**DAY 37**

**Cross Site Scripting (XSS):**

🡪Basics of JS

The websites which take user input and create a dynamic page (search page, comments, FAQ, review, stories, user registration, profile page) with the user given input and doesn’t validate the input both on server-side and client side leads to XSS.

Where we can inject javascript code which can make the website work according to our JS code.

In the attackers point of view it can be a malicious JS which can :

1. Steal cookies

2. Hijack a session

3. Make the website redirect to malicious websites

4. Run a keystroke logger where the regular users credentials can be stolen.

3 main types of XSS vulnerability:

1. Reflected XSS

2. Stored XSS/persistent XSS

3. DOM (Document Object Model) based XSS

DOMs are executed by the browsers and the servers ignore DOM’s value sometimes

XSS writeups:

Microsoft writeups:

🡪pethuraj.com/blog/Microsoft-bug-bounty

Google images stored XSS:

🡪sites.google.com/site/bugbountybughunter/home

Facebook XSS