# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **7/18/24** | **Tabitha Pawlowski** |  |

## 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

Tabitha Pawlowski

**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?

Our client, Artemis Financial, is a consulting company that specializes in individualized savings, retirements, investment, and insurance plans for their customers. The web application will focus on the client’s personal financial information, making secure communication an essential concept for this company. To earn and keep the client’s trust, keeping data secure will need to be the top priority. This web application will be used with customers around the world, so how to keep international transactions secure will need to be considered. It is very likely that there are governmental restrictions that will need to be considered as well, since Artemis Financial is a global financial institution that will in part be working with governmental agencies. There are several different types of external threats that our client may face now and in the future. Any financial institution will be vulnerable to attacks from hackers trying to gain access to the financial information of its customers, but Artemis specializes in larger clients, such as entrepreneurs, businesses, and governmental entities. This increases the likelihood of attempted attacks on the system and their customers. To help keep this web application secure from attacks, modernizing the system with updated libraries and technologies will be the first line of defense. The more frequent the updates, the less time hackers have to become familiar with the system and learn how to manipulate it. Updating the database and using encryption techniques, RBAC roles, and more will help keep the web application secure and help maintain its integrity and quality.

**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.

There are many areas of security that apply to Artemis Financial’s software application. One of these areas include input validation. It is assumed that customers will be able to access their information through a website by entering in personal authenticating information that proves they are who they claim to be. This can be a username, password, last four digits of a social security number, or other identifying information. It is important that this information is validated and has checks to make sure that the response is appropriate for the given conditions. Another area of security that is important for Artemis is cryptography and encryption. Not only should username and passwords be encrypted, but the financial information stored within the system should be securely encrypted to prevent hackers from accessing this information. Code quality is also an essential security feature for this software application. It is important that the code for the application is written with the highest level of quality and with integrity. Last but not least, encapsulation is also a key security technique that Artemis financial should deploy to keep their application safe and secure. The system will need to hold a large amount of information that pertains to the customer’s financial assets. Encapsulation will help keep this data and the structures they are stored in safe from unauthorized users from accessing them.

**3. Manual Review**

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

One vulnerability I found was that the business name is sent through a request parameter in the CRUDController class. This means that the business name can be seen in the url, which can be unsafe and lacks privacy. The second and third vulnerabilities that I found are that the CRUDController and GreetingController classes do not have any input validation. These classes ask for the business name and customer name, but do not check to make sure that the given input is a valid and appropriate response. The fourth vulnerability is that the read\_document in the DocData class is hard coded, which could lead to some issues when trying to access and read the database. The fifth vulnerability I found is that in the customer class, the account number is a private variable, but the account balance is public. This is also sensitive information that should be private or protected to help keep it secure. The sixth vulnerability within the code base is that there is no encryption for the data inputted or stored in the program at this time. Encryption will be important to help keep customers’ information safe. The seventh vulnerability found within the code during inspection is that the only validation within the program is the try and catch block in the DocData class. The CRUDController and GreetingController classes could also benefit from a try and catch block, as well as more input validation all around.

**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

|  |  |  |  |
| --- | --- | --- | --- |
| Dependency | Vulnerability ID | Description | Solution |
| [bcprov-jdk15on-1.46.jar](#l1_991c96a4e31e6c19e2b9136c8955bd423f2d) | |  | | --- | | 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:\*:\*:\*:\*:\*:\*:\*](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:\*:\*:\*:\*:\*:\*:\* | | 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. | Update to Bouncy Castle 1.78.1 |
| [classmate-1.5.1.jar](#l2_3fe0bed568c62df5e89f4f174c101eab2534) |  | Library for introspecting types with full generic information  including resolving of field and method types. | Update to Apache 2.4.62 |
| [hibernate-validator-6.0.18.Final.jar](#l3_7fd00bcd87e14b6ba66279282ef15efa30dd) | [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. | Update to Hibernate Validator 8.0.0 |
| [jackson-core-2.10.2.jar](#l4_73d4322a6bda684f676a2b5fe918361c4e5c) | cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | Core Jackson processing abstractions (aka Streaming API), implementation for JSON | Update to Jackson 2.17.0 |
| [jakarta.annotation-api-1.3.5.jar](#l6_59eb84ee0d616332ff44aba065f3888cf002) | cpe:2.3:a:oracle:projects:1.3.5:\*:\*:\*:\*:\*:\*:\* | General data-binding functionality for Jackson: works on core streaming API | Update to Jakarta 3.0.0 |
| [jakarta.validation-api-2.0.2.jar](#l7_5eacc6522521f7eacb081f95cee1e2316484) |  | Jakarta Annotations API | Update to Jakarta 3.1.0 |
| [jboss-logging-3.4.1.Final.jar](#l8_40fd4d696c55793e996d1ff3c475833f836c) |  | Jakarta Bean Validation API | Update to JBoss 3.6.0 |
| [jul-to-slf4j-1.7.30.jar](#l9_d58bebff8cbf70ff52b59208586095f46765) |  | The JBoss Logging Framework | Update to SLF4J 2.0.13 |
| [log4j-api-2.12.1.jar](#l10_a55e6d987f50a515c9260b0451b4fa217dc) | [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) | JUL to SLF4J bridge | Update to Log4j 2.23.1 |
| [log4j-to-slf4j-2.12.1.jar](#l11_dfb42ea8ce1a399bcf7218efe8115a0b7ab) |  | The Apache Log4j API | Update to Log4j 2.23.1 |
| [logback-core-1.2.3.jar](#l12_864344400c3d4d92dfeb0a305dc87d95367) | [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) | The Apache Log4j binding between Log4j 2 API and SLF4J. | Update to Logback 1.5.6 |
| [slf4j-api-1.7.30.jar](#l13_b5a4b6d16ab13e34a88fae84c35cd5d68ca) |  | logback-core module | Update to SLF4J 2.0.13 |
| [snakeyaml-1.25.jar](#l14_8b6e01ef661d8378ae6dd7b511a7f2a33fa) | [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) | The slf4j API | Update to 1.2.2 |
| [spring-boot-2.2.4.RELEASE.jar](#l15_225a4fd31156c254e3bb92adb42ee8c6de8) | [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) | YAML 1.1 parser and emitter for Java | Update Spring Boot to 3.3.2 |
| [spring-boot-starter-web-2.2.4.RELEASE.jar](#l16_ec75d01d212b5229c16d872fb127744c0ed) | [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) | Spring Boot | Update Spring Boot to 3.3.2 |
| [spring-core-5.2.3.RELEASE.jar](#l17_3734223040040e8c3fecd5faa3ae8a1ed6d) | [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) | Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container | Update Spring Core to 6.1.11 |
| [spring-web-5.2.3.RELEASE.jar](#l18_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) [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 Core | Update Spring Web 6.1.11 |
| [spring-webmvc-5.2.3.RELEASE.jar](#l19_745a62502023d2496b565b7fe102bb1ee22) | |  |  | | --- | --- | | [r](#l19_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) [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 | Update Spring Web mvc to 6.1.11 |
| [tomcat-embed-core-9.0.30.jar](#l20_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) | Spring Web MVC | Update the Tomcat embedded core to 11.0.0-M222 |
| [tomcat-embed-el-9.0.30.jar](#l21_406e0c7cc45204c0f81853d73e8cfedfa4e) |  | Core Tomcat implementation | Update the Tomcat embedded El to 11.0.0-M22 |
| [tomcat-embed-websocket-9.0.30.jar](#l22_33157f6bc5bfd03380ebb5ac476db0600a0) | [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 | Update the Tomcat embedded websocket to 11.0.0-M22 |

**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.

There are a few steps that can be taken to help mitigate the identified security vulnerabilities for Artemis Financial’s software application. Many issues would be resolved by updating the dependencies to a newer version, helping keep quality of code high and the possibility of hackers manipulating the system low. In addition, adding various input validation and encryption among the code would help amplify the security within the application. Utilizing encapsulation will help keep the data stored and transmitted through the website safe and protected. Lastly, not inputting variables through a request parameter will help keep personal information secure and gives attackers less of a chance to intercept customer information.