****

# 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** | **[24-02-2024** | **[Ugochuku Enyi Ebere]** |  |

## 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

[Ugochuku Enyi Ebere.]

## Algorithm Cipher

[SHA-256. SHA-256 stands for secure hash algorithm 256-bit. According to Google support, Cryptographic hash algorithms produce irreversible and unique hashes. The larger the number of possible hashes, the smaller the chance that two values will create the same hash. A collision happens when an algorithm produces the same hash value for two different pieces/bits of data. In other words, the SHA-256 algorithm ensures that collisions do not occur. As discussed last week, hash functions generate unique hash values based on the data content, meaning that when a change in the data occurs, the hash value also changes. This is a function that SHA-256 provides, which also serves as part of the reason I recommended it.

Now, let’s talk about hash functions. They provide data integrity. They obtain digital data and convert it into a hash value based on the content of the data, which means a change in data or unique data will result in a unique or different hash value. Hash functions store passwords and even things like a person’s digital signature.

Bit levels describe the size of a cryptographic key, so the bigger the number, the higher the level of security and amount of resources it would require. On to the use of random numbers, symmetric versus non-symmetric keys. Random numbers are used to generate keys for cryptography. When we generate a key, we don’t want attackers to be able to guess what the keys are. If they can, they gain access to the information we are trying to protect. So, randomly generated keys provide a layer of security from such a threat.

Symmetric keys vs asymmetric keys. Asymmetric keys use a pair of keys. One is a public key, and the other is a private key. Information can be encrypted with one but can only be decrypted with the other key, ensuring confidentiality. Symmetric keys use the same key for encryption and decryption. These are useful when encrypting large amounts of data.

Encryption goes a long way, even as far as 600 BC (Thales Group, 2023). Over the years, it has evolved from being used to send messages during wars to commercial use, and to what it is today, it has developed into something that can be applied to several forms of information, making sure to protect that information or try to, and seeing how long it has been around, primarily positives can be drawn from its use.]

## Certificate Generation

[A computer screen with white text

Description automatically generatedA screenshot of a computer

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.

[I could not figure out a way to make the local host secure, after fiddling around with it at some point it wouldn’t connect to the localhost. I wonder if this has to do with the certificate being selfsigned.]

## 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 generatedA screenshot of a computer

Description automatically generated.]

## Functional Testing

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

[A computer screen shot of a program

Description automatically generated.]

## Summary

[In the refactored code, there were several things I did. Step one was installing/integrating the maven dependency check plug-in. Updating the check version to 9.0.9 so that the dependency check contains updated information regarding the vulnerabilities published. I also make use of SHA-256 as the hashing cipher. In order to ensure that vulnerabilities are taken care of, or reported, keeping the dependency check plugin updated is the way to go. Added a RestController to act as the controller for the RESTful endpoint. Suppressing the vulnerabilities and adding them to a created suppression file would help drop/suppress the number of vulnerabilities to a minimum. I did/attempted to suppress as many as I could by obtaining the suppression codes from several vulnerabilities.]

## Industry Standard Best Practices

[For this project, there was documentation provided. In order to adhere to industry standard practices, I followed the advice and steps provided, to ensure that the company gets exactly what they asked for. I also made sure that my code was readable and easy to follow along to with comments on the code. Industry best practices ensure that the code is not prone to errors or vulnerabilities from the jump, as that is the first line of defense. Also, with their application, others who will come along to work on or collaborate using the application can understand where they are and how to proceed.]