Name- Shivani
Rollno - 52 (1022762)

Subject - Information security

Q1 Ans

i) SQL injection Vulnerabilities → Sql injection vulnerabilities refer to areas in website code where direct user input is passed to database. Bad actors utilize these form to inject malicious code, sometimes called payloads into a website database. This allows the cybercriminal to access the website in a variety of ways including.

- Injecting malicious/ Spam posts into a site.
- Stealing customer information

ii) Cross site Scripting (XSS) - Cross site scripting targets an application's users by injecting 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 a the manner desired by the attacker. XSS allows attackers to execute

Shivani

Script in the victim's browser which can hijack (2) user sessions, deface web sites or redirect the user to malicious site

- Session hijacking
- Spam content being distributed to unsuspecting visitors.

3) Command injection - Command injection vulnerabilities allow attackers to remotely pass and execute code on the website's hosting server, This is done when user input that is passed to the server, such as header information is not properly validated allowing attackers to include shell commands with the user information.

- Hijack an entire site.
- Hijack an entire hosting server

4) Cross-site Request forgery (CSRF) - Cross site Request forgery is forged request came from the cross site

CSRF attack is an attack the occurs when a malicious website, email or program

Shinchi

Causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated. As a result attackers may be able to take to the following actions using valid user input

- Change order values and product prices
- Transfer funds one account to another

4) 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 server, database and platform.

Shifani