Gerardo Martinez

Professor West

4/25/2021

Journal Module Eight

Adoption of the secure coding and not leaving it till the end has become a best practice since taking this class. While applying this concept I have learned the importance of developing secure code along the processes of the development life cycle and why it is best to practice it along from the beginning till the end. By doing this developer’s have practice and shown the importance of valuing the work they create and the importance of keeping unwanted users from entering or altering valued user’s information. Doing this also builds a great reputation not only for the developer, but the company.

The evaluation and assessment of risk with cost benefits ensure that in the long run the recovery state will not be as costly from attacks and vulnerabilities. Applying the concept of secure coding through the lifecycle of development lowers the risk to the system and potential costly repairs.

Zero trust, is a great rule of thumb that can and should be understood by developers while producing blocks of code. Through the course I have learned to never trust what a user can input into the system through the simple cin command of cpp files. Not all users are friendly users to the system and not all users want exactly the same thing when entering a system. So applying the zero trust concept we can develop code that protects the “good” users from the bad users and limits the bad cookies from what they have access to.

Implementations and recommendations for secure policies are best practiced by keeping them up-to-date with the system that it is being performed on. Removing any obsoletes policies that are no longer required and applying up-to-date policies that keep a system safe can be applied in recommendations. Implementing these secure policies with all developing teams through class training and assuring that they are being applied in the development state can assure for best practices.