

Ans 1)

## Types of website Vulnerabilities.

### SQL injection Vulnerabilities

SQL injection Vulnerabilities refer to areas in website code where direct user input is passed to a database.

- injecting malicious/spam posts into a site
- stealing customer information
- Bypassing authentication to gain full control of website.

### Cross-site Scripting (XSS)

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

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

### 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.

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

Bumatt.



## Cross-Site Request Forgery (CSRF)

Cross site request forgery are less common, but can be quite jeopardous. CSRF attacks trick site users or administrators to unknowingly perform malicious actions for the attacker.

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

*[Signature]*