Michael Tricoli

CS-405

Professor Hodde

June 25, 2022

**8-2 Journal: Portfolio Reflection**

**Adoption of a secure coding standard, and not leaving security to the end**

After finishing this class, I see how important implementing security into your code can save you in a professional environment. Using proper formatting and types of encryptions so that you worry less about hackers getting into your system. Applying these standards during initial coding and not having to go back later will save a lot of time and headaches. Your reputation is on the line when creating programs and they need to be secure. This way no sensitive information gets leaked, and you won’t possibly lose a job or clients over data breaches.

**Evaluation and assessment of risk and cost benefit of mitigation**

There are so many different types of protection methods that can implemented into your code. Deciding how much security you need and when is it overkill for time you are investing into the program. Knowing what levels of security to keep and what to leave out become important when getting the framework together of any program you’re working on. Making sure that you take each piece of your code and see what’s the best way to add layers of security without harming the performance or time it takes to finish. After completing this course I will be able to look over different policies and procedures and see where security must be strict and where we can save time by using minimal protection based on the information that is being handled by the program.

**Zero trust**

Something I already see a lot of in the IT world is Zero Trust practices. Never trust that the users will be safe when accessing information whether it be on purpose or by mistake. By taking away power and privileges from different levels of users you can make the entire network or program a more secure place. Even for the people you give power too you want to make sure if they were hacked you can still minimize the amount of data leaked or stolen by a hacker. Reading privileges where needed and for users with write privileges have proxies and two form auth to make sure the people using the credentials are the right people.

**Implementation and recommendations of security policies**

No matter where you work security polices should be in place. Whether its simply locking the computer every time you walk away from your desk or even time out when away from keyboard for a few minutes. These types of added security can be used anywhere a computer is used and not only when coding. The best way I think is to break down every step of a user’s access and see what they would be able to see. A white hacker style approach trying to break in and then build your security policies based on what weaknesses you found along the way. Then these will be incorporated for all future use cases when developing security or coding.