

Description automatically generatedA computer screen shot of a program

Description automatically generated

## Summary

## I just revised my code to fix a few security flaws. The most meaningful change I made was installing a security controller. I also chose SHA-256 as the hashing cipher because it is known for its prominent level of security. In addition, I recommend performing monthly dependency checks to identify any potential vulnerabilities. By taking these steps, I am confident that my code is secure.

## The best industry practices would be:

## Sensitive data must be protected both at rest and in transit to ensure the security of data and storage transfers. Standard encryption methods should be employed to encrypt sensitive data at rest, and secure communication protocols such as HTTPS should be used to protect data in transit.

## Authentication and password management must be secure, and strong password rules, hashing techniques, and multi-factor authentication should be implemented to improve user access control.

## To minimize the risk of exploitation, software updates must be applied promptly, and known vulnerabilities must be patched as soon as possible.