****

# 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** | **5/22/22** | **Emma McCarter** |  |

## Client



## Developer

Emma McCarter

My client Artemis Financial is goal oriented and desires to modernize their business plan. In order to obtain modernization, they must implement and apply the most up-to-date software security. Artemis Financial wants our help to secure their operation from all external threats. They value secure communications as a part of their company, and it is our mission to execute all requirements, so they feel their software is secure for all current and prospective clients. For Artemis Financial, secure communication ensures that no confidential/private data is tampered or encrypted while being sent and received. Potential external threats, specifically for Artemis, are other software security companies, wanting to know their system and how they operate, or hackers who want to extort the company, whether for money or information. Artemis does have the ability to make international transactions, only if access is granted and, in this case, there are no government restrictions on secure communications. Lastly, the main modernization requirement is the ever-evolving web application technologies. Modernization refers to user accessibility and feasibility, without either of those, a user is likely to exit an application and search for a better company/site.

While reviewing the Vulnerability Assessment Process Flow Diagram, the areas of security that are applicable to Artemis Financial’s software application are Input Validation and Client/Server. Input Validation, due to Artemis using RESTful APIs, is a top choice and because it is a safeguard for all web applications. Validation is the first line of defense for security, creates that protection for what data and allowed versus what should be rejected. Client/Server ensures that client information, or data being sent internally, is secure. We will aid Artemis in this process, client/server communication is the data most sought after from hackers and needs to be securely sent and received.

After manually inspecting the code, additional vulnerabilities include APIs and Encapsulation. APIs, which Artemis currently use, can create concrete security for any software, but if they are not properly created and secured, they can be a huge weakness, especially for Artemis since they want to modernize their software security, which includes tighter, more secure security. Encapsulation is a process which encapsulates functions within an operating function (Veracode). If the function is not properly structured, gaps in the code can allow unwanted/restricted access to become accessible.

A dependency check was run on Artemis Financial’s software application to identify all security vulnerabilities in the code. The output from the dependency check report were the following – 38 dependencies scanned, 74 vulnerabilities found, and 0 vulnerabilities suppressed. Below are the vulnerability codes with a short description, all coming directly from my dependency report (See attached document).

1. [CVE-2016-1000352](https://nvd.nist.gov/vuln/detail/CVE-2016-1000352) **is seen as unsafe and it should be removed.**
2. **CVE-2020-10693 is a bug and it allows hackers to bypass input controls set up by developers.**
3. CVE-2020-25649 is a flaw where the entity expansion is not secured properly, this is seen as a high threat.
4. CVE-2020-9488 is improper validation of certificate that could allow the connection to be intercepted by a hacker and lead to a security attack.
5. CVE-2020-22950 can cause issues with unsupported versions, this can affect service conditions.
6. CVE-2022-27772 was a vulnerable to hijacking, it only affects products that are no longer supported by the server.
7. CVE-2022-29885 does not protect against all threats.

The steps needed to remedy the identified security vulnerabilities for Artemis Financials are to modernize its software security so it can evolve as advancements have, as well as hackers. All the vulnerabilities listed above can be reviewed and code functionality can be regenerated to ensure security. Functions will have to be removed to make sure hackers cannot manipulate externally, or even internally.

References

*Encapsulation vulnerabilities*. Veracode. (n.d.). Retrieved May 22, 2022, from https://www.veracode.com/security/encapsulation-vulnerabilities