VIKAS SINGH PANWAR
(1022772) BSc (IT)

[Ans-1]

The diffrent types of vlunerability for hacking a website or web application:-

→ Network Vulenerabilities

These are issues with a network's hardware or software that enpose it to possible intrusion by an outside party.

→ Operating System Vulenerabilities

It is effectively an error in the code or the logic of operation within the OS or the application software.

→ Human Vulenerabilities

The weakest link in many cybersecurity architectures is the human element.

User errors can easily expose sensitive data, create exploitable access points for attackers, or disrupt systems.

→ Process Vlvenerabilities

It is the process of identifying, evaluating, treating and reporting on security vlvenerabilites in systems and the software that runs on them.

Most common website security vulenerabilities :-

1) SQL INJECTIONS
is a type of web application security vluenerability in which an attacker attemps to use application code to get acess-

2) CROSS SITE SCRIPTING (XSS)
targets on application's users by injecting tools, usually a client script such as java script.

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

4.) Insecure Direct Object References

when a web application exposes a reference to an internal implementation object.

5.) Security Misconfiguration

encompasses several types of vlunerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration.

6.) Cross Site Request Forgery (CSRF)

is a malicious attack where a user is tricked into performing an action he or she didn't intend to do.