Journal 8-2: Portfolio Reflection

In this course we found that security isn’t a single piece of software. It is something to be developed over the entirety of new applications. And always needs to be considered in the development of software. For code to be considered secure, there needs to be standards.

One of those standards is not leaving security to the end. But beginning with the end goal in mind. Leaving security until the end leaves it as a last thought. Where vulnerabilities can be introduced and large amounts of refactor may be needed in order. Potentially requiring even more time since it’s close to the end of the development lifecycle.

According to the System Sciences Institute at IBM, it costs approximately six times more to fix a bug in the implementation stage rather than during the design phase (burns). In this case, security fixes are a required to be fixed as it can allow unauthorized or unauthenticated users to access your program. The cost to fix these vulnerabilities increase as the development lifecycle continues.

Adopting a secure coding standard is also a must. Having programmers and users adopt a standard keeps behaviors consistent. While allowing new vulnerabilities to be identified and handled simply by having a secure coding standard in place. Some vulnerabilities are worse than others and require higher prioritization. But a policy can help these issues get identified before they become a production vulnerability.

Once in production, one way to handle security is through a zero trust policy. Not assuming there is any network edge is a simple way to identify how zero trust works. Whether a user is within the organizations network or outside. They must follow the requirements that are be authenticated, authorized, and validated for security configuration (Raina). At the end of the day, black hats can reach your systems from within the network depending on business model. Treat all users and connections as if they were black hats.

# References

Ellie Burns. (2022) The cost of fixing bugs throughout the SDLC - Tech Monitor. Retrieved April 21, 2022, from <https://techmonitor.ai/technology/software/cost-fixing-bugs-sdlc>

Kapil Raina. (2022) What is Zero Trust Security? Principles of the Zero Trust Model. Retrieved April 22, 2022, from https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/