****

# 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** | **6-20-2023** | **Stormey Trayter** |  |

## 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

Stormey Trayter

## Algorithm Cipher

The cipher chosen for this case study is SHA-256. SHA-256 is known for its substantial output size and a high level of cryptographic security. Nevertheless, it should be noted that despite its 256-bit hash value, there remains a possibility of collisions. (Thakkar, 2022) Nonetheless, the likelihood of encountering two distinct inputs that yield the same hash value is exceedingly low. (Thakkar, 2022) Both SHA-2 and SHA-3 are families of cryptographic hash functions that offer 256-bit hashes. SHA-3 was specifically developed as a response to identified security vulnerabilities in SHA-2. (Grimes, 2018) Therefore, based on the findings, it is recommended to utilize SHA-3 for enhanced security.

## Certificate Generation

Insert a screenshot below of the CER file.

## 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.

[Insert screenshots here.]

## Secondary Testing

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

[Insert screenshots here.]

## Functional Testing

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

[Insert screenshots here.]

## Summary

[Insert text.]

## Industry Standard Best Practices

[Insert text.]

Citations

Jena, B. K. (2023). What Is AES Encryption and How Does It Work? Simplilearn.com.

https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

Computer Security Division, Information Technology Laboratory, National Institute of Standards

and Technology, U.S. Department of Commerce. (n.d.). AES Development –

Cryptographic Standards and Guidelines | CSRC | CSRC. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development