Andrew McPherson  
CS-405  
12/18/2022

8-2 Journal:  
 Portfolio Reflection

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

It is important that you develop or apply a secure coding standard for the specific programming language being used for a project early in the development life cycle. This is mostly because different programming languages have different vulnerabilities or coding standards that may apply to that specific language, and it should be considered which language should be best for your project. This also comes into play by not leaving security to the end, as secure coding principles and practices should be implemented in every step or stage of development instead, even from the start. Defining not only a secure coding standard, but doing so at the start, or very early, in development is ideal.

* Evaluation and assessment of risk and cost benefit of mitigation

One of the reasons you don’t want to wait till the end to apply some level of security is that encountering issues or problems can be extremely costly to fix later, and such problems could have been resolved sooner in development. While there may be some cost involved with implementing security sooner, not having any security, or even until after an attack is much more costly, not only to your company but any of your customers. It is better to be preventative and prepared than to wait until after the fact to install some sort of security.

* Zero trust

The Zero Trust approach is essentially changing the way we verify users, and by default assume they cannot be trusted. It adds another level of the authentication process even beyond 2-factor authentication. Instead of just using username and passwords for verification and authentication it goes beyond it to ensure if a user, or device can be trusted or not, as well as what resources that specific device or user is required to use, and usually nothing beyond that.

* Implementation and recommendations of security policies

Security is a constantly changing thing, it is not static or stagnant and security policies will update and evolve over time. Using a security policy, with best practices, standards and other policies can be useful for your development project because in most cases they are well known, documented, and laid out before you as a good roadmap to follow and implement to have truly secure software.