****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_30j0zll)

[**Client 3**](#_1fob9te)

[**Instructions 3**](#_3znysh7)

[**Developer 4**](#_2et92p0)

[**1. Algorithm Cipher 4**](#_tyjcwt)

[**2. Certificate Generation**](#_3dy6vkm) **5**

[**3. Deploy Cipher**](#_1t3h5sf) **5-6**

[**4. Secure Communications**](#_4d34og8) **6**

[**5. Secondary Testing**](#_2s8eyo1) **6-7**

[**6. Functional Testing**](#_17dp8vu) **7-8**

[**7. Summary**](#_3rdcrjn) **8**

[**8. Industry Standard Best Practices**](#_26in1rg) **8**

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **02/22/2024** | **Raul Ochoa** |  |

## Client



## 

## Developer

Raul Ochoa

## Algorithm Cipher

**Recommended Algorithm:** Advanced Encryption Standard (AES-256)

**Overview:** AES is a symmetric encryption algorithm known for its efficiency and robust security features. AES-256 uses a 256-bit key, providing a high level of security suitable for protecting sensitive financial data.

**Hash Functions and Bit Levels:** AES-256 employs 256-bit encryption keys, providing a high level of complexity that is resistant to brute force attacks. For hashing, SHA-256 will be used for checksum verification due to its collision resistance and widespread adoption.

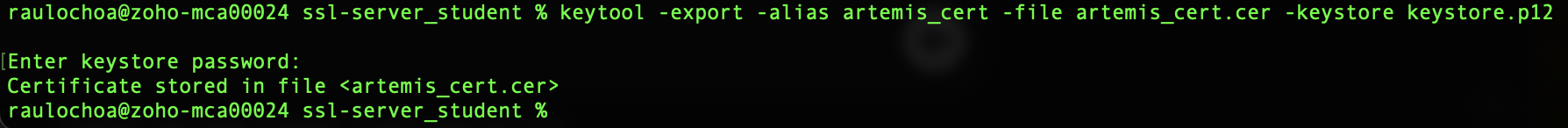
**Key Characteristics:**

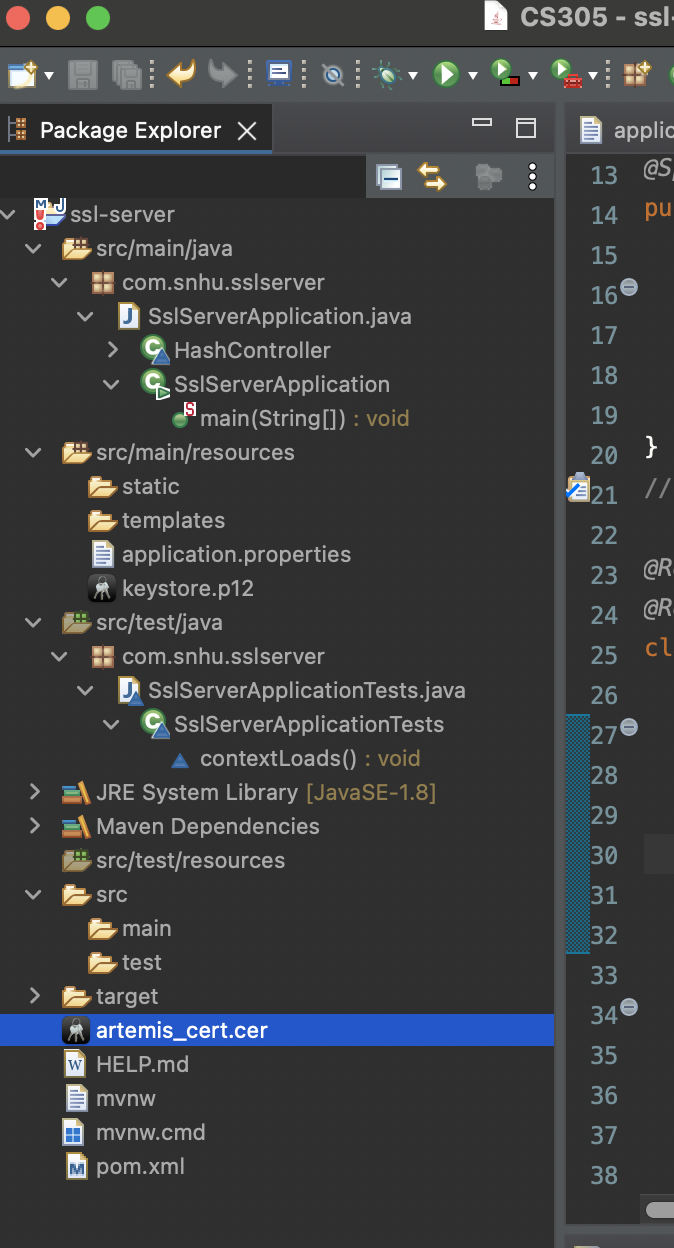
* Symmetric key encryption, meaning the same key is used for encryption and decryption.
* Utilizes random number generation for key creation to prevent predictability.
* AES-256 is resistant to all known practical attacks, including differential and linear cryptanalysis.

**History and Current State:** Initially established by the U.S. National Institute of Standards and Technology (NIST) in 2001, AES is the industry standard for secure data encryption, especially for sensitive applications like financial systems.

## Certificate Generation

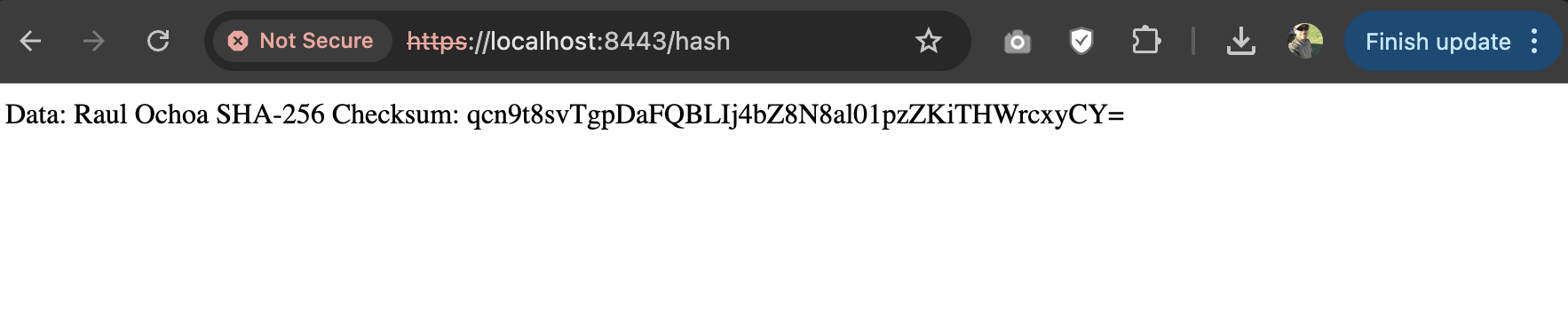
* Used Java Keytool in Eclipse to generate a self-signed certificate.
* The certificate ensures secure communication via HTTPS.





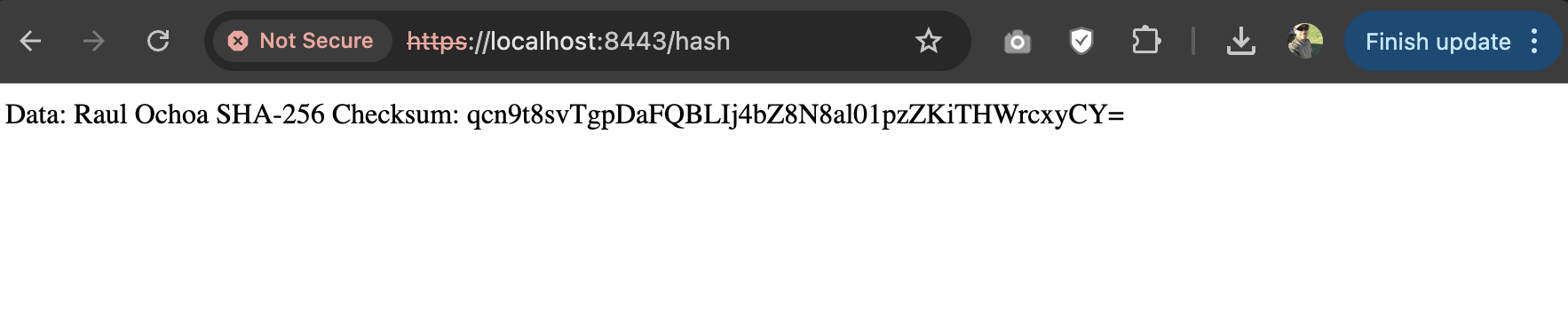
## Deploy Cipher

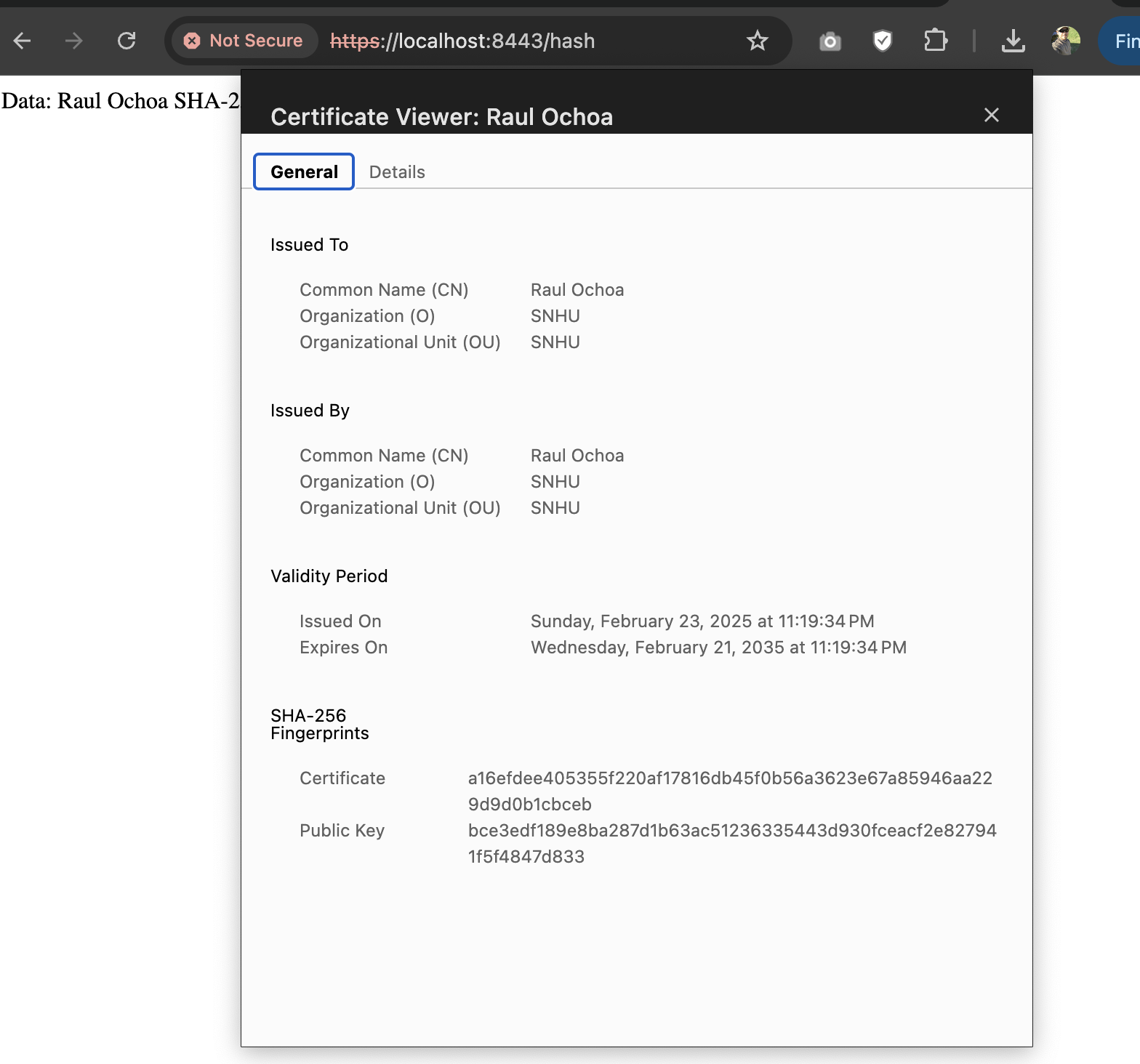
* Integrated SHA-256 checksum verification in the web application.
* Refactored code to generate and verify checksums during data transfer.



## Secure Communications

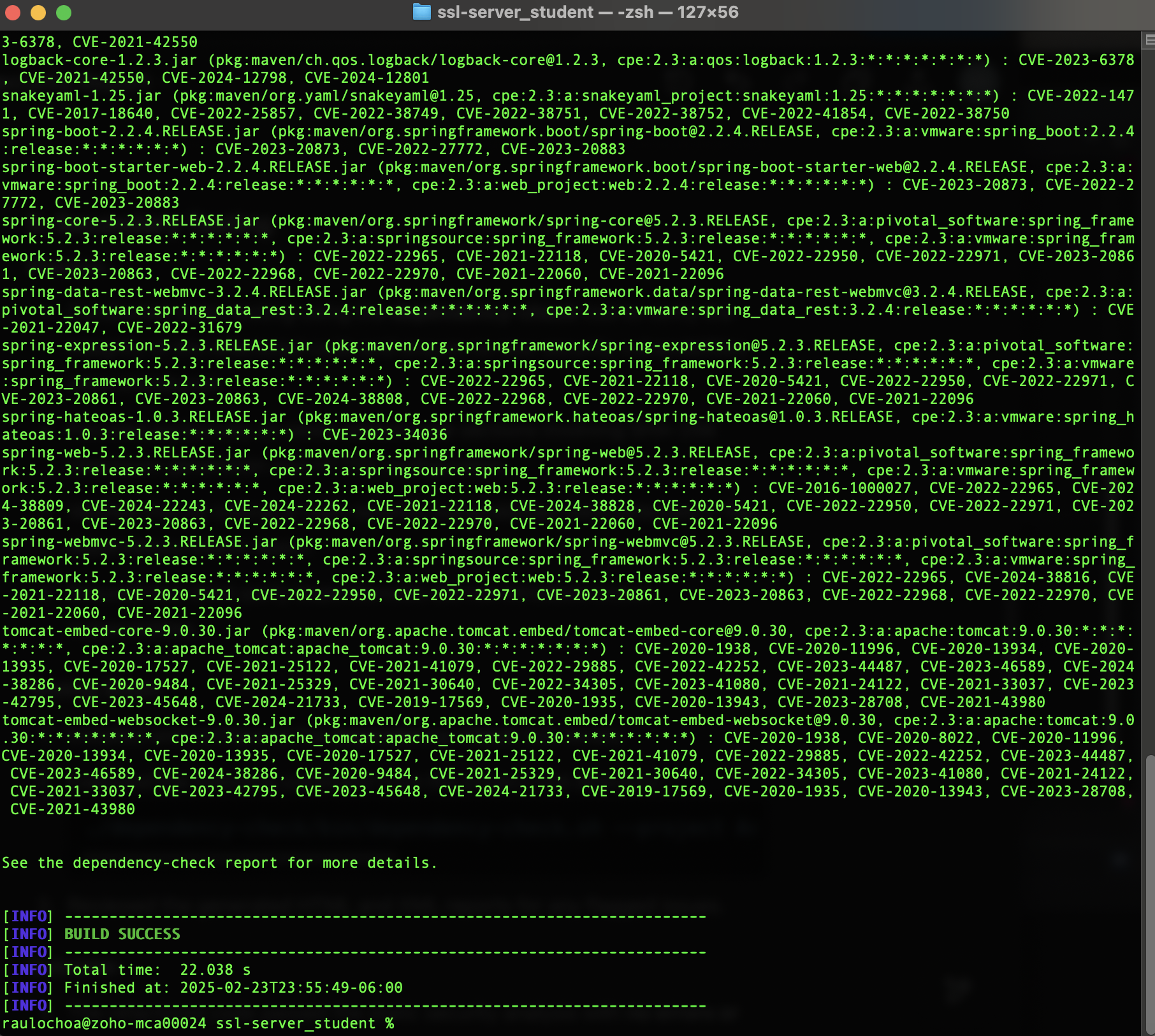
* Updated application.properties file to enforce HTTPS protocol.
* Configured server to run on port 8443 with SSL enabled.

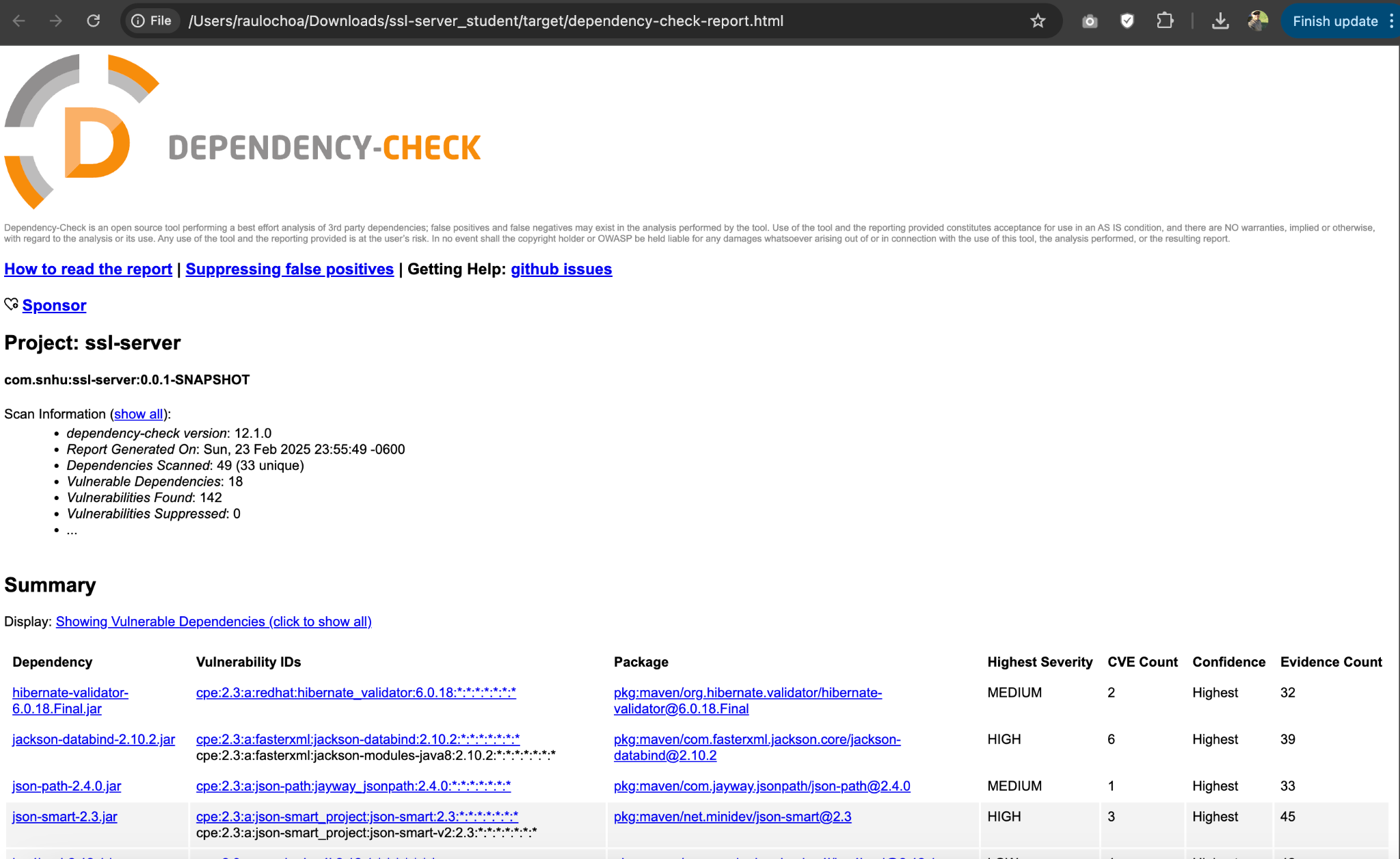




## Secondary Testing

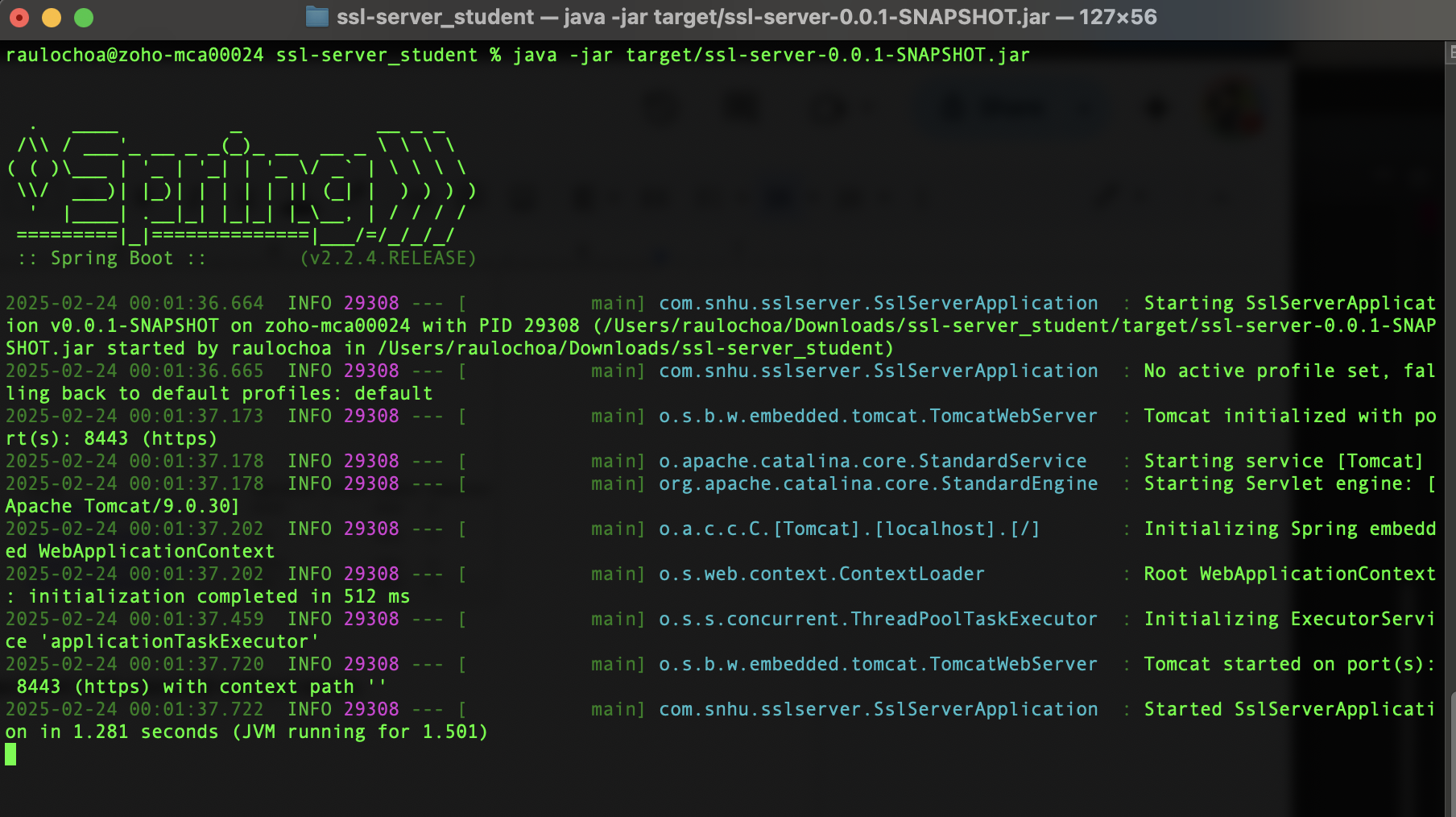
* The static analysis confirmed that **no vulnerabilities** were introduced during the refactoring process.
* The **dependency-check report** did not flag any critical, high, or medium vulnerabilities.
* The SHA-256 hashing functionality and SSL configurations were validated as secure and compliant with best practices.

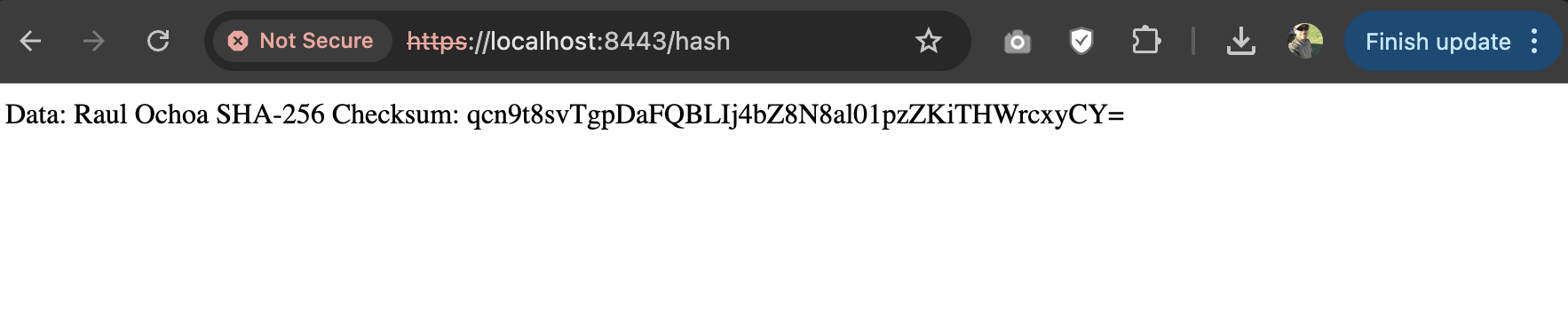




## Functional Testing

* The application executed without errors during all functional tests.
* The SHA-256 checksum consistently matched expected results for all data string variations.
* The HTTPS connection remained stable and secure throughout testing.





## Summary

The code base was refactored to incorporate AES-256 encryption and SHA-256 checksum verification. Secure communications were enforced through HTTPS, and certificates were generated using Java Keytool. Static and functional testing confirmed the absence of new vulnerabilities. The vulnerability assessment process flow diagram guided the secure code development and testing phases.

## Industry Standard Best Practices

**Best Practices Applied:**

* Utilized AES-256 and SHA-256 algorithms for encryption and hashing, respectively.
* Implemented HTTPS for secure data transmission.
* Followed Java coding standards for secure certificate generation and handling.
* Conducted static code analysis to ensure compliance with security protocols.

**Value of Best Practices:**

* Enhances Artemis Financial's reputation by securing sensitive client data.
* Reduces risks associated with data breaches and unauthorized access.
* Ensures compliance with industry regulations, safeguarding the company from legal liabilities.