* SQL Injection is caused by accepting data from an unauthorized source and not checking the validity of the source. It can be fixed by securing the database and checking the code for bugs which can be exploited by the hacker.
* The cause for an IDOR attack is that the code is having some bugs through which the URL can easily be tampered with and it can be used to access other users profile and make changes to it. It can be fixed by adding the browser session functionality through which the credentials of the user are stored in the browser and URL tampering is prevented.
* The cause of phishing attack is using a cloned website and typing the credentials without checking the validity of the website. It can be resolved by checking the security of the website and not typing the credentials into an unsecured website.
* Another type of vulnerability is brute force attack in which a programme is designed to generate random passwords and inject it into the credentials it can be fixed by using a secured and long password.