****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_heading=h.30j0zll)

[**Client 3**](#_heading=h.1fob9te)

[**Instructions 3**](#_heading=h.3znysh7)

[**Developer 4**](#_heading=h.2et92p0)

[**1. Algorithm Cipher 4**](#_heading=h.tyjcwt)

[**2. Certificate Generation 4**](#_heading=h.3dy6vkm)

[**3. Deploy Cipher 4**](#_heading=h.1t3h5sf)

[**4. Secure Communications 4**](#_heading=h.4d34og8)

[**5. Secondary Testing 4**](#_heading=h.2s8eyo1)

[**6. Functional Testing 4**](#_heading=h.17dp8vu)

[**7. Summary 4**](#_heading=h.3rdcrjn)

[**8. Industry Standard Best Practices 4**](#_heading=h.26in1rg)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2/14/2024** | **Vy Huynh** |  |

## Client

in

## 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 have 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.

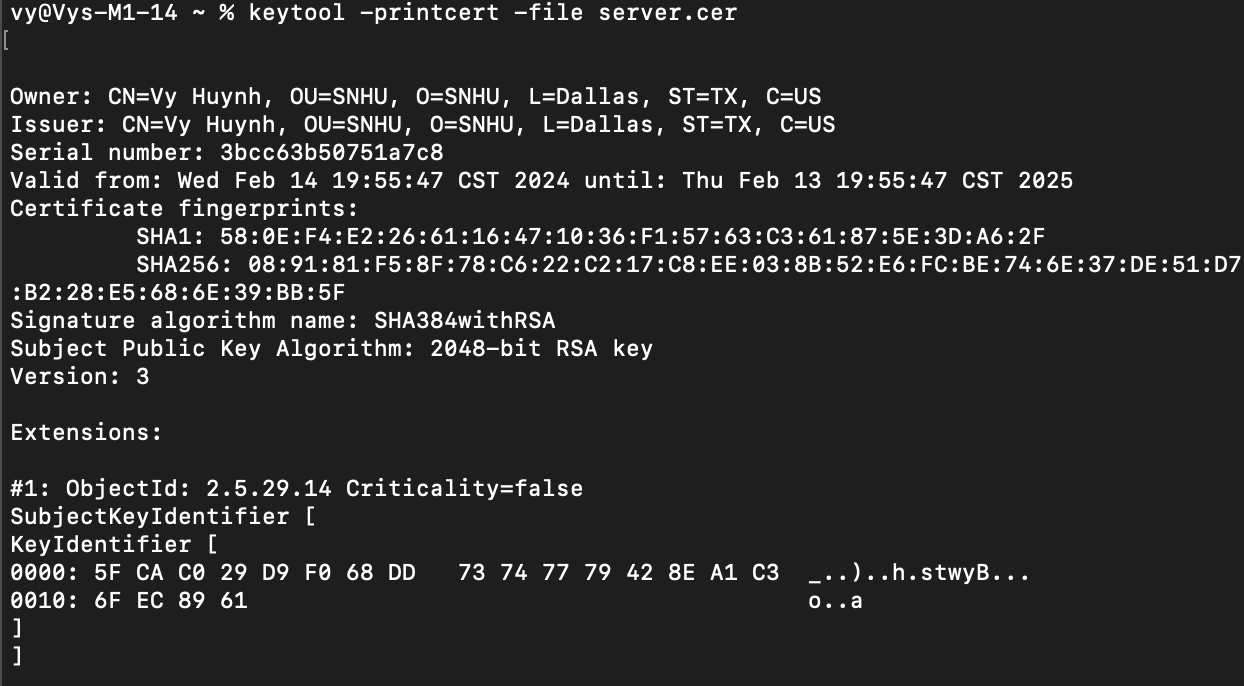
## Developer

Vy Huynh

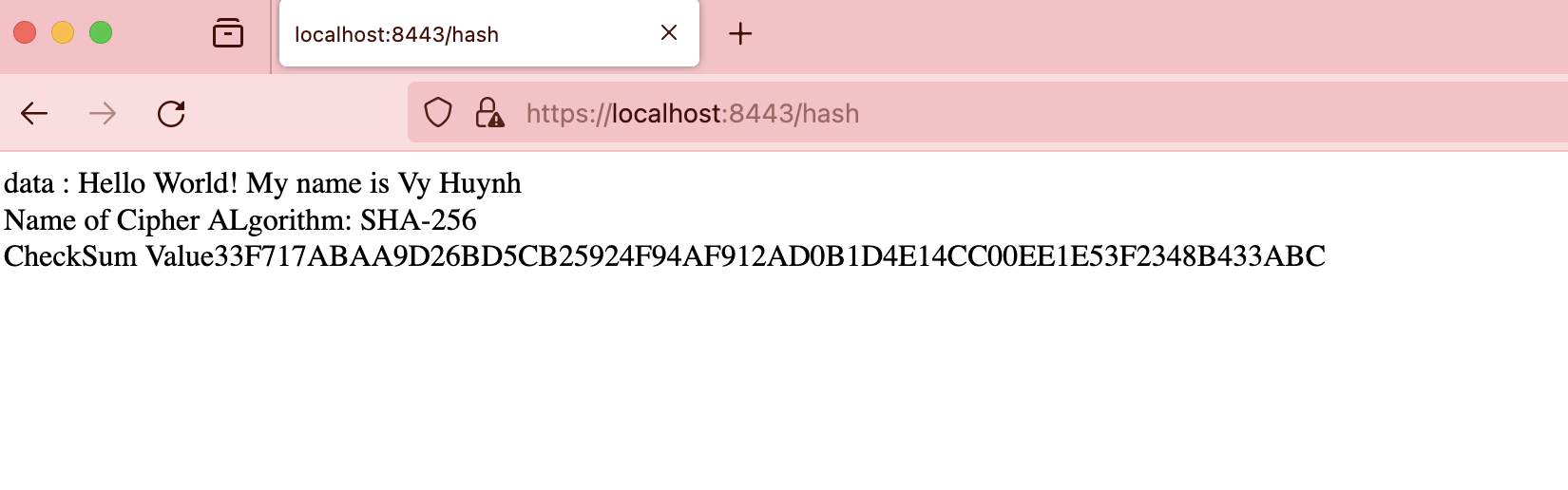
## Algorithm Cipher

The cipher that Artemis Financial should use is AES256. The reason to use AES256 over 128 is that 256 is much more secure than 128, which means that sensitive information like customer financial information is much safer with AES256 encryption. AES cipher encrypts plaintext into ciphertext that other parties besides the user can not access and read; this helps protect customers’ sensitive information from hackers and prevents hackers from quickly accessing the information. AES uses “bits” to encrypt the plaintext into cipher text. The main difference between 256 and 128 is that 256 uses more ‘bits’ to encrypt the plain text; the formula for AES will usually be 2 to the power, so for 256, it will be 2 to the power of 256, making it incredibly and nearly impossible to brute force. AES uses a symmetric key, which is more efficient than an asymmetric key. The main difference between asymmetric and symmetric is that symmetric uses a shared key to encrypt and decrypt; unlike asymmetric, symmetric is more efficient, which is better when a lot of data needs encrypting. The history of encryption started with the most popular and basic encryption technique, the Caesar cipher. Later, AES was developed after the government created the AES encryption technique, and today, it’s one of the most popular encryptions widely used by many organizations.

## Certificate Generation



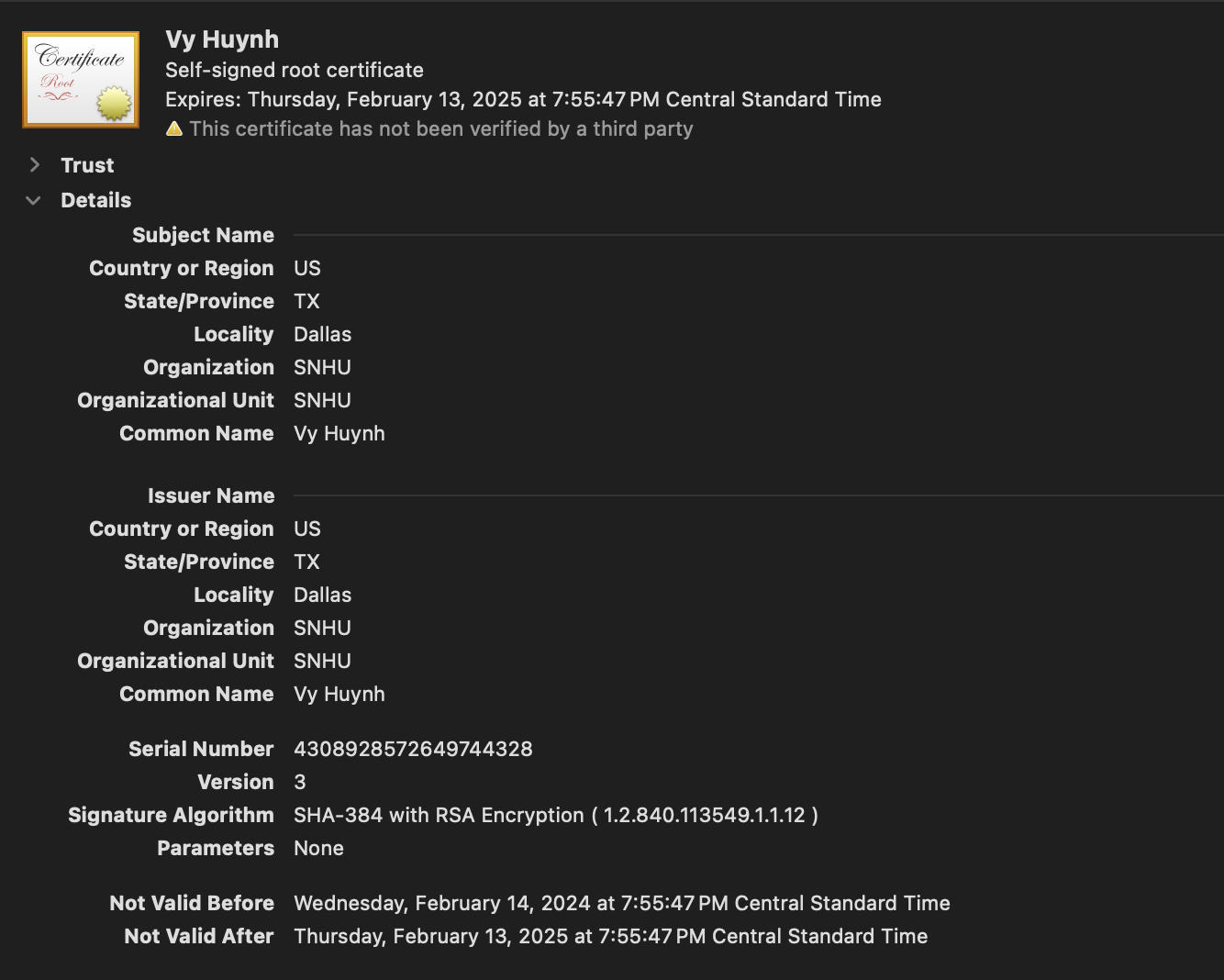
## Deploy Cipher



## Secure Communications

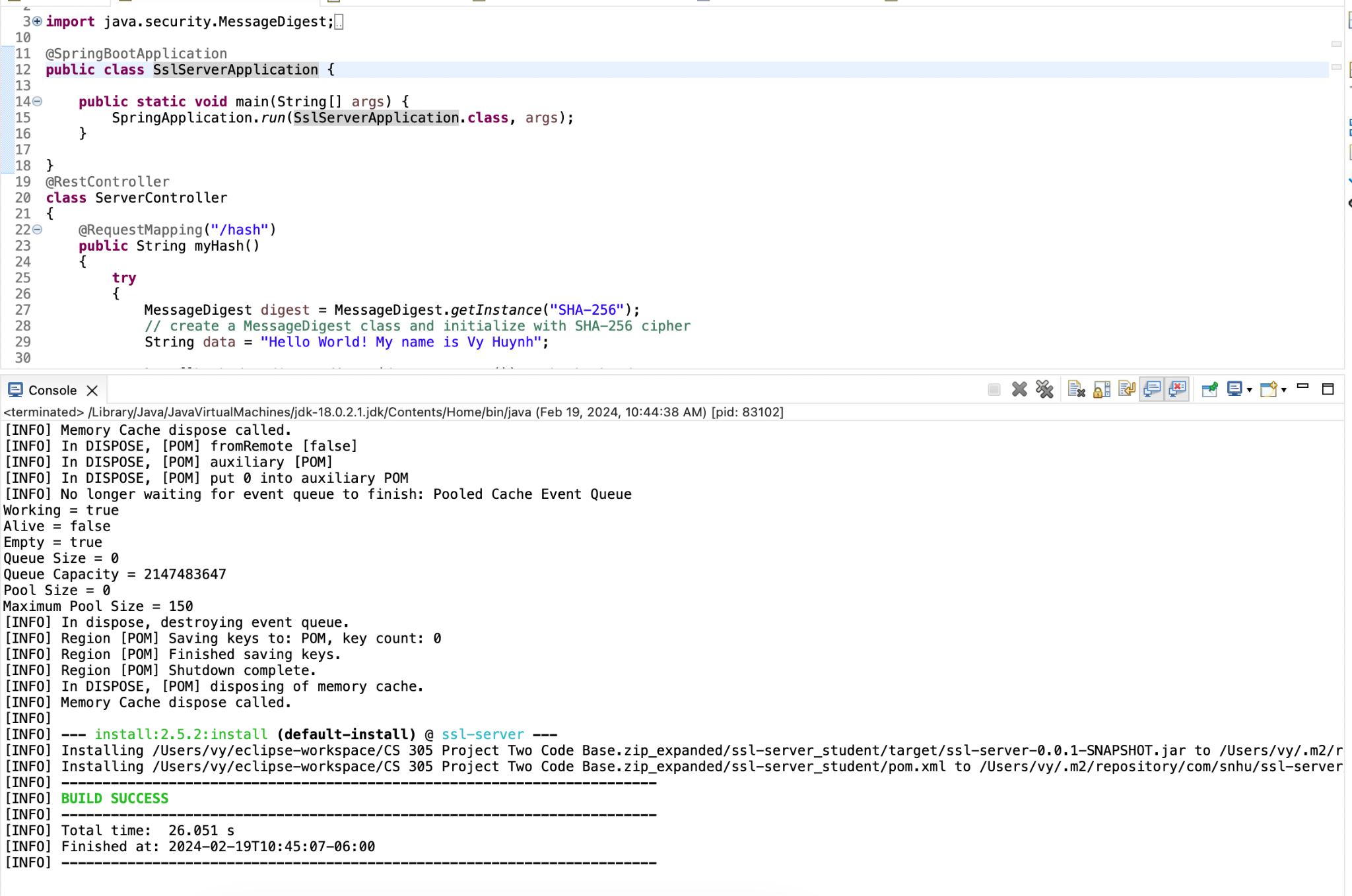
Insert a screenshot below of the web browser that shows a secure webpage.

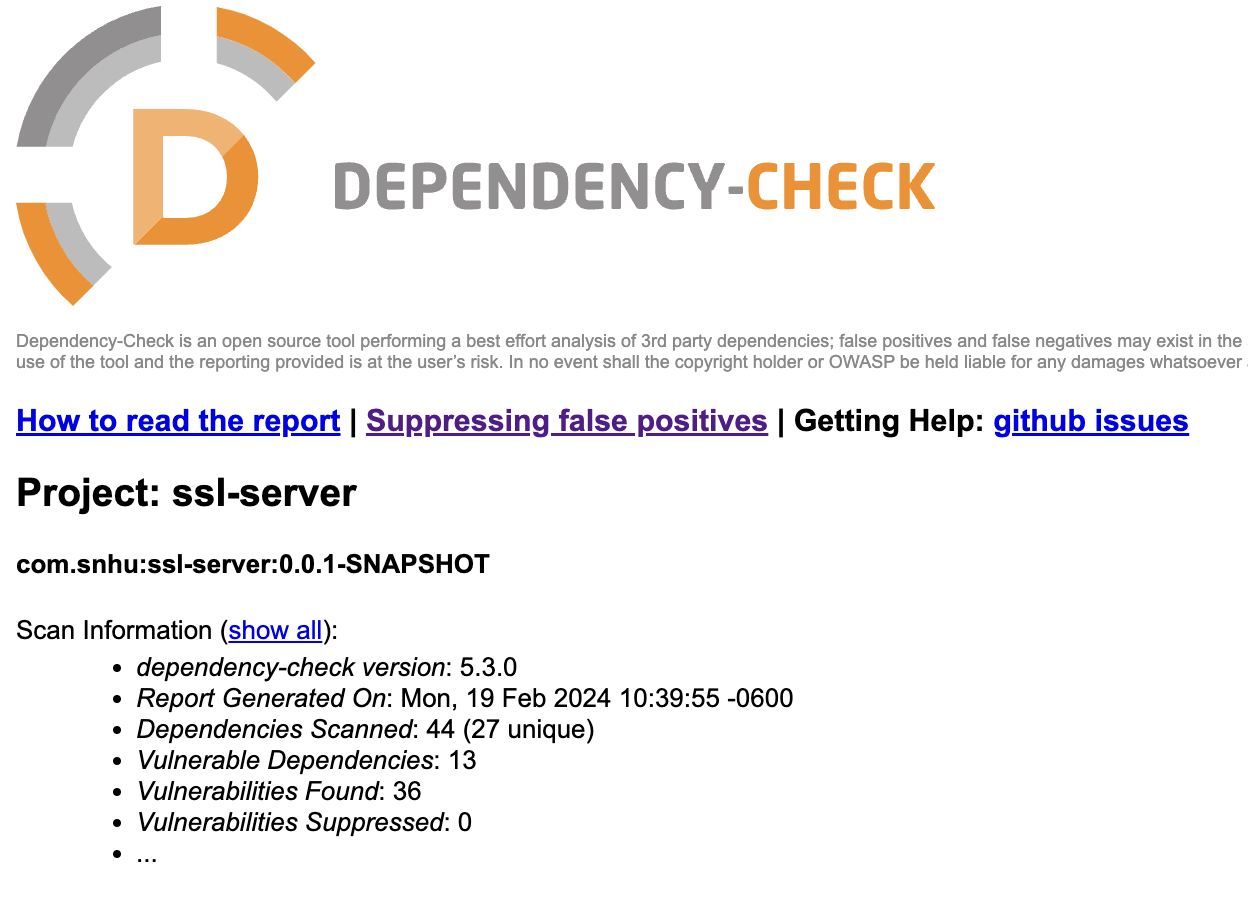




## Secondary Testing

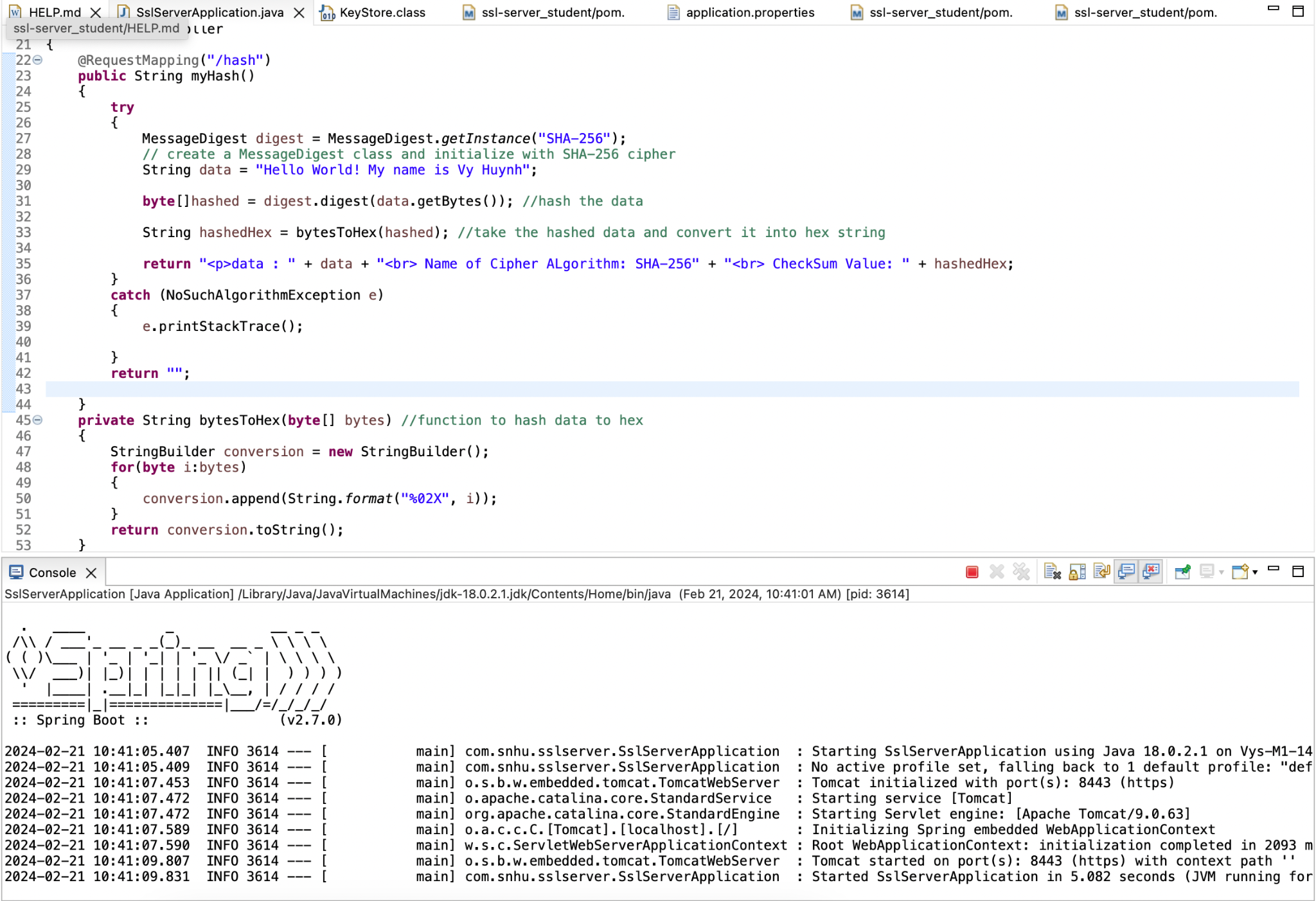
Insert screenshots below of the refactored code executed without errors and the dependency-check report.





## Functional Testing

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



## Summary

Based on the vulnerability assessment process flow diagram, the code has been refracted to follow the diagram by first having input validation; there are no boxes that allow the user to insert their input, which will prevent the possibility of having an injection attack. Next, by creating a keystore, ensure there are valid APIs and secure API connections. Next, cryptography and encryption ensure that information is secure and there is no potential for leaking data. The extra layer of security was added to the code by having a keystore, and a certificate to verify that communications between server clients are secure. Another one that helps add to security is a catch that allows handling code errors; this helps with potential security risks that a hacker can exploit and prevents a possible location that a hacker might be able to exploit.

## Industry Standard Best Practices

I use industry best practices with encryption, error handling, and secure communications. Following industry best practices is essential because it helps protect secure and sensitive information. This prevents unauthorized people from accessing information. Following industry best practices allows help to stay within regulations and make sure that the company is not breaking any rules or doing anything that they are not supposed to. Finally, staying within regulations helps maintain trust between consumers and the company; consumers are more likely to trust a company if the customers themselves know that they value protecting the customers' information as much as the customers'. Having a good reputation for caring about privacy can help with bringing more customers.