Name - Preeti Pal
Rollno - 1022773
Subject - Information Security
Course - BSc (IT) 6th sem.

Question 1.

Study the different types of Vulnerability for hacking a website or web application.

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 successful, this allows the attacker to create, read, update, alter, or delete data stored in the back-end database.

2) CROSS-SITE SCRIPTING (XSS)

It targets an application's users by injecting code, usually a client side script such as JavaScript, into a web application 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.

Broken authentication and session management encompass several security issues, all of them having to do with maintaining identity of a user.

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 and database keys.

Preeti Pal

Continue Q1

When an application exposes a references to one of these objects in a URL, hackers can manipulate it to gain access to a user's personal data.

5) Security Misconfiguration.

It encompasses several types of Vulnerabilities all centered on lack of maintenance or a lack of attention to the web application configuration. A secure configuration must be defined and deployed for the application, frameworks, application server, web server, database server and platform. Security misconfiguration gives hackers access to private data or features and 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 3rd 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 the victim's already authenticated browser. Targets include web application like social media, in browser email clients, online banking, and web interfaces for network devices.

Preeti