Tonessa V. Chatten

Journal 8-1: Reflection

During this course, I have learned the importance of using secure coding practices and guidelines. Adopting a secure coding standard ensures that the project will be consistent throughout and as secure as possible. When developing a program, it is crucial to implement security from the very beginning, starting at the planning stage before any development begins. This proactive approach ensures that security is not overlooked while maintaining the program's integrity and safety throughout the development process. Waiting until the end to address security risks can result in having to scrap the entire project and start over, wasting time and money and potentially damaging your reputation.

All developers should adopt the zero-trust policy to enhance security throughout their systems. This policy dictates never trusting a source and always verifying before accepting anything from it. This approach reduces the risk of attackers exploiting vulnerabilities and prevents data breaches. Treating everything as a potential threat until proven safe helps prevent unauthorized access to private information.

When developing a program, it is critical to consider security throughout the process. Security should be integrated from the very start and not left until the end. Practices such as exceptions, unit testing, encryption coding, static code analysis, and similar methods are important throughout the process. Adopting a secure coding standard and employing principles like Triple A (Authentication, Authorization, Accounting) and Defense in Depth will further ensure that your code is as secure as possible.