Timothy Kelly

CS-405: Secure Coding

8-2 Journal: Portfolio Reflection

April 24, 2021

This has been a very challenging course for me with all the different material and information surrounding cyber security. I constantly felt like the material was over my head at times, but I enjoyed that it brought me out of my comfort zone. It allowed me to experience the various ways attacks are implemented and coordinated, as well as the structure of some of the methods used. Coding standards seem like something that always comes up in every course because without this, there is no order, no basic structure, no guidelines. Never hard code sensitive information seemed to stick out for me when it came to adopting one of my own. With all the different ways that someone can obtain personal information, it only seems obvious that you wouldn’t want to hard code anything related to this. Personally, this is almost the same as an attack into someone’s system in a way that you’re essentially giving this information away without any protection.

I believe it goes without saying at this point that no one should leave security till the end. This should be integrated into the program just like any other main feature. By implementing security strategies from the beginning, you allow your program to grow along with security risks and standards opposed to redesigning the program at the end to fit these security techniques into the project. You may also eliminate a costly update or mistake by implementing security measures early. I believe you also need to take into account the type of program that is being developed and what information needs to be protected. This brings us back to the motive of thinking like an attacker and what information is going to potentially be vulnerable if left unprotected.

Zero trust tends to tie into everything learned throughout this semester. By integrating security measures from the very beginning, you’re already thinking like an attacker and protection from any untrusted source. I believe we all wish we could rely on basic security measures, but due to the state of the world and intentions of others, it all comes back to the lack of trust and assuming every type of attack on a network is malicious. All of this just enhances one’s ability to be more cognizant and aware of their surroundings and vulnerability.