# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **January 26, 2025** | **Atsushi Ogata** |  |

## 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

Atsushi Ogata

**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?

Since the client, Artemis Financial, is a financial consulting company and, therefore, works with sensitive financial information, secure communications are essential to the company. Secure communication would help prevent unauthorized access to this information and ensure that the data is not tampered with during transmission. If the client conducts interactional transactions, there would be additional regulations and standards that they need to comply with.

Governmental restrictions on secure communications are also important to consider. Some jurisdictions may require data to be stored within the country, and encryption laws may dictate the type and strength of encryption used.

External threats present now and in the immediate future include but are not limited to phishing attacks, SQL injection, cross-site scripting attacks, and man-in-the-middle attacks. These threats exploit both the human factor and technical vulnerabilities.

If Artemis Financial wants to modernize, the following requirements would need to be considered. Firstly, open-source libraries are commonly used in development. However, these may introduce vulnerabilities, and therefore, regular dependency checks should be conducted and updates be made frequently. Web application technologies are constantly evolving, introducing more functionality with each iteration. However, these would require additional layers of security to ensure API gateways are secured and secure authentication is enforced.

**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.

While all areas of security are important, there are several key areas that must be addressed to secure Artemis Financials’ web application. Firstly, Input Validation is essential to sanitize user inputs and prevent attacks such as SQL injection. As the application would be reliant on a RESTful API, it should be a high priority to protect data exchanges and prevent unauthorized access. Further, cryptography is important since it protects sensitive information, and client/server security allows communications to remain secure through HTTPS and secure authentication.

**3. Manual Review**

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

Vulnerabilities found in the code include the following.

1. In the DocData class, the read\_document method establishes a connection to the database without sanitizing the inputs, exposing it to SQL injection.
2. In the DocData class, database credentials (“root”, “root) are hardcoded. This makes the code easily exploitable if the source code is accessed.
3. In the CRUDController and GreetingController classes, the @RequestParam parameters are used directly without being validated and sanitized, thus making it vulnerable to injection attacks.
4. In the DocData class, the SQLException in the read\_document method is only logged with e.printStackTrace(). This can potentially expose stack traces to attackers.
5. In the customer class, the account\_balance variable can be accessed from outside the class.
6. In the myDateTime class, the setMyDateTime does not validate the input values for seconds, minutes, or hours, which could lead to invalid or malicious data being processed.
7. In the DocData class, the database connection is not closed which can lead to potential resource leaks.

**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

Multiple dependencies were identified after a static test using dependency check Maven. The results are shown below.

| **Dependency** | **Vulnerability IDs↑** | **Package** | **Highest Severity** | **CVE Count** | **Confidence** | **Evidence Count** |
| --- | --- | --- | --- | --- | --- | --- |
| [log4j-api-2.12.1.jar](#l6_a55e6d987f50a515c9260b0451b4fa217dc5) | [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) | CRITICAL | 5 | Highest | 46 |
| [tomcat-embed-core-9.0.30.jar](#l14_ad32909314fe2ba02cec036434c0addd19b) | [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) | [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 | 27 | Highest | 39 |
| [bcprov-jdk15on-1.46.jar](#l2_991c96a4e31e6c19e2b9136c8955bd423f2d) | [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) | HIGH | 20 | Highest | 37 |
| [jackson-databind-2.10.2.jar](#l10_0528de95f198afafbcfb0c09d2e43b6e0ea) | [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 | 6 | Highest | 39 |
| [spring-beans-5.2.3.RELEASE.jar](#l21_0250c8c641433dc06b1b44e4563fa08a2fb) | [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) | [pkg:maven/org.springframework/spring-beans@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-beans@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | HIGH | 1 | Highest | 28 |
| [spring-context-5.2.3.RELEASE.jar](#l23_7750c95c96c7a1885c8b1b503ba915bc33c) | [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) | [pkg:maven/org.springframework/spring-context@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-context@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | MEDIUM | 1 | Highest | 28 |
| [spring-expression-5.2.3.RELEASE.jar](#l24_d0c6bb10758805b2153c589686b8045554b) | [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) | [pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | MEDIUM | 4 | Highest | 30 |
| [spring-web-5.2.3.RELEASE.jar](#l20_dd386a02e40b915ab400a3bf9f586d2dc4c) | [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) | [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=5.3.0) | HIGH | 8 | Highest | 28 |
| [spring-webmvc-5.2.3.RELEASE.jar](#l22_745a62502023d2496b565b7fe102bb1ee22) | [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) | [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=5.3.0) | HIGH | 2 | Highest | 30 |
| [logback-classic-1.2.3.jar](#l4_7c4f3c474fb2c041d8028740440937705ebb) | [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-classic@1.2.3](https://ossindex.sonatype.org/component/pkg:maven/ch.qos.logback/logback-classic@1.2.3?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | HIGH | 2 | Highest | 32 |
| [logback-core-1.2.3.jar](#l5_864344400c3d4d92dfeb0a305dc87d953677) | [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=5.3.0) | HIGH | 4 | Highest | 32 |
| [hibernate-validator-6.0.18.Final.jar](#l17_7fd00bcd87e14b6ba66279282ef15efa30d) | [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) | MEDIUM | 2 | Highest | 36 |
| [snakeyaml-1.25.jar](#l9_8b6e01ef661d8378ae6dd7b511a7f2a33fae) | [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) [cpe:2.3:a:yaml\_project:yaml:1.25:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Ayaml_project&cpe_product=cpe%3A%2F%3Ayaml_project%3Ayaml&cpe_version=cpe%3A%2F%3Ayaml_project%3Ayaml%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) | CRITICAL | 10 | Highest | 28 |
| [spring-boot-2.2.4.RELEASE.jar](#l3_225a4fd31156c254e3bb92adb42ee8c6de81) | [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=5.3.0) | CRITICAL | 3 | Highest | 32 |

**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 found in the application, developers should start by sanitizing user inputs in the read\_document method of the DocData class to prevent SQL injection attacks. Also, proper input validation and output encoding should be implemented in the CRUDController and GreetingController classes to mitigate injection risks. Further, hardcoding database credentials in the source code should be avoided. Instead, environment variables should be used to handle sensitive information. In the customer class, the account\_balnace variable should be secured. This can be done by encapsulating it to prevent unauthorized access. Input values in the myDateTime class should be validated so that only valid data is processed. Database connections should be closed after use in the DocData class to prevent resource leaks. To address the vulnerabilities found by the dependency check, affected dependencies should be updated to their latest versions. If no update is available, it may be necessary to consider using alternatives.