Raj

Name – Raj Khan Bagga
Sub – Information Security
Roll no – 43
Course – B.Sc (IT)
University Roll no – 1022753

Ques ①

→ Most common website security vulnerabilities:

i) 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

ii) Cross site scripting (XSS):
It targets an application's users by injecting code, usually a client-side script such as Java-script, 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.

iii) Broken Authentication and session management:-
Broken authentication & session management encompass several security issues, all of them having to do with maintaining the identity of a user. If authentication credentials & session identifiers are not protected at all times, an attacker can hijack an active session & assume the identity of a user.

iv) Insecure direct object References:

It is when a web a web application exposes a reference to an internal implementation object. When an application exposes a reference to one of these objects in a URL hackers can manipulate it to gain access to a users personal data.

v) Security Misconfiguration:

Security Misconfiguration encompassion several types of vulnerabilities all centered on a lack of attention to the web application configuration. Security misconfiguration gives hackers access to private data or features and can result in a complete system compromise.