# CS 305 Project One

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **11/13/2024** | **Brandon Murphy** |  |

## 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

Brandon Murphy

**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?**

Artemis financial is a consulting company that develops individualized financial plans for its customers. This includes plans such as savings, retirement, investments, and insurance. It is important to have the client’s communications secured internally and externally because if their information gets out this could lead to people using this information on the client in an attempt to phish or scam them.

* **Are there any international transactions that the company produces?**

In dealing with clients with no specified restrictions financial plans such as saving, and investments specifically, it would make sense that the company would be dealing with international transactions or have the potential to do so being a financial firm.

* **Are there governmental restrictions on secure communications to consider?**

Artemis Financial will also need to follow government regulations regarding financial transactions and communications, which will affect data retention policies and security requirements. Some basic regulations include but are not limited to assuring they are compliant with 15 U.S. Code Chapter 98, 17 CFR Part 248, Subpart A, 15 U.S. Code Subchapter I, 15 U.S. Code 45, and HIPPAA. Penalties include fines of up to 28 million if found negligent.

* **What external threats might be present now and in the immediate future?**

External threats that are present now would be outside sources leaking client data and phishing attacks regarding this data. Since Artimis Financial deals with client savings, investments, insurance and retirement there is a high probability that there will be other sources they will be dealing with regarding client data. These transactions can be potential weak points in the security of client data externally. A fix could be to maybe have the client verify these transactions as they take place and assume the risks of the transactions taking place with external sources.

* **What modernization requirements must be considered, such as the role of open-source libraries and evolving web application technologies?**

Applications and bugs are constantly being patched and found technology is constantly evolving as well therefore having up to date maintenance checks. Artemis Financial needs to ensure that their libraries stay up to date within their application to ensure the current fixes for bugs and security threats are implemented.

**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.

* Input validation – When collecting user input validating it is crucial. As this program does allow input string validation is necessary to avoid any potential failures or SQL injection.
* APIs – As this application will run not just internally but externally as well such as on end users web browser a well-developed API will be necessary. API’s help to verify users by authentication and authorization, protect user data with API gateways, data classification, schema validation, and web application firewall.
* Cryptography – Cryptography is necessary as international transfers with proprietary customer information will be included with the transfers. The data should be secured in a fashion that can comply to both U.S. regulation and any regulation to its destination country.
* Code Error – This should work in tandem with the API and Input validation. Proper error handling will be necessary especially when dealing with input validation to prevent unauthorized access or privilege access violations.
* Code quality – When working with an end user including input and API the code quality is imperative to ensure that there is no unintentional data exposure.

**3. Manual Review**

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

Before inputting a more updated version and performing the dependency check I inspected the code for other shortcomings. I noticed in the CRUDController class Business names are sent as request parameters which is counter productive regarding input validation and secure coding practices. In the Greeting controller the input was not verifying, and I don’t think it was validating because there was no output. There also seemed to be no authentication scheme present. There is also no API, the program has no way for an end user to understand how to interact with it unless accessing the code. Artemis Financial would need to develop some type of data encryption for both storing information as well as sending international transactions that can comply with international regulations. The code quality was excellent though lacking an API so not fully functioning making not really user friendly.

**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:

A screenshot of a check

Description automatically generated

* 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

**Name:**

bcprov-jdk15on-1.46.jar

**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.

**Solution:** Upgrade to newer or safer Bouncy Castle JCE Provider version, 1.55 and earlier the ECIES implementation allowed the use of ECB mode which was regarded as unsafe.

**Identifier:** [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=11.1.0)

[**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)

**Name:**

hibernate-validator-6.0.18.Final.jar

**Description:**

Hibernate's Bean Validation (JSR-380) reference implementation.

**Solution:** Upgrade to hibernate-validator-6.0.20

**Identifier:** [**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=11.1.0)

[**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)

**Name:**

jackson-databind-2.10.2.jar

**Description:**

General data-binding functionality for Jackson: works on core streaming API

**Solution:** Upgrade to current version

**Identifier:** [**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=11.1.0)

[**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)

**Name:**

log4j-api-2.12.1.jar

**Description:**

The Apache Log4j API

**Solution:** Upgrade to 2.13.2 which supports this feature. Previous versions can set the system property mail.smtp.ssl.checkserveridentity to true to globally enable hostname verification for SMTPSconnections.

**Identifier:** [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=11.1.0)

[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)

**Name:**

logback-core-1.2.3.jar

**Description:**

logback-core module

**Solution:** A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data. Upgrade to latest version.

**Identifiers:** [**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=11.1.0)

[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)

**Name:**

snakeyaml-1.25.jar

**Description:**

YAML 1.1 parser and emitter for Java

**Solution:** SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. Recommend upgrading to version 2.0 and beyond.

**Identifier:** [**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=11.1.0)

[**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)

**Name:**

spring-boot-2.2.4.RELEASE.jar

**Description:**

Spring Boot

**Solution**: In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache**.** Upgrade to latest version.

**Identifier:** [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=11.1.0)

[**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)

**Name:**

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

**Description:**

Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container

**Solution:** In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache. Upgrade to latest version.

**Identifier:** [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=11.1.0)

[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)

**Name:**

spring-core-5.2.3.RELEASE.jar

**Description:**

Spring Core

**Solution:** In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition. Upgrade to latest version

**Identifier:** [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=11.1.0)

[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)

**Name:**

spring-expression-5.2.3.RELEASE.jar

**Description:**

Spring Expression Language (SpEL)

**Solution:** Upgrade to latest version

**Identifier:** [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=11.1.0)

[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)

**Name:**

tomcat-embed-core-9.0.30.jar

**Description:**

Core Tomcat implementation

**Solution:** Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue**.**

**Identifier:** [**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=11.1.0)

[**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)

**Name:**

tomcat-embed-websocket-9.0.30.jar

**Description:**

Core Tomcat implementation

**Solution:** Upgrade version to 8.5.64 or to a newer version.

**Identifier:** [**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=11.1.0)

[**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)

**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.

After reviewing the reports, a majority of the systems identified security vulnerabilities can be mitigated by upgrading to the later versions to fix these vulnerabilities and bugs found. Vulnerabilities I found in the code itself would be to move request parameters to headers or body rather than URI, Remove hard-coded database connection credentials, and implement a secure authentication scheme.