Morgan Masapollo

08/24/2024

CS405 Secure Coding

8-2 Journal

Having a proper security standard that everyone follows is very important for the team to adopt and follow as they are completing their coding projects and assignments. Security should begin being integrated as soon as possible so that testing can ensue and catch any errors within the security when it's added to the code as fast as possible. A good rule of thumb is to never leave security to the end as it will make it harder to integrate and will waste more time and resources if something goes wrong.

Along with integrating security as soon as possible and following the coding standards that already exist when it comes to creating new projects, there should be time set aside in the beginning of the project and during the project to evaluate potential risks so that tests can be completed and proper security measures can be implemented. This will save time, money, and resources as it would allow for the security to be created as soon as possible and with regular testing there will be a decrease in potential for having to backtrack on the code which unwinds progress made. This would mean more time has to go into the project so it costs the company more to complete.

The zero trust policy is an important one to always have in your head regardless of the type of project. This policy serves as a reminder that when you are building security you cant put full trust in the employees or the customers, you have to create layers that will make it so there is extra protection if an employee attempts to access something or if that employees credentials get stolen. This policy helps to remind developers that there needs to be additional levels besides just authorization so that if someone becomes compromised or an employee tries anything there will be additional walls to ensure the attacker will not have instant access to whatever sensitive data they are attempting to get to.

Security policies are important to implement because it is what keeps the company safe. By holding the employees to their policies it helps keep their data safe from getting compromised but it also means that if the associate tries anything there are fail safes in place which will create a trail back to the associate or deny the associate access if they are attempting to get into areas they aren’t supposed to be. If a company or area doesn’t have security policies in place I would immediately recommend them as it is leaving the company at high risk of an attacker getting ahold of the data. For instance recommending work emails that can only be emailed by other work emails, this would decrease the risk of getting emails with links that would give an attacker access. Or adding in proximity location so that if a logon was attempted from an unfamiliar place or if the company is in person only, attempted login from outside the given zone which would deny the login from happening.