Nicholas Glover

8/18/2023

**CS-405: Module Eight Portfolio Reflection Journal**

Security must not be left to the end of the development cycle. It leads to preventable vulnerabilities slipping past inspection and testing phases and leads to less security overall. A way to mitigate the potential vulnerabilities is by adopting a secure coding standard and including security throughout the entire development cycle. It also has the benefit of catching flaws and vulnerabilities in the earlier stages of development when they aren’t as difficult to fix or patch.

When it comes to the cost of evaluating systems and mitigating threats, the most efficient strategy is to deal with the source of the issue when it first crops up. As the development cycle goes on, the cost of fixing an issue increases as the system grows and becomes more complicated. That means that flaws and vulnerabilities can easily snowball into very expensive issues to mitigate. It’s much easier to pay the cost of implementing a secure coding standard and proper testing procedures than it is to mitigate the threats they would have caused if they’d been left to the end of the development cycle.

As software continues to evolve, security must evolve with it. In the past, users’ tended to only access secure information on site, so it was easy to secure and the site was usually secured and that was it. Now that users are accessing data from all over and not necessarily on-site, security must evolve to keep the data secure. That’s where a zero trust policy comes in. It treats all users as not to be trusted until they pass the necessary security checks to access only the data that they need. It minimizes the risk to the rest of the system and minimizes the potential entry points for hackers to exploit.

Security policies are excellent guidelines to ensure the system and the data remain safe and secure. They contain the best practices to follow in order to maintain a consistent code base which minimizes the potential vulnerabilities and flaws that could be added due to inconsistent code. It’s in companies’ best interest to maintain their security policies and keep them up to date because the threats to data security are always evolving and the policies must evolve with them.