****

# CS 305 Project Two

**Practices for Secure Software Report**

Table of Contents

[Document Revision History 3](#_Toc33111302)

[Client 3](#_Toc33111303)

[Instructions 3](#_Toc33111304)

[Developer 4](#_Toc33111305)

[1. Algorithm Cipher 4](#_Toc33111306)

[2. Certificate Generation 4](#_Toc33111307)

[3. Deploy Cipher 4](#_Toc33111308)

[4. Secure Communications 4](#_Toc33111309)

[5. Secondary Testing 4](#_Toc33111310)

[6. Functional Testing 5](#_Toc33111311)

[7. Summary 5](#_Toc33111312)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **08/08/2022** | **Dan Stull** |  |

## Client



## Developer

Dan Stull

After researching the best Algorithm Cipher that would fit the requirements, I believe Artemis Financial would benefit significantly from using AES in the form of the SHA-256 as the hash function that will decrypt their sensitive materials.

Looking into AES's history, it is plain to see that it has a wonderful track record against outside attacks. It is important to note that it has been broken using brute force. However, this doesn’t often all that happen. When the bytes increase from 128 to 192 to 256, the complexity of the encryption increases as well.

While AES is used in smaller businesses, it is also used in large corporations, medical facilities, and governmental agencies, proving how much trust is given to the cipher.

There are two types of ciphers: the non-symmetric and the symmetric. AES is symmetric. What does this mean? AES uses the same digital key to encrypt and decrypt the data. In contrast, the non-symmetric ciphers generate a unique key for both the encryption and decryption processes. And these digital, generated keys are produced in 128, 198, and 256 bits. Each one, in essence, is more robust and secure (making it harder to crack) than the last. The number of bits refers to the length of the key.

Throughout history, ciphers have been used to keep sensitive data from falling into the wrong hands. The Enigma machine was used in World War II to send encrypted messages and to find and decrypt enemy messages sent from base to base. From these beginnings, we find ourselves in a day in time where encryption is vital. With cyber attacks more common than ever, strong cipher like the AES, DES, and many others are needed to keep sensitive data from falling into the wrong hands.

## 2. Certificate Generation

## Text Description automatically generated

## 3. Deploy Cipher

Graphical user interface, text, application, email

Description automatically generated

## 4. Secure Communications

Refactor the code to convert HTTP to the HTTPS protocol. Compile and run the refactored code to verify secure communication by typing **https://localhost:8443/hash** in a new browser window to demonstrate that the secure communication works successfully.

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

Graphical user interface, text, application, email

Description automatically generated

## 5. Secondary Testing

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

I created a suppression.xml and went through the checklist but found no vulnerabilities that were false negatives.

## 6. Functional Testing

Text

Description automatically generated

## 7. Summary

After adding a route for the checksum in the refactored code, I utilized a hash function to encrypt it. In this case, the SHA-256, as was described earlier. The addition of the SHA-256 strengthened the program's security, adding to the already robust strength of the RESTful API. Utilization of a certificate ensured that the data being shared was secure and ended up where it was supposed to go. Providing a cert improves security for the user, Artemis Financial, and the developer (client and server). And the addition of exception throws only helped to reinforce the security.

Checking for updates is crucial in ensuring programs are safe and reliable. An out-of-date version can be an “in” for a cybercriminal, and up-to-date applications can better fight against known vulnerabilities. These steps, though many, were taken to ensure the security of Artemis Financial.

As a web developer, an essential aspect of the job, which needs to stay at the forefront of one’s mind, is the client's security. In today’s world, cyber threats are prevalent, happening daily with criminals learning and using more loopholes that have yet to be sniffed out. But with steadfast monitoring of encryptions, updating and maintaining dependencies, checking for false positives, and reviewing the code while in development and post launch, we as web developers can make it much harder for criminals to breach programs and attain vital data.