****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc127263295)

[Document Revision History 3](#_Toc127263296)

[Client 3](#_Toc127263297)

[Instructions 3](#_Toc127263298)

[Developer 4](#_Toc127263299)

[1. Cipher Algorithm 4](#_Toc127263300)

[2. Certificate Generation 5](#_Toc127263301)

[3. Deploy Cipher 6](#_Toc127263302)

[4. Secure Communications 6](#_Toc127263303)

[5. Secondary Testing 7](#_Toc127263304)

[6. Functional Testing 8](#_Toc127263305)

[7. Summary 10](#_Toc127263306)

[8. Industry Standard Best Practices 10](#_Toc127263307)

[9. Reference 11](#_Toc127263308)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **3.0** | **13 February 2023** | **Sergio Mateos** | **Artemis Financial modernize require the most current and effective software security.** |

## Client



## Instructions

Global Rain, a software engineering company, specializes in custom software design and development. Global Rain has a mission which is “Security is everyone’s responsibility”, securing companies against malicious user has been an important subject in recent years between companies since as technology scale, malicious users grow with it. Artemis Financial, a consulting company that develops financial plans, has recently a partnership with Global Rain to modernize their software and implement the most current and effective software security. Artemis Financial has a high amount of individual personal information, that why Global Rain needs to make sure to secure and protect the integrity of Artemis Financial.

## Developer

Global Rain will assign Sergio Mateos as the developer. Sergio Mateos will address any security vulnerability.

## Cipher Algorithm

Algorithms Cipher are mathematical formulas designed to hide valuable values and content of data. As part of the formula, the cipher algorithm uses a key to encrypt data. Cipher Algorithms need this key to decrypt the data in a readable format. Cipher Algorithm increases the size of its key as part of its protection process, while the key increases the size, the computing time to decrypt the key increase which makes it difficult for malicious users to have access to delicate data.

Artemis Financial is seeking to increase its security as part of its modernization process. As we know, Artemis Financial works with sensible data like financial status, addresses, names, etc. Artemis Financial need to make sure that the information of their user is secure and unbackable for external users other than them and their clients. As part of my analysis, I will suggest using SHA-256. Secure Hash Algorithm (SHA) is a cryptography hashing algorithm that converts text into a string of 256 bits (32 bytes). SHA-256 was developed by the US Government National Security Agency (NSA) and the National Institute of Standard and Technology (NIST) which was introduced as the successor to the SHA-1 family. SHA-256 divide its processes into five different stages.

1. Padding Bits: Add extra bits to the message.
2. Padding Length: Add 64 bits and the plaintext multiply by 512.
3. Initializing the Buffers: Default values for buffers.
4. Compression Function: The message is broken down into multiple blocks.
5. Output: Final hash digested.

In data security, the use of symmetric and nonsymmetric keys means that the data encrypted can only be decrypted by a single key or two. A symmetric key, also known as a private key, is an encryption method in that only one key is viable to encrypt and decrypt data. The key relies on mathematical functions to encrypt and decrypt data. It calls “symmetric” because only one key can encrypt and decrypt data. A nonsymmetric key or Asymmetric key is a cryptography process that includes two keys. The public key encrypts data and the private key decrypts. The public key is available to use compared to the private key which keeps secret. There is another important topic in cryptography which is random numbers. Random numbers or Pseudo-Randomness is a mathematical function that outputs a series of random numbers, but these numbers have a congruent sequence. The use of random numbers generates keys that are used to encrypt or decrypt data.

Algorithm Encryption is historically used to secret write and hide messages. Encryption derivates from the Greek word Kryptos, which means hidden. One of the earliest moments of the encryption is in 500-600 BC when the Hebrews write hidden messages in the Old Testament of the Bible, this process was known as Atbash. Atbash was a process where the Hebrews reverse the letter in the alphabet A becomes Z, B becomes Y, and so on. Later on, Spartans, create a different algorithm encryption called Scytle, which was used in the war to communicate and consisted of writing messages on a rod with specific measurements and wrapping pieces of patches to encode the message. This type of algorithms encryption was popular until the use of mathematics becomes more useful. In the 15th century, Leon Battista creates the first polyalphabetic cipher. Polyalphabetic cipher is a combination of multiple alphabets and with the use of a cipher to message was able to be decoded. As time moves forward, encryption becomes a more useful tool. During World War II (WWII) Nazi Enigma machine help them to encrypt messages and send them to their allies, this was a risk in war since the opposite side can’t have access to their information and this could be a risk of loose the war. But the Britain, Alan Turing’s innovates in the encryption field and creates an algorithm that helps them to decrypt their message. Now, algorithm encryption plays a huge role in Information Security, as technology matured algorithm encryption becomes more complex, usually becoming a Symmetric and Asymmetric (Nonsymmetric) Algorithm.

## Certificate Generation

Graphical user interface, text, application, email

Description automatically generated

## Deploy Cipher

## 

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

## Secure Communications

HTTP

Graphical user interface, text, application, email

Description automatically generated

HTTPS

Graphical user interface, text, application, email

Description automatically generated

## Secondary Testing

## 

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

## Text Description automatically generated

## Functional Testing

Software syntactical, logical, and security vulnerabilities could be present in the code developed. Even I the execution of the code was successfully achieved; malicious users could find different ways to access the data in our code. On the myHash method, the value of the user is passed straight to the be hash. This type of error could be exploited and end up in leaking of information.

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

## Summary

The Global Rain developer has successfully used the Vulnerability Assessment Process Flow to prevent Artemis Financials’ web application to have any leak of information. The code was refactored to allow the traffic to come thru and check for vulnerabilities.

* 1. Input Validation: Input validation was noticeable since the input are sent straight to be hash. Failing to validate could open the door for malicious users to access the Artemis Financial web application.
  2. API: The API was developed to return a checksum of string. The checksum authenticates the user. The creation of a RESTful application will secure the API.
  3. Cryptography: The cipher algorithm pushes the string a created a hash. The hash prevents the code would be decrypted and exposing important information.
  4. Client/Server: The addition of the certification demonstrate that the data could be transfer secure,
  5. Code Quality: The code provides comments that allow the developer to know what the method and its function are. Also, easy, and understandable variables facilitate the understanding of the code.

Security of the software application was by first securing the RestCrontrollers. The best cipher algorithm that I decided to implement was SHA-256 as it’s the most secure, it runs fast, and the change of collision is minimum. Creating a safe way to communicate is achieved by hashing the information using an Secured Socket Layer (SSL) connection. This will secure the information between Artemis Financials and its clients.

## Industry Standard Best Practices

As a developer, I will suggest checking the dependency check at least three times a month, we know that the technology is moving at a fast speed, so a constant check of the dependency will ring the newest vulnerabilities. Enforcing strong encryption to prevent easy access to the client information and even if they were available to break into the system, the data would remain secure. Preventing using components with known vulnerabilities will minimize the knowledge about our system and access to it. One of the most outstanding problems highlighted by KirkpatrickPrice, a website dedicated to technology and innovation, said: “Passwords are a weak point in many software systems” (KirkpatrcikPrice, 2022), this statement is important to understand and implement in our users and staff, a weak password can lead to easy access to the system. Educating staff and users about passwords it’s crucial for the success of the web application.

One recommendation, it’s to inform and educate about social engineering. Social engineering is the art of manipulating individuals to divulge sensitive information via different methods. Based on Crowdstrike, a top worldly cyber security company, “Social engineering attacks are of great concern to cybersecurity professionals because, no matter how strong the security stack is and how well-honed the policies are, a user can still be fooled into giving up their credentials to a [malicious actor](http://crowdstrike.com/cybersecurity-101/threat-actor)”. Educating and preparing their customer for this type of attack must be a goal to achieve for every customer.

## Reference

Jena, B. K. (2022, November 11). *What is SHA-256 algorithm: How it works and applications [2022 edition]: Simplilearn*. Simplilearn.com. Retrieved February 14, 2023, from https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

*Encryption: The past, present, and future*. AXEL.org - Bringing awareness to data custody. (2021, May 28). Retrieved February 14, 2023, from https://www.axel.org/2021/05/28/history-of-encryption/

8 secure coding practices learned from Owasp. KirkpatrickPrice Home. (2022, December 16). Retrieved February 15, 2023, from https://kirkpatrickprice.com/blog/secure-coding-best-practices/

What is social engineering? attack techniques + prevention: Crowdstrike. crowdstrike.com. (2022, November 30). Retrieved February 15, 2023, from https://www.crowdstrike.com/cybersecurity-101/social-engineering-attacks/