Esi McAllen

CS-405

4/24/22

Portfolio Reflection

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

Coding standards hold everyone accountable. If you create standards, it makes it hard to stray and question how something should look like. Not leaving security to the end is a concept that lets programmers know to start with security rather than finish. Ultimately, if you leave things to the end, it allows for opportunities to be missed.

* Evaluation and assessment of risk and cost benefit of mitigation

Knowing the risks before you do something is always important both technically and not. Knowing your risks and benefits of mitigation can help before the coding is done because you can know what to prevent in terms of hackers.

* Zero trust

Zero trust is a concept that means, in terms of security, the benefit of the doubt should not be given to anyone. In this concept, you should require authorized and accounted for.

* Implementation and recommendations of security policies

Security policy recommendations should always be considered. A compromised security can risk the reputation of your company and also compromise the information to client’s data in return losing their trust.