****

# 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** | **[04/20/2025]** | **[Jian Wang]** |  |

## 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

Jian Wang

## Algorithm Cipher

The most suitable encryption algorithm for Artemis Financial's needs is AES-256.

First, AES-256 has a 256-bit key length. The 256-bit key length ensures that even if the attacker has sufficient computing power, he cannot crack the encrypted file. It can effectively defend against brute force attacks. Secondly, this is a symmetric encryption method with small computational complexity and fast encryption speed. It will have better encryption efficiency. At the same time, AES is already a very mature encryption algorithm that can effectively defend against man-in-the-middle attacks (MITM).

About risks, all symmetric encryption algorithms have a major disadvantage, that is, the sender and the receiver use the same key. Once the key is lost, the encryption becomes invalid. Although asymmetric encryption algorithms such as RSA can solve this problem, but asymmetric encryption algorithms are complex and slow, and are only suitable for a small number of particularly important transactions. Considering that Artemis Financial has a wide range of business and a large transaction needs, it is not suitable to use asymmetric encryption algorithms.

Regarding government regulations, Artemis Financial has international business, so it is necessary to consider the government regulations of major global markets. In the United States, AES fully complies with FIPS encryption requirements and is a recommended product. In the European Union, AES also fully complies with GDPR requirements. As you can see, AES is already a widely accepted method.

About the best cryptographic algorithm, RSA is the best in terms of security, but it is slow. In terms of overall performance, AES is the best choice. However, due to its complexity, AES-256 has relatively high hardware requirements. Therefore, Artemis Financial can consider using different levels of AES according to the security level of its data. For example, the highest-level files use AES-256, and low-level files use AES-192 or even lower.

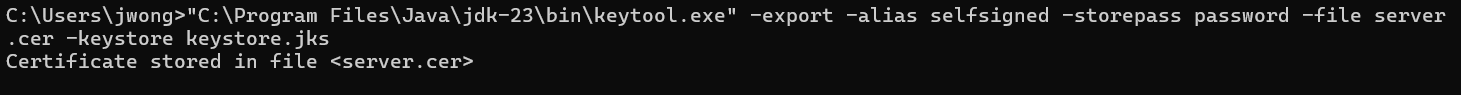
Regarding hash functions and random numbers, hash functions usually enhance encryption algorithms, but they cannot encrypt by themselves. The main function of random numbers is to ensure the randomness of the key and prevent the key from being predicted. Random numbers also play an auxiliary role in encryption algorithms. Random numbers and hash functions jointly assist encryption algorithms, making simple keys more complex and unpredictable.

Encryption algorithms are closely related to the development of human technology. From the alphabet move position method to the famous Enigma machine during World War II to the encryption algorithms in today's computer age, they all rely on the progress of technology. Today's advanced AES-256 will soon be eliminated with the development of quantum computers in the future. Therefore, there is no forever secure password or algorithm. Keeping information updated in a timely manner is the best encryption method.

## Certificate Generation

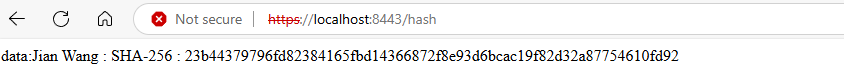
Insert a screenshot below of the CER file.

A computer screen shot of a black screen

AI-generated content may be incorrect.

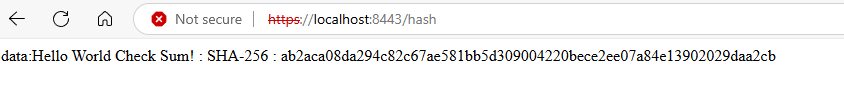
## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

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



## Secondary Testing

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

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

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 screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Summary

First, use OWASP Dependency-Check to scan and identify potential vulnerabilities. Second, perform risk assessment, analyze vulnerability applicability, determine that some CVEs are not applicable, and mark them as false positives. Then, take mitigation measures, create suppression.xml, and suppress false positives through suppression.xml optimization to ensure that the report focuses on real risks. Refactor the code to enhance input validation and exception handling to prevent potential injection attacks. Finally, perform verification and rerun OWASP Dependency-Check to confirm that the suppressed vulnerabilities in the report are marked as "Suppressed" and no new vulnerabilities are introduced.

To enhance application security, the following security layers are implemented:

1. HTTPS encryption: Configure Spring Boot to use a self-signed certificate (keystore.p12)

2. Secure hash algorithm: Use the SHA-256 algorithm to calculate data hashes to ensure data integrity.

These measures build multi-layer security protection through encrypted transmission, data integrity verification, and vulnerability management.

## Industry Standard Best Practices

Application of industry standard best practices OWASP Dependency Check: Run Dependency-Check regularly, manage false positives in combination with suppression.xml, ensure vulnerability database updates, optimize vulnerability management, and improve work efficiency. Secure Coding: Follow the principle of least privilege to minimize risks Encrypted transmission: HTTPS and SHA-256 hashing provide secure data transmission to ensure company data security.