Tyler Pease

CS 405-T4239

8-2 Journal: Portfolio Reflection

4/23/2023

Adopting a secure coding standard is important to make sure every person is on the same page with security. This makes everything be completed to the same standard of work. Leaving security to the end is never a good idea because it will cause a lot of problems in the long run. The best way is to address security as it comes along, there are many examples of this along the preproduction and production cycles. Leaving it to the end could lead to forgetting about said errors, or those vulnerabilities being exploited.

Evaluation and assessment of risk and cost benefit mitigation is also an important aspect of secure coding. Assessing how much risk something has is important to be able to determine how much of a factor a certain vulnerability will affect the security of the system. The cost benefit of mitigation is used to determine if the cost of fixing the vulnerability is worth the money to mitigate it or not. These two works together to give a better understanding of how severe the threats are to the system and whether or not they are worth fixing.

The zero-trust policy is worth thinking about in that it makes the developer consider that no one can be trusted when it comes to the security of the system. Every user can create problems for the system, whether or not they are accidental or malicious in nature. So, implementing a zero-trust policy would treat every user the same in which will mitigate the risk factors. Leaving less inputs for users helps to ease vulnerabilities since there is less room for the user to break the security of the system.

Implementations and recommendations of security policies help companies decide how they want to approach security for their system. Implementation can take a good amount of time especially if a company has completely changed it’s security policies.