****

# 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** | **2/28/2025** | **Eaton** |  |

## 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

[Insert your name here.]

## Algorithm Cipher

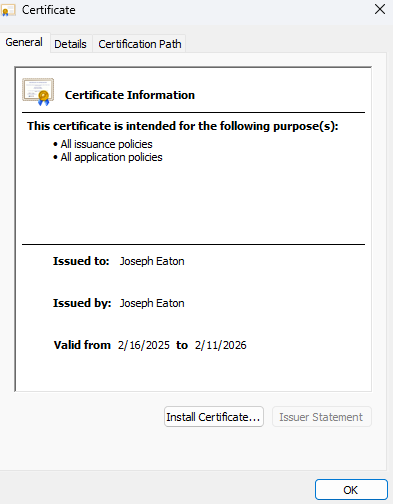
When looking at the needs of Artemis Financial the encryption algorithm cipher that I would have to recommend would have to be the Advanced Encryption Standard (AES). Seeing as AES uses 256-bit encryption making it improbable for hackers to crack into it given that “with current 2020 technologies it would likely take a billion years to break an AES-encrypted message” (Mohn,2024, p. 10) making it one of the most secure encryption algorithms we can go with and seeing as we are going to be dealing with a lot of sensitive information with our customers ensuring the highest level of security should be a given. When looking at what security protection best practices that will need to be considered include long key length which AES will use either a 128-bit or 256-bit encryption both being quite secure. With this we will have to use proper key management to functionally store, generate and rotate through cryptographic keys to ensure that the keys remain confidential and are protected from unauthorized access. Which is why that can be a risk of using AES as if key management is handled poorly, we can risk exposing encrypted data. Another risk with AES is that it requires a higher overhead in terms of the systems that will be using it will need to be more powerful as it is generally more taxing than weaker algorithms. With Artemis Financial working outside of just the states some government regulations we will need to consider and comply with include General Data Protection Regulation or GDPR, the Payment Card Industry Data Security Standard or PCI DSS which requires a strong encryption for anything financial, and The Sarbanes-Oxley act which is a law that requires the protection of users data to prevent fraudulent activities. All three of these government regulations can be met using AES as it will be encrypting all this data that is required by these regulations. Artemis Financial after adopting AES will be able to put it to use by encrypting the financial transactions within their databases and will be able to ensure the data integrity in all of their backup storage and log file while ensuring their Api and webservices data is also protected by AES-GCM which is able to check the integrity and authentication of any additional data whilst providing authenticated encryption. For all these reasons I think that AES is the best cipher to consider, especially AES-256 as it has not been broken through conventional computing yet and will not be for the foreseeable future. The main reason you would not want to go with the most secure cipher would have to be the operational cost and having to have better systems to use it in general but AES does have other encryption options that will still be considered secure if this is an issue that needs to be addressed.

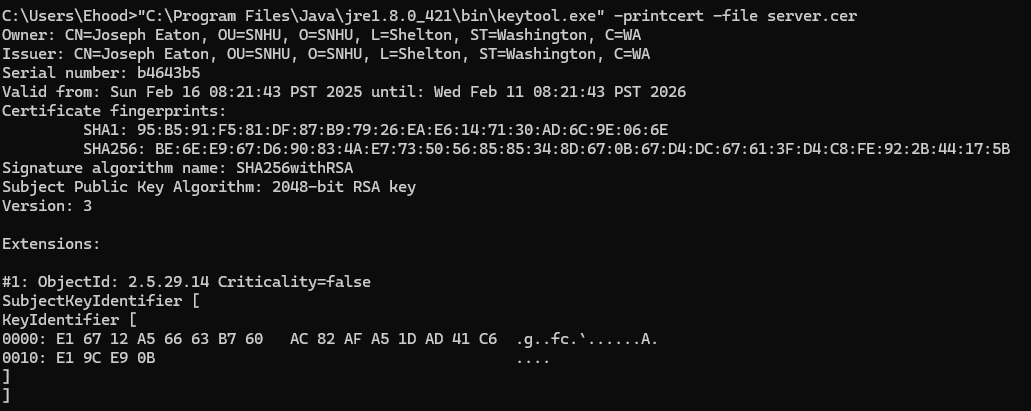
When looking at the purpose of the Bit levels in AES the first thing to start with is what does bit level mean well The bit level will determine how secure the encryption algorithm is meaning the higher the bit level the higher level of security at a cost of performance as they will be more complex to encrypt. For AES, the bit level recommended is AES-256 as it will be the most secure for Artemis financial, as it will have

possible keys which will all be randomly generated to prevent attackers from predicting them. Pairing this with a Hash Function that is used to verify that encrypted data has not been tampered with will ensure that Artemis Financial will be secure. Along with being secure, AES uses Symmetric Encryption, which allows for a fast and efficient process which will remain secure if the keys are responsibly managed. As for some history and the current state of AES to be aware of is AES was a replacement for DES in the US government which was 56 bit which started to fall behind the advancement of technology, so the government saw the work of cryptographers Joan Daeman and Vincent Rijman which was called Rijndael which was a 128- ,192-, and 256- bit encryption so the government chose it to be the replacement as it was easily implemented in software, hardware and firmware and was quite secure. The current state of AES is that it is still miles away from being brute forced by current technology but with the advancement of quantum computing this may change.

## Certificate Generation

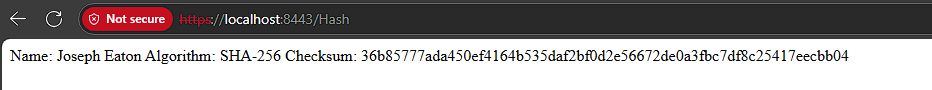
Insert a screenshot below of the CER file.





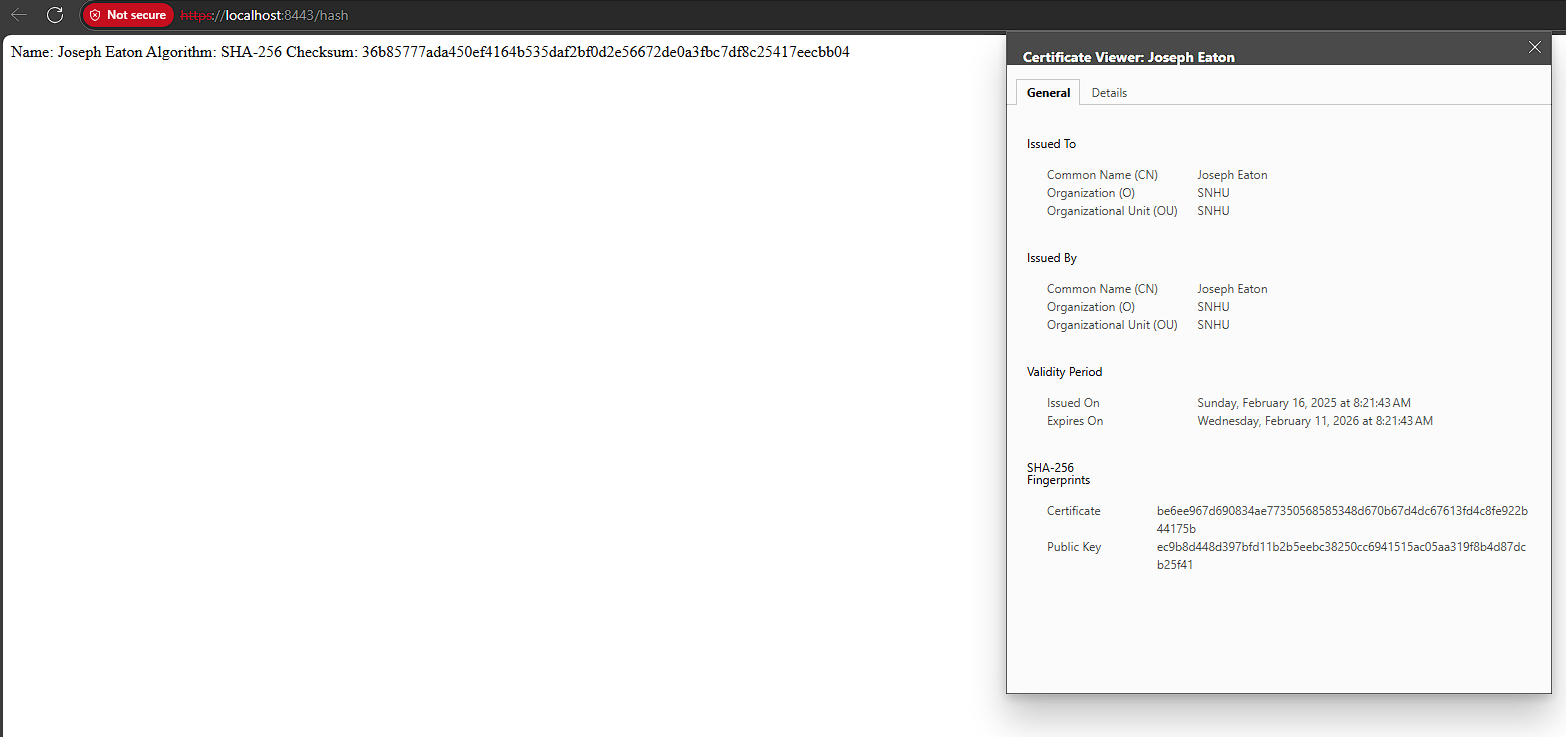
## Deploy Cipher

Insert a screenshot below of the checksum verification.



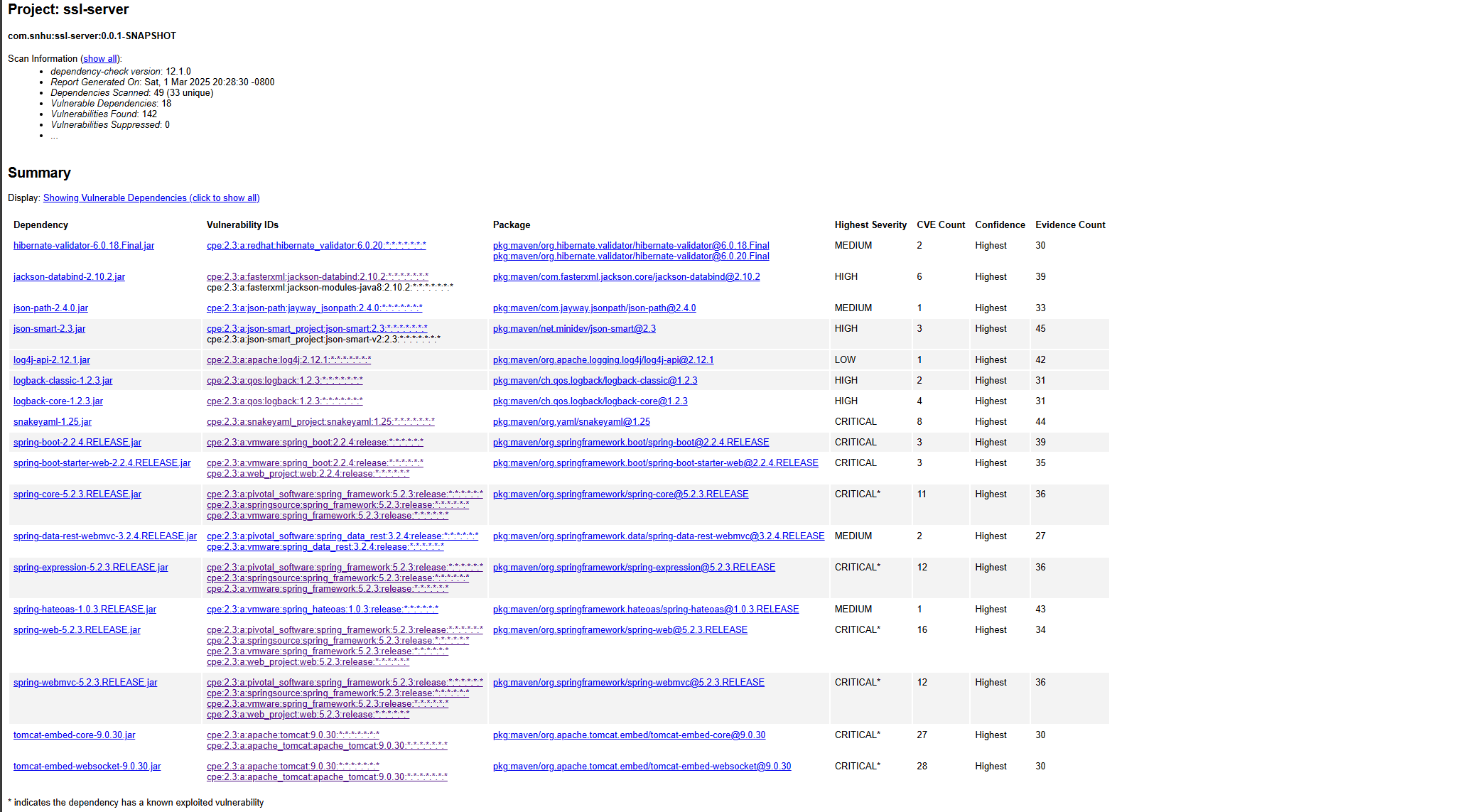
## Secure Communications

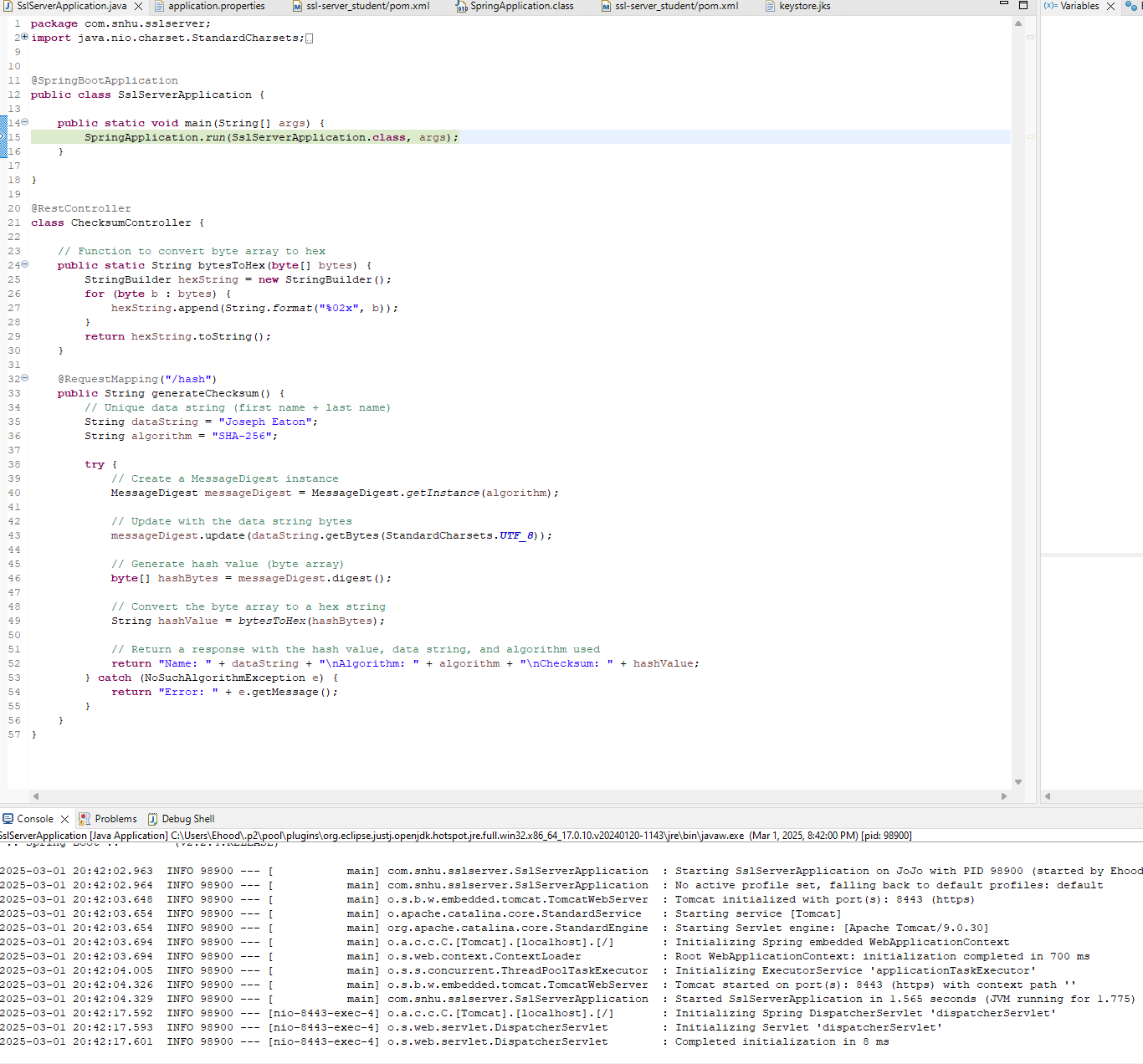
Insert a screenshot below of the web browser that shows a secure webpage.

For the life of me could not get a secure browser not exactly sure why. But 

## Secondary Testing

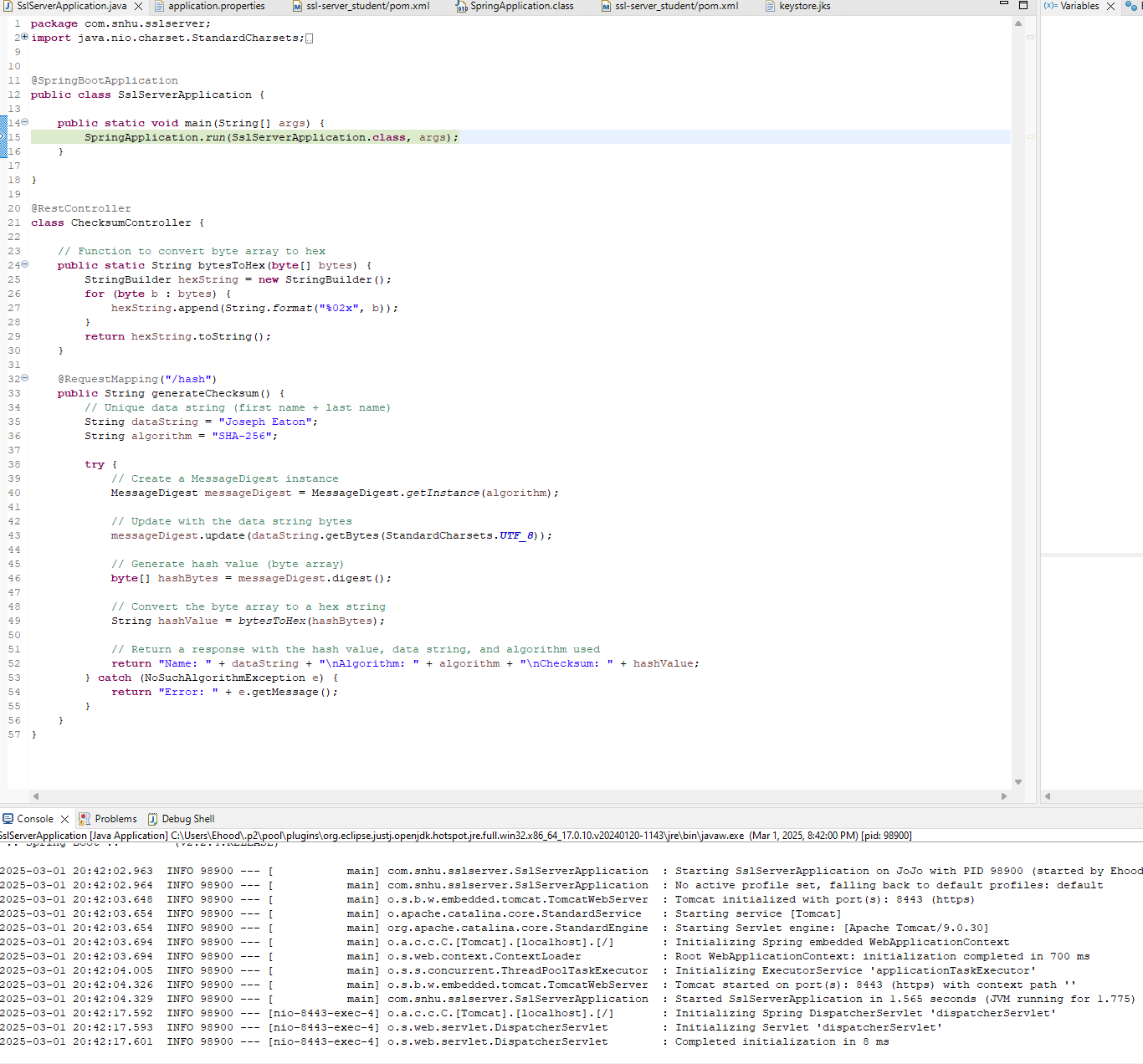
Insert screenshots below of the refactored code executed without errors and the dependency-check report.





## Functional Testing

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



## Summary

When looking at the changes in the refractured code I made sure to take use of SHA-256 which is a cryptographically secure hashing algorithm which was used for generating a secure hash which would help prevent collisions. Using NoSuchAlgorithmException would allow for a controlled error message along with error handling when an algorithm is not found. Using restful API and spring boot allowed us to create a secure connection. And when it comes to encapsulation, we ensure that a string would be encoded and turned into bytes using getBytes(StandardCharsets.UTF\_8). When it came to my process of adding layers of security, I started wanting to secure the users data and using sha-256 for hashing and or handling any exceptions. While wanting to focus on a basic form of error handling to prevent some threats posed to my program.

## Industry Standard Best Practices

When looking at how I used industry best practices to maintain the software applications existing security we can break down some different practices that were used.

First off, we are using SHA-256 which is used to hash our given string which ensures that the hashing process is safe against any common vulnerabilities like collision attacks. We also used UTF-8 encoding which encoded out strings into bytes which made for a consistent and secure handling process of data throughout different platforms. When looking at how the code handled exceptions like NoSuchAlgorithmException we ensured that a simple error message would be procked with our revealing any sensitive information. We also made sure that secure connections would be made by converting HTTP to the HTTPS protocol to make for secure communication. The use of spring boots security features is also being used as we are using Spring boot. By sticking to the industry's best practices when it comes to security practices it is beneficial for a company's overall well-being to adhere to these best practices as it enhances their ability to defend from any cyber threats that may target there company and allows protection of any clients/users information through data protection which helps the company maintain its trust of clients and reputation as a whole. Focusing on security best practices allow for a company to build better products that will bolster their success and public reputation by maintaining this security.