CS 405 Module Eight Journal: Portfolio Reflection

Kelly Illescas

April 23, 2023

A secure coding standard must be adopted in any organization in order to ensure the organization maintains the highest level of security in its programs and systems. It is necessary to incorporate security awareness and mindfulness at all times because a program or system can potentially be hacked at any time during the development process. All phases of programming are vulnerable to attack, and must be carefully evaluated to ensure errors are caught in a timely and safe manner.

Because security is of the utmost importance in programming, and especially because the cost can rise to very high levels, it is necessary to evaluate the cost of mitigation based upon how severe the issue is to manage. For instance, if a repair carries an extremely high cost but is a low-level threat, it might be wiser to ignore it for the sake of a lower-cost, higher-level threat. Adopting zero trust in all aspects of programming is also a must. This will ensure that a program or system is even more effective in regard to security, as all users are automatically mistrusted and must authenticate each time they log in or use a program.

Security policy implementation is valuable because it will help to avoid issues after deployment of a program. When policies are put in place, it is less likely that mistakes will occur because outcomes are very clear. All programmers must be aware of and keep abreast of emerging security policy recommendations as well, because they are changing almost daily.