****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_heading=h.vdy1jqj4uyg2)

[**Client 3**](#_heading=h.qgesjkuq8wvk)

[**Instructions 3**](#_heading=h.zytcuibai2)

[**Developer 4**](#_heading=h.5202eflpolme)

[**1. Algorithm Cipher 4**](#_heading=h.wcum38po5ugf)

[**2. Certificate Generation 4**](#_heading=h.hv4y15oummeu)

[**3. Deploy Cipher 4**](#_heading=h.7qra4pit03zc)

[**4. Secure Communications 4**](#_heading=h.22d4qo51flpr)

[**5. Secondary Testing 4**](#_heading=h.dxy0z7nxcr60)

[**6. Functional Testing 4**](#_heading=h.u3uyw5pd7hdf)

[**7. Summary 4**](#_heading=h.hgyfizqd0t3k)

[**8. Industry Standard Best Practices 4**](#_heading=h.jsltdiubzuvn)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **10/26/2025** | **Neema Taghipour** |  |

## 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

Neema Taghipour

## Algorithm Cipher

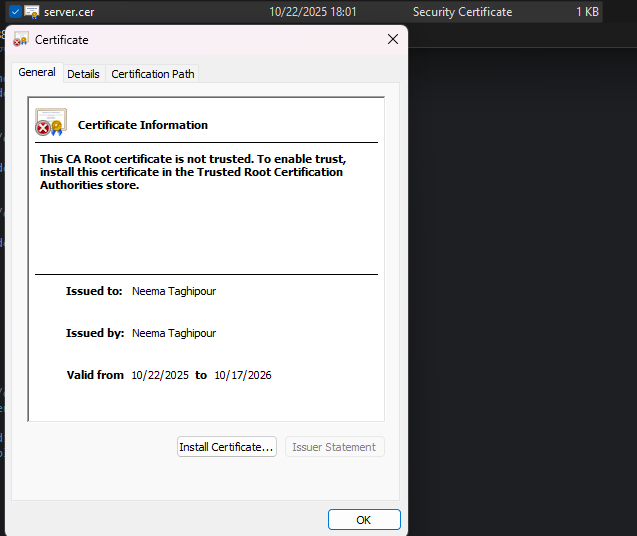
The algorithm I selected was the SHA-256 algorithm. This algorithm is a cryptographic hash function that transforms any input into a fixed 256-bit hash value. Since it is a one-way process, it allows for the secure encryption of valuable data.

The SHA-256 Algorithm is named after its specific 256-bit hash output encryption that allows it to be secure. If even a single bit in the input is changed the output is completely different. This ensures that the financial data of Artemis Financial is kept secure even if an attacker has partial-information.

Unlike typical RSA or AES algorithms, the SHA-256 algorithm does not use any encryption keys. Instead, the SHA-256 provides a fixed signature that represents the original data.

The SHA-256 is backed by the U.S. National Security Agency and was designed to replace older algorithms in the SHA iterations. Since the SHA-256 algorithm has been developed, it has quickly become an industry staple and is used for cryptographic hashing in a wide-range of applications. Although it was developed in 2001, it remains cryptographically secure and still is used throughout a wide-range of industries.

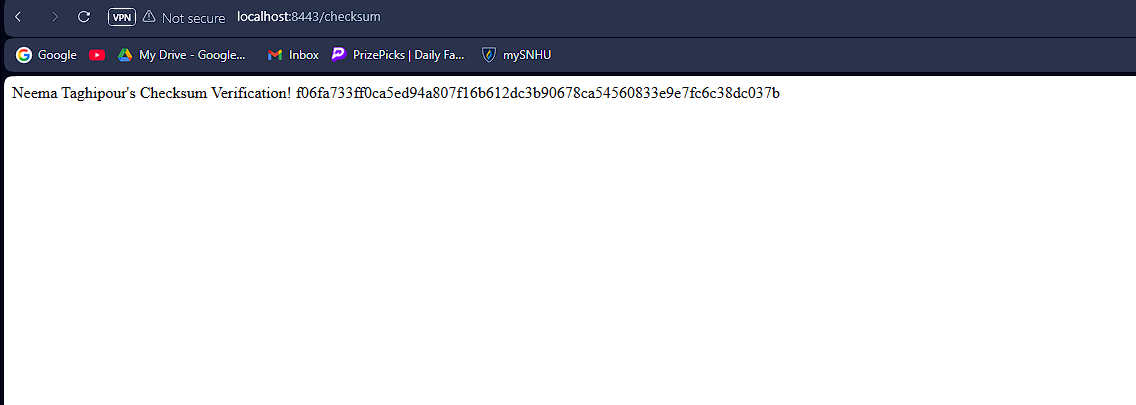
## Certificate Generation



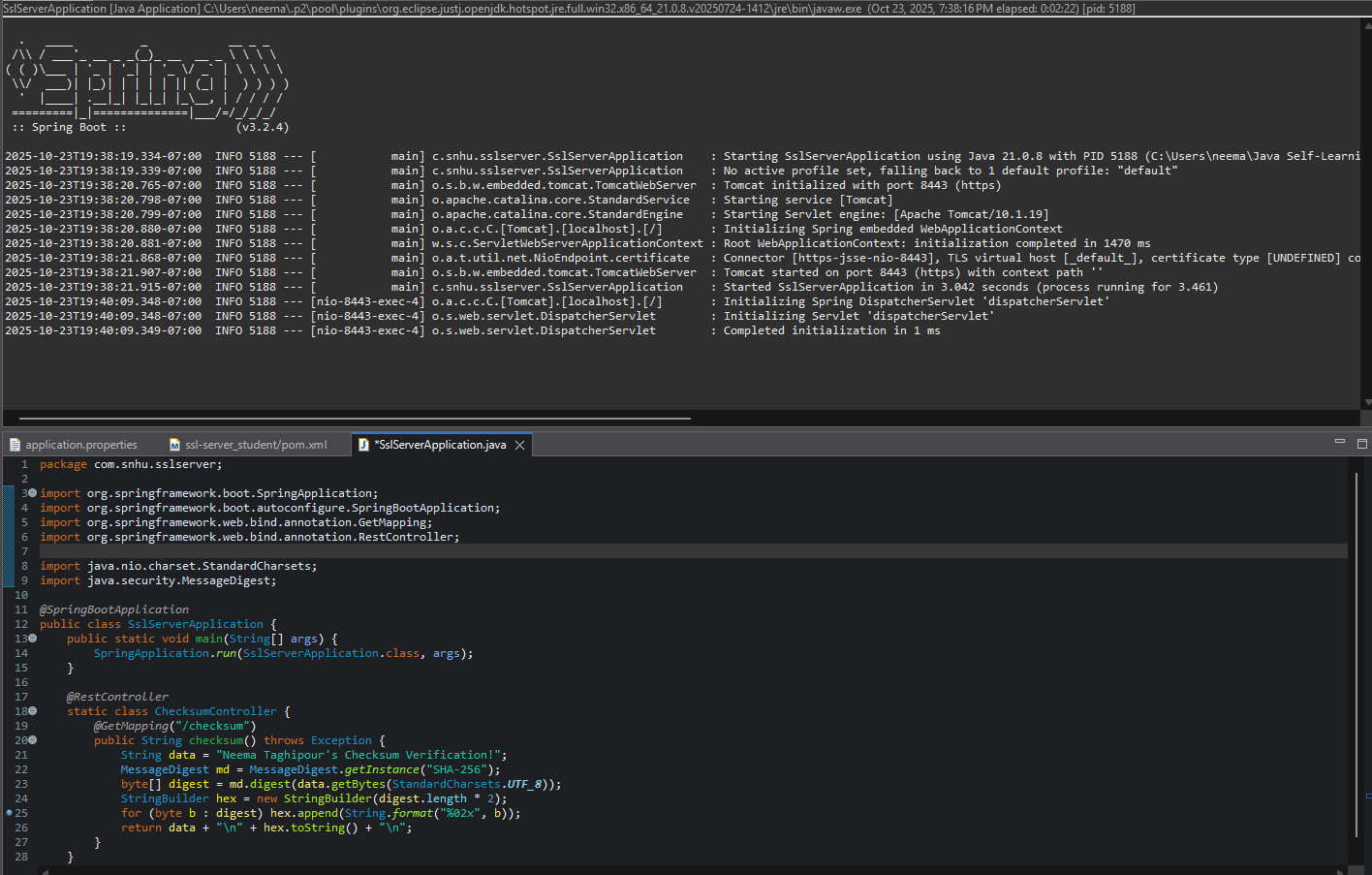
## Deploy Cipher

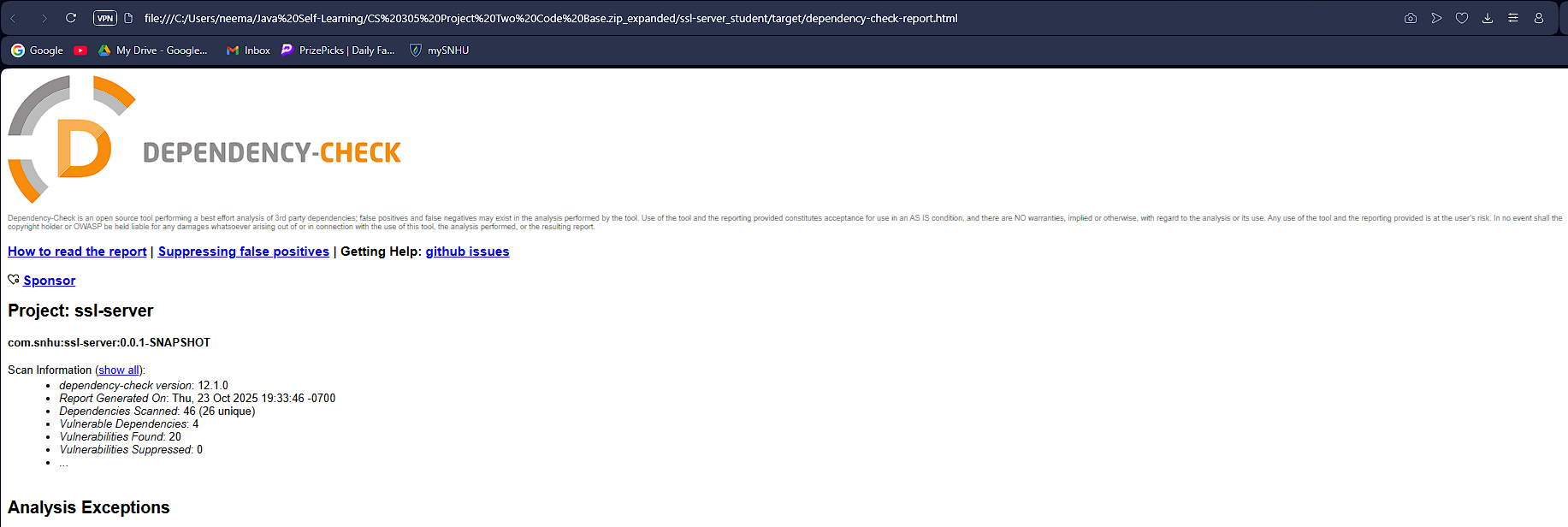


## Secure Communications

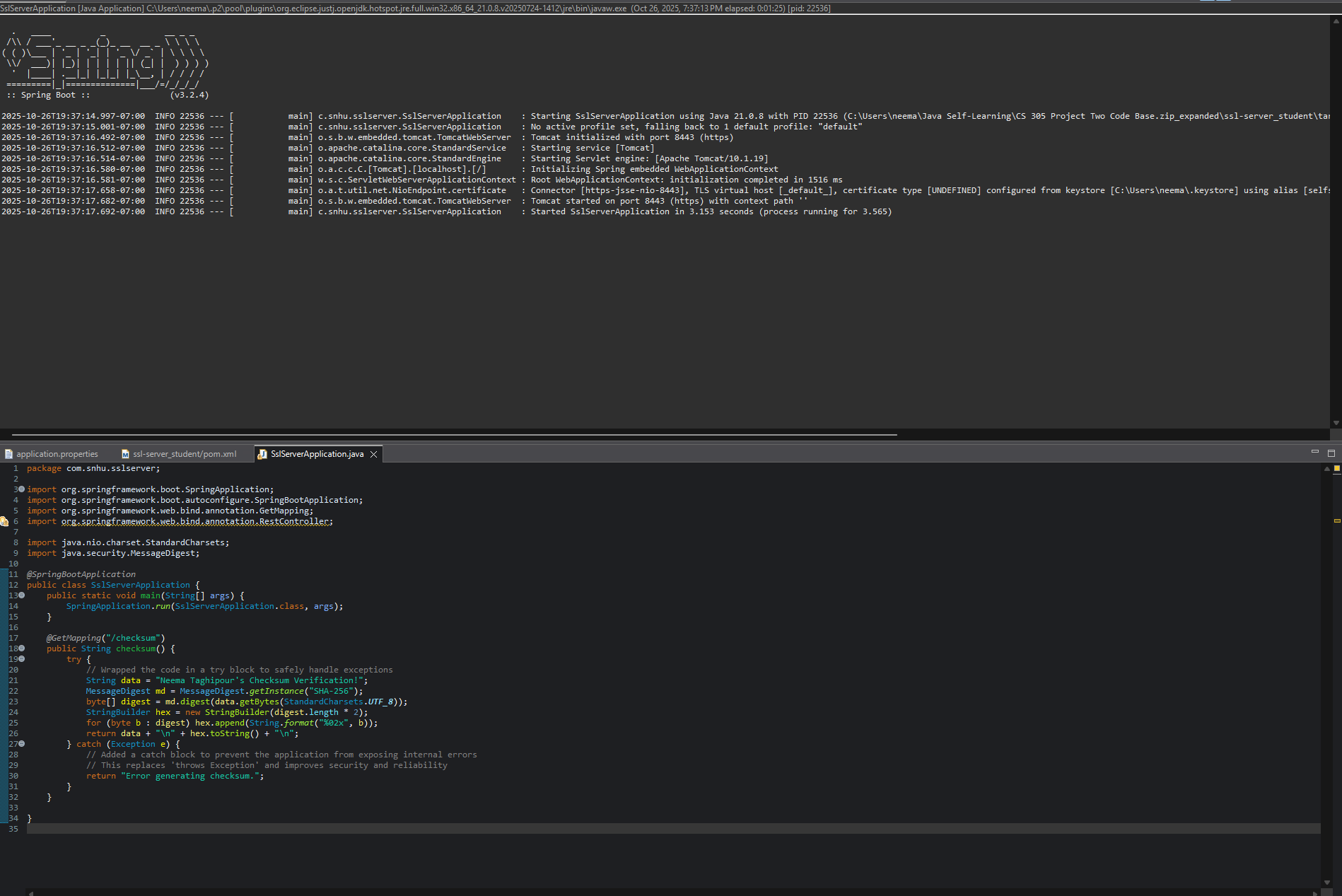


## Secondary Testing





## Functional Testing



## Summary

The edits I have made to the refracted code decreased the vulnerabilities that were present in the application. From the diagram, the main areas I focused on improving were error and exception management. Originally the checksum function used an error declaration that risked internal system information. By replacing the checksum method with a try/catch method, this vulnerability was easily resolved.

My specific process for adding layers of security started by a manual review of the Vulnerability Assessment Process Flow Diagram. Then, I proceeded to review the application's code and structure. I updated the code to match modern industry standards and ensured the application could properly follow the Software Development Life Cycle.

## Industry Standard Best Practices

I followed industry standard best practices to maintain the software application’s security by deploying a cryptographic hashing algorithm that aligns with modern-day secure coding standards. The SHA-256 algorithm is a secure algorithm that meets a wide-range of cryptographic criteria and allows for the safe encryption of valuable information.

Following industry standards is essential to this application because it is meant to be deployed on an international basis to hold extremely sensitive consumer financial information. If any of the information were to be breached, the company would suffer massive consumer losses and would likely never be able to recover as a staple in the industry. Adhering to the best practices allow for both the company and the consumers of the product to safely use the product they believe in.