Offensive Approach to Hunt Bugs

Cross Site Scripting

Background Concept about XSS

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

- An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

Impact of XSS

- Cookie theft
- Keylogging
- Phishing
- URL Redirection

Types of XSS

- Reflected XSS
- Stored XSS
- DOM-based XSS

How to Hunt for XSS

- Find a Input Parameter , Give any input There . If your input reflect or stored any where there may be XSS
- Try to execute any Javascript code there , if you succeed to execute any javascript there then there is a xss
- Exploitation of XSS