****

# 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** | **July 18, 2021** | **Andrew Wepplo** |  |

## 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

Andrew Wepplo

## 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?

*Secure communications are essential to the company, especially because they handle the financial policies and the physical resources of their customers, and this can always be the target of threats and different forms of attacks. There could be international transactions that the company produces, therefore, they should be considered and prepared for. In addition, any company that handles finances is regulated by government communication restrictions to avoid corruption, mismanagement or collapse. There are always going to be threats towards financial institutions which typically stem from access to PII of the customers and fraud on their network linked accounts. There are several requirements that must be considered but a very important system to include would be an open-source library for its ability to reduce handling cost, and errors and to maintain easy and convenient access to all of the data and to support growth and efficiency.*

## 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.

*Creating code that follows the best security practices is essential to reduce the threat of attacks and breaches in personal information and specifically in this instance the client/ server connections must be secure because they could easily provide entry points for intruders to gain access to the data being sent between the company and its customers. Also, there are several other relevant areas of security including ensuring the code is error free, and input validation needs to verify that the customers that should have access to their various accounts are validated correctly. Lastly, API’s are extremely pertinent because Artemis used a RESTful web API to maintain protected communications and their main goal is ensuring the security of this specific interface and finding the applications vulnerabilities.*

## 3. Manual Review

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

*There is not a proper login/ authentication process in place currently, and there is no way to validate the requests, which makes the system unnecessarily vulnerable to outside attacks.*

## 4. Static Testing

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

*a. bcprov-jdk15on-1.46.jar Multiple vulnerability recommendation: complete current update.*

1. *CVE-2013-1624*
2. *CVE-2015-6644*
3. *CVE-2015-7940*
4. *CVE-2016-1000338*
5. *CVE-2016-1000339*
6. *CVE-2016-1000341*
7. *CVE-2016-1000342*
8. *CVE-2016-1000343*
9. *CVE-2016-1000344*
10. *CVE-2016-1000345*
11. *CVE-2016-1000346*
12. *CVE-2016-1000352*
13. *CVE-2017-13098*
14. *CVE-2018-1000613*
15. *CVE-2018-5382*

*b. Log4j-api-2.12.1.jar Single vulnerability recommendation: complete current update.*

1. *CVE-2020-9488*

*c. Snakeyalm-1.25.jar Single vulnerability recommendation: complete current update.*

1. *CVE-2017-18640*

*d. Jackson-databind-2.10.2.jar Single vulnerability recommendation: complete current update.*

1. *CVE-2020-25649*

*e. Tomcat-embed-core-9.0.30.jar Multiple vulnerability recommendation: complete current update.*

1. *CVE-2019-17569*
2. *CVE-2020-11996*
3. *CVE-2020-13934*
4. *CVE-2020-13935*
5. *CVE-2020-13943*
6. *CVE-2020-17527*
7. *CVE-2020-1935*
8. *CVE-2020-1938*
9. *CVE-2020-8022*
10. *CVE-2020-9484*
11. *CVE-2020-24122*

f. *Hibernate-validator-6.0.18Final.jar Single vulnerability recommendation: complete current update.*

1. *CVE-2021-0693*

*g. Spring-core-5.2.3.RELEASE.jar Single vulnerability recommendation: complete current update.*

1. *CVE-2020-5421*

## 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.

*To remedy these security vulnerabilities identified above, the recommended focus is on securing customer PII, by switching to HTTPS for all communications between client/ server and two factor authentication must be executed to validate identity of users trying to gain access and to protect their data while accessing the interface and make an attack on the system much more difficult to acquire the information.*