Liu, Kevin

25, April 2025

CS-405 Secure Coding

Professor Dewin Andujar

Portfolio Reflection

Adopting a secure coding standard early in the development cycle is essential for producing software resilient to attacks. While waiting until the end often leads to complete and costly recoding and in worse case scenarios, leave vulnerabilities unaddressed. Therefore, secure coding practices help identify risks early and saves time and money. Risk assessment is very important for software companies. For example, mitigating a low-cost, high-impact vulnerability yields a better return than addressing a rare, low-impact issue. Zero Trust is an interesting mindset of security where no trust is given, until after verification. Instead of trusting users and devices , it assumes every action is a potential threat that needs to be verified for safety. It also means that security will constantly be going through continuous process of verification. Implementing and recommending security policies ensures strong and robust security. A well-defined policy supports employes in outlining safe code and support compliance. Security policies should also be revisited regularly and adjusted to real-world threats and business needs.