Hillary Loyd

Professor Mike Prasad

CS 405 Secure Coding

February 26th, 2023

Portfolio Reflection

It is very common knowledge that incorporating security through the Software Development Lifecycle should be something that is started early. However, this practice is something that is often overlooked and maybe left to the end in some cases. If security principles and practices are incorporated as an everyday process, this will reduce the risk associated with security that may be seen. This goes back to the common practice of thinking about secure coding right out of the gate when developing a system. This could be from using testing, Triple-A Framework, Defense in Depth from the start.

Security threats can happen from any internal or external area. When looking at risk, it should be known that what may be seen as a threat today might not be the threat that will happen in the future. If secure coding practices are kept throughout the process then the cost of addressing the risk is much lower than mitigating the threats when they are happening. Like stated before this can be implemented with simple coding techniques, testing that will start at the beginning of development and often throughout the process and post production, and running static code analysis after another portion of code is added.

Zero trust should be assumed all the time. This is because the traditional authentication methods that are in use are failing as technology is advancing. Everything should be verified to make sure that it is not a threat. While still using something like a username and password, things like two factor authentication or even single sign-on access could be used to help verify that the user or device is what it is saying it is.

Security policies are a guideline for us to follow. This will ensure that the code is safe as well as the data that is being stored, transmitted, and used remains secure and safe. Not only is creating security policies a must but so Is reviewing, maintaining the, and making sure that everyone is using them for every project that is being developed. This will help maintain a consistent implementation of secure coding for the system.