Junyu Liang

Southern New Hampshire University

CS 305 Software Security Week 8

04/26/2024

* Briefly summarize your client, Artemis Financial, and their software requirements. Who was the client? What issue did they want you to address?
* What did you do very well when you found your client’s software security vulnerabilities? Why is it important to code securely? What value does software security add to a company’s overall well-being?
* What part of the vulnerability assessment was challenging or helpful to you?
* How did you increase layers of security? In the future, what would you use to assess vulnerabilities and decide which mitigation techniques to use?
* 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?
* What resources, tools, or coding practices did you use that might be helpful in future assignments or tasks?
* 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?

Artemis Financial is a reputable financial company dedicated to developing customizable financial services to meet the needs of individual consumers while prioritizing data security to prevent unauthorized access. As their customer, the main issue they asked me to address was enhancing the security of their software infrastructure to protect sensitive information and ensure compliance with regulatory standards.

One aspect of my expertise in identifying software security vulnerabilities is conducting thorough dependency testing to uncover potential weaknesses in the system. This meticulous approach is crucial because secure coding reduces the risk of data breaches and cyberattacks, thereby preserving the company's reputation and fostering trust among customers. Software security is integral to the overall health of a company, as it not only protects sensitive data, but also increases credibility and attracts more customers.

A challenging aspect of vulnerability assessment is distinguishing between real threats and false positives in the vast amount of data generated. However, I mastered this challenge by refining my analytical skills and utilizing a variety of tools to discern actionable insights from the evaluation results.

To enhance the security layer, I implemented SSL certificates and integrated HTTP posts into the system. Going forward, I intend to employ advanced vulnerability assessment techniques and leverage industry best practices to identify appropriate mitigation strategies for specific threats.

Ensuring the functionality and security of code and software applications requires a rigorous testing process and continuous monitoring. After refactoring the code, I conducted thorough testing to detect any newly introduced vulnerabilities and address them in a timely manner to maintain the integrity of the system.

Throughout the project, I took advantage of resources such as the web browser view in Eclipse, which proved invaluable in gaining insight and optimizing security protocols. In addition, I adhere to coding best practices and keep abreast of the latest developments in cybersecurity to improve my skills and proficiency for future tasks.

From this assignment, I will present my vulnerability assessment report, demonstrating my ability to effectively identify, analyze, and mitigate security vulnerabilities. This reflects my skills, knowledge and experience in software security and reinforces my commitment to ensuring robust and secure systems for my customers.