Portfolio Reflection

Ryne Williams

Department of Computer Science, Southern New Hampshire University

CS 405: Secure Coding

Olga Mills

10/16/2023

Adopting a secure coding standard is imperative to ensuring that data and sensitive information is kept safe from hackers. Keeping a focus on security at the beginning of the development process will help to increase the level of security and reduce the number of flaws and vulnerabilities in code by finding and fixing issues before the testing phase and having a better knowledge of what types of vulnerabilities to look out for. This will also help to speed up the testing phase, as it will potentially leave much less to find by way of vulnerabilities and flaws. Overall, implementing security coding standards at the beginning of the development process will help to speed up the development process and reduce costs.

The cost of extended testing, multiple rounds of testing, and reworking code to get rid of vulnerabilities and flaws can add up in a single project, especially when dealing with large development teams. The time it takes to test large amounts of code, send the code back to be fixed, and then retested can potentially double the cost of manpower in a single project when it comes to coding security. Companies not implementing security standards at the beginning of the process also leaves systems and programs at risk of infiltration from hackers who steal data and sensitive information to sell or use maliciously. Implementing security standards can greatly reduce the amount of exploits that a hacker could use to infiltrate a system and help to properly secure user data and information.

Zero trust is a concept that means that no one is safe, and everyone is a threat. This is a concept to help with security by considering all angles of attack and who could potentially infiltrate the system. It is important to monitor all activity in a system or program to ensure if someone is using their access for malicious means, it is caught and handled immediately. It is also important to limit access to all users to only the functions and services that are needed to complete their tasks. Zero trust also helps during the coding process by considering all angles in attacks and helps to guard against them. This can help to keep security of programs and systems higher and make it more difficult for hackers to infiltrate a system.

It is recommended to implement security policies that covers all relevant aspects of security vulnerabilities, as well as known issues that could be the source of issues for the system. Security policies should be implemented as soon as possible to mitigate the likelihood of attacks from hackers. There may be issues with training and culture change that can cause problems; however, these issues can be mitigated by implementing safety coding standards one at a time over a set period of time. This will help to allow the development and testing team to fully understand each standard before another is introduced, as well as minimize the stress that can come with learning new standards at such a fast pace.