****

# 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** | **12/6/2022** | **Joseph Castrigno** |  |

## 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

Joseph Castrigno

## Algorithm Cipher

SHA-256 is one of the algorithms supported by MessageDigest. SHA-256 can theoretically be compromised, but a brute force attack is computationally infeasible (Ellis, 2018).

SHA-256 uses 256 bits. Exact details about SHA-256 aren’t public knowledge, but it is known that it is built with a Merkle-Damgard structure derived from a one-way compression function. That function is created with the Davies-Meyer structure from a specialized block cipher.

Symmetric cryptography is typically used for encryption rather than signing. A key is used to scramble information. That same key is used to both encrypt and decrypt the information. This makes the secrecy of the key vital to the security of the communication. Asymmetric cryptography is usually used for signing. Instead of using one key, there are two – one private key kept by the sender and one public key made publicly available. The private key signs the data and the public key validates the signature. The public key can’t be used to derive the private key.

## Certificate Generation

Insert a screenshot below of the CER file.

Text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Graphical user interface, text, application, email, website

Description automatically generated

## Secure Communications

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

Graphical user interface, text, application, email, website

Description automatically generated

## Secondary Testing

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

Text

Description automatically generated

Text

Description automatically generated

## Functional Testing

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

Graphical user interface, text, application, Teams

Description automatically generated

## Summary

In the Vulnerability Assessment Process Flow Diagram, we’ve addressed an important area of security: cryptography. We’ve implemented a secure hashing algorithm to ensure the data we send and receive is safe from prying eyes. We’ve done so while ensuring that no additional dependency vulnerabilities were added to the application.

## Industry Standard Best Practices

Applying industry best practices adds value because it prevents problems before they occur. If company data was compromised, it could take large amounts of resources to remedy the situation. It also helps avoid costly lawsuits and stay in compliance with government regulations. A company’s public image can be affected by the security of its data. Poor public perception could lead to loss of sales and scare potential customers.

Ellis, S. (2018, December 13). *The beautiful hash algorithm*. Medium. Retrieved November 28, 2022, from https://steviecellis.medium.com/the-beautiful-hash-algorithm-f18d9d2b84fb#:~:text=Since%20executing%20a%20brute%2Dforce,resistant%2C%20for%20now%20at%20least.

N-able. (2021, April 1). *SHA-256 algorithm - N-able*. N-able. Retrieved December 6, 2022, from https://www.n-able.com/blog/sha-256-encryption#:~:text=SHA%2D256%20is%20a%20patented,as%20long%20as%20when%20unencrypted.