****

# 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** | **Oct. 14, 2022** | **Eric Wallace** |  |

## Client



## Developer

Eric Wallace

## Algorithm Cipher

1. **Provide a brief, high-level overview of the encryption algorithm cipher.**

AES is the encryption I chose for this project. AES is the industry standard for encrypting data today. After 20 plus years it has never been broken and experts say that it is virtually unbreakable.

1. **Discuss the hash functions and bit levels of the cipher.**

Hash functions are like encryption algorithms in that they are meant to scramble data but that is where the similarities end. Hash functions take in input of alphanumeric or a list of numbers and outputs a hash value. Ex. Someone sending a message could send the message through a hash function and then attach that hash value to the message and send it, when the receiver gets the message, they can then run the message through the same hash function, compare the two hash values, if they match than the message is authentic if they don’t the message has been tampered with.

Bit levels are the number of bits output by the hash function.

1. **Explain the use of random numbers, symmetric versus non-symmetric keys, and so on.**

Random numbers in cryptography are used to ensure keys are secure and do not reveal any information about the hashes used to create the key. They are selected by the algorithm from a large subset of number and form a distribution.

Symmetric encryption (key) only uses one key which is created during the hashing process, the same key is used to encrypt and decrypt the data. The sender will input a password or phrase and the receiver must enter the same password or phrase to decrypt the data

Asymmetric encryption uses a private and public key for encrypting and decrypting. The receiver of the data will send the sender of the data their public key, the sender will use that key to encrypt the data and send the data. After receiving the data, the private key is used to decrypt the data.

1. **Describe the history and current state of encryption algorithms.**

Encryption has been around for nearly 4,000 years; the Egyptian’s used it to protect knowledge because they felt education was only allowed to those of higher society. In the 1940’s encryption was used in the German Enigma which led to the institutionalization of cryptography.

In modern times cryptography, security of encryption does not depend on the algorithm, but the secrecy of the keys used to encrypt the data. A lot of people believe the security lies in the algorithm which is a misunderstanding of how encryption works. Securing the internet is a very complex problem because while computers are great at providing users with information, they can also complete billions of mathematical operations per second which make them perfect for breaking encryption.

The encryption used by most today including the U.S. government and the NSA is based on AES block cipher encryption. To date AES has never been broken with the exception of it being setup or implemented incorrectly. It has been said to break a SHA256 AES encryption would take somewhere around 4 human lifetimes using the most powerful computers today and using a standard computer it would take around 500 to 600 years. I would say the state of encryption is rock solid.

## Certificate Generation

Insert a screenshot below of the CER file.

Text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A picture containing text

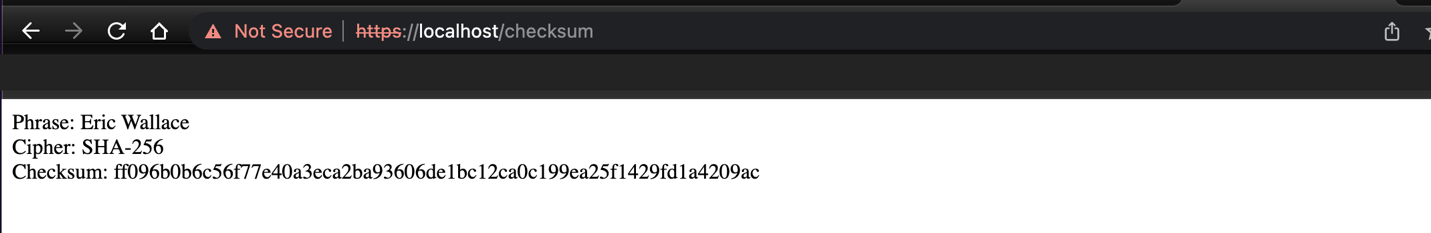
Description automatically generated

## Secure Communications

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

I included two screenshots, the first one shows that the checksum is getting created while on a secure page, Chrome puts a line through https because it can’t verify the certificate.

The second screenshot shows that the browser is using the self-signed certificate to verify that it is a secure webpage.



Graphical user interface, text, application

Description automatically generated

## Secondary Testing

## The POM file does not show any errors, I included a suppression file for the two vulnerabilities shown, the versions that are shown in the list are at the latest version but have vulnerabilities don’t show any resolution.

## Text Description automatically generated

## Text Description automatically generated

## Text Description automatically generated

Graphical user interface, text, application, Teams

Description automatically generated

## Functional Testing

Text

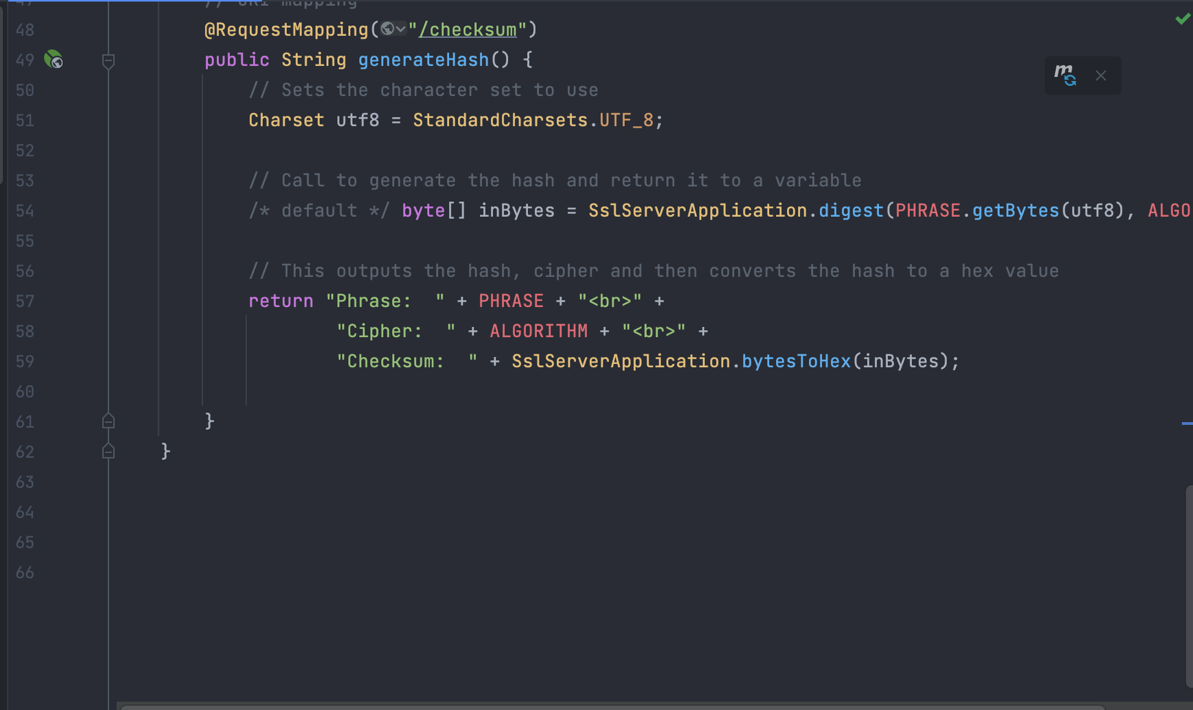
Description automatically generated

Text

Description automatically generated

Text

Description automatically generated



## Summary

The areas in the Vulnerability Assessment Flow Diagram addressed by refactoring my code was Input Validation, APIs, Cryptography, Code Quality and Code Error

The process for adding levels of security was first to create a self-signed certificate and a keystore. Then in the application.properties I changed the configuration to access the keystore and certificate by securing it with a password. This made the application use the SSL and the certificate that was created at the beginning.

## Industry Standard Best Practices

I applied industry standards by using Snyk to verify my code created no security bugs or vulnerabilities. Snyk also scans dependencies for vulnerabilities and did not find any vulnerabilities with the code that I have control over.

I applied industry standards by commenting code, naming conventions, and using correct modifiers so methods aren’t available to other classes or methods. All outdated libraries and packages were updated to the latest versions to reduce the number of possible vulnerabilities.

The value of applying industry standards is that code is more readable, reduces the number of bugs, reduces the number of possible attacks on the application and the number of vulnerabilities an application can and possibly will have.