**Portfolio Reflection**

Alexis Indick

Computer Science Department, Southern New Hampshire University

CS 405: Secure Coding

Dr. Mike Prasad

June 25th, 2023

Security is an important fundamental of coding. Every programmer should adopt secure policies when it comes to their applications. Reading the secure coding standards of the specific language they are using will help immensely with not making fatal mistakes in the code and keep attacks from happening. No programmer should leave security to the end. Security should be implemented at every stage of development no matter what. If we leave security just for the end, we will end up making more mistakes and even not catching a lot of mistakes. But if we implement security throughout, we have fewer mistakes and less work to do in the end.

A team of developers do need to assess the risks and cost benefits of mitigating when finding vulnerabilities. Some vulnerabilities are not as important as others so that’s why there are levels of priority to vulnerabilities and how much of a threat they could be. If a vulnerability has a higher priority, that is a good indicator that needs to be mitigated immediately. Those of lower priority are usually not much of a threat but still should be taken care of. It is risky to not mitigate problems that arise in code throughout the entire development process. By not fixing them quickly, we risk a lot since hackers can monopolize on it quickly.

The zero-trust model is an important model that is meant to protect against cyberattacks. Though users may find it annoying, it’s meant to protect them. The model itself means that no one is trusted which pertains to multifactor authentication and how it will ask you to submit a pin sometimes. By doing this, we prevent many attacks from happening versus not implementing zero-trust.

Security policies should be implemented at all stages of development just like secure coding standards. By keeping track of these policies in a written document, it helps the team to remember what they should be following and practicing. The security policy should have coding standards based on the language or languages being used for the project. The standards should be easy to understand and not vague so that everyone can refer to it and remember it. Showing threat levels and priorities of those threats is important since the team needs to know how serious a threat is. Keeping good communication with the team on these policies is important to make sure no one is behind or confused also.