****

# 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** | **4/10/2023** | **Jeffrey Carlson** |  |

## 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

Jeffrey Carlson

## Algorithm Cipher

SHA-256 is a cryptographic hash function that generates a 256-bit hash value from an input message. The algorithm uses several mathematical operations to create a highly randomized output. It uses random numbers to add complexity to the message and prevent attacks. It is a symmetric-key algorithm, meaning the same key is used for encryption and decryption. Encryption algorithms have a long history and are used to secure sensitive data like passwords and financial transactions. However, there is controversy over restricting their use for national security or law enforcement purposes.

## Certificate Generation

Insert a screenshot below of the CER file.

[Insert screenshots here.] Text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Graphical user interface, text, application, website

Description automatically generated

## Secure Communications

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

[Insert screenshots here.] Graphical user interface, text, application, website

Description automatically generated

## Secondary Testing

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

[Insert screenshots here.] Text

Description automatically generatedTable

Description automatically generated with medium confidence

## Functional Testing

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

[Insert screenshots here.]

## Summary

When adding security layers to a software application, potential risks and threats are identified and a security plan is developed. The security measures include validating user input, implementing secure login, using encryption, and error handling. After implementing the security measures, the application is thoroughly tested to ensure they work as intended. The application is monitored regularly for new security issues using vulnerability assessments and penetration testing.

## Industry Standard Best Practices

[Insert text.]

Industry standard best practices for secure coding are important to maintain the security of a software application. These practices involve updating the software, using strong passwords, encrypting sensitive data, validating user input, and monitoring security events. Following these practices can help a company avoid security incidents, comply with regulations, gain customer trust, and focus on business goals.