CS405 Module 8 Journal: Portfolio Reflection

Adopting and abiding by a secure coding standard is important in ensuring that you are creating good software. It is a good development practice to decide on a secure coding practice, and then abide by it. This will ensure that your code is not only secure, but is consistent throughout. It is also important to begin creating your system with security always in mind. By embedding security measures into the development cycle from the beginning, developers can minimize risks more effectively and avoid the pitfalls of addressing security as an afterthought. When security is left to the end, vulnerabilities often remain undetected until it is too late, leading to costly fixes and potential breaches. It is important to remember that the later a problem is found, the more costly it is to fix. Secure coding standards provide guidelines for developers to write code that is resilient to common attacks, such as SQL injection or buffer overflows.

Both evaluating and assessing risk is equally important, as it allows organizations to make informed decisions about which vulnerabilities to address and how to allocate resources. Risk assessment involves identifying threats, estimating the likelihood of them happening, and evaluating the impact that they can have. Once risks are identified, cost and benefit analyses can help determine if they are worth addressing. For example, while some risks may warrant immediate action due to their high impact, and high likelihood, others may require a different approach that considers the cost of implementation versus the potential consequences of leaving them unaddressed.

In a zero-trust model, all access requests are treated as potential threats until they have been verified and cleared. This is regardless if the requests come from inside or outside of the organization. This approach minimizes the attack surface and reduces the risk of bad actors moving throughout the system.

Implementing and recommending security policies is important for maintaining consistency and compliance across an organization. Security policies serve as a roadmap for how to handle important or sensitive data, respond to incidents, and ensure that guidelines are being followed. Effective policies should be clear and regularly updated to address threats that are always evolving. Threats are always changing, and the people who would attack your system or organization are always adapting and learning. So your security and coding policies must always be changing and evolving too.