Offensive Approach to Hunt Bugs

SSRF

Background Concept about SSRF

- Server Side Request Forgery (SSRF) refers to an attack where in an attacker is able to send a crafted request from a vulnerable web application.

Impact of SSRF

- Abuse trust
- Bypass ip whitelisting
- Bypass host based authentication
- Read resource
- Scan the internal network

How to Hunt for SSRF

- You have to find any parameter that may have some kind of external interaction or they can interact to external domain

  Example :

- Any.com/index/php?uri=http://external.com

Lets Hunt SSRF on these websites

- testphp.vulnweb.com
- Www.japanpost.jp

Possible Related parameter to Hunt for SSRF

dest redirect uri path continue url window next data reference site html val validate domain callback return page view dir show	file document folder root path pg style pdf template php_path doc feed host port to out navigation open result

Exploitation of SSRF

- Read file from server
- Scan the Internal Network
- SSRF with RFI