****

# 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** | **2/22/25** | **Colin Timko** |  |

## 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

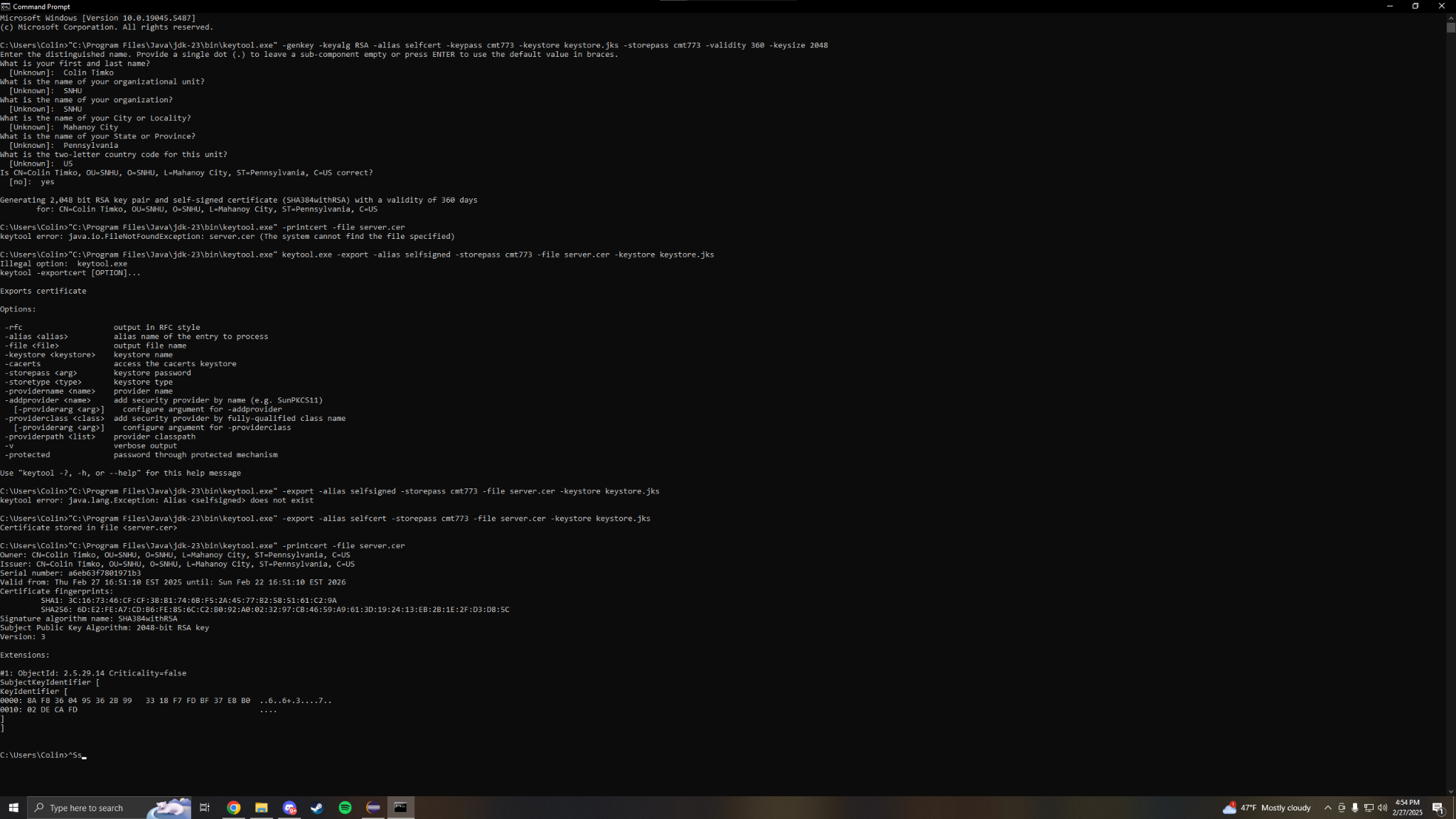
Colin Timko

## Algorithm Cipher

The cipher that is recommended for Artemis Financial is Advanced Encryption Standard (AES). AES is good because it provides a significant amount of protection especially against brute force attacks with either 128, 192, or 256 key sizes. AES puts data into 128 bit blocks and encrypts them separately. It uses the same key for both encryption and decryption and uses random numbers in order to create these keys. It is important to handle these keys carefully as poor implementation of AES is one of the possible issues with this cipher. AES was developed in 2001 and was replacing DES and is now used by many government agencies and is one of if not the most popular cipher used today.

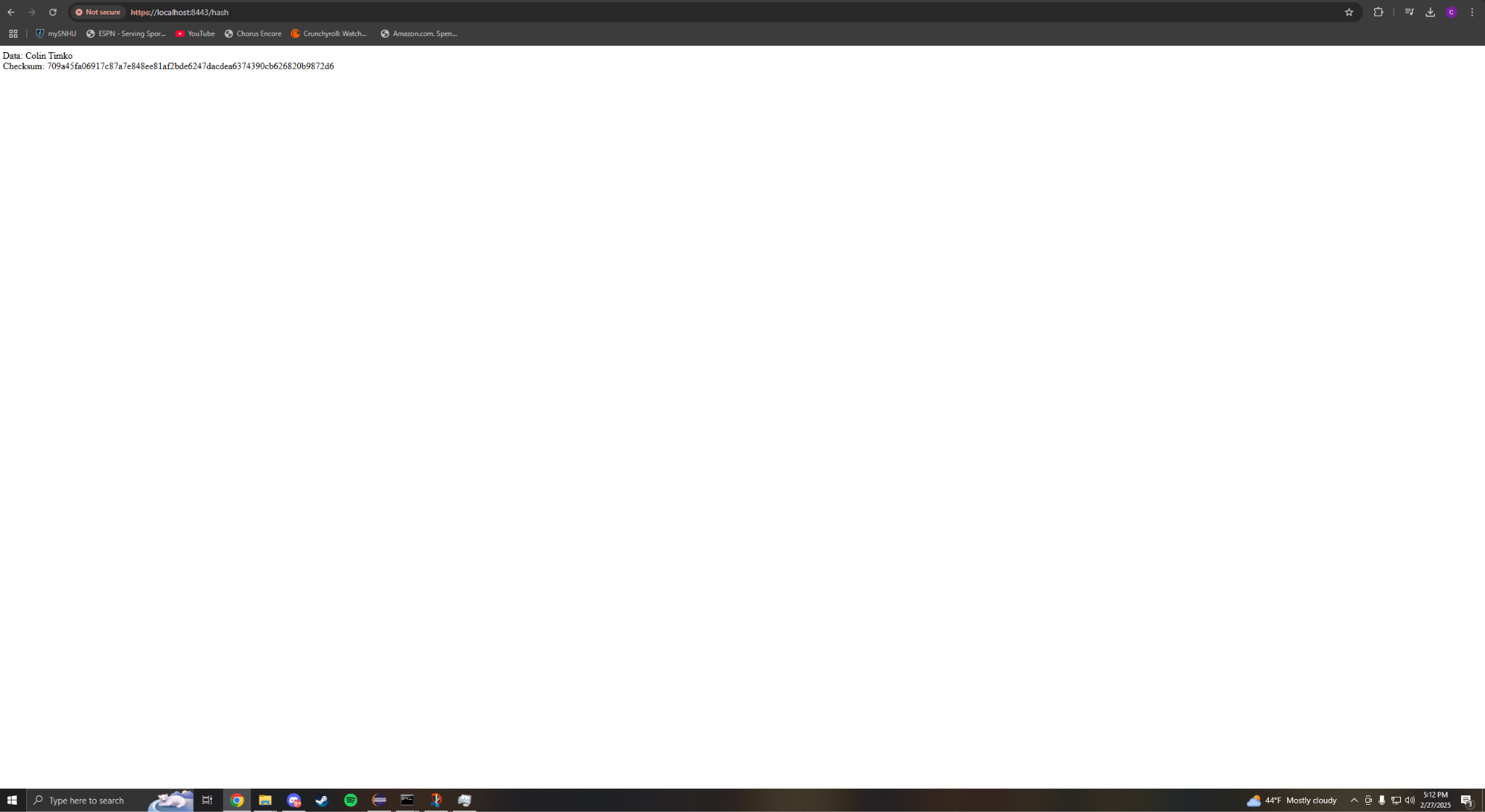
## Certificate Generation

Insert a screenshot below of the CER file.



## Deploy Cipher

Insert a screenshot below of the checksum verification.



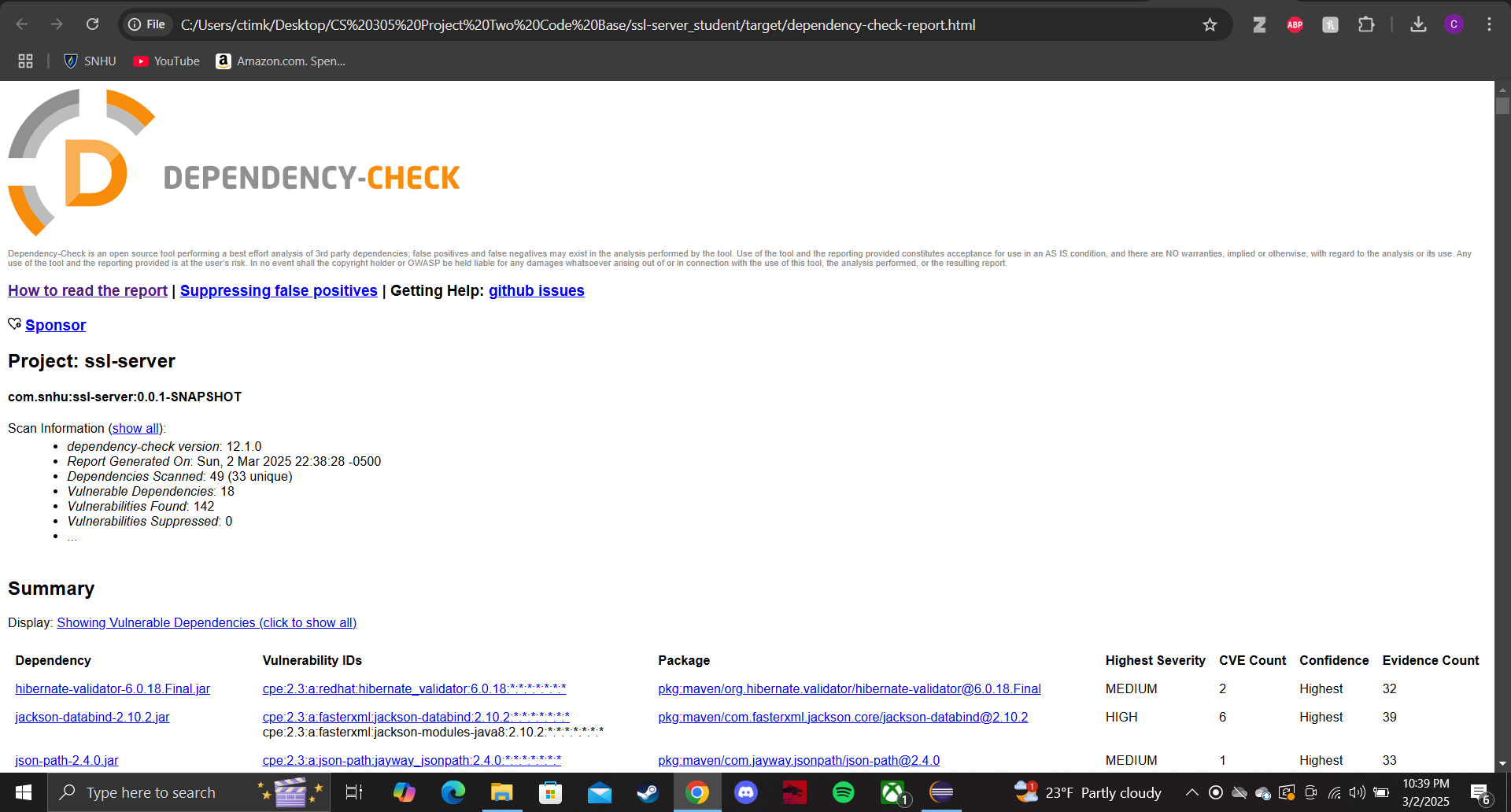
## Secure Communications

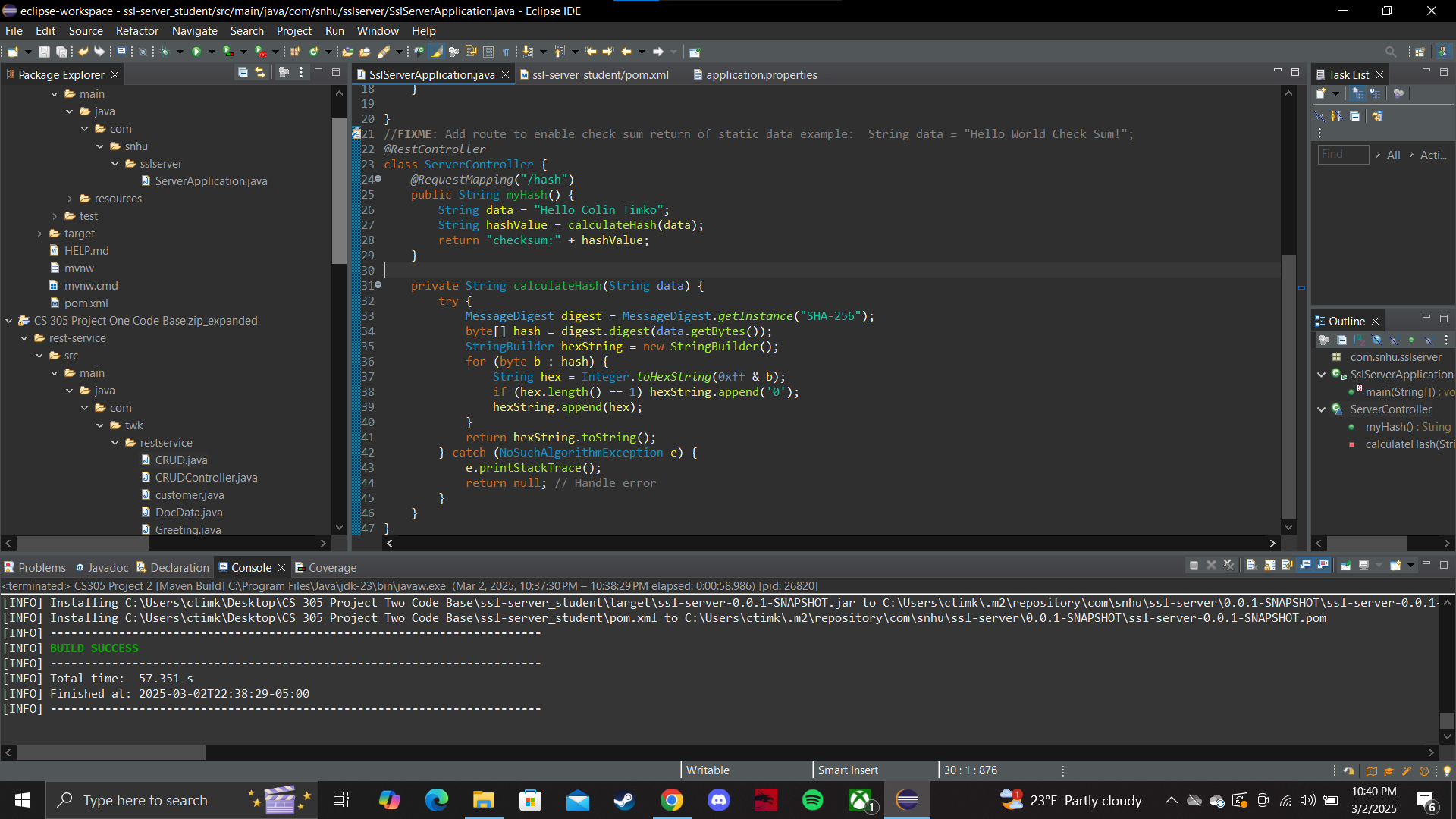
Insert a screenshot below of the web browser that shows a secure webpage.

[Insert screenshots here.]

## Secondary Testing

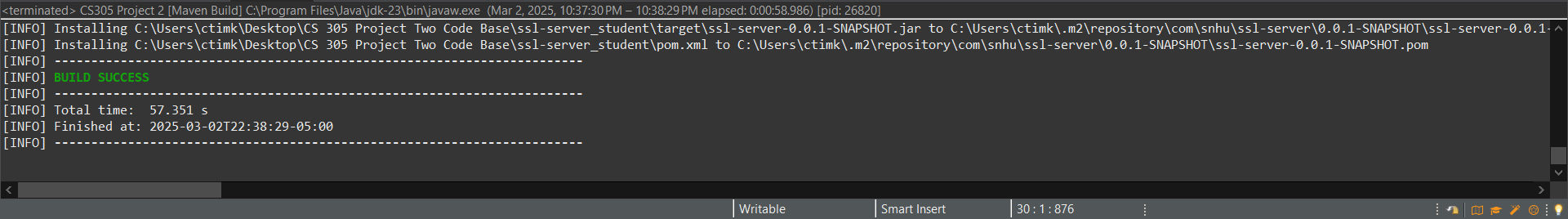
Insert screenshots below of the refactored code executed without errors and the dependency-check report.





## Functional Testing

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



## Summary

In the code base it is important to have good security. One example of security I implemented from the vulnerability assessment process flow diagram was error handling. I implemented a way to return null if the code does not execute properly which is important to make sure that errors give the correct information and also does not reveal too much to the user that is unnecessary. Another example is using the industry standard coding to make sure that the code is secure, easy to understand and fix, and works as intended. Cryptography is also important because we want to make sure that we are encrypting the data that is generated to avoid any type of threat actor from stealing data.

## Industry Standard Best Practices

Using industry standard practices is super important because it can make it easier to debug and fix possible errors and it can also add layers of security if done right. If an issue arises with the code base using best practices makes it easier for someone within the company to look at the code and spot vulnerabilities and furthermore fix them.