****

# 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** | **8/18/2024** | **Kevin Bagayas** | **System Recommendations** |

## 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

Kevin Bagayas

## Algorithm Cipher

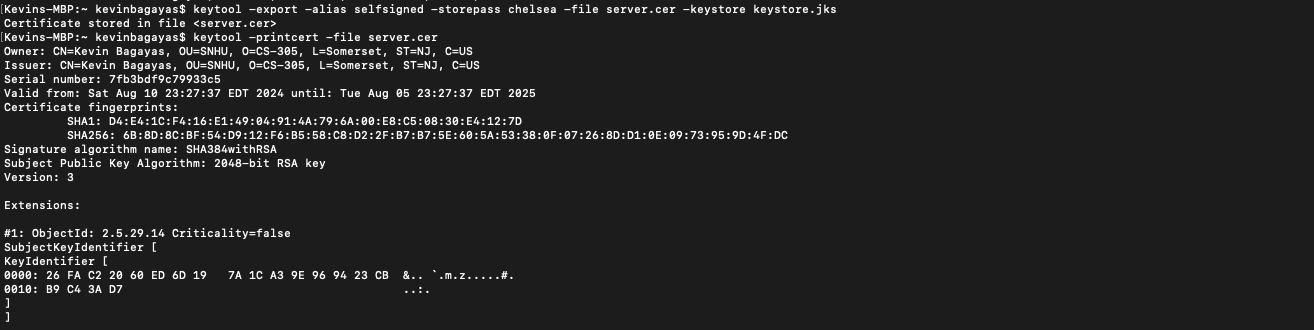
I would recommend the Advanced Encryption Standard (AES) as an encryption algorithm cipher for its long-term file archiving based on the list of Java Security Standard Cipher. It is the commonly used algorithm to encrypt and decrypt protected data. It uses 128-, 192- and 256-bit level security which it makes more secured.

The risks involved with my recommendation would be that the security environment tends to evolve with constant threats every year. An example would be a supercomputer deciphering it making it obsolete. Another risk would be using the different bit levels not considering the storage and making the system slower.

This algorithm cipher will be used to encrypt Artemis Financials’ long term archive files. In terms of the banking and financial sector, they would be using the 256-bit AES encryption to protect digital files and transactions. This makes AES ideal for these kind of processes/transactions because of its multiple rounds of encryption making it harder to break or hacked. The only disadvantage that I would not choose AES is when used with low-end devices it tends to be slow.

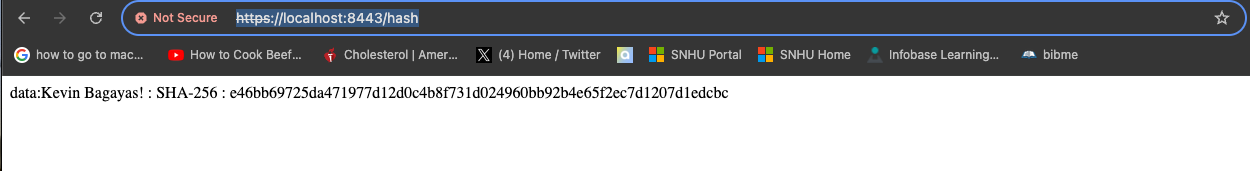
The use of hash functions in AES is wherein it takes a variable bit string as input and outputs a fixed-length string. According to (Jena, 2024), the AES is a symmetric block cipher algorithm with a block/chunk size of 128 bits. Converting these individual blocks and join them together once encrypted to form the ciphertext.

## Certificate Generation



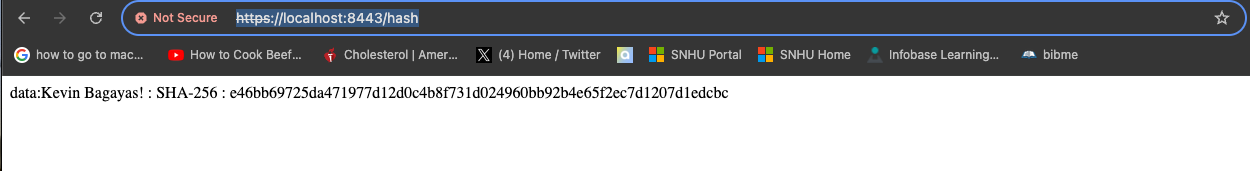


## Deploy Cipher

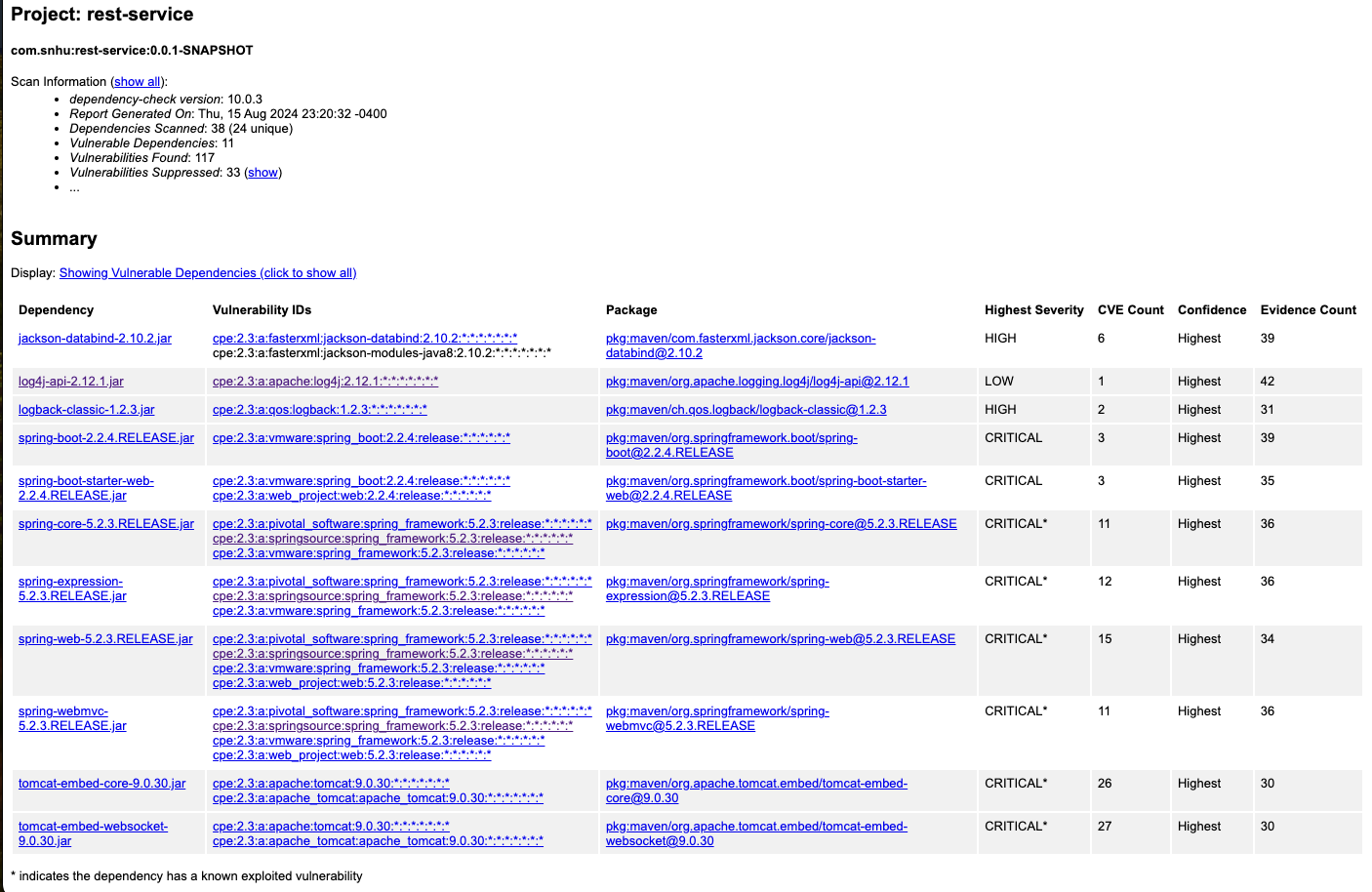


## 

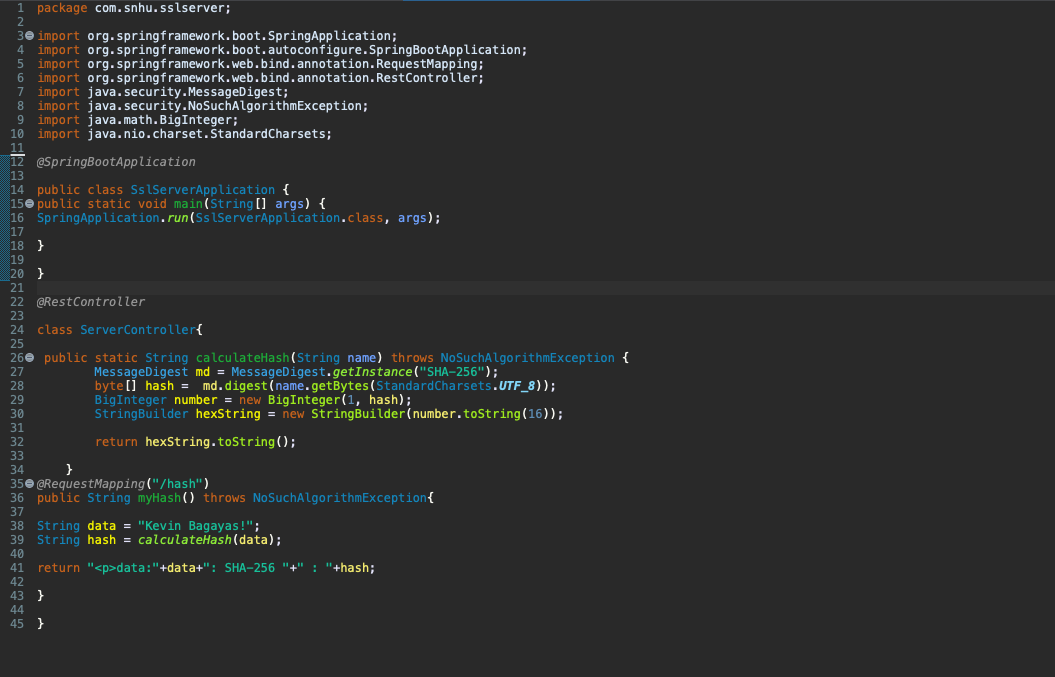
## Secure Communications



## Secondary Testing



## Functional Testing



## Summary

The code has been refactored and complies with security protocols by following these steps.

* Crypto hash is used or placed in the code that would in turn produces a checksum.
* HTTPS used instead of HTTP to provide more security.
* Self-signed certificate generation and store in a keystore file
* Secondary static testing to test the refactored code
* Suppression of dependencies

## Industry Standard Best Practices

In order to maintain industry standard best practices for secure coding, variety of steps where followed:

* Input Validation: Proper user input validation limits and prevents system attacks.
* Strong Encryption Algorithm based on the needed capacity and storage.
* Regular and constant security system updates: maintaining up-to-date system makes the system more resistant to common attacks mode.
* Secure data and transmission
* Error handling and logging

Sources:

‌Jena, B. K. (2023, February 9). *What Is AES Encryption and How Does It Work? - Simplilearn*. Simplilearn.com. <https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption>