****

# 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** | **4/18/2024** | **Dakota Wolfe** |  |

## Client



## Instructions

Submit these completed practices for a 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

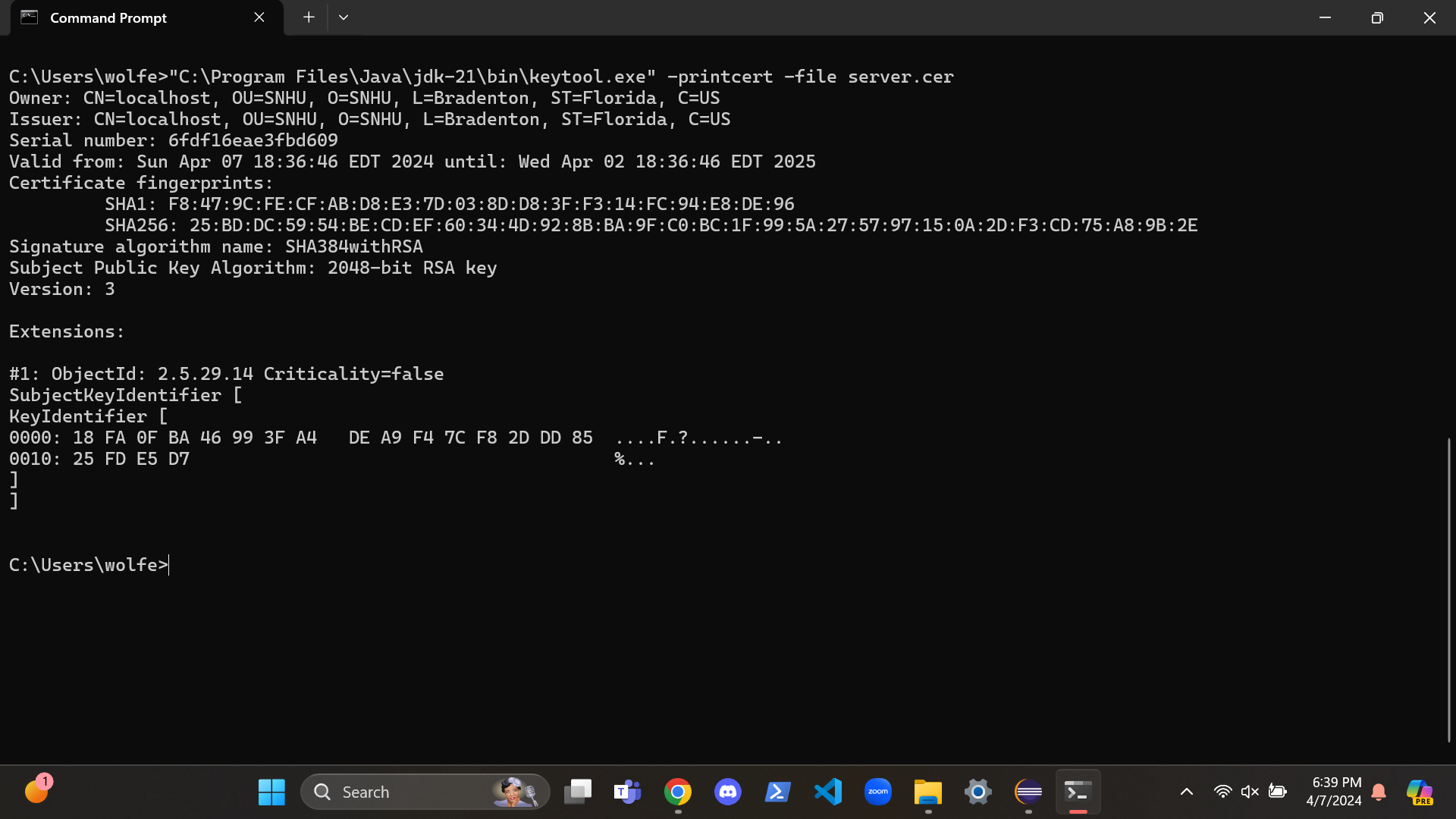
Dakota Wolfe

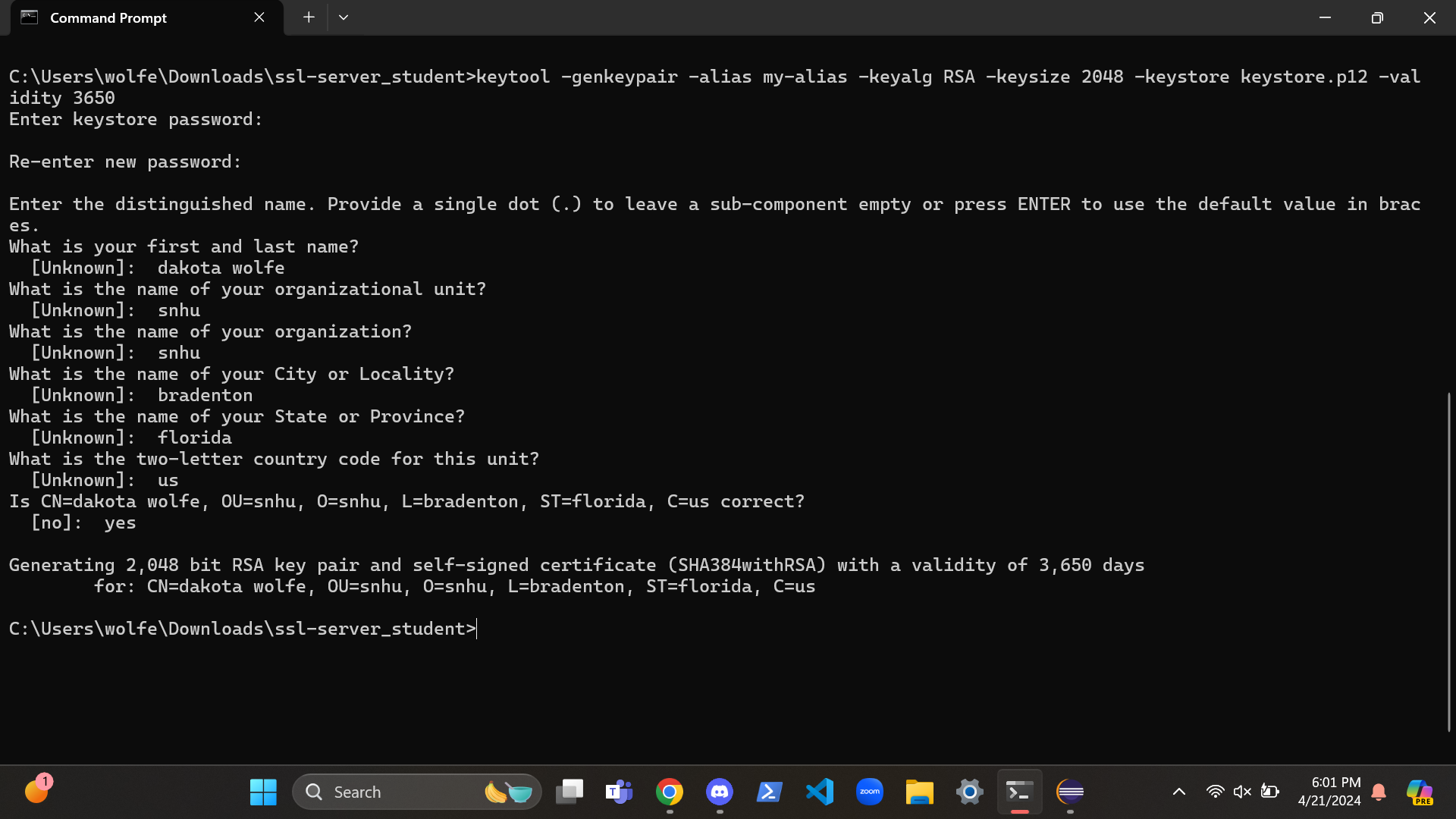
## Algorithm Cipher

Artemis Financial should use AES (Advanced Encryption Standard) as their algorithm cipher. The Federal Information Processing Standards Publication 197 details AES as, “...a FIPS-approved cryptographic algorithm that can be used to protect electronic data …a symmetric block cipher that can encrypt and decrypt information”. The usage of AES would center around the encryption of Artemis Financial’s archive files. Files will be encrypted with AES using an encryption key. Authorized users will then access the data using the corresponding decryption key. The purpose of this cipher’s hash functions are to maintain the confidentiality of the data involved. AES works with bit levels of 128, 192, or 256. AES also uses the same key for encryption and decryption, better known as symmetric encryption. AES replaced DES in 2001, and has since been the encryption standard throughout the tech industry.

## Certificate Generation

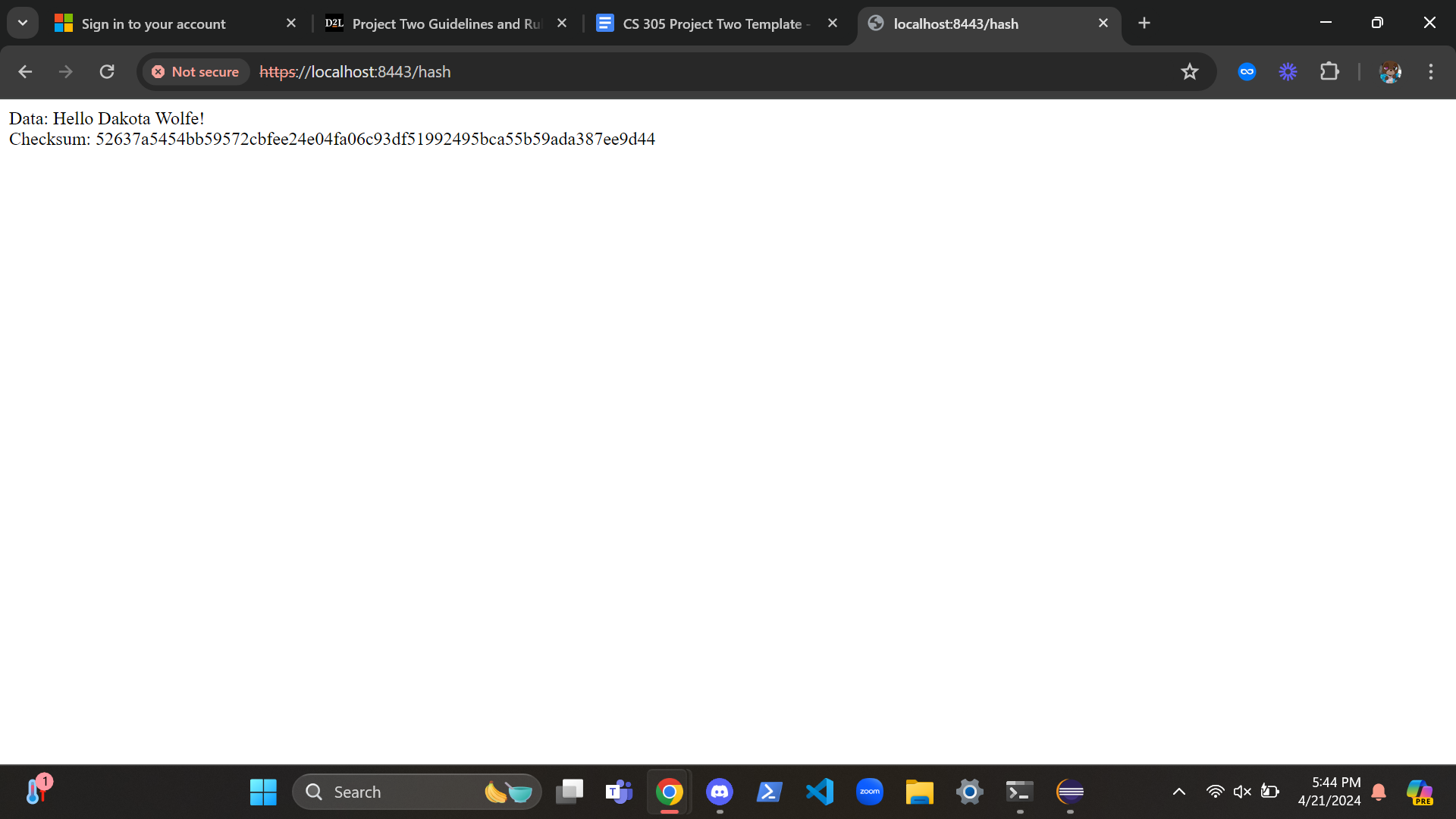
Insert a screenshot below of the CER file.

****

****

## Deploy Cipher

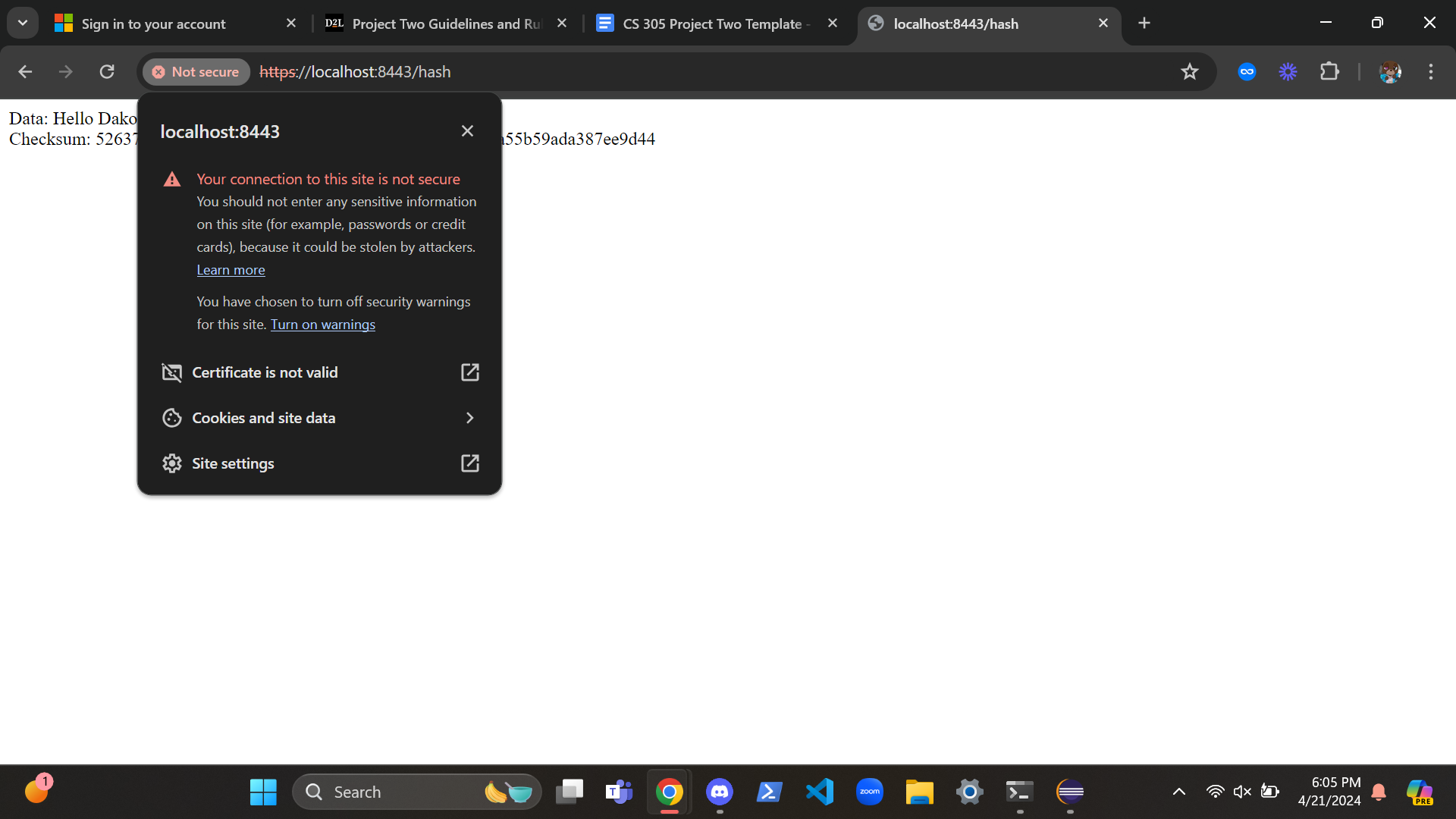
Insert a screenshot below of the checksum verification.



## Secure Communications

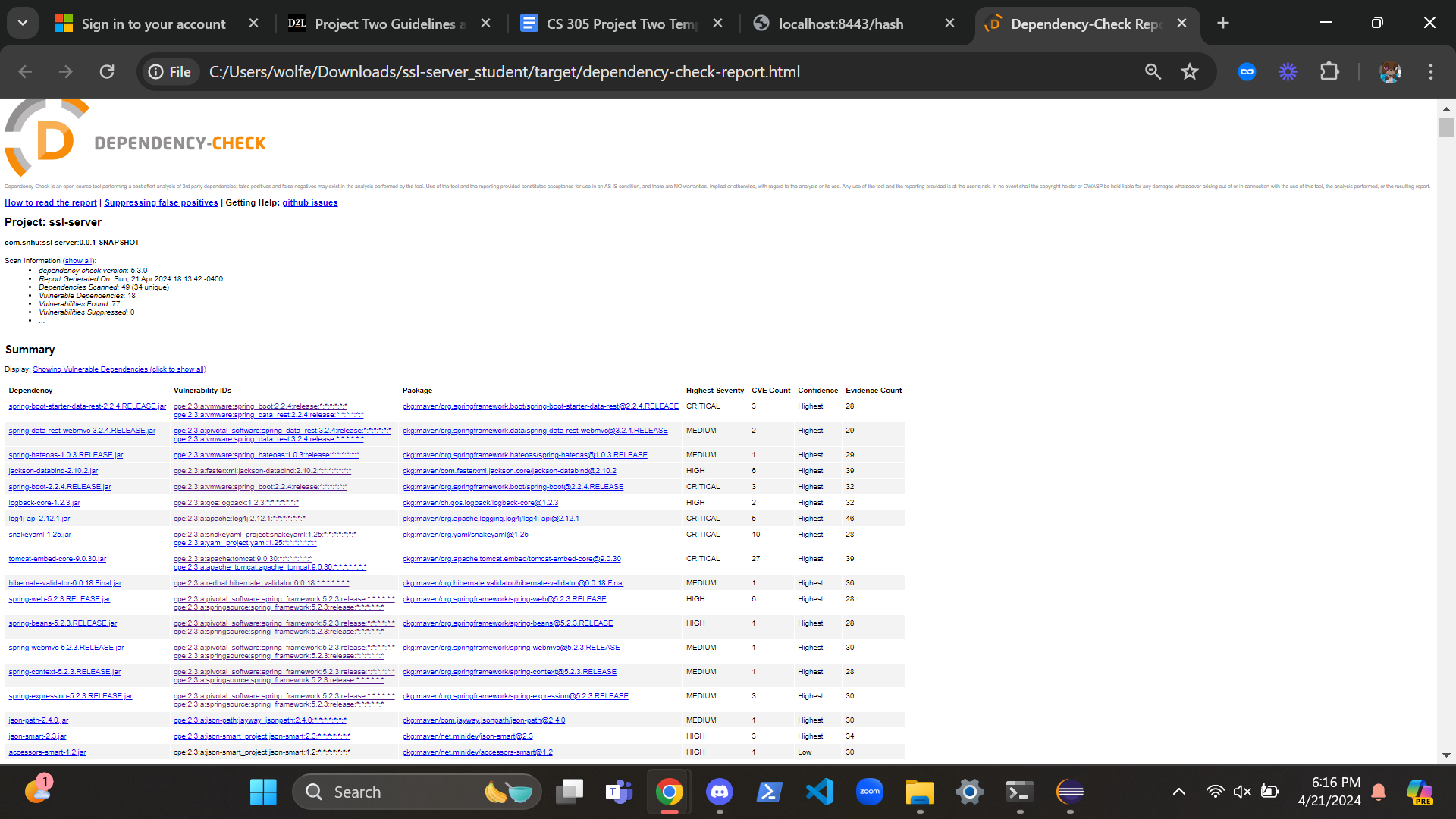
Insert a screenshot below of the web browser that shows a secure webpage.

I enabled HTTPS but the web browser does not trust my certificate.



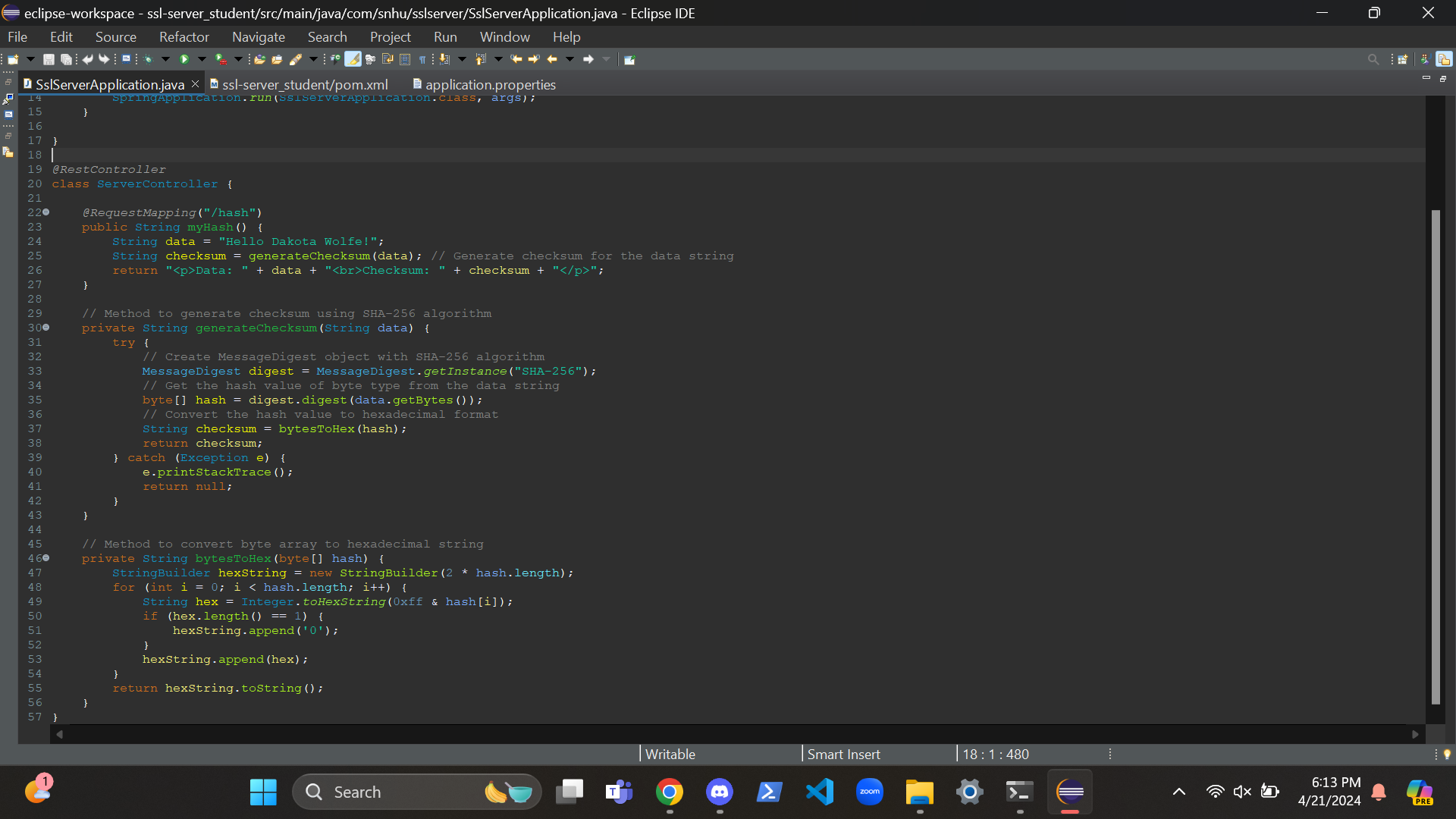
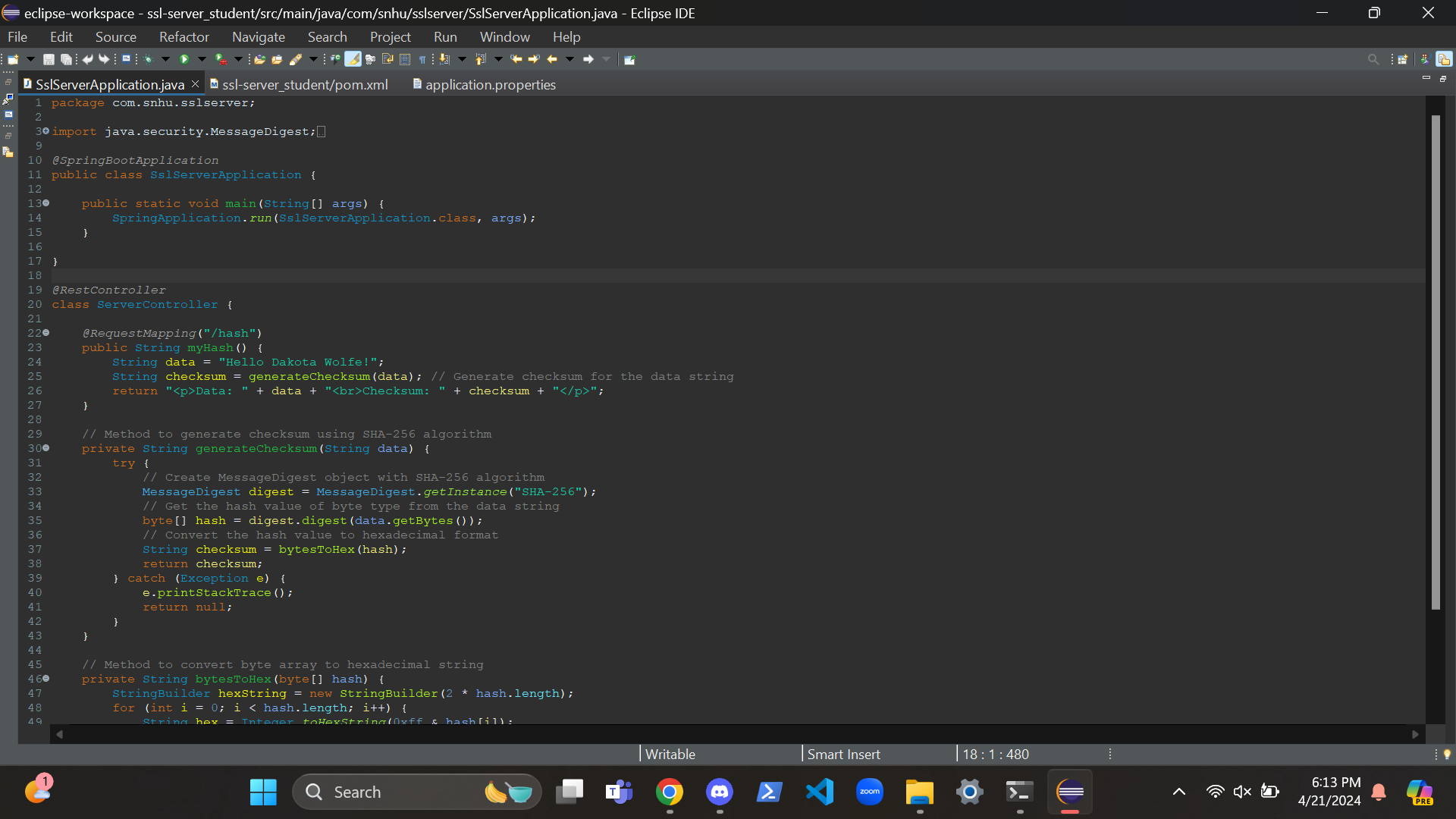
## Secondary Testing

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 modified to fall in line with security testing protocols. One addition to the code is the use of SHA-256. SHA-256 is used alongside the generateChecksum() method to generate checksum data for the input. This code also utilizes HTTPS, which encrypts the communication between client and server. Another security benefit is the use of error handling. This prevents the app from crashing when encountering an error.

## Industry Standard Best Practices

This application follows industry standard best practices in a number of ways. The app shows proper encapsulation by separating different functions and classes. Another example of the code following RESTful API design through the use of annotations like @RequestMapping and @RestController. Using error handling to prevent the app from crashing is also in line with industry standards. Finally, the code is well-organized and commented on.