

**CS 305 Project One**

**Artemis Financial Vulnerability Assessment Report**

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| **1.0** | **[09/26/2021]** | **Jordan Stelivan** |  |

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

Jordan Stelivan

**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?**

They are dealing with multiple clients who are trasmitting sensetive data (i.e. savings, retirement, and investment account information) for consulting. This data will often involve directly linking accounts to Artemis Financial as well as discussions around owned properties. Making Secure communicaitons one of the top priorities for this company.

* **Are there any international transactions that the company produces?**

Yes, any clients that seek consulting from Artemis Financial could come from any country across the globe. Secondly, any information a client may posses could link to other, international, accounts or holdings.

* **Are there governmental restrictions about secure communications to consider?**

According to NCSL (<https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>), many states within the U.S. require adequate secuirty when handling personal information. It also mentions that "more than half the states" have data disposal laws. These are some of the things to consider when addressing the web applications secure communications and data handling processes.

* **What external threats might be present now and in the immediate future?**

Competing companies and 'Dark net' hackers may currently be the biggest threat. Corporate espianoge, client poaching, and information theft are are real security issues we need to be aware of when developing security for this application.

* **What are the “modernization” requirements that must be considered, such as the role of open source libraries and evolving web application technologies?**

The most important "modernization" requirement would be that of mobility and access. The application will be required to run on various forms of browsers, as no one browser is used by everyone, and the application will need to be acessible on mobile platforms (this could be seen as an extentsion of the 'running on various browsers', but could also include the release of a seperate mobile application).

**2. Areas of Security**

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

Input Validation: Our first concern will be the input validation aspects of the application. We do not want any end user to be able to access other users information (even if by accident), or worse, the administrative aspects of the application. Validating user input and confirming user prvleges will prevent any access issues within the system.

APIs (Optional): Depending on how the application interacts with user account information, we may need the application to address other Financial institution applications and their API.

Cryptography: Secure encryption, especially with concerns for 'user to consultant' communications, will be a must in ensuring client information is not picked up anywhere along the process. Likewise, all communications between user financial institutions and Artemis Financial will need to be encrypted properly.

Client/Server: Our main concern here will be mitigating 'web proxy interception' attacks. Most users will be accessing their account information from personal computers, or mobile devices, and as such we want to make certain we can validate the incoming information is to be trusted by the system.

Code Quality: As always, Code Quality is a must. Keeping the application code well written will hopefully prevent any SQL injections and stop any invaders from gaining access to the raw data within the application.

**3. Manual Review**

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

Upon inspecting the code we can see the following areas as possible vulnerabilites; For the first level we're dealing with Input Validation, Client/Server, Code Error, and Code Quality. Within the second level; Controllers, Data Access, and Services.

**4. Static Testing**

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

* **The names or vulnerability codes of the known vulnerabilities**

The list of vulnerability codes are as follows:

bcprov-jdk15on-1.46.jar, log4j-api-2.12.1.jar, snakeyaml-1.25.jar, jackson-databind-2.10.2.jar, tomcat-embed-core-9.0.30.jar, hibernate-validator-6.0.18.Final.jar, spring-core-5.2.3.RELEASE.jar, and spring-jcl-5.2.3.RELEASE.jar

* **A brief description and recommended solutions provided by the dependency check report**

Most of the solutions provided by the check report suggest updating various libraries and dependancies to more current version that solve the listed issues.

* **Attribution (if any) that documents how this vulnerability has been identified or documented previously**

Published Vulnerabilities (CVE-2020-9488), includes a list of references on the documented issues.

**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 Financial’s software application.*

Based on our static testing, our first steps for improving our software's security is to update some of our older libraries and dependancies being used within the applicaiton. I.e. JDK 1.5 to JDk 1.7 (one of the listed vulnerabilities exists in the 1.5 version of JDK, but has since been patched by the 1.7 JDK). We also need to update our certificate validation and ensure there is no "host mismatch in Apache Log4j SMTP appender" as pointed out by CVE-2020-9488 under the log4j-api-2.12.1.jar reported issue.