****

# 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** | **20 Apr 2024** | **Daniel Collins** | **Final security practices report** |

## 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

Daniel Collins

## Algorithm Cipher

The recommended cipher algorithm that best fits Artemis Financials needs is the Secure Hash Algorithm 256 (SHA). The SHA-256 is a widely used cipher that uses 256 bits for encryption; the more bits you have, the harder it is to break, but requires more processing power so some consideration is necessary when deciding which bit size to use. It produces a fixed 256-bits to hash blocks of text, instead of one bit at a time; using these ensures efficiency and security. Random numbers are used to create these keys and these numbers are unpredictable which increases security. When choosing the most secure cipher, some things must be considered such as performance, the more bits a cipher has, the longer it takes to encrypt and decrypt data. System compatibility is another as not all systems support all ciphers.

Cryptography has been used for over 3000 years; in ancient Egypt and Rome, simple substitution methods were used. More complex substitution methods were used by Queen Elizabeth I’s spymaster, Sir Francis Walsingham, who used them to uncover plots against the monarch. In modern times, more data to protect meant that more sophisticated and efficient methods were necessary. The Data Encryption Standard 56-bit was created in 1975 and was widely used until computational power increased and a more secure method was needed. In 2001, the SHA-256 was released, and since it uses more bits, it more far more secure and has been the most commonly used cipher algorithm, and the one I recommend for Artemis Financial.

## Certificate Generation

Insert a screenshot below of the CER file.

A screenshot of a computer program

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated

## Secure Communications

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

A screenshot of a computer

Description automatically generated

## Secondary Testing

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

A screen shot of a computer program

Description automatically generated

A computer screen with text

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

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

A screen shot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

## Summary

The areas of security that were addressed by refactoring the code were input validation, cryptography, and code quality.

The following changes have been made to the code to enhance the security and stability of the program:

1. Upgraded from Java 1.8 to 21, ensuring compatibility with current security features.
2. Upgraded Spring Boot 2.2.4 to 3.2.5 for Java compatibility and security.
3. Upgraded Maven dependency check from version 5.3.0 to 9.1.0.
4. Upgraded Jackson BOM to version 2.17.0 eliminating the last vulnerable dependency.
5. Implemented @NotBlank for input validation.
6. Used SHA-256 cryptographic hash algorithm to ensure checksum security.
7. Used OWASP Dependency Check to identify vulnerabilities.
8. Implemented NoSuchAlgorithmException to catch errors.

By upgrading Java and other frameworks, I ensured that the program’s foundations had the most current security features. I used HTTPS to secure data transmissions by generating a SSL certificate and configuring it with Spring Boot to provide a secure server port (8443). Lastly, scanning for vulnerabilities with Maven Dependency Check then refactoring the code to eliminate vulnerable dependencies adds another layer of security to this program.

## Industry Standard Best Practices

Industry standard best practices were followed by developing secure code; upgrading frameworks and Java, using input validation, and error handling helped to ensure this. Dependency scanning was used to identify and repair vulnerable dependencies. Communication was secured by using a SSL certificate, enabling the use of HTTPS to encrypt all data transmissions, and with a SHA-256, we are able to verify the integrity of the data.

Using these practices helps ensure the trust of Artemis Financials’ customers by creating a secure, reliable product. A single data breach may be enough to damage a company’s hard earned trust, and this product was designed to be secure, now and in the future.