****

# 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** | **22 Feb 2024** | **Matthew Taylor** |  |

## 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

Matthew Taylor

## Algorithm Cipher

The algorithm cypher that I would recommend to Artemis Financial would be Advanced Encryption Standard (AES). This would be used to protect the sensitive data that is collected and stored by Artemis Financial. AES offers three different key sizes of 128, 192, and 256 bits. These key sizes are large which makes them difficult to crack. This is really important for information that is particularly sensitive. However, I would not necessarily recommend the largest key size, because as the key size increases, so does the time it takes to decrypt. I would recommend 128 bits since trying to brute force that would be nearly impossible for most. Another disadvantage is that AES used symmetric encryption rather than asymmetric encryption. This means that there is only one key in use to encrypt and decrypt the data. Despite these few disadvantages, I think that it is still the best option for Artemis Financial as it is plenty secure to the point that many really large industries use it such as banking, healthcare, and even the government uses it to encrypt their top secret data sometimes.

## Certificate Generation

Insert a screenshot below of the CER file.

A computer screen shot of a computer

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated

## Secure Communications

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

A screenshot of a computer

Description automatically generated

## Secondary Testing

Insert screenshots below of the refactored code executed without errors and the dependency-check report.

A screen shot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

## Functional Testing

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

A screen shot of a computer program

Description automatically generated

## Summary

In my code I added a Rest Controller as a class called ServerController. This allows for secure interactions with the API. I also used a hashing cypher to use in a checksum. I used the SHA-512 cypher as it is really secure, and with the highest bits it runs the lowest chance of collisions.

## Industry Standard Best Practices

Using RESTful APIs is one way in which I made sure to be following the industry standard best practices. Another way is that I used a maven dependency check to check the application for any vulnerabilities that may exist in the application due to any dependencies. This should continue to be done periodically as well as making sure that the dependency check plugin stays up to date. This will help the company maintain security.