1. Study ------- application.

2) SQL Injection Vulnerabilities (SQLi).

- SQL injection vulnerabilities refer to areas in website code where direct user input is passed to a database. Bad actors utilize these forms to inject malicious code, sometimes called payloads, into a website's database. This allows the cybercriminal to access the website in a variety of ways, including,

- Injecting malicious/ Spam posts in a Site.
- Stealing customer information
- By passing authentication to gain full control of the website.

2. Cross - Site Scripting (XSS).

- It occurs when attackers inject scripts through unsanitized user input or other fields on a website to execute code on the Site. It is used to target website visitors, rather than the website itself.

3. Command Injection.

- Command injection vulnerabilities allow attackers to remotely pass & 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.

4. File Inclusion (LFI/RFI).

- Remote file inclusion attacks use the include ~~information~~ functions in Server-Side web application language like Php to execute code from a remotely Stored file. Attackers host malicious files and then take advantage of improperly Sanitized user input to inject an include function into the victims' Site Php code. Following can be initiated using this:

- Deliver malicious payloads that can be used to include attack & phising.
- Include malicious Shell files on publicaly available websites.

5. Cross-Site Request Forgery (CSRF).

- It's attacks are less common, but can be quite jeopardous. CSRF attacks trick Site users or administrators to unknowingly perform malicious actions for the attacker. As a result, attackers may be able to take the following actions:

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

- All these actions using valid user input.