Name - Sushmita Semwal
Course - B.Sc IT
Roll No - 1022770
Subject - Information Security And Cyber Law Practical
Date - 17/6/21
Sign -

1) Different types of vulnerability for hacking a website or web application are

1) SQL Injection :- Injection is a security vulnerability that allows an attacker to alter ~~background~~ backend SQL statements by manipulating the user supplied data.
- An attacker can inject malicious content into the vulnerable fields
- Sensitive data like usernames, passwords etc can be read from the data base
- Database can be modified
- Administration Operation can be executed on the database

2) Cross Site Scripting :- It is also known as XSS. XSS vulnerabilities target scripts embedded in a page that are executed on the client side ie user browser rather then at the server side. • Attackers can use XSS to execute malicious scripts on the user's browser
- Making the use of this security ~~vulnerability~~ vulnerability, an attacker can inject scripts into the application, can steal session cookies, deface websites, and can run malware on the victim's machine

3) Broken Authentication and Session Management :- The websites usually create a session cookies and session Id for each valid session, and these cookies contain sensitive data like username, password, etc. When the session is ~~sensitive~~ ended either by logout or browser closed abruptly these cookies should be invalidated

- Making use of this vulnerability, an attacker can hijack a session, gain unauthorized access to the system which allows disclosure & modification of unauthorized information
- The sessions can be hijacked using stolen cookies or sessions using XSS.

4) Insecure Direct Object References -> It occurs when a developer exposes a reference to an internal implementation object such as a file, directory, or database key as an URL or as a FORM parameter. The attacker can use this information to access other object and can create a future attack to access the unauthorized data
- Using this vulnerability, an attacker can gain access to unauthorized internal objects, can modify data or compromise the application

5) Security Misconfiguration -> Security Configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform. If they are properly configured, an attacker can have unauthorized access to sensitive data or functionality. Sometimes such flaws result in complete system compromise. Keeping the software up to date is also a good security.
- Making use of this vulnerability, the attacker can enumerate the underlying technology & application server version information, database information and gain information about the application to mount few more attacks.