****

# 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

Shona Robinson

## Algorithm Cipher

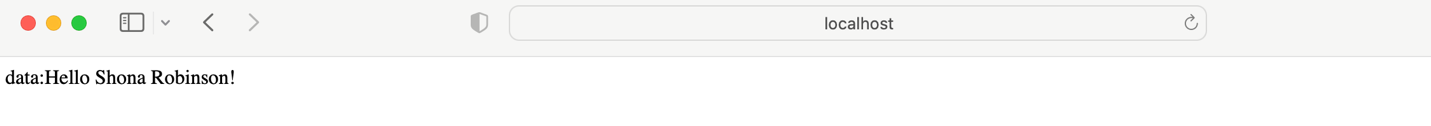
To select an appropriate encryption algorithm cipher, it's very important to consider the level of security required and the type of data being encrypted. A very common used encryption algorithm is Advanced Encryption Standard (AES), which is a symmetric key algorithm that uses a block cipher. AES provides strong encryption and is widely used in various applications. Hash functions are used in encryption algorithms to transform data into a fixed-size output, which is usually used as a digital fingerprint or signature of the data. The bit level of a cipher refers to the size of the key used for encryption. The larger the key size, the more secure the encryption will be. Random numbers are often used to generate cryptographic keys or to add randomness to encryption algorithms. Symmetric keys are used for encryption and decryption by the same key, whereas non- asymmetric keys use different keys for encryption and decryption. The history of encryption algorithms goes back, with various techniques used to protect information from unauthorized access. Modern encryption algorithms uses complex mathematical functions and are continually evolving to provide stronger security.

## Certificate Generation

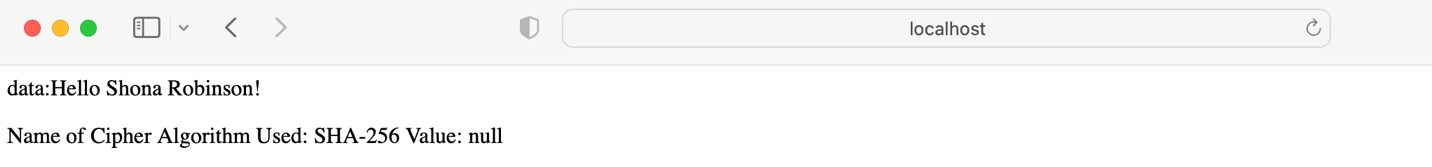
Insert a screenshot below of the CER file.Text, letter

Description automatically generated

## Deploy Cipher



## Secure Communications



## Secondary Testing

## Graphical user interface, text, application, email Description automatically generated

## Graphical user interface, text, application, email Description automatically generated

## Functional Testing

Graphical user interface, text, application

Description automatically generated

## Summary

In my refactoring code, I’ve added a secure RestController to the application to serve as the secure controller. This class, addresses the secure coding concern in the Vulnerability Assessment Diagram and fulfills that concern. I’ve chosen to use SHA-256 as the hashing cipher for this function, and the code is very minimal to reduce the potential of any attack to surface.

I’ve also updated the version of the Maven Dependency check version from 5.3.0 to 6.0.3, so that the static dependency checking is as accurate and up to date as possible.

To maintain the current security of the application, I’d recommend that the dependency checker is ran at least once or twice per month to check for new vulnerabilities that have been discovered so that they may be fixed. Additionally, updating the plugins in the pom.xml configuration file is necessary every so often to ensure that the plugins remain up to date.

## Industry Standard Best Practices

There were a number of industry standard best practices that I used specifically in this project such as:

Code Quality, Testing, Security, and Performance Optimization. Code Quality: Writing clean, readable, and maintainable code that follows industry-standard coding conventions and guidelines. Testing: Writing automated tests to ensure that the code behaves as intended and catches bugs early on in the development process. Security: Implementing security measures to protect against potential security threats and vulnerabilities. Performance Optimization: Writing efficient code that runs quickly and consumes minimal resources.

These best practices were used to help ensure that the software is reliable, secure, and maintainable, and they also improved my productivity.