**Client**

I engaged with Artemis Financial, which sought expertise to modernize its operations and enhance the security of its web-based software applications, especially in managing financial transactions and data securely.

**Key Issues Addressed**

* I focused on protecting client financial data during transactions and communications, a critical aspect given Artemis Financial's involvement in international transactions.
* I ensured compliance with various data protection laws and encryption standards, which are pivotal in maintaining client trust and legal compliance.
* I worked on modernizing open-source libraries and evolving web application technologies to safeguard against potential security risks.

**Achievements in Identifying Software Security Vulnerabilities**

I successfully identified multiple vulnerabilities, particularly in areas of input validation and secure API interactions. My efforts highlighted issues in the CRUDController and GreetingController classes, where user inputs were not properly validated, and in the RestServiceApplication class, which could potentially expose sensitive information due to insecure API interactions.

**Importance of Coding Securely**

Secure coding is essential to protect against unauthorized access and data breaches, ensuring the confidentiality and integrity of sensitive information. For a company like Artemis Financial, robust software security preserves client trust, maintains regulatory compliance, and reduces the risk of financial and reputational damage.

**Challenging or Helpful Parts of the Vulnerability Assessment**

The manual review of code and static testing using the dependency-check plugin were particularly helpful. These steps enabled a thorough identification of vulnerabilities and provided a structured approach to mitigating them.

**Increasing Layers of Security**

I proposed updating vulnerable libraries, enhancing input validation, and implementing strict access control measures. These steps are crucial for building a more secure application framework.

**Future Tools and Techniques for Assessing Vulnerabilities**

I plan to continue using tools like the OWASP Dependency-Check plugin and consider integrating other static analysis tools like SonarQube or Snyk to regularly assess and mitigate vulnerabilities.

**Ensuring Functional and Secure Applications**

After refactoring the code, I recommended thorough testing and validation to ensure that no new vulnerabilities were introduced. This approach is essential to maintain the functional integrity and security of the application.

**Resources and Practices for Future Tasks**

I will continue using secure coding practices, regular dependency checks, and adherence to security best practices like encryption and error handling in future software development projects.

**Demonstrating Skills to Future Employers**

From this assignment, I can showcase my ability to perform comprehensive vulnerability assessments, my understanding of secure coding practices, and my proactive approach to mitigating security risks. The detailed vulnerability assessment report, including my findings and mitigation strategies, serves as a practical demonstration of my skills and knowledge in software security.

This comprehensive understanding and approach not only helped Artemis Financial but also equipped me with valuable skills and knowledge applicable to future security challenges in the software development field.