****

# 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** | **10/08/2023** | **Michael Moreno** |  |
| **1.1** | **10/11/2023** | **Michael Moreno** | **Algorithm Cipher & Certificate Generation** |
| **1.2** | **10/14/2023** | **Michael Moreno** | **Completed** |

## Client



## Developer

Michael Moreno

## Algorithm Cipher

For Artemis Financial's web application to ensure secure communications and add a data verification step in the form of a checksum, I recommend using the combination of the Transport Layer Security (TLS) protocol along with SHA-256 for hash-based data verification.

* Brief Overview: TLS is a protocol that provides secure data transfer over the internet. It encrypts data in transit to protect it from eavesdropping and ensures data integrity. SHA-256 is a cryptographic hash function that can be used for data verification.
* Hash Functions and Bit Levels: SHA-256 employs a 256-bit hash function, ensuring data integrity through secure checksums.
* Random Numbers: Secure random numbers are generated during the TLS handshake for key exchange, and SHA-256 can be used to create checksums for data verification.
* Symmetric vs. Asymmetric Keys: TLS uses both symmetric and asymmetric keys during its handshake. Asymmetric keys are used for key exchange, while symmetric keys are employed for data encryption.
* History and Current State: TLS is the current standard for secure communication over the internet. It is continually updated to address security vulnerabilities and stay current with the latest cryptographic standards. Implementation: Artemis Financial should integrate TLS into their web application, securing the communication channel. Additionally, they can implement SHA-256 to create checksums for data verification. When data is transferred, they can compute SHA-256 checksums on both ends (sender and receiver) to ensure data integrity. Secure Coding Protocols: Artemis Financial should also follow secure coding practices throughout their software development process. This includes input validation, protection against common vulnerabilities (e.g., SQL injection, cross-site scripting), and ensuring proper key management for encryption. By using TLS and SHA-256 in this manner, Artemis Financial can enhance the security of their web application, safeguarding their client data and financial information while meeting modern security standards and best practices.

## Certificate Generation

A computer screen with white text

Description automatically generated

## Deploy Cipher

A screenshot of a computer

Description automatically generated

## Secure Communications

I could not get my local browser to show secure with a self signed certificate. Likely due to some of the work security that I have on my home computer.

A screenshot of a computer

Description automatically generated

## Secondary Testing

A screenshot of a computer program

Description automatically generated

A screenshot of a computer error

Description automatically generated

## Functional Testing

Introduced error handling and logging.



## Summary & Industry Standard Best Practices

I applied industry standard best practices for secure coding to mitigate against known security vulnerabilities.

1. **Hashing Algorithm Selection:**
   * The industry standard best practice is to use strong and secure hashing algorithms.
2. **Error Handling:**
   * I implemented robust error handling with try-catch blocks in critical areas of the code. This is a fundamental secure coding practice. It helps the application gracefully handle exceptions and prevents potential crashes or exposing sensitive information.
3. **Logging:**
   * I introduced logging using the Java **Logger** class, another best practice. Logging is vital for monitoring and diagnosing issues, as it provides a record of the application's behavior. In case of errors or security incidents, logs can be invaluable for incident response and forensic analysis.

The value of applying these industry standard best practices for secure coding to the company's overall wellbeing is significant:

1. **Security Assurance:**
   * By following these practices, the company can ensure that its software is less vulnerable to known security threats. This reduces the risk of data breaches, unauthorized access, and other security incidents.
2. **Maintaining Reputation:**
   * Security breaches can lead to significant reputational damage. Secure coding practices help protect the company's image and brand by reducing the likelihood of security incidents.
3. **Regulatory Compliance:**
   * Many industries have strict regulatory requirements regarding data protection and security. Secure coding practices assist in achieving compliance with these regulations, preventing legal and financial consequences.
4. **Cost Savings:**
   * Addressing security vulnerabilities during development is more cost-effective than fixing them after deployment. The cost of dealing with a security breach can be substantial.
5. **Customer Trust:**
   * Secure applications build trust with customers and users. They are more likely to use and recommend the company's products or services when they know their data is protected.

In summary, applying industry standard best practices for secure coding not only protects the software application but also has a direct and positive impact on the company's overall security posture, reputation, compliance, and financial health. It's a proactive approach to mitigating security risks and ensuring the long-term success of the company.