Maridelle Anne Gonzales

June 24, 2025

CS405

8-1 Journal

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

Adopting a secure coding standard early in the development process is super important because it helps catch security issues before they become big problems. Leaving security checks until the end can lead to expensive fixes and risky vulnerabilities slipping through. Throughout the course readings, I learned that integrating security standards into every stage of coding makes the whole process smoother and builds safer software from the ground up.

* Evaluation and assessment of risk and cost benefit of mitigation

When it comes to evaluating risk and deciding which vulnerabilities to fix first, it’s essential to balance the severity and likelihood of threats against the cost of mitigation. Not every risk requires the same attention, so focusing on the highest priority issues like SQL injection or buffer overflows makes sense to get the most impact for the effort. The course showed how tools and automation can help assess these risks faster and more accurately.

* Zero trust

Zero Trust really changes the security mindset by assuming no one is automatically trusted, even inside the network. This approach fits well with secure coding and risk management because it adds layers of verification and limits access to only what’s needed. It’s a shift from traditional perimeter defenses to a more realistic, ongoing way to protect systems in today’s complex environments.

* Implementation and recommendations of security policies

Implementing security policies needs to be clear, repeatable, and supported by tools like static analyzers and automated testing. Policies are not just rules but guides that help developers consistently build secure code and handle risks effectively. The course highlighted that policies should evolve with emerging threats and technology, encouraging continuous learning and adaptation. Together, these approaches create a solid defense-in-depth strategy that protects both the software and its users.