Dominic Aguirre

CS405

04/28/24

Module 8 Journal

Working on security throughout the making of an application if more efficient and better for a program outcome. When you implement coding standards from the beginning it helps prevent mistakes that could be overlooked when going though in implementing security in the end. Making it part of the overall structure helps stop common security mistakes before they can be a problem and helps the overall program be safer. Having overall better security combined with regular testing throughout the design process can help catch mistakes and make the program overall more secure and harder to penetrate.

Evaluating risks is important is very important when trying to mitigate risks. A very good way of evaluating a program is often to get into the head of who might want into the program, how might they want to attack your application? What information would that want or what systems would they want access too? These evaluations are very important when making an application secure as when overlooked can cost companies a large amount of money if an unwanted user ever does gain access, not to mention the damage to the company’s reputation.

Zero trust is a concept in software security where no matter where traffic comes from it’s treated as it was someone who might not be trusted. For example, even if traffic for a website is coming from where the website is hosted its still treated as a foreign entity and all of the traffic is tracked and verified in order to make sure its not a hacker impersonating a user of the company.

Implementing a security policy is one of the best things a company can do in order to keep an application safe. Not only will it help stop problems before they can come up, but it can also keep everyone on the same page when it comes to best coding practices. Mitigating a problem before it comes up is always better than fixing it later and having a set of security policies in place is the best way to do this.