****

# 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** | **November 20, 2022** | **Dhiren Gurung** |  |

## 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

Dhiren Gurung

## Interpreting Client Needs

Artemis Financial company is a consulting company and provides the financial plans. Client’s company provides the saving, retirement, investments, and insurance. Artemis Financial company might have the external threats because there is the financial transaction over the web application and the company needs to security to protect their software from the possible external threats. Artemis Financial company wants to modernize their services and wants to use secure software for their clients. Artemis has the web-based application to operates their transactions.

## Areas of Security

APIs: APIs is another important software security area because it safely delivers the request from Artemis Financials’ web-based application and response from servers using the Hypertext Transfer Protocol.

Cryptography: Cryptography is important for Artemis Financial to keep the user information secure and through the cryptography, it converts the readable data into unreadable data.

Client/Server: Client/Server is an important area of the software security for Artemis Financial web-based application because it secures the data transfer from the server and protect do safe deliver.

Code Error: There might have several code errors during the software development and updates. To protect from the Artemis Financials’ web application code error should be minimized so that it protects from the external threats as well as increase the reliabilities of the software.

Encapsulation: To protect from the direct access, encapsulation ensures Artemis Financials’ application unauthorized access, and it is very important to deny the third-party access to the application.

## Manual Review

According to the vulnerabilities assessment of the Artemis Financials’ report indicated that there is the vulnerabilities in validation because there is low base score and improper validation where the attacker may attack software through input validation. Another issue of the vulnerability cryptography based on the report. There is information exposure an android user where attackers may obtain sensitive information.

## Static Testing

Information Exposure where base score is low (3.3) where the code is **CVE-2015-6644** (OSSINDEX. There is a CWE-320 Key Management Errors where the CVSSv3 base score is 3.7 that is the vulnerability where the third party can reveal the details of the users. There is CWE-354 Improper Validation of Integrity Check Value where base score is 3.6 and 4.4 where the attackers are allowed through the input validation.

## Mitigation Plan

Based on the manual review of the testing report the vulnerabilities should be fixed to protect the data from the attackers. Validation should more accurate, to keep secure user’s information, cryptography should be strong so that the readable data converts into the unreadable. For the android user attacker may have the higher access information so the android issued should be fixed.