****

# 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** | **Wesston Reed Mccollum** |  |

## 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

Wesston Reed Mccollum

## Algorithm Cipher

The algorithm cipher used in this project is the SHA256 cipher. This cipher uses 256-bit keys, meaning collisions are highly unlikely as it would be a chance of 1 in 2^256. This is important, as the more bits in a key, the more possible iterations an attacker will have to try to iterate through to attempt to break it. This cipher is symmetric however, which means that its key is used to both encrypt and decrypt data, but with the use of certificates it is safely transported from server to client.

## Certificate Generation

Insert a screenshot below of the CER file.

Graphical user interface, text, application, email

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Graphical user interface, text

Description automatically generated

## Secure Communications

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

Graphical user interface

Description automatically generated

## Secondary Testing

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

Graphical user interface, text, application

Description automatically generated

A screenshot of a computer

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

The code now includes a cryptographic transfer of information, using the SHA256 cipher to encrypt and decrypt information. This information is sent through a secure client/server connection. It was important to ensure that all code was working properly with the best practices used for securing the connections.

## Industry Standard Best Practices

The code that was refactored ensured that the information was being encrypted with a high complexity algorithm, with its key being secured with certificates. These ensure a safe passage of information without fear of interception or eavesdropping. This is important for companies to ensure client and company safety, as well as prevent financial loss.