Ethan Klukkert

Professor Mill

CS-405 Portfolio Reflection

June 22, 2023

Portfolio Reflection

Adoption of a secure coding standard is crucial in the development of secure applications. As developers plan out an application, there has to be a consistent way of coding applications to fulfill security needs. Developers can have many different ways to solve a problem in mind, but security must be kept consistent. Security must not be left until the end. It has to be standardized and implemented from the start, otherwise security will not be at a desired level. If security is left until the end, then there is a risk that most if not all of the code has to be rewritten in the context of a secure application. This could potentially double the development time of an application, and the security can still not be as good as it could be. By starting and ending with security, an application will only need to be reviewed once for adherence to user needs.

A recommendation for a security policy is the Zero Trust best practice. This means when a network is unable to be closed, then the main point of security is identification and verification. All users who access data in the network are properly identified and allowed only the access they need to satisfy their needs. All other users who are not identified do not gain access, hence the phrase “zero trust”. No user can be trusted, unless they are properly identified for the data they want to access through the form of roles.