****

# 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** | **[Date]** | **[Your Name]** |  |

## 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

Aaron Doss

## Algorithm Cipher

Artemis Financial needs an encryption algorithm that would be used for encrypting archived files. Based on the needs of Artemis Financial, I would recommend using the SHA-256 cipher algorithm. I chose the SHA-256 algorithm as it is one of the most secure hash functions available for use. The algorithm has approximately a 0.01% chance of collisions which also suits the purposes for this assignment. The SHA-256 outputs characters of either lowercase letters or numbers 0-9. This means that there are 3664 possibilities of two different data points having the same hash value. This means that a collision would be extremely unlikely.

## Certificate Generation

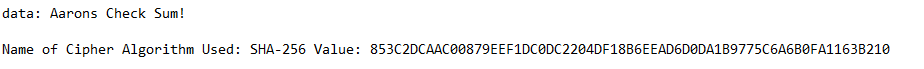
Insert a screenshot below of the CER file.

A screen shot of a computer

Description automatically generated

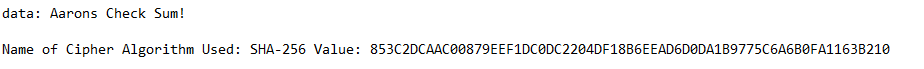
## Deploy Cipher

Insert a screenshot below of the checksum verification.



## 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 screen shot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

A screen shot of a computer program

Description automatically generated

## Summary

While refactoring my code, I added a secure Rest Controller to the program to act as a secure controller for the RESTful endpoint. I also chose to use and implement the SHA-256 cipher due to its notoriety and how well it suited the needs of the client Artemis Financial. The version of the Maven Dependency check was updated from 5.3.0 to 9.1.0 to ensure the dependency report was accurate and up to date.

## Industry Standard Best Practices

In order to meet the industry standards, I would suggest running the dependency check monthly to ensure that the API’s used remain secure. The ServerController class also addresses the secure coding aspect of the Vulnerability Assessment Diagram.