Name: Sanchit Chaudhary
Course: B. Sc. (IT) 6th Sem
U. Roll no: 1022757
Subject: Information security & Cyber laws

Subject Code: PB160
Sign: Sanchit Chaudhary

Answer)

There are some common types of website or web application vulnerabilities that are frequently exploited by attackers. While this isn't an exhausted list of all the possible vulnerabilities a determined attacker may find in an application, it does include some of the most common vulnerabilities websites or web application today:

1) SQL Injection Vulnerabilities (SQLi)

SQL injection vulnerabilities refers to areas in website code where direct user input is passed to a database. this allows the cybercriminal to access the data website in a variety of ways, including:

- Injection malicious/spam ports into a site
- Stealing customer information
- Bypassing authentication to gain full control of the website

Due to its versatility, SQL injection is one of the most common exploited website vulnerability. It is frequently used to gain access to open source content management system (CMS) application, such as Joomla, Wordpress and Drupal.

2) Command Injection :-

Command injection vulnerabilities allow attackers to remotely run and execute code on the

the websites hosting server. this is done when user input that is parsed to the server, such as header information, is not properly validated, allowing attackers to include shell commands with the user information. Command Injections attacks are particularly critical because they can allow bad actors to initiate the following:

- Hijacks an entire site.
- Hijack an entire hosting server
- Utilize the hijacked server in botnet attacks

One of the most dangerous and widespread command injection vulnerabilities was the shellshock vulnerability that impacted most Linux distributions

3) Cross-Site Request Forgery (CSRF)

these attacks are less common, but can be quite jeopardous. CSRF attacks tricks the site users or administrators to unknowingly perform malicious actions for the attackers. As a result attackers may be able to do the following actions using valid user input:

- Change order values and product prices
- Transfer funds from one account to another
- Change user password to hijack accounts

These types of attacks are particularly dering for ecommerce and banking sites where attackers can gain access to sensitive financial information.

A CSRF attack was recently used to seize all controll of a Brazilian bank's DNS setting for over five hours.

4) Cross-Site Scripting (XSS) ?

It occurs when attackers inject scripts through unsanitized user input or other fields on a website to executed code on a website. Cross site scripting is used to target website visitors, rather than the website server itself. this often means attackers are injecting javascript on the website, so that the script is executed in the visitors browser. Browser are unable to discern whether or not the script is intended to be part of the website resulting in malicious actions including.

- Session hijacking
- Spam content being distributed to unsuspecting visitors
- Stealing session data.

Some of the largest scale attacks against Wordpress have been from cross-site scripting vulnerabilities However, XSS is not limited only to Open Source application. Recently, a cross site scripting vulnerability was found in gaming giant Steam's system that potentially exposed login credentials to attackers.