Ankit Sati Roll - 14 (1022724)

Sol 1 - Vulnerability of hacking website :-

1) SQL Injection -

Injection is a security vulnerability that allow an attacker to alter backend SQL statements by manipulating the user supplied data.

Injection occurs when the user input is sent to an interpreter as part of command or query and tricks the interpreter into executing unintended commands and gives access to unauthorized data.

example - SQL injection on the login pages using input fields and URL's interacting with the database.

2) cross site Scripting -

XSS vulnerabilities target scripts embedded in a webpage that are executed on the client side. These flaws can occur when the application takes untrusted data and send it to the web browser without proper validation.

3) Broken Authentication & Session Management :-

The websites usually create a session cookie and session ID for each valid session, and these cookies contain sensitive data like username, password, etc.

When the session is ended either by logout or browser closed abruptly, these cookie should be invalidated.

Making use of this vulnerability, an attacker can hijack a session and gain unauthorized access to the system.

4) Cross Site Request Forgery :-

CSRF is a forged request came from the cross site.

cross site request forgery attacks is an attack that occurs when a malicious website, email, or program causes a user's browser to perform an unwated action on a trusted site for which the user is currently authenticated.

Using this vulnerability as an attackers can change user profile information, change status, create a new user on admin behalf, etc.

5) Failure to restrict URL Access :-

Web applications check URL access rights before rendering protected links and buttons. Applications need to perform similar access control checks each time these pages are accessed.

In most of the applications, the privileged pages, locations and resources are not presented to the privileged user.

- Making use of this vulnerability attacker can gain access to the unauthorized URL's, without logging into the application and exploit the vulnerability. An attacker can access sensitive pages, invoke functions and view confidential information.