

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

Pentester Lab: From SQL to Shell

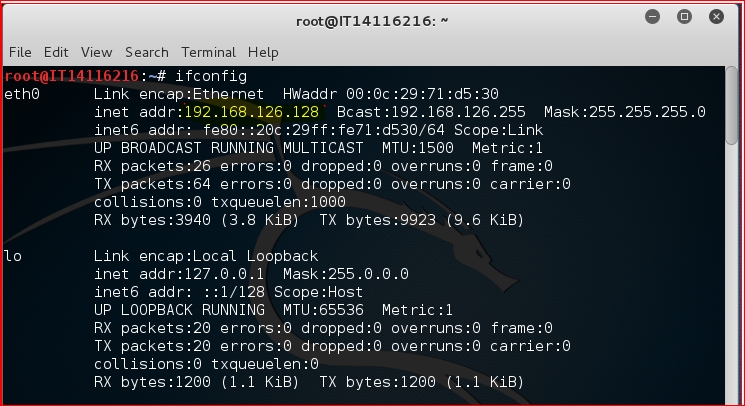
Information Security Project

L.R.M.O Lankarathne

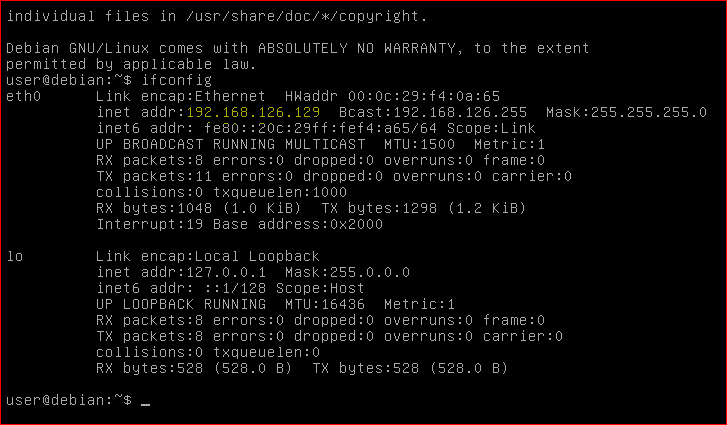
IT14116216

* Check Whether both IP address are in same range

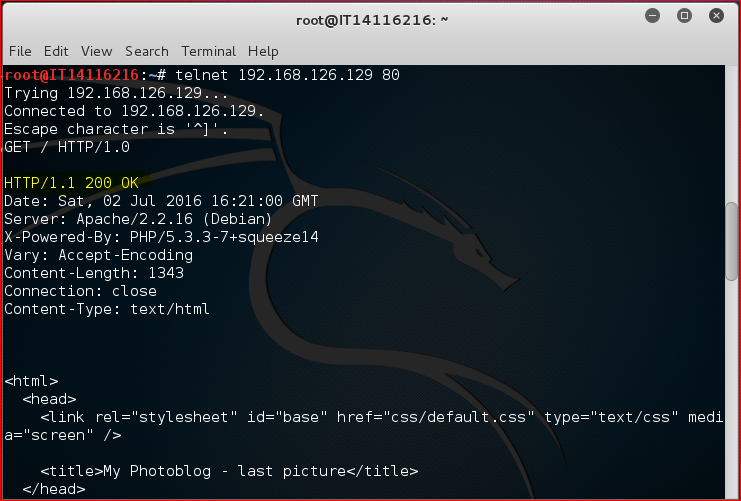
IP Address of Attacker



IP Address of Victim

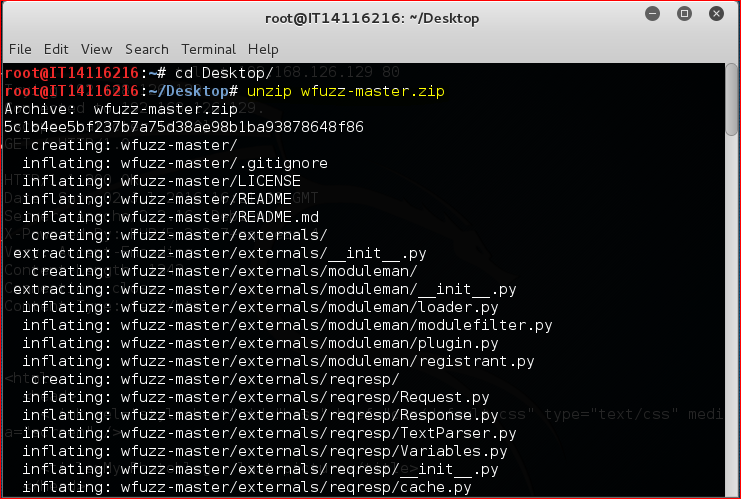


* Inspecting HTTP Headers



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

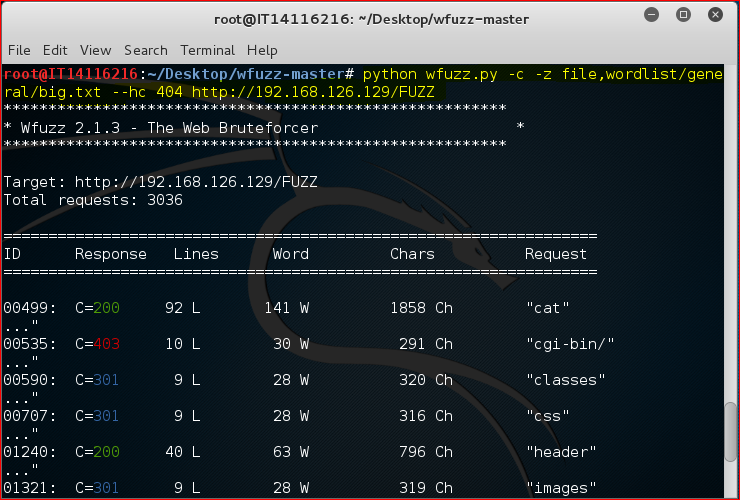
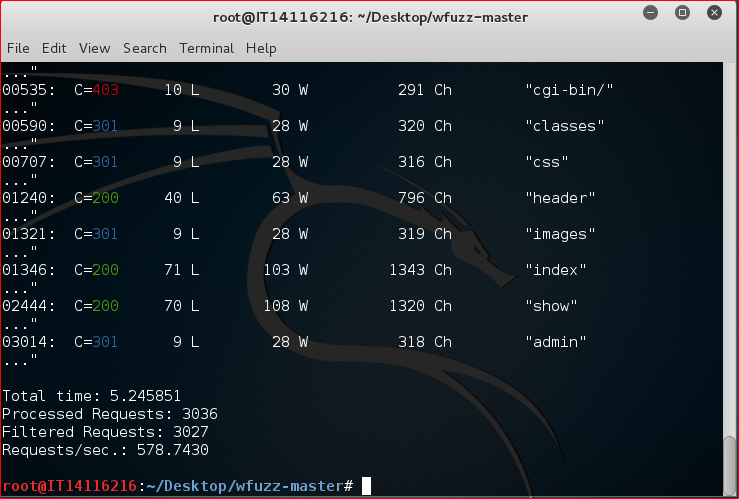
* Inspecting HTTP Headers



First download the zip file and unzip using *Unzip* command in kali

The tool wfuzz used to detect directories and web pages on server using brute force

In this command



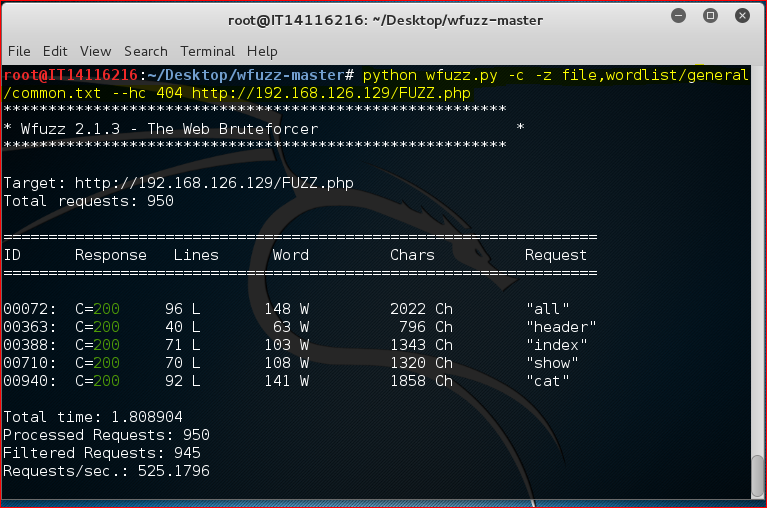
Then we doing brute force attack according to the following screen shot

* *-c*  use to output returns with colors
* *-z file,worldlist/general/big.txt* tells wfuzz to use the file *worldlist/general/big.txt* as a dictionary to brute force.
* --hc 404 tells wfuzz to ignore the response if the response code is 404.
* <http://192.168.126.129/FUZZ> tells wfuzz to replace the word FUZZ in the URL by each value found in the dictionary.

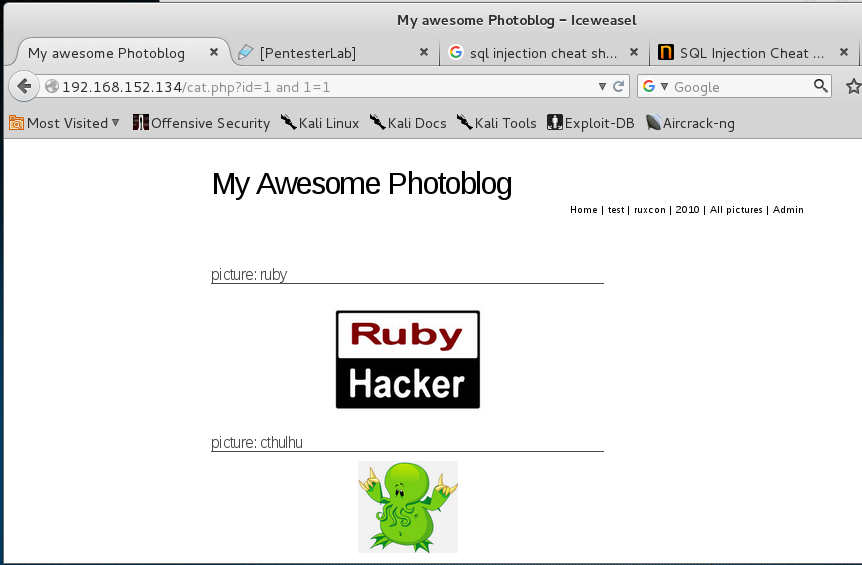
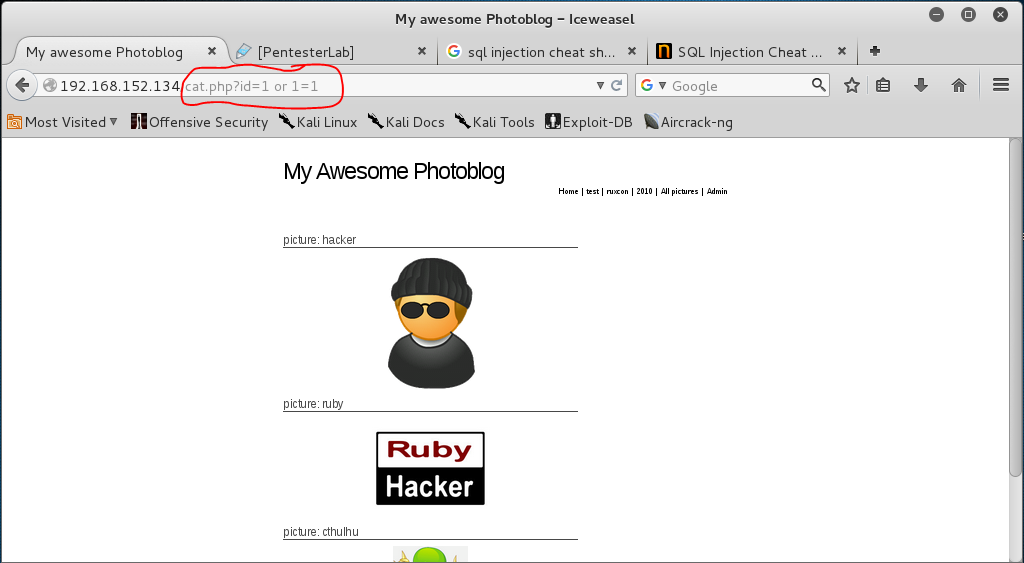


Detection Based on Integers

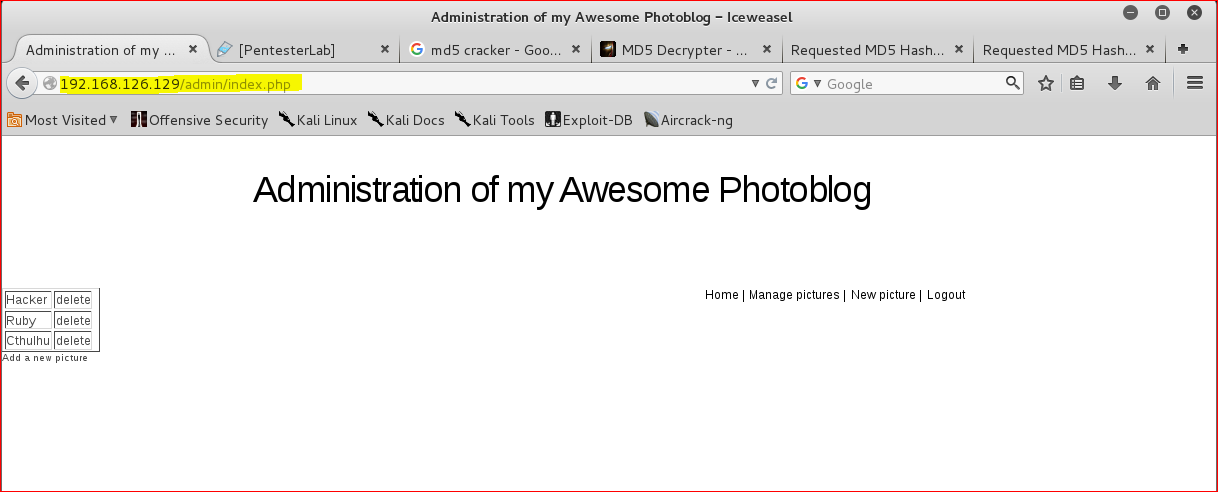
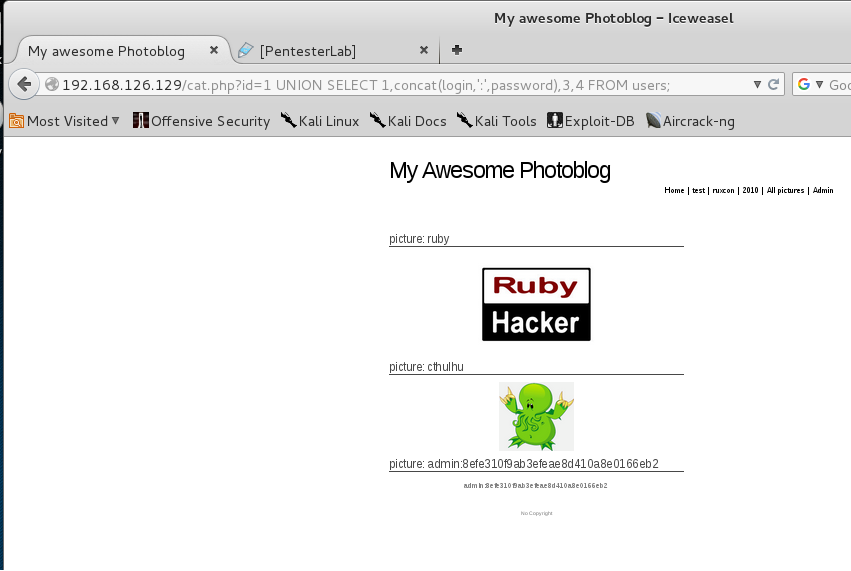
* Detection and Exploitation of SQL Injection



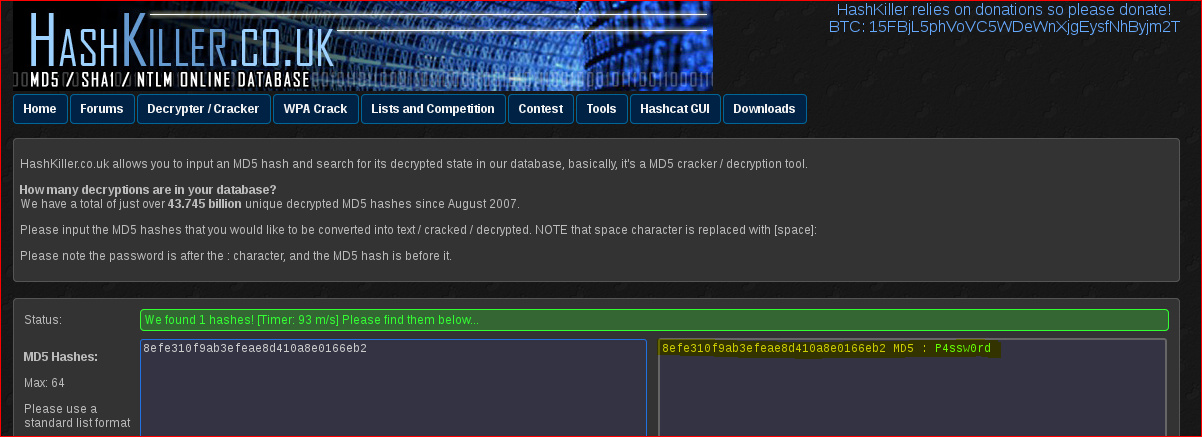
FUZZ can detect php script on the server



Detection Based on Strings



Access the administration pages



Cracking the Password

* Access to the Administration pages and code execution