**CS405 8-2 Journal**

I believe that keeping security at the front of your mind throughout the whole development of software is very crucial in ensuring that it is as secure as possible. Most developers aren’t thinking about the security of the software when developing but about ensuring that it works properly. By doing this you will be able to reduce the vulnerability of the software from attacks and hackers. I think that every developer should adopt some type of standard related to security and development starting at the beginning. I also think that when developing software developers need to discuss the security standards and code that is needed for the software that they are developing. This will help the risk of an attack and strengthen their code as they develop it.

Since you can’t predict where or how an attack may take place you need to think about decisions thoroughly before coming to one. This is because threats can come from anywhere even internally and attackers are always looking for new ways to attack so you can’t assume that the same attacks will occur in the future even if they have happened in the past. If certain threats aren’t handled correctly, they can cause major issues. It isn’t very costly if these threats are handled appropriately but can be costly if you compare it to the risks that come with the attacks. If you are consistent with implementing certain coding techniques such as starting to test your code from the beginning and conducting multiple code analysis, then you can improve your odds of attacks not being successful against your software.

Just like everything else in the world, technology is always evolving into bigger and better things. By incorporating zero trust in your development plan, you can improve the security in your software in case the traditional authentication methods fail. With this being said every user must be verified/authenticated before allowing access to any computer, network, or data. Some ways to accomplish this is by implementing 2 step authentication, biometric authentication, or simply using their username and password. Another feature that has been popular lately is the single sign on feature.

Security policies are a very vital part of ensuring that our code and data are secure from any kinds of attacks. Once these policies are created you need to ensure that you keep them maintained and review them to know that they are still fitting the needs of the company. You need to keep these policies up to date and current because they are essentially the core principles and standards for coding that will need to be incorporated into any development projects that are being created within the organization. This will keep all development projects consistent with one another as well as safe and secure. The FTC has done a great job in keeping up with evolving technology and risks. Due to this they were able to learn about common vulnerabilities through real life lessons. Some examples of this would be user authentication, storing or transmitting any data, and controlling how much access a user has to the database. There are a ton of different best practices that should be followed to keep your data secure but one that I will mention is patching. Patching requires a user to enter a password to access the system. By doing this you are helping prevent the wrong user or unauthorized user from accessing certain data that they shouldn’t be accessing.