# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **03/18/2025** | **Nyzheir Warner** | **Implemented Client Needs** |
| **2.0** | **3/19/2025** | **Nyzheir Warner** | **Implement Area of Security – Manual Review** |
| **3.0** | **3/20/2025** | **Nyzheir Warner** | **Implement Static Testing – Mitigation Plan** |

## Client



## Developer

Nyzheir Warner

**1. Interpreting Client Needs**

Artemis Financial is a consulting company that develops individualized financial plans for customers, including savings, retirement, investments, and insurance. Due to the nature of their dealings Artemis Financial deals with sensitive customer information such as SSN, Bank Accounts, Retirement Accounts, and Investment Accounts. It is of utmost importance that Artemis Financial maintain client trust by avoiding security breaches and enforcing the highest level of scrutiny when it comes to customer protection and security. It’s unclear whether Artemis Financial conducts international transactions but it is possible there are some international transitions taking place in terms of international investments as a part of investment portfolios. Artimis Financials must comply with rules and regulations determined by CISA (Cybersecurity and Infrastructure Security Agency) and FDIC (Federal Deposit Insurance Corporation) which are in charge of making sure financial institutions implement the proper safety measures to safeguard customer data and order them to disclose data-sharing practices. As vital as financial institutions are, they are exposed to plenty of external threats such as phishing and social engineering attacks, malware and ransomware, DDoS attacks, API vulnerabilities and even Insider threats. Artemis Financials has also expressed the desire to modernize their operations, a step towards achieving this included incorporating new technology such as WebSocket’s and Serverless computing. Along with the introduction of open-source software which allows for immense leaps in technological ability by providing access to a vast pool of reusable software components for free means Artimis can innovate without allocating a massive number of resources prior.

**2. Areas of Security**

Input Validation

Input from untrusted sources must be validated before use. Maliciously crafted inputs may cause problems, whether coming through method arguments or external streams. (Oracle, 2019) Without validation malicious users are able to abuse SpEL to perform injection attacks and access sensitive system components. It is important to validate user input to match only expected and safe command patterns which will lower risk of potential attacks.

API

Since we will be expecting user input through Rest API endpoints, we are at the same time exposing functions through these endpoints, it is extremely important that these interactions are secure. We need to use proper authentication and authorization techniques to ensure our system and user are safe. API security is the process of protecting APIs from attacks. Because APIs are very commonly used, and because they enable access to sensitive software functions and data, they are becoming a primary target for attackers. (Kovacic, 2022)

Client / Server

For Similar reasons as the API explanation, it is important to secure connections between the Client / Server to protect both the user and our system. Data is exchanged between client and server including user input and a subsequent response. According to OWASP TLS certificate should be valid and have the correct domain name, not be expired, and be installed with intermediate certificates when required. Additionally, for connections requiring authenticated access and all other sensitive information TLS connections should be utilized. This maintains that the Client/Server connection is authentic and secure, any failed TLS connections should not fall back to an insecure connection. (OWASP, 2010)

Code Error

Errors generated at any part of the application lifecycle should be properly and securely handled. The system should avoid exposing sensitive stack traces or detailed error information to the user. If not handled properly error messaging can help attackers understand how the system works without directly viewing the source code.

Code Quality

The best defense for your system is to start building the system with security in mind. High code quality is essential in preventing the introduction of potential vulnerabilities during the development process. Bad coding practices and sloppy code can lead to unintended behavior and exploitation. Improper code logic can make it easier for attackers to exploit flaws within your system.

Encapsulation

Encapsulation helps ensure that internal system components and functions are protected from being manipulated by unauthorized access. In the context of this scenario evaluations produced by SpEL should be executed in a controlled manner that restricts it from accessing other methods, classes, and data minimizing the potential for attacks on the system.

Cryptography

While handling sensitive information it is the standard to make sure all data is encrypted both at rest and in transit. Using technology protocols such as HTTPS and Server/Client-side encryption will help keep user information safe from potential malicious attacks.

**3. Manual Review**

Customer Class

1. Customer Class Name Should be capitalized to Customer not customer.
2. On line 5 the account\_balance variable declaration should be private
3. Should include standard getters and setters for private variables.
4. Customer should have a customer constructor for the object.

MyDateTime Class

1. MyDateTime class should follow proper naming conventions from myDateTime to MyDateTime
2. Lines 5-7 should be declared private variables to adhere to Encapsulation principles.
3. MyDateTime should have a custom constructor for the object

URL endings

1. All URL endpoints should check input against a while list as well as set an input limit to protect against overflow

Error Handling

1. It appears no thought has been put into error handling in any place of the code base which should be addressed.

**4. Static Testing**

hibernate-validator-6.0.18.Final.jar

* CPE - [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)
* Description - Hibernate's Bean Validation (JSR-380) reference implementation.

jackson-databind-2.10.2.jar

* CPE - [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)
* Description - General data-binding functionality for Jackson: works on core streaming API

log4j-api-2.12.1.jar

* CPE - [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)
* Description - The Apache Log4j API

logback-classic-1.2.3.jar

* CPE - [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)
* Description - logback-classic module

logback-core-1.2.3.jar

* CPE - [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)
* Description - ogback-core module

snakeyaml-1.25.jar

* CPE - [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)
* Description - YAML 1.1 parser and emitter for Java

spring-boot-2.2.4.RELEASE.jar

* CPE - [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)
* Description - Spring Boot

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

* CPE - [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)
* Description - Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container

spring-core-5.2.3.RELEASE.jar

* CPE - [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)
* Description - Spring Core

spring-expression-5.2.3.RELEASE.jar

* CPE - [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)
* Description - Spring Expression Language (SpEL)

spring-web-5.2.3.RELEASE.jar

* CPE - [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)
* Description - Spring Web

spring-webmvc-5.2.3.RELEASE.jar

* CPE - [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)
* Description - Spring Web MVC

tomcat-embed-core-9.0.30.jar

* CPE - [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)
* Description - Core Tomcat implementation

**bcprov-jdk15on-1.46.jar**

* CPE - [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)
* Description - 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.

**5. Mitigation Plan**

1. Input Validation – Implement a whitelisting function to check user input before processing it inside our application as well as restricting input type and length.
2. Secure API Interactions – We can enforce Spring Security to authenticate and authorize interactions with our system and application endpoints using tokens on PUT and POST requests.
3. Client / Server Communication – Require HTTPS for all interactions as well as verifying TSL certificates.
4. Error Handling – proper handle error handling and hide detail messages from users.
5. Code Quality – Refactor the code base to adhere to proper coding practices as according to OWASP standards.
6. Encapsulation – Make sure each class adheres to the principle of encapsulation making sure variables are hidden and method are properly exposed when needed.
7. Based on the findings in the Static test spring-boot-starter-parent should be upgraded to a version 3.4.+ and bouncy castle provider package should be upgraded to a version 1.78.+ to take care of vulnerabilities in current dependencies.

Works Cited

Kovacic, D. (2022, February 13). *API Security: The Complete Guide to Threats, Methods & Tools*. Bright Security. https://brightsec.com/blog/api-security/

Oracle. (2019). *Secure Coding Guidelines for Java SE*. Oracle.com. https://www.oracle.com/java/technologies/javase/seccodeguide.html

OWASP. (2010). *OWASP Secure Coding Practices Quick Reference Guide [Draft v2.1 -With identities added] Copyright and License*. <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/assets/docs/OWASP_SCP_Quick_Reference_Guide_v21.pdf>

*About the Federal Deposit Insurance Corporation (FDIC)*. (n.d.). Www.fdic.gov. <https://www.fdic.gov/about>

FFIEC. (2022). *Replaces October 2018 Resource Guide Cybersecurity Resource Guide for Financial Institutions*. <https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf>

Imperva. (n.d.). *Financial Services Cybersecurity | Threats & Solutions | Imperva*. Learning Center. <https://www.imperva.com/learn/data-security/financial-services-cybersecurity/>

Magnus. (2023, March 22). *The advent of open-source software has transformed modern software development by granting access to a vast pool of reusable software components, frameworks, and libraries. It has altered the software industry, allowing individuals to contribute to the development of software applications and democr*. Linkedin.com. https://www.linkedin.com/pulse/role-open-source-software-modern-development-magnusmageltd/