**Artemis Financial Security Portfolio**

This repository contains artifacts and reflections from my work with Artemis Financial during the Computer Science program. Below are my responses to the provided questions:

**Brief Summary of Artemis Financial and Software Requirements:**

Artemis Financial is a leading financial services company focusing on investment management. Throughout the course projects, we engaged with Artemis Financial to assess vulnerabilities in their software systems and to implement secure coding practices. The client's primary concern was to ensure the integrity and confidentiality of their financial data, as well as to protect their systems from potential cyber threats.

**What I Did Well in Identifying Software Security Vulnerabilities:**

During the vulnerability assessment, I meticulously analyzed Artemis Financial's software systems, identifying various vulnerabilities such as SQL injection, cross-site scripting (XSS), and inadequate access controls. My attention to detail and thorough understanding of common security pitfalls enabled me to pinpoint potential areas of exploitation. Coding securely is crucial as it mitigates the risk of data breaches, protects sensitive information, and preserves the reputation and trustworthiness of the company. Software security adds significant value to a company's overall wellbeing by safeguarding against financial losses, regulatory penalties, and reputational damage.

**Challenging or Helpful Aspects of the Vulnerability Assessment:**

One challenging aspect of the vulnerability assessment was prioritizing vulnerabilities based on their severity and potential impact on Artemis Financial's operations. Additionally, identifying vulnerabilities that could lead to sophisticated attacks required extensive research and analysis. However, this process was also beneficial as it enhanced my understanding of evolving cybersecurity threats and the importance of staying updated with industry best practices.

**Increasing Layers of Security and Future Mitigation Techniques:**

To enhance security layers, I implemented various mitigation techniques such as input validation, parameterized queries, and role-based access controls. In the future, I would leverage automated vulnerability scanning tools and conduct regular penetration testing to assess vulnerabilities comprehensively. Additionally, adopting a proactive approach to security by implementing security frameworks like OWASP Top 10 can further strengthen Artemis Financial's defenses against emerging threats.

**Ensuring Functional and Secure Code:**

After refactoring the code, I conducted rigorous testing, including unit tests, integration tests, and security testing, to ensure both functionality and security. Code reviews by peers and security experts were also instrumental in identifying potential vulnerabilities introduced during the refactoring process. Continuous monitoring and periodic code audits are essential to maintain the integrity and security of the software application over time.

**Resources, Tools, and Coding Practices:**

Throughout the projects, I utilized various resources such as OWASP guides, security forums, and online tutorials to deepen my understanding of software security principles and practices. Tools like Burp Suite, OWASP ZAP, and static code analysis tools proved invaluable in identifying and mitigating vulnerabilities efficiently. Embracing secure coding practices such as least privilege, principle of least astonishment, and secure defaults will be beneficial in future assignments or tasks involving software development and security.

**Examples for Future Employers:**

From this assignment, I would showcase artifacts such as the vulnerability assessment report, secure coding guidelines, and evidence of code refactoring and testing. These demonstrate my ability to identify and mitigate security risks, implement secure coding practices, and ensure the overall integrity and security of software systems. Additionally, I would highlight my proactive approach to security, continuous learning, and willingness to adapt to evolving cybersecurity challenges.