****

# 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** | **1-31-21** | **Michael Divis** |  |

## 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

Michael Divis

## 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?

The company hiring our software security team is named Artemis Financial. They are very interested in security for their software since they deal with finances of many people. It is a crucial part to have success for their company so they can provide good security for all their customers. The company works with businesses all around the world, so they are going to need a very secure system to protect all investments and clients. There are going to be government restrictions with secure connections to consider, there are only going to be limited options for what to use software wise to be able to take oversees clients so that source may have limited access depending what restrictions are in place. There are many threats to always be aware of now and in the future. There are always people interested in hacking in to get their hands on free information or money. Especially going with clients overseas it opens the door to many more threats. Some modernization requirements would be using specific software to gain access or specific functionality using libraries and web pages and browsers and having the application be able to update alongside the web browser being used.

## 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.

There are a few areas of security that will need to be met for this project. The first will include input validation if the users have accounts and passwords to see their information through the company. This would try to keep hackers from logging into admin accounts or single accounts to gain access to info. If the company is doing investments, they may want a way to include some investor information or stock information using API’s, in that case we would need to cover that field for an area of security as well. Cryptography is a must when using passwords and logins especially with banking and financial information being on the line. Code error could be another area covered because we do not want to have the code crashing out during a transaction. We want to have flawless processing and so this should be covered. The code error ties into code quality a bit in my opinion and should be covered to ensure strong code and security. The last area needed to be covered could be encapsulation where we would be storing customer information as well as finances and investments will all be stored in a data structure.

## 3. Manual Review

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

While running the application and loading the webpage it seems like errors have not been handled. This gives us issues in security because if all errors are not handled there could be places where hackers can find a way in using multiple methods to tear through the code to find the weak point. Having the error page come up is not good because now the page is up, and the code is running but there is no data being displayed because of the error. This could give someone with knowledge a way into the system to be able to pull out information that they should not have access to.

## 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:

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

* *Vulnerable Dependencies*: 6
* *Vulnerabilities Found*: 30
* *Vulnerabilities Suppressed*: 0
* *NVD CVE Checked*: 2021-01-31T20:48:19
* *NVD CVE Modified*: 2021-01-31T17:02:40
* *VersionCheckOn*: 2021-01-31T20:48:19

## Summary

Display: [Showing All Dependencies (click to show less)](file:///C:\Users\Admin\Desktop\dependency-check-report.html)

| **Dependency** | **Vulnerability IDs** | **Package** | **Highest Severity** | **CVE Count** | **Confidence** | **Evidence Count** |
| --- | --- | --- | --- | --- | --- | --- |
| [slf4j-api-1.7.30.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l1_b5a4b6d16ab13e34a88fae84c35cd5d68cac922c) |  | [pkg:maven/org.slf4j/slf4j-api@1.7.30](https://ossindex.sonatype.org/component/pkg:maven/org.slf4j/slf4j-api@1.7.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 |  | 29 |
| [bcprov-jdk15on-1.46.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l2_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) | [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) | [pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46](https://ossindex.sonatype.org/component/pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | Unknown | 15 | Highest | 37 |
| [spring-boot-2.2.4.RELEASE.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l3_225a4fd31156c254e3bb92adb42ee8c6de812714) | [cpe:2.3:a:pivotal\_software:spring\_boot:2.2.4: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_boot&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_boot%3A2.2.4) | [pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 | Highest | 32 |
| [logback-core-1.2.3.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l4_864344400c3d4d92dfeb0a305dc87d953677c03c) | [cpe:2.3:a:logback: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%3Alogback&cpe_product=cpe%3A%2F%3Alogback%3Alogback&cpe_version=cpe%3A%2F%3Alogback%3Alogback%3A1.2.3) | [pkg:maven/ch.qos.logback/logback-core@1.2.3](https://ossindex.sonatype.org/component/pkg:maven/ch.qos.logback/logback-core@1.2.3?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 | Highest | 32 |
| [log4j-api-2.12.1.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l5_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) | [pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1](https://ossindex.sonatype.org/component/pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | LOW | 1 | Highest | 46 |
| [jul-to-slf4j-1.7.30.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l6_d58bebff8cbf70ff52b59208586095f467656c30) |  | [pkg:maven/org.slf4j/jul-to-slf4j@1.7.30](https://ossindex.sonatype.org/component/pkg:maven/org.slf4j/jul-to-slf4j@1.7.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 |  | 28 |
| [jakarta.annotation-api-1.3.5.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l7_59eb84ee0d616332ff44aba065f3888cf002cd2d) |  | [pkg:maven/jakarta.annotation/jakarta.annotation-api@1.3.5](https://ossindex.sonatype.org/component/pkg:maven/jakarta.annotation/jakarta.annotation-api@1.3.5?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 |  | 32 |
| [snakeyaml-1.25.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l8_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) | [pkg:maven/org.yaml/snakeyaml@1.25](https://ossindex.sonatype.org/component/pkg:maven/org.yaml/snakeyaml@1.25?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | HIGH | 1 | Highest | 28 |
| [jackson-databind-2.10.2.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l9_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | [cpe:2.3:a:fasterxml:jackson: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&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson%3A2.10.2) [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) | [pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | HIGH | 1 | Highest | 39 |
| [jackson-core-2.10.2.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l10_73d4322a6bda684f676a2b5fe918361c4e5c7cca) | [cpe:2.3:a:fasterxml:jackson: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&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson%3A2.10.2) | [pkg:maven/com.fasterxml.jackson.core/jackson-core@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.core/jackson-core@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 | Highest | 45 |
| [jackson-datatype-jdk8-2.10.2.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l11_dca8c8ab85eaabefe021e2f1ac777f3a6b16a3cb) | [cpe:2.3:a:fasterxml:jackson: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&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson%3A2.10.2) cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | [pkg:maven/com.fasterxml.jackson.datatype/jackson-datatype-jdk8@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.datatype/jackson-datatype-jdk8@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 | Highest | 39 |
| [tomcat-embed-core-9.0.30.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l12_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) | [pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | CRITICAL | 11 | Highest | 39 |
| [tomcat-embed-el-9.0.30.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l13_406e0c7cc45204c0f81853d73e8cfedfa4e00945) |  | [pkg:maven/org.apache.tomcat.embed/tomcat-embed-el@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-el@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 |  | 36 |
| [jakarta.validation-api-2.0.2.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l14_5eacc6522521f7eacb081f95cee1e231648461e7) |  | [pkg:maven/jakarta.validation/jakarta.validation-api@2.0.2](https://ossindex.sonatype.org/component/pkg:maven/jakarta.validation/jakarta.validation-api@2.0.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 |  | 29 |
| [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l15_7fd00bcd87e14b6ba66279282ef15efa30dd2492) | [cpe:2.3:a:hibernate: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%3Ahibernate&cpe_product=cpe%3A%2F%3Ahibernate%3Ahibernate-validator&cpe_version=cpe%3A%2F%3Ahibernate%3Ahibernate-validator%3A6.0.18) [cpe:2.3:a: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%3Ahibernate&cpe_product=cpe%3A%2F%3Ahibernate%3Avalidator&cpe_version=cpe%3A%2F%3Ahibernate%3Avalidator%3A6.0.18) [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) | [pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final](https://ossindex.sonatype.org/component/pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 | Highest | 36 |
| [jboss-logging-3.4.1.Final.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l16_40fd4d696c55793e996d1ff3c475833f836c2498) |  | [pkg:maven/org.jboss.logging/jboss-logging@3.4.1.Final](https://ossindex.sonatype.org/component/pkg:maven/org.jboss.logging/jboss-logging@3.4.1.Final?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 |  | 45 |
| [classmate-1.5.1.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l17_3fe0bed568c62df5e89f4f174c101eab25345b6c) |  | [pkg:maven/com.fasterxml/classmate@1.5.1](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml/classmate@1.5.1?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) |  | 0 |  | 47­­­­­­­­ |
| [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\Admin\Desktop\dependency-check-report.html#l18_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:springsource\_spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* | [pkg:maven/org.springframework/spring-core@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-core@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | MEDIUM | 1 | Highest | 30 |

## 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.

After running testing and checking over the software there is a lot to be done. There are a lot of packages that have vulnerabilities that need to either be dealt with or the package used needs to be changed out and use another one in place. The software needs to be able to handle errors, so it does not get held up on a single page errored out it just keeps on going or uses a built-in error message box. Being that the software needs to be able to communicate with outside the country customers we need to follow all specific guidelines and makes sure we are following the rules and have secure connections all around.