Steven Rodas

CS-405

10.27.2024

***Module 8-2: Journal***

Throughout this course I learned a ton about software security and the industry’s best security practices. Security has always been crucial to the success and health of any software but security seems to be more important today than it has ever been. With the amount of information we deal with instantaneously and how interconnected the world is through technology, there are more risks to consider when developing your software. Nowadays, it seems like there’s a critical bug being found in software we use daily coming up every year. Popular platforms and companies have fallen victim to malicious attacks and attempts to steal sensitive information in recent years and the effects of these attacks are still being felt. In order to achieve robust security, there are numerous steps within the development process that developers can implement to mitigate the risk. For example, adopting a secure coding standard and not leaving security to the end is a crucial step to securing your code. Coding standards and guidelines are there for developers to read, follow, and implement them accordingly. These standards are oftentimes lessons learned from previous developers or entities that experienced a vulnerability and reported on the findings. These coding standards are important to follow as they provide developers with a framework for how they should be conducting their work and the steps to take when developing their software. Additionally, not leaving security to the end is pivotal as you want to incrementally test your code for vulnerabilities and bugs as you go. When security is left to the end of the development process, serious bugs are found that could be layered between thousands of lines of code and could seriously derail an entire development lifecycle. Considering these steps and implementing them into your development is a significant process in developing any type of software, regardless of the complexity.