****

# 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** | **[Date]** | **[Your Name]** |  |

## 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

C.J. Cline

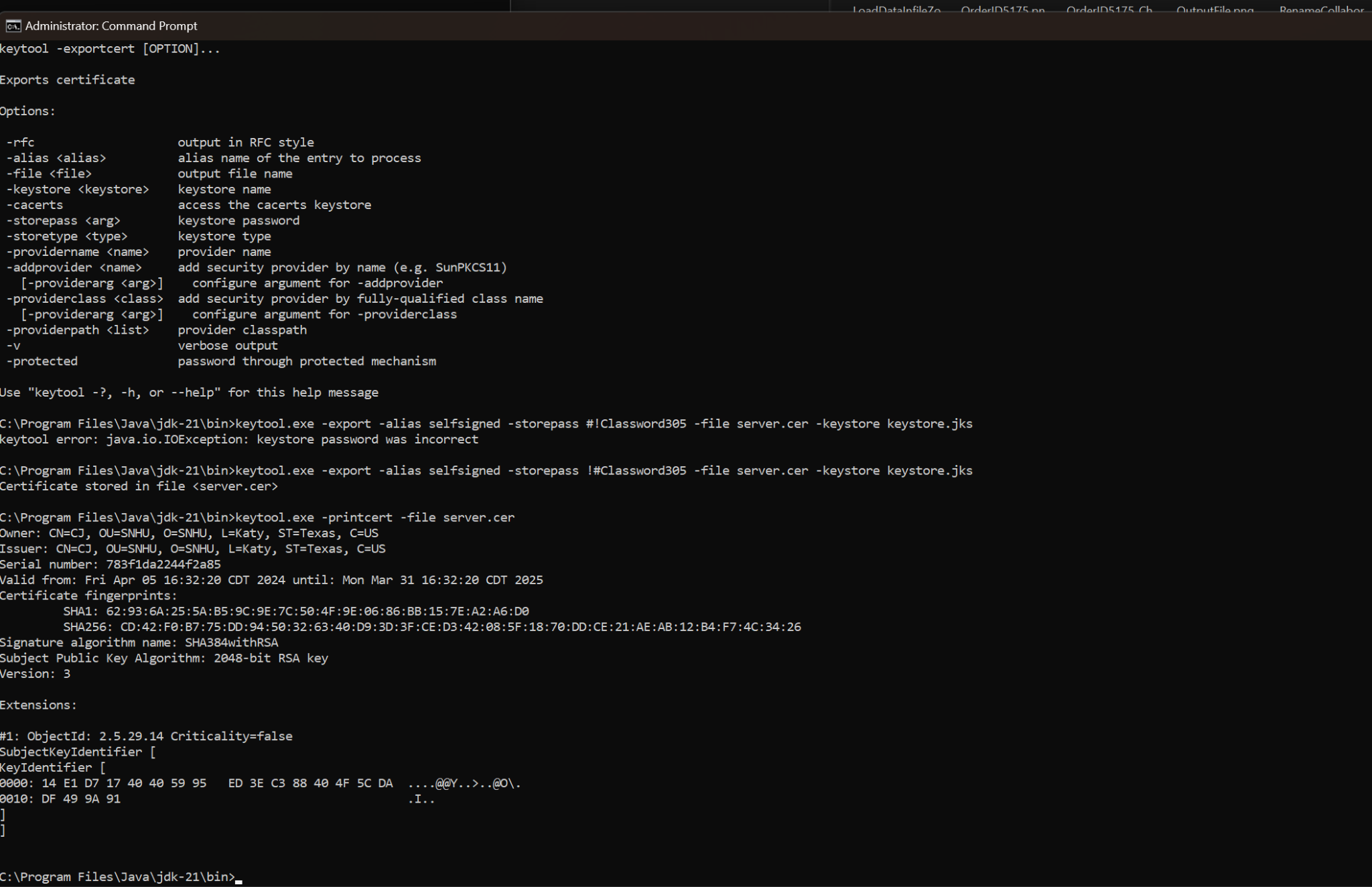
## Algorithm Cipher

I’ve chosen SHA-256, a cryptographic hash function published by the NIST. It's a published standard one-way encryption and to use over as part of an API, it allows for a program to be sent over https::// with an encryption that is difficult to decipher without the key.

It is created through the process of generating a random key of random numbers, then modifying the location of all items within the original message and then moving the location of the items in new first round of encryption within the message, then repeating the randomization process for 11 rounds until no individual character can be identified as a repeated.   
It's important to note that SHA is a 256-bit encryption. This is basically the size and the number of possible bit combinations per item as time passes the encryption method will need to use a larger size encryption, but this functions as the standard for now as with its predecessors which used smaller bit sizes such as MD5 (128 bits) as computers get faster at decoding it will always be necessary to increase the internal bit size and for more complex encryptions.

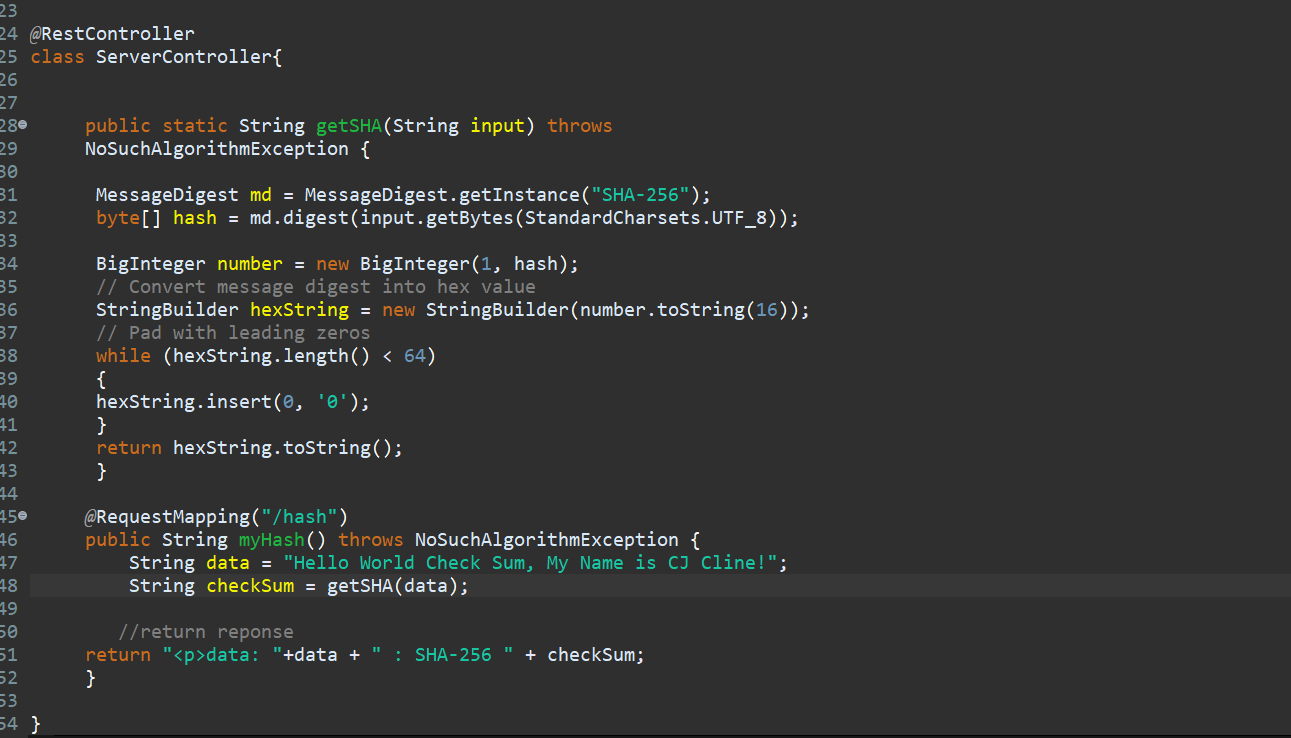
## Certificate Generation

Insert a screenshot below of the CER file.



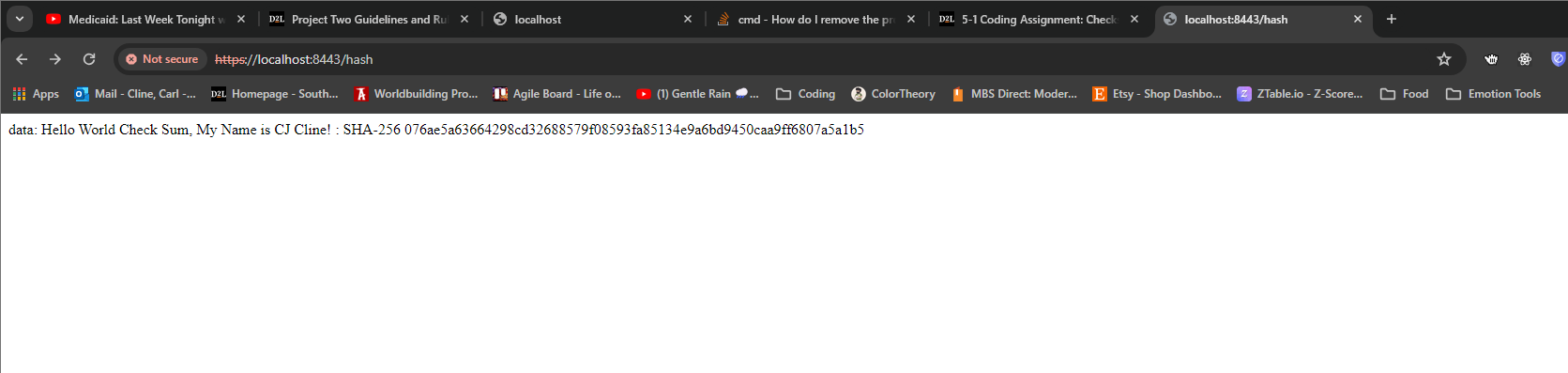
## Deploy Cipher

Insert a screenshot below of the checksum verification.



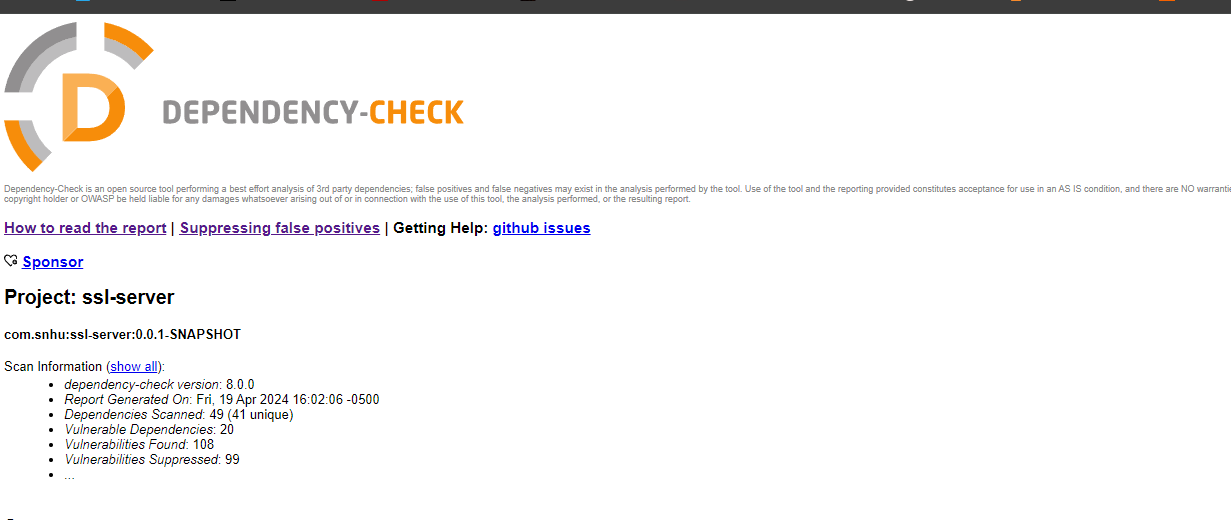
## Secure Communications

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

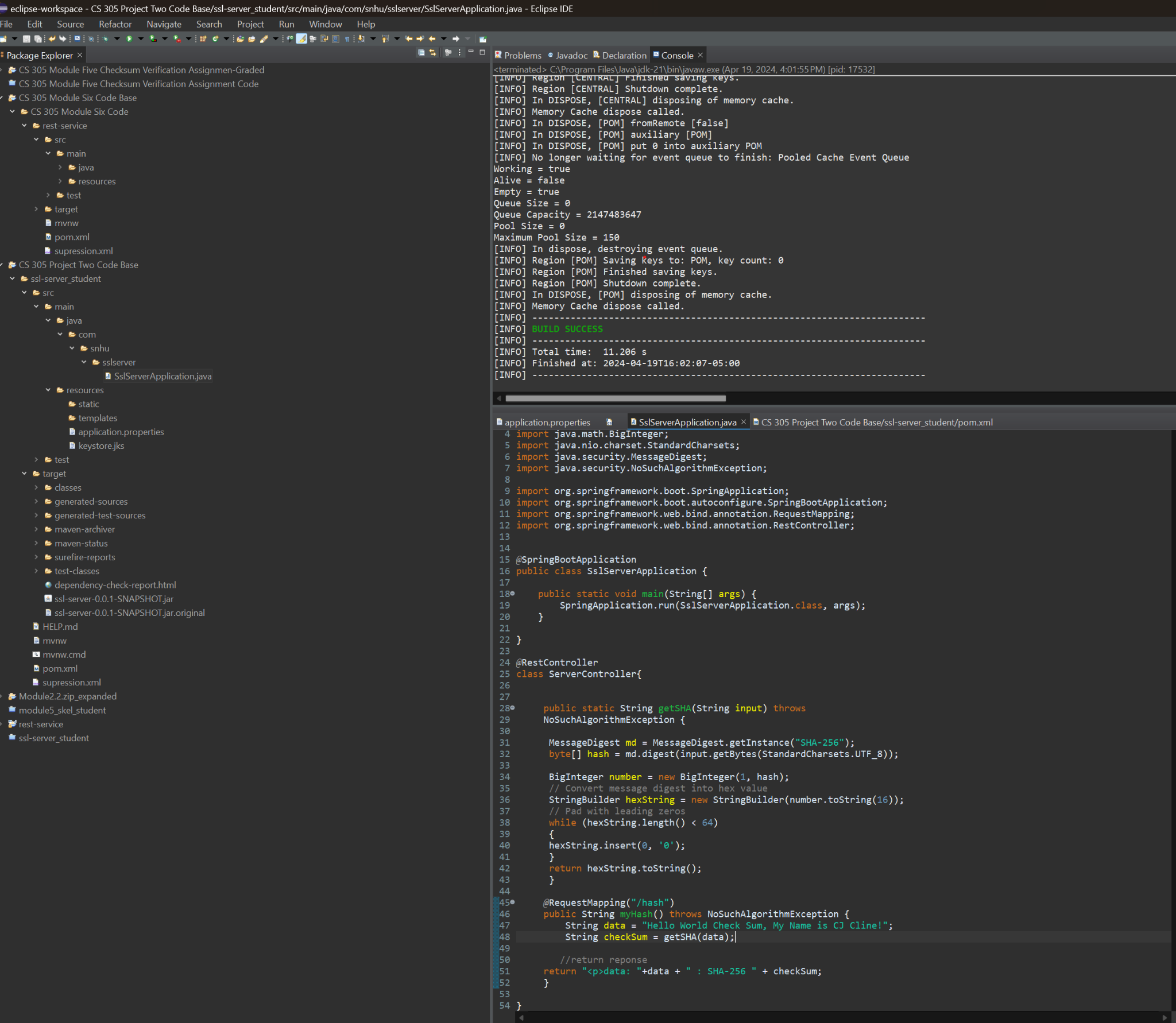


## Secondary Testing

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



## Functional Testing



## Summary

The code has been refactored to include encryption and certifications, certifications are designed to allow for both parties to ensure that they are speaking to their intended targets certifications allows for verification of by the passing of the public keys to intended parties. The encryption has been included so that if the transmission between users is compromised then the data will remain encrypted without either user's private key to decipher the code.

## Industry Standard Best Practices

Its important to secure your clients and customers information as both are vital to their trust with each other. Unintended security leaks could lead to businesses having damage to their reputation, or financial damages or financial business advantages being lost. While the customers are often just as much at risk private expenditures could be discovered as well as direct access to credit cards and other information that could lead to identify fraud and other disastrous outcomes.

It’s that everyone on the development team considers that security is a cornerstone to a long term satisfactory relationship between everyone involved.