NAME = RACHANA -SHARMA

FATHER NAME = PAWAN KUMAR

UNIVERSITY ROLL No = 1022752

CLASS ROLL No = 42

COURSE = BSc. IT

SEM = 6th sem

PAPER NAME = ~~RACHANA~~ INFORMATION SECURITY & CYBER LAWS

PAPER CODE =

Ques 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. SQL injection is one of the most prevalent types of web application vulnerabilities

2. CROSS SITE SCRIPTING (XSS)

⇒ Cross-site scripting targets an application's users by injection code, usually a client-side script such as JavaScript, into a web application's output. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by Rhasma.

Signature

the attackes. XSS allows attackers to execute scripts in the victim's browsers which can hijack users sessions, deface websites or redirect the users to malicious sites.

3. BROKEN AUTHENTICATION & SESSION MANAGEMENT

⇒ Broken authentication & session management encompass several security issues, all of them having to do with maintaining the identity of a user. If authentication credentials and session identifiers are not protected at all times, an attacker can hijack an active session and assume the identity of a user.

4. INSECURE DIRECT OBJECT REFERENCES

⇒ Insecure direct object references is when a web application exposes a reference to an internal implementation objects. Internal implementation objects include files, database records, directories and database keys. when an application exposes a reference to one of these objects in a URL, hackers can manipulate it to gain access to a user's personal data.

Sharma
signature

## 5. SECURITY MISCONFIGURATION

⇒ Security misconfiguration encompasses several types of vulnerabilities all centered on a 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 servers, web servers, database servers 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)

⇒ CSRF is a malicious attack where a user is tricked into performing an action he or she didn't intend to do. A third-party website will send a request to a web application that a user is already authenticated against (eg. their bank) The attacker can then access functionality via the victims already authenticated browsers. Targets including web applications like social media, in browser email clients, online banking, web interfaces & network devices.

Rhasma
Signature

NAME = RACHANA - SHARMA

COURSE = BSC.IT (6th sem)

ROLL No = 1022752 (42)

## 7. INSUFFICIENT TRANSPORT LAYER PROTECTION

⇒ Deals with information exchange between the user (client) and the server (application). Applications frequently transmit sensitive information like authentication details, credit card information, and session tokens over a network.

Vulnerable objects:-

- Data sent over the network.

## 8. Unvalidated Redirects and forwards.

⇒ The web application uses few methods to redirect and forward users to other pages for an intended purpose. If there is no proper validation while redirecting to other pages, attackers can make use of this and can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Rhasmg
Signature