Name - Gaurav Singh Parihar
Course - B.Sc IT 6th sem
Roll no - 1022733
Sub - Information security & cyber law

Q1-

A Web application is an application based on the client server mode. The server provides the database access. ~~and~~ It is hosted on a web server. web application are ~~used~~ usually written in languages such as Java, C#, PHP, and websites are written in HTML, etc.

Most web application and websites are hosted on public servers accessible via the internet. This makes them vulnerable to attacks due to easy accessibility

- Different types of vulnerability of hacking a website a web application.

-> SqL injection :- is a security vulnerability that allows an attacker to alter backend sqL statements by manipulating the user supplied data. to bypass login algorithms()

-> Cross Site Scripting (XSS) :- XSS vulnerabilities target scripts embedded in a page that are executed on the client side i.e. user browser rather then at the server side. These flaws can occur when the application takes untrusted data and send it to the web browser without proper validation.

-> Insecure Direct
Object references :- It occurs when a developer expose a reference to an internal implementation object, such as a file, directory, or database key & in URL or as a form parameter. The attacker can use the ~~inff~~ information to access ~~ob~~ other objects and can create a future attack to access the unauthorized data

-> Cross site Request forgery :- it is a forgery request come from the cross site. CSRF attack is an attack that occurs when a malicious website, email, or program causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

-> Security Misconfiguration :- Security configuration must be defined and deployed for the application, frameworks, application server, web server, database server. if these are properly configured, an attacker can have unauthorized access to sensisitive data or functionality.