Name - Ishmita Raturi
RollNo - 1022736 (26)
Course - B.Sc(IT)
Subject - Information Security Subject Code -
Paper - Regular Practical Exam.

* Study the different types of vulnerability for hacking a website of web application :

A website vulnerability is a weakness or misconfiguration in a website or web application code that allows an attacker to gain some level of control of the site, and possibly the hosting server.

Types of Website vulnerability :

There are 5 common types of website vulnerabilities that are frequently exploited by attackers.

(1.) Sql Injection vulnerabilities (SQL) - This refers to areas in website code whereas direct user input is passed to a database. This allows the cybercriminal to access the website in a variety of ways, including:

- Injecting malicious / spams posts into a site.
- Stealing customer information.
- Bypassing authentication to gain full control of the website.

2.) Cross-site Scripting (XSS) - This occurs when attackers inject scripts through unsanitized user input or other fields on a website to execute code on the site. Browsers are

are unable to discern whether or not the script is intended to be part of the website, resulting in malicious actions, including.

⊙ Session ~~hijat~~ hijacking.

⊙ Spam content being distributed to ~~o~~ unsuspecting visitors.

⊙ Stealing session data.

(3.) Command Injection: Command injection vulnerabilities allow attackers to remotely pass and execute code on the website hosting server. Command injection attacks are particularly critical because they can allow bad actors ~~to~~ initiate the following:

⊙ Hijack an entire site.

⊙ Hijack an entire hosting server.

⊙ Utilize the hizacked server in botnet attacks.

(4.) File Inclusion: (LFI/RRI) - Remote file inclusion (RFI) attacks use the include functions in server-side web application languages like PHP to execute code from a remotely stored file. The inclusion can then be used to initiate the:

⊙ Deliver malicious payloads that can be used to include attack and phishing pages in a visitors browsers.

Ishula Kaluri
1022736 (2B)
Information security.

- Include malicious shell files on publicly avalable websites.
- Take control of a website adminpanel or host-server.

(5.) Cross-site Request Forgery (CSRF) – attacks are less common but can be quite jeopardous. CSRF attacks trick site users or administators to unknowingly perform malicious actions for the attacker. As a result, attackers may be able to take the following actions using valid user ~~poi~~ input:

- change order values and product prices.
- Transfer funds from one account to another.
- change user passwords to hijack accounts.