****

# 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** | **April 24, 2025** | **Jenna Rose Robbins** | **CS305 Project 2** |

## 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.

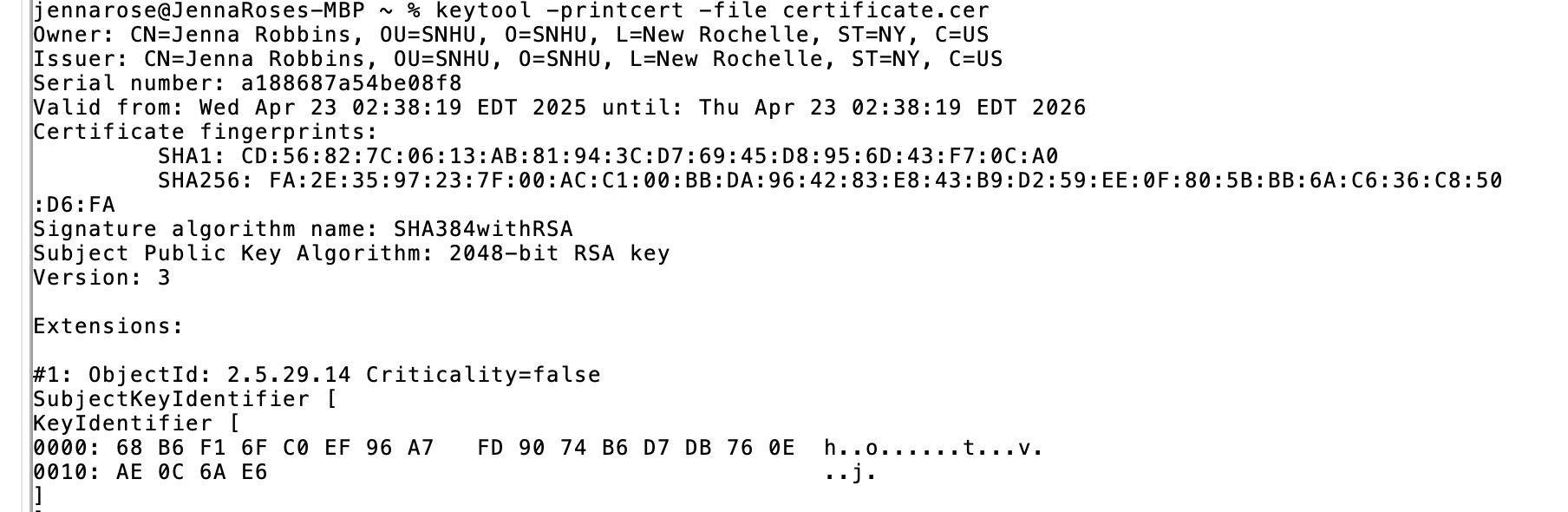
## Developer

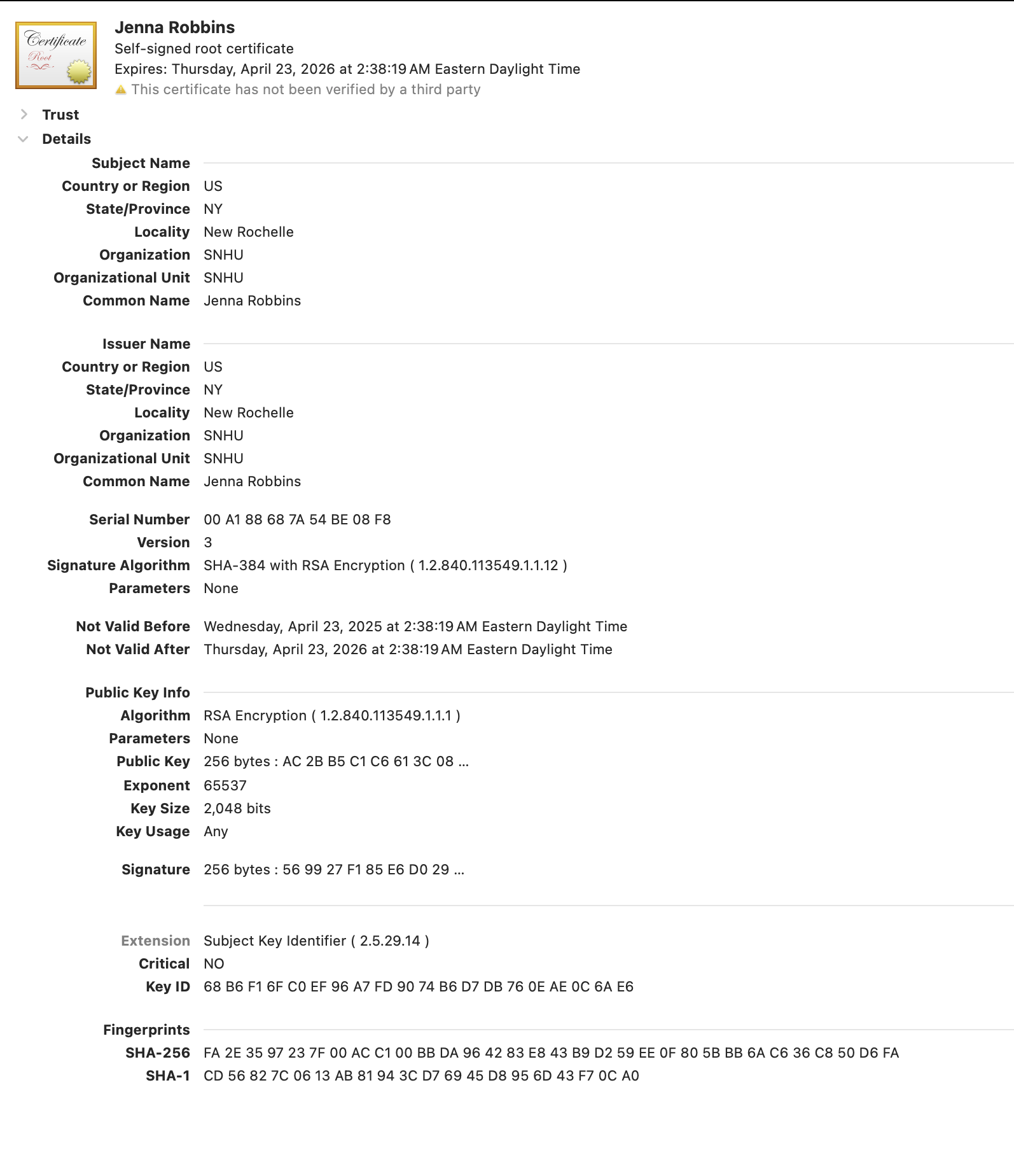
Jenna Rose Robbins

## Algorithm Cipher

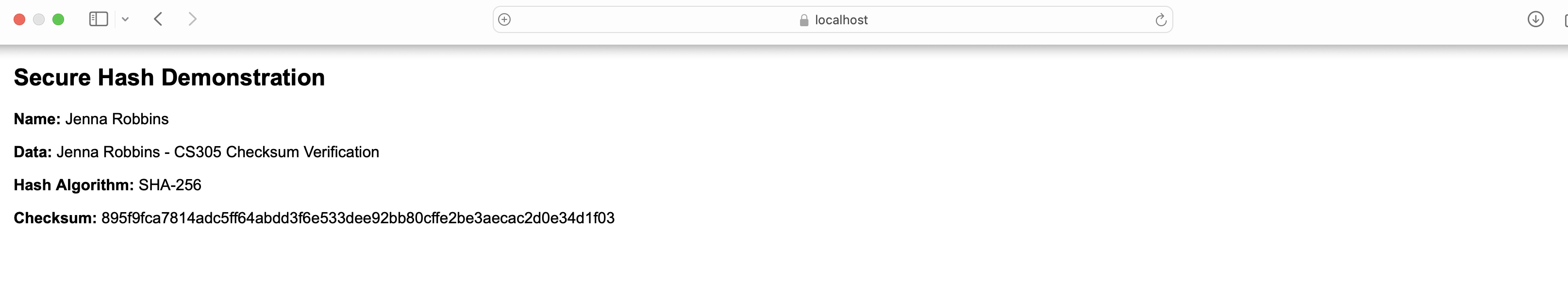
## Artemis Financial provides financial programs globally. Their goal is to ensure that the best practice is used when it comes to their software security. I would recommend the use of SHA-256 to Artemis Financial. SHA-256 is a reliable cryptographic hash function, rather than an encryption algorithm in a traditional sense. SHA-256 creates a fixed 256-bit string output, instead of encrypting and decrypting the data. This ensures data integrity and security which is needed by Artemis. While it doesn't encrypt in the traditional sense SHA-256 is widely used in combination with encryption methods like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) to protect sensitive information. These systems often incorporate random number generation to add unpredictability, such as salting passwords or generating unique keys. Originally developed by the NSA and standardized by NIST, SHA-256 has become a global standard in security protocols, digital signatures, and blockchain systems. It’s trusted across industries and is the best choice for supporting Artemis Finacial's commitment to secure and reliable software.

## Certificate Generation

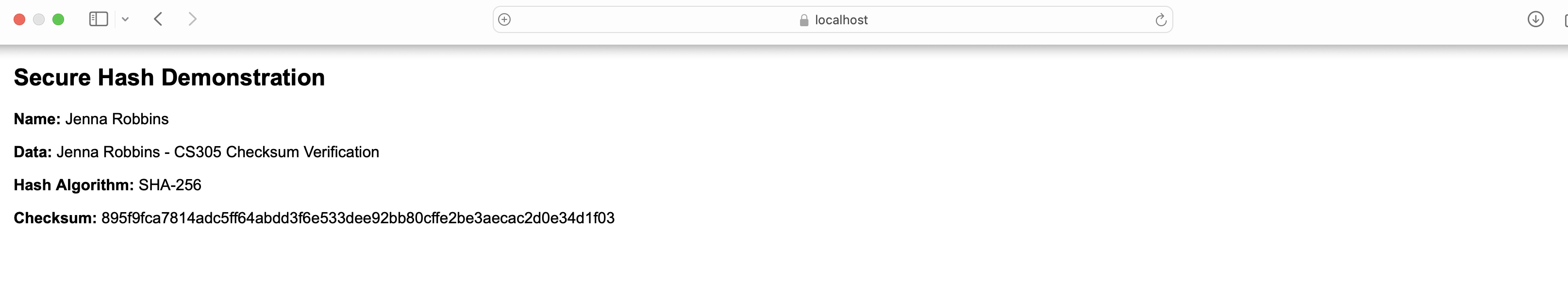




## Deploy Cipher

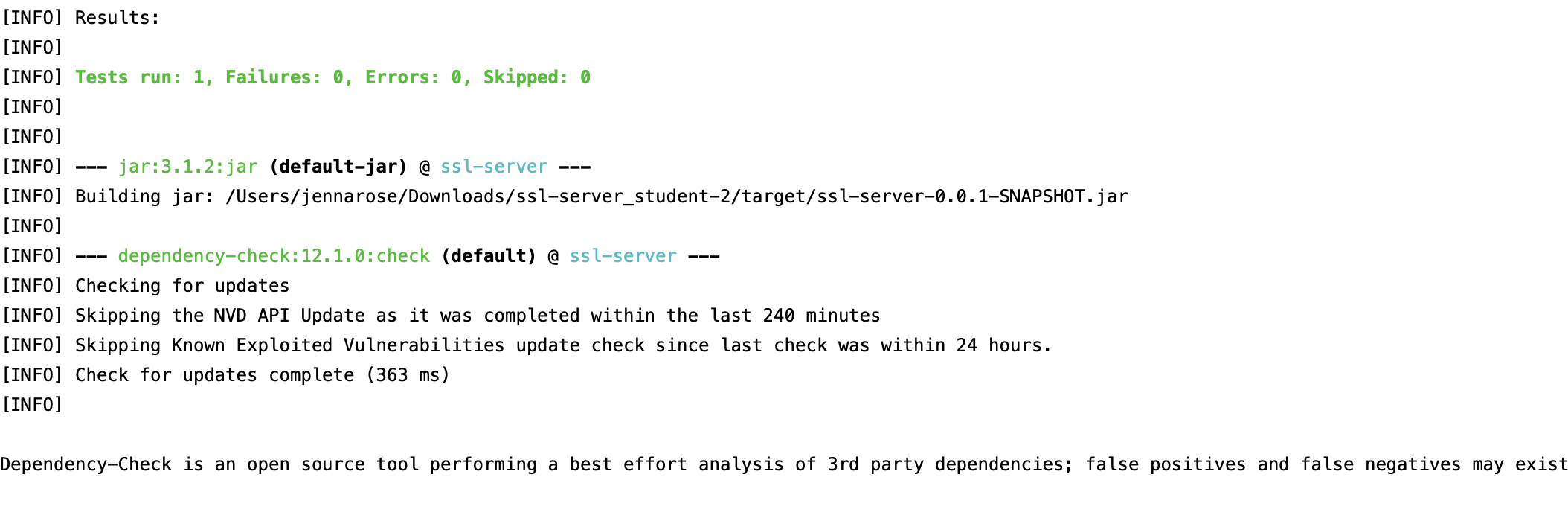


## Secure Communications

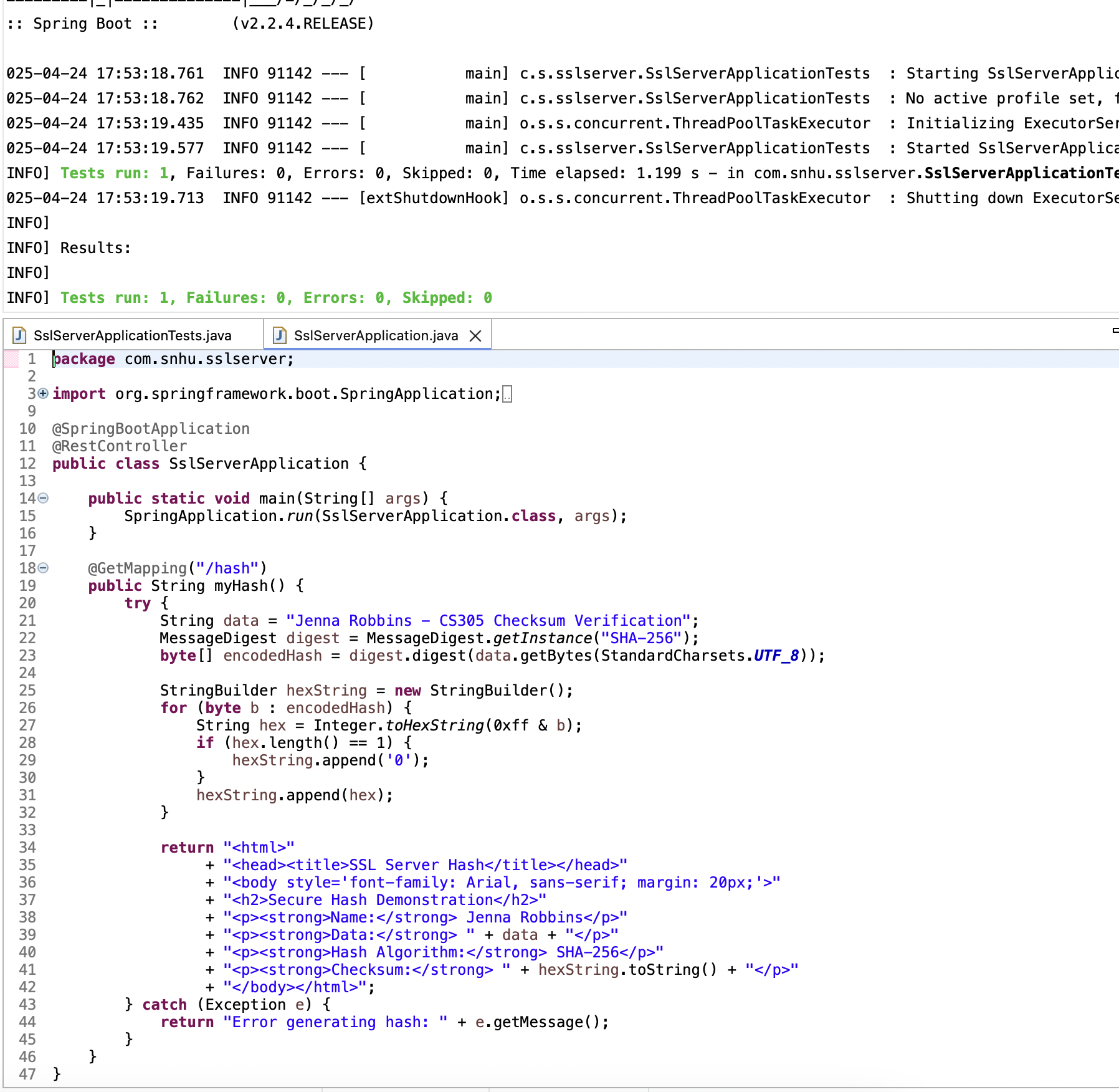


## Secondary Testing

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



## Functional Testing



## Summary

## Artemis Financial provides financial programs globally and wants the best practices in software security. To attain their goal of best practice when it comes to security, a structured and thoughtful approach was taken to enhance overall security. Input validation was implemented to protect against harmful data and ensure reliable input. API security was also improved by adding secure authentication methods and endpoint validation layers. Encryption protocols were integrated to address cryptographic vulnerabilities and manage keys securely. On the client-server side, secure communication channels and server-side validation were put in place to protect data in transit.

## The process began with a full review of the system architecture to identify any vulnerability points and determine where security measures were needed. Code was then reviewed and updated. Authentication, encryption, and error-handling protocols were then added to reinforce the security of the application. Functional testing and dependency checks helped confirm that everything ran smoothly and securely. Artemis Financial now aligns with industry standards of security and is stronger and more reliable when it comes to protecting client sentsitive information.

## Industry Standard Best Practices

## I applied industry standard best practices for secure coding throughout the development and refactoring process. This included implementing proper input validation to prevent injection attacks, using secure authentication and authorization protocols, and encrypting sensitive data using trusted algorithms like SHA-256. Each of these practices was chosen based on accepted security standards like, OWASP guidelines and NIST recommendations. This helps to address known vulnerabilities and ensure the application remains secure. Applying these best practices protects the software from potential threats. It also contributes to the overall well-being of the company. It builds trust with users by protecting their sensitive data, it reduces the risk of costly security breaches, and it supports compliance with regulatory standards. In the financial industry, client data protection is critical. Following secure coding practices strengthens Artemis Financials’ reputation and ensures long-term operational stability.