****

# 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** | **[Date]** | **[Your Name]** |  |

## 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.

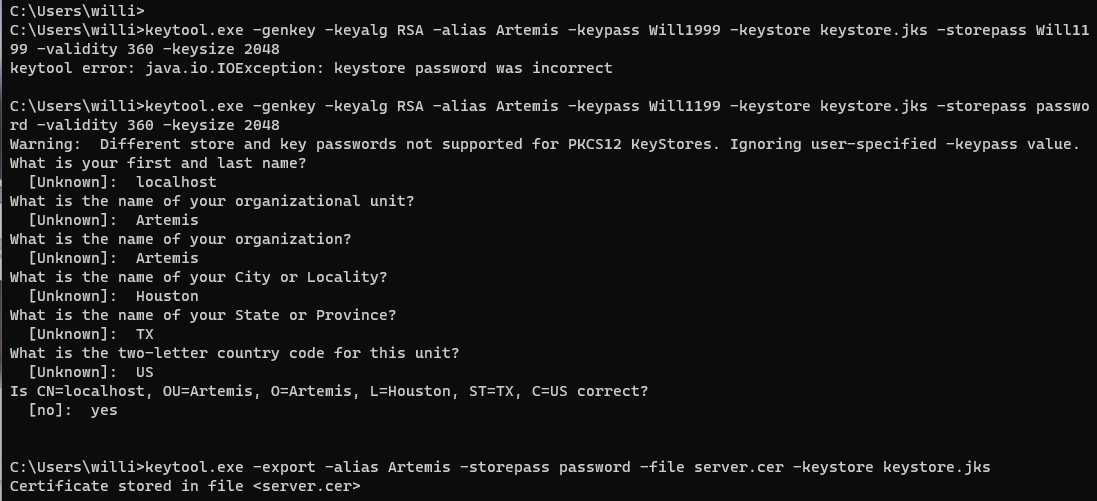
## Developer

William Page

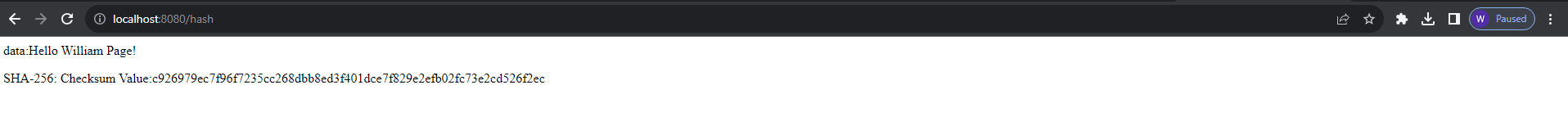
## Algorithm Cipher

Considering the security requirements of Artemis Financial the most suitable encryption algorithm cipher to deploy for their web application is SHA-256. SHA-256 is a cryptographic hash function that generates a fixed-size hash value of 256 bits from variable-length input data. This hash value serves as a digital signature for the data, ensuring its integrity and authenticity. It is known for its ability to handle diverse data lengths, while consistently producing a 256-bit hash output. While not directly using random numbers, SHA-256 plays a vital role in secure communications by generating checksums for transferred data. It acts as a verification mechanism. Unlike encryption algorithms, SHA-256 does not involve keys, making it suitable for data verification purposes. The financial sector has adopted SHA-256 due to its resistance against cryptographic attacks. Its continued use in various financial systems attests to its reliability. Overall, SHA-256 is perfect for the needs of Artemis Financial which is why it has been implemented into the refactored code.

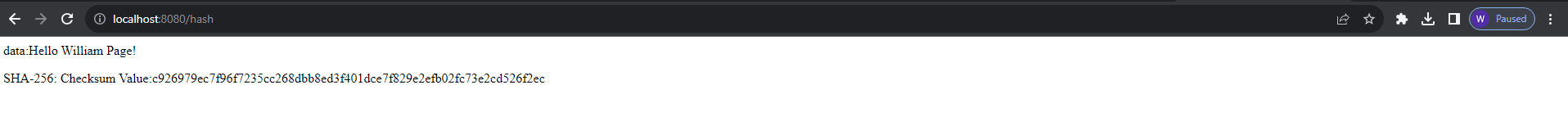
## Certificate Generation



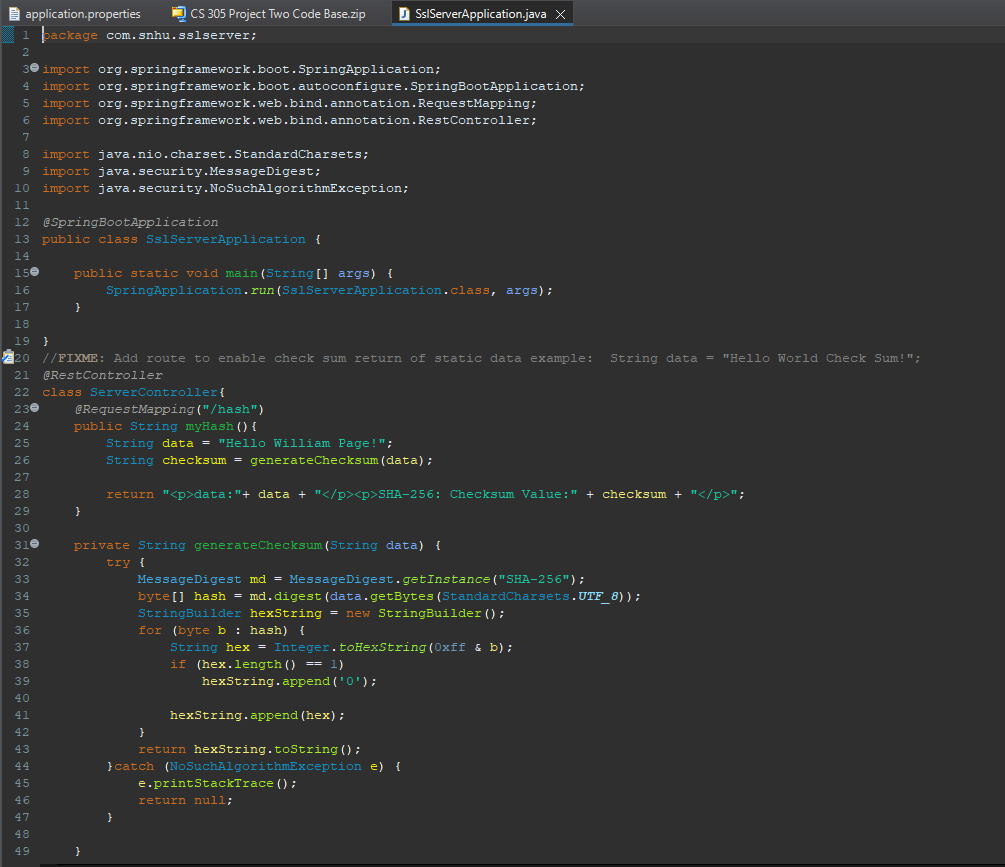
## Deploy Cipher

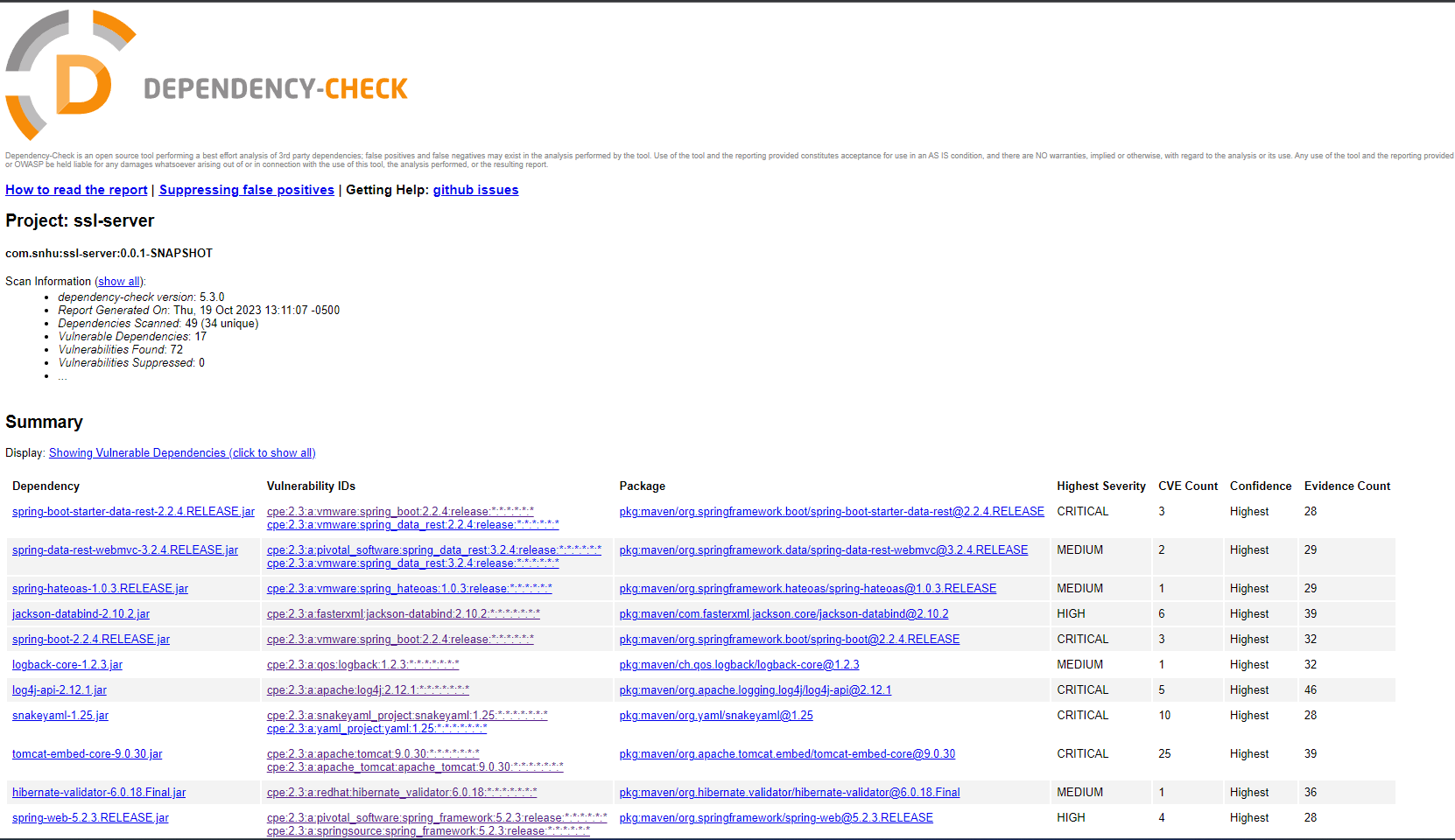


## Secure Communications

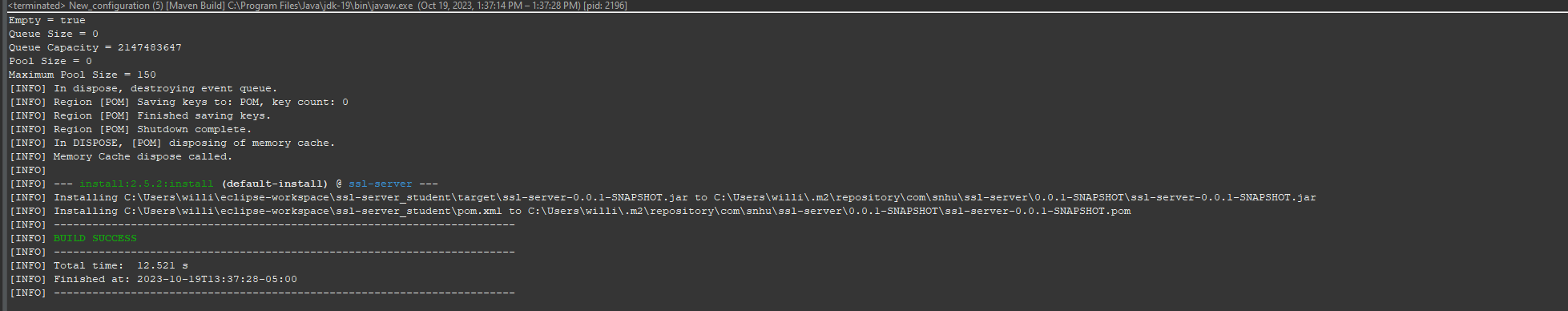


## Secondary Testing





## Functional Testing



## Summary

The code for the Artemis Financial app has been enhanced to meet security standard needs. The code has a hash function which will generate a SHA – 256 checksum for the data that is provided. With this hash it mitigates any security risk with the data. The app has also been updated to use https which is with SSL. Using https ensures the data in transit and prevents attacks during that process. It also has a self-signed certificate which is used to establish a secure connection. The projects pom.xml file uses the latest version of OWSAP Dependency check. This helps show vulnerabilities and also provides possible solutions as well. Security measures were implemented throughout the project to better ensure the security of the employees and customers.

## Industry Standard Best Practices

Some of the industry best practices include upgrading to use https which ensures the security of the data in transit which is ensured through SSL encryption. Having this in place ensures that a man in the middle attack will not affect the data of Artemis Financial. Also having a SHA – 256 algorithm cyphers will help ensure that data is not tampered with as well as having the self-signed certificates. Having the latest dependency check will help keep the code safe from any known vulnerabilities or bring the known vulnerabilities to light so that the company can put the proper measures in place to be prepared for them.