Nellie Umanah

04/24/2021

Reflection

Adoption of a secure coding standard, and not leaving security to the end

I remember one of our discussions talking about not leaving security to the end for many reasons. One of the reasons are developers will not catch the bugs in time until after the software has been hacked. It is important to make a simple easy to read code break it down into pieces and test the code in chunks. It might seem like a longer process, but it saves a lot of time and money in the long run.

Zero trust based off readings is a security concept centered on the belief that organizations should not automatically trust anything inside or outside. Instead, it has to verify anything that wants to connect to the systems before it allows them access. “The strategy Zero Trust boils down to trust no one” says Charlie Gero, CTO of Enterprise and Advanced Projects Group.

Implementation and recommendations of security policies

I believe that each code that will be written into sections and it should be tested each section so that each bug is caught so that the code won’t be vulnerable to any attacks. It would save so much money and time when it comes to implementations. Testing a code during the implementation stages are very important because it will also tell developers if this code works or not.