****

# 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** | **20241222** | **Benjamin A. Lambert** |  |

## 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

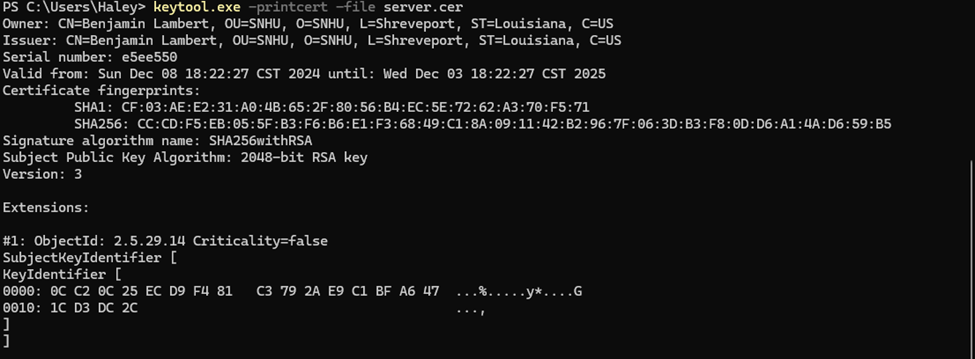
Benjamin A. Lambert

## Algorithm Cipher

For Artemis Financial, I recommend utilizing the Advanced Encryption Standard (AES) as the encryption algorithm of choice. Known for its combination of security and efficiency, AES is particularly well-suited for long-term data protection. Its 256-bit key length provides a high level of resistance against decryption efforts, thanks to the complex computations involved. Additionally, as a symmetric encryption method, AES typically outperforms asymmetric algorithms in terms of speed, making it ideal for encrypting large volumes of data. AES was introduced in 1997 as a successor to the aging DES algorithm and has undergone extensive testing to ensure its robustness. It has since become the global standard for encryption, offering a trusted solution for securing sensitive information. By implementing AES, Artemis Financial can safeguard its data, maintain compliance with regulatory standards, and defend against various security threats.

## Certificate Generation

Insert a screenshot below of the CER file.



## 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

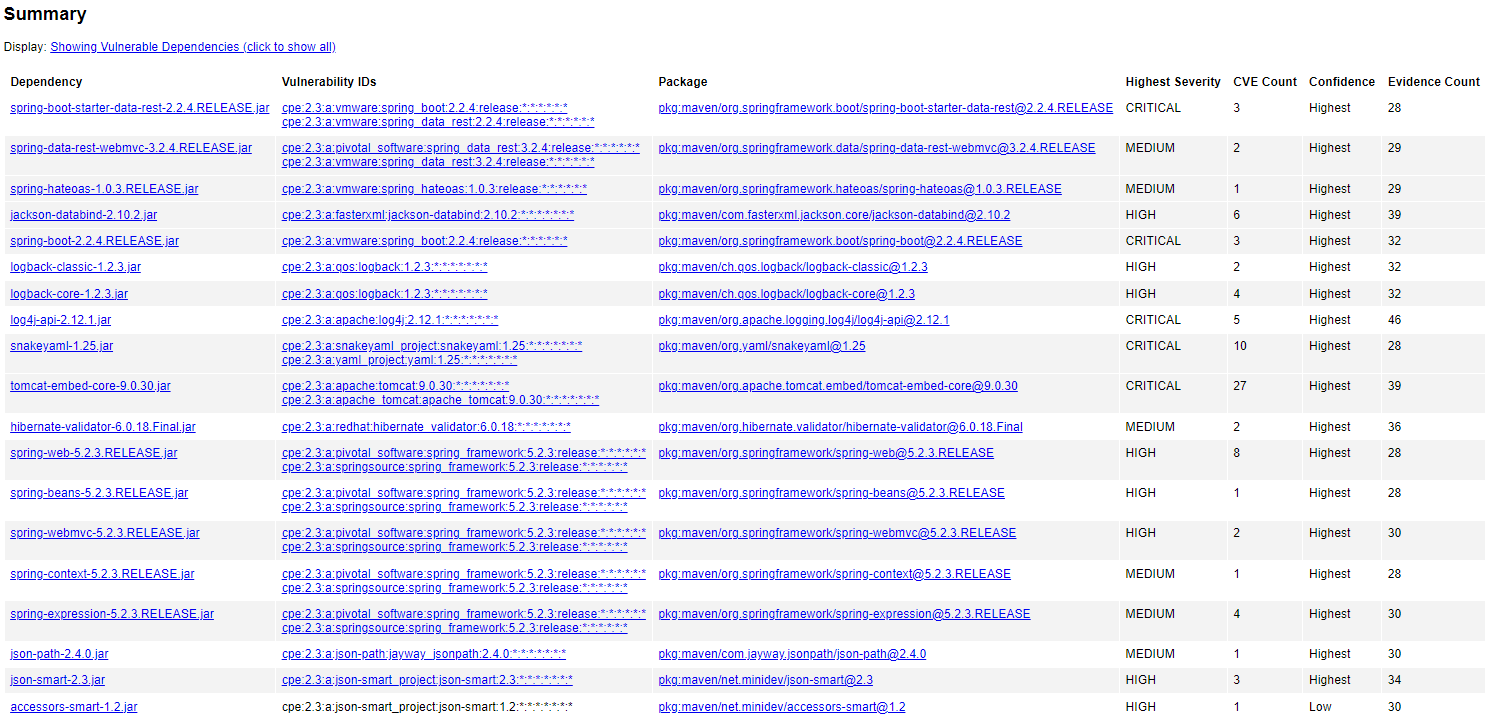
Description automatically generated

## 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



## Functional Testing

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

A screen shot of a computer program

Description automatically generated

## Summary

I refactored the code base by introducing a REST controller that calculates a SHA-256 hash for data. By using this algorithm I address the security concern for data integrity. Using SHA-256 to generate a checksum, data can be verified by calculating its hash and checking it against a stored value. Another area I reviewed was error handling. By carefully considering multiple scenarios, I ensured that the system didn’t fail silently or expose the system to vulnerabilities. Overall, the original code had no functional endpoint and my additions addressed potential vulnerabilities while increasing functionality.

## Industry Standard Best Practices

SHA-256 is highly regarded in the industry and by implementing it, we adhered to industry standards for cryptographic operations. Furthermore, I implemented a “try-catch” block around the MessageDigest implementation which ensures that exceptions are handled very carefully. The value of applying industry standard best practices for secure coding is that it increases security integrity, and scalability and compliance. The selected algorithm aligns with industry best practices for securing sensitive data and ensures that even if data is intercepted it can be detected by its hash value. Furthermore, using this algorithm ensures that the application will be compliant with regulatory requirements and helps avoid legal issues for the company.