****

# 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 5](#_Toc102040762)

[6. Functional Testing 6](#_Toc102040763)

[7. Summary 6](#_Toc102040764)

[8. Industry Standard Best Practices 7](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2/17/2023** | **Jonathan Borntreger** |  |

## 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

Jonathan Borntreger

## Algorithm Cipher

The algorithm that I personally would recommend using that fits Artemis Financial’s needs would be SHA-256. SHA stands for secure hash algorithm. It is a very secure way to up the security of your websites. This cipher will turn any input length into an encrypted string with 256 bit length. This makes anyone trying to read what is encrypted virtually impossible. This is one of the most secure hashing functions out there, so it really is the best choice. SHA-256 does not use any key so it is neither symmetric nor asymmetric. It is just a hash function that takes an arbitrary input length into a fixed output length. Cryptography has been around for thousands of years and as time goes on it gets more and more common. Back then they would only use it for secret messages between leaders or during battles. Now encryption is used pretty much everywhere online. For instance, passwords/files are all encrypted to make sure the data stays safe from hackers.

## Certificate Generation

Text

Description automatically generated

## Deploy Cipher

A picture containing logo

Description automatically generated

## Secure Communications

Graphical user interface, text, application, email

Description automatically generated

## Secondary Testing

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

1. **Functional Testing**

I added comments and no new vulnerabilities or errors were found.

Text

Description automatically generated

## Summary

The main area I focused on was to follow secure coding practices. I made sure to add comments so you can understand what is going on in the code. I also made use of cryptography by using SHA-256 to encrypt a message. In this case I used the string “Hello World Check Sum!” If you look back up at the screenshots, you’ll see that this was turned into a random string fixed length. I made sure to add a try and catch block to handle an error happening during the code. It’ll stop the code if the algorithm requested is not available for the project to use. I also made sure to run the dependency check before I made any changes to the code to make sure I wasn’t introducing any more vulnerabilities. In the future is would be beneficial to keep patching the software to remove any new vulnerabilities.

## Industry Standard Best Practices

To keep up with industry standards I made sure to keep security in the front of my coding process. I tried to add comments and validation where I could in order to make sure the code base stays secure. I also made sure to include error handling in the code as well. I also ran dependency checks as I went to make sure I wasn’t adding any new vulnerabilities. This made it a lot easier to find vulnerabilities since I was testing in small increments. It is very valuable to ensure that you follow industry standard best practices. If you are a business owner you want to make sure your customers’ data is secure so that they trust you and keep using you. As a customer you also want to know that your data is in good hands. An unsecure system could lead to data breaches and theft.