Task 4.3D

Name of Student

Institutional Affiliation

**Introduction**

This lab practical involves testing an SQL injection using an SQL Virtual Machine obtained from Vulnhub (Vulnhub, 2020). The vulnerability testing in this case is done from a separate machine but present on the same network, that is, Kali Linux OS. The virtual machines run on Oracle VM VirtualBox. In this practical, I will be testing if the SQL database can be hacked into by using SQL injection.

**Steps and Procedures**

On running the machine, the first step is to determine its IP Address. This is done using the if config command as shown in Figure 1. The IP address is given as 192.168.1.6

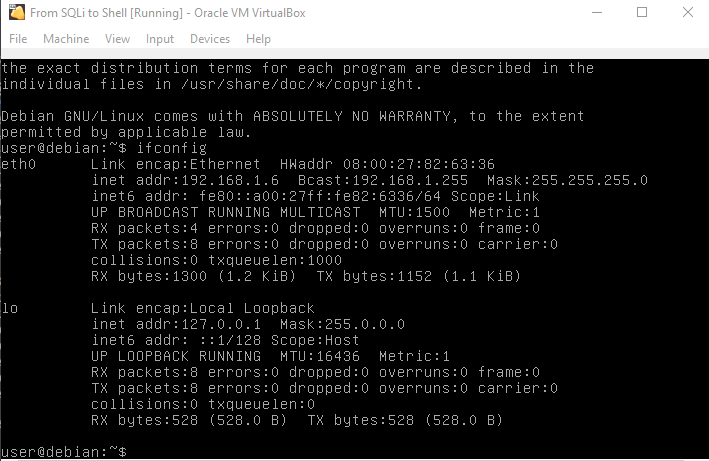


Figure 1: SQL Virtual Machine IP Address

The second step is to start up the Kali Linux machine and identify its IP Address. The IP address is then identified as 192.168.1.8. The next step is to determine if the two machines can communicate with each other. A ping command is used to ping the other machine’s IP address which returns a successful connection as shown.

Nmap is one of the best network mappers and vulnerability detectors in a network. The -sV is used for detecting the services present on the network, the -A parameter is used to perform service and OS detection with the -T5 helping in faster execution, and the -O command is used in scanning the operating system of the host. The results in Figure 3 show that the machine has an open port 80 which is mainly used in HTTP protocols.

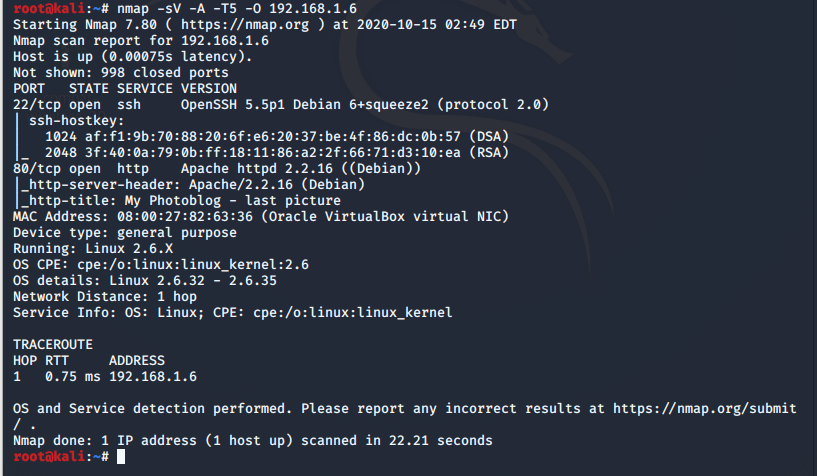


Figure 3: Nmap Scan

The next step was to identify what the web address had. On opening the address had, on a web browser, the website hosted on the machine was visible as shown in Figure 4.

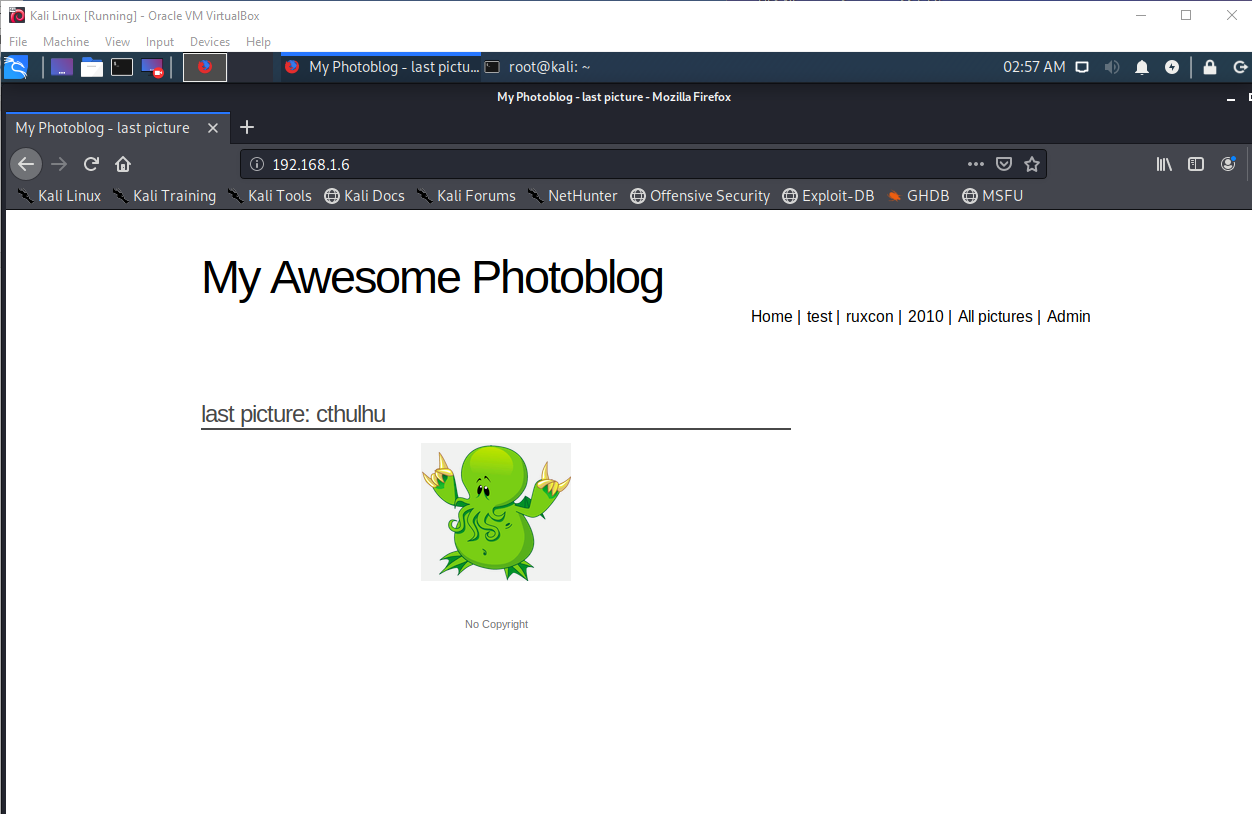


Figure 4: Web Homepage

The website contains various users and pictures present. It also has an admin panel which requires a user login and password. In order to exploit the vulnerability, I used sqlmap since it is one of the best penetration testing tolls available regarding databases and sql injection. The first step with sqlmap was to identify the databases present on the server by using the address obtained from the website. The –dbs command is used to list these databases as shown in Figure 5.

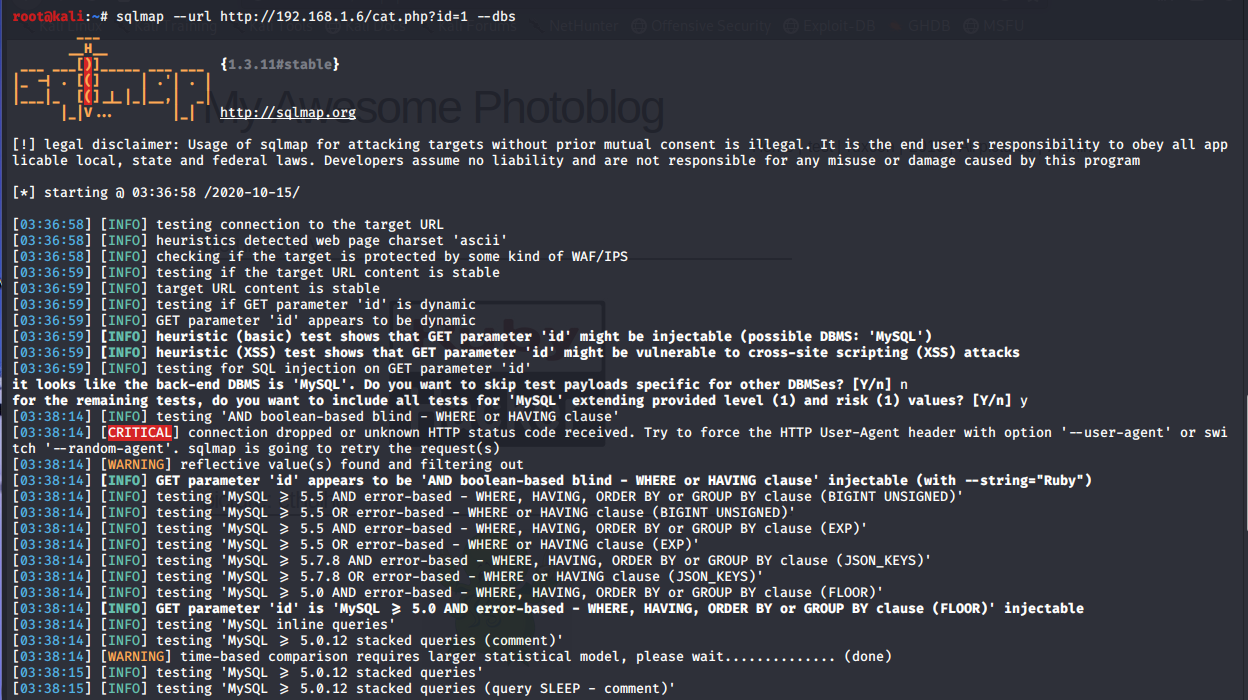


Figure 5: Sqlmap databases

As viewed in Figure 6, there are two databases present: information\_schema and photoblog database.

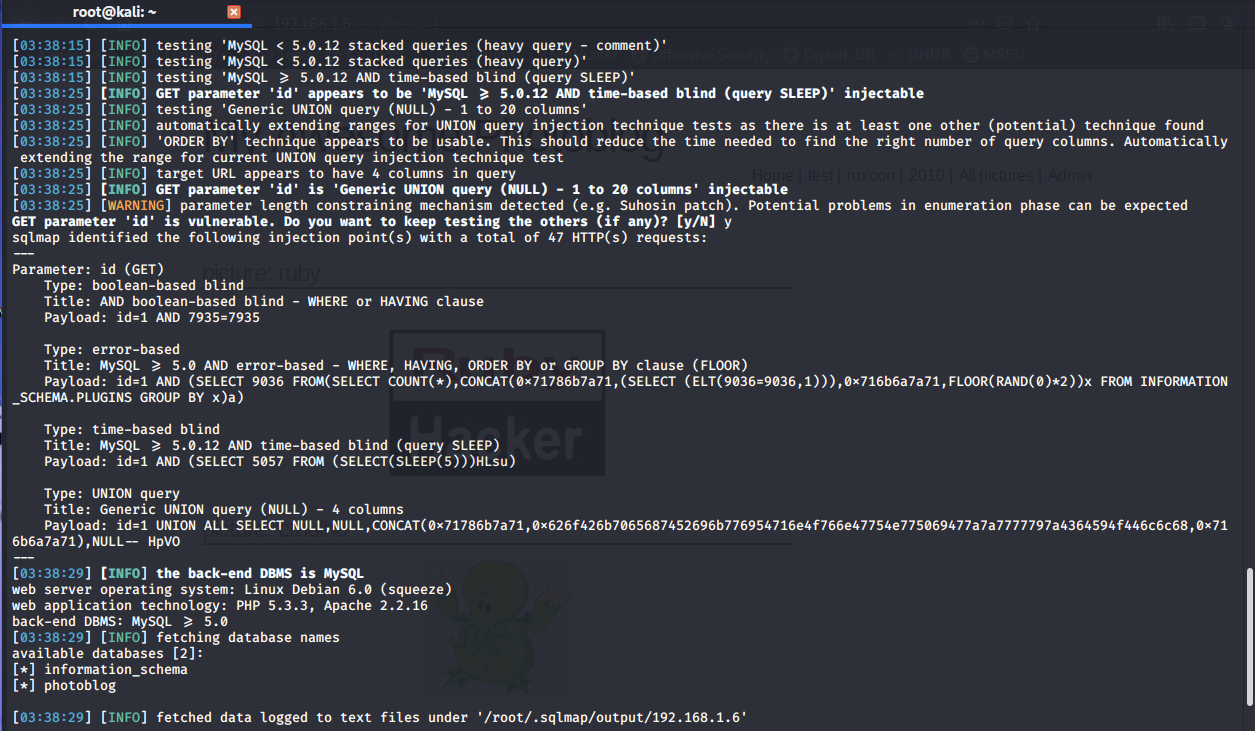


Figure 6: Sqlmap databases (cont.)

The information\_schema contains the metadata of the database objects and datatypes so the main focus is on the photoblog database. The first command after identifying the database, is to determine the tables which are present. This is done using the sqlmap –tables command as shown in Figure 7. This identifies three tables: categories, pictures, and users.

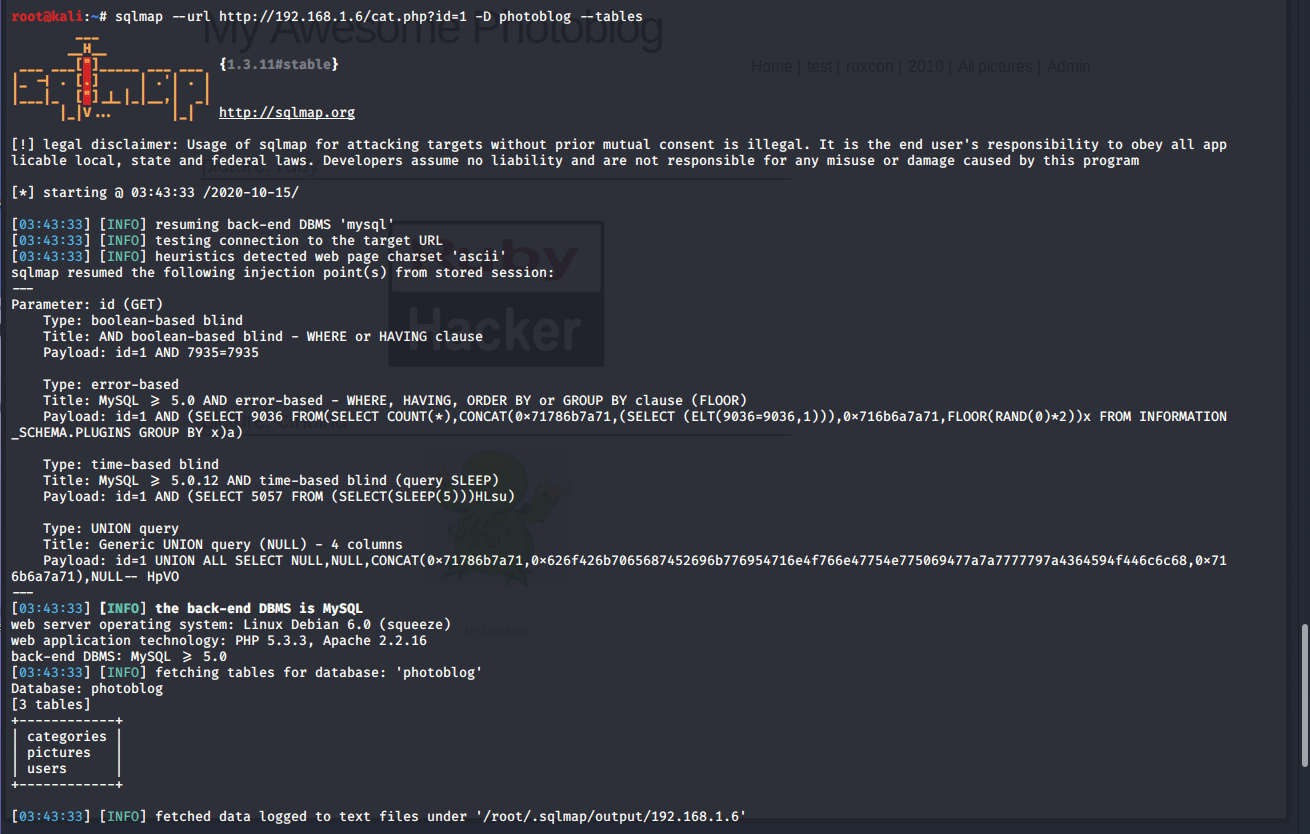


Figure 7: Sqlmap tables

The next step is to identify the columns present in the users table. This is because the users table most likely contains details of the user and the password. This is done using the sqlmap –columns command as shown in Figures 8 and 9.

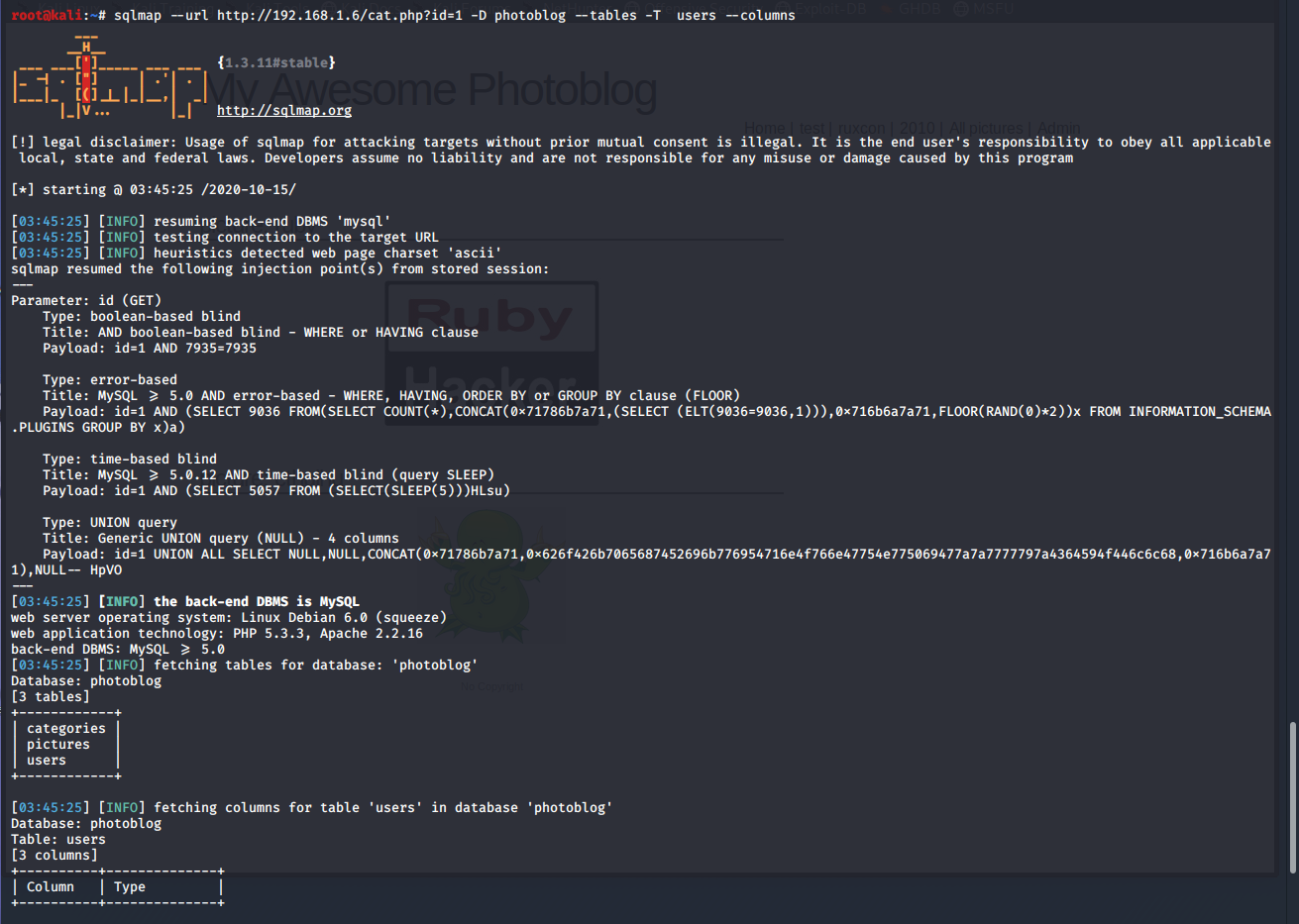


Figure 8: Sqlmap columns

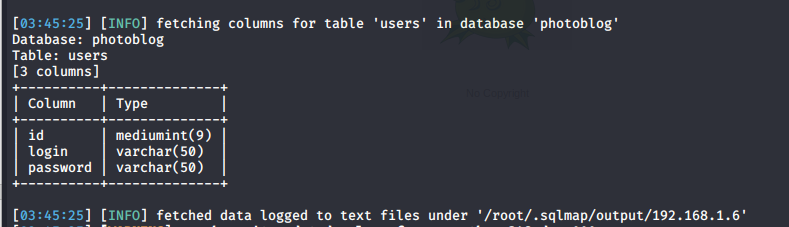


Figure 9: Sqlmap columns (cont.)

After identifying the column names of the table which are: id, login, and password, it is possible to perform an SQL injection. By adding an SQL code below to the browser, it is possible to obtain the username and login details. This shows a successful SQL injection. However, the password is in MD5 hash format as shown in Figure 10.

UNION SELECT 1,concat(login,':',password),3,4 FROM users;

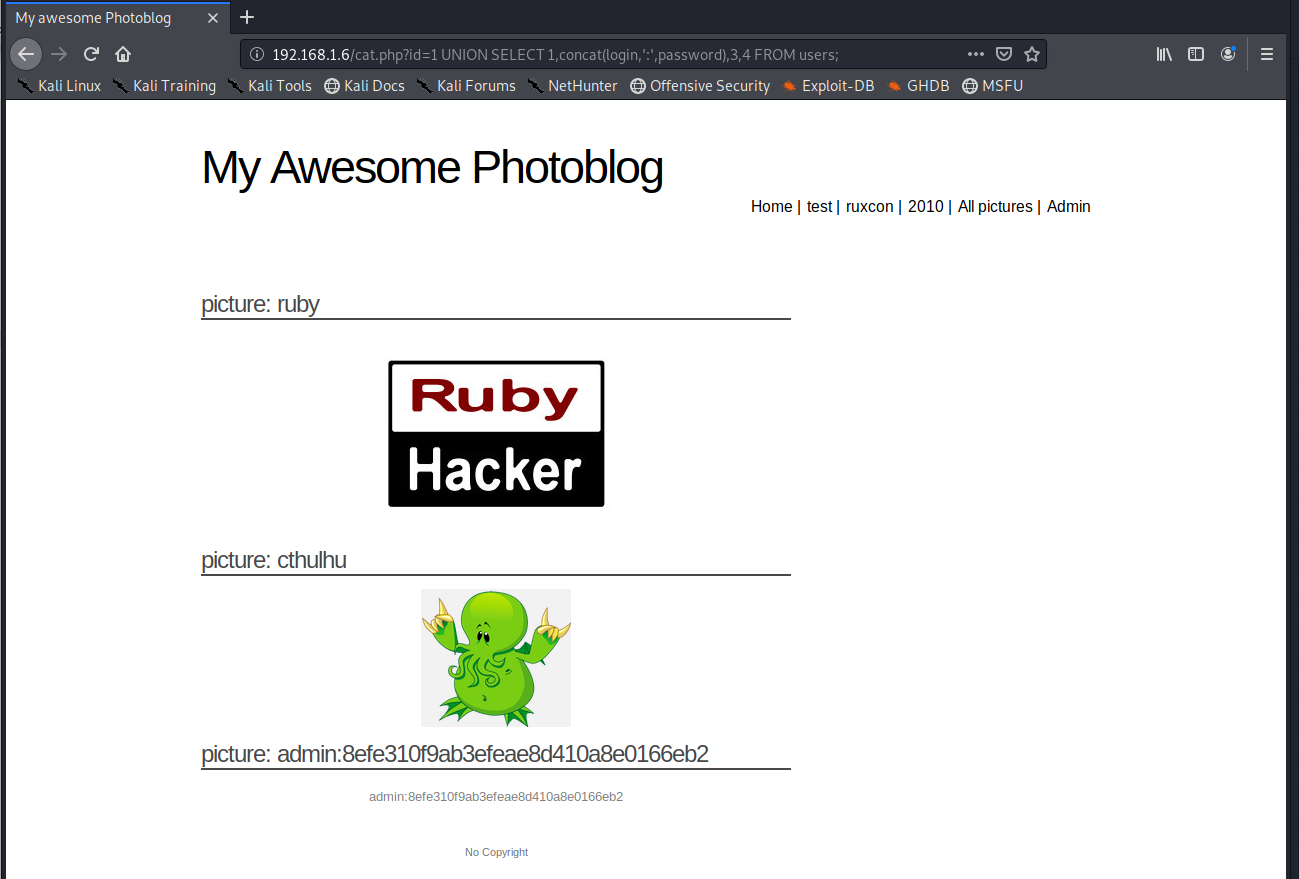


Figure 10: SQL Injection Attack

An MD5 decryptor can then be used to determine the password as shown in Figure 11 which is given as P4ssw0rd

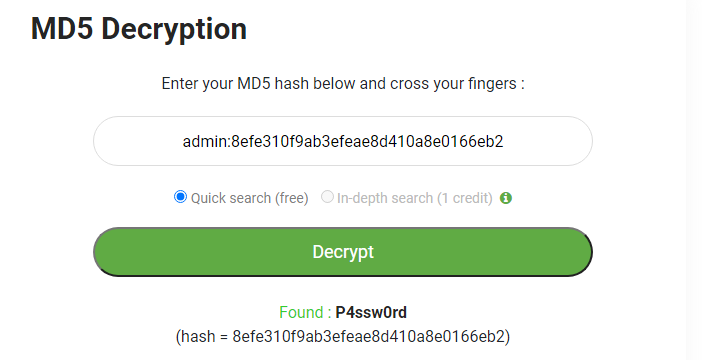


Figure 11: MD5 decryption

**Alternatively:**

After identifying the columns: id, login, and password; the data requires to be obtained by using a –dump command as shown in Figure 12. When executing the command, sqlmap requires you to specify if you require to have a dictionary-based attack. This attack scans for the password by using a dictionary file. I chose the default dictionary file which comes pre-installed in order to determine if I can find the password and user. As shown in Figure 13, the login and password fields are obtained as: admin and P4ssw0rd respectively.

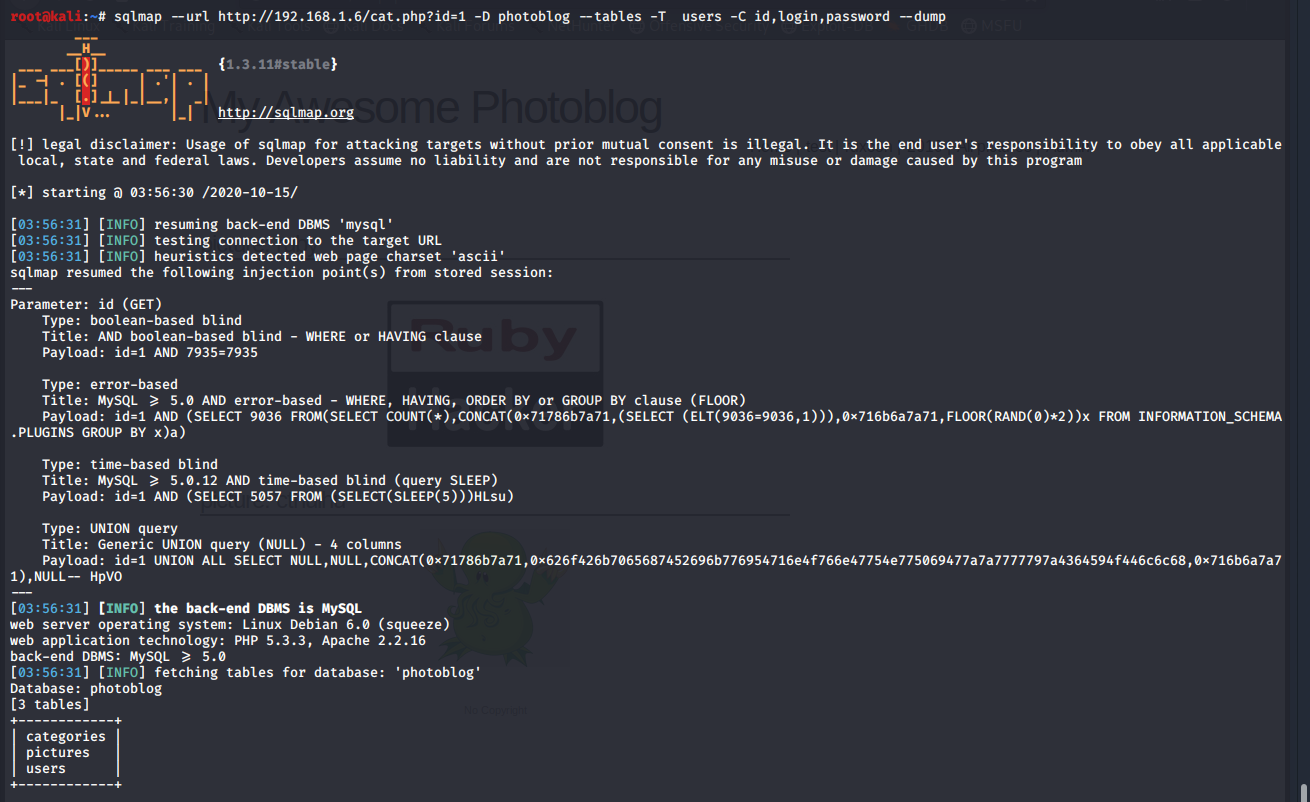


Figure 12: Sqlmap SQL Injection



Figure 13: Sqlmap SQL Injection Success

The admin and password details are used to login to the system and a successful login is possible with options to do multiple admin functions such as deleting users and uploading pictures as shown in Figure 14.

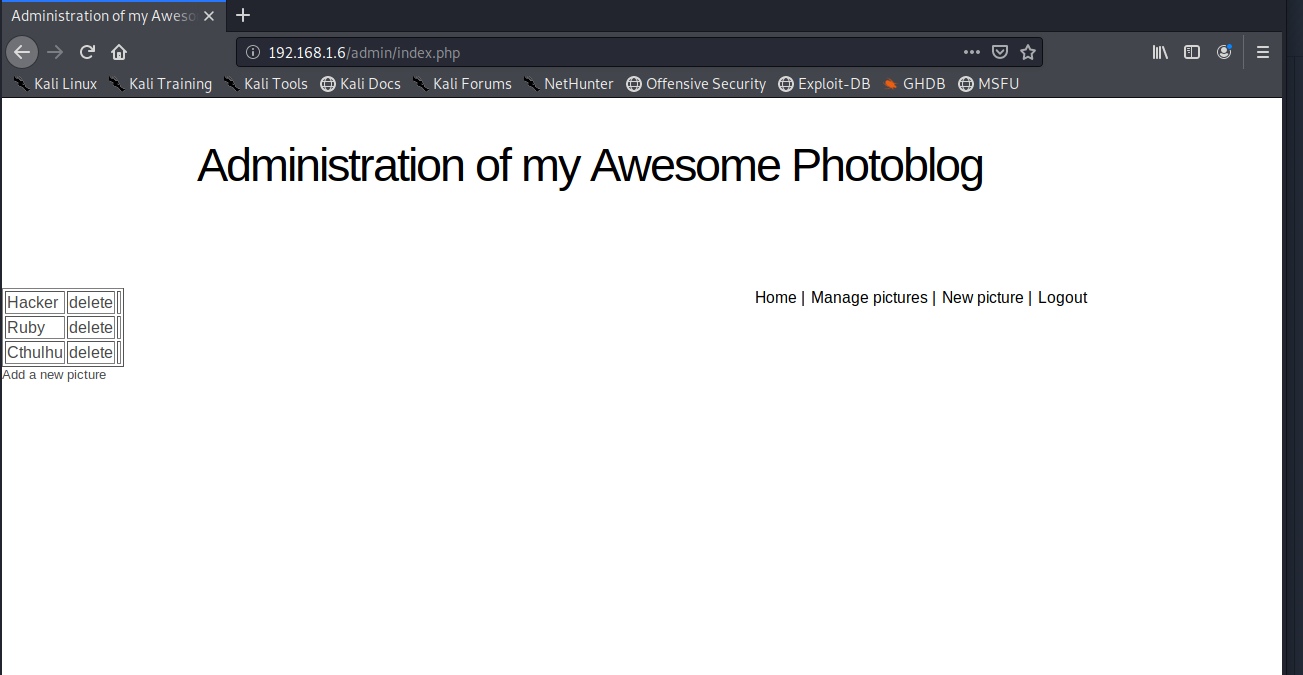


Figure 14: Successful Login