****

# 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** | **4/25/24** | **Jonathan Wallick** |  |

## 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

Jonathan Wallick

## Algorithm Cipher

Encryption algorithm ciphers are used to protect financial institutions data across the world from hackers attempting to steal their data. When a hacker attempts to steal data from a user’s account, the encryption ciphers keep the data safe by using a key unknown to the hacker. After reviewing the details of Artemis financials’ specific situation, I would recommend using SHA-256 cipher algorithm. SHA-256 has 256-bit keys of encryption which allows for a large number of possibilities for the keys to be encrypted. When data is input, a hash function is created by taking the value and compressing it into a hash value. The level of encryption is dependent on the number of bits, so for SHA-256 case, there would be 256 combinations inside the encryption. Most encryption keys need to be very difficult to crack to keep the data safe, which is why random numbers are sometimes used to create the key as secure as possible. A symmetric key is used to encrypt data and then the same key is used to decrypt as well. Asymmetric keys use both a public and private key using a different one to encrypt and decrypt data. This option is much slower than a symmetric key but is much more secure. As modern computer technology grows, so too has cryptography. Symmetric keys and public keys are two of the more popular algorithms used today. As for what the future holds, analysts expect that with the growth of quantum computing, today’s algorithms could eventually be cracked. Quantum-safe algorithms are being developed to combat this potential threat in the ever-changing world of cyber security.

## Certificate Generation

A screenshot of a computer

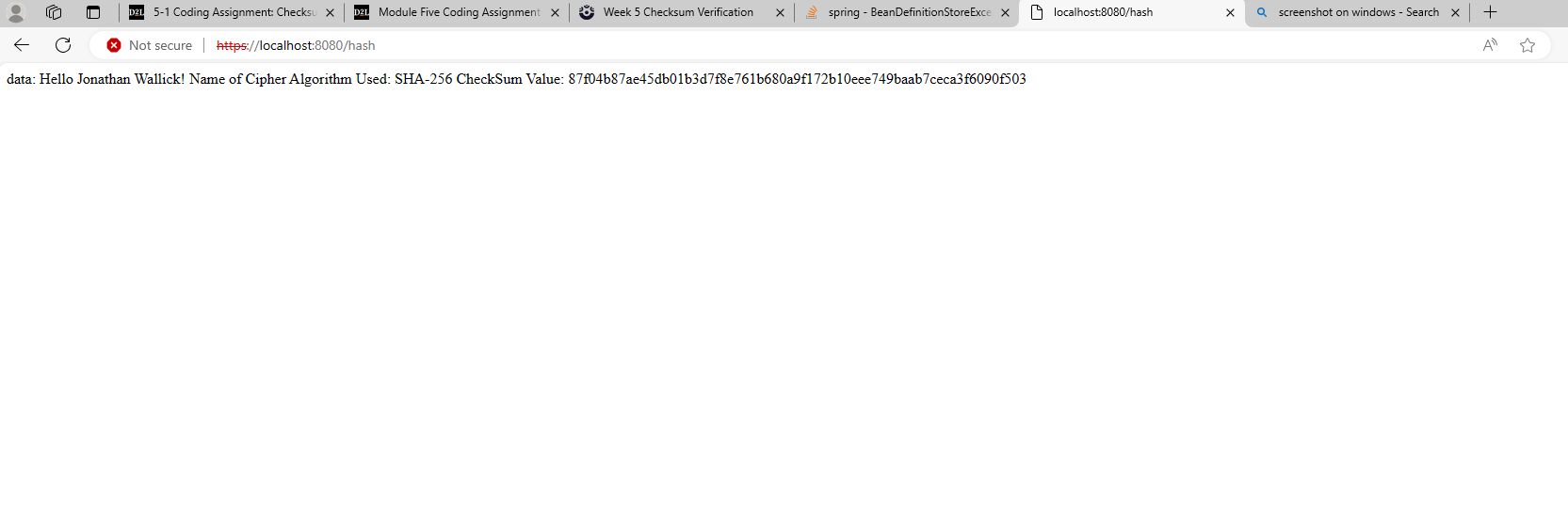
Description automatically generated

## Deploy Cipher

A computer screen shot of a computer screen

Description automatically generated

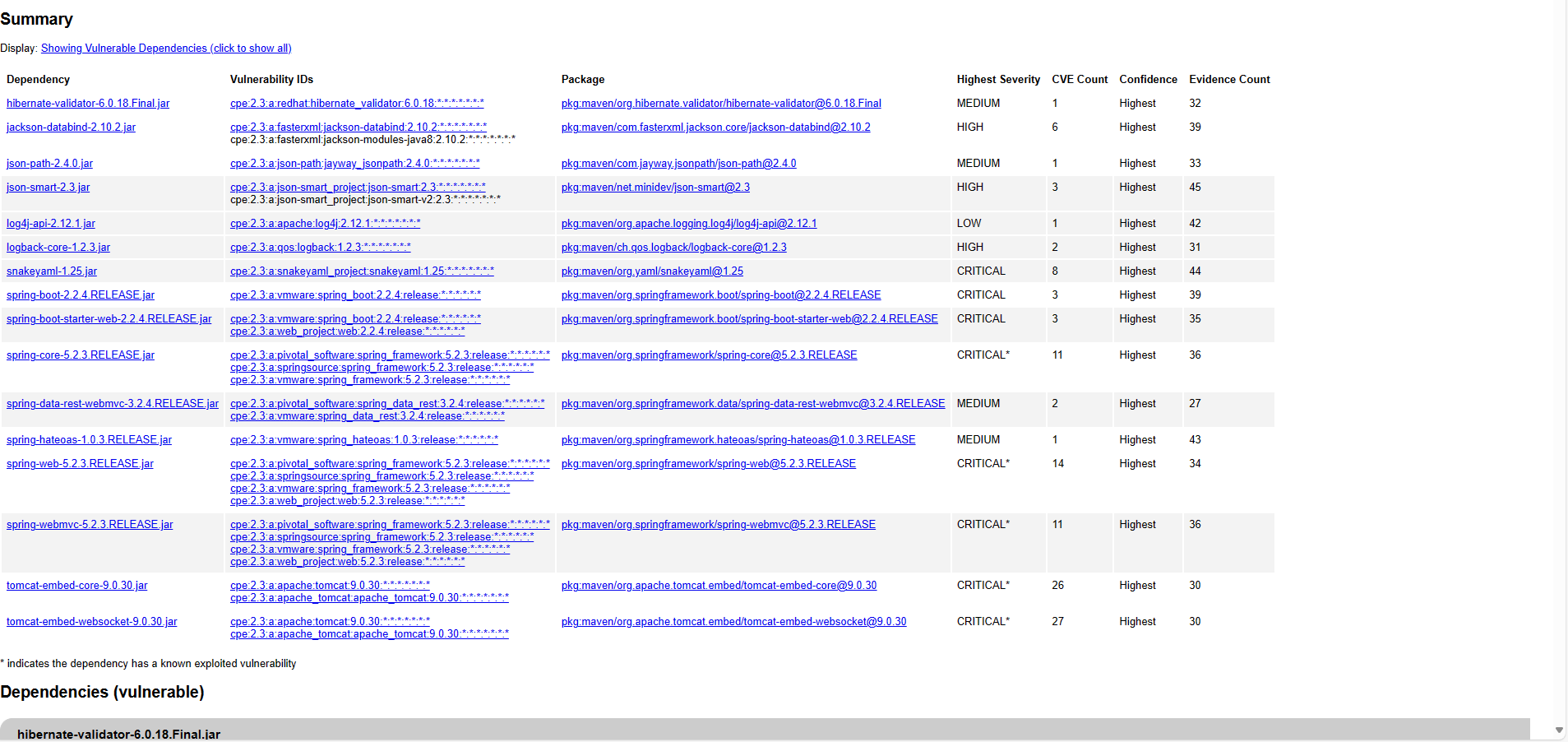
## Secure Communications



## Secondary Testing

A screenshot of a computer

Description automatically generated



## Functional Testing

A screenshot of a computer

Description automatically generated

## Summary

The refactored code now includes a restController for the hash program. Refactoring the code in this way while adding in SHA-256 encryption makes the software much more secure. This cipher can avoid collisions due to being 256 bits.

## Industry Standard Best Practices

Making sure the software plugins are all up to date can help keep the software secure, as well as running dependency checks to reveal any potential security vulnerabilities. Keeping the software up to date as well as running vulnerability tests can go a long way to keeping Artemis Financials’ data safe for its customers.