1) Web Sites Vulnerability →

a) SQL Injection →

It is a type of web application security vulnerabilit in which an attacker attempts to use application code to access on corrupt database content.

If successfull this attack allow attacker to create, read, update, alter data.

b) Cross Site Scripting →

XX S on Cross Site Scripting targets an application's user by injecting code usually as a client side script such as Javascript into a web application's output.

c) Broken Authencation & Session Managmut

This encompass several security issues, all of them having to do with maintaining the authentication credentials and session identifiers are not protected at all times, an attacker can hijack.

c) insecure Direct Object Reference →

Insecure Direct object reference is when a web application exposes a reference to an internal implementation object include files, database record.

d) Security Misconfiguration →

It encompasses several type of vulnerability all centered on a lack of maintenance on a lack of attention to web application config

— X —