Dylan Hardison

10/26/25

8-2 Journal: Portfolio Reflection

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

Secure Coding is crucial to creating any form of code. Default to zero trust, a malicious user will find and use any inkling of a security flaw to exploit your code and steal sensitive data. Always code like someone is trying to use that code to harm someone or something else.

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

At first glance, secure coding increases the build time and build costs of creating code but in the event of a security breach the increased upfront costs and time will seem miniscule compared to the reputation damage, time spent finding and resolving the security flaw, legal fees, etc.

**Zero trust**

Zero trust module refers to the idea that nobody should be trusted, including those that work within the same company until they have proven their identity through the use of authentication methods.

**Implementation and recommendations of security policies**

The security policy is a corporate document that is created to guide and hold employees accountable for their role in maintaining the security of the company systems and applications. By having a security policy, a company can show staff what is expected of them, and how the company is going to facilitate and enable them to be more secure, and clearly discusses the potential consequences for the company and the employee should they fail to comply with the policy.