****

# Practices for Secure Software Report

# Reynaldo Ortiz

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** | **12/13/2023** | **Reynaldo Ortiz** |  |

## 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

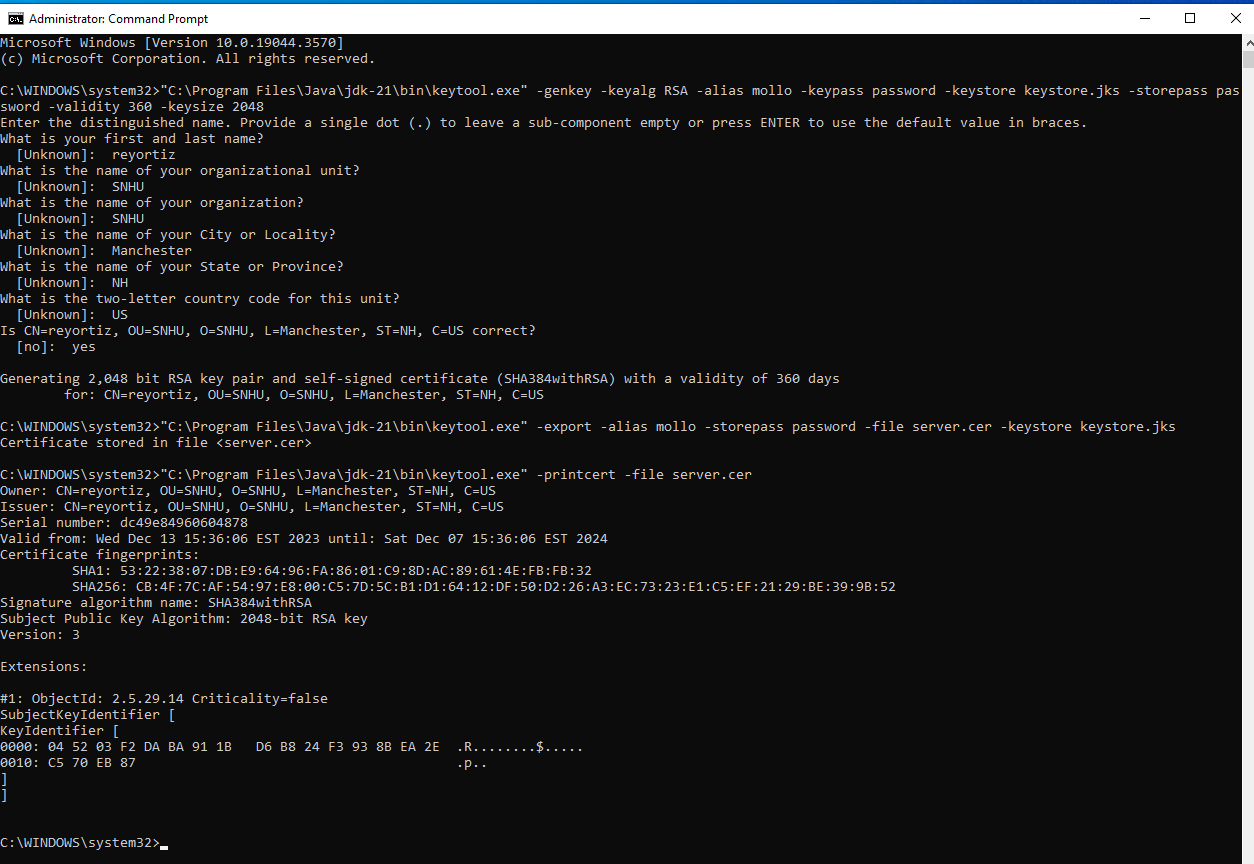
Reynaldo Ortiz

## Algorithm Cipher

The company Artemis Financial is asking for additional security for its web application to guarantee secure communications. Keeping in mind that the most likely attack to occur with a financial institution is hackers attempting to gain access by accessing saved information, encryption would be the top recommendation. What this will do is make the files useless to any hacker without a key. My recommendation for the firm would be asymmetrical communication, this will provide the secure communication they are seeking. What this means for them is that the encryption key is public, and the decryption key is private. The use of SHA-256 cipher is recommended to provide a higher level of security since the information could and would be sent externally. The SHA-256 algorithm uses a random number generator; this will create an encryption that would ensure the desired level of security by creating a non-reversible checksum that checks the file's legitimacy. The SHA-256 will be used by the hash function to produce a checksum of the given message.

## Certificate Generation

Insert a screenshot below of the CER file.



## Deploy Cipher

Insert a screenshot below of the checksum verification.

[Insert screenshots here.]

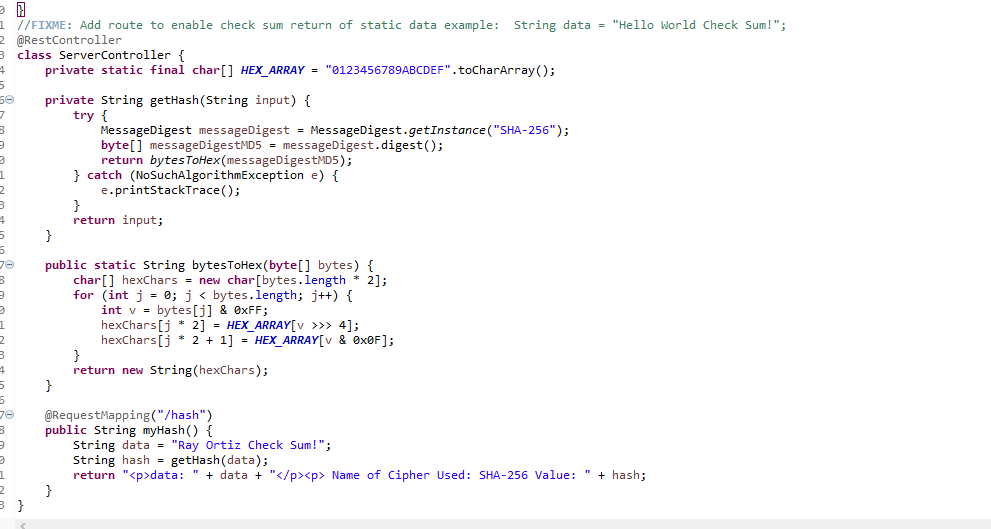
## Secure Communications

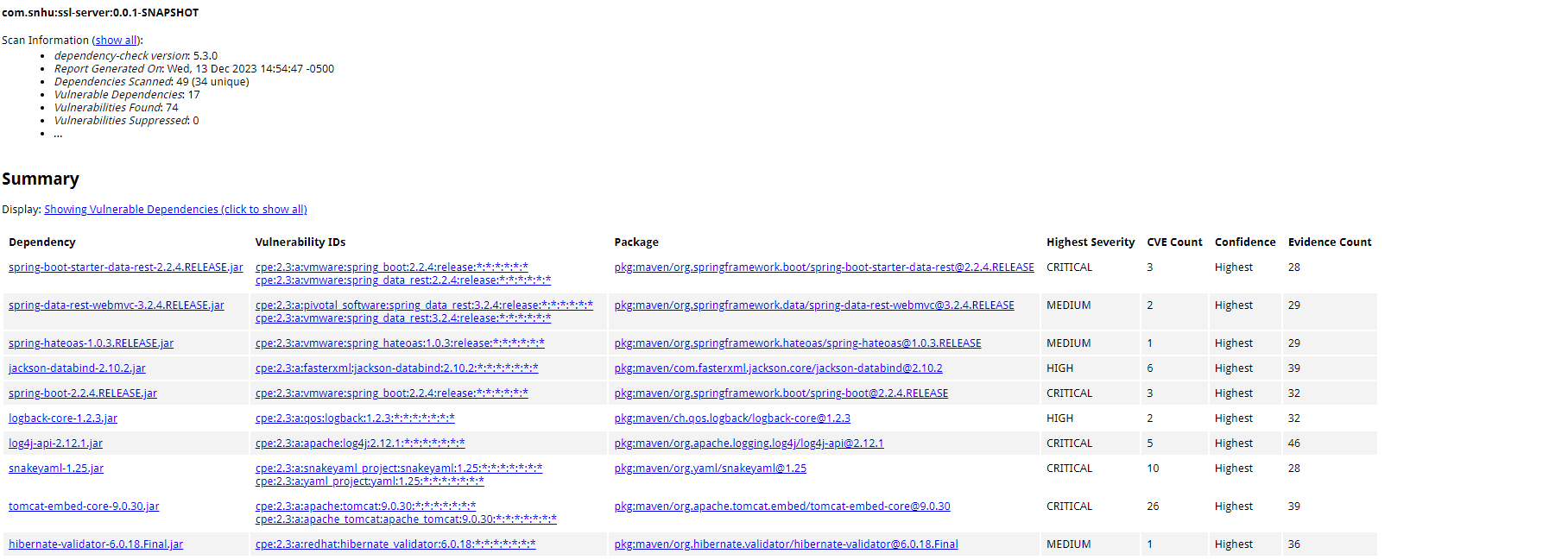
Insert a screenshot below of the web browser that shows a secure webpage.

[Insert screenshots here.]

## Secondary Testing

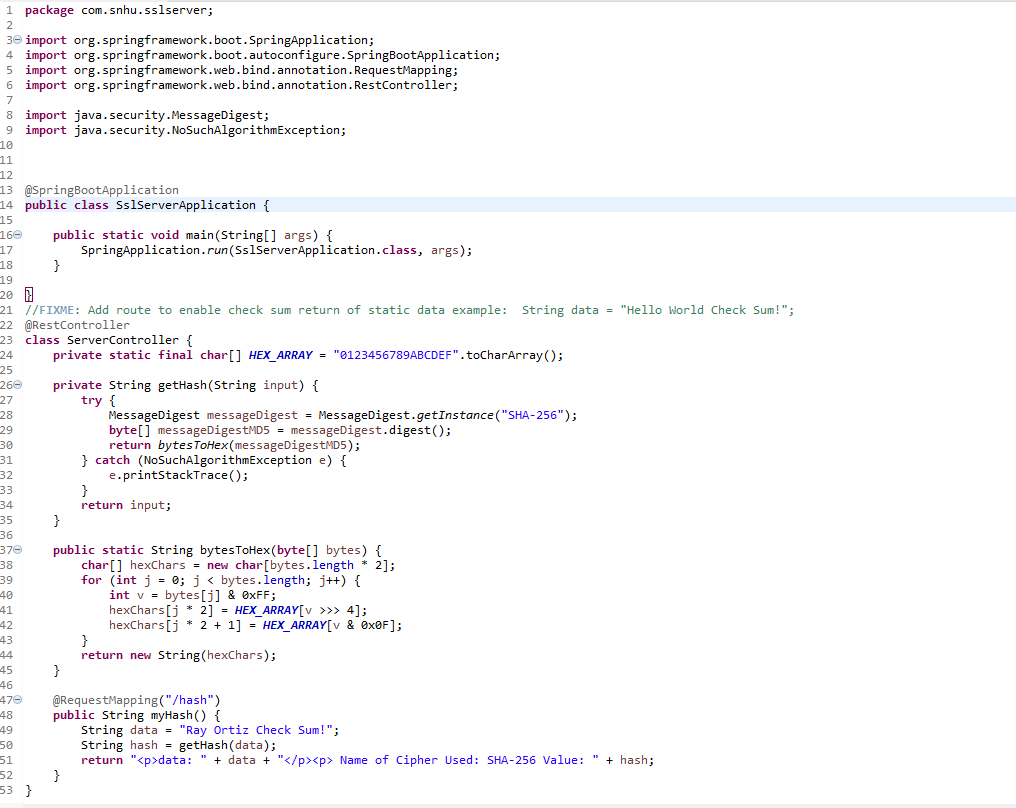
Insert screenshots below of the refactored code executed without errors and the dependency-check report.





## Functional Testing

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



## Summary

To refactor the code for Artemis Financial to comply with the software security testing protocols, the following steps where followed.

* A crypto hash was added to the code so it could generate a checksum for the transmitted data.
* The protocol was changed from HTTP to HTTPS.
* A self-signed certificate was generated and imported it into the keystore file.
* A secondary static testing was ran of the refactored code using the OWASP Dependency-Check Maven this to ensure that it wouldn’t introduce any new vulnerabilities.

## Industry Standard Best Practices

To maintain the software application's current security and apply industry standard best practices for secure coding, I followed the steps outlined below:

* The use of input validation and output encoding thus preventing most common attacks to the system.
* A strong encryption algorithm (AES) was used with a key length of at least 256 bits.
* The self-signed certificate was utilized to secure the HTTPS connection.