Nathan Kintu

CS-405

Portfolio Journal Reflection

Aug-19th-2023

In this course, the significance of employing secure coding practices and guidelines has been underscored. Opting for a secure coding standard not only ensures uniformity across the project but also maximizes its security. It is imperative to embed security measures within the program right from its inception, starting at the planning stage before actual development commences. This proactive approach safeguards against security oversights during development, maintaining the program's security integrity throughout. Delaying security implementation until the project's conclusion poses the risk of project abandonment and restart, squandering time, money, and reputation.

Developers are encouraged to adopt the zero-trust policy to bolster the security of their systems. This policy emphasizes the need to verify all sources before trusting them, thereby lowering the risk of attackers exploiting vulnerabilities and causing data breaches. Operating under the assumption that everything is a potential threat until proven otherwise is essential to safeguard private information from unauthorized access.

It is vital to prioritize security continuously during the program development process. Start by integrating security measures at the project's inception rather than deferring them. Incorporate elements such as exceptions, unit testing, encryption protocols, static code analysis, and related methods consistently while coding. Embracing a secure coding standard alongside Triple A and Defense in Depth strategies is key to maximizing the security of your code.