# CS 305 Project One

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **5/25/2024** | **Stephanie Douglas** | **Interpreting Client Needs, Areas of Security, Manual Review, Static Testing, Mitigation Plan** |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In this report, identify your security vulnerability findings and recommend 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 include images or supporting materials. If you include them, make certain to insert them in 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

Stephanie Douglas

**1. Interpreting Client Needs**

Determine your client’s needs and potential threats and attacks associated with the company’s application and software security requirements. Consider the following questions 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 on secure communications to consider?
* What external threats might be present now and in the immediate future?
* What modernization requirements must be considered, such as the role of open-source libraries and evolving web application technologies?

Artemis Financial creates financial plans for their customers. These plans include information regarding customer savings, retirement, investments, and insurance. It is highly important the company maintains secure communications and systems to ensure their customer information is not compromised and they are obeying laws. The current understanding is that the system does not require international transactions, thus laws and security regarding international transactions can be ignored. However, there are governmental restrictions that need to be considered regarding secure communications. Financial Privacy Rule and the Safeguards Rule are a few examples of regulations in place to keep customers financial information secure (*Financial Privacy*, 2021). Following coding best practices and using up-to-date software with no known vulnerabilities could decrease the risk of an attack and protect customer’s financial information against external threats. When code is developed and all vulnerabilities are removed, it is important to know that over time new vulnerabilities may arise in the current code. Applications must be maintained overtime to remain secure. For example, open-source libraries used in the application may become vulnerable post-deployment. Running Dependency Check reports should be a security measure to maintain the security of the system throughout its existence. Likewise, the same can occur for programming languages, web development technologies. It is important to follow current and future security standards for the programming languages used to reduce risk.

**2. Areas of Security**

Refer to the vulnerability assessment process flow diagram. Identify which areas of security apply to Artemis Financials’ software application. Justify your reasoning for why each area is relevant to the software application.

**Input validation**: The customer inputs information and/or documents in the application. The user inputs need to be validated with appropriate error handling to be secure.

**APIs**: The application is a RESTful API. The API should follow secure standard practices including authentication, strong API keys, and HTTPS implementation (Doronin, 2023).

**Cryptography**: REST APIs use cryptography by encryption through TLS certificates. TLS certificates must be in place for secure HTTPS transmission.

**Code Error**: Secure error handling is important for REST APIs to reduce risk of a data breach. API errors should use appropriate HTTP status codes for security purposes. Inappropriate error handling may lead to stack traces, database dumps, and error codes displayed to the hacker (Ferragamo & Bird).

**Code Quality**: Secure coding practices and patterns is a security area that applies to this application as code syntax can largely impact how secure an application is.

**Encapsulation**: Secure data structures are relevant to this application as the code includes classes that encapsulate variables and methods. Without correct encapsulation, the application is subject to cross domain attacks and unauthorized access to data and functions (*Encapsulation 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.

* The pom.xml file lists Spring Boot 2.2.4.RELEASE, Spring Core 5.2.3.RELEASE, and Logback Core 1.2.3 dependencies, which were previously determined to have vulnerabilities.
* The DocData.java file displays the username and password in code on line 27. It also describes in plain text the database name, username, and password on line 32. These should not be hard coded in the java file, instead the user should be required to enter username and password to gain access. In addition, the username and password are both “root”, which is too simple and easy to guess.

A screen shot of a computer code

Description automatically generated

* In the CRUDController.java file, the code @RequestParam(value="business\_name") is vulnerable to SQL injection. The value is received as an untrusted parameter from the /read webpage.

A close-up of a code

Description automatically generated

* In the GreetingController.java file, the code @RequestParam(value = "name", defaultValue = "World") is vulnerable to SQL injection. The value is received as an untrusted parameter from the /greeting webpage.

A close-up of a computer code

Description automatically generated

* In the myDateTime.java file, the variables should be declared as private variables. The retrieveDateTime and setMyDateTime methods should be declared as public.A screen shot of a computer code

  Description automatically generated
* In Customer.java file, the account\_balance variable should be declared as private. Also, the showInfo method should be changed to getAccountNumber method to access the private variable.

A computer code with text

Description automatically generated

**4. Static Testing**

Run a dependency check on Artemis Financials’ software application to identify all security vulnerabilities in the code. Record the output from the dependency-check report. Include the following items:

* The names or vulnerability codes of the known vulnerabilities
* A brief description and recommended solutions provided by the dependency-check report
* Any attribution that documents how this vulnerability has been identified or documented previously

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dependency** | **Vulnerability IDs** | **Package** | **Highest  Severity** | **CVE  Count** | **Confid-ence** | **Evidence Count** |
| [bcprov-jdk15on-1.46.jar](#RANGE!l1_991c96a4e31e6c19e2b9136c8955bd) | cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.46:\*:\*:\*:\*:\*:\*:\* | [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=7.1.2) | HIGH | 21 | Highest | 38 |
| 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:\*:\*:\*:\*:\*:\*:\* |
| [hibernate-validator-6.0.18.Final.jar](#RANGE!l3_7fd00bcd87e14b6ba66279282ef15e) | [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=7.1.2) | MEDIUM | 1 | Highest | 34 |
| [jackson-core-2.10.2.jar](#RANGE!l5_73d4322a6bda684f676a2b5fe91836) | cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | [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=7.1.2) | HIGH | 2 | Low | 47 |
| cpe:2.3:a:json-java\_project:json-java:2.10.2:\*:\*:\*:\*:\*:\*:\* |
| [jackson-databind-2.10.2.jar](#RANGE!l6_0528de95f198afafbcfb0c09d2e43b) | [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=7.1.2) | HIGH | 6 | Highest | 41 |
| cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* |
| [log4j-api-2.12.1.jar](#RANGE!l11_a55e6d987f50a515c9260b0451b4f) | [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=7.1.2) | LOW | 1 | Highest | 44 |
| [logback-core-1.2.3.jar](#RANGE!l13_864344400c3d4d92dfeb0a305dc87) | [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) | [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=7.1.2) | HIGH | 2 | Highest | 33 |
| [snakeyaml-1.25.jar](#RANGE!l15_8b6e01ef661d8378ae6dd7b511a7f) | [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=7.1.2) | CRITICAL | 8 | Highest | 46 |
| [spring-boot-2.2.4.RELEASE.jar](#RANGE!l16_225a4fd31156c254e3bb92adb42ee) | [cpe:2.3:a:vmware: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%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_boot&cpe_version=cpe%3A%2F%3Avmware%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=7.1.2) | CRITICAL | 3 | Highest | 39 |
| [spring-boot-starter-web-2.2.4.RELEASE.jar](#RANGE!l17_ec75d01d212b5229c16d872fb1277) | [cpe:2.3:a:vmware: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%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_boot&cpe_version=cpe%3A%2F%3Avmware%3Aspring_boot%3A2.2.4) | [pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=7.1.2) | CRITICAL | 3 | Highest | 35 |
| [cpe:2.3:a:web\_project:web: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%3Aweb_project&cpe_product=cpe%3A%2F%3Aweb_project%3Aweb&cpe_version=cpe%3A%2F%3Aweb_project%3Aweb%3A2.2.4) |
| [spring-core-5.2.3.RELEASE.jar](#RANGE!l18_3734223040040e8c3fecd5faa3ae8) | [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) | [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=7.1.2) | CRITICAL | 11 | Highest | 36 |
| [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) |
| [spring-web-5.2.3.RELEASE.jar](#RANGE!l19_dd386a02e40b915ab400a3bf9f586) | [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) | [pkg:maven/org.springframework/spring-web@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-web@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=7.1.2) | CRITICAL | 14 | Highest | 34 |
| [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:web\_project:web: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%3Aweb_project&cpe_product=cpe%3A%2F%3Aweb_project%3Aweb&cpe_version=cpe%3A%2F%3Aweb_project%3Aweb%3A5.2.3) |
| [spring-webmvc-5.2.3.RELEASE.jar](#RANGE!l20_745a62502023d2496b565b7fe102b) | [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) | [pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=7.1.2) | CRITICAL | 11 | Highest | 36 |
| [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:web\_project:web: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%3Aweb_project&cpe_product=cpe%3A%2F%3Aweb_project%3Aweb&cpe_version=cpe%3A%2F%3Aweb_project%3Aweb%3A5.2.3) |
| [tomcat-embed-core-9.0.30.jar](#RANGE!l21_ad32909314fe2ba02cec036434c0a) | [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) | [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=7.1.2) | CRITICAL | 26 | Highest | 33 |
| [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) |
| [tomcat-embed-websocket-9.0.30.jar](#RANGE!l23_33157f6bc5bfd03380ebb5ac476db) | [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) | [pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=7.1.2) | CRITICAL | 27 | Highest | 32 |
| [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) |

**bcprov-jdk15on-1.46.jar**

There are several vulnerabilities related to this package. To remove these vulnerabilities upgrade to version 1.78, which currently has no known vulnerabilities (*Bouncy Castle Provider*, 2024).

**hibernate-validator-6.0.18.Final.jar**

The above dependency validates invalid EL expressions in the message interpolation processor and bypass input sanitation (*CVE-2020-10693*, 2022). A solution for this dependency in the code base is to upgrade to red-hat-jboss-eap-upgrade-7\_3\_2 (*Red Hat JBoss EAP: Improper input validation in the interpolation of constraint error messages (CVE-2020-10693)*, 2023).

**jackson-core-2.10.2.jar**

There are two vulnerabilities within this dependency. CVE-2022-45688 vulnerability allows for a Denial of Service (DoS) through the XML.toJSONObject component in hutool-json v5.8.10 via XML or JSON file (*CVE-2022-45688 Detail*, 2023). To resolve these vulnerabilities the dependency should be upgraded to the latest stable release, which is 2.17 (*Jackson releases* 2024). By performing this upgrade it is expected to remove the second vulnerability as well.

**jackson-databind-2.10.2.jar**

As previously discussed, the Jackson dependency will need to be upgraded to the latest stable version to resolve this vulnerability.

**log4j-api-2.12.1.jar**

The vulnerability CVE-2020-9488 intercepts an SMTP connection through improper certificate validation, which is removed in version 2.13.1 (*CVE-2020-9488 Detail*, 2023). Upgrade code to use this upgraded package to remove the vulnerability.

**logback-core-1.2.3.jar**

This dependency has two vulnerabilities. CVE-2023-6378 is a vulnerability that allows a Denial-Of-Service attack in the receiver component (*CVE-2023-6378 Detail*, 2023). On the other hand, vulnerability CVE-2021-42550 allows an attacker to edit configuration files with required privileges (*CVE-2021-42550 Detail* 2022). Both vulnerabilities are removed with Logback version 1.2.13, however it is best to upgrade to the latest version 1.5.6 (*Logback Core Module*, 2024).

**snakeyaml-1.25.jar**

This dependency has eight known vulnerabilities. All vulnerabilities are removed by version 2.0 and above (*SnakeYAML*, 2023). The source code should be upgraded to one of these versions.

**spring-boot-2.2.4.RELEASE.jar**

The 2.2.4 version of Spring Boot has three vulnerabilities, including a risk that attackers may hijack the temporary directory (*CVE-2022-27772 Detail*, 2024). Upgrading to any version from 3.1.6 to the latest 3.3.0 will remove this vulnerability (*Spring Boot*, 2024).

**spring-boot-starter-web-2.2.4.RELEASE.jar**

As described above, when the Spring Boot dependency is upgraded to the latest version this will also remove the Spring Boot Starter Web vulnerability (*Spring Boot Starter Web* , 2024).

**spring-core-5.2.3.RELEASE.jar**

**spring-web-5.2.3.RELEASE.jar**

**spring-webmvc-5.2.3.RELEASE.jar**

The above three dependencies can be grouped together to decide the appropriate upgrade to remove all vulnerabilities. When comparing the three dependencies within maven repository website, Spring Web has fewer version options without vulnerabilities. Upgrading to the latest version 6.1.8 is recommended to remove all vulnerabilities (*Spring Web* , 2024).

**tomcat-embed-core-9.0.30.jar**

**tomcat-embed-websocket-9.0.30.jar**

The above two dependencies have several vulnerabilities. By upgrading to the latest Tomcat Embed version 11.0.0-M20 all known vulnerabilities will be removed (*Tomcat Embed Core*, 2024).

**5. Mitigation Plan**

Interpret the results from the manual review and static testing report. Then identify the steps to mitigate the identified security vulnerabilities for Artemis Financial’s software application.

**Manual Review Mitigation Plan**:

The manual review of the source code revealed that there is missing code, as well as some security vulnerabilities. Before writing the missing code for the application to work as expected, it is important to address and fix the vulnerabilities. Below are the mitigation steps to reduce vulnerabilities in the source code.

* Change user credentials from “user” to a more secure password.
* In the DocData.java file, remove database name, username, and password references and require user to input login credentials to gain access.
* Add input validation and query parameterization to CRUDController.java and GreetingController.java files.
* Add appropriate declaration of variables to myDateTime.java and customer.java files.
* Declare the retrieveDateTime and setMyDateTime methods as public in the myDateTime.java file.
* Change the showInfo method to getAccountNumber method to access the private variable and return the account number.

**Static Testing Mitigation Plan**:

The Dependency Check reveals several vulnerabilities that need to be addressed. Below are the steps to reduce known vulnerabilities in dependencies.

* Upgrade Bouncy Castle Provider to version 1.78
* Upgrade hibernate-validator-6.0.18 to red-hat-jboss-eap-upgrade-7\_3\_2
* Upgrade jackson-core-2.10.2 and jackson-databind-2.10.2 to version 2.17
* Upgrade log4j-api-2.12.1 to version 2.13.1
* Upgrade logback-core-1.2.3 to version 1.5.6
* Upgrade snakeyaml-1.25 to at least version 2.0
* Upgrade spring-boot-2.2.4 and spring-boot-starter-web-2.2.4 to version 3.3.0
* Upgrade spring-core-5.2.3, spring-web-5.2.3, and spring-webmvc-5.2.3 to version 6.1.8
* Upgrade tomcat-embed-core-9.0.30 and tomcat-embed-websocket-9.0.30 to 11.0.0-M20

References

*Bouncy Castle Provider*. Maven Repository. (2024, April 18). https://mvnrepository.com/artifact/org.bouncycastle/bcprov-jdk18on

*CVE-2020-10693*. CVE website. (2022, April 19). https://www.cve.org/CVERecord?id=CVE-2020-10693

*CVE-2020-9488 Detail*. NVD. (2023, November 6). https://nvd.nist.gov/vuln/detail/CVE-2020-9488

*CVE-2021-42550 Detail*. NVD. (2022, December 12). https://nvd.nist.gov/vuln/detail/CVE-2021-42550

*CVE-2022-27772 Detail*. NVD. (2024, April 25). https://nvd.nist.gov/vuln/detail/CVE-2022-27772

*CVE-2022-45688 Detail*. National Vulnerability Database. (2023, March 9). https://nvd.nist.gov/vuln/detail/CVE-2022-45688

*CVE-2023-6378 Detail*. NVD. (2023b, December 5). https://nvd.nist.gov/vuln/detail/CVE-2023-6378

Doronin, E. (2023, June 13). *REST API vs API: What’s the difference?* Directual blog. <https://www.directual.com/blog/rest-api-vs-api>

*Encapsulation Vulnerabilities*. Veracode. (n.d.). https://www.veracode.com/security/encapsulation-vulnerabilities

Ferragamo, J., & Bird, J. (n.d.). *Improper Error Handling*. OWASP Foundation. https://owasp.org/www-community/Improper\_Error\_Handling

*Financial Privacy*. Federal Trade Commission. (2021, July 16). https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/financial-privacy

*Jackson releases*. GitHub. (2024, March). https://github.com/FasterXML/jackson/wiki/Jackson-Releases

*Logback Core Module*. Maven Repository. (2024, April 17). https://mvnrepository.com/artifact/ch.qos.logback/logback-core

*Red Hat JBoss EAP: Improper input validation in the interpolation of constraint error messages (CVE-2020-10693)*. Rapid7. (2023, November 8). https://www.rapid7.com/db/vulnerabilities/red\_hat-jboss\_eap-cve-2020-10693/

*SnakeYAML*. Maven Repository. (2023, August 27). https://mvnrepository.com/artifact/org.yaml/snakeyaml

*Spring Boot Starter Web*. Maven Repository. (2024d, May 23). https://mvnrepository.com/artifact/org.springframework.boot/spring-boot-starter-web

*Spring Boot*. Maven Repository. (2024c, May 23). https://mvnrepository.com/artifact/org.springframework.boot/spring-boot

*Spring Web*. Maven Repository. (2024e, May 22). https://mvnrepository.com/artifact/org.springframework/spring-web

*Tomcat Embed Core*. Maven Repository. (2024f, May 8). https://mvnrepository.com/artifact/org.apache.tomcat.embed/tomcat-embed-core