****

# 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** | **2.18.25** | **Ryan Schermerhorn** |  |

## 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

Ryan Schermerhorn

## Algorithm Cipher

Recommend an appropriate encryption algorithm cipher to deploy, given the security vulnerabilities, and justify your reasoning. Review the scenario and the supporting materials to support your recommendation. In your practices for secure software report, be certain to address the following actions:

* 1. Provide a brief, high-level overview of the encryption algorithm cipher.
  2. Discuss the hash functions and bit levels of the cipher.
  3. Explain the use of random numbers, symmetric versus non-symmetric keys, and so on.
  4. Describe the history and current state of encryption algorithms.

The main goal of Artemis Financial is to offer financial programs all over the world. I suggest going with SHA256 or SHA384 as the encryption algorithm. This way, all important information can be safely protected from hackers or being accessed by anyone who isn’t cleared to do so. The SHA-256 or SHA384 would be ideal choices since the hash function creates randomly assigned bit levels. When setting up the hash function, the input value gets compressed first, and the hash value ends up being the name of that compressed data. The length of the encryption depends on the bit levels used. Symmetric keys are the easiest type of encryption, they work by combining plain text with a key to do the encrypting, and they follow the AES-256 standards.

## Certificate Generation

Insert a screenshot below of the CER file.

A screen shot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Could not get Cipher to work.

A screenshot of a computer program

AI-generated content may be incorrect.

## Secure Communications

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

A computer screen shot of a black screen

AI-generated content may be incorrect.

Cannot run code will not run properly.

## Secondary Testing

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

A screenshot of a computer

AI-generated content may be incorrect.

## Functional Testing

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

A screenshot of a computer program

AI-generated content may be incorrect.

## Summary

Based on my code, I think I may be having some issues with the hash value and some input values. These issues may be a cause for concern security wise. The code isn’t working efficiently making it vulnerable to attacks. There is also an issue with the HTTPS, I am not getting the outcome necessary to be able to complete the secure connection or the functional testing. The web page doesn’t load with the current code. I seem to also be having issues with eclipse start up, giving me an error and making me delete a folder from the main eclipse folder. I did update the maven dependency from 8.4.0 to the current version of 12.1.0 as well. Choosing the SHA-256 was a great choice, and it seems to be that part works okay.

## Industry Standard Best Practices

To mitigate security vulnerabilities in the given in the code, I tried to apply as many industry-standard best practices that align with secure coding principles as possible. These best practices help protect the application from attacks such as injection, cross-site scripting (XSS) and data leaks while ensuring maintainability and scalability. These practices also help reduce security risks of data breaches, help with customer trust and help minimize legal risk when completed correctly. By applying secure coding best practices, the company enhances the resilience, security, and long-term sustainability of the software. Keeping up with regular patch work and updates help as well. This approach not only safeguards sensitive data but also strengthens the company’s position as a trustworthy technology provider.