Jerrett Gonsalves

CS-405-R4487

Professor Conlan

April 26, 2024

Course Reflection

Security is an important concept that should be considered at every stage of development to mitigate potential threats. Adoption of a secure coding standard ensures that all team members are aware of common pitfalls that leave systems vulnerable to threats. Leaving security to the end of the development allows for security vulnerabilities to go missed and bubble up. Towards the end of the development cycle, there is typically less budget to deal with security vulnerabilities and there is the possibility of having to rework code to handle vulnerabilities which can leave applications vulnerable. The immediate cost of having to design and implement a secure coding standard is significantly less than the remediation that would occur after a vulnerability has been exploited. Organizations may able to use their funds to handle remediation costs, but repairing relationships with customer bases is a lot more difficult.

The most secure way to implement a secure coding standard is to implement a zero-trust policy. This essentially means that there are policies and procedures in place to consistently monitor and audit the system for any suspicious activity regardless if the activity occurs from outside or inside the organization. This is due to the fact that threats can come from outside or inside the organization and even external threats can successfully authenticate and authorize themselves to perform dangerous actions on a system by exploiting vulnerabilities. A zero-trust policy will likely slow down development and potentially the user experience as the more secure a system is, the more training and time it takes to correctly implement those security standards and there is also a possibility that the system may incorrectly identify a normal user interaction as a threat and interrupt their experience. For some systems, this is better than if a vulnerability were to actually be exploited, such as in financial web portals. In other cases, such as using social media, this sort of intense security might make the user distance themselves from the product. This is why it is important to carefully evaluate what aspects of your system need to be secured and the potential damage that could occur if it were to be exploited rather than just implementing zero-trust in all aspects of the system.