The completed Artemis Financial Practices for Secure Software Report

Simin Mottahedi

**Briefly summarize your client, Artemis Financial, and their software requirements. Who was the client? What issue did they want you to address?**

Artemis Financial, a financial service company, needed assistance in addressing the security vulnerabilities in its respective software system.

The company was focused on ensuring that the software system is developed and implemented in a secure manner and environment.

Along with mitigating the potential risk and vulnerabilities the aim of the company is to generate a safe environment for maintaining confidentiality, integrity, and availability of their financial data and services[[1]](#footnote-1).

**What did you do very well when you found your client’s software security vulnerabilities?**

Throughout the process involvement and completion, different vulnerabilities of the Artemis Financial System have been identified. Performing meticulous analysis of the software application, resulted in revealing weaknesses like inadequate authentication mechanisms and data encryption, along with insufficient input validation and potential code injection vulnerabilities. Expertise in the relevant field helped in providing valuable insights into the potential risks and weaknesses enabling addressing the vulnerabilities effectively.

**Why is it important to code securely? What value does software security add to a company’s overall wellbeing?**

Professionalism and proficiency in identifying and addressing security vulnerabilities highlight the importance of coding securely. Addressing the fact that secure coding practices are essential for several reasons[[2]](#footnote-2). The nature of safeguarding sensitive data and unauthorized access and mitigating the risk of malicious attacks, such as data breaches or theft. By implementation of proper security measures, the company can ensure the safety and privacy of its client’s information. The software application’s reliability and integrity is directly proportional with the secure coding practices. The chances of the software malfunctioning have been minimized as of the vulnerabilities have been identified on an early stage of the assignment not only malfunctioning other disturbances or in simple words obstacles that may overpower the software proper functioning like system crashes, or other failures that can result in huge financial losses or reputational damage[[3]](#footnote-3). On a final note, it can be concluded that software security sets the benchmark for any company’s well-being in the respective market and competition by showcasing an image of providing top-quality security for its customer’s financial information and privacy.

**What part of the vulnerability assessment was challenging or helpful to you?**

The process of vulnerability assessment is full of both challenges and benefits. The complexity level of Artemis Financial Software System was one of the main challenges associated. A comprehensive approach is required for understanding the underlying architecture. Continuous learning and adaptability are required to match the evolving nature of security threats and stay updated on the latest vulnerability detection techniques. Along with that the assessment also provided numerous benefits, introducing to an in-depth knowledge of the potential risk associated with the financial software system. Through performing the task expertise in the relevant field has emerged and the confidence towards dealing with similar kind of situations in the future was boosted by performing securing testing and analysis methodology, such sought of experience developed confidence of identifying similar cases in the future with proper norms of mitigation strategies.

**How did you increase layers of security? In the future, what would you use to assess vulnerabilities and decide which mitigation techniques to use?**

Multiple layers of security have been implemented for enhancing the level of security for Artemis Financial. The aim was on several targets to avoid any kind of unnecessary breakdown due to code injection attacks etc. and implement robust data encryption techniques and methods to protect and safeguard sensitive data.

The future may seek to employ a combination of manual code reviews, automated vulnerability scanning, and penetration testing tools to completely address vulnerabilities. Identification of potential flaws and proper mitigation implementable strategies and measures relating to the requirements of the software system, such an approach can be considered to meet the level of changes in the working conditions.

**How did you make certain the code and software application were functional and secure? After refactoring the code, how did you check to see whether you introduced new vulnerabilities?**

Rigorous testing and validation process has been followed for ensuring both functionality and security[[4]](#footnote-4). For verifying the nature and the response generated was up to the expectations by the software, several level and mode of testing were conducted such as unit testing and system testing. For testing the software’s response against identified variabilities, security testing was also conducted in the pre-launch phase of the software.

**What resources, tools, or coding practices did you use that might be helpful in future assignments or tasks?**

Integrated development environments for example visual studio, eclipse, pycharm can be used as a resource for improving the productivity in coding. There are some online coding platform such as GitHub, bitbucket for implementing version control and tracking the changes or collaborating with other developers and management of the codes. A clear and concise documentation is also needed to be kept for the coding and unit testing frameworks should be used for ensuring correctness and easier maintenance such that it can help in future assignment.

In my opinion Creating SSL certificates and also dependency check tool are useful tool to use.

**Employers sometimes ask for examples of work that you have successfully completed to show your skills, knowledge, and experience. What might you show future employers from this assignment?**

I'd like to emphasize the final document because it demonstrates that I'm familiar with software security and capable of identifying vulnerabilities. They can also offer comments and responses from the activity to show their growth and critical thinking skills. By discussing the successful identification of weaknesses in the Artemis Financial System and the actions taken to address them, they demonstrate their capacity for problem-solving. They can highlight the meticulous testing and validation processes used to ensure the code's functionality and security and show how they drew on tools like the OWASP guidelines.

# 

Anwar C, Hady S, Rahayu N, Kraugusteeliana K. The Application of Mobile Security Framework (MOBSF) and Mobile Application Security Testing Guide to Ensure the Security in Mobile Commerce Applications. Jurnal Sistim Informasi dan Teknologi. 2023 Jun 20:97-102.

Assal H, Chiasson S. 'Think secure from the beginning' A Survey with Software Developers. InProceedings of the 2019 CHI conference on human factors in computing systems 2019 May 2 (pp. 1-13).

Filus K, Boryszko P, Domańska J, Siavvas M, Gelenbe E. Efficient feature selection for static analysis vulnerability prediction. Sensors. 2021 Feb 6;21(4):1133.

Khan RA, Khan SU, Khan HU, Ilyas M. Systematic mapping study on security approaches in secure software engineering. IEEE Access. 2021 Jan 18;9:19139-60.

1. [↑](#footnote-ref-1)
2. . [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. [↑](#footnote-ref-4)