****

# 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** | **12/11/2022** | **Benjamin White** |  |

## 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

Benjamin White

## Algorithm Cipher

The algorithm cipher chosen for this system is SHA-256. Because this cipher utilizes a 256-bit key, there is an extremely low likelihood of collisions. While this encryption is slower to generate comparted to 128-bit ciphers, the security of a 256-bit cipher is unparalleled. To this day, SHA-256 has not been compromised as opposed to MD5 hashing algorithms. Even the smallest changes to the source file result in an entirely different hash value (TV, 2021). Additionally, SHA-256 is the modern standard hashing algorithm for many government agencies and financial institutions.

The two types of encryption keys are symmetric and asymmetric. While symmetric encryption utilizes a single key that must remain protected at all times, asymmetric encryption utilizes both a public and a private key. In asymmetric encryption, a public key is used to encrypt data and the private key is used to decrypt the data. Keys are created utilizing a random number generator to prevent keys from having any likeness to each other.

In 1976, IBM developed the Data Encryption Standard. At the time, DES was considered the most secure cipher. DES proved to be the first modern symmetric cipher algorithm (Shea, 2020). Today, DES has become relatively unused, as much more secure asymmetric cipher algorithms have begun being used.

## 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

Description automatically generated

## Secure Communications

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

Graphical user interface, text, application, email

Description automatically generated

(same screenshot from #3. This demonstrates a secure https connection. The browser is flagging this site because Chrome does not like self-signed certificates.)

## Secondary Testing

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

Graphical user interface, text, website

Description automatically generatedText

Description automatically generated

Graphical user interface, text, application

Description automatically generated with medium confidence

## Functional Testing

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

Graphical user interface, text

Description automatically generated

As you can see from above console output, the refactored code executes without errors.

## Summary

The development of this system involved addressing multiple areas of security. Primarily, server/client and cryptography were addressed. By implementing a SSL certificate, we allow Artemis Financial customers the peace of mind that the site they are accessing is authentic. Additionally, this ensures the connection between the client and server are secure. Cryptography was addressed by implementing the SHA-256 cipher algorithm. The implementation of this cipher allows for data to be encrypted before it is sent to the server and stored. Again, because SHA-256 has yet to be cracked, this ensures sensitive data that is sent to the Artemis Financial web app is secure. Also, implementing the HTTPS connectivity ensures browser sessions are protected.

## Industry Standard Best Practices

By utilizing Java’s MessageDigest class, we ensure that our codebase can be quickly and easily updated should SHA-256 become obsolete in the future. Implementing this change is as easy as specifying a different cipher algorithm on line 27 (String cipher = “SHA-256”). By creating modular and abstracted code, we make our system easy to future-proof. Additionally, running dependency checks to evaluate potential vulnerabilities allows us to ensure our dependency versions are safe. Following these principles allows Artemis Financial to maintain trust from their customers. Part of this means frequently running dependency checks to ensure that no additional vulnerabilities have surfaced.

**References**

Chris Veness, www.movable-type.co.uk. (n.d.). *Movable type scripts*. SHA-256 Cryptographic Hash Algorithm implemented in JavaScript | Movable Type Scripts. Retrieved December 11, 2022, from <https://www.movable-type.co.uk/scripts/sha256.html>

Rezky TV. (2021, April 1). *Benefits of SHA-256*. Medium. Retrieved December 11, 2022, from <https://rizkigbastian47.medium.com/benefits-of-sha-256-dd9d7e60ea17>

Shea, Sharon. “Cryptography Basics: Symmetric Key Encryption Algorithms.” *SearchSecurity*, TechTarget, 28 Jan. 2020, https://www.techtarget.com/searchsecurity/feature/Cryptography-basics-Symmetric-key-encryption-algorithms.