****

# 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** | **01/18/2023** | **Austin Sonka** |  |

## 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

Austin Sonka

## Interpreting Client Needs

Artemis Financial is a financial business that deals with customers’ money and goes over the customers’ goals, wants, and needs with their money. Having access to many customers’ money and valuable information makes the business a hacker paradise if they can get in. This brings the first concern to us that security is a big need for this company in order to be successful. The second concern would be communication with the government, the company must deal with the government’s regulations since Artemis heavily deals with money, transactions, and stocks. If the company fails to communicate with the government, then the situation can fail to be insured and lose customer trust. Some present and future concerns could be security, as technology is ever growing, the need for updates and patches grow at the same rate. This would make sure the data is protected along with the API and the structure of the entire network. However, a current requirement that adds an extra layer of security is the two-factor authorization. Two factor authorization allows the customer to not only add a single password but also security questions or even a text message to their number giving them a special code needed to finalize the login.

## Areas of Security

After reviewing the Vulnerability Assessment Process Flow Diagram (VAPF), the number one area of security that needs looking at is securing the code. The code is like a root of a tree, there needs to be a strong baseline for the tree to grow upward and strong. With poor code or weeks roots can lead to pests and other diseases in the roots that can destroy the tree from within. This brings us to errors like too many login attempts, password resets, and username resets should be handled by a department on the Artemis Financial side. Things like RESTful API and web services need to highly secure as valuable information and input is being handled

1. **Manual Review**

When there is a request, there are not validate for their authority. This can lead to attacks from any hacker who sees this hole in the code.

To piggyback off the first issue, this is no system to validate the verification. This can lead to the same problem listed above.

The web address is missing a secure HTTPS. This loses customer confidence as it is not a secure link anymore.

## Static Testing

bcprov-jdk15on-1.46.jar – update to latest version

* CVE-2013-1624
* CVE-2015-6644
* CVE-2016-1000341
* CVE-2016-1000342
* CVE-2016-1000343
* CVE-2016-1000352
* CVE-2017-13098
* CVE-2018-1000613
* CVE-2018-5382
* Log4j-api-2.12.1.jar – update to latest version
* CVE-2020-9488
* Snakeyalm-1.25.jar – update to latest version
* CVE-2017-18640
* Jackson-databind-2.10.2.jar - update to latest version
* CVE-2020-25649
* Tomcat-embed-core-9.0.30.jar – update to latest tomcat version
* CVE-2019-17569
* CVE-2020-11996
* CVE-2020-13934
* CVE-2020-1938

## Mitigation Plan

In conclusion, to further this business we need to assess the current and future problems in security like changing the web base to HTTPS to not only gain customer confidence but keep the data secure. The second would be to add a two-factor authentication system to protect customers’ login credentials and information. Fix the dependencies we found in the static testing. Last but not least would be to do a hard check on the code to really make sure it is secure.