Zac Gonzalez

21 April 2022

CS - 410

Prof. Hodde

**8 – 1 Journal**

I have learned a lot throughout this course. It is detrimental to adopt a secure coding standard. If a business leaves security to an end, which would mean to not priotize security until the end of development, that business can come into a world of trouble. Security vulnerabilities can pop up in any stage of development. That is why it is extremely important to focus on security from the start of development all the way through until the end of development.

It can be incredibly risky and costly for a business to put security on the back burner. If an attack occurs, the business can lose a lot of money along with loads of time wasted on fixing the issue. This can be prevented using secure coding. If a business chooses to not prioritize security, they are leaving themselves vulnerable to security threats.

Modern security policies often-times include a “Zero Trust” policy. Zero Trust involes not allowing access to information to anyone by default. This means that all users must prove they are truly who they are every time they want to access the information. This may be tedious at times, but it is worth the time and energy. With a Zero Trust policy, attackers have a much harder time gaining access to the information they are trying to hack into.

As I’ve stated above, it is important to implement various security policies to ensure there is proper protection from attackers. I would recommend not leaving security to the end, evaluating and assessing the risk and cost benefit of implementing secure coding standards, and utilizing a Zero Trust policy. If all three of these security measures are utilized, it will be much more difficult to hack into, thus increasing security for the business.