****

# 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** | **12/14/2024** | **Zachary Abbe** |  |

## 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

Zachary Abbe

## Algorithm Cipher

I would recommend that Artemis Financial to use the SHA-256 for the encryption algorithm cipher. This will help secure the transactions of their users across their servers. Using this encryption allows all the critical information to be protected by bad actors attempting to gain unauthorized access to the servers. The hash function contains random bits and don’t follow a set pattern, which ups its security. The hash value itself is made up from the name of the compressed data, and the length of the encryption is determined by the bit levels.

While symmetric keys are the simplest form of encryption to use, its based on using plain text and an encryption key. While Asymmetric or non-symmetric keys are considered to be more secure based on the way the data is encrypted, as detailed above. They both fall within the AES-256 standards though.

The history of encryption has been used as a means to give secret messages to people without others being able to distinguish the details. This can be seen with the Spartans in 600 BC using the Scytale to send encrypted messages during battle. In a larger scale, during WW2 allied and axis forces, used secret messages during radio transmissions, and would be well hidden inside a slew of sometimes nonsensical information. This led to the creation of the departments dedicated specifically to code breaking, IE NSA Code Breakers.

## 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

It shows that its converted to HTTPS but its added as a security exception when added to the browser and connecting to the server.

A computer screen with white text

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 screen

Description automatically generatedA screenshot of a computer

Description automatically generatedA 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

With my new Refactored code, I have added a secure RestController to the java file SslServerApplication and it is the controller for the hash RESTful endpoint of the program. This addresses the secure coding concern that is in the Vulnerability Assessment Diagram and fulfills all the necessary requirements of it. This uses the SHA-256 for the cipher as it’s the most secure, and the code itself is as minimal as possible so that we can lessen the chance of an attack. This runs on the most up to date version of maven, which currently is at 11.1.1, and produces a report that shows the most current up to date vulnearabilites.

## Industry Standard Best Practices

Overall I have done my best to mitigate known security vulnerabilities, while maintaining the applications current security, while also using industry-standard best practices for secure coding. Overall these are what should be used in order to make sure that the software security is properly maintained: Input Validation, Secure authentication and password management, Principle of least privilege, secure data storage and transmission, regular security updates, and error handling. This is all stuff that has been covered during the course of this class.

Using the industry best practices for secure coding protects sensitive information, complies with regulations, implements cost savings, while gaining the trust of our customers. This brings the company an overall better product to use, and distribute to their clients.