Portfolio Journal Reflection

During this course, I have learned the importance of using secure coding practices and guidelines. Adopting a secure coding standard ensures that the project will be consistent throughout and be as secure as possible. When developing a program, it is important to begin implementing security within the program from the very beginning. This means from the planning stage, before you even begin developing. This ensures that security does not get overlooked throughout the development of the program and it stays secure throughout. By waiting until the end to begin implementing security, you risk having to scrap the entire project and starting all over, wasting time, money, and your reputation.

The zero trust policy should be adapted by all developers to increase security throughout their system. This policy states to never trust a source and always verify before accepting anything from the source. This reduces the risk of a vulnerability being found by an attacker and a data breach occurring. Everything should be treated as a threat until proven safe to prevent unwanted persons from accessing private information.

When developing a program, it is important to always keep security in mind throughout the development process. First, always being implementing security from the very start and do not leave it to the end. It is also important to use things like exceptions, unit testing, encryption coding, static code analysis, and other similar methods throughout the development process when writing code. Adapting a secure coding standard and using Triple A and Defense in Depth will also ensure that your code is as secure as possible.