Molly Vaughns

CS 405 – Secure Coding

Jospeh Kovicac

June 24, 2025

Assignment 8-2 Portfolio Reflection

* Adoption of a secure coding standard, and not leaving security to the end

Adopting a secure coding standard is important, as it prevents the threat of attack throughout development and beyond. It should be standard practice in all steps of all projects and not left until the end. This helps discover vulnerabilities earlier, increasing the effectiveness of the layers of security. If security is left until the end, it can result in database breaches, which can harm company reputation and be costly.

* Evaluation and assessment of risk and cost benefit of mitigation

The vulnerabilities that can be more costly should be prioritized over ones that aren’t as likely to be exploited, ensuring the security is in place without overstretching resources, budget, and time available. How many resources should be designated to each area of development can help to spread the resources out, using them most effectively and efficiently.

* Zero trust

Zero-trust is becoming more necessary as cloud computing and storage are a common choice for mainstream applications. Confirming each device’s permissions, this is a form of zero-trust. This helps developers consider the potential for attacks that might not be in the forethought.

* Implementation and recommendations of security policies

The recommendations and implementations depend on the system and what sort of data is being stored/accessed. Regardless, a layered approach is encouraged to prevent possible attacks. This can help protect a variety of data types for companies. It is important to protect the system across the board so would-be attackers don’t just move onto what they would consider an easier target, without regard to the data stored.