****

# 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** | **[7/10/2023]** | **[Matthew Bartrum]** |  |

## 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

[Matthew Bartrum]

## Interpreting Client Needs

Artemis Financial to looking to update their operation to keep up with the current market. The company needs software that has a clean web API that will protect them from external threats. It is our goal to give them the best standard with OWASP. For their website we need to make sure that they have secure processes and infrastructure. Let members have stronger authentication to their accounts to stray away from members getting hacked. While they update their new system, we must give them a time frame for each part of the project. This will align with what they need to do legally to keep their members updated and to let them know if they need to take any action if any outage will happen for a time. Finally, we need to investigate the code they currently have and how we can make it better for them. This could include with members having CD, drafts, loans, and savings accounts. We need to find out what areas of the code need the most amount of work for security and minimize each one risk.

## Areas of Security

Below is the list of areas of security that Artemis is going to need.

API – Artemis dealing with clients all over the world and these members will be always using the system. We need to validate and make sure that these applications are easy to use and do what they are supposed to do. This goal is not only for the clients, but for the employees that work there. Proper validation and accounts should only be privilege to what the role is. An example of this would be that tellers are allowed to view and add payment to a loan but are not allowed to refinance a loan. That would be only allowed for the loan officer. For the client side that are only allowed to deal with accounts that they create or are shared with. For the employee side we need to have proper roles made and have that documentation.

Input Validation – We need to make sure that data is not being improperly pulled. For example, clients should not be able to take out more than they have, and should not be able to add money, unless it is processed. We need to make sure that correct syntax fields are made to enforce good business context. Should have file upload validation for each client to allow tellers to know who they are dealing with and that it matches the account. Also, for users to share a copy of the title or any documentation is in the correct file format.

Code Quality – As Artemis Financial is transferring to a new system they need to make sure it’s good quality. The system needs to not only be following government standards while having documentation with that. The program needs to run good and the code itself needs to be easy to understand. Need to have clear comments that people can look back on. Need to look how data flows through the program and make sure the process is correct.

Encapsulation- Artemis has many accounts that deal with information being shared in different areas. Accounts should not have access to other accounts unless allowed in a protocol. When these accounts are messing with data from logs and that they are properly being done.

Cryptography – website needs a way to keep ways hard from people able to hack from the website itself and keep things crypted.

## Manual Review

While looking through the code I see a warning over the DocData.jave from src/main/java. On line 26 get a warning that states the value of the local variable con is not used. Junit testing went well and showed no errors throughout the program. The system is using a JRE System Library version 1.8 which needs to be updated to the newest version. While going through the next couple weeks of testing we need to test with Junit and maven while doing the updates.

## Static Testing

While looking at the report we have plenty of vulnerabilities that are from the range of critical to low. This is going to be the list and idea solutions for each of them. Below is a list of all the vulnerabilities, risk level, and solutions to each.

|  |  |  |  |
| --- | --- | --- | --- |
| Dependency` | Highest Severity | Description | Solution |
| [tomcat-embed-websocket-9.0.30.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l22_33157f6bc5bfd03380ebb5ac476db0600a04168d) | Critical | Core Tomcat implementation | Disable the conector to stay away from breaches |
| [tomcat-embed-core-9.0.30.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l20_ad32909314fe2ba02cec036434c0addd19bcc580) | Critical | Core Tomcat implementation | Disable the conector to stay away from breaches |
| [spring-webmvc-5.2.3.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l19_745a62502023d2496b565b7fe102bb1ee229d6b7) | Critical | Spring Web MVC | upgrade to the newest version due to it may have exploit to it |
| [spring-web-5.2.3.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l18_dd386a02e40b915ab400a3bf9f586d2dc4c0852c) | Critical | Spring Web | upgrade to the newest version due to issues java deserialzion untrusted data. |
| [spring-core-5.2.3.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l17_3734223040040e8c3fecd5faa3ae8a1ed6da146b) | Critical | Spring Core | upgrade to the newest version due RCE via data binding. |
| [snakeyaml-1.25.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l14_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) | Critical | YAML 1.1 parser and emitter for Java | Use SnakeYami SafeConsturctor when parsing content to restric deserialization  Ugrade to the newest version |
| [pring-boot-starter-web-2.2.4.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l16_ec75d01d212b5229c16d872fb127744c0ed46ed8) | High | Starter for building web, including RESTful, applications using Spring  MVC. Uses Tomcat as the default embedded container | Curent versoin is unsupported needs to be updated |
| [spring-boot-2.2.4.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l15_225a4fd31156c254e3bb92adb42ee8c6de812714) | High | Spring Boot | Update to the newest version due to unsupported |
| [jackson-databind-2.10.2.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l5_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | High | General data-binding functionality for Jackson: works on core streaming API | Update to the newest version |
| [bcprov-jdk15on-1.46.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l1_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) | High | The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms.  This jar contains JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.7. | Needs to be updated to the newest version of BouncyCastle |
| [logback-core-1.2.3.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l12_864344400c3d4d92dfeb0a305dc87d953677c03c) | Medium | logback-core module | Update to the newest version |
| [hibernate-validator-6.0.18.Final.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l3_7fd00bcd87e14b6ba66279282ef15efa30dd2492) | Medium | Hibernate's Bean Validation (JSR-380) reference implementation. | upgrade to the newest version due to bug in the message proccessor |
| [log4j-api-2.12.1.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en%2DUS&rs=en%2DUS&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmatthew_bartrum_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F7f6f701e1b604027982587139410c1c4&wdorigin=OFFICECOM-WEB.MAIN.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=25359e88-8ca8-44cd-bdde-7143ac705274&wdenableroaming=1&mscc=1&wdodb=1&hid=6D45C6A0-901C-3000-C0DC-5BF524FB42BB&jsapi=1&jsapiver=v1&newsession=1&corrid=6eae912e-e056-480a-8a57-a2aad0f9551d&usid=6eae912e-e056-480a-8a57-a2aad0f9551d&sftc=1&cac=1&mtf=1&sfp=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush&rct=Normal&ctp=LeastProtected#l10_a55e6d987f50a515c9260b0451b4fa217dc539cb) | Low | The Apache Log4j API | Bank needs to have apprioate certficates with the correct host.  Need protocols to be made for man in the middle attacks and  use SMTPS connection with the update of Apache Log4j 2 .12.3 and 2.13.1 |

A lot of the issues apply to outdated systems. While going forward each team and their assignment need to investigate to find what would the proper upgrade to each of the areas. Which upgrade is decided, it needs to be added to the list of solutions.

## Mitigation Plan

We need to meet with members of the board to come up with a plan, dates, and times for the project. This will allow us to have a game plan to have everything ready for our team, The credit union team, and for the members. Legally the members need to be updated to allow them to do what they need to do when we come into a situation of needing to turn off the system. The best plan to attack each risk is to start from the highest and to go the lowest. Each solution needs to explain what we did and any word files for other documentation that legally will need to be done. For audits of the system everything needs to be clear and easy to understand. Finally, we need to have a signature from our team and the CEO of Artemis.