Nimish Rana
1022745
Bsc(IT) 6th

Ans 1 Common security vulnerabilities for hacking a website are :-

1 :- SQL INJECTIONS

SQL injection is a type of web application security vulnerability in which an attack attempts to use application code to access or corrupt database content.
If successfull, this allows the attacker to create, read, update, alter or delete data stored in backend database.

2 :- Crosssite scripting

It target an applications user by injecting code, usually a client-side script such as Javascript, into a web application's output. The concept of XSS is to manipulate client side script of a web application to execute in the manner desired by the attacker.

(3) :- Broken authenication & session managment

It encompass several security issue all of them having to do with maintaing the identity of user.
If authentication credentials & session identifier are not protected at all the.

NB

(4) Insecure Direct object References

Insecure - direct object reference is web a web application exposes a reference to an internal implementation objects. Internal implementation objects include files, database records, directories & database keys when an application exposes a reference.

(5) Security Misconfiguration

It encompass several types of vulnerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration. A secure configuration must be defined & deployed for the application, frameworks.

(6) => Cross Request Forgery (CSRF)

It is a malicious attack where user is tricked into performing an action he or she didn't intend to do. A third parties website will send a request to web application that a user is already authenticated with eg (Her bank);