Benjamin Strickland

CS-405

August 18, 2021

Module 8 Journal: Reflection

Part of the purpose of this course was to instill in me that security is just as important as functionality, and must be included in every stage of development, starting from the beginning. I think that purpose has been met. With the ever-increasing interconnectedness of our digital lives, we have to assume that an attack will happen. When the attack occurs, although we might not be the target of the attack, it can still impact us. However, if we approach the development of software with a zero-trust policy, we might be able to mitigate the attack entirely. And even if we can’t stop the attack from happening, we might be able to limit the damage it causes, figure out how it happened, and take steps to ensure it doesn’t happen again.

“An ounce of prevention is worth a pound of cure” is an old saying that I have heard. It means that damage done is far more difficult to repair than what it might have cost to prevent the damage in the first place. This is a good mind set to have with software security. Even if it adds time to the development process, and even if it causes a hit to performance, security is worth it. This is because damage prevented is generally worth the cost. Naturally, this is a case of diminishing returns where more security might cost a lot with only a little benefit, but we should also keep in mind the damage a successful attack can cause to the users’ trust in our brand in the longer term. Trust is something that cannot be bought back.

One of the significant takeaways of this course was how to find and implement security policies. It is good to know that there is an entire security community built around improving security policies and standards, as well as offering instructions on how to implement them.