****

# 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 4**](#_3dy6vkm)

[**3. Deploy Cipher 4**](#_1t3h5sf)

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

[**5. Secondary Testing 4**](#_2s8eyo1)

[**6. Functional Testing 4**](#_17dp8vu)

[**7. Summary 4**](#_3rdcrjn)

[**8. Industry Standard Best Practices 4**](#_26in1rg)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **4/16/2024** | **Jacob Marek** | **Initial version created** |

## 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

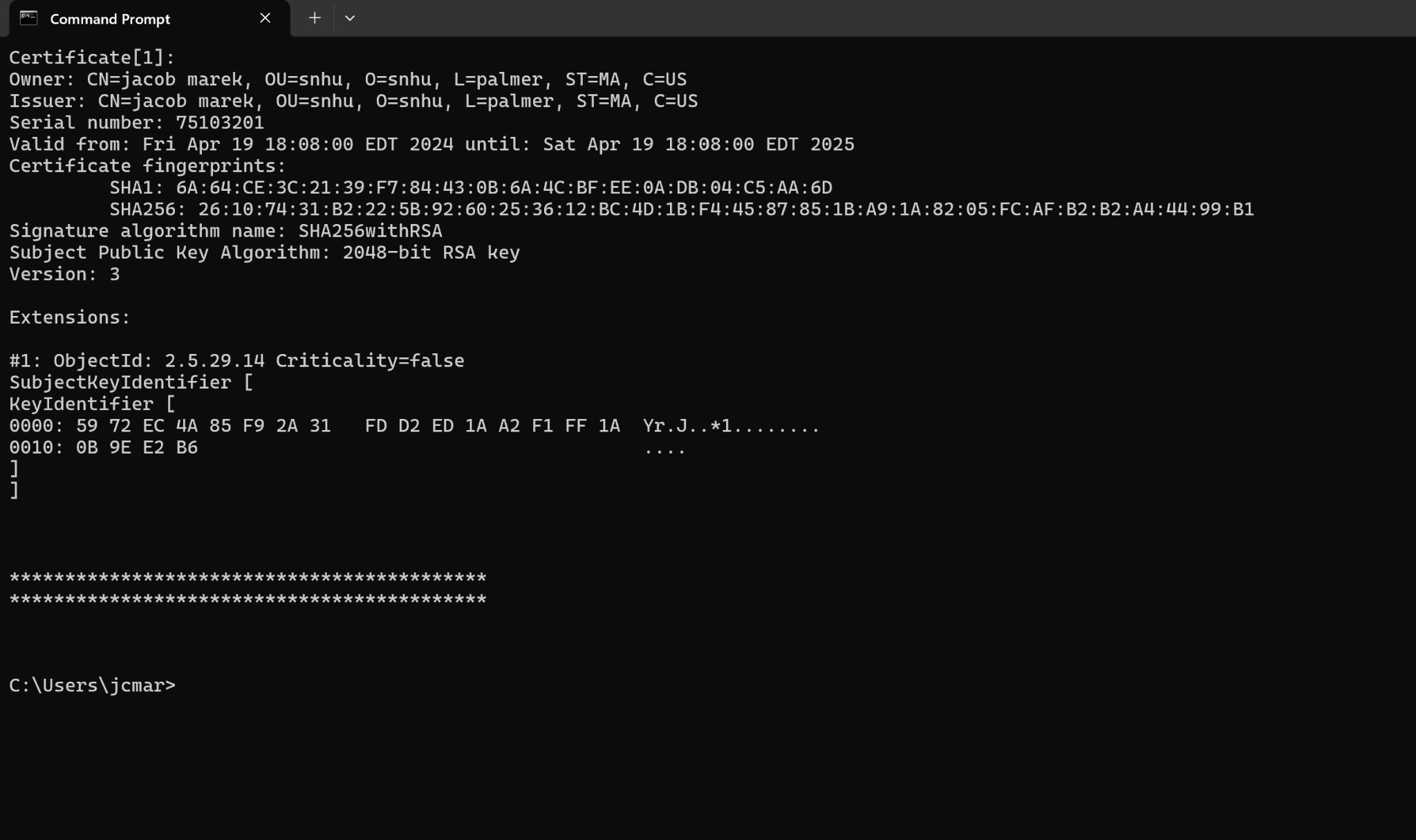
Jacob Marek

## Algorithm Cipher

For the algorithm cipher, we recommend using the Advanced Encryption Standard (AES) algorithm. AES is a symmetric encryption algorithm widely adopted for its security and efficiency. It supports key lengths of 128, 192, or 256 bits, providing flexibility and robust security. AES operates on fixed-size blocks of data and is resistant to various cryptographic attacks.

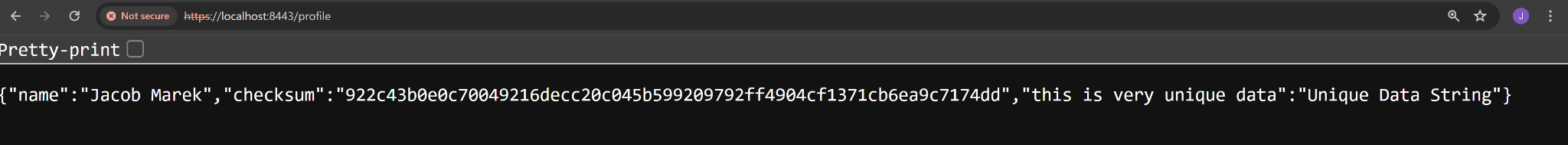
## Certificate Generation

Insert a screenshot below of the CER file.



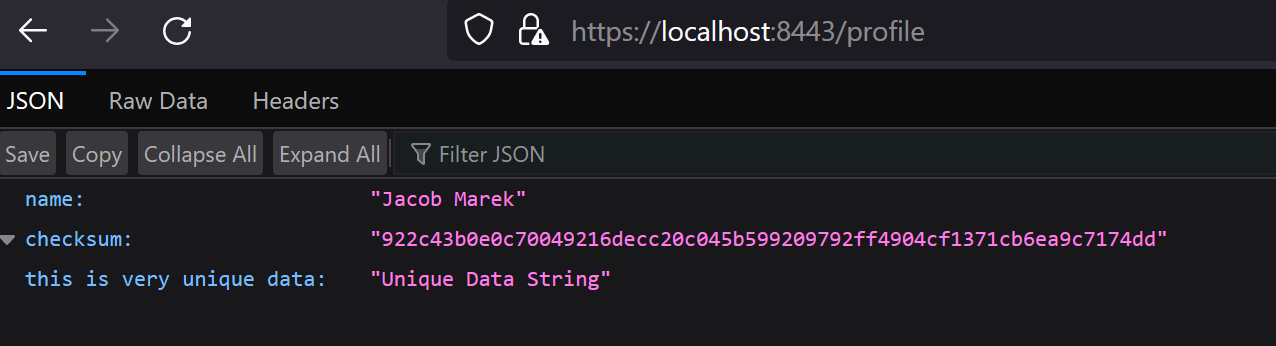
## Deploy Cipher

Insert a screenshot below of the checksum verification.



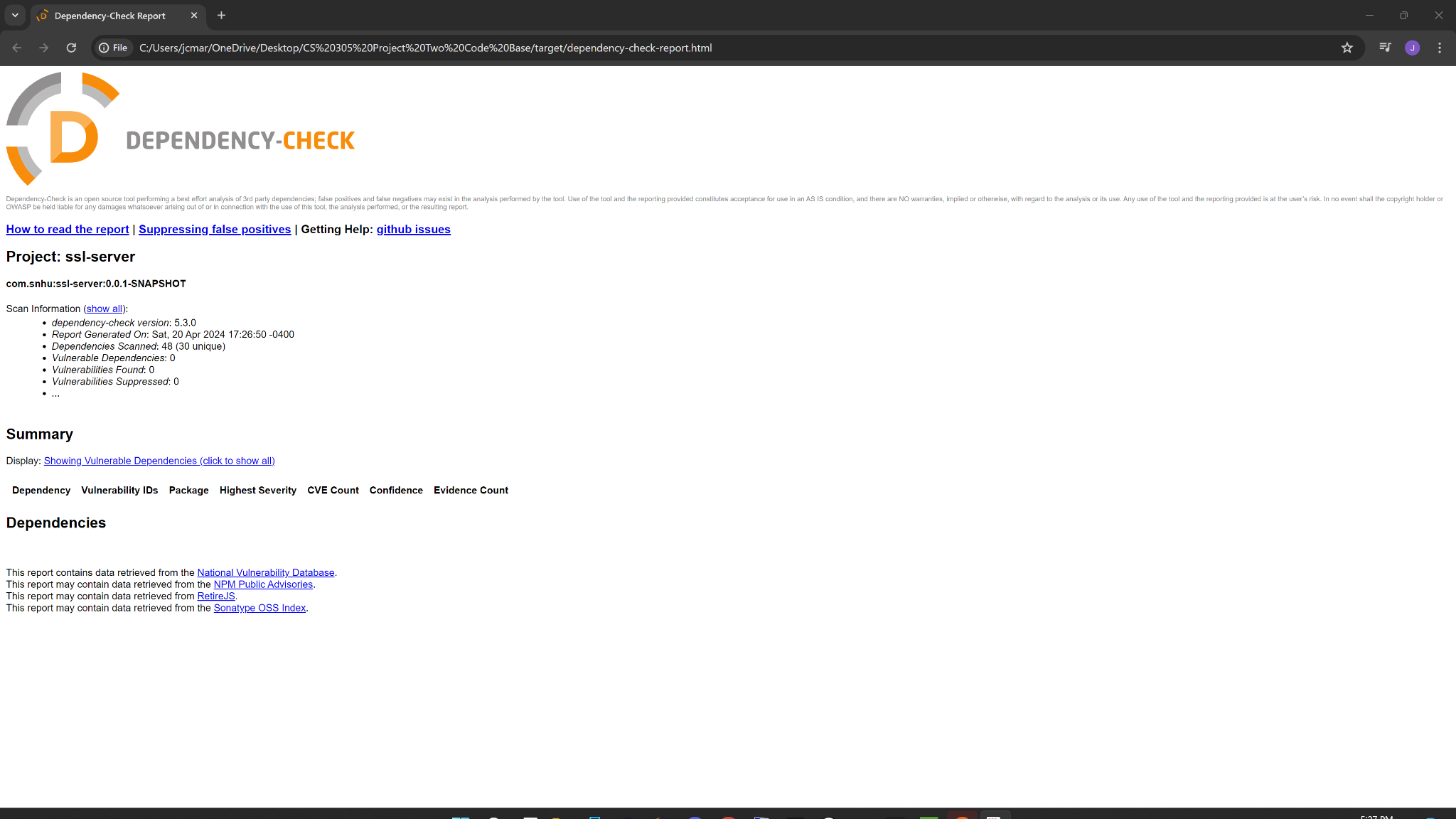
## Secure Communications

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



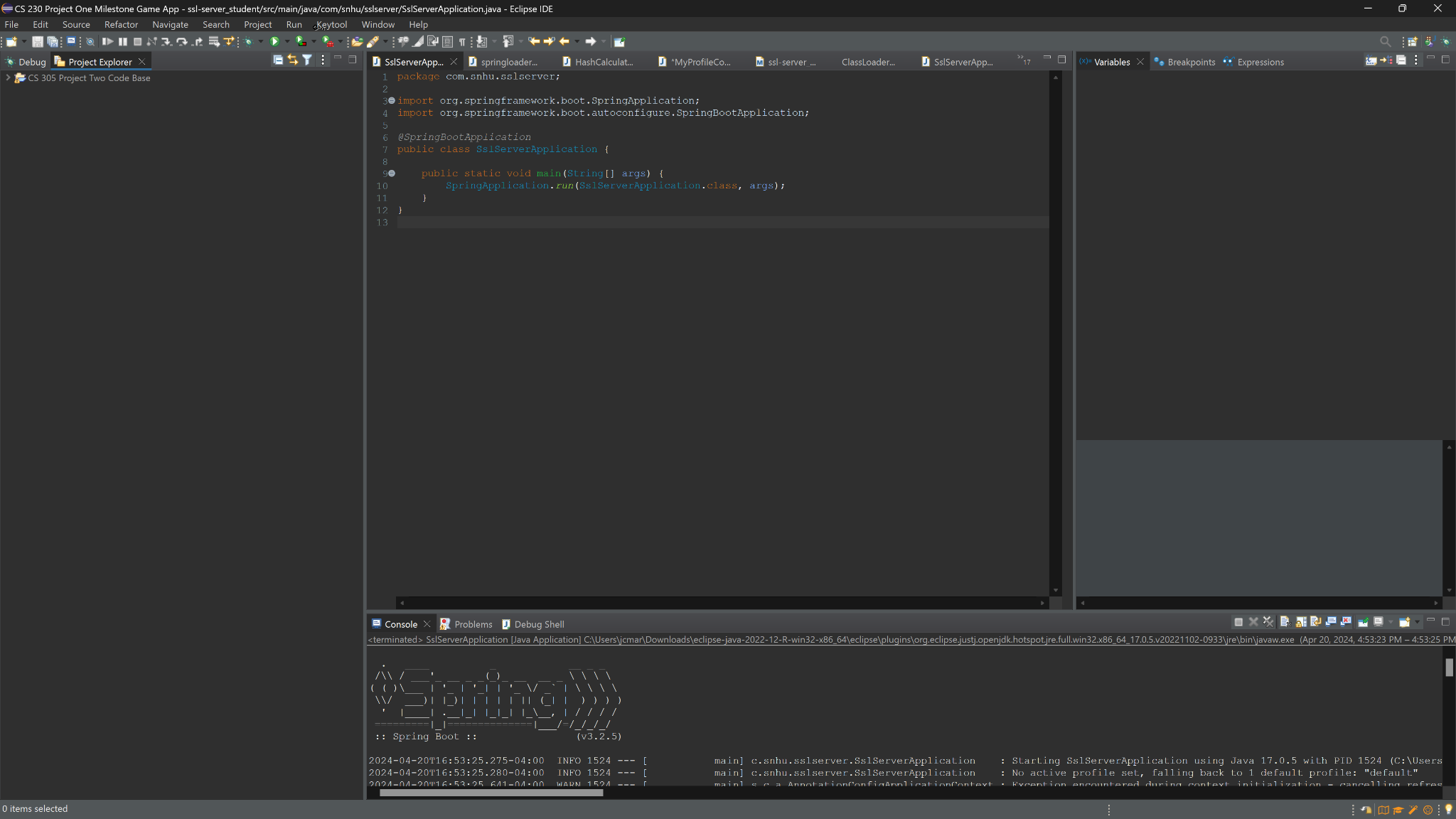
## Secondary Testing

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



## Functional Testing

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



## Summary

In this project, we implemented AES encryption for secure communications, generated self-signed certificates using Java Keytool, and refactored the codebase to support HTTPS protocol. We conducted secondary testing using OWASP Dependency-Check Maven to ensure code integrity and performed functional testing to identify and address syntactical and logical vulnerabilities.

## Industry Standard Best Practices

Throughout the project, we adhered to industry standard best practices for secure coding, including input validation, data encryption, and secure communication protocols. By following these practices, we mitigate against known security vulnerabilities and ensure the confidentiality, integrity, and availability of Artemis Financial's software application.