****

# 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** | **10/16/2022** | **Brady Steele** | **Document Updates** |

## 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

Brady Steele

## Algorithm Cipher

The encryption algorithm cypher that I have chosen to deploy for Artemis Financial is the Advanced Encryption Standard, or AES. “The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information” (Bernstein & Cobb, 2021). The Advanced Encryption Standard was developed by the National Institute of Standards and Technology in 1997, as a new competing method to the Data Encryption Standard, or DES. Due to its focus on classified government information, the AES is designed to be extremely long and tedious to crack with brute force methods, making it ideal to secure financial information. After its adoption by the federal government, “AES soon became the default encryption algorithm for protecting classified information, as well as the first publicly accessible and open cipher approved by the NSA for Top Secret information” (Bernstein & Cobb, 2021). Extensive use in the private sector, with widespread adoption, means that the success of and support for AES speaks for itself.

“A hash function is a unique identifier for any given piece of content. It’s also a process that takes plaintext data of any size and converts it into a unique ciphertext of a specific length” (Crane, 2021). Within the AES symmetric block cipher, there are three different block ciphers to choose from, the 128-bit key length, 192-bit key length, and 256-bit key length. This cipher is symmetric, which means that the same key will be used on both ends of the encryption and decryption, so “the sender and the receiver must both know -- and use -- the same secret key” (Bernstein & Cobb, 2021). Asymmetric ciphers mean that the key is different for the sender and the receiver. One of the downsides to asymmetric ciphers is that the implementation time is longer, versus symmetric ciphers.

The Data Encryption Standard was used by the federal government until the 1990s when the Advanced Encryption Standard was created and adopted, due to its increased security, cost, and implementation ease and speed. I believe that the AES would be a big asset to Artemis Financial, as valuable, personal information is handled in the financial world, and needs a very high level of security and confidentiality.

## Certificate Generation

Insert a screenshot below of the CER file.

Text

Description automatically generated

Text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Graphical user interface, text, application, email

Description automatically generated

## Secure Communications

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

A picture containing graphical user interface

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

Text

Description automatically generated

There are some present vulnerabilities such as a hardcoded password, that would need to be abstracted for a secure environment.

## Summary

The areas of security that were incorporated for this application were APIs, Cryptography, Client/Server, Code Error, and Code Quality. Each of these components plays a crucial part in maintaining the secure environment.

The biggest security contribution for this project was the self-signed certificate that was created, which allowed for HTTPS connection to the localhost:8443. Using the keytool, I was able to create a secure certificate, to ensure that connections to the application were healthy.

The first layer of security that I worked on in this application was the above mentioned self-signed certificate. This certificate and key were generated, allowing us to ensure secure traffic to the webpage, and providing a solid foundation of security on which to build the project. Next, we needed to choose an algorithm cipher to encrypt and decrypt the user’s data and protect the information of our customers. Once the AES-256 cipher was chosen, I was able to utilize the checksum to verify that the data was being hashed properly. Finally, to ensure that all vulnerabilities were accounted for and taken care of, including false positives, a dependency check was run. This report allowed me to scan through a list of potential vulnerabilities in the application, and to remedy them before they were exploited.

## Industry Standard Best Practices

I incorporated industry standard best practices for secure coding, by ensuring that all transactions with the webpage were secure through HTTPS. In addition, running the dependency check allowed me to patch up any vulnerabilities from deprecated software versions and known exploits, allowing me to protect the application and the user’s data from any breach. Some more best practices could’ve been utilized such as abstraction of sensitive data such as passwords or plain text fields, but that was not incorporated fully into the project. Applying these industry standard best practices is very valuable to the organization, because the company can keep up with the current state of security exploits and data privacy. If the company is consistently applying these practices, customers can be assured that their data is protected and will not be easily compromised. Refusing to apply these practices does not look good for the company and places not only the users at risk, but the company as well, as they may not be complying with regulations.

Works Cited

Bernstein, C., & Cobb, M. (2021, September 24). *What is the Advanced Encryption Standard (AES)? definition from searchsecurity*. SearchSecurity. Retrieved September 25, 2022, from https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

Crane, C. (2021, January 25). *What is a hash function in cryptography? A beginner's guide*. Hashed Out by The SSL Store™. Retrieved September 25, 2022, from https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/