XSS – Cross Site Scripting

Hcon Delhi

Alok Saini

What is Xss?

- XSS Stands for Cross Site Scripting.
- XSS is a web application vulnerability.
- It exists because of improper input validation by the web application developer.

- In Xss the malicious user inject the malicious code into the vulnerable page.

- Its a vulnerability that can be in client side or server side of Application code.

- Irrespective of the vulnerable code either client side or server side, injected code always executes at client side.

Types of Xss

- Persistent XSS

- Non- Persistent XSS

Persistent Xss

- In a Persistent Xss vulnerability the injected code is stored in attacked website code.

- The Injected Code will execute everytime the vulnerable page is opened.

Non-Persistent Xss

- In Non Persistent Xss the injected code is not stored on the vulnerable page.

- Its Executes only when vulnerable page is provided injected code at execution time.

Risk Factor

- Xss Vulnerability is the most found in the wild, because of highly low risk.

- Xss is execute on client side so no real deface, or harm to web applicaton is possible.

Uses

- Even with no access to server side code and content, xss can be higly dangerous.
- Persistent Xss can be used to stole user credientials and cookies.
- Non Persistent Xss is used for relative phishing purposes.