Dan Stull

CS 405]

06/22/2023

Journal Module 8

From the readings and the assignments throughout this course, I’ve learned the necessity of using secure coding practice and guidelines. Following these practices and guidelines will foster a more secure program from the beginning rather than problem-solving at the end. Implementing this approach at the beginning of development is crucial, saving the developer time and resources.

Utilizing the Zero Trust policy will mitigate many issues with hackers attempting to gain access to the application’s vital information. Requiring new and old users to constantly authenticate themselves upon each login will minimize future issues. Everything should be treated as a treat until proven otherwise.

One of the very first things one must do when developing anything is to keep security in mind, which should then carry through to the final days of development. Implementing it from the start will alleviate many issues that can pop up in the final days of development, which can cause a full-on re-working of the program, not to mention time and money. As far as the security measures that should be utilized and often, they include exceptions, unit testing, encryption coding, static code analysis. And not to mention keeping Triple-A (authentication, authorization, and Account) as well as the three standards of the encryption policy, in mind throughout.