* Sonu Mehra * 1022768(58) Sonu...
* Bsc IT

Ans1) Common security vulneration for hacking a websites are:-

1) SQL INJECTIONS :- SQL intection is a type of web application security vulneration in which an attack attempts to use application code to access or corrupt database content. If successfull, this allow the attackes to create, read, update, alter or delete data stored in backend database.

2) Cross site Scripting :- It target an application's user by intecting code, usually a clint-side script. such as Javascript, into a web application output. The concept of XSS is to ~~manipulate~~ manipulate client side script of a web application to execute in the manner desired by the attackers.

3) Broken authenication & Session mangement
It encompass several Security issues, all of them having to do with maintaing the identity of a user. If authentication credentials & Session identifiers are not protected at all times.

Sonu

4) Insecure Direct object Refrence:-

Insecure, direct object reference is when a web application express a refrence to an internal implementation object. Internal implementation of object include files, database records, directories & database key.

5) Security Misconfiguration

It encompasses several type of volnerabilites all centered on a lack of maintanance or a lack of attention to the web application configuration. A Security configuration must be defined & deployed from the application, frameworks.

6) Crosssite Request fugery-

It is a malicious attack where a user is tricked into performing an action he or she did'nt intend to do. A third panty website will send a request to a web application that a user is already authenticated aginst.

Sonu