Ques 1:- Study the different types of vulnerability for hacking a website or web application.

Ans 1:- Most common website Security Vulnerabilities are:-

1) SQL Injections:- SQL injection is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content. If successful, this allows the attacker to create, read, update or delete the data stored in the back-end database.

2) Cross Site Scripting (XSS):- Cross-site scripting (XSS) targets an applications users by injecting code, usually a clien-side script such as Java Script, into a web application's ~~output~~ output.

3) Broken Authentication & Session Management:- Broken authentication and session management encompass several security issues, all of them having to do with maintaining the identity of a user.

4) Insecure Direct Object References:- Insecure direct object reference is when a web application exposes a reference to an internal implementation object. Internal implementation objects include files, database, records and database key.

Sign:-
Thilche

5:- Security Misconfiguration:- Security misconfiguration encompasses several types of Vulnerabilities all centered on a lack of maintenance or lack of attention to the web application configuration. A secure configuration must be defined and ~~developed~~ deployed for the application, frameworks and platform.

6:- Cross - Site Request forgery (CSRF) :- Cross - Site Request Frogury (CSRF) is a malicious attack where a user is tricked into performing an action he or she didn't intend to do. A 3rd party ~~web~~ website will send a request to web application that a user is already authenticated against (eg., their bank).

Sign:-