****

# 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** | **8/21/24** | **Dathan Pompa** |  |

## Client



## Developer

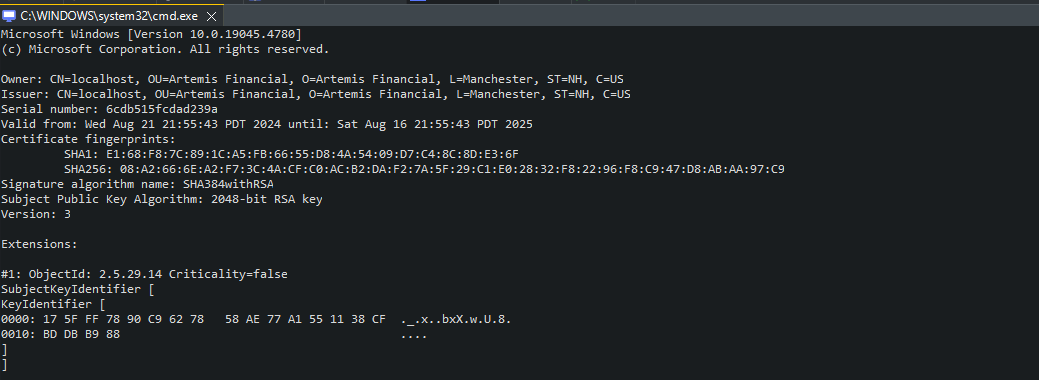
Dathan Pompa

## Algorithm Cipher

Artemis Financials software should have an AES encryption as my recommendation.

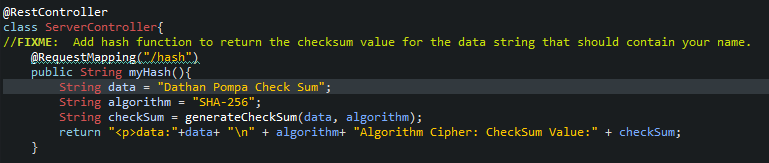
It’s a symmetric key cipher, utilizes the same key for decrypting and encrypting. It has various bit levels, but I recommend using 256. It creates random numbers and letters so that encryption keys are unique always. AES has been the standard after it replaced DES. AES was introduced in 2001 and has repelled cryptanalysis since.

## Certificate Generation



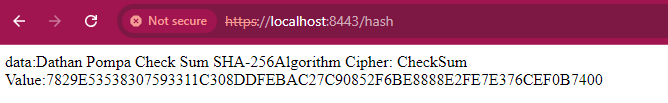
## Deploy Cipher

Insert a screenshot below of the checksum verification.

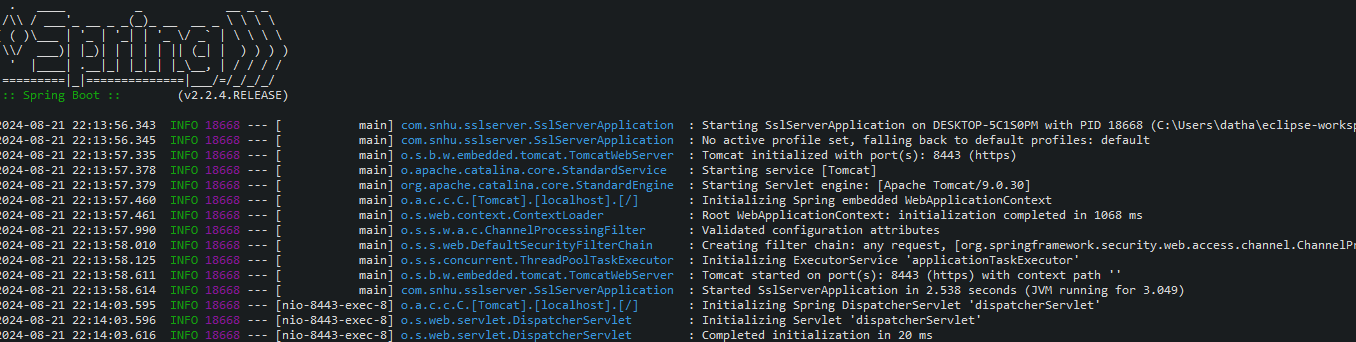


## Secure Communications

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

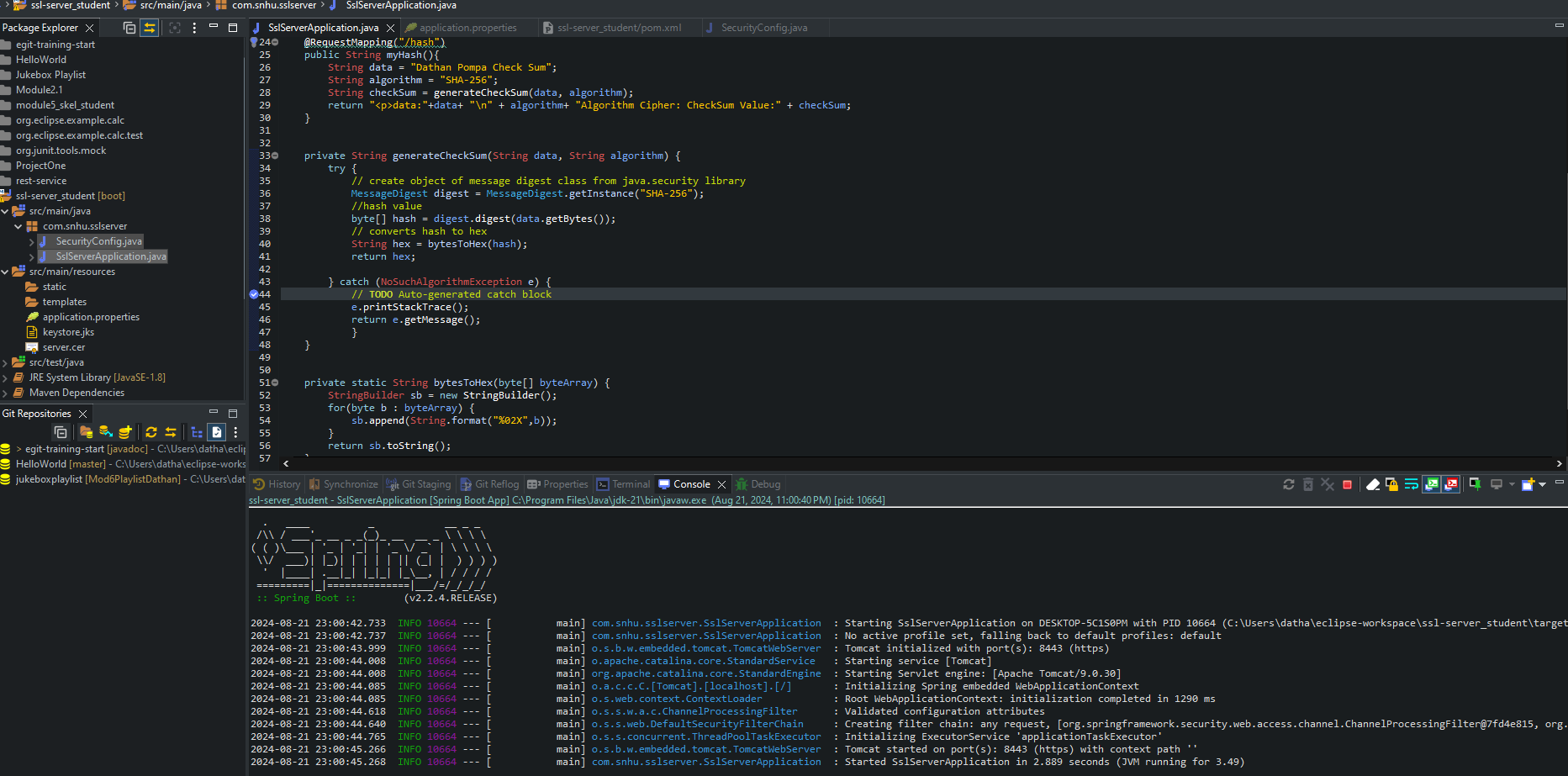


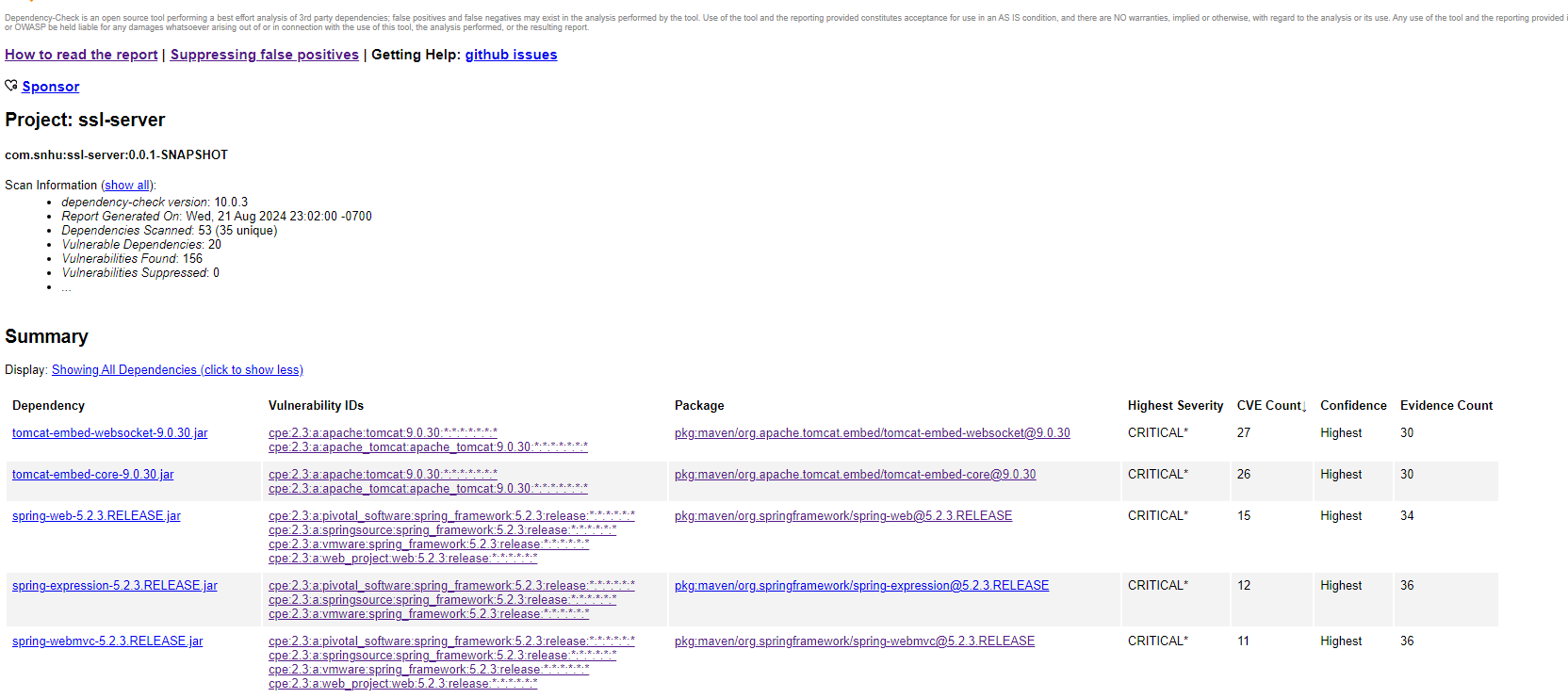
It says not secure because I did not import my created certificate into my browsers trusted store, but it is launched with https.



## Secondary Testing

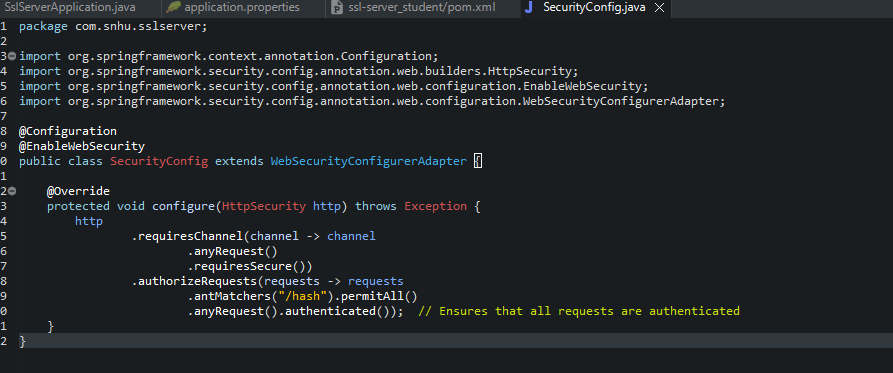
Insert screenshots below of the refactored code executed without errors and the dependency-check report.

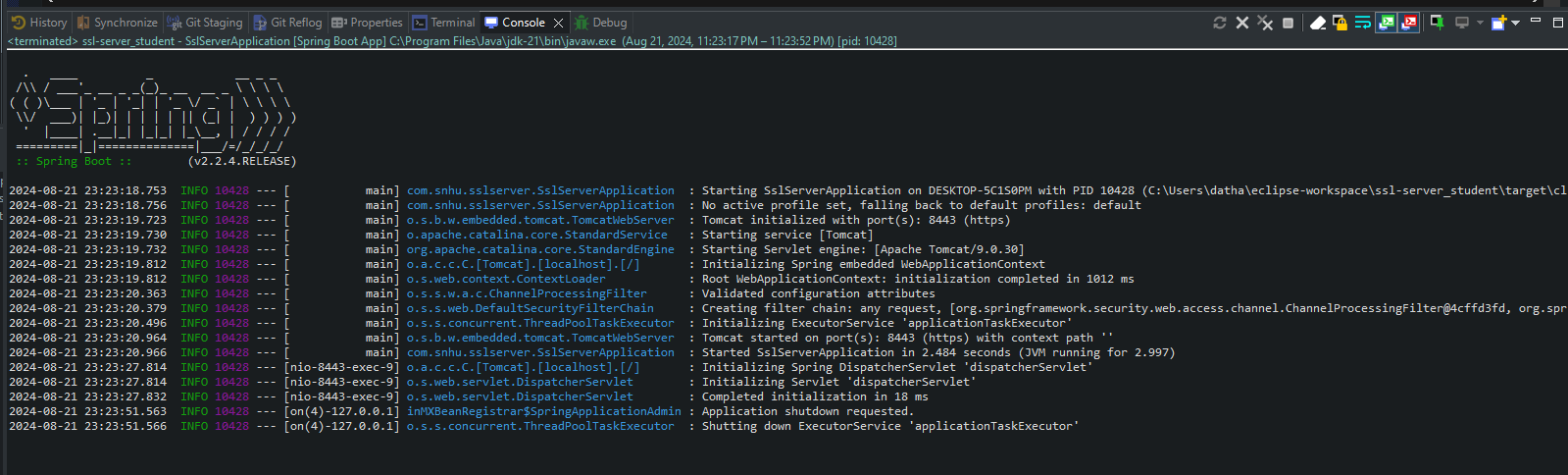




## Functional Testing

In my application.properties file I removed the security.require-ssl line because it has been deprecated. I instead created my own websecurityConfigurer using lambda expressions.





## Summary

My application was refactored to enforce https communications. This made sure that all data being sent to client and server is encrypted. I used a checksum verification with a SHA 256 hash algorithm that made sure that data is securely transmitted. I also created a security configuration because of the deprecated security.require-ssl property. This configuration enforces authentication in all requests and allows /hash endpoint into the whitelist.

Checking the dependency report, I was able to find some critical information. The critical vulnerabilities are jackson databind, Log4j, spring framework, and tomcat. Some key actions that I have taken were to update the dependencies when I could. I also used input validation so that I can enhance my security configuration.

My layers of security involved adding https. This was the first layer because I made sure all communication between client and server are encrypted data in transit to one another. I enforced authentications for all requests so that unauthorized users cannot access resources. The last was my checksum generation made sure that any tampering of data when being transmitted is found.

## Industry Standard Best Practices

I made sure I applied industry standard best practices in my software by encrypting data during transmission. This means I enforced https which follows best practices for secure communication. I applied dependency management which lets us see third party libraries and their known vulnerabilities. It allowed me to update those that needed to and made me more aware of current threats in my software. I used a hashing algorithm SHA 256 for the checksum generator which will follow the best practices for cryptographic hashing. I made a modular security configuration which lets me know what security settings are in place for my software. This promotes modular design and enhances the software's maintainability. I maintained the security problems introduced before and after refactoring. I updated my dependencies as much as possible as well. Some values of apply industry standards are enhancing security, making sure compliance is met, and improving trust amongst others. Enhancing security will make sure that data risks are reduced, I am ensuring that communications between server and client are secure, and I enhanced our data integrity. I had to make sure this software complied with requirements that handle sensitive financial information. Being able to improve the users' trust is important to everyone. This leads to a company's success and reputation.