****

# 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** | **04/16/2024** | **Harley Reimels** |  |

## 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

Harley Reimels

## Algorithm Cipher

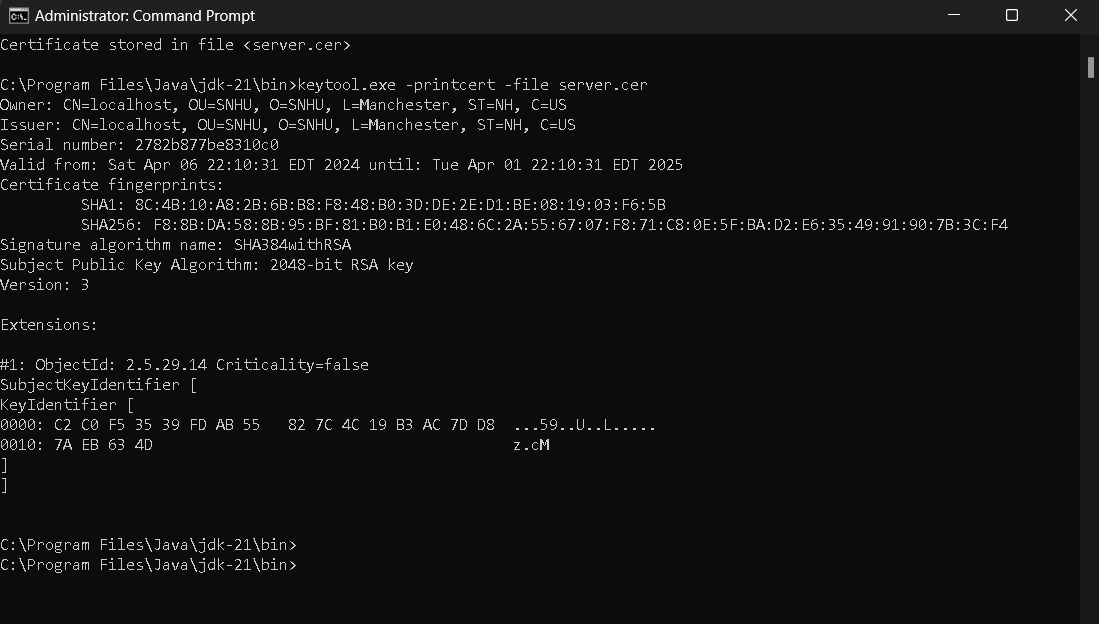
The cipher I will be using is SHA-256. SHA-256 is the most used hash function presently, the 256 refers to the length it produces in bits. By taking in data and performing mathematical equations on that data, we get a secure hashed result. The use of random numbers is one of the core foundations of cryptography. By implementing random numbers, you can change a password by shifting it left, or right that many letters. This alone is not very secure and can be easily cracked with a brute force attack. For a cipher to work, a key must be generated to encrypt the message, and decrypt the message. Symmetric keys use the same key for encryption and decryption, while Asymmetric keys have one key for encrypting, and one for decrypting. Each type has different advantages, Symmetric is usually more efficient, while Asymmetric is good for general use. Ciphers have been around for a very long time, one of the more famous ciphers is known as the Ceaser cipher. This cipher just shifts letters by N amount, meaning there are 25 possible different ways to code a single message. As technology advanced, so have our needs for more secure ciphers.

## Certificate Generation

Insert a screenshot below of the CER file.

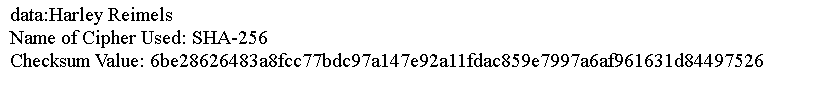
A screenshot of a computer program

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

You can see that it is not https, but it is not official but self signed, and that is why we get the strikethrough.

A screenshot of a computer

Description automatically generated

Also further proving we are using HTTPS, we see that it is launched this way from java using springboot.



## 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

Refer to the Vulnerability Assessment Process Flow Diagram. Highlight the areas of security that you addressed by refactoring the code.

Discuss your process for adding layers of security to the software application.

I added a cipher that encodes data, this process makes it almost impossible to fool the computer into thinking it is accessing a website in which is not the website itself, protecting the user. I had also added a certificate that enables https which means we know that we have reached the website we wanted.

## Industry Standard Best Practices

Best practices involve keeping the pom up to date, its dependencies and plugins. Also running a dependency check at least once a month, as new vulnerabilities are being discovered every day. The main reason security being so important is to keep people’s faith in the company. Money can be lost, money can be gotten back, but once you lose the faith of client, that is something that is almost impossible to get back.