Name: Janishq Singh
Course: BSc-IT (6th Sem)
Rollno: 1022771

Subject: Information Security

Q1 The different types of vulnerability that a person faces to a websites are:

- SQL injection
- Cross Site Scripting
- Broken Authentication and Session Management.
- Insecure Direct Object Reference
- Security misconfiguration
- Cross Site Request forgery.
- DOS attack.

i) SQL injection:
Injection is a vulnerability that allow an attacker to alter backend SQL statement by manipulating the user data. Injection occurs when user data is sent to interpreter as part of command and the interpreter is tricked into executing such command which gives access to unauthorized data.

ii) Cross Site Scripting:
Making the use of Cross Site Scripting, attacker can inject Scripts into the application and hence can steal session cookies, deface website, and can run malware on the victim's machines. Also known as XSS vulnerabilities It basically target Scripts embedded in a page executed on client side.

Janishq

iii) Broken Authentication & Session Management ÷

Making use of Broken Authentication & Session Management, an attacker can ~~highja~~ hijack a session, gain ~~at~~ unauthorized access to the system which allow disclosure and modification of unauthorized information. Sessions are hijacked using stolen cookiess or session using XSS(cross site Scripting). Vunerable objects here are ÷(i) Session ID exposed on URL lead to session fixation attack
ii) Session Timeout (iii) Session reused by low privilage user

(iv) Insecure Direct Object Reference ÷

Using this vulnerability, attacker gain access to unauthorized internal object, can even modify data or compromise the application ~~Here~~ It occur when developer expose a reference to an internal implementation object.

(v) Cross Site Request Forgery ÷

It came from cross site. Basically here a attacker can change user profile information, change status, create new user on admin behalf etc. This attack occur when a ~~user~~ malicious website, email, or program cause a user's browser to perform unwanted actions.

(vi) DOS attack ÷ Denial-of-Service attack is meant to shutdown a machine/Network making it inaccessible

Tanisha.