****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions Error! Bookmark not defined.](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 5](#_Toc102040760)

[4. Secure Communications 5](#_Toc102040761)

[5. Secondary Testing 5](#_Toc102040762)

[6. Functional Testing 7](#_Toc102040763)

[7. Summary 7](#_Toc102040764)

[8. Industry Standard Best Practices 8](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2/23/2025** | **Sumiko Mitchell** |  |

## Client



## Developer

Sumiko Mitchell

## Algorithm Cipher

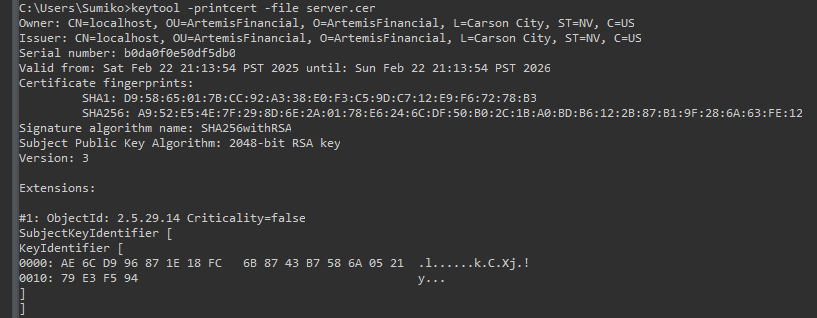
Artemis Financial has requested that Global Rain strengthen its web application by adding secure communication mechanisms to verify data transfers via a checksum. Global Rain recommends implementing the Advanced Encryption Standard (AES) with a 256-bit key length (AES-256). AES-256 is a symmetric block cipher that takes data and divides it into 128-bit sections. Each section, or block, goes through 14 rounds of substitution and transposition operations. Since this is a symmetric cipher, it uses the same key for encryption and decryption.

Global Rain recommends combining AES-256 encryption with the Secure Hash Algorithm (SHA-256) for checksum verification. SHA-256 produces a unique 256-bit value as a digital fingerprint for data verification. Artemis Financial's web application will use Java's SecureRandom class to generate cryptographically secure random numbers for initializing vectors and keys.

AES encryption has a proven track record since the National Institute of Standards and Technology (NIST) selected it as the recommended encryption algorithm for all federal agencies and incorporated it into the Federal Information Processing Standards (FIPS) 197 in 2001 (Cybersecurity and Infrastructure Security Agency (CISA) & Federal Partnership for Interoperable Communications (FPIC), 2024). Financial institutions have adopted AES for compliance with regulations like ISO/IEC 27001 (Barker, 2024) and the Gramm-Leach-Bliley Act (Guide to the Gramm–Leach–Bliley Act, 2018), which combined with its status as an encryption algorithm with no known practical attacks, makes it the ideal choice for Artemis Financial's security needs.

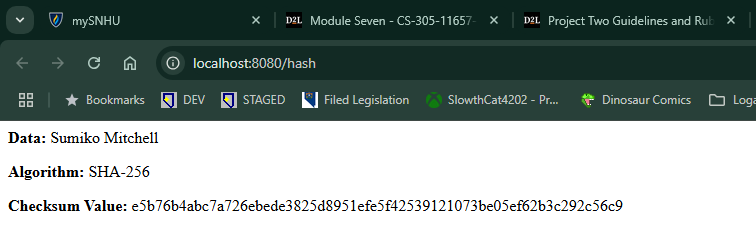
## Certificate Generation

A screenshot of the CER file



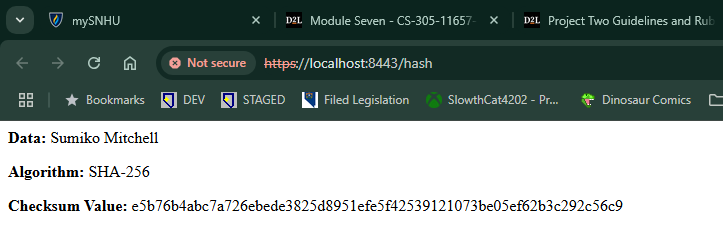
## Deploy Cipher

A screenshot of the checksum verification (http://localhost:8080/hash)



## Secure Communications

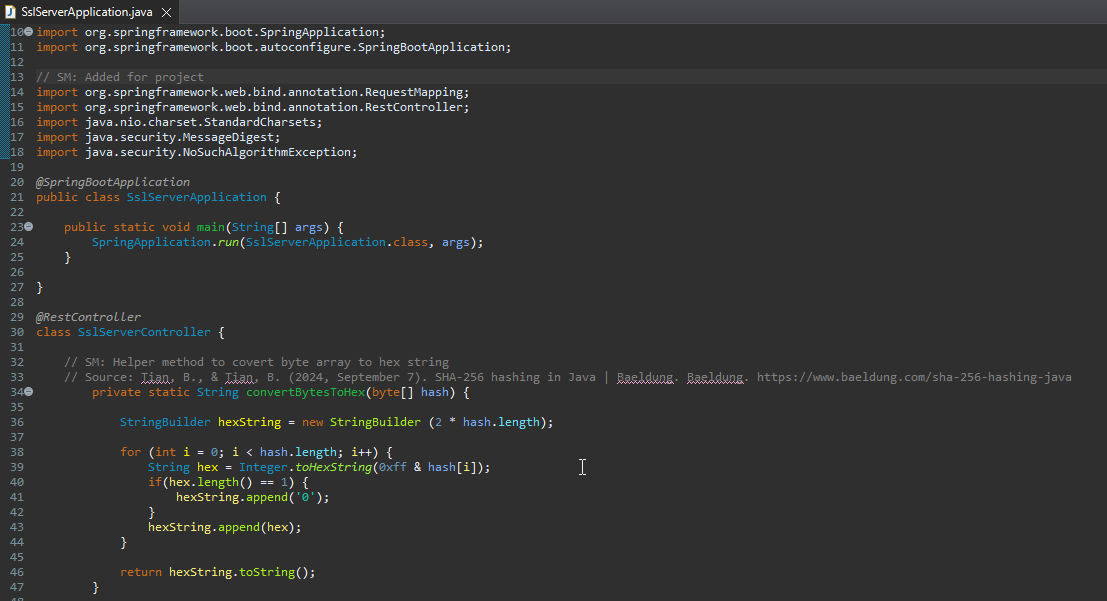
A screenshot of a web browser showing a secure webpage (https://localhost:8443/hash)

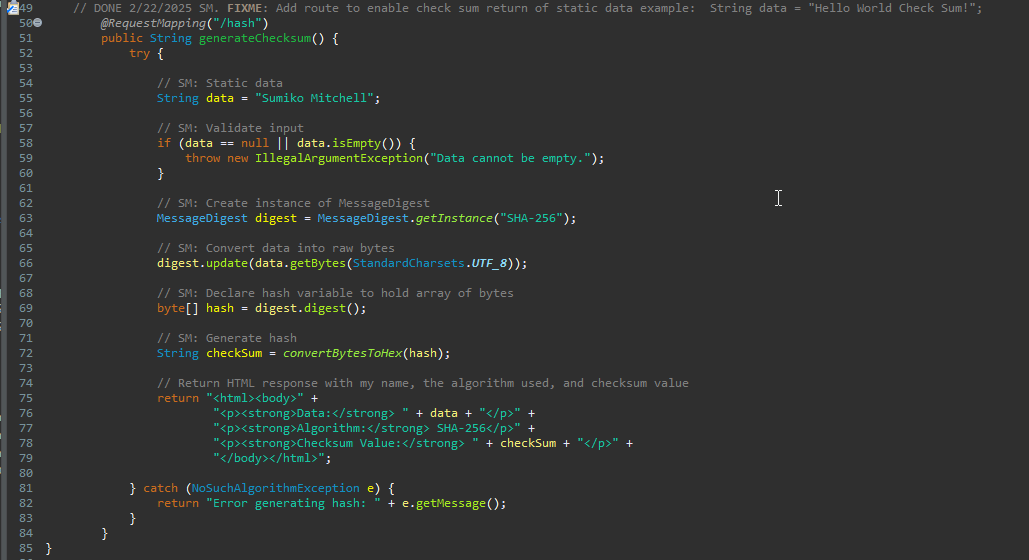


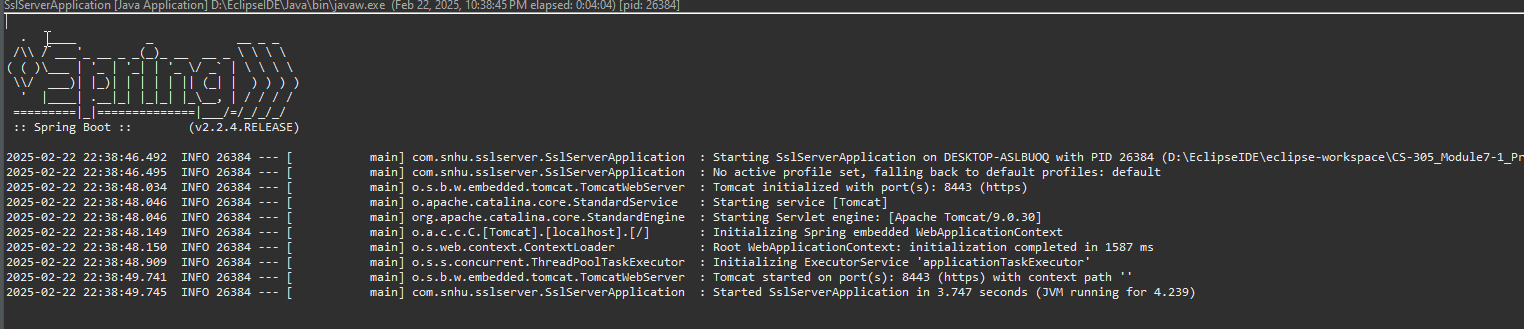
**Note:** The security warning shown in the HTTPS screenshot is expected behavior as I am using a self-signed certificate (server.cer) for development purposes.

## Secondary Testing

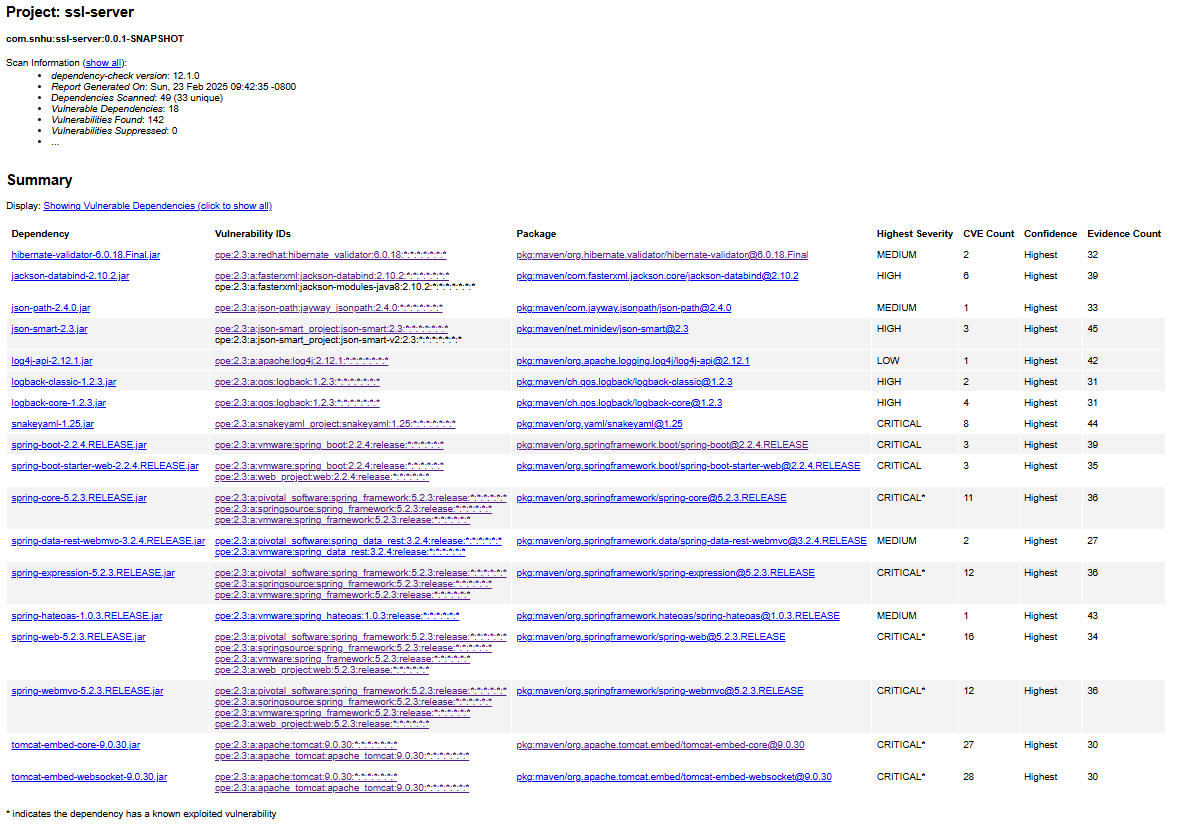
Screenshots of the refactored code executing without errors



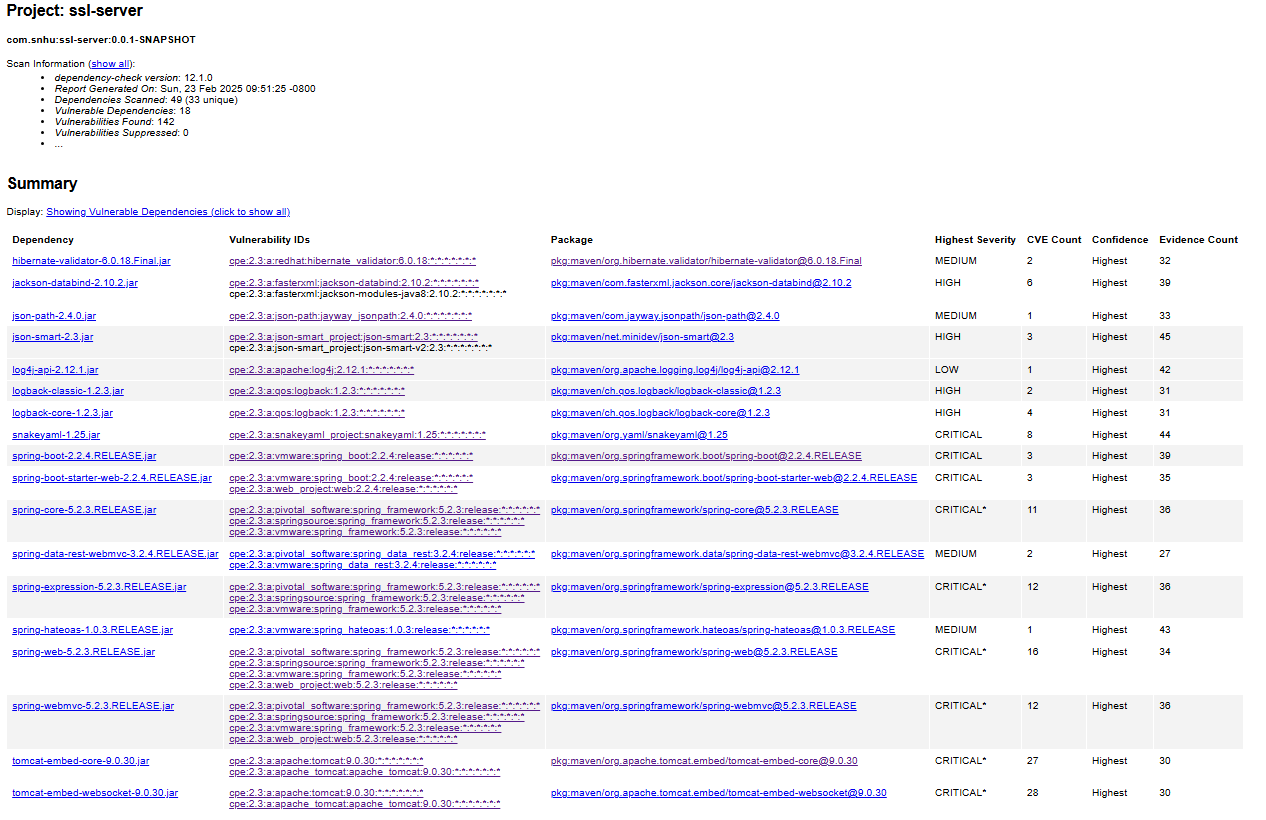


****

Screenshot of dependency-check report ***before*** refactoring



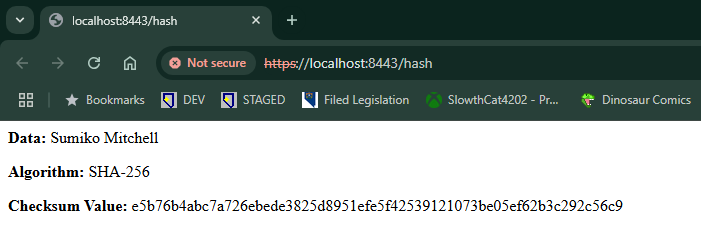
Screenshot of dependency-check report ***after*** refactoring



**Note:** No new security vulnerabilities were introduced through code refactoring.

## Functional Testing

A screenshot of the refactored code executing without errors.



## Summary

The code refactoring process successfully implemented multiple security layers in Artemis Financial's web application, addressing key vulnerability areas identified in the assessment flow diagram. The improvements included implementing SHA-256 for checksum verification, converting to HTTPS protocol with SSL/TLS encryption on port 8443, adding input validation, updating the dependency-check plugin to version 12.1.0, and implementing proper exception handling for cryptographic operations. Each security measure was tested independently and as part of the integrated system to ensure proper operation without introducing new vulnerabilities.

## Industry Standard Best Practices

The implementation followed secure coding best practices by using NIST-approved cryptographic algorithms (SHA-256 and AES-256), enforcing HTTPS-only communication with proper SSL/TLS configuration, implementing secure key store management, and maintaining regular security scanning of dependencies using OWASP dependency-check with a custom suppression file. By following these practices, Artemis Financial can securely handle client financial data while complying with industry regulations and standards.

**REFERENCES**

Cybersecurity and Infrastructure Security Agency (CISA) & Federal Partnership for Interoperable Communications (FPIC). (2024). Transition to Advanced Encryption Standard (AES). In *CISA | DEFEND TODAY, SECURE TOMORROW* (pp. 1–3). <https://www.cisa.gov/sites/default/files/2024-05/23_0918_fpic_AES-Transition-WhitePaper_Final_508C_24_0513.pdf>

Barker, S. (2024, June 27). ISO 27001 explained simply. High Table. <https://hightable.io/iso-27001/>

Guide to the Gramm–Leach–Bliley Act. (2018, February 1). <https://iapp.org/resources/article/guide-to-the-gramm-leach-bliley-act/>