

# 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](#_Toc102040759) 6

[3. Deploy Cipher](#_Toc102040760) 7

[4. Secure Communications](#_Toc102040761) 7

[5. Secondary Testing](#_Toc102040762) 8

[6. Functional Testing](#_Toc102040763) 9

[7. Summary](#_Toc102040764) 10

[8. Industry Standard Best Practices 1](#_Toc102040765)1

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| 1.0 | 08/18/2021 | Oleksandra Kondieieva |  |

## 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

Oleksandra Kondieieva

## Algorithm Cipher

Implementing security best practices is essential in defending the Artemis Financial system against various security attacks. After careful consideration of Artemis Financial's possible vulnerabilities and business needs, I recommend using Advanced Encryption Standard (AES) as the company's encryption algorithm cipher. AES is the Federal Information Processing Standard, established by the U.S. National Institute of Standards and Technology (NIST) in 2001 as a specification for electronic data encryption (GeeksforGeeks,2024).   
 AES keys may be vulnerable to brute force attacks, and it is essential to prevent the cryptographic keys from leaking. AES supports 128, 192, or 256-bit keys. I recommend using 256-bit keys to ensure safety. In addition, I suggest using the Rivest–Shamir—Adleman encryption algorithm cipher (2048 or 4096 bits) to encrypt the AES keys.

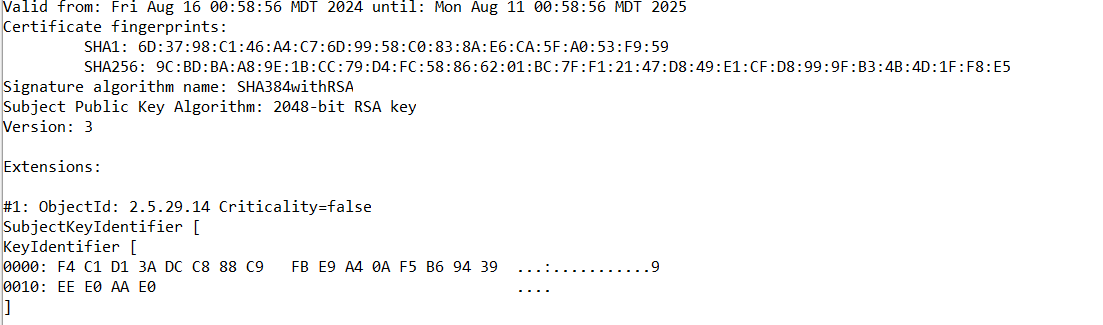
The proposed two-cipher combination will cover the performance of symmetric encryption and the security of asymmetric encryption. Since AES is a type of symmetric encryption (the information is encrypted and decrypted with the same key), the private key for decryption should be sent along with the encrypted data. In order to protect the decryption key when sending, the RSA algorithm cipher will be applied. The sender and the receiver will have public and private keys. The private keys will be used for encryption, and only their private keys can decrypt the data encrypted by the public keys. The information from the sender will be encrypted using AES ciphers. The private key that must be sent to the receiver for decryption will be encrypted using the RSA technique. The receiver's public key will encrypt the AES private key. The encrypted data, along with the encrypted key, will be sent to the receiver. At this time, the receiver can decrypt the AES key using the private RSA key. After decryption of the AES key, the data can be decrypted.   
 One reason that the most secure ciphers are not proposed is the performance issues and the amount of data. As a standard, AES can manage big chunks of data without losing performance. On the other hand, the asymmetric ciphers that are considered the most secure are limited in the amount of data they can encrypt and are slower in performance.

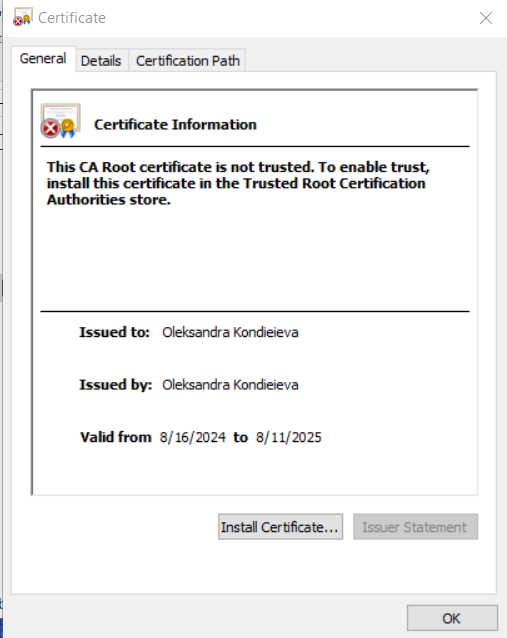
One of the ways cipher ensures that data that was sent hasn't been altered after sending is by using the hash function. A sender creates a hash (unique code) after creating a message. The message, together with the code, is sent to the receiver. Like in the sender case, the receiver hash function takes the message as an input and generates a unique code. The message is original if the received and produced codes are the same. Even the slightest change in the message will result in generating a completely different hash.  
 Bit levels in the cipher ensure the security of the generated key. For example, the AES cipher algorithm can use 128, 192, or 256-bit keys. At the same time, RSA keys can be 2048 or 4096 bits. The longer the key, the more secure it is and less prone to brute-force attacks. That being said, using longer keys will result in losing performance time since they take longer to compute.  
 Cipher algorithms use different techniques to ensure the security of information. One of these techniques is using random numbers to ensure the creation of unique and strong keys.  
 There are two types of keys in cryptography – symmetric and asymmetric. As I mentioned before, it is essential to meet business needs and ensure the best possible security level for data protection. The same key is used for encrypting and decrypting data in asymmetric encryption. Thus, the key must be sent to the receiver with the encrypted information to decrypt it. In the case of asymmetric encryption – the public and private keys are used. Both a sender and a receiver generate both keys. A sender will use the receiver's public key to encrypt the information that can only be decrypted by the receiver's private keys. In this case, the private key doesn't need to be sent over the network, which results in better security but slower performance.

Encryption algorithms have evolved throughout the years, from the first cipher machines to the current AES/RSA cipher algorithms. Likewise, encryption techniques, the type of security attacks, and the technologies that attackers possess have been improving as well. Thus, it is important to implement the best security practices and stay on top of the new security technologies. Only constant monitoring and implementation of security techniques will mitigate the risk of possible attacks.

## Certificate Generation

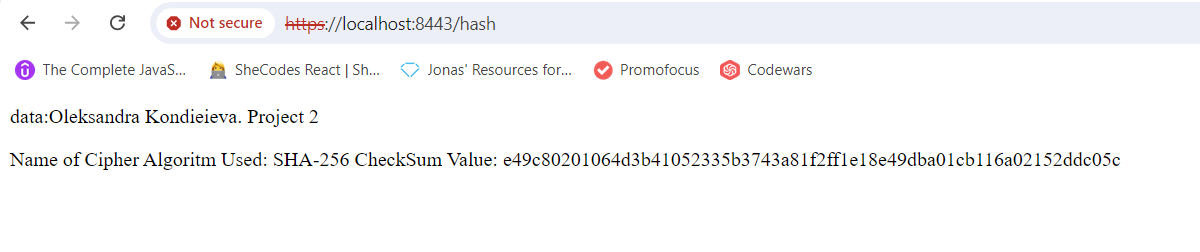
Insert a screenshot below of the CER file.





## Deploy Cipher

Insert a screenshot below of the checksum verification.



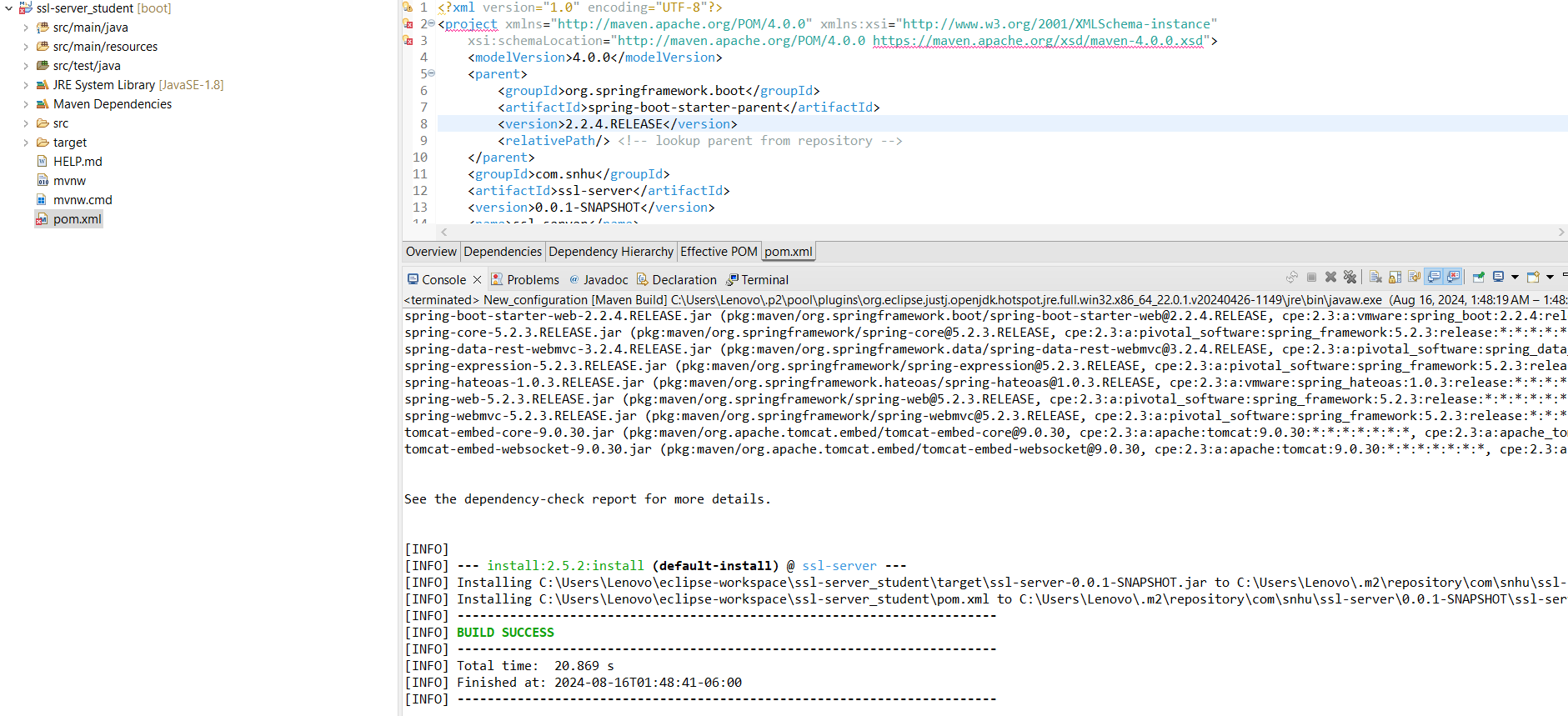
## Secure Communications

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

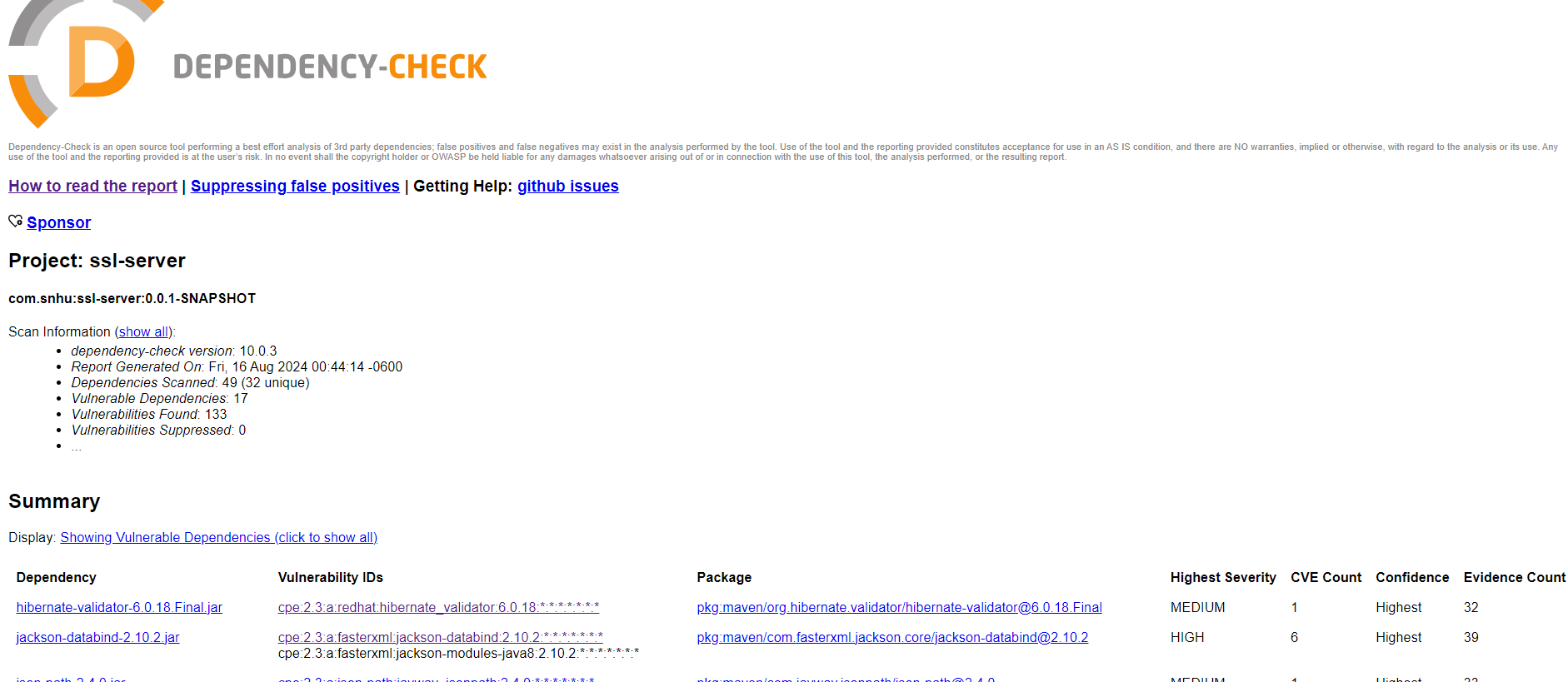
## 

## 5. Secondary Testing

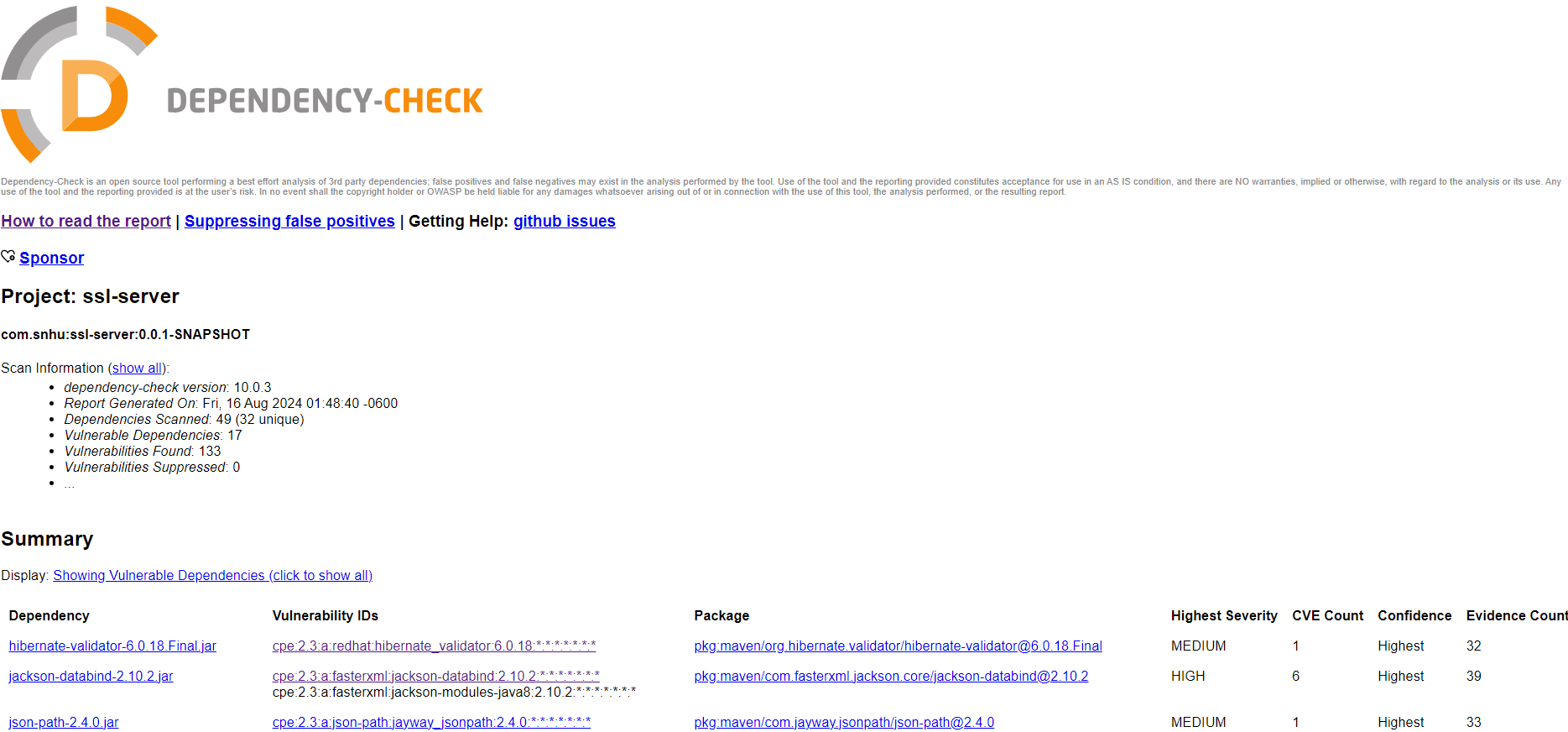
Insert screenshots below of the refactored code executed without errors and the dependency-check report.



The dependency check report before refactoring:

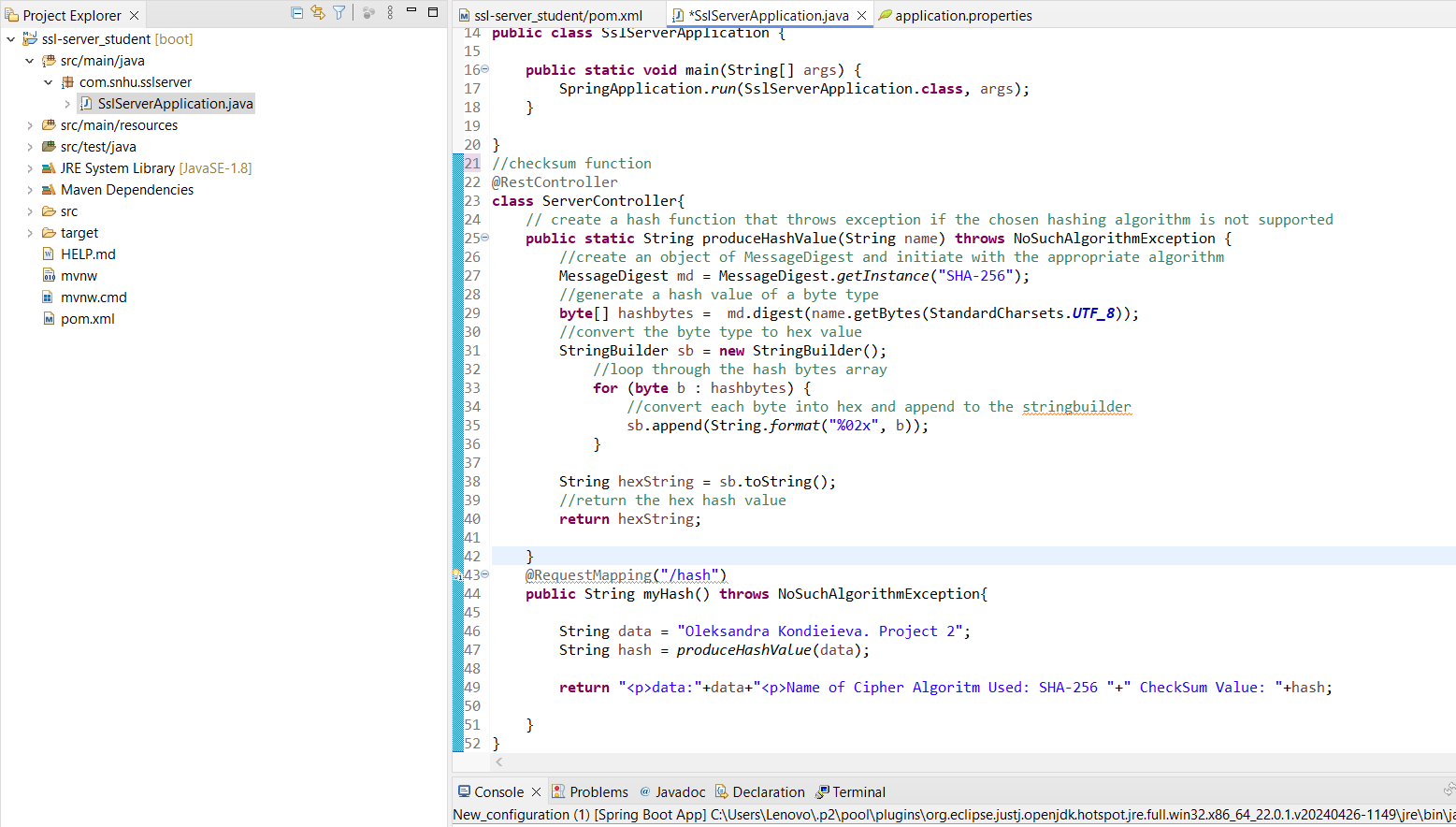


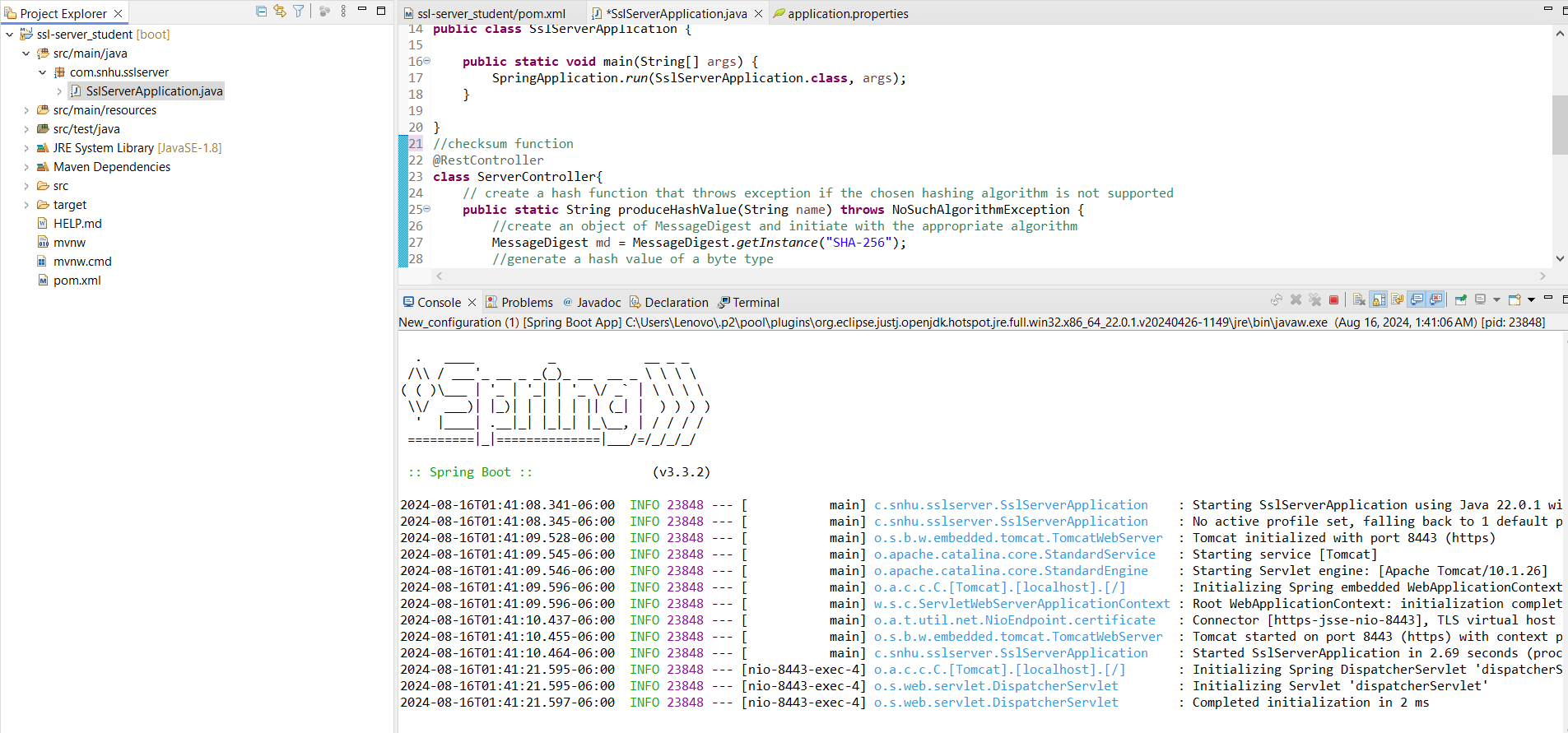
The dependency check report after refactoring:



## 6. Functional Testing

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





## 7. Summary

While working on the ArtemisFinancial website and addressing security vulnerabilities and possible threats, the code was refactored to follow the best industry practices. Considering the vulnerability assessment process flow diagram, the security areas assessed were cryptography and code quality. The hash function was implemented using a secure hash algorithm- SHA-256. By generating unique hash values for different data sets, hashing ensures data integrity. Implementing encryption cipher algorithms and cryptographic hash functions adds security layers to the software, making it less prone to possible security attacks. By providing a 256-bit value, SHA-256 limits possible collisions and improves performance time. SHA-256 is a one-way function that makes it almost impossible to reverse in order to retrieve the original message.  
 The secure connection was also established by generating a self-signed certificate of authority. The main goal of the CA is to verify the server/website/organization so that users can be sure about who they communicate with and if the data from a particular website can be trusted. Since Artemis Financial will be handling a lot of personal information and sensitive data, it is essential to establish a chain of trust to establish secure communication and authenticate other entities that will be used in the process. According to the regulatory requirements, financial institutions should protect customer data. A certificate of authority plays a significant role in data protection and communication security.  
 Another level of application security is dependencies. I generated dependency-check reports to find vulnerable dependencies that the project is based on, ways to eliminate them in the future, and workarounds to mitigate the risk of security threats.

## 8. Industry Standard Best Practices

To maintain the application's existing security, I regularly checked the code after refactoring for any warnings. I also ran additional dependency-check reports to see if new vulnerabilities appeared. I refactored code in small iterations, understanding the problem, designing, implementing, and testing. This approach helped me incorporate best industry practices.  
 Implementing industry-standard best practices for secure coding brings significant benefits to ArtemisFinancial. A secure application is a running and trusted application. Using cybersecurity best practices mitigates the risks of possible attacks, protects sensitive data, boosts the company's reputation, and attracts more clients by presenting itself as a trustworthy business. This also reduces the cost of dealing with possible future attacks by addressing them early in the software development life cycle. Implementing encryption cipher algorithms and cryptographic hash functions adds security layers to the software, making it less prone to possible security attacks. Applying industry best practices ensures that the company complies with the regulations in its business field.

REFERENCES:

Awati, R., & Loshin, P. (2021, September 1). *What is a Certificate Authority (CA)?*. Security. https://www.techtarget.com/searchsecurity/definition/certificate-authority

Baeldung, W. by: (2024, May 11). *SHA-256 hashing in Java*. Baeldung. <https://www.baeldung.com/sha->256-hashing-java

GeeksforGeeks. (2024, July 16). *Advanced encryption standard (AES)*. [https://www.geeks](https://www.geeks/) forgeeks.org/advanced-encryption-standard-aes/

Crane, C. (2023, May 25). *What is a hash function in cryptography? A beginner’s guide*. Hashed Out by The SSL StoreTM. <https://www.thesslstore.com/blog/what-is-a-hash-function-in-> cryptography-a-beginners-guide/#:~:text=Hash%20functions%20are%20a %20way,a %20means%20of%20identity%20verification.

Java Security Standard Algorithm Names. (n.d.). https://docs.oracle

Rimkienė, R. (n.d.). *What is AES encryption and how does it work? | Cybernews*. What is AES encryption and how does it work? <https://cybernews.com/resources/what-is-aes-> encryption/ .com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm- names

Singh, A. (n.d.). *Difference between AES and des ciphers*. Shiksha . [https://www.shiksha](https://www.shiksha/). com/online-courses/articles/difference-between-aes-and-des-ciphers-blogId- 158769#:~:text=The%20main%20difference%20between%20AES,attacks%20using %20modern%20computing%20power.