# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **07.20.2025** | **Kayle Church** |  |

## 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

Kayle Church

**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 handles sensitive financial and personal data, including customer financial records, biometric identifiers, Social Security numbers, and banking information. As such, secure communication, both internally and externally, is crucial to maintaining client trust and regulatory compliance. Due to the nature of financial services, it is highly likely that Artemis conducts both domestic and international transactions, which necessitates the use of secure, encrypted channels that adhere to regional compliance requirements such as GDPR or U.S. federal guidelines.

While there may not currently be explicit government restrictions affecting Artemis's secure communication protocols, proactive implementation of secure channels remains critical. This includes TLS encryption, secure token-based authentication, and safeguarding against man-in-the-middle attacks. External threats such as phishing, credential stuffing, SQL injection, and unauthorized access are immediate concerns, especially with customer data being transmitted or stored.

To modernize operations, Artemis must ensure their web applications integrate up-to-date open-source libraries that are regularly patched against known vulnerabilities. The adoption of contemporary technologies (such as RESTful APIs, secure storage mechanisms, and automated dependency checking) will help reduce risk and align the application with industry best practices for cybersecurity.

**2. Areas of Security**

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

The following areas from the Vulnerability Assessment Process Flow Diagram are applicable to Artemis Financial’s web application:

* **Input Validation**: User input fields are vulnerable to injection attacks and must be validated server-side. The current implementation accepts raw input from the URL, which is unsafe and may expose the application to exploitation.
* **APIs**: The system lacks a clear, structured RESTful API. Without a well-defined interface, client interaction becomes insecure and unpredictable. A secure API framework would control access, manage sessions, and prevent unauthorized data exposure.
* **Cryptography**: Sensitive client data, particularly in international transactions, must be encrypted at rest and in transit using modern cryptographic standards. The current lack of encryption introduces the risk of data breaches.
* **Error Handling**: Improper error messages can disclose internal system details. Code components like DocData.java contain try/catch blocks but lack structured logging or user-friendly error responses. Robust error handling should be implemented to maintain both user experience and application security.
* **Code Quality**: While the code is readable and organized, the absence of API integration, proper input handling, and secure storage mechanisms diminishes its effectiveness. Ensuring high code quality through secure development practices and code reviews is essential to maintain long-term software health.

**3. Manual Review**

Continue working through the vulnerability assessment process flow diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

A manual inspection of Artemis Financial’s codebase revealed several security concerns:

* **Missing Input Validation**

The application accepts unsanitized user input via the URL, with no evidence of server-side validation libraries such as Apache Commons Validator.

* **Unsecured Data Submission via URL**

Input is handled through GET requests in the URL rather than secure POST methods, making sensitive data vulnerable to exposure in browser history and server logs.

* **Absence of a RESTful API**

There is no structured or documented API for external interaction, leaving the system without standardized access control or clear request/response handling.

* **Lack of Cryptographic Measures**

No encryption mechanisms were found for storing or transmitting sensitive financial and personal data, posing significant security and compliance risks.

* **No Encryption for International Transactions**

The application fails to provide cryptographic safeguards that would meet international standards for data privacy and financial transaction security.

* **Incomplete Error Handling**

In DocData.java, try/catch blocks are present, but broader exception management, logging, and user feedback mechanisms are missing throughout the codebase.

* **No User Guidance or Feedback**

Without an API or structured front-end, users have no clear way to interact with the application, increasing the likelihood of misuse or misconfiguration.

* **Code Quality Issues Affecting Security**

While the structure is readable, missing core components such as input validation, encryption, and API integration reduce the application’s overall security and usability.

**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 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

Using the Maven dependency-check plugin, several outdated or vulnerable dependencies were identified. Key findings include:

|  |  |  |  |
| --- | --- | --- | --- |
| **Dependency** | **Vulnerability** | **Description** | **License** |
| [bcprov-jdk15on-1.46.jar](file:///C:\Users\kayle\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:bouncy\_castle\_for\_java: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%3Abouncy_castle_for_java&cpe_version=cpe%3A%2F%3Abouncycastle%3Abouncy_castle_for_java%3A1.46) cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-  crytography-api:1.46:\*:\*:\*:\*:\*:\*:\* cpe:2.3:a:bouncycastle:the\_bouncy\_castle\_  crypto\_package\_for\_java:1.46:\*:\*:\*:\*:\*:\*:\* | 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. | Bouncy Castle Licence: http://www.bouncycastle.org/licence.html |
| [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l3_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: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) | Hibernate's Bean Validation (JSR-380) reference implementation. | <http://www.apache.org/licenses/LICENSE-2.0.txt> |
| [jackson-core-2.10.2.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l5_73d4322a6bda684f676a2b5fe918361c4e5c7cca) | cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | Core Jackson processing abstractions (aka Streaming API), implementation for JSON | <http://www.apache.org/licenses/LICENSE-2.0.txt> |
| [jackson-databind-2.10.2.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l6_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\*  cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | General data-binding functionality for Jackson: works on core streaming API | <http://www.apache.org/licenses/LICENSE-2.0.txt> |
| [log4j-api-2.12.1.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l11_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) | The Apache Log4j API | <https://www.apache.org/licenses/LICENSE-2.0.txt> |
| [logback-classic-1.2.3.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l13_7c4f3c474fb2c041d8028740440937705ebb473a) | cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\* | logback-classic module | [http://www.eclipse.org/legal/epl-v10.html, http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html](http://www.eclipse.org/legal/epl-v10.html,%20http:/www.gnu.org/licenses/old-licenses/lgpl-2.1.html) |
| [logback-core-1.2.3.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l14_864344400c3d4d92dfeb0a305dc87d953677c03c) | cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\* | logback-core module | [http://www.eclipse.org/legal/epl-v10.html, http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html](http://www.eclipse.org/legal/epl-v10.html,%20http:/www.gnu.org/licenses/old-licenses/lgpl-2.1.html) |
| [snakeyaml-1.25.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l16_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) | cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25:\*:\*:\*:\*:\*:\*:\* | YAML 1.1 parser and emitter for Java | Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt> |
| [spring-boot-2.2.4.RELEASE.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l17_225a4fd31156c254e3bb92adb42ee8c6de812714) | cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\* | Spring Boot | Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0> |
| [spring-boot-starter-web-2.2.4.RELEASE.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l18_ec75d01d212b5229c16d872fb127744c0ed46ed8) | [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) [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) | Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container | Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0> |
| [spring-context-5.2.3.RELEASE.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l19_7750c95c96c7a1885c8b1b503ba915bc33ca579a) | [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) | Spring Context | Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0> |
| [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l20_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) | Spring Core | Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0> |
| [spring-expression-5.2.3.RELEASE.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l21_d0c6bb10758805b2153c589686b8045554bfac2d) | [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) | Spring Expression Language (SpEL) | Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0> |
| [spring-web-5.2.3.RELEASE.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l22_dd386a02e40b915ab400a3bf9f586d2dc4c0852c) | [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: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 Web | Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0> |
| [spring-webmvc-5.2.3.RELEASE.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l23_745a62502023d2496b565b7fe102bb1ee229d6b7) | [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: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 Web MVC | Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0> |
| [tomcat-embed-core-9.0.30.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l24_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\_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) | Core Tomcat implementation | Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt> |
| [tomcat-embed-websocket-9.0.30.jar](file:///C:\Users\kayle\Downloads\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l26_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\_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) | Core Tomcat implementation | Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt> |

Each identified dependency should be updated to the latest patched version, as outlined in the dependency-check report.

**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.

To mitigate the vulnerabilities discovered through both manual review and static testing:

1. **Input Validation**: Implement server-side validation using a proven library such as Apache Commons Validator. Enforce strict input types and ranges.
2. **API Security**: Design and implement a RESTful API using frameworks like Spring Boot. Secure endpoints with token-based authentication and rate limiting.
3. **Cryptography**: Apply AES encryption for data at rest and TLS for data in transit. Ensure compliance with regional encryption standards.
4. **Error Handling**: Introduce global exception handlers and logging mechanisms. Sanitize all error messages to avoid leaking stack traces or system info.
5. **Dependency Updates**: Update all vulnerable libraries to the most recent stable versions as outlined in the dependency-check results.
6. **Configuration Hardening**: Modify system settings to disable legacy or unsafe features, such as alias expansion in SnakeYAML or insecure SMTP configurations.

Implementing this mitigation plan will enhance Artemis Financial’s security posture and reduce exposure to known attack vectors.