****

# 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** | **12/14/2024** | **Sachin Gurung** | **Project Two Version 1.0** |

## 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

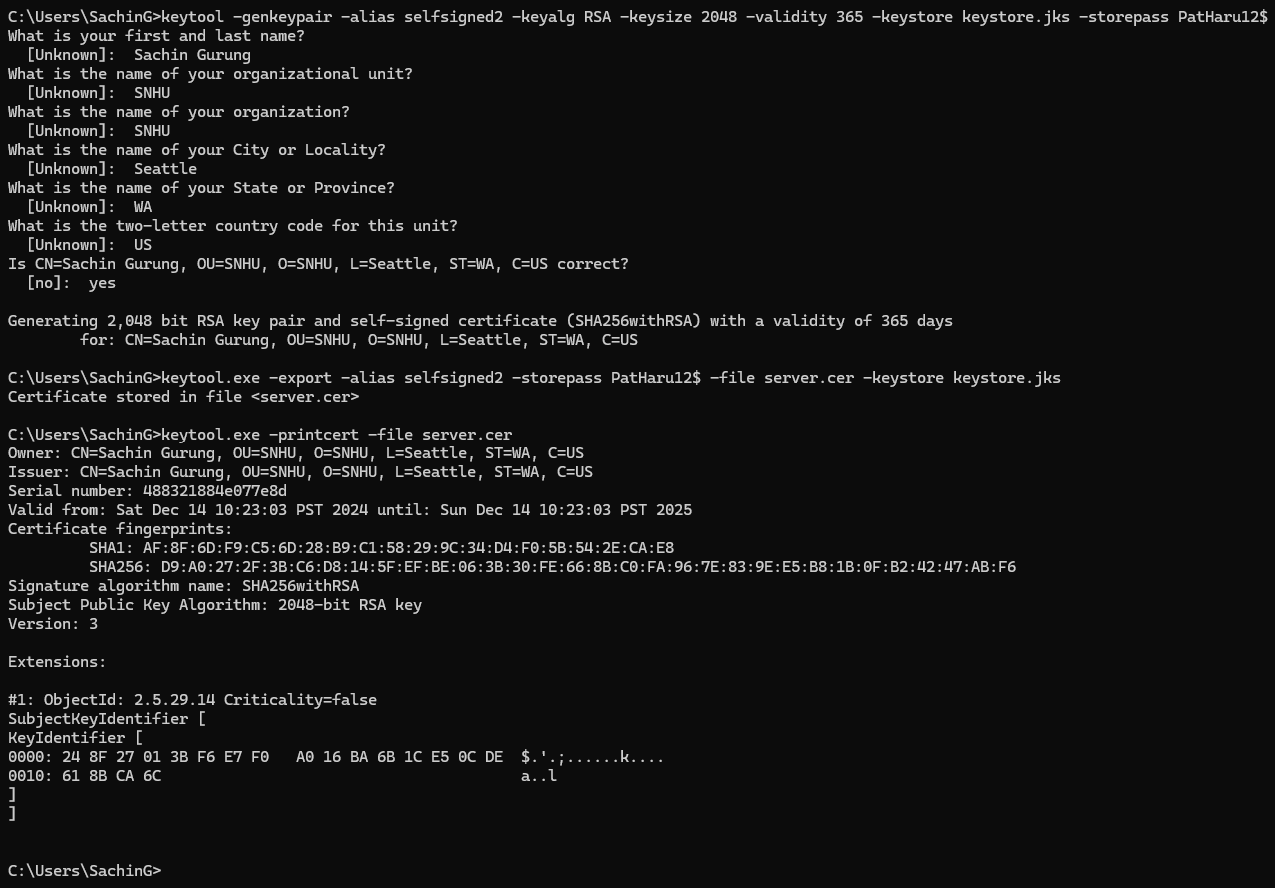
Sachin Gurung

## Algorithm Cipher

The selected encryption algorithm for this project is SHA-256. This was chosen due to its cryptographic hash function known for its robustness and is widely used in secure communication protocols. It is resistant to pre-image and collision attacks and this makes it a reliable option. This chosen algorithm is suitable for data verification processes. SHA-256 ensures data integrity by generating a unique fixed-size hash for any input data. This was developed by the NSA in 2001 and became a widely adopted standard. The algorithm uses a 256-bit hash function which provides a large space to make brute force attack infeasible. At present, SHA-256 is widely used across industries for secure hash generation.

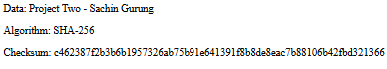
## Certificate Generation

Insert a screenshot below of the CER file.



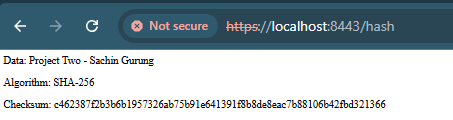
## Deploy Cipher

Insert a screenshot below of the checksum verification.



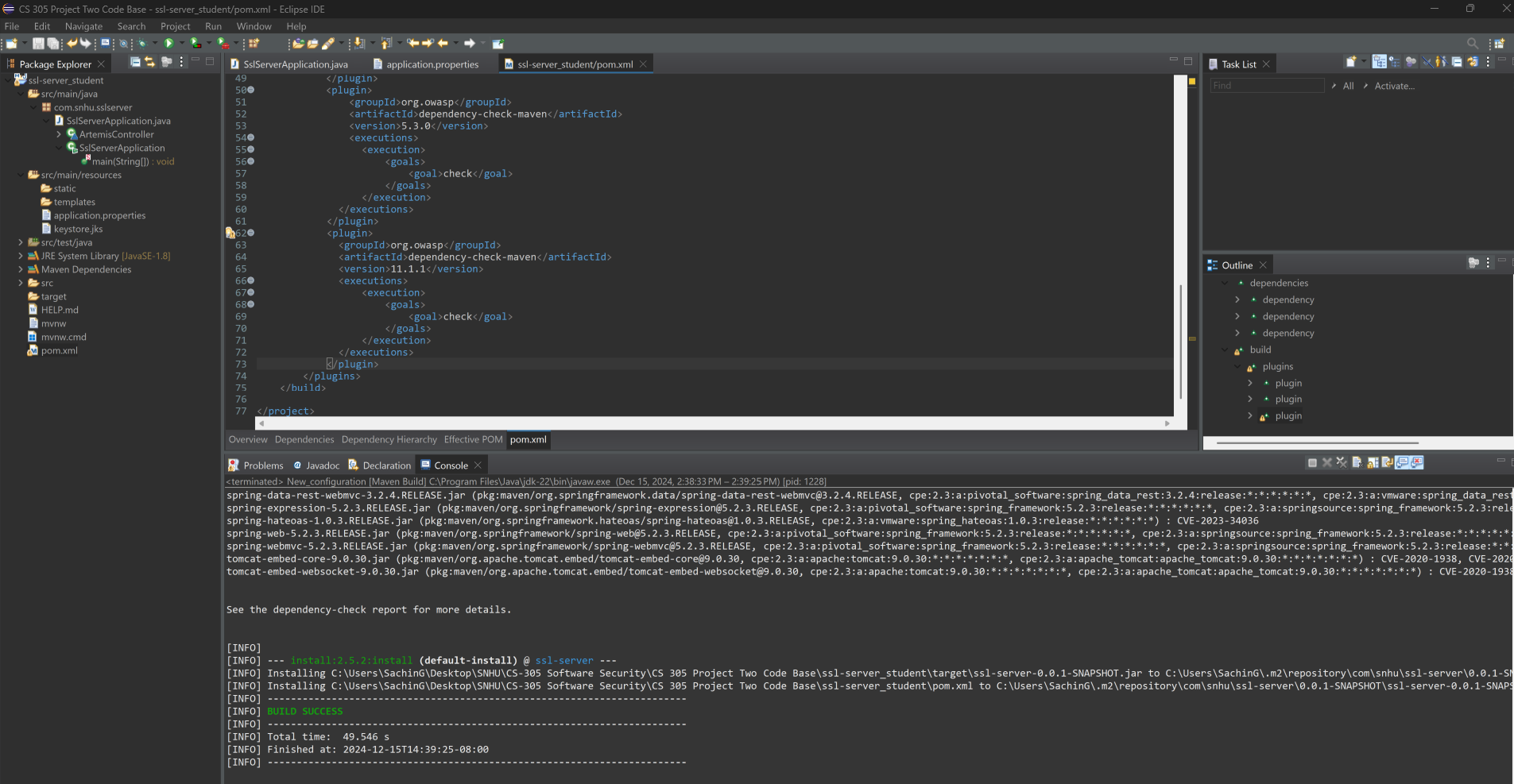
## Secure Communications

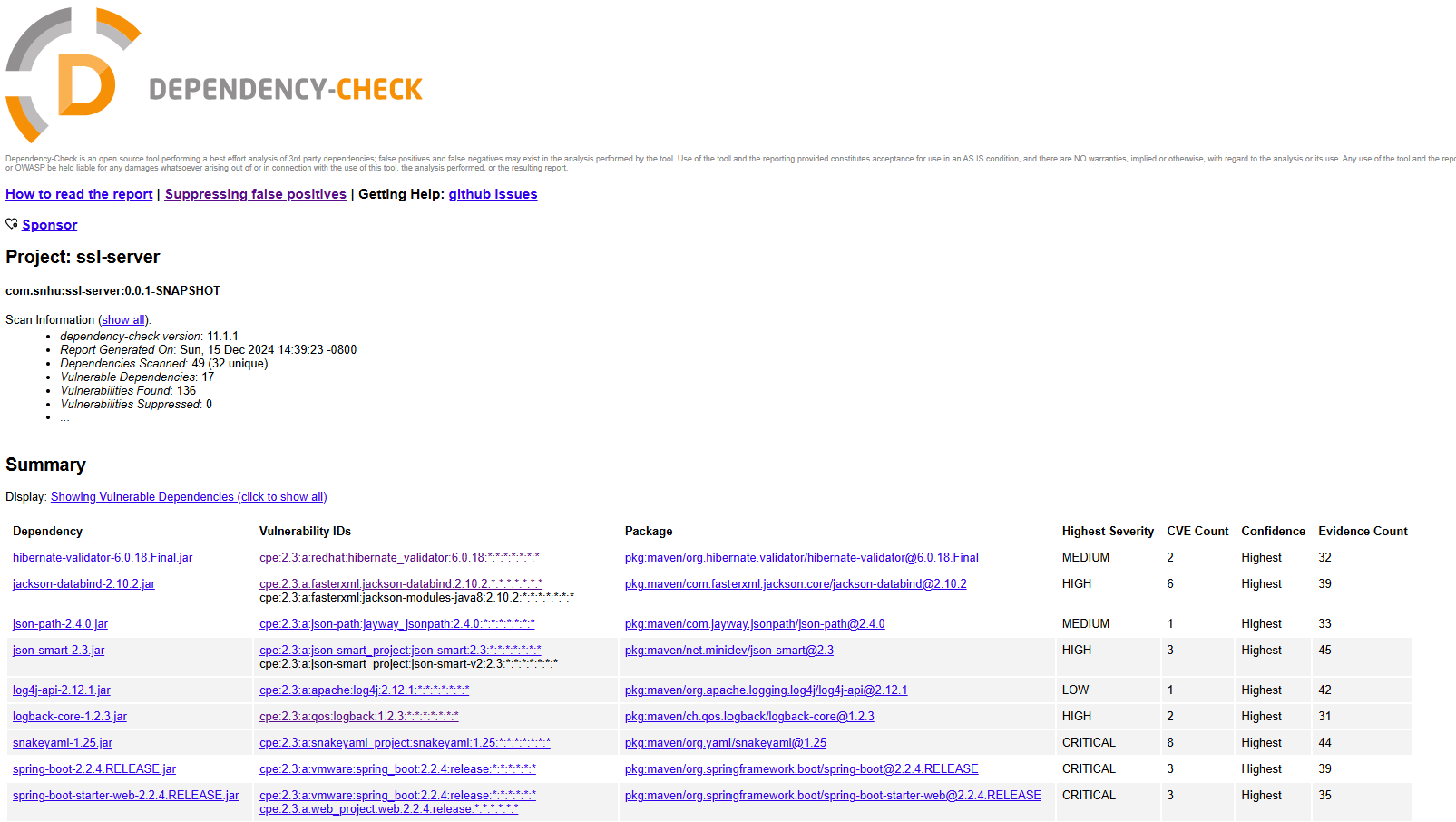
Insert a screenshot below of the web browser that shows a secure webpage.



## Secondary Testing

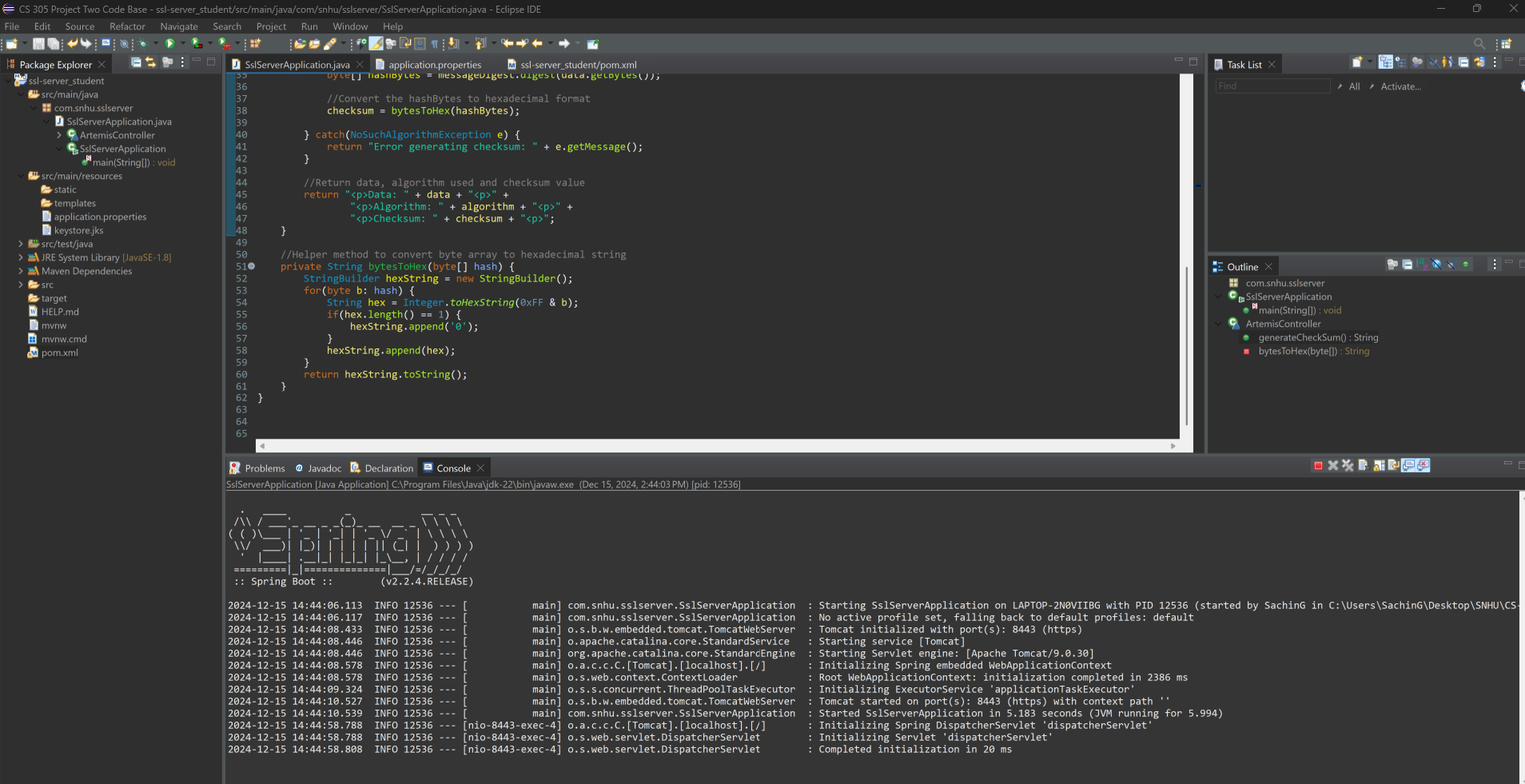
Insert screenshots below of the refactored code executed without errors and the dependency-check report.





## Functional Testing

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



## Summary

The code has been refactored and it includes the secure checksum generation endpoint “/hash” using the SHA-256. This ensures the data integrity and secure communication. It also has the secure HTTPS -enabled communication set up with a self-signed SSL certificate that helps protect data transmission and interception. The code has been validated against known vulnerabilities using the OWASP dependency-check to ensure no new risks has been introduced.

The process of adding layers of security includes the integrated SHA-256 checksum functionality for data integrity and secure communication, HTTPS enabled using a self-signed certification and performing static testing with the OWASP dependency-check to identify the vulnerabilities.

## Industry Standard Best Practices

In this project, I’ve applied the industry standard best practices to mitigate vulnerabilities. Encryption has been done using SHA-256 for secure checksum generation. HTTPS has been enabled with self-signed certificate to ensure encrypted communication. Static testing has ben done using OWASP dependency-check to identify and resolve security vulnerabilities in dependencies. This definitely adds value to the company because it enhances the software’s resilience against attacks, protects the sensitive data and because of these, it’ll create a better reputation for Artemis Financial.