Aman Singh

Roll No - 1022721

BSCIT - 6 sem

Ans 1 - Common security vulnerabilities for hacking a websites 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 successfull, this allows the attacker to create, read, update, alter or delete data stored in backend database.

2) Cross site Scripting

It targets an application's users 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 scripts of a web application to execute in the manner desired by the attacker.

3) Broken authentication & session management

It encompass several ~~[illegible]~~ 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 ~~[illegible]~~ times, an attacker can hi-jack an active session & assume the identity of user.

Aman singh

Aman

1022721

BSCIT 6 sem

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, directories & database keys. When an application exposes a reference to one of these objects in a URL, hackers can manipulate it to gain access to user's data.

5) Security MisConfiguration

It encompasses 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. Security misconfiguration gives hackers access to private data or features & can result in a complete system compromise.

6) Cross site Request forgery (CSRF)

It is a malicious attack where a user is tricked into performing an action he or she didn't intend to do. A third party website will send a request to a web application that a user is already authenticated against (e.g their bank). The attacker can then access functionality via victim's already authenticated browser.