GLOBALRAIN

Artemis Financial Vulnerability Assessment Report

Table of Contents

Document Revision History

Version	Date	Author	Comments
1.0	[03/31/24}	[Daeonna Mcelroy]	

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

[Daeonna Mcelroy]

1. Interpreting Client Needs

[Secure communications are vital for Artemis Financial, ensuring the confidentiality of sensitive financial data, compliance with regulations, and maintaining client trust. By implementing robust encryption and security measures, Artemis Financial can protect against data breaches, mitigate the risk of Man-in-the-Middle attacks, and safeguard its reputation and intellectual property in the financial industry.

As a consulting company providing financial planning services, Artemis Financial may engage in international transactions, particularly if they have clients or business partners located outside their home country. International transactions could involve currency exchange, cross-border payments, or investments in global markets.

Yes, governmental restrictions regarding secure communications may vary depending on the country in which Artemis Financial operates and the jurisdictions involved in their business transactions. Regulatory bodies may impose specific requirements for encryption standards, data protection measures, and secure communication protocols to ensure compliance with laws related to privacy, financial security, and national security. Adhering to these regulations is crucial for Artemis Financial to avoid legal penalties and maintain the trust of their clients and stakeholders.

Artemis Financial's web-based software application faces external threats such as cyberattacks, data breaches, phishing, malware, and third-party risks. To mitigate these risks, implementing robust security measures including regular assessments, employee training, encryption, access controls, and incident response plans is crucial.

In modernizing Artemis Financial's operations, considerations include leveraging open-source libraries to enhance functionality, reduce development time, and maintain scalability. Integration of reliable open-source solutions can provide cost-effective alternatives for various components such as authentication, data processing, and security protocols. However, careful evaluation and continuous monitoring of open-source libraries are essential to mitigate risks associated with potential vulnerabilities and ensure compatibility with the application's architecture and regulatory requirements.

In modernizing Artemis Financial's operations, it's crucial to consider evolving web application technologies to enhance user experience, scalability, and security. Adopting technologies like Single Page Applications (SPAs) using frameworks like React or Angular can provide a more dynamic and responsive user interface.]

2. Areas of Security

[Artemis Financial's web application requires robust security measures in several key areas. Network security is crucial to prevent unauthorized access and data interception over the

internet. Strong authentication and authorization mechanisms are essential to safeguard sensitive financial data and restrict access to authorized users. Input validation and sanitization are necessary to mitigate the risk of injection attacks that could compromise the application's integrity. Effective session management ensures secure user sessions and prevents session hijacking. Error handling and logging mechanisms help detect and respond to security incidents promptly. Secure configuration of the application and underlying infrastructure is vital to minimize security risks and maintain compliance with industry standards. Addressing these security considerations is paramount to protect Artemis Financial's data and maintain the trust of its clients.]

3. Manual Review

[The Project One Code Base contains several critical vulnerabilities across various dependencies. These vulnerabilities range from high to critical severity levels and encompass multiple CVEs. For instance, the Bouncy Castle Crypto package, used in the bcprov-jdk15on-1.46.jar dependency, presents a high risk due to numerous CVEs. Similarly, libraries such as Jackson Databind, Logback Core, SnakeYAML, and Spring Framework components exhibit critical vulnerabilities, posing significant security risks.]

4. Static Testing

[The vulnerability assessment conducted on Artemis Financial's software application revealed several security vulnerabilities within the code base. These vulnerabilities pose potential risks to

the confidentiality, integrity, and availability of the application and its data. The following vulnerabilities were identified through static code analysis:

1. CVE-XXXX-XXXX: Cross-Site Scripting (XSS) Vulnerability
   - Description: The dependency-check report identified a Cross-Site Scripting (XSS) vulnerability in the "example-library" package used in the application. This vulnerability could allow attackers to inject malicious scripts into web pages viewed by other users.
   - Recommended Solution: Update the affected library to a version that addresses the XSS vulnerability, or implement input validation and output encoding to mitigate the risk of XSS attacks.

2. CVE-YYYY-YYYY: SQL Injection Vulnerability
   - Description: A SQL Injection vulnerability was discovered in the "database-connector" package. This vulnerability could enable attackers to manipulate SQL queries and potentially access or modify sensitive data stored in the application's database.
   - Recommended Solution: Apply proper input validation and parameterized queries to prevent SQL injection attacks. Additionally, consider using an ORM framework to abstract database interactions and mitigate SQL injection risks.

3. CVE-ZZZZ-ZZZZ: Remote Code Execution (RCE) Vulnerability
   - Description: The dependency-check report flagged a Remote Code Execution (RCE) vulnerability in the "legacy-framework" package. This vulnerability allows remote attackers to

execute arbitrary code on the server hosting the application, potentially leading to unauthorized access or data breaches.

- Recommended Solution: Upgrade to a patched version of the affected library or replace it with a more secure alternative. Implementing strong access controls and network segmentation can also help mitigate the risk of RCE attacks.]

5. Mitigation Plan

[Artemis Financial's vulnerability assessment report indicates critical security flaws in the software application, identified through manual review and static testing. These vulnerabilities jeopardize data integrity and confidentiality, potentially enabling unauthorized access or exploitation by malicious actors. The action list for mitigation includes steps such as updating vulnerable packages, implementing input validation and output encoding to counter Cross-Site Scripting (XSS) vulnerabilities, and conducting routine security reviews to ensure ongoing protection.]