****

# 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** | **01/23/2022** | **Alexis Alexander** |  |

## 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

Alexis Alexander

## 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 Financial is a financial consulting company that develops individualized financial plans for its customers. The financial plans that are developed include retirement plans, savings plans, insurance plans, and investment plans. The customers of Artemis Financial are not solely based in the United States which leads to international transactions that will need to be produced.

Artemis Financial would like our assistance with securing their RESTful web API from any external threats. While securing and modernizing the web API, we need to make sure that Artemis Financial is still able to meet the guidelines for secure communications internationally and locally within the United States. The external threats that may present themselves now and, in the future, include data interception, phishing attacks, denial of service attacks, and ransomware.

Modernization of the current API usually translates to using cloud services and open-source libraries. Transitioning to these services does not guarantee any type of security so it will be important to regularly check open-source libraries for vulnerabilities and implement extra security if a cloud service or any other service (infrastructure, platform, software) is being used to avoid any API vulnerabilities.

## 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: The RESTful API will take input from both the client and the customer. This input will need to be validated to avoid possible system disfunction due to inappropriate or incorrect input.
* API’s: The current system includes a RESTful API. When the system is modernized the RESTful API will still need to be able to properly authenticate users and determine the access needed to the API based upon the user.
* Cryptography: The client deals with customers’ bank information and personal information for financial planning purposes. This information does not need to be stored in plain text and will need to be encrypted.
* Client/Server: The client and server will need to establish a secure connection to help prevent any data interception.
* Code Error: Any error from input from anyone who has access to the system needs to be properly handled to prevent system disfunction. The code also needs to handle multiple requests as an attacker will sometimes try to overwhelm the API with multiple requests and cause a denial-of-service attack.
* Encapsulation: The data within the system needs to be properly encapsulated to not expose classes and functions of the web application to unauthorized users.

## 3. Manual Review

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

* In CRUDController, input for business name is not validated.
* In DocData, access control needs to be implemented to read document. The access parameters need to ensure that an Artemis Financial employee or client has access to the document and that the user accessing the document should be accessing the document.
* Data is not encapsulated. For example, the account number and balance that is presented in customer.
* It does not look like the current service uses HTTPS.
* There does not seem to be an authentication system for users. There should be a required username and password required with two factor authentication to gain access to the system in any manner.

## 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

| **Dependency** | **Vulnerability IDs** | **Solutions** | **Attribution** |
| --- | --- | --- | --- |
| [bcprov-jdk15on-1.46.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l1_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) | cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.46:\*:\*:\*:\*:\*:\*:\* cpe:2.3:a:bouncycastle:bouncy\_castle\_crypto\_package:1.46:\*:\*:\*:\*:\*:\*:\* [cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Abouncycastle&cpe_product=cpe%3A%2F%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api&cpe_version=cpe%3A%2F%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api%3A1.46) cpe:2.3:a:bouncycastle:the\_bouncy\_castle\_crypto\_package\_for\_java:1.46:\*:\*:\*:\*:\*:\*:\* | Update to version 1.70 | Unknown |
| [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l3_7fd00bcd87e14b6ba66279282ef15efa30dd2492) | [cpe:2.3:a:redhat:hibernate\_validator:6.0.18:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aredhat&cpe_product=cpe%3A%2F%3Aredhat%3Ahibernate_validator&cpe_version=cpe%3A%2F%3Aredhat%3Ahibernate_validator%3A6.0.18) | Red Hat JBoss Enterprise Application Platform 7.3 for RHEL 8 | The vulnerability has been identified and documented via Bugzilla.  https://bugzilla.redhat.com/show\_bug.cgi?id=CVE-2020-10693 |
| [jackson-databind-2.10.2.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l5_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | [cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Afasterxml&cpe_product=cpe%3A%2F%3Afasterxml%3Ajackson-databind&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson-databind%3A2.10.2) cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | Red Hat JBoss Enterprise Application Platform | The vulnerability has been identified and documented via Bugzilla  https://bugzilla.redhat.com/show\_bug.cgi?id=1887664.  \ |
| [log4j-api-2.12.1.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l10_a55e6d987f50a515c9260b0451b4fa217dc539cb) | [cpe:2.3:a:apache:log4j:2.12.1:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Alog4j&cpe_version=cpe%3A%2F%3Aapache%3Alog4j%3A2.12.1) | Update to version 2.13.2 | The vulnerability has been documented on via Apache Issues  https://issues.apache.org/jira/browse/LOG4J2-2819 |
| [logback-core-1.2.3.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l12_864344400c3d4d92dfeb0a305dc87d953677c03c) | [cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aqos&cpe_product=cpe%3A%2F%3Aqos%3Alogback&cpe_version=cpe%3A%2F%3Aqos%3Alogback%3A1.2.3) | Update to version 1.3.0-alpha11 or 1.2.9 | The vulnerability has been documented via qos.ch  https://jira.qos.ch/browse/LOGBACK-1591 |
| [snakeyaml-1.25.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l14_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) | [cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Asnakeyaml_project&cpe_product=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml&cpe_version=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml%3A1.25) | Update to version 1.26 | The vulnerability is documented via fedora  https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/PTVJC54XGX26UJVVYCXZ7D25X3R5T2G6/ |
| [spring-aop-5.2.3.RELEASE.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l15_9cdd9a1dd636331767fffcc7fe49a7bb00e7b34b) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) [cpe:2.3:a:vmware:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3) | Update to version 5.2.9 | The vulnerability is documented via tanzu vmware  https://tanzu.vmware.com/security/cve-2020-5421 |
| [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l17_3734223040040e8c3fecd5faa3ae8a1ed6da146b) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) [cpe:2.3:a:vmware:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3) cpe:2.3:a:vmware:springsource\_spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* | Upgrade to version 5.3.14 or higher | The vulnerability is documented via tanzu vmware  https://tanzu.vmware.com/security/cve-2021-22060 |
| [tomcat-embed-core-9.0.30.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l18_ad32909314fe2ba02cec036434c0addd19bcc580) | [cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Atomcat&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A9.0.30) [cpe:2.3:a:apache\_software\_foundation:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_software_foundation&cpe_product=cpe%3A%2F%3Aapache_software_foundation%3Atomcat&cpe_version=cpe%3A%2F%3Aapache_software_foundation%3Atomcat%3A9.0.30) [cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_tomcat&cpe_product=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat&cpe_version=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat%3A9.0.30) | Update to version 9.0.36 or 10.0.0-M6 | This vulnerability has been documented via Debian  https://www.debian.org/security/2020/dsa-4727 |
| [tomcat-embed-websocket-9.0.30.jar](file:///C:\Users\asale\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l20_33157f6bc5bfd03380ebb5ac476db0600a04168d) | [cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Atomcat&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A9.0.30) [cpe:2.3:a:apache\_software\_foundation:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_software_foundation&cpe_product=cpe%3A%2F%3Aapache_software_foundation%3Atomcat&cpe_version=cpe%3A%2F%3Aapache_software_foundation%3Atomcat%3A9.0.30) [cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_tomcat&cpe_product=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat&cpe_version=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat%3A9.0.30) | Update to version 9.0.36 or 10.0.0-M6 | This vulnerability has been documented via Debian  https://www.debian.org/security/2020/dsa-4727 |

## 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 mitigate the vulnerabilities within the dependencies used, we can update the dependencies to newer versions that resolve the vulnerabilities that were found. For the two vulnerabilities that cannot be solved with a simple upgrade, we can download a Redhat JBoss Enterprise Application to resolve those issues. For the coding vulnerabilities, we can make the transition to HTTPS for all communication. We also need to implement an authentication system for access to the API. All customer data needs to be encrypted and all information that requires input will require input validation. Exception handlers should be included with controllers to delegate how exceptions are handled by the system when incorrect items are entered.