Ismael DeRocco

Southern New Hampshire University

CS-405

6/25/2023

Portfolio Reflection

When thinking about secure coding, it’s important to think about how to set up security right at the beginning of the project and not leave it to the end. It’s easier to add security measures as you go instead of doing it all at once. When looking at the program, it’s important to make sure all input has some security or validation. This protects the program from breaking if the wrong type of information is typed in. This could also help in the case of key loggers as well to make sure the data isn’t being stored.

There are many risks when not thinking about security when creating a program. When working for a big company, there could always be hackers trying to steal information for many reasons, usually financial. They would take the data and sell it to other hackers or possibly even other countries if the company works close with the government. It might take more time to code when also adding security but that will save money in the long run. If you don’t start with the security and get hacked, it will cost much more money to fix the situation than it was to get the security up to code.

When coding everything should be considered as zero trust. This is the concept of you can’t trust anyone when coding a secure program. The program should be built with default, not allowing any user to access or manipulate the system. The privileges should be granted to each person accessing the system. Not every user should have the same privileges or any administrative commands. By using passwords and usernames, it can be tracked on when things are done in the system and by whole. Without any credentials, the user should not be able to access anything in the system. This is a good measure in protecting the system from outsiders and hackers.

There are many different things that can be done to protect yourself from threats. The first would be to add security to your system. This should be done in layers since one piece of security like a firewall won’t protect you from everything. By adding different types of security like malware protection, and a VPN you can create a secure system that can depend on itself from hackers. In addition to protecting, there should also be a 2-step authentication to help the users’ passwords and usernames stay safe from hackers who might attempt to phish them. Lastly, the coding practice should also be altered to have security in mind. Like when adding an input, there should be a system to check if the input is valid to ensure that the program won’t break due to incorrect format type. These breaks give the hackers a point where they can potentially get into the system. Every part of the code should be flawless, and each function should only have one function so that it’s easier for the code not to be broken into. Security is an important part in coding, and by altering your perception in security, companies can save both time and money with their product.