**CS 305 Project One Template**

**Document Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| **1.0** | **9 Feb 2025** | **Tyler Allsopp** |  |

**Client**

Artemis Financial

**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**

Tyler Allsopp

**1. Interpreting Client Needs**

Artemis Financial handles sensitive financial data and must prioritize secure communications to protect client transactions, prevent fraud, and comply with financial regulations. Key considerations include:

* **Value of Secure Communications**: Ensures data confidentiality, integrity, and availability, protecting client trust and regulatory compliance.
* **International Transactions**: If the company processes international transactions, it must comply with financial regulations such as GDPR and PCI DSS.
* **Governmental Restrictions**: Compliance with encryption standards and secure data transmission laws.
* **External Threats**:
  + Phishing attacks targeting employees and customers.
  + Data breaches from insecure API endpoints.
  + Supply chain attacks from vulnerable third-party libraries.
* **Modernization Requirements**:
  + Adoption of secure open-source libraries.
  + Implementation of secure software development best practices.
  + Continuous monitoring for new vulnerabilities.

**2. Areas of Security**

Based on the vulnerability assessment process flow, the following security areas apply to Artemis Financial’s software application:

* **Data Encryption**: Protects sensitive financial data during transmission and storage.
* **Authentication and Authorization**: Ensures only authorized users access critical financial services.
* **Secure Coding Practices**: Prevents injection attacks, cross-site scripting (XSS), and insecure API exposure.
* **Third-Party Library Security**: Regular updates and monitoring of dependencies to avoid vulnerabilities.
* **Network Security**: Implementation of firewalls, intrusion detection systems (IDS), and VPNs.

**3. Manual Review**

Identified vulnerabilities from manual code inspection:

1. **Hardcoded Credentials** – Found credentials stored in source code.
2. **SQL Injection** – Unsanitized user input in SQL queries.
3. **Cross-Site Scripting (XSS)** – Lack of input validation in web forms.
4. **Insecure Direct Object References (IDOR)** – Unprotected endpoints exposing sensitive data.
5. **Weak Session Management** – No automatic session expiration.
6. **Improper Error Handling** – Stack traces exposing internal logic.
7. **Outdated Libraries** – Use of deprecated encryption algorithms.
8. **Lack of Input Validation** – No input sanitization on API requests.
9. **Excessive Permissions** – Overprivileged user accounts in the database.
10. **Unprotected File Uploads** – Allows execution of malicious scripts.

**4. Static Testing**

**Dependency Check Findings:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Library** | **Vulnerability** | **Description** | **Remediation** |
| hibernate-validator-6.0.18.Final.jar | CVE-2020-10693 | Improper message interpolation allowing attackers to bypass input sanitization. | Upgrade to the latest version. |
| jackson-databind-2.10.2.jar | CVE-2020-25649 | XML external entity (XXE) vulnerability. | Upgrade to latest version. |
| log4j-api-2.12.1.jar | CVE-2021-44228 | Remote code execution vulnerability. | Upgrade to Log4j 2.17.0 or later. |
| snakeyaml-1.25.jar | CVE-2017-18640 | Entity expansion vulnerability. | Upgrade to latest SnakeYAML version. |
| spring-aop-5.2.3.RELEASE.jar | CVE-2020-5408 | Bypass protections against RFD attacks. | Upgrade to latest Spring version. |
| tomcat-embed-core-9.0.30.jar | CVE-2021-25329 | Request smuggling vulnerability. | Upgrade to latest Tomcat version. |

**5. Mitigation Plan**

**To address identified vulnerabilities, the following actions are recommended:**

* **Code Refactoring:**
  + Remove hardcoded credentials and implement environment variable storage.
  + Use parameterized queries to prevent SQL injection.
  + Validate and sanitize all user inputs to prevent XSS.
* **Upgrade Dependencies:**
  + Update all vulnerable libraries to their latest stable versions.
  + Replace deprecated encryption algorithms with secure alternatives.
* **Enhance Authentication & Authorization:**
  + Implement multi-factor authentication (MFA).
  + Restrict user access based on least privilege principle.
* **Improve Security Configuration:**
  + Enforce secure session management policies (automatic logout, session expiration).
  + Implement proper error handling to avoid exposing sensitive data.
* **Strengthen Network Security:**
  + Apply HTTPS/TLS encryption.
  + Use a Web Application Firewall (WAF) to prevent attacks.
  + Monitor and log security events for threat detection.

By implementing these mitigation strategies, Artemis Financial can significantly enhance the security of its software application and reduce potential threats.