

### [Sri Lanka Institute of Information Technology](http://www.sliit.lk/)

Pentester Lab: From SQL to Shell II

Information Security Project

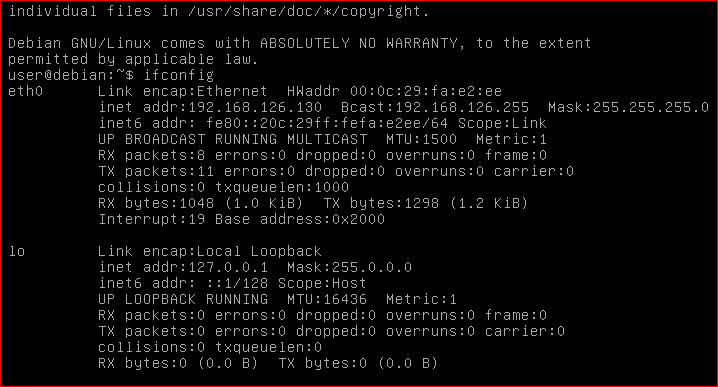
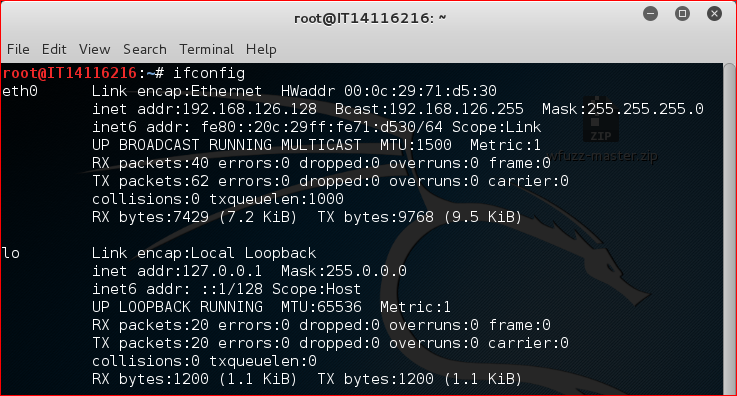
L.R.M.O Lankarathne

IT14116216

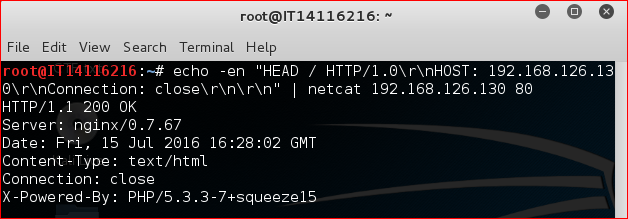
* Check Whether both IP address are in same range

IP Address of Attacker

IP Address of Victim



* inspecting HTTP Headers



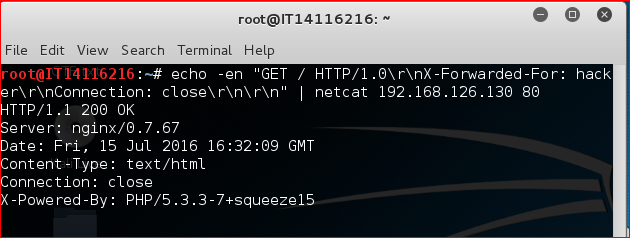
Lots of information can retrieved by connecting to the web server using telnet.

Using HEAD will save you from getting all the page's content. Using Connection: close tells the server to close the connection after processing our request. This will ensure that the command returns immediately.

* Detection and Exploitation of SQL Injection

We can easily send requests using the command line. However, we can see that sending the payload

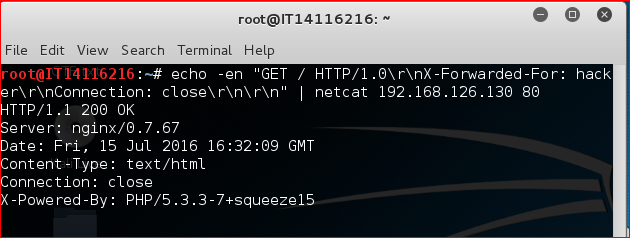
Hacker



X-Forwarded-For. X-Forwarded-For is traditionally used to get the IP address of the client.  X-Forwarded-For is mostly used when the application is behind a reverse-proxy. X-Forwarded-For is only set when the application run behind a reverse-proxy, the code will correctly work in most cases. However, this code assumes that an attacker cannot forge this header.

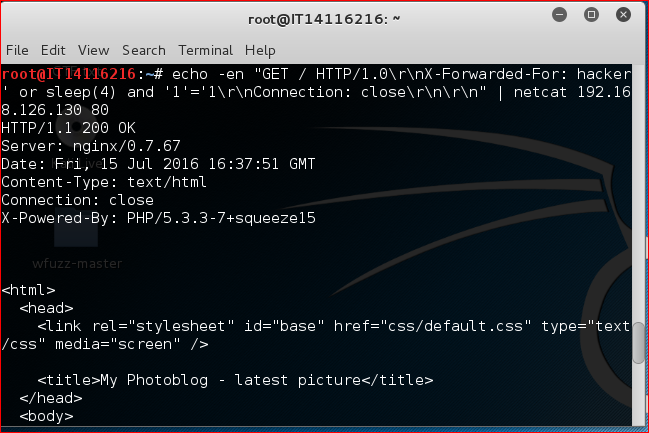
We can easily send requests using the command line. However, we can see that sending the payload

Hacker’



It’s give the same result and there is no easy way to see that this parameter is injectable.

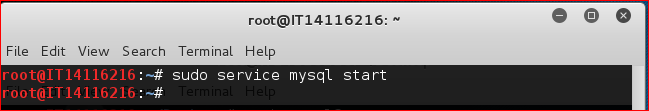
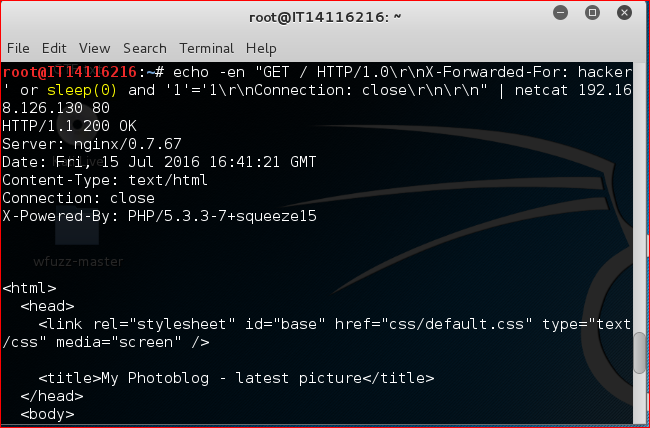
Using time-based detection to find the vulnerability by checking the time difference. We can see that this payload:



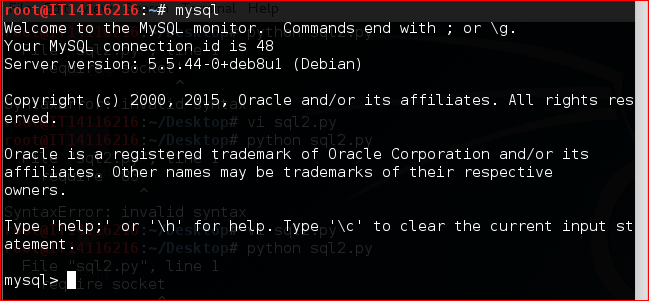
In this case results will give after 4 seconds, because we use sleep (4)

* **Manual Exploitation**
* Exploitation of Blind SQL Injection

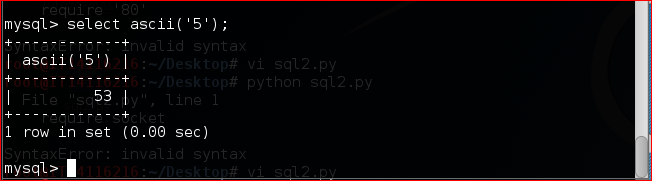
First start the mysql server using sudo service mysql start



Then run the mysql server using mysql command

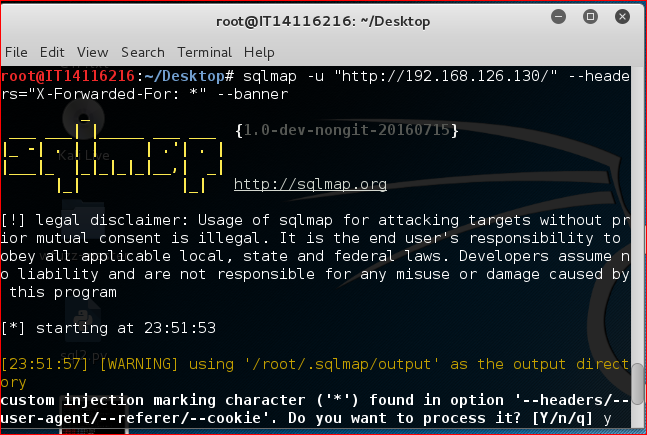


Get the ascii value of 5,

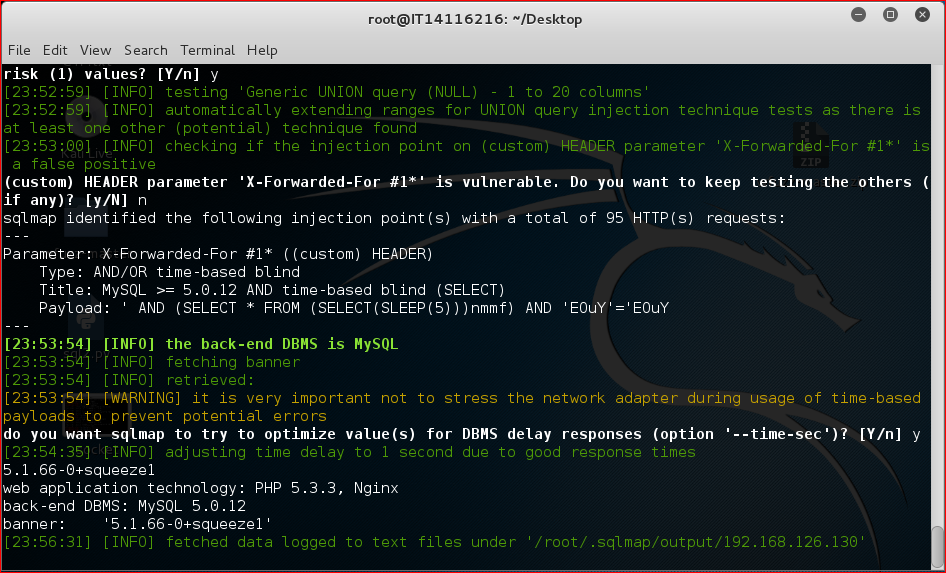


* **Exploitation with SQLmap**

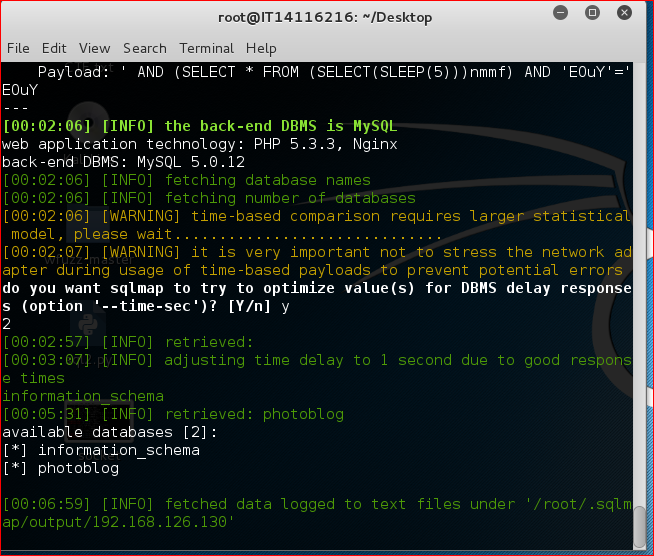
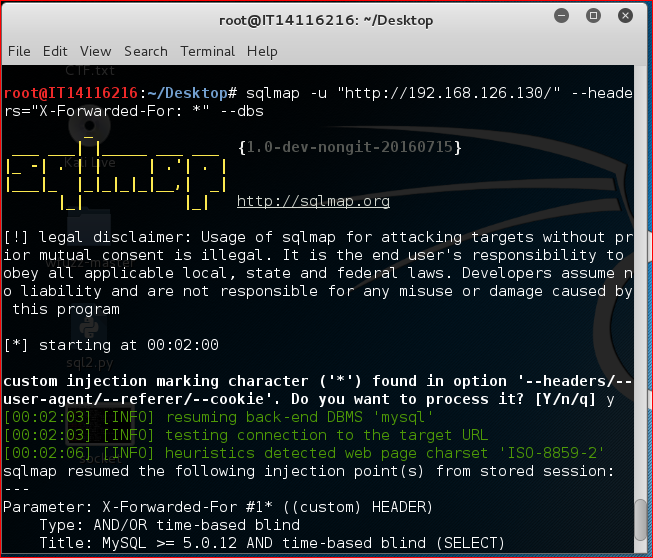
Using sqlmap we can exploit injection,



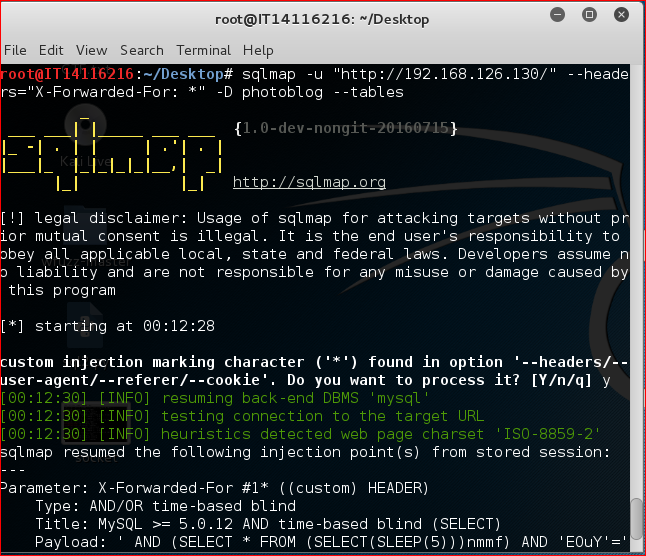
After testing different SQL injection methods, SQLMap returns above the banner:

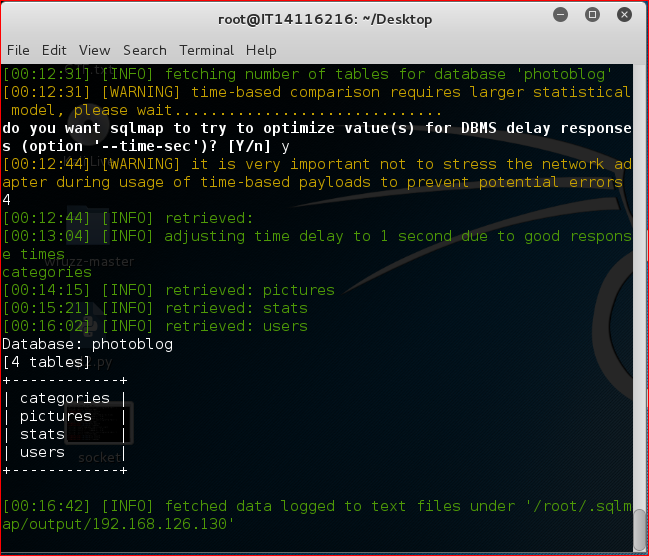


--dbs retrieve the list of databases

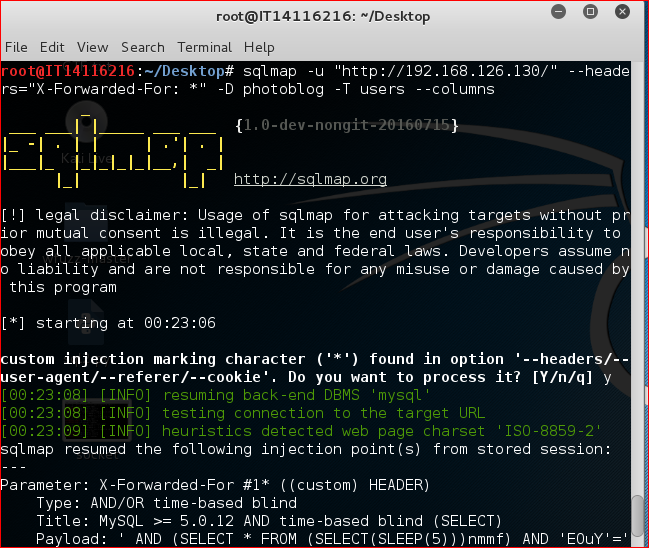
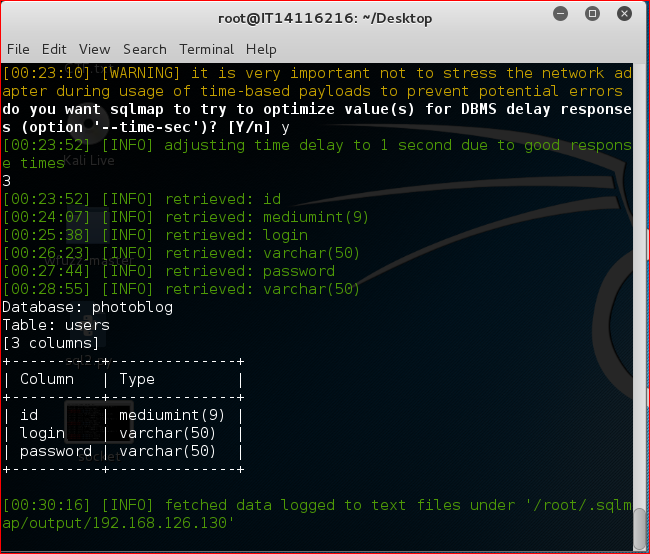


-D photoblog --tables to get the list of tables

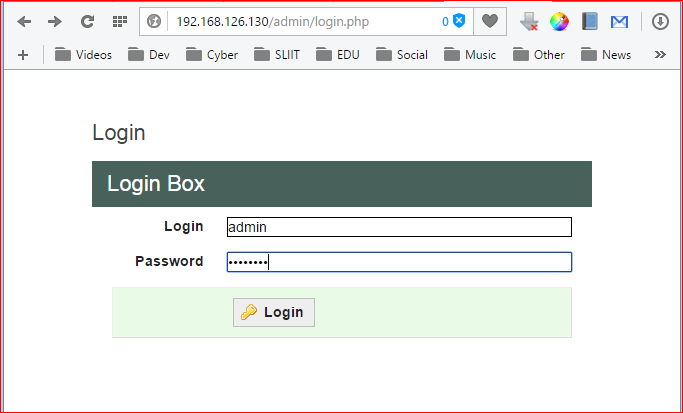
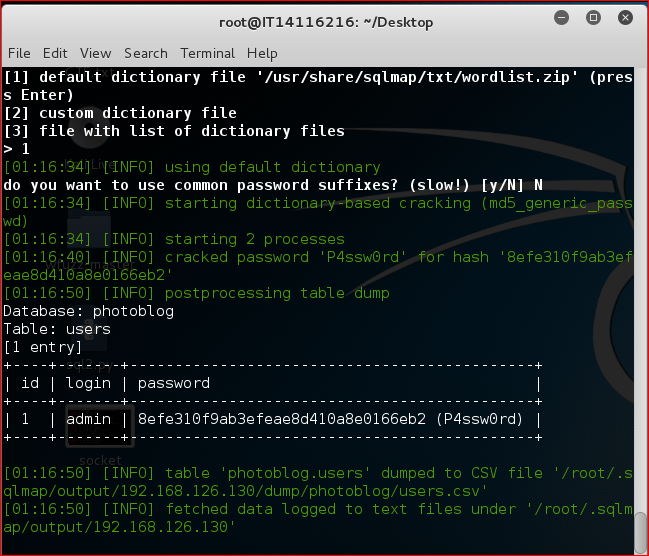
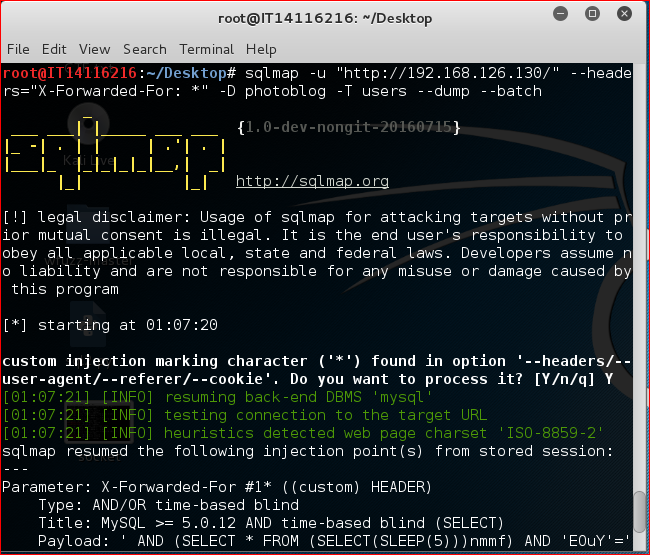




-D photoblog -T users --columns for the list of columns:



Dump the table users by using the following command:



# **Access to the administration pages and code execution**

