

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **10/12/2023** | **Ken Jarvis** |  |

## 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

Ken Jarvis

## Algorithm Cipher

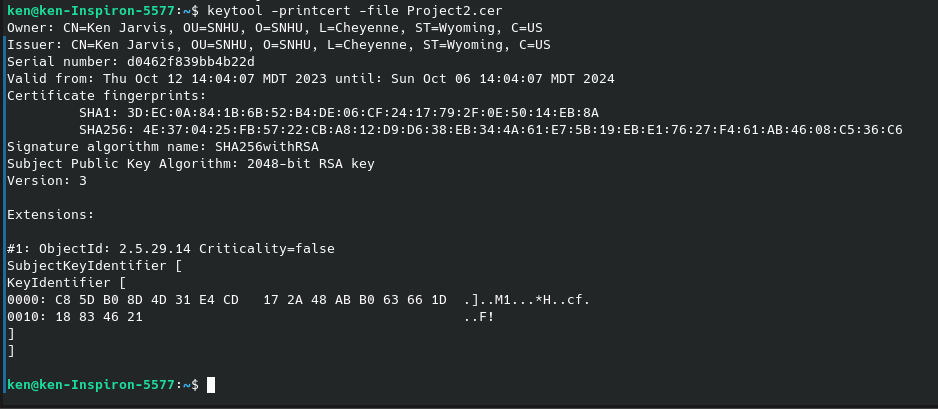
To secure Artemis Financial files, I recommend the Advanced Encryption Standard (AES). AES is a widely used algorithm to secure sensitive information. It is a block cipher that encrypts data in fixed sizes (128 bit, 192 bit, or 256 bit). This algorithm fixed number of rounds that varies depending on the key size. It uses a combination of substitution, permutation, and mixing operations to achieve security.

There are no hash functions in AES, it is used for encryption and decryption. Hash functions are used for data verification and uses variable-length inputs to compare against. AES on fixed size blocks of data of 128, 192, 256 bits. It uses random number in the key generation process. It is generated securely and is very unique. The key is symmetric in that it is used to both encrypt and decrypt data. Whereas non-symmetric uses a different key for encryption and decryption.

Encryption algorithms have been around since 600 BC when ancient Spartans used a device to code messages that could only be read when using another device to decode it. The devices consisted of a leather strap wrapped around a wooden rod, a simple process, but quite effective. AES on the other-hand was developed in 2001 by the U.S. National Institute of Standards and replaced the outgoing Data Encryption Standard. Today AES is still effective, taking a super computer many years to decrypt one of its algorithms. But as time goes on, AES will one day meet the end of its life cycle and have to make way for a newer more secure standard.

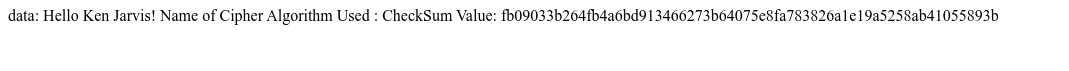
## Certificate Generation

Insert a screenshot below of the CER file.



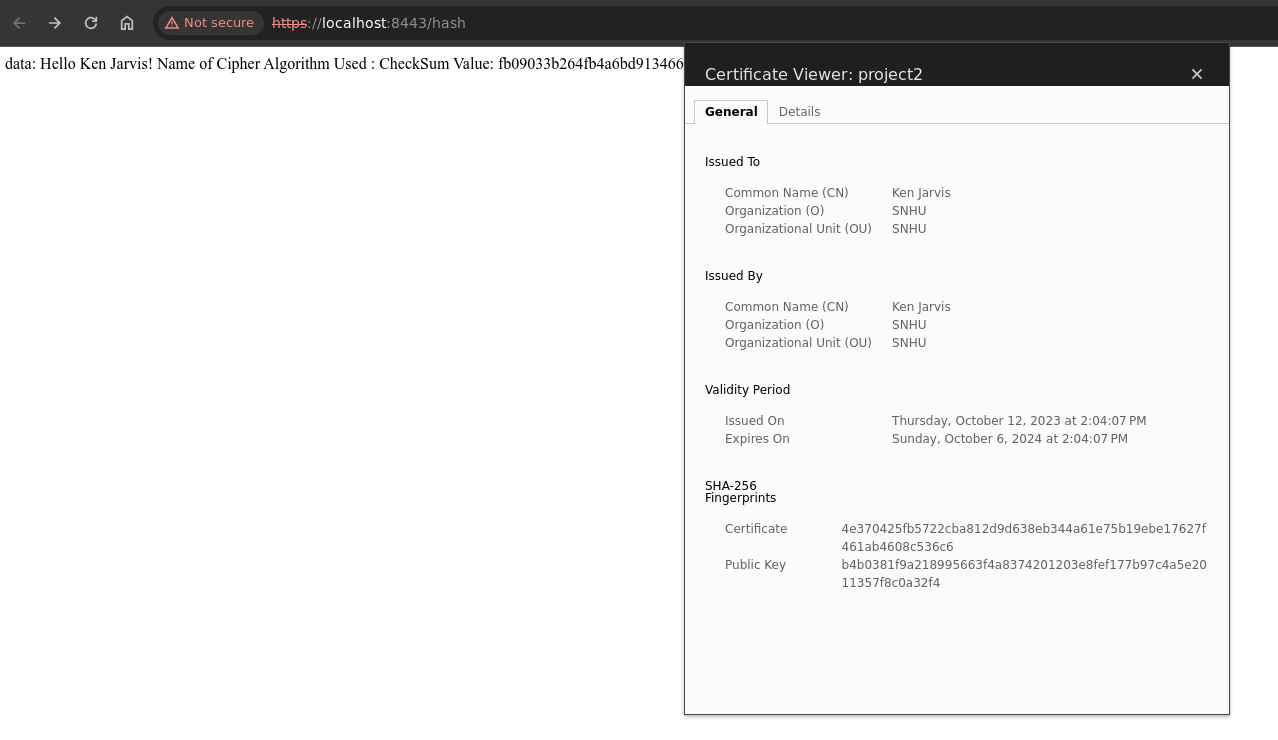
## Deploy Cipher

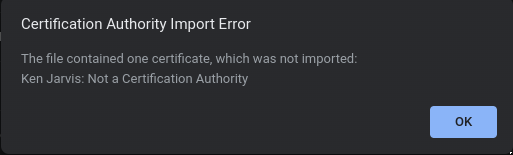
Insert a screenshot below of the checksum verification.



## Secure Communications

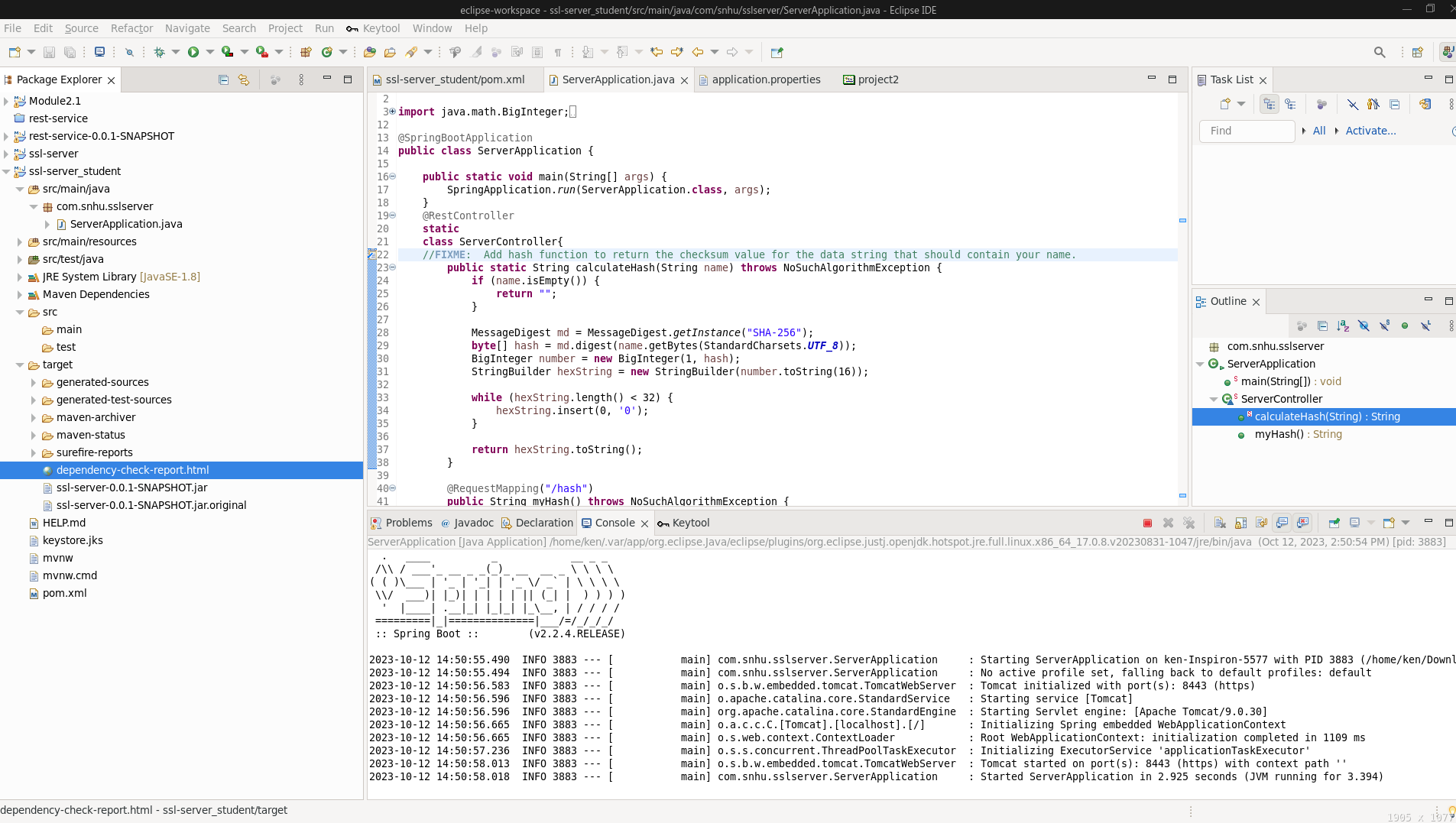
Insert a screenshot below of the web browser that shows a secure webpage.

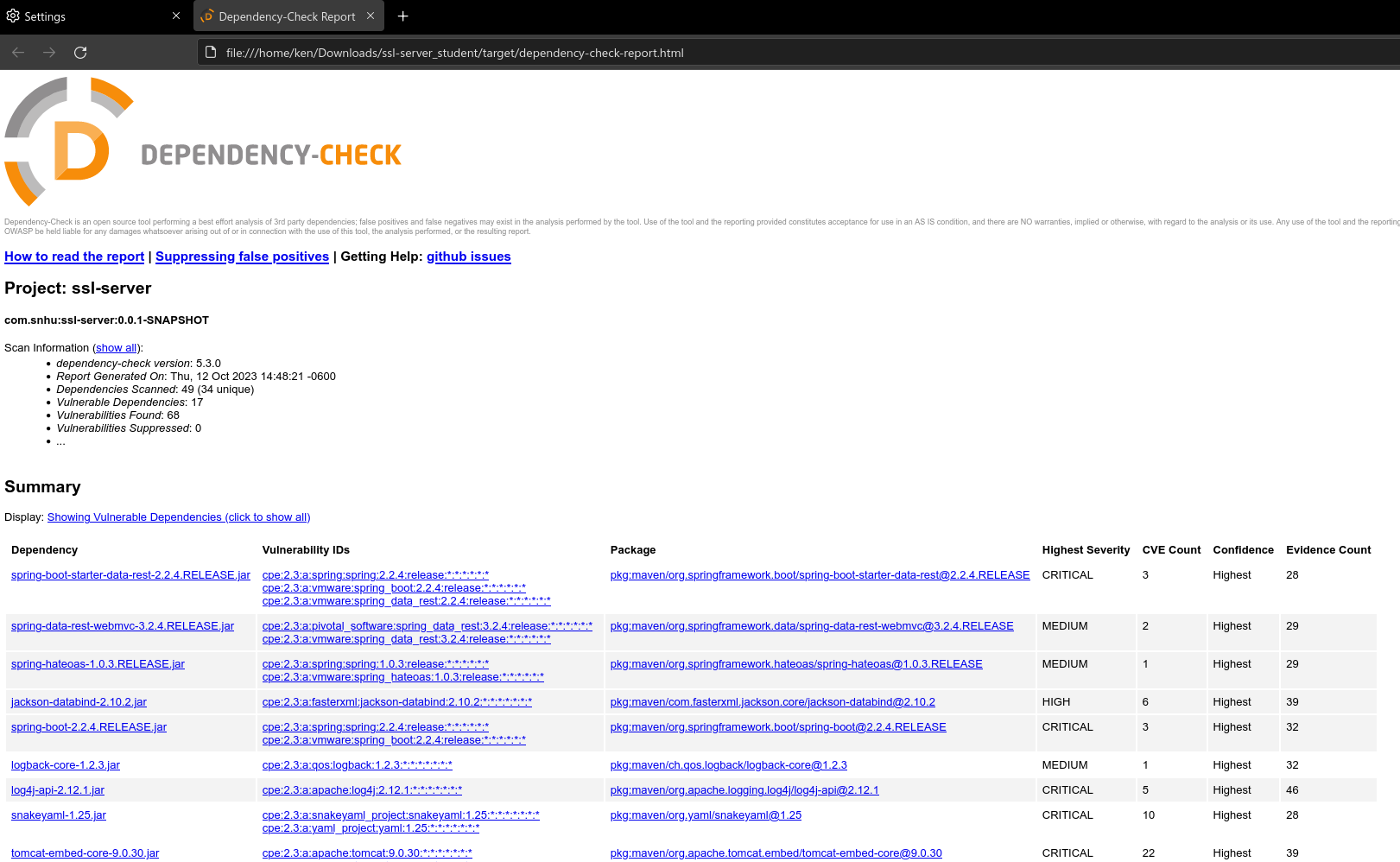
My Browser will not allow me to add my certificate as I am not a certification authority. If could, the browser would show it as secured.



## Secondary Testing

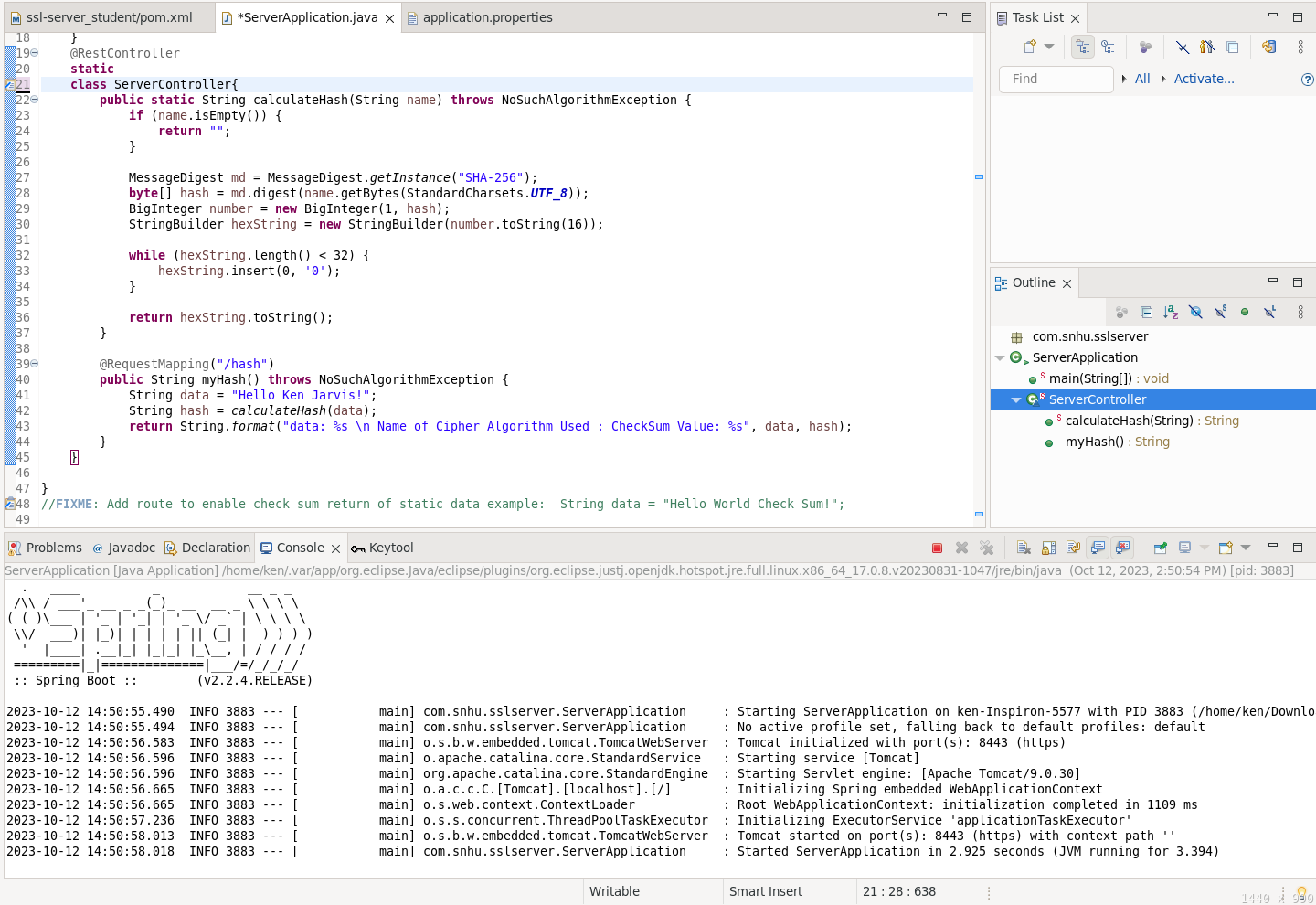
Insert screenshots below of the refactored code executed without errors and the dependency-check report.

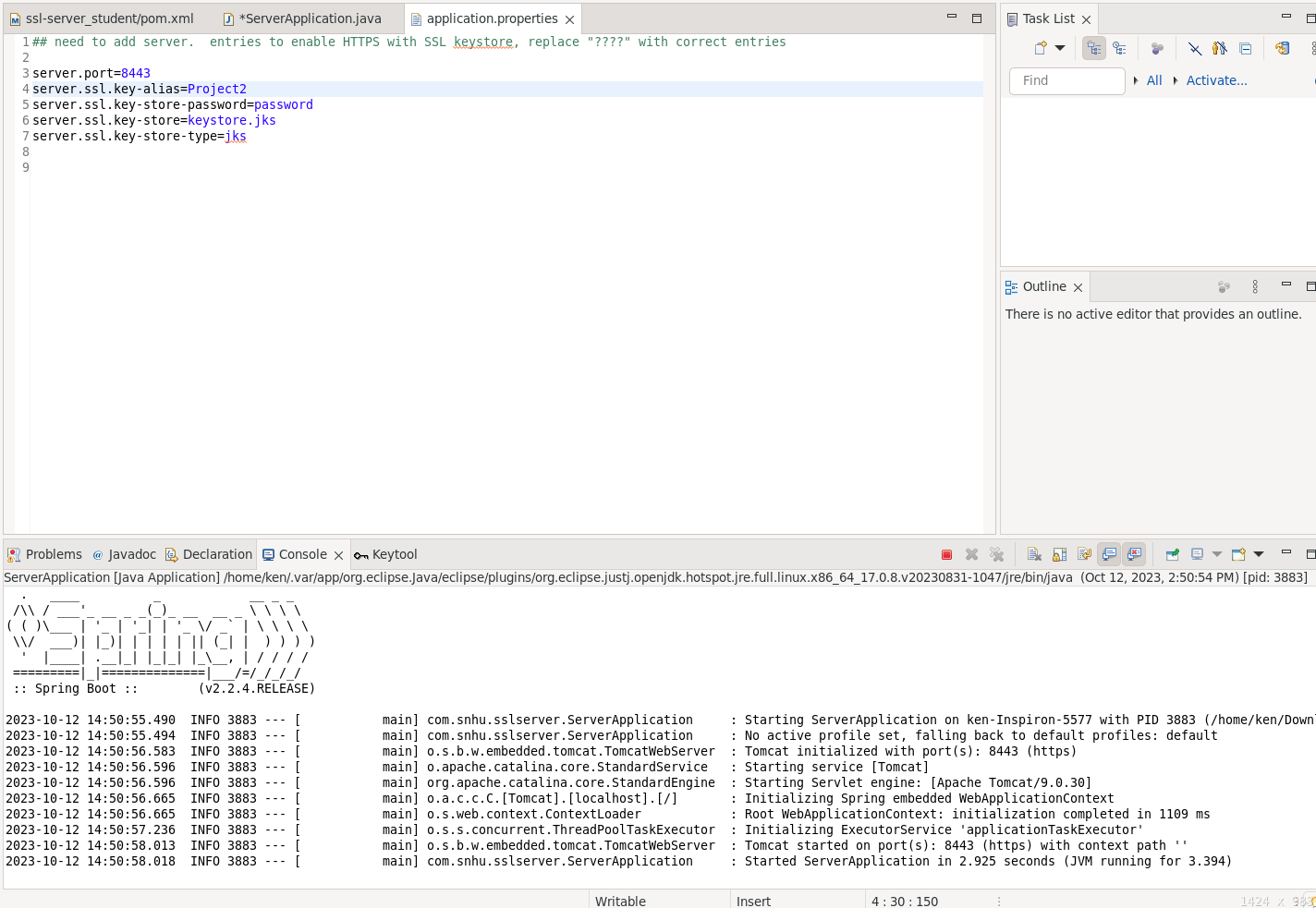




## Functional Testing

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





## Summary

After reviewing the Vulnerability Assessment Process Flow diagram, I can determine that any Input validation and APIs used with this connection will be secured using AES encryption. The cryptography uses a 128 bit algorithm with the SSL lock in a password protected keystore that only the server and client can access. I not receive any coding errors. By adding layers of security, I limit the avenues a person can take to access the data being transmitted.

## Industry Standard Best Practices

I have introduced the industry best practices of updating all packages to the latest edition. By doing so, I patch many vulnerabilities that have been discovered. By implementing encryption, I ensure that data is protected from end to end. AES helps protect data from unauthorized access and breaches, ensuring confidentiality and integrity. By applying the industry standard best practices, I reduce security risk, I comply with the legal requirement mandated by the government, I enhance customer trust and the companies reputation.