****

# 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** | **12-11-2022** | **Kyle Mosely** |  |

## 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

Kyle Mosely

## Algorithm Cipher

Artemis Financial seeks additional security for their web-based application, ensuring secure communications. The best recommendation would be encryption, as the most likely attack would be a bad actor; gaining financial gain by accessing information stored. This measure would make files useless without the key. As the firm seeks secure communication, asymmetric communication is recommended. The key within the asymmetric communication would make the key to encrypt as public and key to decrypt as private. For the highest security measure, recommendations of SHA-256 algorithm with 256-bit keys to encrypt. SHA-256 would provide a high level of encryption, combined with many different combinations with the key 256 bit length. SHA-256 uses Java’s random number generation to ensure encryption is secure, creating a check-sum that is not reversible, verifying the validity of the file. The hash function is recommended to use the SHA-256 cipher as a means to create a checksum with provided message.

## Certificate Generation

Insert a screenshot below of the CER file.

Text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Graphical user interface, text, application

Description automatically generated

## Secure Communications

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

Graphical user interface, text, application

Description automatically generated

## Secondary Testing

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

Text

Description automatically generated  
Text

Description automatically generated

## Functional Testing

Insert a screenshot below of the refactored code executed without errorText

Description automatically generated

## Summary

During refactoring, I added a secured RestController to work apart of my secure controller. The ServerController works as it match the problems present in the vulnerability assessment. I chose to work with the SHA-256 cipher as it is very secure and runs low risk of collisions. To maintain the security of the application, I would recommend running dependency checks once or twice a month to ensure everything remains up to date. Keeping the plugins in the pom.xml up to date in latest iterations will assist in ensuring high security.

## Industry Standard Best Practices

a. The initial thing I did to completing industry standards is utilizing a certificate for the user details, this will be used to authenticate the user when communicating between two parties. We also hashed the data details with a secure algorithm that would make it really challenging to attempt to crack from outside parties from the transaction. I had also deployed a dependency check for any high-risk factors that would cause communication failures, and refactoring the code as needed.

b. Following industry standard security practices is crucial to the security of the company’s information as well as the protection of the customers that work with them. Some possible things that could happen should a company not secure their platform includes financial, industry, legal, ect. implications. There is also the need to protect the customer’s data, ensuring they are secure with the information stored and transmitted.