****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_1tnh8tqpdzzq)

[**Client 3**](#_ik5g3hkb10s8)

[**Instructions 3**](#_6k0u14ij35oq)

[**Developer 4**](#_2873p54nnwjw)

[**1. Algorithm Cipher 4**](#_i6l6lahugp1t)

[**2. Certificate Generation 4**](#_3jmlro7n6d4f)

[**3. Deploy Cipher 4**](#_mnc1bgiz4d42)

[**4. Secure Communications 4**](#_6vpovpl2ple7)

[**5. Secondary Testing 4**](#_lcflk9judixo)

[**6. Functional Testing 4**](#_4ibywxoy8vci)

[**7. Summary 4**](#_c5min3fxebxm)

[**8. Industry Standard Best Practices 4**](#_byqmsugoa323)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **6-22-25** | **Zach Shires** |  |

## 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

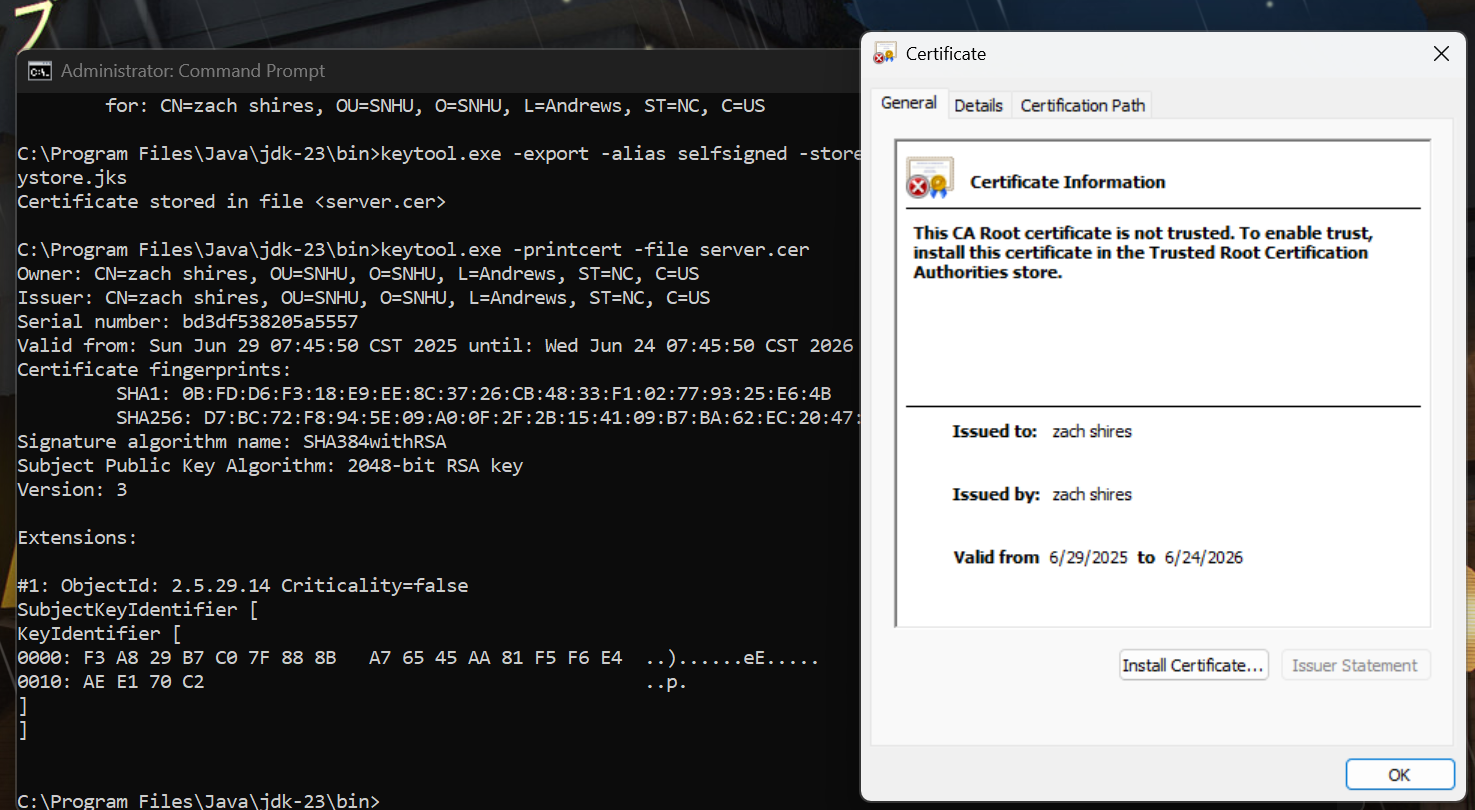
Zach Shires

## Algorithm Cipher

The algorithm cipher I recommend deploying is the AES encryption algorithm. It is a symmetric block cipher consisting of 128-bit blocks, and there are three different key sizes of 128, 192, and 256 bits. Since it is symmetric, the same secret key is used for both encryption and decryption. By itself, AES is deterministic, so the same key and plaintext always produce the same ciphertext. This can introduce a predictability problem, so to overcome this, it uses random numbers to ensure that if someone were to encrypt the same message twice, they would still get different outputs. To describe its history, it was created by both the NIST and the broader community roughly 25 years ago. They hosted a competition to see who could create a new standard that would resist the technological advancements in the century to come, as previous standards were becoming brute-forceable.

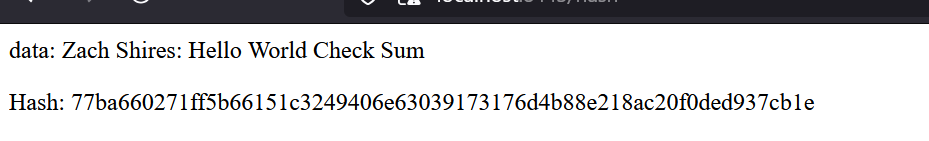
## Certificate Generation

Insert a screenshot below of the CER file.



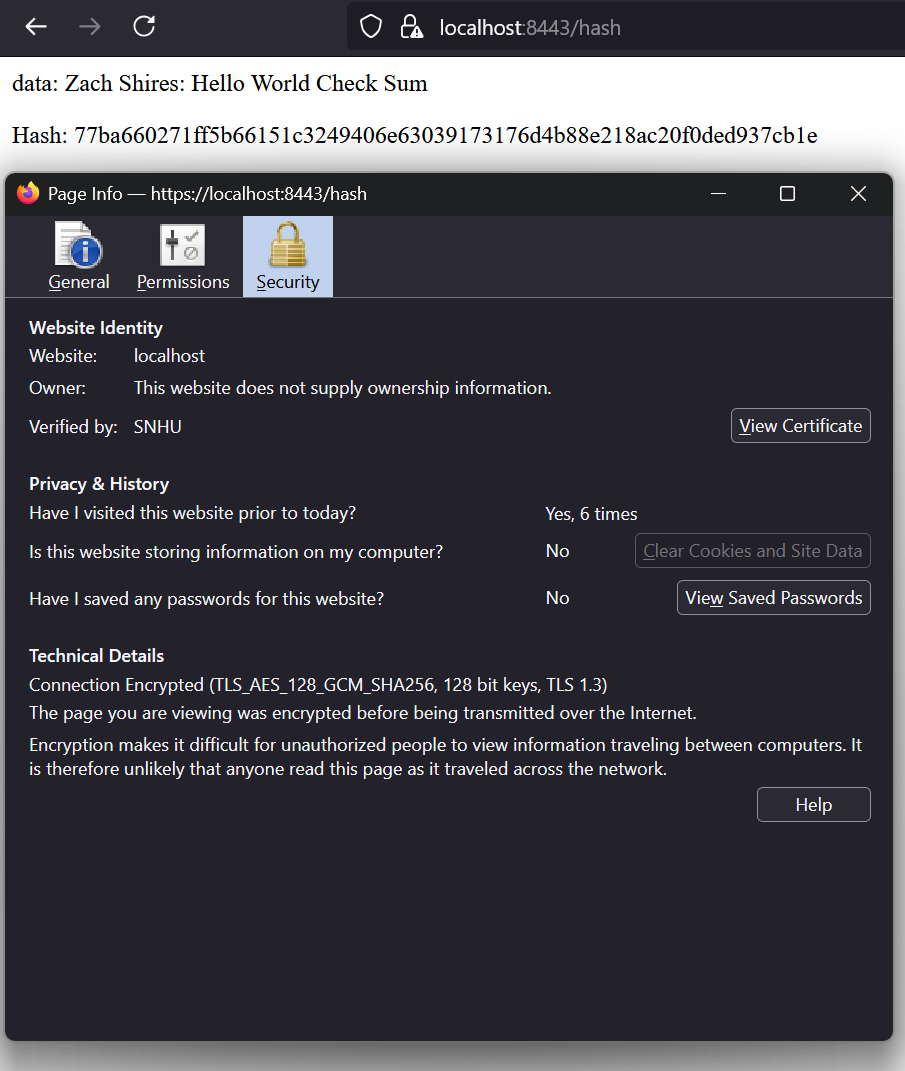
## Deploy Cipher

Insert a screenshot below of the checksum verification.



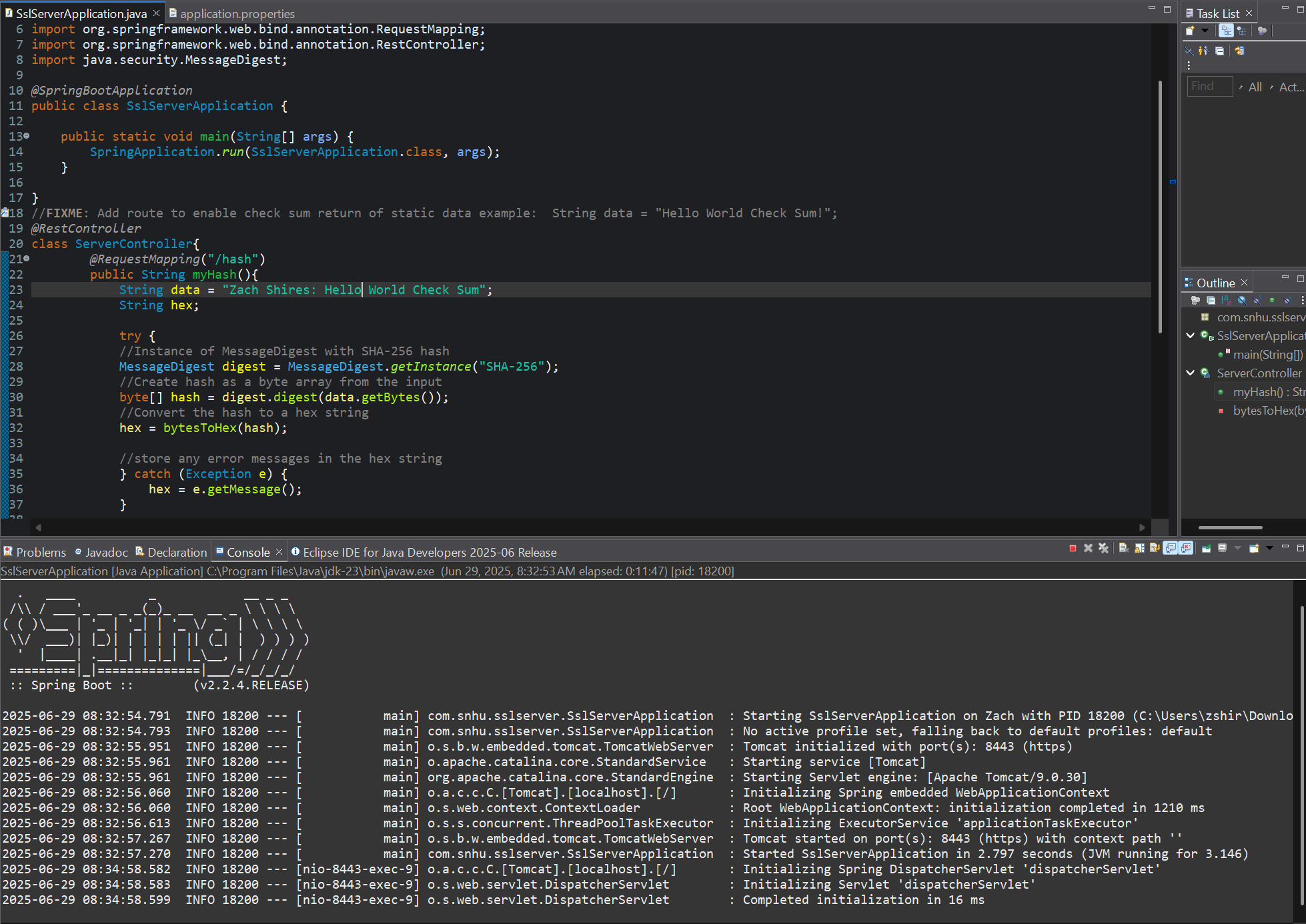
## Secure Communications

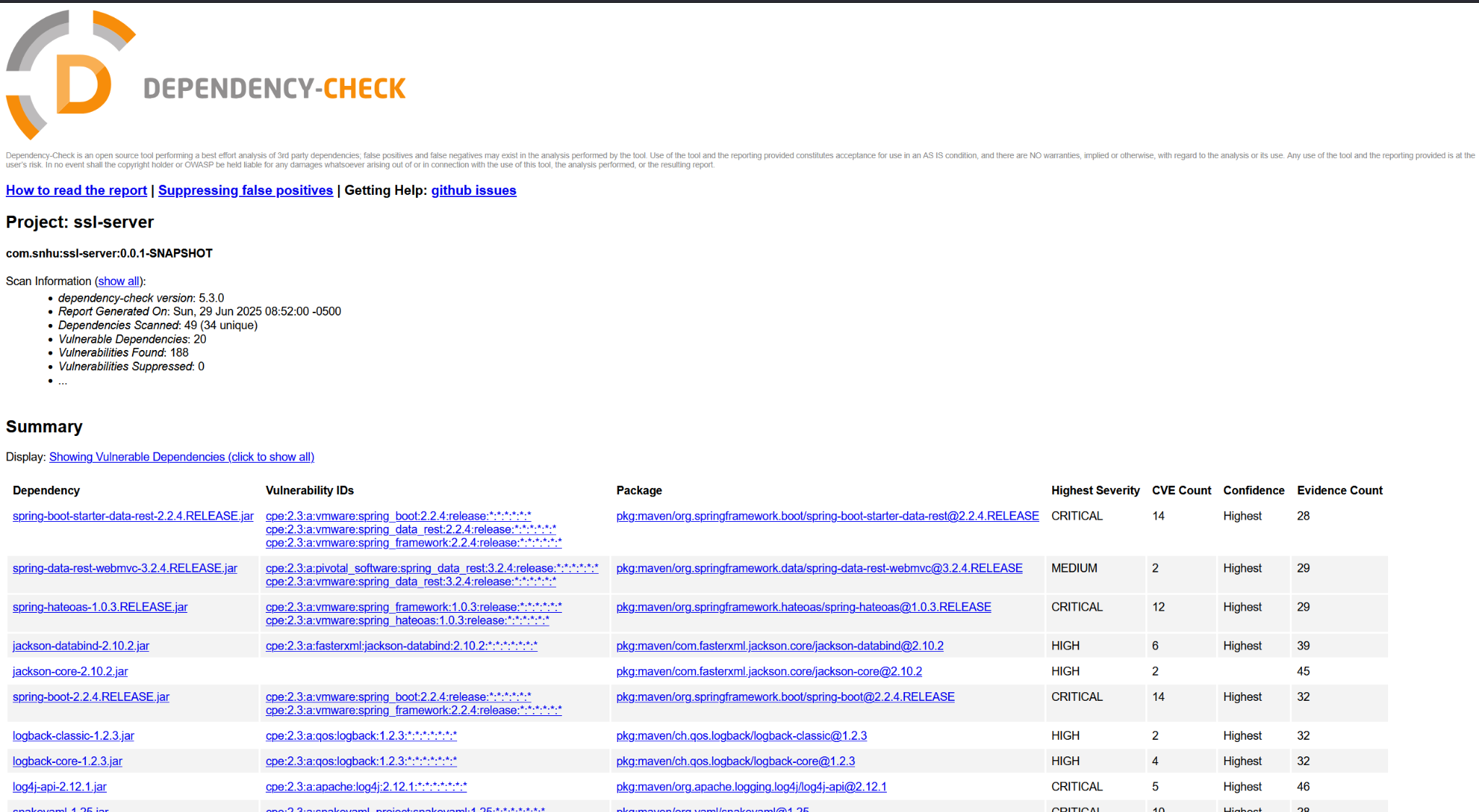
Insert a screenshot below of the web browser that shows a secure webpage.



## Secondary Testing

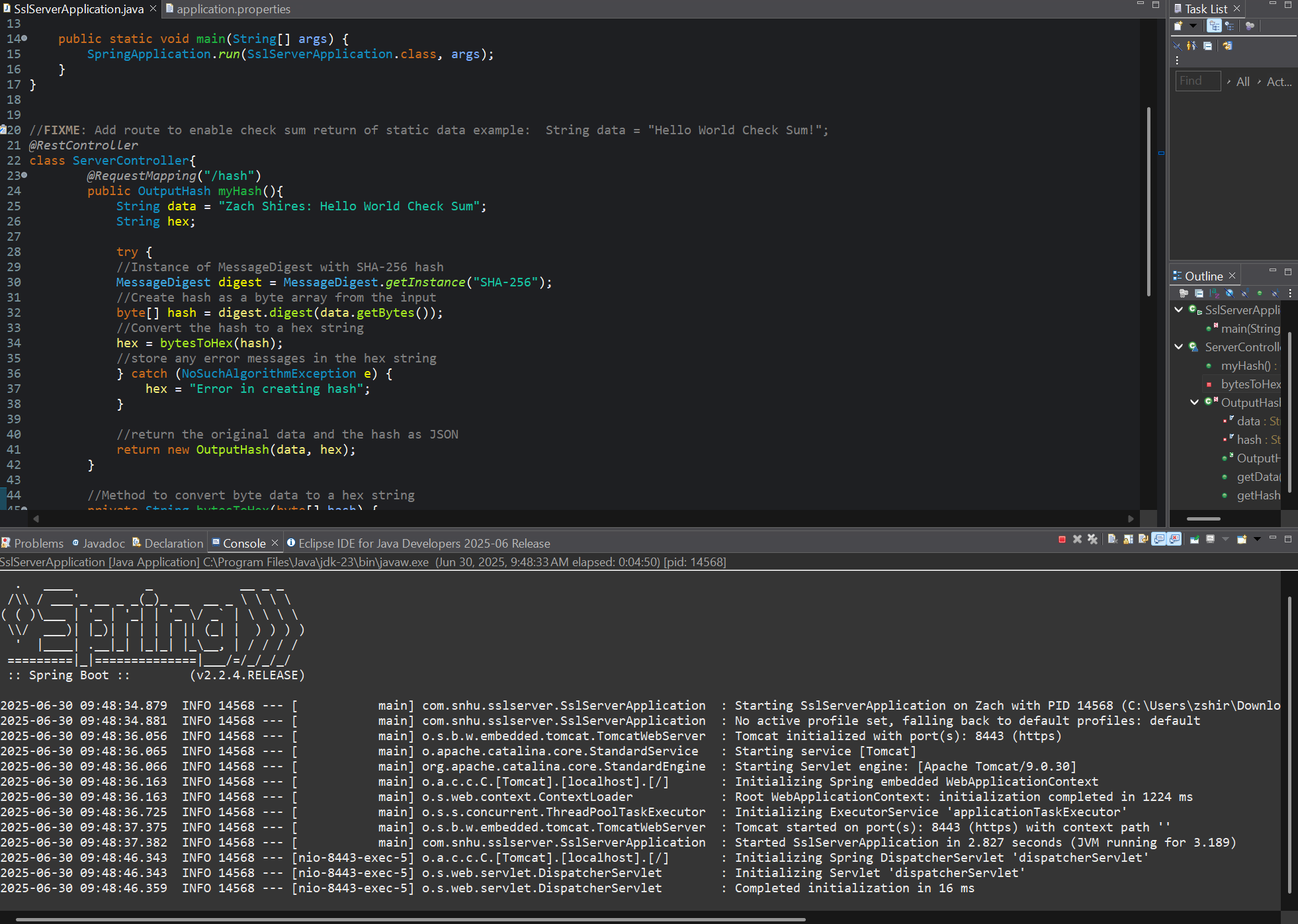
Insert screenshots below of the refactored code executed without errors and the dependency-check report.





## Functional Testing

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



## Summary

The areas of security I addressed were cryptography, code errors, APIs, and encapsulation. I started by implementing an encryption algorithm cipher, where data is hashed to a unique 256-bit string. The webpage was also secured by configuring the webpage to deliver content over HTTPS via enabling SSL with a self-signed certificate. In the functional testing step, I identified additional potential security vulnerabilities. The program was leaking internal exception messages, so I changed the error message to a generic error. I also encapsulated the data in a response object that outputs JSON instead of raw HTML, preventing potential cross-site scripting attacks.

## Industry Standard Best Practices

To maintain the program's existing security, I used the following best practices: HTTPS instead of HTTP, input and output handling, the SHA-256 cryptographic algorithm, and secure REST APIs. Applying these best practices for Artemis Financial is crucial, as the data is at high risk of a variety of attacks and exploits. By applying them, we keep the data secure from any breaches. These practices are also necessary to comply with the financial industry regulations put in place, avoiding potential legal penalties.