**Module Eight Journal: Portfolio Reflection**

Mitchell Lynds

Southern New Hampshire University

CS 405: Secure Coding

Mike Prasad

April 23rd, 2023

This course has covered lots of important best practices that I will continue to use going forward. Many of the covered principles interact and overlap. Organizations which adhere to principles like Triple-A, the adoption of a secure coding standard, not leaving security until the end, risk assessments, and zero trust architectures will almost by definition end up with a strong example of defense-in-depth.

The adoption can help prevent time consuming reworks of code and keep consistent practices across a team. Writing code without obvious vulnerabilities can be an important early layer to a defense-in-depth strategy. Not leaving security to the end can go hand in hand with architecting for security by allowing system designers to safely separate systems.

Performing risk assessments is a great way to prioritize the mitigation of vulnerabilities. Some vulnerabilities may have a high associated cost of mitigation, but a risk assessment may reveal that it is not necessary to entirely mitigate this vulnerability for this particular system. It also may reveal some quick fixes that can greatly improve the security of the system.

I really think of zero-trust as the logical extreme of a Triple-A implementation. It is an architecture where each sensitive process and dataset is its own subsystem and users are thoroughly authenticated at each step. Even for the accounting principle of Triple A, using a zero trust architecture makes it much easier to track which users are doing what.

While an individual working on their own project may be able to get away without a formally adopted security policy, any sufficiently large team will need to adopt a security policy document in order to effectively implement all of these concepts. Security is something that needs to be kept in mind by all developers at every stage, so a set of rules and standards is important. Without a security policy some “layers” of the defense-in-depth strategy may be missed.