****

# 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** | **12/09/2022** | **Farooq Ahmed** |  |

## 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

Farooq Ahmed

## Algorithm Cipher

Data is a valuable resource for every company and our client, Artemis Financial handles customer’s information and their financial resources. Data needs to be secured all the time weather it is in transit or at rest. Data is usually protected during rest in the database, but in transit attackers can take advantage of less secure protocols and exploit the information. We can use Transport Layer Security (TLS) to protect data while in transit and this protocol has been revised several times and have implemented new security techniques. Artemis Financial is looking for encrypting archive files, which is going to be stored for a long time and appropriate solution would be to use Standard Hash Algorithm (SHA) since this institution handles huge amounts of customer’s data and this cipher algorithm can ensure security and confidentiality of the data. For customers, it provides data integrity so you can verify the correctness of the data. To be specific, we must use SHA-256 because even by brute force, it will take 2 to the power 256 (2^255) number of possible keys to crack the cipher and you can rest assure that your data will be safe and secure from unwanted threats and breaches. We can also use SHA-128, which is also sufficient for archive files. This cipher can be broken if we neglect the vulnerabilities exist in the software and poor software design can lead the data breaches easily by hackers. We need to make sure everyone in your organization has right number of privileges or role to perform their duties, which falls under Access Control area. Any unauthorize access can lead to security breach. Even government agencies use this encryption to secure their top secret information and SHA-256 is expected to be strong enough to secure data for couple decades. Federal government continues to improve the encryption as the new threat arises and try to stay one step ahead of hackers.

Hash functions are a way to ensure data integrity and they serve as a check-sum verification making sure the data hasn’t been tempered. It protects against unauthorized modification, protect stored passwords, and operate at different speeds to suit different purposes. A hash function takes the plaintext and generate a hashed value output. The purpose of bit level is to protect the information during transit and rest, and the higher the bits are the stronger bit cipher level are. Currently, there are currently 128 bit and 256 bit cipher, which are recommended. Use of Random numbers eliminates predictability and there is no pattern to the number generated. So, it will be difficult for attackers to obtain information and they will eventually give up on trying to hack the system. Symmetric keys utilize private key to encrypt and decrypt the data. As for Asymmetric keys generate a key pair consisting of public and private keys. Public key use for encrypting the data and private key use for decrypting the data.

The history of encryption algorithms goes way back to ancient Egypt, Greek, and Roman Empire era. It was used to communicate secret messages during wars and still in use today. It is a technique of writing and hiding messages from malicious third party interference. The first encryption was the substitution cipher, which used a simple method of replacing units (a group of letter or individual letter) with other units based on the set of substitution rules like C=N, V=A, etc. The purpose of encryption was to conceal the data and prevent it from falling into wrong hands, and the concept is same yet until this day. Currently, Standard Hash Algorithm (SHA) is the most well-known cryptography system today. It has continued to grow and improve over the past few years ensuring security against all kinds of threat.

## Certificate Generation

Insert a screenshot below of the CER file.

Text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Graphical user interface, application

Description automatically generated

## Secure Communications

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

Graphical user interface, application

Description automatically generated

## Secondary Testing

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

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

## Functional Testing

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

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

## Summary

We have added the RESTController to our application to serve as a secure controller for /hash endpoint, which address the security concerns in the Vulnerability Assessment Diagram. Standard Hash Algorithm is the perfect choice for hashing cipher and the code is very minimal. Maven Dependency is updated to latest version, which is 7.3.0, so the dependency-check report is up-to-date and accurate. We have suppressed the vulnerabilities.

## Industry Standard Best Practices

We will have to keep revising the code every year to ensure that security at its best and can protect the application from any threats.