CS 405 Secure Coding

8-2 Journal: Portfolio Reflection

Alfredo Gomez

April 24, 2022

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

Adopting a secure coding standard is extremely important. Not only to myself as an induvial developer, but to a company as well. Companies are the ones that are more susceptible to security breaches since they house so much personal information. Leaving security to the end is what allows hackers to access the personal information. And based on the reading and videos throughout the course, I’ve learned that hackers are looking for reputation more then money. Being able to access personal information and show other hackers that you were able to do it is what they’re after. So leaving security to the end is the worst thing that a developer or company can do.

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

Being able to evaluate and assess risk is key to keeping sensitive information secure. Not only is it keeping information safe, but it’s also reducing the amount of funds that it takes to recover from a security breach. Risk will always be present, but it’s how you prepare for the risk that matters.

**Zero trust**

Zero trust policies are vital to keeping information safe and secure. By upgrading security to require two step authentication is a great tool. Not trusting anything is a great way to ensure that you are always prepared for a breach. Keeping up with all security standards is another method to an effective zero trust policy. You must watch out for internal and external threats.

**Implementation and recommendations of security policies**

In conclusion, by implementing security policies, you are ensuring that you do not become another statistic. Companies continue to get hacked and sensitive information is being stolen. By having a successful security policy in place is a great way to ensure that everyone’s sensitive information stays safe and secure.