

81
Ans Most Common Website Vulnerabilities

1. SQL Injections

SQL Injection is a type of web application security ~~vulnerability~~ vulnerability in which an attacker attempts to use application code to access or corrupt database content.

2. Cross Site Scripting (XSS)

It ~~low~~ targets an application users by injecting code, usually a client side script such as JavaScript into a web application output.

3. Broken Authentication & Session Management

If this is not protected at all times, an attacker can hijack an active session and assume the identity of user.

4. Insecure Direct Object References:

It is when a web application exposes a reference into an internal implementation object.

5. Cross Site Request Forgery (CSRF)

It is a malicious attack where a user is tricked ~~to~~ into performing an action he/she didn't intend to do. A third party website will send a request to a web application ~~and~~ that a user is already authenticated against eg bank.