****

# 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** | **8/10/23** | **Crystal Berkhan** |  |

## 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

Crystal Berkhan

## Algorithm Cipher

Considering Artemis Financials’ needs and system, I believe the best encryption algorithm cypher for this company is Advanced Encryption Standard SHA-256. Artemis Financials needs a strong algorithm cipher to protect and secure client information and SHA-256 is impossible to crack. Secure Hash Algorithm (SHA-256) is a cryptographic hash function used to verify the integrity of text by converting the any length of text into a string of 256 bits. Hash functions produce a unique hash value from a piece of text, and it is not decryptable. SHA-256 is efficient, reliable, and extremely fast; furthermore, it is currently used in the Bitcoin network and website authentication.

Hash functions are created by taking the input value and converting it to a compressed value. The bit levels are based on the length of the encryption keys; furthermore, the longer the length, the stronger the encryption. Using random numbers to generate secret keys allows for stronger protection and reduces the predictability of secret keys. This makes it difficult for unauthorized users to access information. Currently, encryption algorithms are utilized in every device and link to protect information; however, encryption algorithms have been used since 600 BC to protect messages. Today, encryption algorithms are widely used to protect the transfer of information.

## Certificate Generation

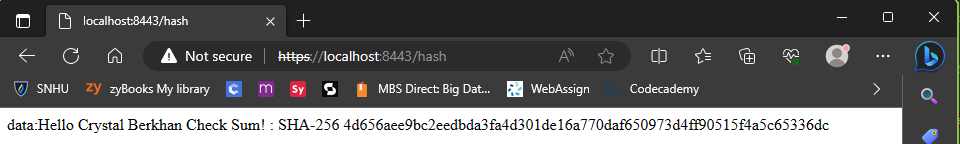
Insert a screenshot below of the CER file.

A screenshot 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.

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

A 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

Referring to the Vulnerability Assessment Process Flow Diagram, I addressed code error, code quality, and cryptography. I refactored the code to add the @RestController and @RequestMapping. This change allowed me to utilize the SHA-256 algorithm cypher and to ensure it would run properly. I verified my code did not have any errors, ran correctly, and ensured the quality of the code was efficient.

## Industry Standard Best Practices

I wrote code that is clean and readable for any adjustments that need to be made in the future for upgrades or maintenance. It is appointment to write high quality code without errors to prevent effecting the software application’s current level of security. Errors in the code could lead to unauthorized access and bugs that prevent the software from functioning the way it was intended. Enacting industry standard practices when creating software, especially for a financial company such as Artemis Financials, is crucial to protect the customers personal and private information.

Rhodes, D. (2022, April 29). *SHA-256 cryptographic hash algorithm*. Komodo Academy | En. https://komodoplatform.com/en/academy/sha-256-algorithm/