****

# 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** | **February, 23 2024** | **Divyesh Rana** |  |

## 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

[Divyesh Rana]

## Algorithm Cipher

Choose a good way to encode information to keep it safe from hackers and explain why you chose it. Please make sure to talk about:

* "Give a quick summary of how the encryption algorithm works. "
* Let's talk about the ways the cipher uses hash functions and bits.
* Please explain how we use random numbers, how symmetric keys are different from non-symmetric keys, and similar topics.
* Explain the past and present of codes that keep information secure.

Artemis Financials’ main goal is to provide financial services to customers all over the world. I suggest using SHA-256 for encrypting data for this specific purpose. This code can keep all the information safe from anyone trying to get to it. It is thought to be one of the safest ways to encode information, and it is very difficult for others to decode or access. It would take a long time and a lot of effort to figure out the code. When talking to banks or other money companies, it's often recommended to use SHA-256 as the code to keep information safe. The SHA-256 hash function and its bits are created using random numbers. When making a hash function, the starting value gets squeezed before it's used. The hash value is the shortened version of the data's name. The size of the encryption is decided by the number of bits used.

256-bit encryption is determined by the number of different ways it can be encrypted. Using random numbers makes it harder for hackers to access information without permission. Unpredictability happens because things are random. Symmetric keys are seen as a simple way to code information. One big benefit of using a symmetric key is that it is quicker to use (Yedakula,K. , 2019), and you only need to have 1 key. Therefore, AES-256 often uses symmetric keys to encrypt plain text using a key. Asymmetric keys, which use two keys, are considered safer than symmetric keys. Internet communication usually uses keys that are not equal in size or strength. Encryption has been around for a very long time, since 600 BC. Thales Group, in the year 2016. With encryption, we can now protect data from people who shouldn't be able to see it. People have always thought that being safe is very important and will continue to think so.

## Certificate Generation

## Create your own certificates using the Java Key tool, which is used in the command line.

Text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

[Insert screenshots here.]

## Secure Communications

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

[Insert screenshots here.]

## Secondary Testing

## Graphical user interface, application Description automatically generated

Text

Description automatically generated

[Insert screenshots here.]

## Functional Testing

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

[Insert screenshots here.]

## Summary

I changed the code by adding a safe Rest Controller to the SSLServerApplication. java It will now be the safe controller for the hash RESTful endpoint. The ServerController class Deals with the problem of writing secure code in the Vulnerability Assessment Diagram and meets all the needed standards. I used SHA-256 for security and made the code simple to make it harder for attackers. I changed the Maven Dependency check from version 5.3.0 to 8.2.1, so that the system is using the latest software version for checking dependencies.

## Industry Standard Best Practices

I used the best ways to write code safely to fix security problems and keep the software secure. In addition to the changes, I talked about in the Summary section, it is very important to put in place the right security measures. Here’s what to use to keep the software safe.

Input validation is checking and cleaning up the information that users enter to make sure it's safe and doesn't cause any harm to the system. This is done to prevent different types of attacks like inserting harmful code, tricking browsers, or sneaking in commands.

Making sure only the right people can access an account by using strong passwords, special codes, and other ways to check if the user is who they say they are.

The principle of least privilege means giving users and apps only the permissions they need to do their job, which helps prevent unauthorized access or actions.

Secure data storage and transmission means keeping information safe. This is done by using strong codes to protect the data when it's stored and when it's being sent. These codes are the same ones that are used by many companies to keep their data safe. Also, using secure communication protocols like HTTPS helps to keep the data safe when it's being sent over the internet.

Regular security updates and patching means making sure that the software and all its parts are always kept up to date to keep it safe from being hacked. This includes quickly adding any security fixes and fixing any known weaknesses to reduce the chances of being attacked.

Error handling and logging: Using the right methods to deal with mistakes and keeping a record of events to spot security problems.

Using best practices for secure coding in the industry is very important for a company. It helps protect important information, follow rules, save money, and build trust with customers and partners. It also makes the company look good and improves its reputation.