****

# CS 305 Project Two

**Practices for Secure Software Report**

Table of Contents

[\_Toc33111301](#_Toc33111301)

[Document Revision History 3](#_Toc33111302)

[Client 3](#_Toc33111303)

[Instructions 3](#_Toc33111304)

[Developer 4](#_Toc33111305)

[1. Algorithm Cipher 4](#_Toc33111306)

[2. Certificate Generation 6](#_Toc33111307)

[3. Deploy Cipher 6](#_Toc33111308)

[4. Secure Communications 7](#_Toc33111309)

[5. Secondary Testing 8](#_Toc33111310)

[6. Functional Testing 10](#_Toc33111311)

[7. Summary 11](#_Toc33111312)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **04/13/2020** | **Brandon Petersen** |  |

## Client



## Instructions

Deliver this completed Practices for Secure Software Report documenting your process for writing secure communications and refactoring code that complies with software security testing protocols.

Respond to the steps outlined below and replace the bracketed text with your findings in your own words. If you choose to include images or supporting materials, insert them throughout.

## Developer

Brandon Petersen

## 1. Algorithm Cipher

Artemis Financial is looking to modernize its operations, including the software they utilize every day. In addition, to upgrade their operations, they want to ensure their software is reliable, secure, and effective. The current software deployed by Artemis Financial is a web interface that's accessible to the public. Artemis Financial explicitly wants to add a file verification step to its web interface. By adding this verification step, Artemis Financial is looking to increase the security of its platform and provide secure communication between itself and its clients. This verification step will be in the form of a checksum when their web interface is being used to transfer data.

When choosing the correct transfer protocol or algorithm to implement in Artemis Financials' web interface, various protocols secure communication differently based on different needs. Taking Artemis Financial's requirements and conditions for secure transmission into consideration, the transfer algorithm will need to handle the transferring of data and data that is currently not being transported. Using the Advanced Encryption Standard, also known as AES, is a robust encryption algorithm that will meet Artemi Financials' needs. The AES algorithm is a block cipher that uses a key of either 128, 192, or 256-bits to encrypt the data. The AES cipher algorithm can encrypt communications and financial transactions and store data.

In addition to the AES cipher, a Hash algorithm is also recommended. The hash algorithm refers to a hash function used to encrypt data. The hash algorithm uses a 256bit encryption key that allows fast and secure communication between the users and the servers. In addition, it has been proven that using the SHA-1 or SHA-2 has a minimal chance of collisions. Since we're generating a key for the users that requires their first and last name, this will provide the system with a somewhat unique set of strings with the checksum hash value. Using a hash algorithm, SHA-256 is an excellent hash function due to its usability to program and has a solid and secure storing method.

The hash algorithm uses a 256bit encryption key that allows fast and secure communication between the users and the servers. In addition, it has been proven that using the SHA-1 or SHA-2 has a minimal chance of collisions. Therefore, a generated key will be needed to ensure the Hash function is reliable. Since we're developing a key for the users that requires their first and last name, this will provide the system with a somewhat unique set of strings with the checksum hash value. In addition, a random number generator can be used to generate a reliable key. A random number generator creates a secure key since it's built upon random bits of data, and a secure key needs to consist of a random combination of numbers, and these combinations cannot be reused. Using a hash algorithm, SHA-256 is an excellent hash function due to its usability to program and has a solid and secure storing method.

Furthermore, a symmetric or non-symmetric function can be used to secure data. The symmetric key is used in both the encryption and decryption of data. Since the symmetric key is encrypting and decrypting the data, the same key used to encrypt the data is needed to decrypt the data. The non-symmetric key uses a separate key for both the encryption and decryption of the data.

For Artemis Financial, AES cipher and Hash algorithm are great choices to implement for encrypting data. The AES cipher has become the standard by the US government and is used to encrypt many of its data and classified information. In addition, many businesses with online storefronts utilize AES encryption to secure all their financial transactions, protecting both their business and customers' private information. Therefore, utilizing the AES cipher is a considerable asset for Artemis Financial with minimal disadvantages. Artemis Financial can use the AES cipher to secure communications between them and clients, secure financial transactions, store and secure private business data, and store and secure clients' confidential information.

## 2. Certificate Generation

The below image contains a screenshot of the self-generated RSA certificate from the Keystore file that provides the information with a time ratio.

## 3. Deploy Cipher

The below image contains a screenshot of the successful test for the checksum value generating the value "Hello World CheckSum." In addition, the image also demonstrates the generated self-signed SSL certificate using the java keytool command in the terminal. The certificate contains all the information provided when using the keytool to develop it.

Text

Description automatically generated

## 4. Secure Communications

The below image contains a screenshot that demonstrates the website was accessed using the HTTPS protocol instead of HTTP. With that said, I was unsuccessful in opening the window in my browser. I was running into a communication error and could not solve the problem. I will continue to work towards a solution for this problem and update once it has been solved.

A screenshot of a computer

Description automatically generated

## 5. Secondary Testing

The below image contains a screenshot showing a portion of the refactored code with no errors. In addition, there is a second image that has no bugs or defects reported by the maven dependency check. To arrive at this solution, the Spring boot needed to be updated to the latest version, 2.6.6, and the necessary maven dependency to be updated to the newest version, which is 7.0.4.

Text

Description automatically generated

Text

Description automatically generated

## 6. Functional Testing

The below image shows a screenshot of the refactored code for the SSL Server Application for functional testing. After reviewing the code, an issue could be found in the input string for the hash function. The code also indicates what is happening, such as using the RestController of RequestMapping. The codebase of the application is structured to make it easy to read and find any errors that arrive when compiling the code.

Text

Description automatically generated

## 7. Summary

After reviewing the code written for Artemis Financial, I have determined the following security vulnerabilities that Artemis Financial faces with this project: APIs, Input Validation, Code Quality, and Cryptography. When implementing APIs, utilizing the Transport Layer Security, TLS will encrypt the data sent to and from the API. The data being sent to and from the API can contain sensitive information. Therefore, utilizing TLS for APIs is vital. In addition, the type of data being sent to the API needs to be limited. Since the API is not being developed in-house for Artemis Financial, that adds another area of failure. Therefore, it's essential that the type of data being sent to the API be limited. The API should only be receiving the information necessary to perform as it's intended to do.

Adding HTTPS protocol to the refactored code is another way to increase the security of Artemis Financial's web interface. This is obtained in the refactored code by adding the checksum for input validation and a self-signed certificate. In addition, ensuring Spring Boot and other aspects of the code are using the most recent versions will add to the application's security and eliminate significant security risks.

**Reference:**

* *Federal Cybersecurity and Data Privacy Laws Directory*. IT Governance. (n.d.), from https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws
* Java security standard algorithm names. (n.d.). Retrieved April 17, 2022, from https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html
* *Secure coding practice guidelines*. Secure Coding Practice Guidelines | Information Security Office. (n.d.), from https://security.berkeley.edu/secure-coding-practice-guidelines
* *The Hashcode function in Java*. Section. (n.d.). Retrieved April 17, 2022, from https://www.section.io/engineering-education/the-hash-code-function-in-java/