****

# Artemis Financial Vulnerability Assessment Report

Table of Contents

[Document Revision History 3](#_Toc32574607)

[Client 3](#_Toc32574608)

[Instructions 3](#_Toc32574609)

[Developer 4](#_Toc32574610)

[1. Interpreting Client Needs 4](#_Toc32574611)

[2. Areas of Security 4](#_Toc32574612)

[3. Manual Review 4](#_Toc32574613)

[4. Static Testing 4](#_Toc32574614)

[5. Mitigation Plan 4](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **3/24/2024** | **Brendalis Sanchez** |  |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In the report, identify your findings of security vulnerabilities and provide recommendations for the next steps to remedy the issues you have found.

* Respond to the five 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 One Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Brendalis Sanchez

## Interpreting Client Needs

Client security needs span from establishing secure communication channels to complying with international financial transactions, adhering to government-imposed encryption and trade restrictions, and protecting against cyber threats like SQL injections and phishing. The client's push towards technological modernization also involves integrating the latest web technologies with vigilance towards emerging security vulnerabilities.

Consider these facets in relation to the client's situation:

* Secure Communication Imperative: Ensuring the integrity and privacy of financial exchanges is crucial for preventing data breaches and preserving customer confidence.
* International Transaction Compliance: Artemis Financial's global operations require adherence to a variety of international cybersecurity protocols and privacy regulations, including the GDPR.
* Governmental Regulatory Compliance: The company must conform to legal standards for secure communication, including specific encryption requirements and export controls.
* Defending Against Cyber Threats: Threats like SQL injection, cross-site scripting, DDoS attacks, and phishing pose risks to both present and prospective operations.
* Technology Modernization and Security: Integration of new web technologies must be conducted alongside the secure use of vetted open-source resources, staying informed of newly identified web application vulnerabilities.

## Areas of Security

Artemis Financial's web platform needs to address principal security domains such as data encryption for financial data protection, user authentication and access management, input validation to block injection threats, secure session handling, meticulous error tracking and logging for incident management, and vigilant dependency oversight to guard against compromised external code. Each security domain is essential for protecting against cyber threats and ensuring regulatory compliance.

Refer to the security domains listed in the Vulnerability Assessment Process Flow Diagram and explain their importance for Artemis Financial's web application:

* Data Encryption
* User Authentication and Access Control
* User Input Validation
* Session Handling
* Incident Tracking and Logging
* Third-Party Code Dependency Oversight
* Infrastructure Security

Not all domains might be pertinent—articulate the significance of each chosen domain.

## Manual Review

Manually inspect the code to examine areas including:

* Risks in data storage and transfer methods.
* Vulnerabilities due to weak authentication processes.
* Inadequate input checks potentially leading to SQL injection.
* Flaws in session handling protocols.
* Oversights in error logging that could expose sensitive information.
* Usage of obsolete third-party resources.

Record specific weaknesses and their codebase locations.

## Static Testing

Static analysis employs tools like dependency-check plugins to identify potential security risks within the codebase without executing the program. After the plugin is set up, a list of discovered vulnerabilities is generated, complete with identifiers, summaries, and mitigation suggestions derived from the analysis report. Acknowledge any previous vulnerability documentation or detection for correct recognition.

Upon completing the dependency-check plugin setup and conducting a static analysis:

* Vulnerability Identifiers: Catalog vulnerabilities along with their identifiers.
* Vulnerability Summaries and Mitigation Advice: Summarize each vulnerability and propose corrective actions as per the analysis report.
* Source Recognition: Credit any pre-existing vulnerability reports or discoveries.

## Mitigation Plan

The response strategy to identified vulnerabilities includes updating or replacing weak dependencies, enhancing authentication and session protocols, enforcing comprehensive input validation, securing data management and transfer, and refining error tracking and incident logging. Each pinpointed weakness requires a specific, tailored solution.

Following the manual inspection and static analysis, draft a series of steps to address the found vulnerabilities:

* Update or replace vulnerable dependencies.
* Bolster user verification and session procedures.
* Introduce thorough input validation measures.
* Ensure the security of data management and communication channels.
* Advance error handling and event logging processes.
* Modernize or change outdated software libraries.

Detail individualized steps for each recognized vulnerability.

In summary, the security evaluation for Artemis Financial's web application entailed an extensive review aimed at fortifying the system against external threats, echoing the mantra that security is a collective responsibility. The conducted reviews and analysis exposed vulnerabilities within vital security aspects, including but not limited to data encryption, user authentication, input validation, session control, error management, and code dependency integrity.

These findings were recorded with actionable solutions, laying the groundwork for a comprehensive countermeasure strategy. This blueprint is a tactical roadmap for fortifying the application against both existing and emergent threats, safeguarding critical financial information, and ensuring adherence to pertinent legal standards. Such security implementations are pivotal for Artemis Financial as it seeks to upgrade its operations and establish its presence as a top-tier financial service provider in a competitive industry.