****

# CS 305 Project One

**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** | **9/10/2021** | **Christal Willett** |  |

## Client



## Instructions

Deliver this completed vulnerability assessment report, identifying your findings of security vulnerabilities and articulating recommendations for next steps to remedy the issues you have found.

Respond to the five steps outlined below and include your findings. Replace the bracketed text on all pages with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

## Developer

Christal Willett

## 1. Interpreting Client Needs

Determine your client’s needs and potential threats and attacks associated with their application and software security requirements. Consider the following regarding how companies protect against external threats based on the scenario information:

* What is the value of secure communications to the company?
* Are there any international transactions that the company produces?
* Are there governmental restrictions about secure communications to consider?
* What external threats might be present now and in the immediate future?
* What are the “modernization” requirements that must be considered, such as the role of open-source libraries and evolving web application technologies?

Artemis Financials is a financial consulting company; Their priority involves creating customized financial plans for its clients and maintains security over those plans and other personal information. Protecting sensitive business/client/intellectual information using a plan of action; This plan of action also consists of team members finding and recording (vulnerability assessment) security vulnerabilities in a given software; As this company is a financial type of business, maintaining secure and encrypted data (i.e., events, clientele/employee address, phone, email, et cetera) is imperative for similar institutions of all magnitudes. As the profile states, Artemis Financial indeed conducts business with customers/agencies/business owners worldwide. Furthermore, Artemis Financials also provides business services and assessments to its clients via the web application, which will help me to identify additional security measures that can be considered in the aspect of business and transactions. I do not think there are any governmental restrictions to consider being that the company conducts business with people around the world. Some threats that may become present soon or later in the future might include injection attacks or even attacks that send custom modified transactions to the web application in an effort to crash the system. Another threat might be someone using stolen information in order to blackmail someone into getting what they want, i.e., money, favors, lies, et. Cetera. Requirements that Artimus Financials must consider on a regular maintenance basis, upgrading obsolete or out-of-date systems to the current standards for best practices; In addition to “modernized” systems, updating code or design from simple input functions to where information is stored on a user’s profile on the application; Furthermore, maintain secure code can also be considered as modern requirements to consider in relation to web applications and the libraries that are used in those applications to accurately secure user information and transaction information/history.

## 2. Areas of Security

Referring to the Vulnerability Assessment Process Flow Diagram, identify which areas of security are applicable to Artemis Financials’ software application. Justify your reasoning for why each area is relevant to the software application.

The identified areas of security that can be applied to the Artemis Financials software are identified with priority in mind; Input validation alone should not be the primary action taken to prevent risks and cyber-attacks, however, in addition to other areas of security, input validation is a security method ensuring that certain forms of data can be entered into a data field. As API can have the tendency to reveal parts of the application that handle identifiers and other sensitive application designs that opens a wide surface for administrative access control, golden to a hacker. Be that as it may, the API area of security offers a guideline to approaching this security vulnerability. Maintaining encrypted data ensures that information is correct and secure. The next area of security to be considered is the cryptography area; The team will focus on encrypting data, with an emphasis on encrypting the correct data; Furthermore, data within any given storage component requires that contents be encrypted properly. Code error handling will have the team working together to eliminate errors on the application i.e., error web pages, errors within a user account. Reducing errors in code can reduce the exposure of sensitive client/business information and ultimately eliminating the vulnerability. Secure coding practices and maintaining the best quality of code is always helpful for teams to produce applications and features that have fewer errors and/or unforeseen behaviors or glitches within the application/application feature. In addition to best coding practices in the industry, ensuring that the data structures and functions with the application are contained or encapsulated in a way that reduces the chances of unauthorized access. Ultimately, once the team has considered each of the areas of security, performing a final review of the code to locate and identify bugs, errors, unexpected behavior issues, and other issues that could be present in the applications code.

## 3. Manual Review

Continue working through the Vulnerability Assessment Process Flow Diagram. Identify all vulnerabilities in the codebase by manually inspecting the code.

Input validation as the users’ input will need to be validated. This security measure ensures that the correct data or information is being entered into the fields. API as the web application’s length of user input as well as numerical input that will need to be validated through string APIs. Also, the application will need to communicate privately from the user to the client/server. Code error because errors from pages “not existing” or from any given individual entering the incorrect type of input into the information fields can be risky if not handled properly; Must be handled quickly and securely. Secure coding ensures that the code quality is adequate as well as that the applications’ code and design follow industry-best standards and practices.

## 4. Static Testing

Run a dependency check on Artemis Financials’ software application to identify all security vulnerabilities in the code. Record the output from the dependency check report. Include the following:

1. The names or vulnerability codes of the known vulnerabilities
2. A brief description and recommended solutions provided by the dependency check report
3. Attribution (if any) that documents how this vulnerability has been identified or documented previously

The codes of the known vulnerabilities include the following: CVE – 2002, CVE – 2003, CVE – 2004, CVE – 2005, CVE – 2006, CVE – 2007, CVE – 2008, CVE – 2009, CVE – 2010, CVE – 2011, CVE – 2012, CVE – 2013, CVE - 2014, CVE - 2015, CVE – 2016, CVE – 2017, CVE – 2018, CVE – 2019, CVE – 2020, CVE – 2021; Solutions to vulnerabilities in software or web applications involve updating computer systems and software to up-to-date versions if any;

## 5. Mitigation Plan

After interpreting your results from the manual review and static testing, identify the steps to remedy the identified security vulnerabilities for Artemis Financials’ software application.

The mitigation plan that I’ve to consider includes steps for improving security measures for solutions to common and other known vulnerabilities among computer systems, both personal and business machines. Furthermore, steps to take include changing request parameters to the <body> to maintain the security of sensitive user data, plan and carry out a plan of action for authentication solutions. All software and related tools used in tandem with other software must be updated to the most current version of the platform. Additionally, trading the HTTP protocol for HTTPS protocol for improved privacy or encrypted data maintaining the safety of personal and business-related data.