****

# 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** | **10/15/2023** | **Brandon Marrero** |  |

## 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

Brandon Marrero

## Algorithm Cipher

Artemis Financials’ primary goal is to provide financial programs on a global scale. I highly recommend adopting the SHA-256 encryption algorithm for securing sensitive information. This encryption method serves as a robust shield against unauthorized access from external sources. SHA-256 employs randomly generated bit levels in its hash function. Before using this function, it compresses the input data, and the resulting hash value serves as the identifier for the compressed information. The encryption's length is determined by the number of bits utilized.

Symmetric keys represent the most straightforward encryption approach, relying on plain text and a key for the encryption process. These keys adhere to the AES-256 standard. On the other hand, asymmetric keys are considered more secure as they involve pairs of keys and find prominent use in internet connections.

The history of encryption can be traced back as far as 600 BC when the Spartans employed the scytale to transmit covert messages during battle. Over time, encryption has continued to evolve. Notably, it played a crucial role during World War II and was later adopted by IBM in the 1970s to protect their customers.

## 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 black and white text

Description automatically generated with medium confidence

## 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 screenshot of a computer

Description automatically generated

## Functional Testing

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

A close-up of text

Description automatically generated

A screenshot of a computer

Description automatically generated

## Summary

In the process of code improvement, I introduced a robust RestController within the SSLServerApplication.java file. This RestController serves as the secure handler for the hash RESTful endpoint. The creation of this ServerController class effectively addresses the security concerns outlined in the Vulnerability Assessment Diagram and meets all the necessary requirements. For enhanced security, I opted to employ SHA-256 as the chosen hashing algorithm for this function, and I ensured that the code is kept minimal to minimize potential attack vectors. Additionally, I updated the Maven Dependency check version from 5.3.0 to 8.2.1, ensuring that the static dependency check aligns with the latest available software version.

## Industry Standard Best Practices

To address well-documented security vulnerabilities and uphold the current security of the software application, I adhered to established industry-standard secure coding practices. In addition to the modifications detailed in the Summary section, it is imperative to institute proper security measures. The following practices should be employed to effectively maintain the software's security:

1. Input validation: Validating and sanitizing user inputs to prevent potential threats such as SQL injection, cross-site scripting (XSS), and command injection.
2. Secure authentication and password management: Enforcing stringent password policies, employing robust hashing algorithms, and incorporating multi-factor authentication (MFA) to bolster user access control.
3. Principle of least privilege: Ensuring that both users and applications possess only the minimal necessary permissions required to execute their tasks, thus diminishing the potential for unauthorized access or actions.
4. Secure data storage and transmission: Encrypting sensitive data when it is at rest using widely recognized encryption algorithms and using secure communication protocols like HTTPS.
5. Regular security updates and patching: Keeping the software application and its dependencies up to date, promptly applying security patches, and addressing any documented vulnerabilities to reduce the risk of exploitation.
6. Error handling and logging: Implementing robust error-handling mechanisms to prevent the inadvertent exposure of sensitive information and maintaining secure logging practices to identify potential security threats.

Implementing industry-standard best practices for secure coding delivers substantial value to a company. It safeguards sensitive data, ensures compliance with regulations, reduces costs, and fosters trust among customers and partners, ultimately contributing to a positive brand image and enhancing the company's reputation.