****

# 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** | **04/16/2023** | **Dan Taylor** |  |

## 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

Dan Taylor

## Algorithm Cipher

Encryption algorithm ciphers are used to "convert the original message... into ciphertext using a key to determine how it is done" (HYPR, 2022). This means that the system will receive input and convert that input into another form to prevent hackers from accessing the original information while it is stored or being transferred. A hash function is a type of encryption algorithm. A has function is said to be "the process of scrambling raw information to the extent that it cannot reproduce back to it's original form" (Simplilearn, 2022). There are many hash function forms that are available for use, and some are more secure than others. That is why a portion of these hash functions are called a secure hash algorithm. Artemis Financial has asked for additional security regarding their web-based financial system. For this application I have decided to implement a secure hash function, specifically SHA-256, as the encryption algorithm cipher. This type of hash function is more secure, stronger and will be less likely to have collisions. SHA-256 was created by the National Security Agency in 2001. It served as a successor to the hash algorithm SHA-1. What makes SHA-256 one of the top used hash functions is because it has a 0.1% chance of having a collision. It provides 256-bits and in theory should have more security because there are more combinations. The larger the hash number is, the lesser the chance the function will create a hash for two values. In other words, this is called a collision.

## 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.

Providing proof that the https is working but the certificate is not secure because it is self-signed.

Graphical user interface, text, application

Description automatically generated

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.

Graphical user interface, text

Description automatically generated with medium confidence

Graphical user interface, text

Description automatically generated

## Functional Testing

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

Graphical user interface, text, application

Description automatically generated

## Summary

Refactoring the code, I have added a secured RestController to work as the secure controller for my programs hash RESTful stop. The ServerController class works to match the problems presented by the vulnerability assessment diagram. I additionally chose to work with the SHA-256 hashing cipher as it’s very secure and runs a very small chance of collisions. To best maintain the current security of the application I would suggest once or twice monthly dependency checks of the application to keep the most up to date on potential vulnerabilities, this will help to protect the company and their sensitive data. Keeping the plugins within the pom.xml additionally would do well to keep the latest iterations of the plugins running ensuring the highest security.

## Industry Standard Best Practices

For project two I tried to focus my refactored code on the API's and cryptography. By doing this I was able to see what a Secure API interaction was by practicing with a RESTful API and a security protocol that was created utilizing a java keytool. The cryptography was handled by creating a hash function that will randomize input data inside of the code. The hash function that we incorporated in this project was helpful in maintaining the security of the information that was present in the code. By utilizing a RESTful API we are able to run the code without directly showing the areas where any sensitive information may be being held. Utilizing a hash function and SHA-256 will make it much harder if not near impossible for a hacker to gain access to any private information. It’s important to note that to maintain the security of this system that the user or customer may never share the key code that was created with anyone who does not have the clearance to access this information. The code and the key should be saved separately and update the folder location inside our application.properties file in our IDE. This is just an extra measure to ensure that in case an individual does gain access to the code, they don't have the access key to decipher such code. It would also be a good idea to have a dependency check done regularly to make sure the system is up to date with any vulnerabilities.

**References:**

Simplilearn. (2022, July 11). What Is SHA-256 Algorithm: How it Works and Applications [2022 Edition]:Simplilearn. Retrieved from https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

HYPR. (2022, August 14). Cipher |Security Encyclopedia. Retrieved from https://www.hypr.com/security-encyclopedia/cipher#:%7E:text=Ciphers%2C%20also%20called%20encryption%20algorithms,determine%20how%20it%20is%20done.