Noah Lane Garza

6/30/2024

CS-405 Secure Coding

Journal: Portfolio Reflection

* ***Adoption of a Secure Coding Standard***

It's essential to adopt a secure coding standard to build robust software. By embedding security practices from the outset, we can proactively mitigate vulnerabilities that may otherwise be exploited. Guidelines from organizations like OWASP or CERT assist developers in crafting code resilient against prevalent threats like SQL injection and cross-site scripting.

* ***Evaluation and Assessment of Risk***

Assessing risks involves identifying potential threats and understanding their impact. Frameworks like the NIST Risk Management Framework help in organizing this process by providing guidelines for integrating security and risk management into the software development lifecycle. Conducting a cost-benefit analysis ensures resources are allocated wisely, balancing potential losses from security breaches against the cost of preventive measures.

* ***Zero Trust***

Zero trust model is a model that has zero trust to any users, devices, applications and therefore must authroize and see permissions for every single thing accessing its resources. It has a strict verification and identification process that identifies every user, device, and application accessing its resources. This model is to prevent data leaks and security breaches.

* ***Security Policies***

Effective security policies establish a framework for safeguarding information assets. A robust Security Governance Framework, such as ISO/IEC 27001, helps manage and protect information systematically. Regular updates and ongoing training are essential to ensure compliance and raise awareness among employees. By having better and stronger security policies, it can mitigate the risk of attacks and losses.