****

# CS 305 Project Two

**Practices for Secure Software Report**

Table of Contents

[Document Revision History 3](#_Toc33111302)

[Client 3](#_Toc33111303)

[Instructions 3](#_Toc33111304)

[Developer 4](#_Toc33111305)

[1. Algorithm Cipher 4](#_Toc33111306)

[2. Certificate Generation 4](#_Toc33111307)

[3. Deploy Cipher 4](#_Toc33111308)

[4. Secure Communications 4](#_Toc33111309)

[5. Secondary Testing 4](#_Toc33111310)

[6. Functional Testing 5](#_Toc33111311)

[7. Summary 5](#_Toc33111312)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2/18/2021** | **Hunter Ewin** |  |

## Client



## Instructions

Deliver this completed Practices for Secure Software Report documenting your process for writing secure communications and refactoring code that complies with software security testing protocols.

Respond to the steps outlined below and replace the bracketed text with your findings in your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

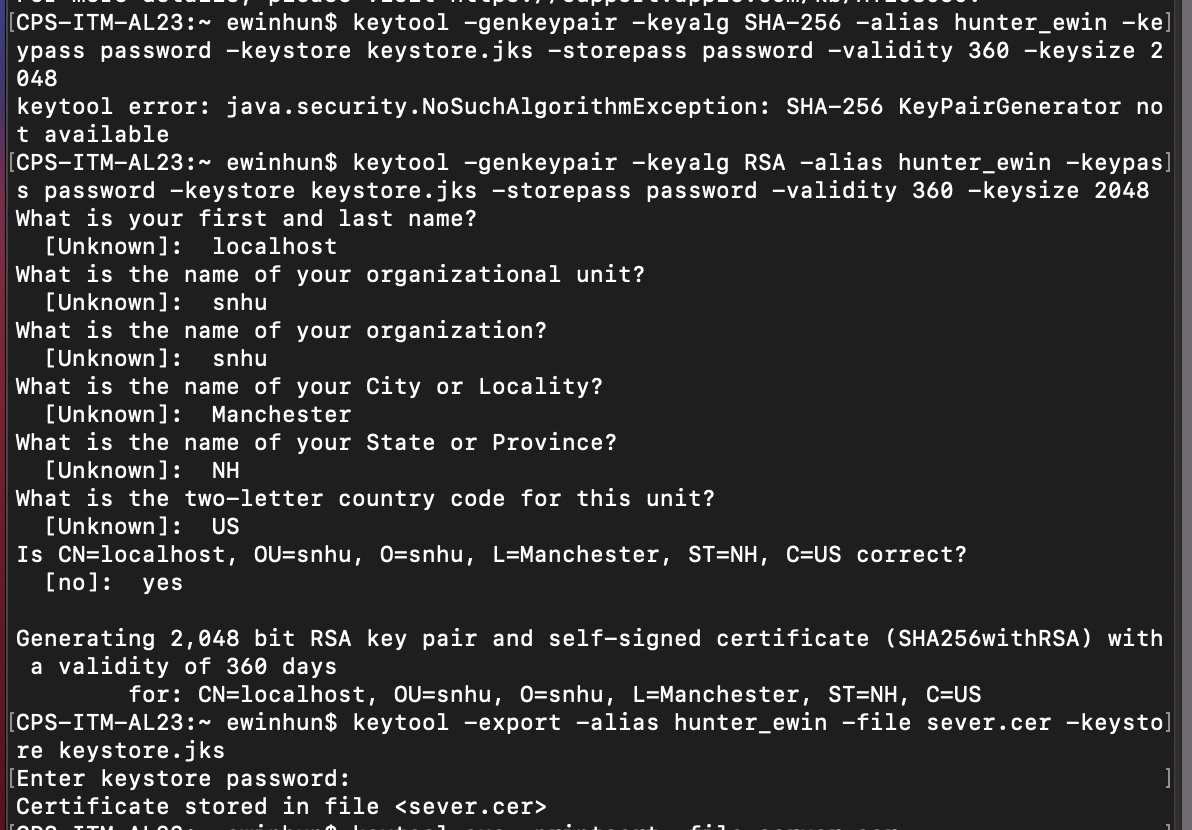
## Developer

Hunter Ewin

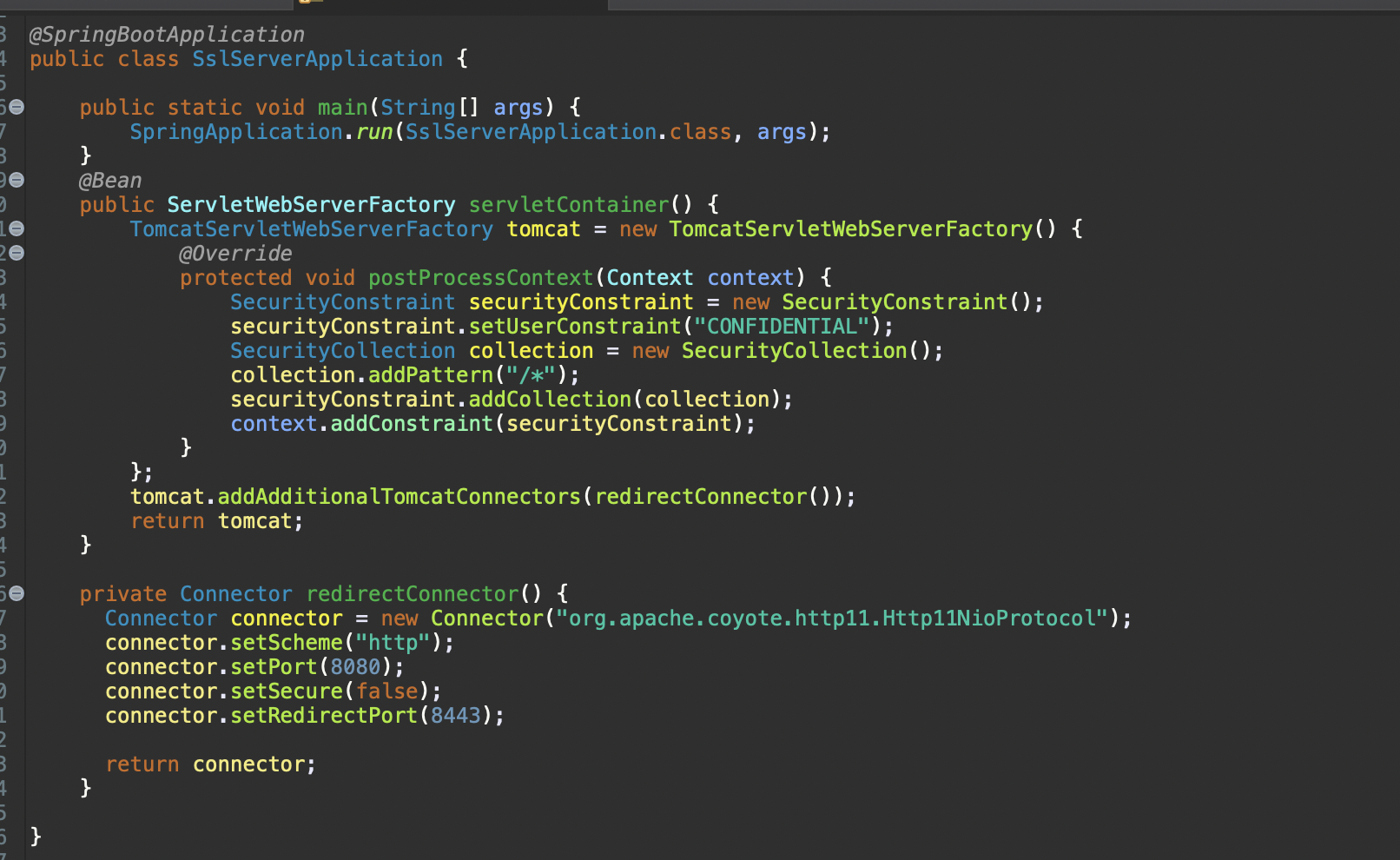
## 1. Algorithm Cipher

I used the SHA-256 algorithm. This SHA-256 will generate a unique 256-bit or 32 byte signature. So far, this algorithm has shown to be the most secure, and has yet to be hacked. Since this is a one way process, this will also make it difficult for any malicious users to hack it as well. There are many hashing algorithms out there, but this one has shown to have the most promise. The MD5 is a hshing function that was developed by the Chinese. It is a 128 bit output, but has shown to have many collisions. As stated above, the best algorithm would be the SHA-256 because of its high security.

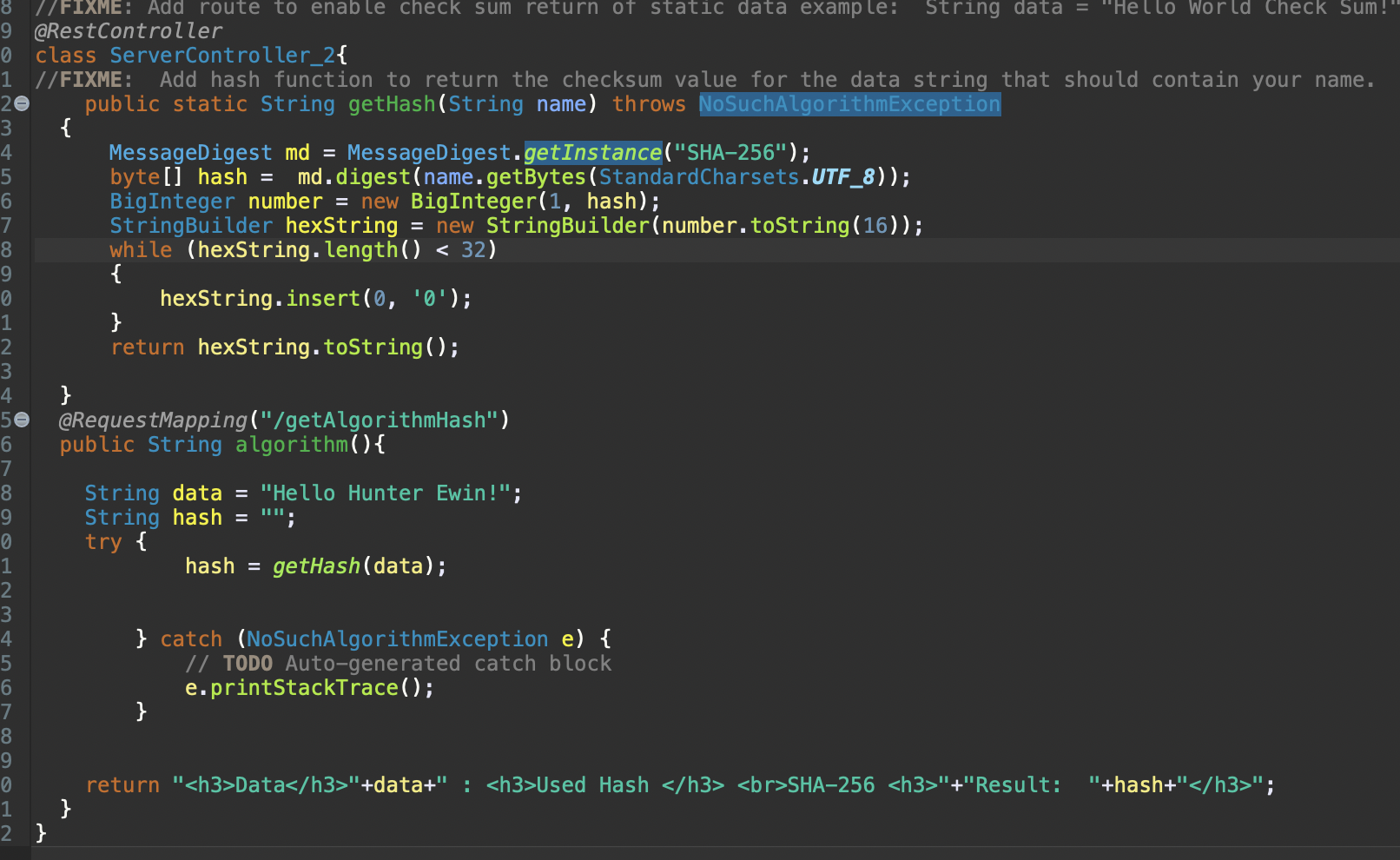
## 2. Certificate Generation



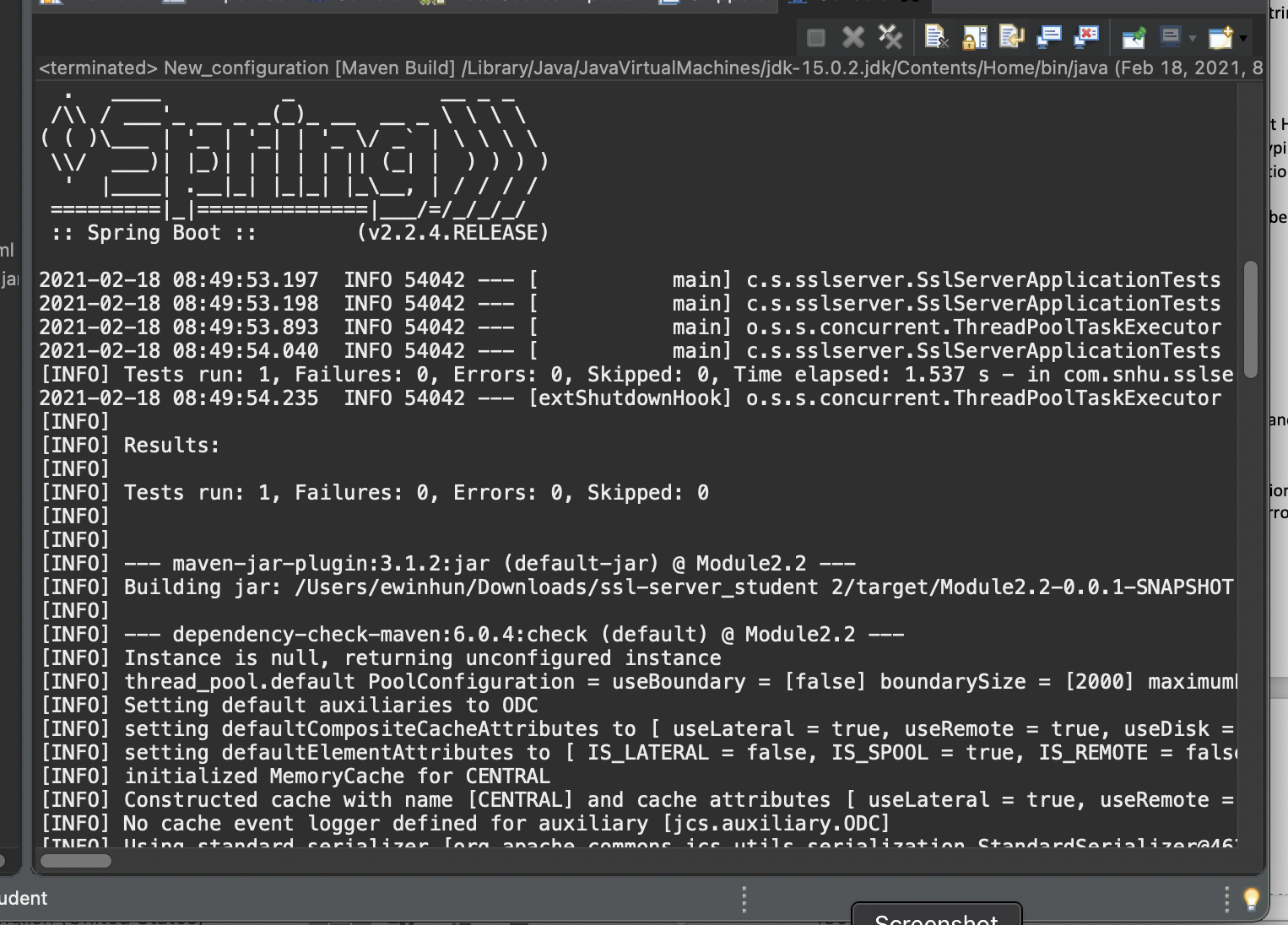
## 3. Deploy Cipher

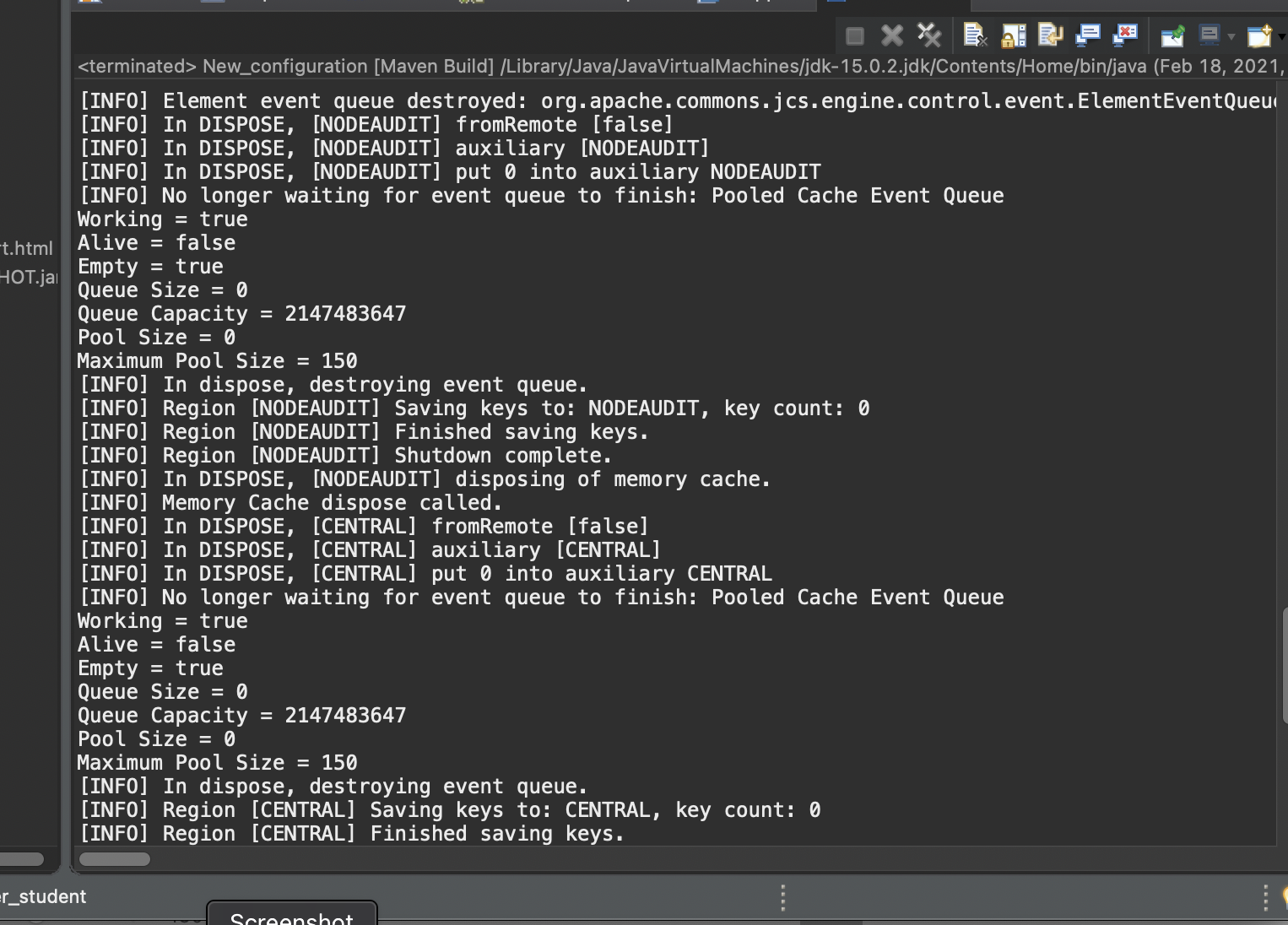


## 4. Secure Communications



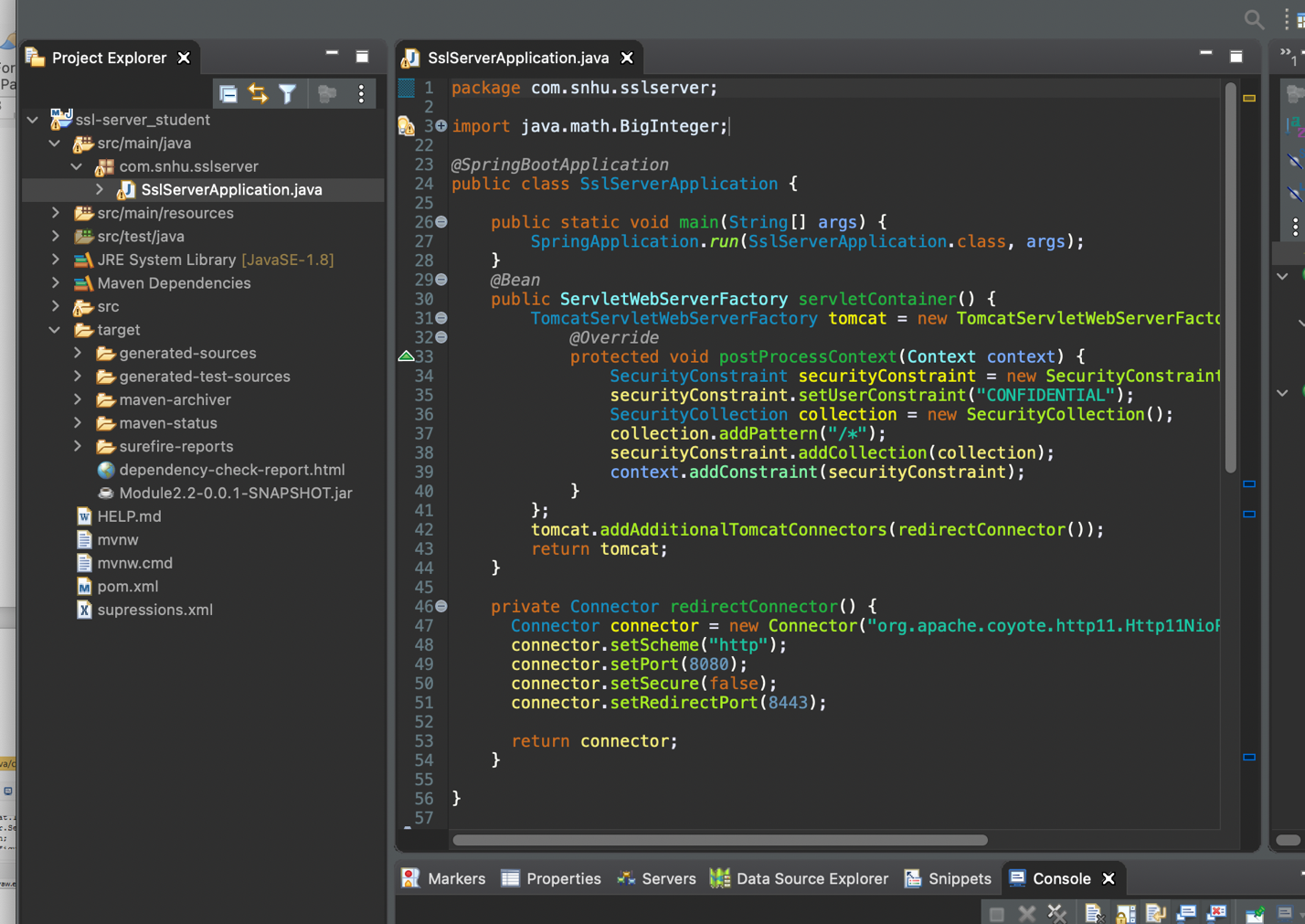
## 5. Secondary Testing







## 6. Functional Testing



## 7. Summary

I used the SHA-256 algorithm since it is a one-way process ensuring much better security. The data is therefore encrypted and sent to the user, and only users can be checked as a key. Any data that will produce the same code will be the text. I also added code to ensure the server was secure by adding in a config file that will generate a key with a certificate.