****

**Artemis Financial Vulnerability Assessment Report**

**Table of Contents**

**Artemis Financial Vulnerability Assessment Report**

Document Revision History

Client

Instructions

Developer

1. Interpreting Client Needs
2. Areas of Security
3. Manual Review
4. Static Testing
5. Mitigation Plan

**Document Revision History**

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **[Date]** | **Geoffrey Nix** |  |

**Client**

**Instructions**

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In the report, identify your findings of security vulnerabilities and provide recommendations for 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 choose to include images or supporting materials. If you include them, make certain to insert them in all 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**

1. **Interpreting Client Needs**

Secure communications are of a tremendous value to a monetary services company like Artemis Financial. Artemis will be handling large amounts of sensitive and highly personal information. Such as:

* Customer financial Data
* Account details
* Transaction records
* Personal identification information

Encryption and other security measures must be used to maintain the integrity and privacy of the data. In doing this, Artemis is demonstrating their commitment to security and will build trust with their clients to handle their valuable information. When client’s know that their information is safe, customer loyalty is enhanced which can result in an expansion of business and more revenue.

Artemis must comply with governmental restrictions and regulations that all financial services companies need to consider. Such as:

* Data protection and privacy laws
* Industry-specific regulations
* National security and surveillance laws
* Export/Import encryption regulations

Staying compliant with these requirements will allow Artemis’s financial dealings to remain legitimate while maintaining the necessary security and privacy.

Anytime there is financial data online there will be a plethora of security threats. Artemis must consider the following substantial threats:

* Cyberattacks
  + Phishing
  + Ransomware
  + Malware
* Insider Threats
  + Corrupt employees, contractors, partners
  + Data theft
  + Accidental disclosure
* Third-Party Risks
  + Third-party vendors
  + Cloud service providers
  + Payment processors
* Emerging technologies
  + Artificial intelligence(AI)
  + Blockchain
  + Internet of Things(IoT)

Artemis will need to implement robust and persistent cybersecurity measures to safeguard all sensitive data. Including constant collaboration with security experts and staying abreast of the latest security threats.

As it pertains to the role of open-source libraries, Artemis must carefully assess the security requirements to ensure that their system’s integrity is not breached. They must consider the following:

* Library selection and evaluation
* Incremental patching updates
* Vulnerability monitoring and mitigation
* Code review
* Secure development practices
* Dependency management
* Code testing

By implementing these security requirements, Artemis will minimize the risks associated with open-source libraries.

1. **Areas of Security**

* Input Validation
* APIs
* Encapsulation
* Code Quality

1. **Manual Review**

* *GreetingController* Class poses an injection vulnerability in the *greeting* method. The user input from the ‘*name*’ request parameter is directly passed to the ‘*SpelExpressionParser*’ w/o any validation or sanitation which could allow an attacker to execute arbitrary Spring Expression Language.
  + The *name* parameter is also used without proper sanitation in the response message as well; which could lead to vulnerabilities if the name input contains malicious scripts
* There is no explicit input validation for the *name* parameter in the *greeting* method and for the *id* parameter in the *number* method. User input validation must be implemented here.
* There are no Authentication and/or authorization mechanisms within the code.
* The user supplied ‘*message*’ in the *greeting* method and the accessed element from the *myArray* in the *number* method both log sensitive user information in the print statement.
* There is no CSRF(Cross-Site Request Forgery) protection.

1. **Static Testing**

| **Dependency** | **Vulnerability IDs** | **Package** | **Highest Severity** |
| --- | --- | --- | --- |
| **hibernate-validator-6.0.18.Final.jar** | [**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=8.2.1) | **MEDIUM** |
| **jackson-databind-2.10.2.jar** | [**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)  **cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\*** | [**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=8.2.1) | **HIGH** |
| **log4j-api-2.12.1.jar** | [**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=8.2.1) | **LOW** |
| **logback-core-1.2.3.jar** | [**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=8.2.1) | **MEDIUM** |
| **mongo-java-driver-2.4.jar** | [**cpe:2.3:a:mongodb:java\_driver:2.4:\*:\*:\*:\*:\*:\*:\***](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Amongodb&cpe_product=cpe%3A%2F%3Amongodb%3Ajava_driver&cpe_version=cpe%3A%2F%3Amongodb%3Ajava_driver%3A2.4) | [**pkg:maven/org.mongodb/mongo-java-driver@2.4**](https://ossindex.sonatype.org/component/pkg:maven/org.mongodb/mongo-java-driver@2.4?utm_source=dependency-check&utm_medium=integration&utm_content=8.2.1) | **MEDIUM** |
| **snakeyaml-1.25.jar** | [**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) | [**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=8.2.1) | **CRITICAL** |
| **spring-boot-2.2.4.RELEASE.jar** | [**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=8.2.1) | **HIGH** |
| **spring-boot-autoconfigure-2.2.4.RELEASE.jar** | [**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-autoconfigure@2.2.4.RELEASE**](https://ossindex.sonatype.org/component/pkg:maven/org.springframework.boot/spring-boot-autoconfigure@2.2.4.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=8.2.1) | **HIGH** |
| **spring-boot-starter-web-2.2.4.RELEASE.jar** | [**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) | [**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=8.2.1) | **HIGH** |
| **spring-core-5.2.3.RELEASE.jar** | [**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) | [**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=8.2.1) | **CRITICAL\*** |
| **spring-web-5.2.3.RELEASE.jar** | [**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) | [**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=8.2.1) | **CRITICAL\*** |
| **spring-webmvc-5.2.3.RELEASE.jar** | [**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) | [**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=8.2.1) | **CRITICAL\*** |
| **tomcat-embed-core-9.0.30.jar** | [**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=8.2.1) | **CRITICAL\*** |
| **tomcat-embed-websocket-9.0.30.jar** | [**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-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=8.2.1) | **CRITICAL\*** |

1. **Mitigation Plan**

* Injection
  + Implement strict input validation to ensure that only expected and safe input is accepted.
  + Avoid executing user input as code or passing it to expression parsers directly.
  + Consider using parameterized queries or prepared statements when interacting with databases to prevent SQL injection vulnerabilities.
* Input Validation:
  + Validate and sanitize all user-supplied input to ensure it meets the expected format and criteria.
  + Use input validation techniques, such as whitelisting or regular expressions, to enforce strong input validation.
* Authentication and Authorization:
  + Implement a robust authentication mechanism to verify the identity of users accessing the application.
  + Use authorization frameworks or role-based access control to enforce proper authorization and restrict access to sensitive resources or actions.
* CSRF Protection:
  + Implement CSRF protection mechanisms, such as using anti-CSRF tokens and validating them on sensitive operations.
  + Apply CSRF protection frameworks or libraries provided by the chosen web application framework, such as Spring Security's CSRF protection.
* Logging sensitive information
  + Avoid logging sensitive information or ensure that sensitive logs are properly secured and accessible only to authorized individuals.
  + Implement log sanitization to remove or mask sensitive data from logs.

In addition,secure coding practices need to be followed, all dependencies need to be kept up to date, scheduled assessments should be performed regularly, and developers should be educated on secure coding techniques.