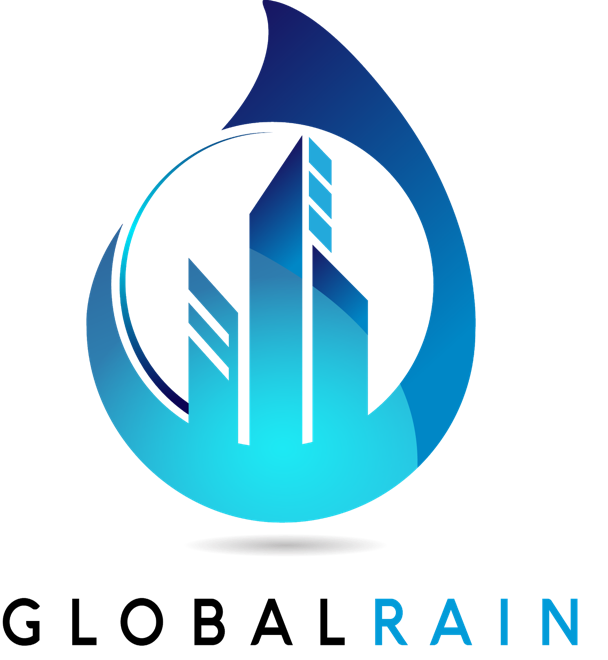
****

# CS 305 Project Two

**Practices for Secure Software Report**

**Table of Contents**

[Document Revision History 3](#_1fob9te)

[Client 3](#_3znysh7)

[Instructions 3](#_2et92p0)

[Developer 4](#_tyjcwt)

[1. Algorithm Cipher 4](#_3dy6vkm)

[2. Certificate Generation 4](#_1t3h5sf)

[3. Deploy Cipher 4](#_4d34og8)

[4. Secure Communications](#_2s8eyo1) 5

[5. Secondary Testing](#_17dp8vu) 6

[6. Functional Testing](#_3rdcrjn) 7

[7. Summary](#_26in1rg) 10

## Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| **1.0** | **Sunday Dec 13th, 2020** | **Timothy Crowell** |  |

## 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

Timothy Crowell

## 1. Algorithm Cipher

Determine an appropriate encryption algorithm cipher to deploy given the security vulnerabilities, justifying your reasoning. Be sure to address the following:

* Provide a brief, high-level overview of the encryption algorithm cipher.
* Discuss the hash functions and bit levels of the cipher.
* Explain the use of random numbers, symmetric vs non-symmetric keys, and so on.
* Describe the history and current state of encryption algorithms.

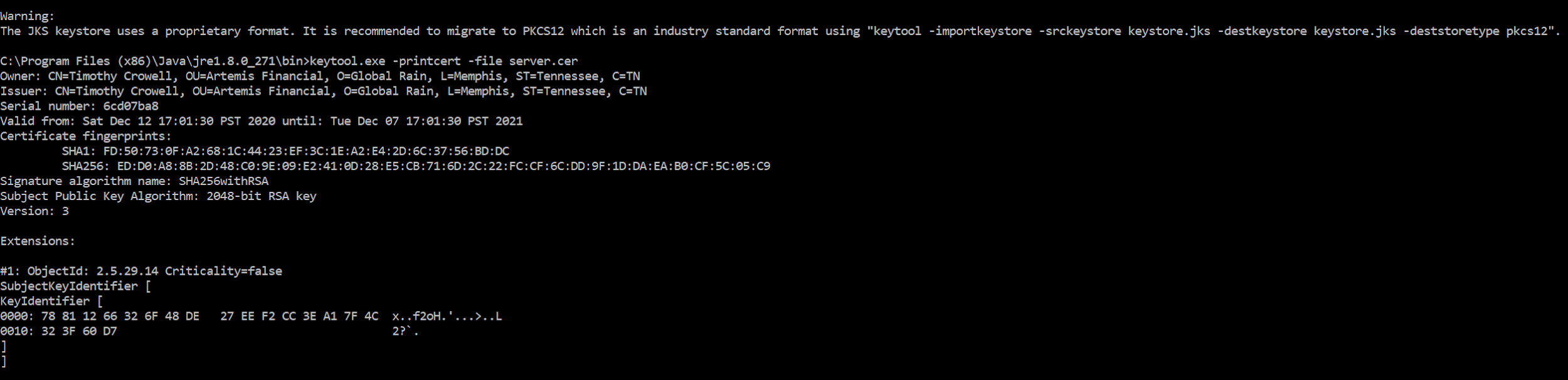
The best encryption algorithm cipher for our system is the RSA asymmetric cryptographic algorithm. RSA is a great choice for security because it is asymmetric, meaning assigns users two keys for encrypting and decrypting, a public key and a private key. Each unique customer of the system will have their own key and will be able to share messages directly with the server. The system will already have the users key information, providing quick and easy use. Hash values are used to sign messages with RSA encryption, ensuring that the recipient knows the sender is legitimate.

One of the first instances of machines using ciphers was the Enigma machine created by Arthur Scherbius during world war 1. This machine created a daily code that could be used to decrypt messages in secret. Today we use cryptography to encrypt messages we send online. There are many types of encryption algorithms such as RSA and AES, with various combinations of keys and encryption methods.

## 2. Certificate Generation

Generate appropriate self-signed certificates using the Java Keytool, which is used through the command line.

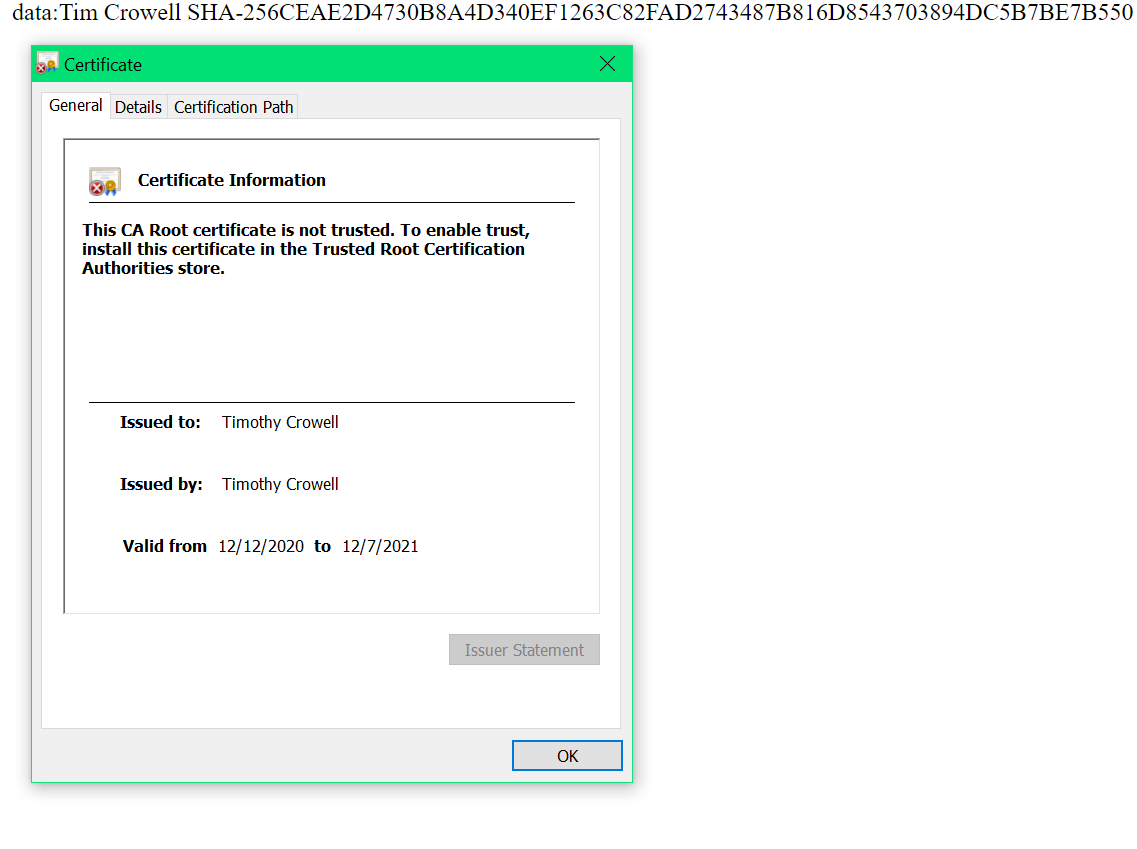
* To demonstrate that the keys were effectively generated, export your certificates (CER file) and submit a screenshot of the CER file below.



## 3. Deploy Cipher

Refactor the code and use security libraries to deploy and implement the encryption algorithm cipher to the software application. Verify this additional functionality with a checksum.

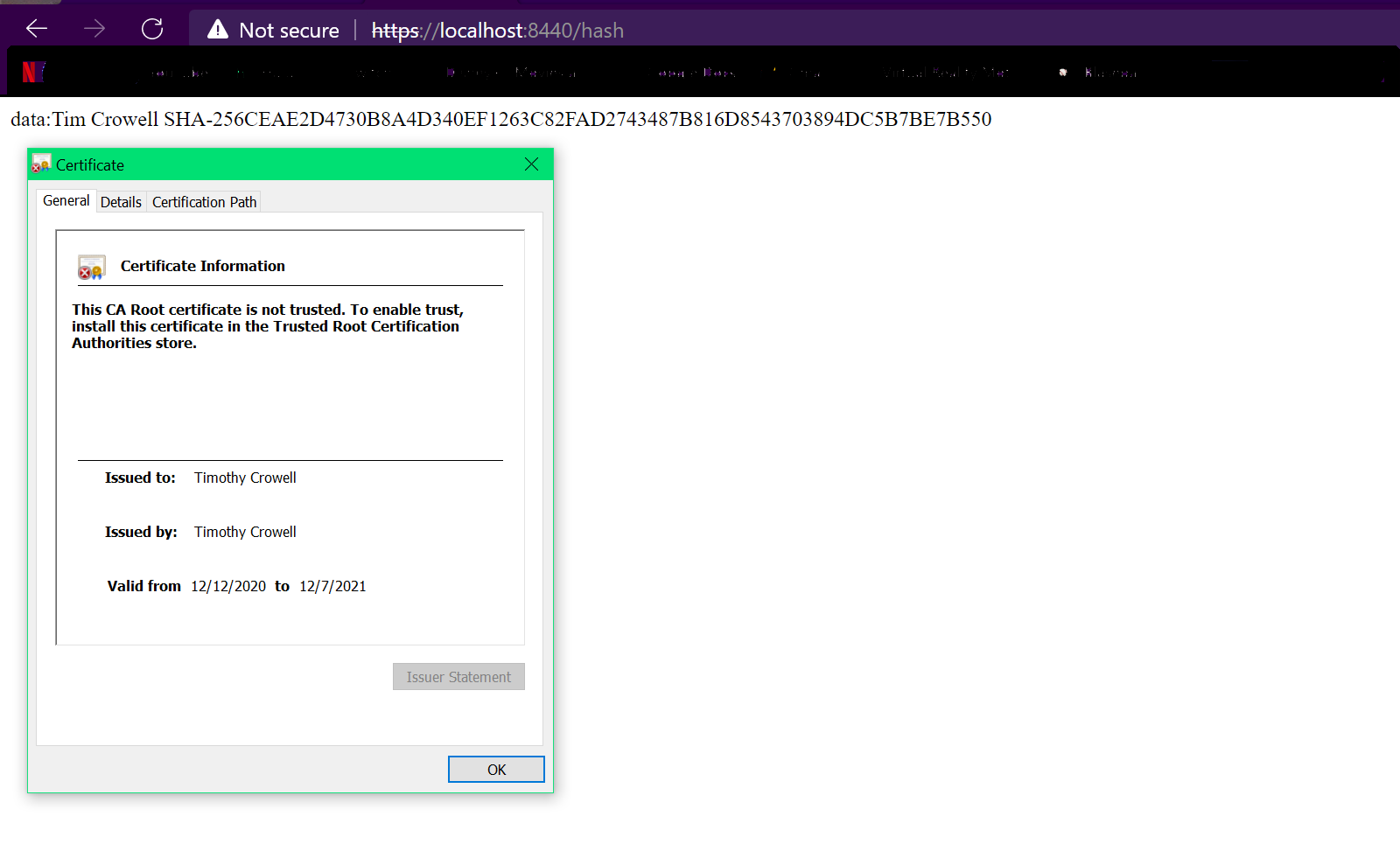
* Insert a screenshot below of the checksum verification. The screenshot must show your name and a unique data string that has been created.



## 4. Secure Communications

Refactor the code to convert HTTP to the HTTPS protocol. Compile and run the refactored code to verify secure communication by typing **https://localhost:8443/hash** in a new browser window to demonstrate that the secure communication works successfully.

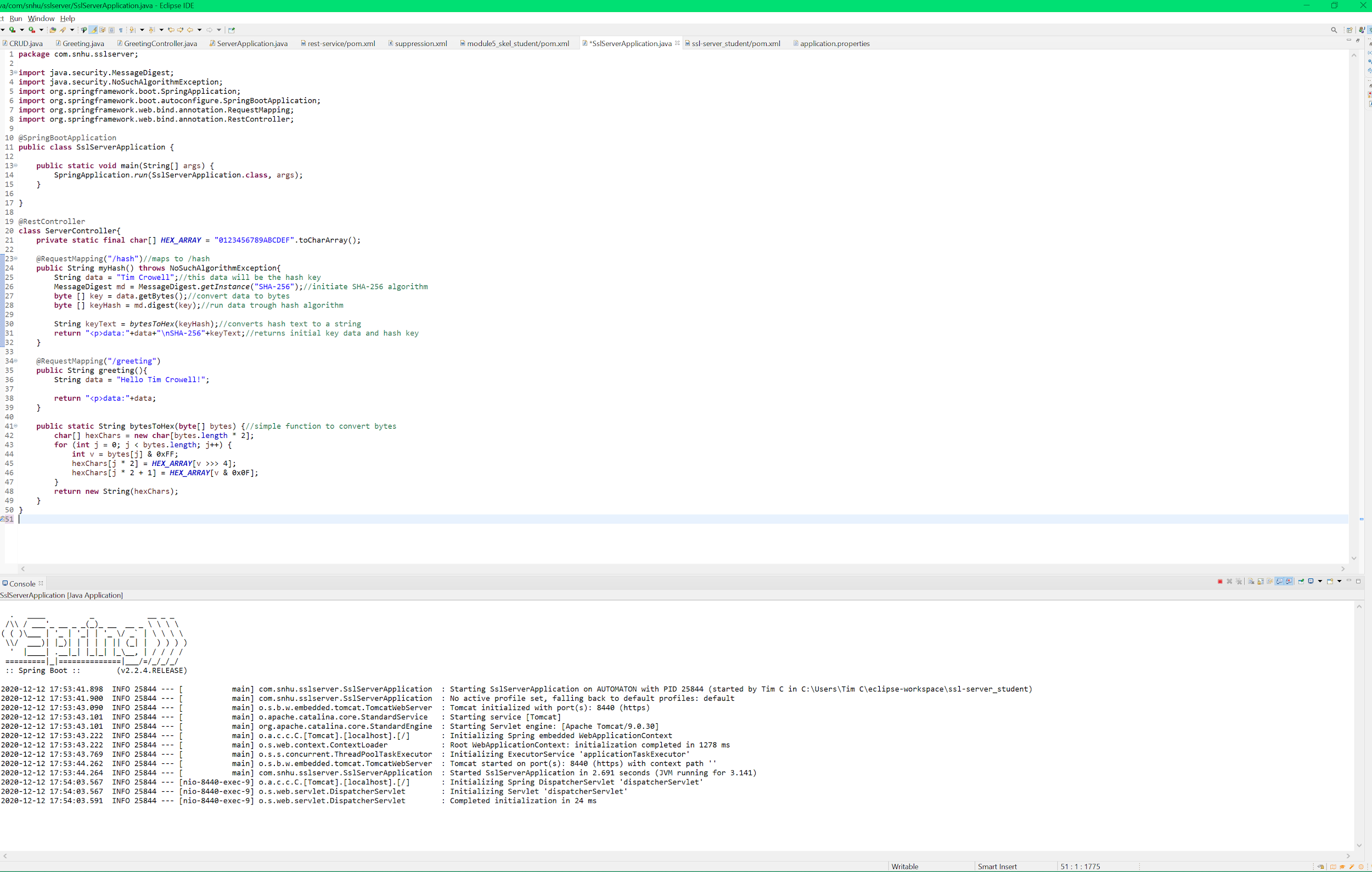
* Insert a screenshot below of the web browser that shows a secure webpage.

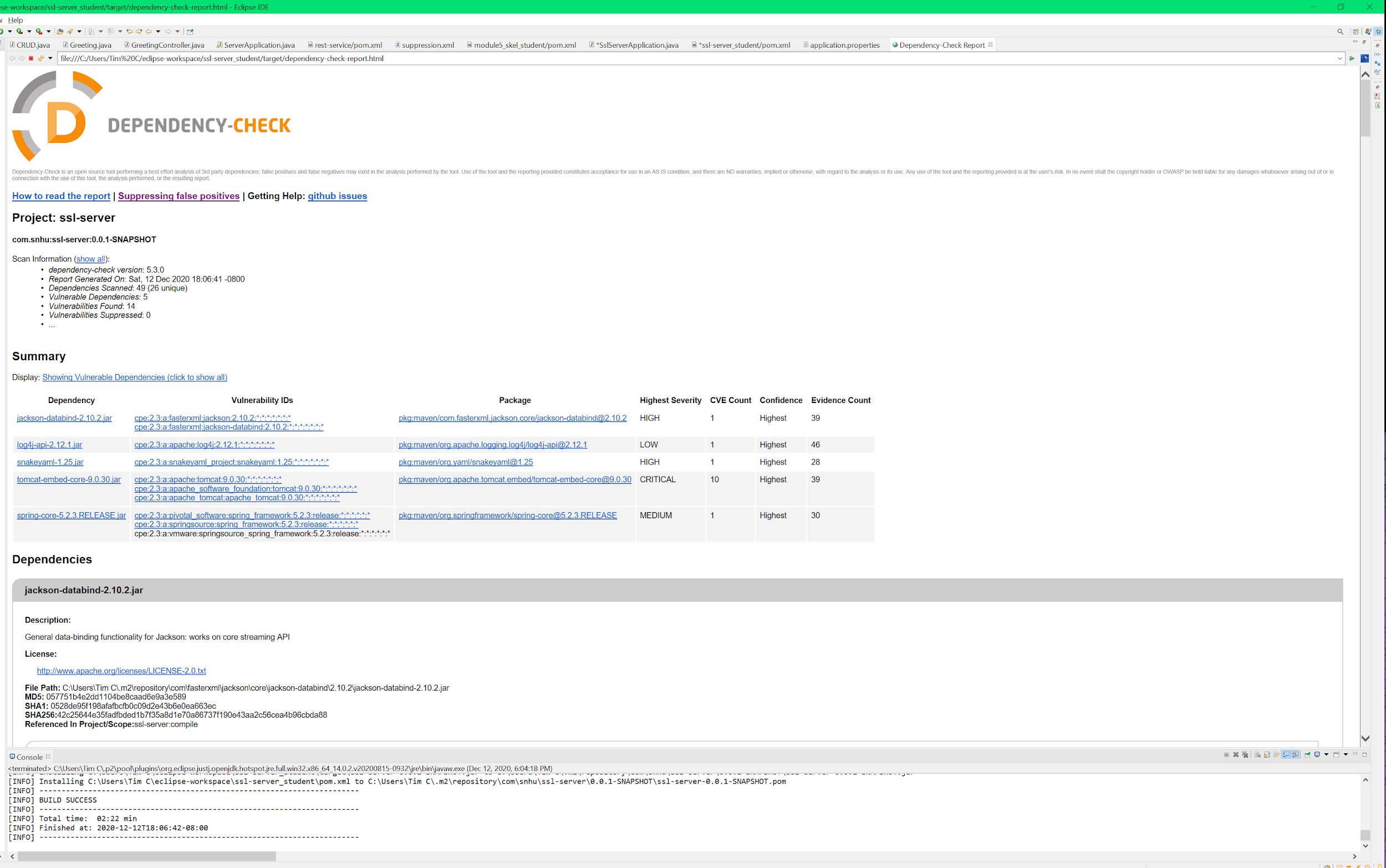


## 5. Secondary Testing

Complete a secondary static testing of the refactored code using the dependency check tool to ensure code complies with software security enhancements. You only need to focus on the code you have added as part of the refactoring. Complete the dependency check and review the output to ensure you did not introduce additional security vulnerabilities.

* Include the following below:
  + A screenshot of the refactored code executed without errors
  + A screenshot of the dependency check report

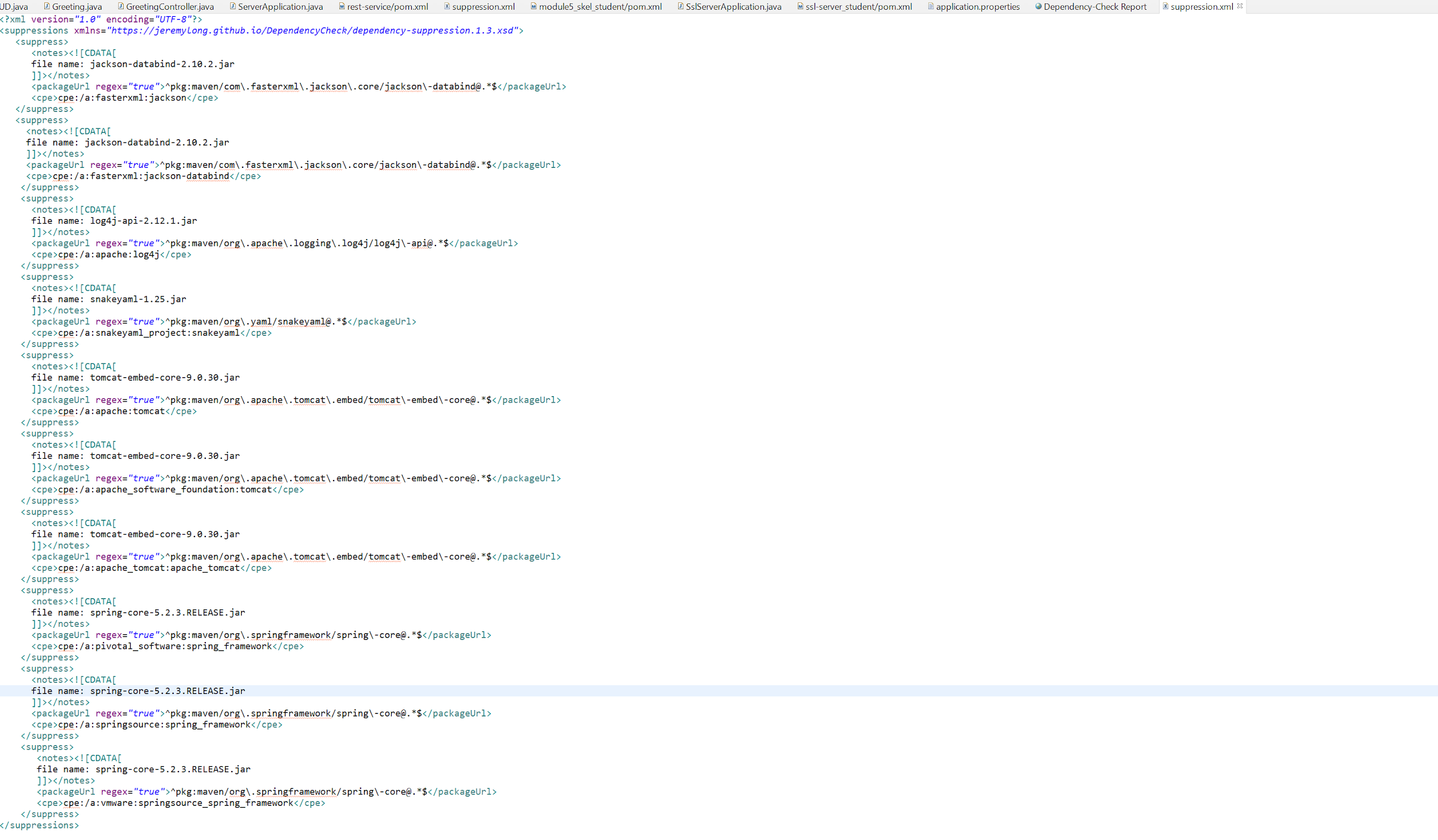


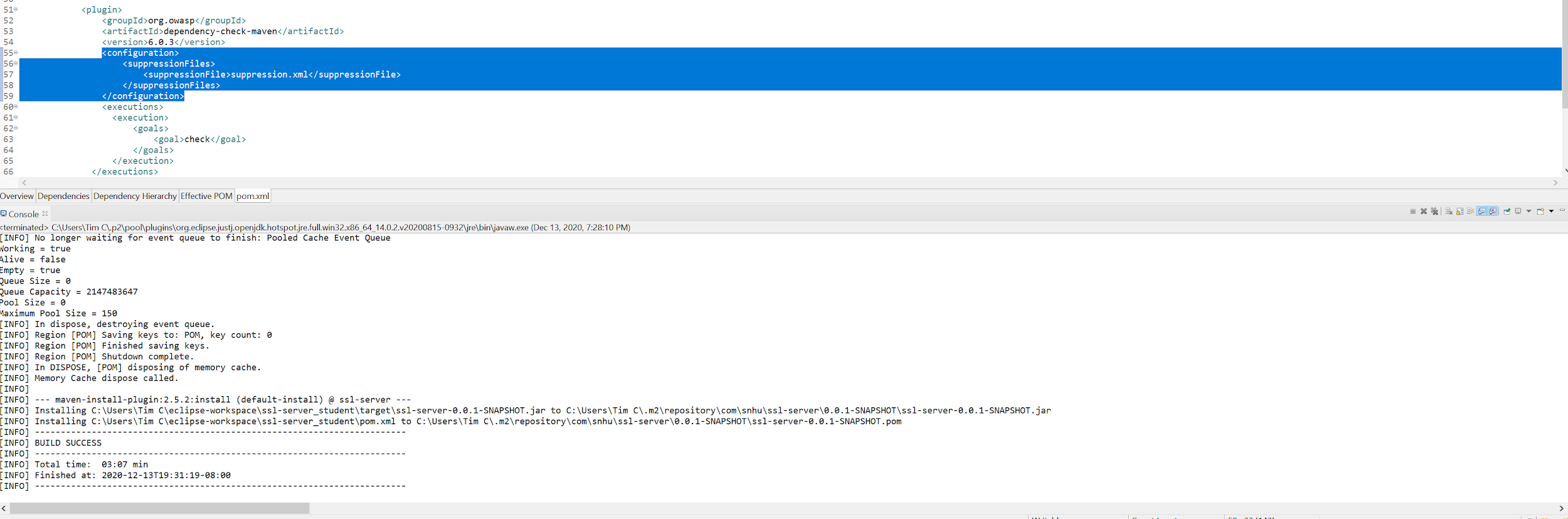


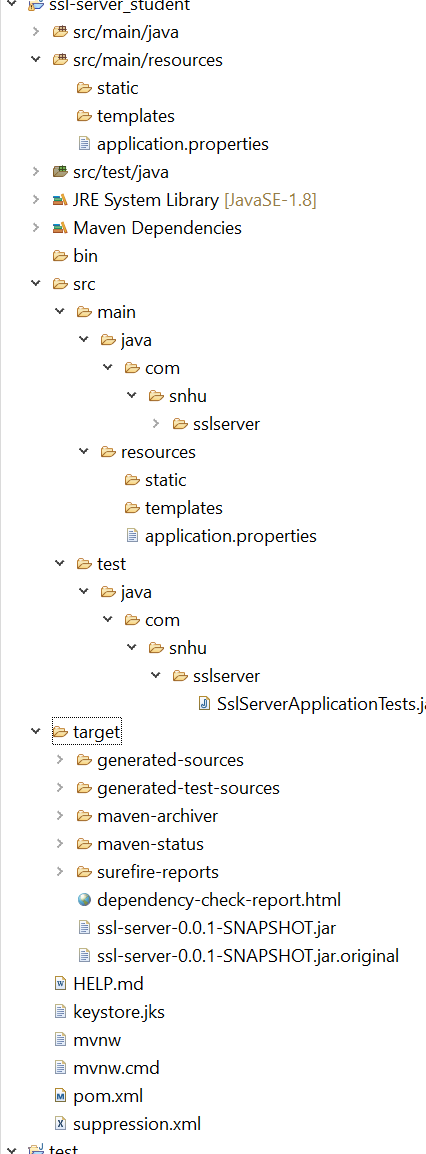
## 6. Functional Testing

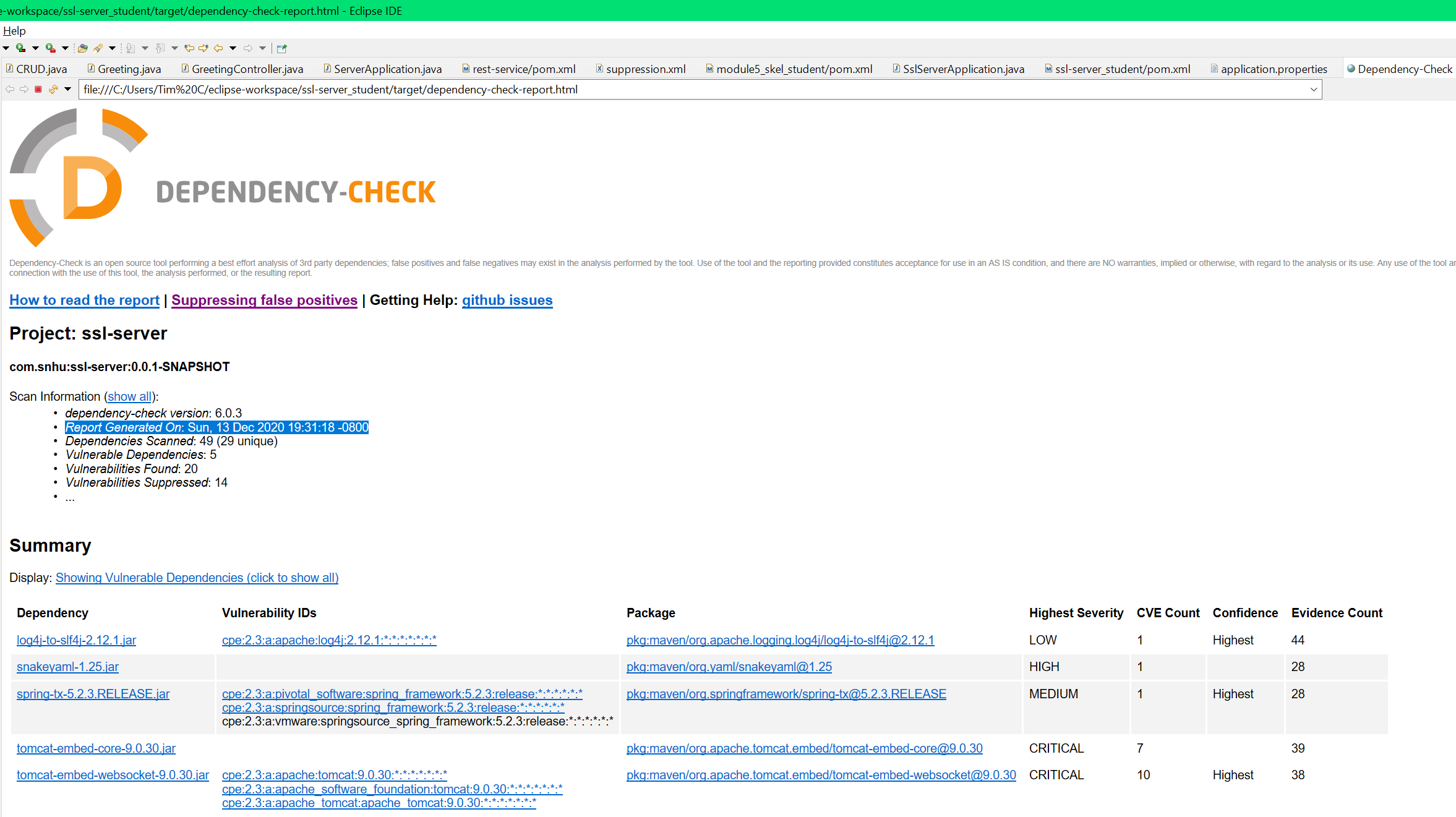
Identify syntactical, logical, and security vulnerabilities for the software application by manually reviewing code.

* Complete this functional testing and include a screenshot below of the refactored code executed without errors.









## 7. Summary

Discuss how the code has been refactored and how it complies with security testing protocols. Be sure to address the following:

* Refer to the Vulnerability Assessment Process Flow Diagram and highlight the areas of security that you addressed by refactoring the code.
* Discuss your process for adding layers of security to the software application and the value that security adds to the company’s overall wellbeing.
* Point out best practices for maintaining the current security of the software application to your customer.

During the process of securing the code for safe consumer use, we cover many of the best security practices. We apply cryptography to our system in the form of an RSA algorithm. Additionally we apply best practices for client / server security by providing a certificate for users to validate. This proves that the website they are connecting to is authentic. In addition to using the RSA algorithm to secure the system, we use the SHA-256 hash algorithm to sign messages sent between users and the system providing secure communications, another best practice for maintaining security.

Adhering to these best security practices and the coding standard provides a clean and stable system that is protected and safe for companies and customers to use. Companies who lose sensitive data lose face and trust with customers. Customers need to know that their data is safe and business and companies that hire developers expect these best practices to be performed to provide that. As a developer, applying these practices through development ensures an excellent system.