**CS-405 Portfolio Reflection**

**Ulises A.**

From this course, one of the biggest takeaways for me has been the importance of treating security as a built in part of software development instead of something added at the end. Adopting a secure coding standard gives developers a clear set of rules and best practices to follow so that security becomes part of the process from the start. Before this class, I didn’t realize how easy it is to overlook simple things like input validation or error handling until they become serious vulnerabilities later. Now I see why “don’t leave security to the end” is a common saying it’s cheaper and more effective to design securely up front than to fix problems after release.

Another key concept was evaluating risk and the cost benefit side of mitigation. In real life, not every threat can be completely eliminated, so it’s about balancing security with resources. For example, encrypting every small piece of non-sensitive data might waste time and money, while skipping it for critical systems would be a major mistake. Risk assessments help teams focus on the most dangerous vulnerabilities first, which is more realistic in a business environment.

The zero trust model also changed how I think about security. The idea that “no one is safe” or that no device, user, or network connection should automatically be trusted makes a lot of sense today, especially with so many remote and cloud-based systems. Implementing zero trust means verifying every access request and constantly monitoring activity, even from inside the network. It’s a stricter mindset, but it’s necessary given how many attacks now come from compromised internal accounts.

Lastly, creating and following strong security policies ties all of this together. Policies define what’s acceptable, how to respond to incidents, and how users and developers should protect data. Good policies don’t just exist on paper they’re supported by training, regular updates, and accountability. If I were to recommend improvements, I’d suggest combining policy enforcement with automated checks or audits so compliance doesn’t rely only on people remembering the rules.

This course has helped me understand that secure coding, risk management, zero trust, and strong policies aren’t separate topics they all connect to form a security first mindset. That’s something I’ll carry forward in my future projects.