****

# 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 5](#_Toc102040759)

[3. Deploy Cipher 6](#_Toc102040760)

[4. Secure Communications 6](#_Toc102040761)

[5. Secondary Testing 7](#_Toc102040762)

[6. Functional Testing 9](#_Toc102040763)

[7. Summary 10](#_Toc102040764)

[8. Industry Standard Best Practices 11](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **02/25/2024** | **Michael Crevier** | **This revision showcases enhancement of the security of a Spring Boot application by integrating AES-256 encryption for data protection and transitioning to HTTPS for secure data transmission, aligning with industry-standard best practices for secure coding.** |

## 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

Michael Crevier

## Algorithm Cipher

For the enhancement of security within Artemis Financial's web application, the adoption of AES encryption, particularly with a key length of 256 bits, is strongly recommended. Renowned for its robust security measures, AES is a symmetric key encryption algorithm that is the gold standard for data protection globally. Utilizing a 256-bit key ensures the highest level of encryption strength, effectively guarding against even the most advanced brute-force attacks. This approach not only meets but exceeds global security standards and regulatory expectations, ensuring that Artemis Financial remains at the forefront of data protection. Adopting AES-256 demonstrates a commitment to maintaining the utmost level of data confidentiality, integrity, and trust, crucial for financial institutions in today's digital landscape.

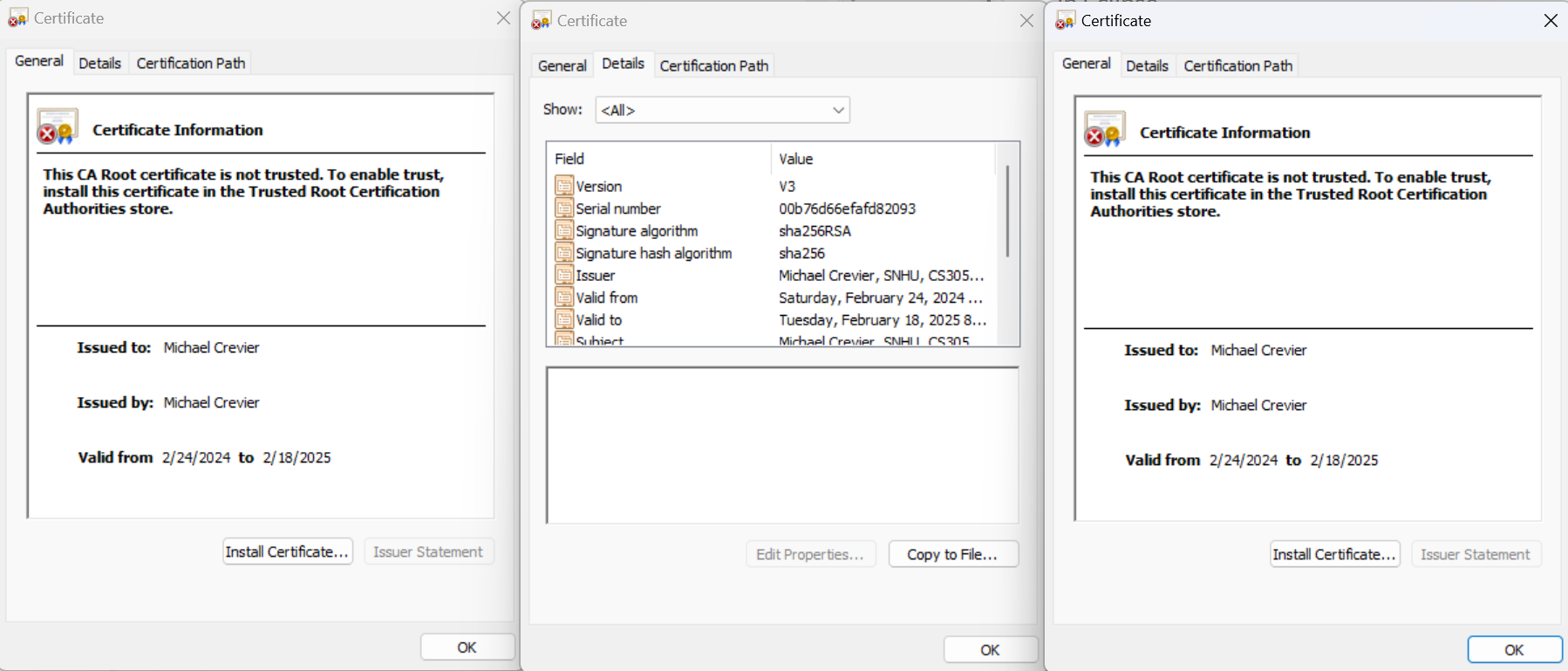
In the context of AES encryption, hash functions play a crucial role in ensuring data integrity and authenticity. While AES itself is not a hash function, cryptographic hash functions are often used alongside encryption algorithms to generate fixed-size hash values from arbitrary input data. These hash values, typically of fixed length, serve as unique digital fingerprints of the original data, facilitating efficient verification of data integrity. The bit level of AES encryption, particularly with a key length of 256 bits, represents the size of the encryption key used in the algorithm. A 256-bit key offers an astronomically large keyspace, making brute-force attacks computationally infeasible. This level of security ensures that even with the rapid advancements in computing power, AES-256 remains resilient against unauthorized decryption attempts, providing robust protection for sensitive data.

Random numbers play a crucial role in encrypting data securely, especially when creating keys for encryption methods like AES. In simpler terms, think of encryption like locking and unlocking a box. With symmetric encryption, the same key is used to both lock and unlock the box, making it efficient for handling lots of data quickly. On the other hand, asymmetric encryption uses two different keys - one to lock the box and another to unlock it. This adds an extra layer of security but can be trickier to manage. It's like having two different keys for your house - one for the front door and another for the back. While it's more secure, it also means more keys to keep track of.

The story of encryption spans centuries, starting with ancient methods like the Caesar cipher and evolving into the sophisticated algorithms we use today, such as AES, RSA, and ECC. AES, which became the U.S. government's standard encryption method, marks a significant milestone in this journey due to its strong security features and widespread adoption. Asymmetric encryption, like RSA, changed the game by introducing the idea of public and private keys, making secure communication possible even over insecure channels. Nowadays, encryption is vital for cybersecurity, keeping sensitive information safe, ensuring privacy, and guaranteeing that digital messages remain intact. Ongoing research in encryption focuses on staying ahead of new threats, improving the building blocks of encryption, and exploring ways to safeguard data in the age of quantum computing.

## Certificate Generation

Insert a screenshot below of the CER file.



## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated

## Secure Communications

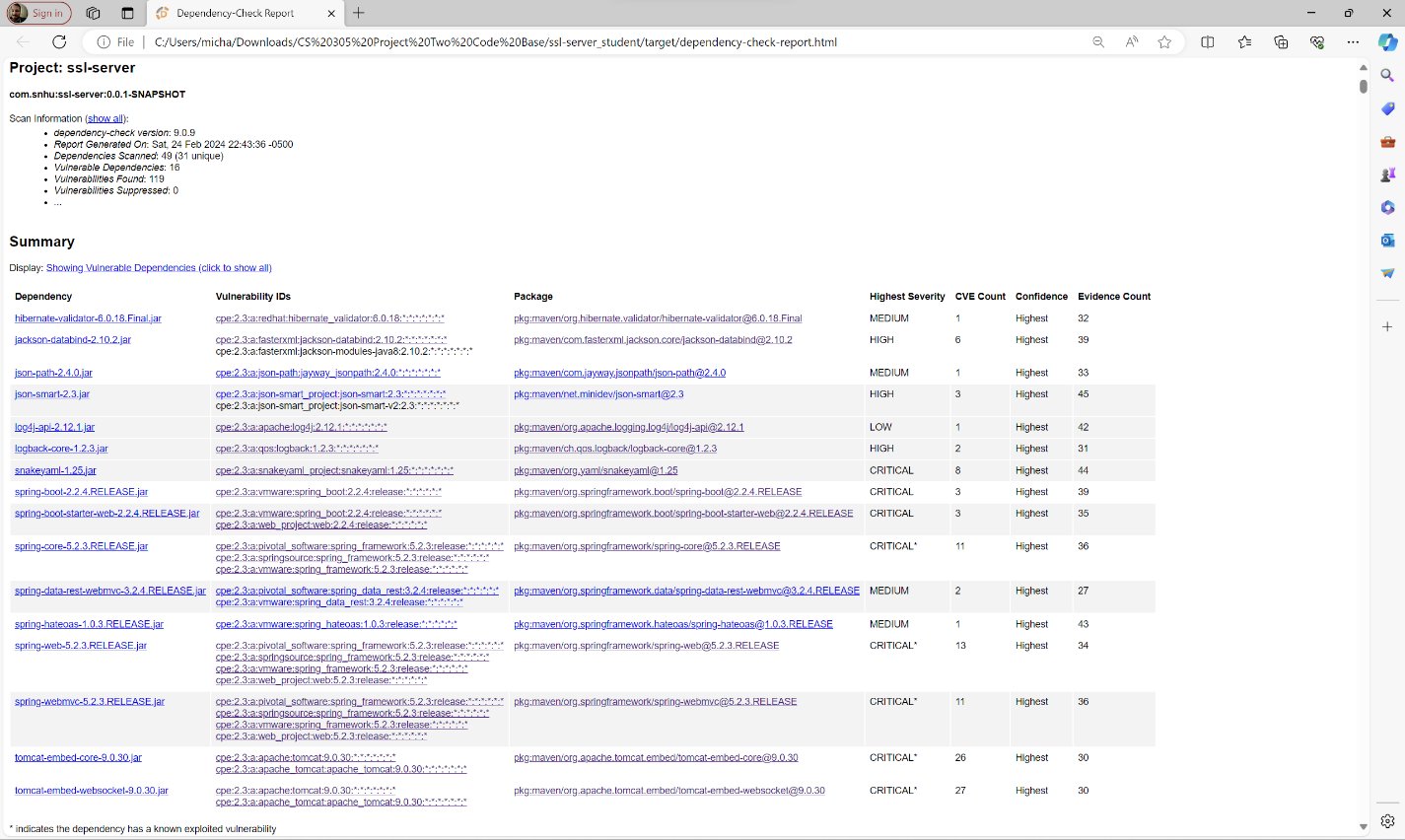
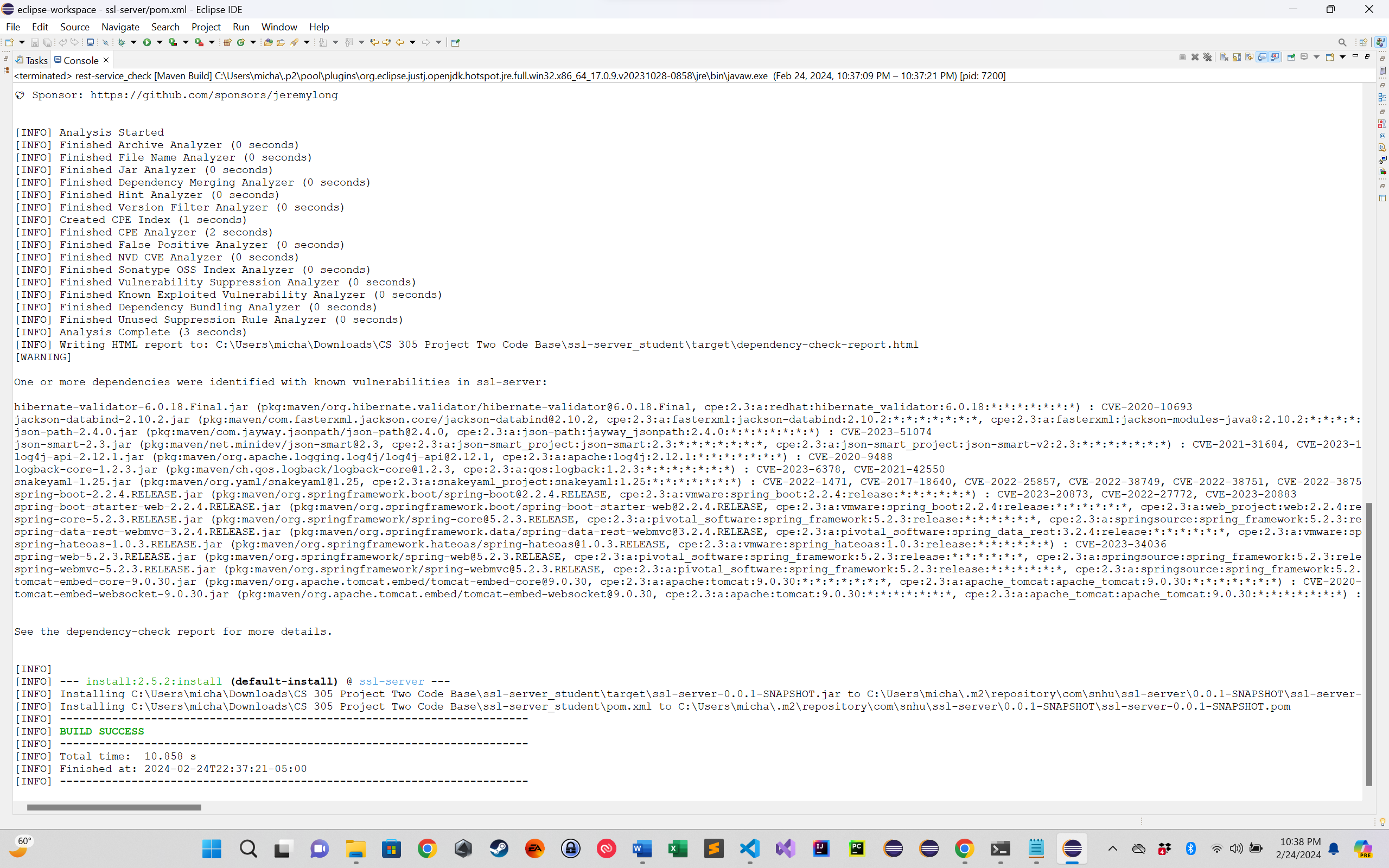
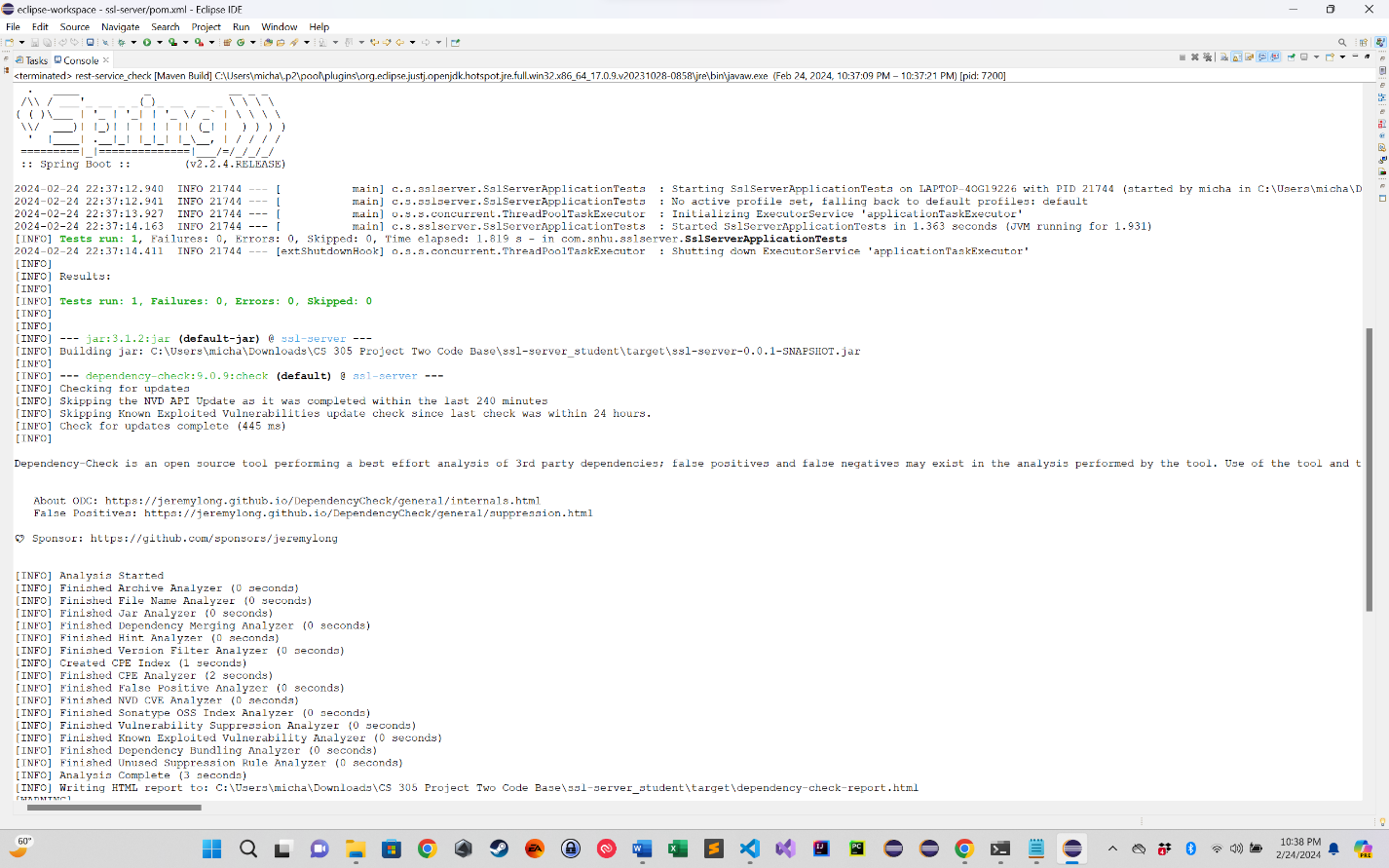
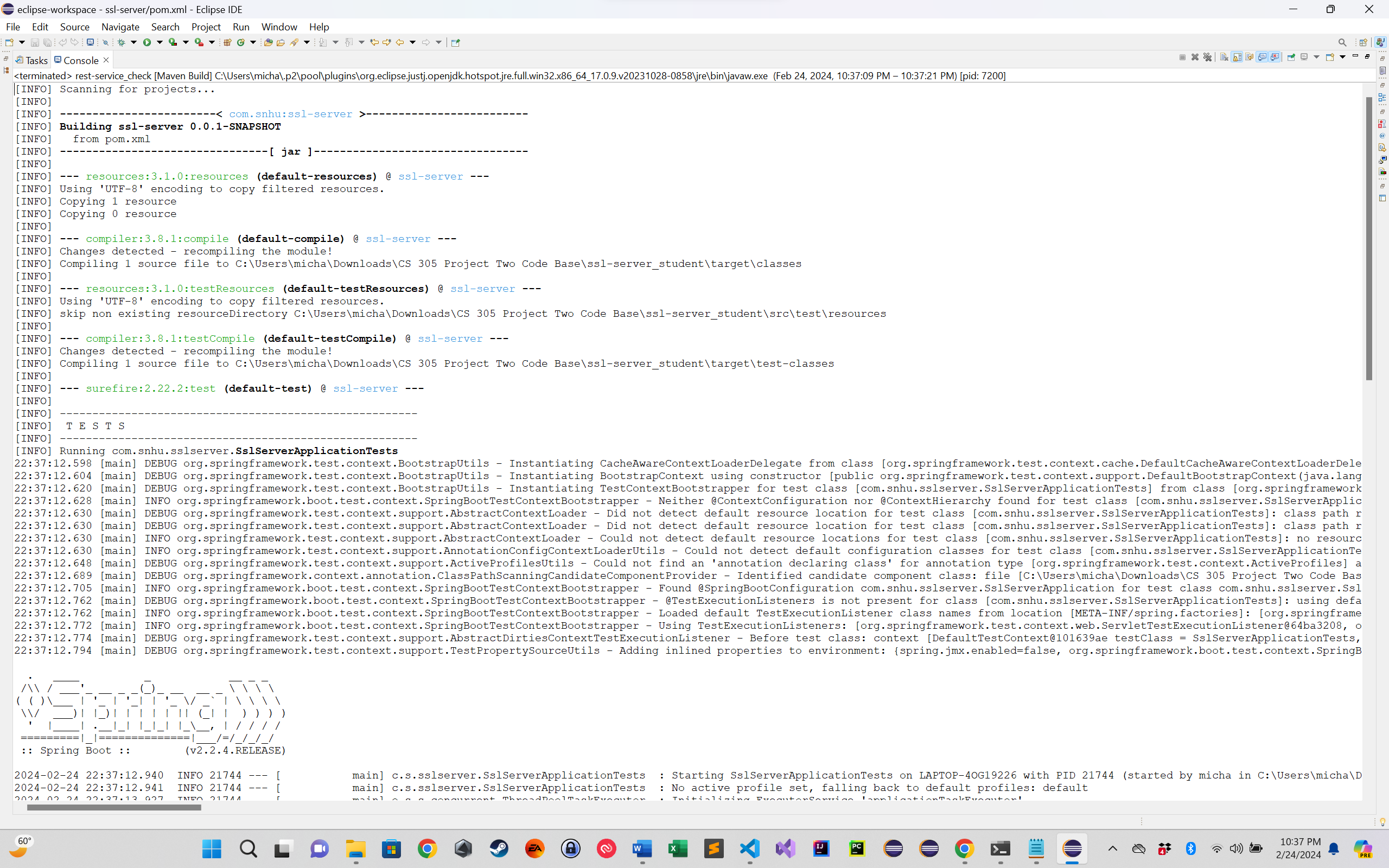
Insert a screenshot below of the web browser that shows a secure webpage.

A screenshot of a computer

Description automatically generated

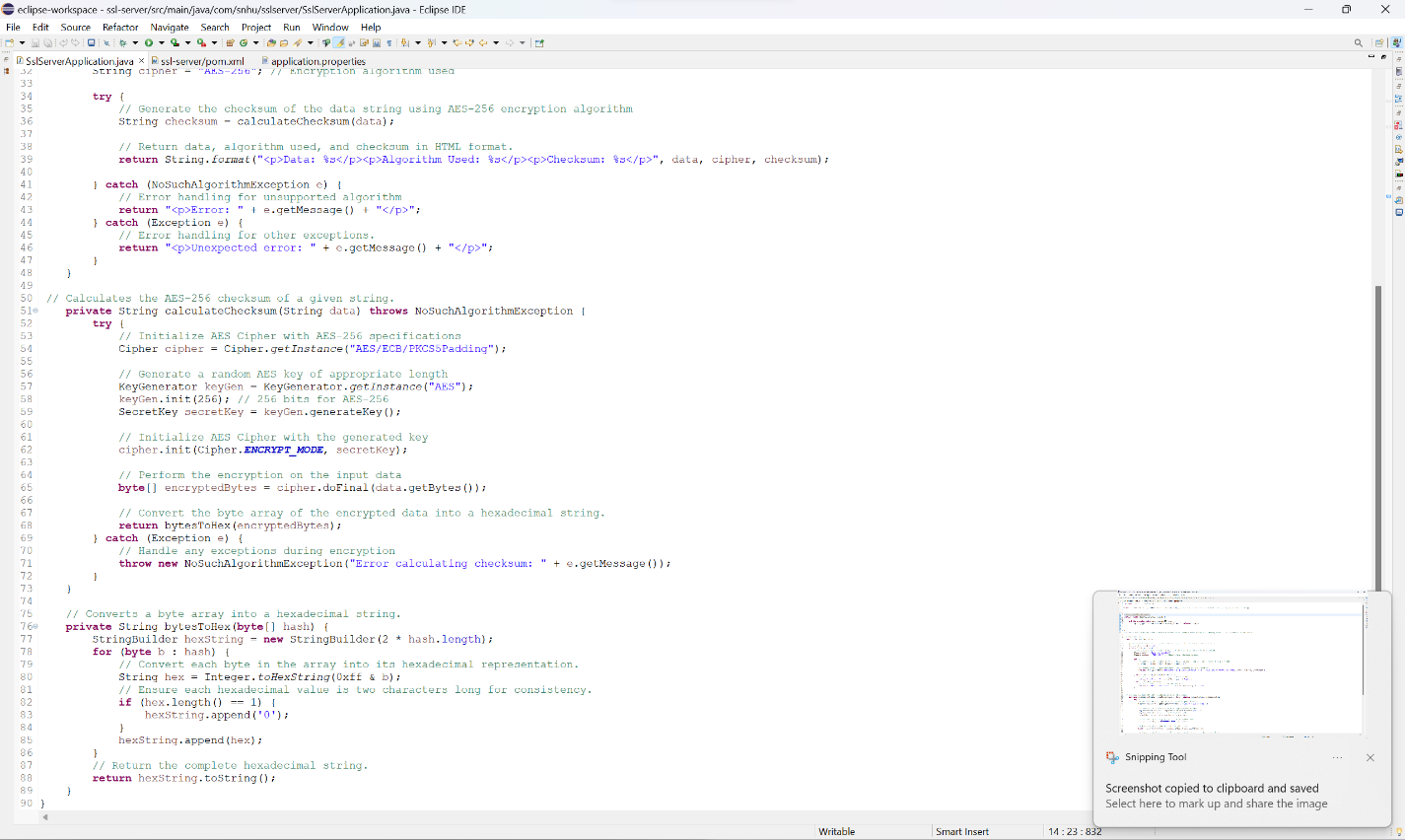
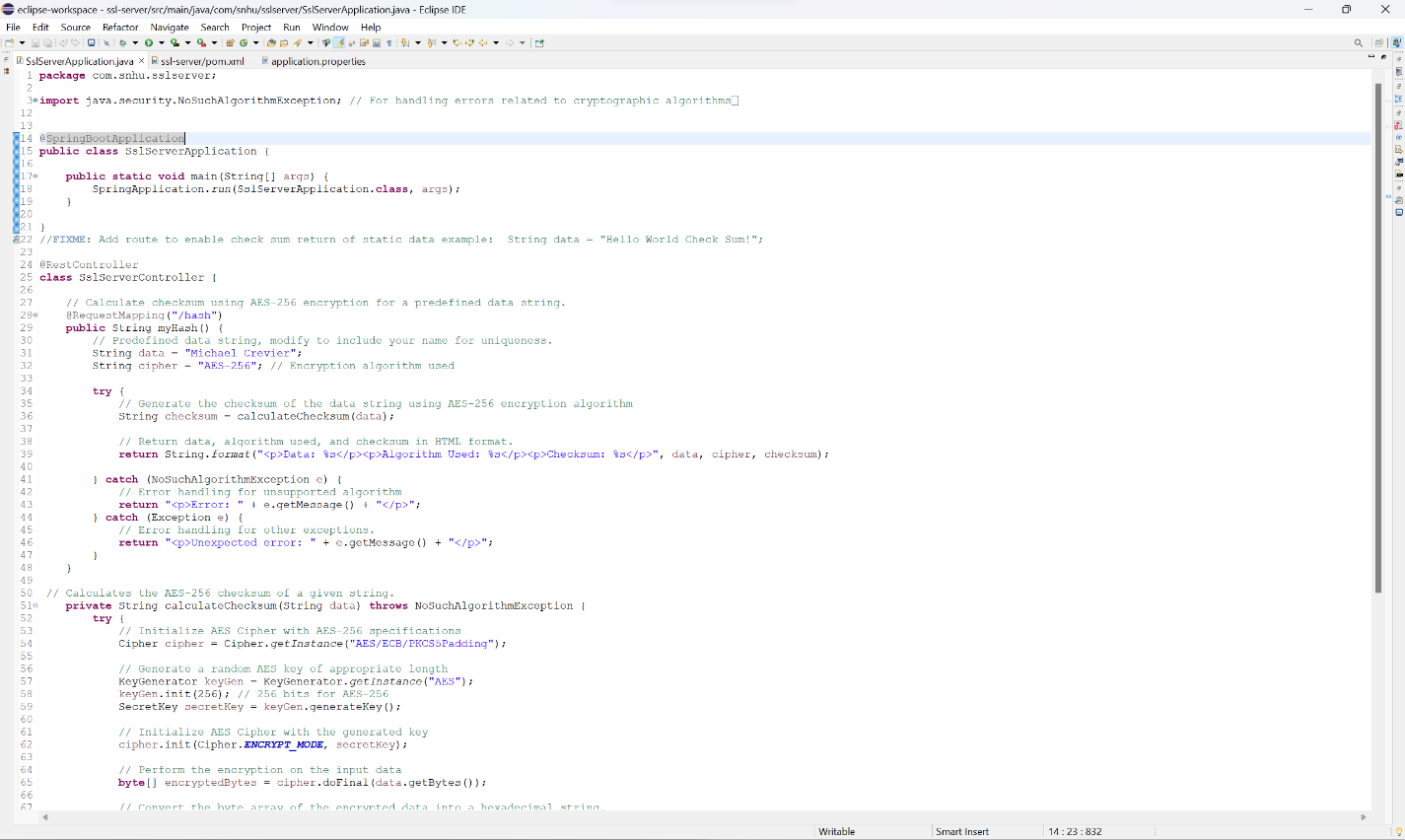
## Secondary Testing

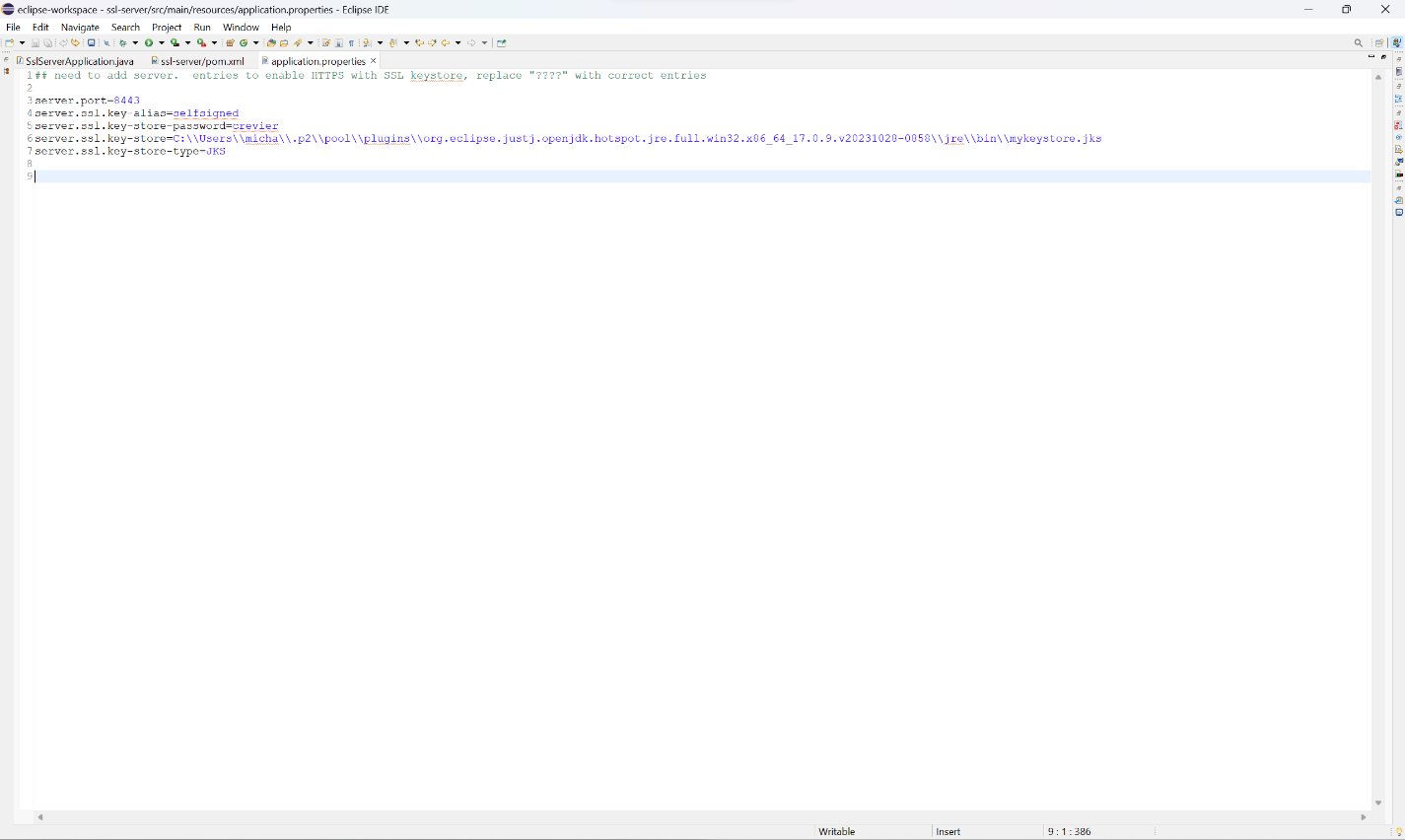
Insert screenshots below of the refactored code executed without errors and the dependency-check report.



## Functional Testing

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





## Summary

During our software's update, we made significant improvements to enhance its security framework, particularly focusing on advanced encryption and secure communication methods. By incorporating AES-256 encryption within a new component of our application designed to manage web requests, we've taken a robust step towards safeguarding sensitive information. This approach aligns with top-tier security practices and emphasizes our dedication to maintaining data confidentiality, making it nearly impossible for unauthorized parties to access. Additionally, transitioning our system's settings from HTTP to HTTPS marks a critical enhancement in securing data as it travels across the internet. This shift ensures that all data transmission is encrypted, dramatically lowering the risk of data being intercepted by malicious actors. Furthermore, these strategic updates not only tighten our software's security measures but also substantially elevate the overall safety and integrity of our data handling processes, providing a more reliable and secure environment for users and stakeholders alike.

Regarding the Vulnerability Assessment Process Flow Diagram, the security enhancements implemented can be mapped onto the diagram to illustrate how each addresses specific vulnerabilities or potential attack vectors. For example, the integration of AES-256 encryption addresses vulnerabilities related to data confidentiality, ensuring that sensitive information remains protected even if intercepted. Transitioning from HTTP to HTTPS addresses vulnerabilities associated with data interception during transit, mitigating the risk of man-in-the-middle attacks. By highlighting these connections, stakeholders gain a clearer understanding of how the security measures align with the identified vulnerabilities and contribute to overall risk mitigation.

## Industry Standard Best Practices

In refining our software, we've diligently applied industry-standard best practices for secure coding to bolster the application's defenses. By implementing AES-256 encryption, we adhere to one of the most widely recognized and recommended security measures for data protection, ensuring that our handling of sensitive information meets the rigorous standards expected in the cybersecurity realm. The transition to HTTPS from HTTP is another critical move, aligning with the universal best practice for securing data in transit. This upgrade encrypts all communication between our servers and clients, effectively shielding it from interception and tampering attempts by external parties. Furthermore, our approach to error handling, which carefully conceals sensitive details from error messages, is directly in line with best practices designed to prevent information leakage that could be leveraged in cyber attacks. These steps, rooted in the current consensus on cybersecurity excellence, directly contribute to a more secure, resilient application. By prioritizing these industry-standard measures, we not only enhance the security of our software but also ensure a safer, more reliable experience for our users, directly impacting the well-being and trustworthiness of our organization.

Adhering to industry-standard best practices for secure coding not only fortifies our software application against potential threats but also contributes significantly to the overall well-being of our organization. By mitigating the risk of data breaches and cyber attacks, these practices safeguard sensitive information, preserve customer trust, and protect the company's reputation. Furthermore, compliance with industry standards and regulations ensures that we meet legal requirements and avoid costly penalties or legal actions. Additionally, by prioritizing security in our development processes, we demonstrate our commitment to providing a secure and reliable product to our users, which ultimately enhances customer satisfaction and loyalty. Overall, investing in industry-standard best practices for secure coding is essential for ensuring the long-term success and sustainability of our organization in an increasingly digital and interconnected world.