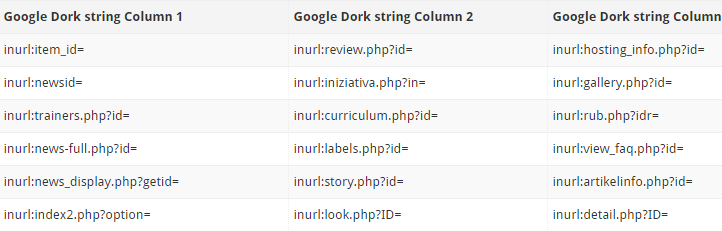
Aim: To Study SQL INJECTION ATTACK using SQLMAP (kali linux)

**STEPS:-**

**Step 1:- Finding a Vulnerable Website** :-

**Step 1.a**: Google Dorks strings to find Vulnerable SQLMAP SQL injectable website

Use the Below String and Search in Google



**Step 1.b**: Initial check to confirm if website is vulnerable to SQLMAP SQL Injection

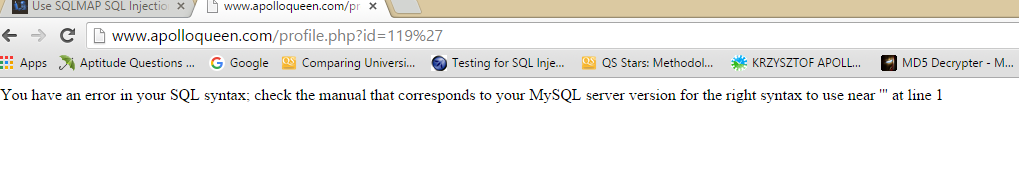
Let’s say you searched using this string **inurl:profile.php?id=** and one of the search result shows a website like this:

<http://www.apolloqueen.com/profile.php?id=119>

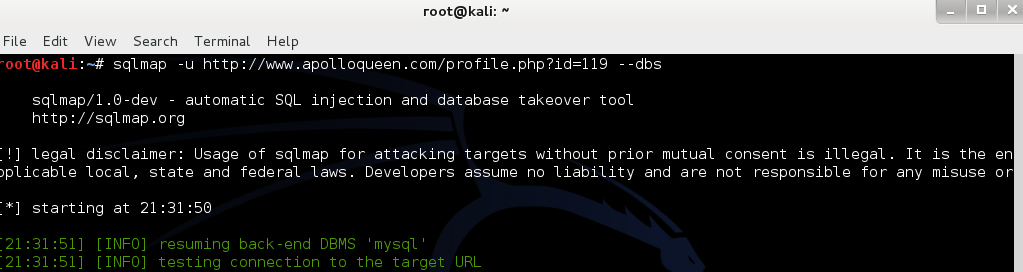
Just add a single quotation mark **’** at the end of the URL.

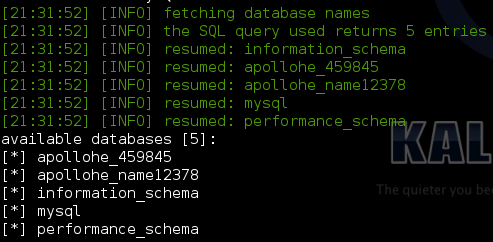
<http://www.apolloqueen.com/profile.php?id=119>’

If the page returns an SQL error, the page is vulnerable to SQLMAP SQL Injection

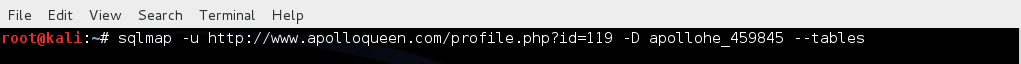


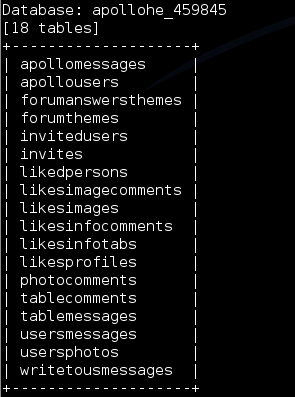
**Step 2:- List DBMS databases using SQLMAP SQL Injection**

****

****

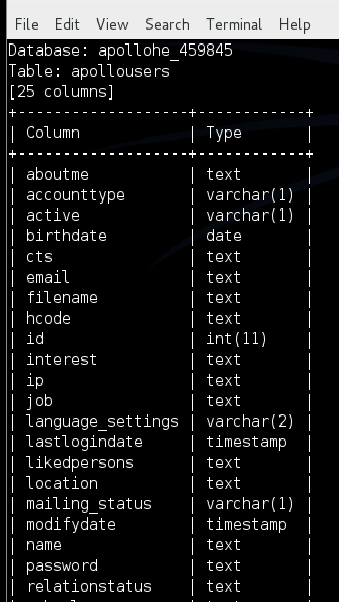
**Step 3: List tables of target database using SQLMAP SQL Injection:-**

****

****

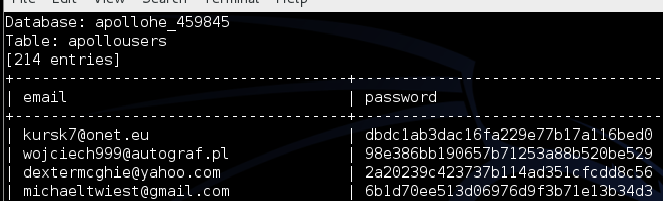
**Step 4: List columns on target table of selected database :-**

**C:\Users\user\Pictures\Screenshots\Screenshot from 2015-10-19 21_37_20.png**

****

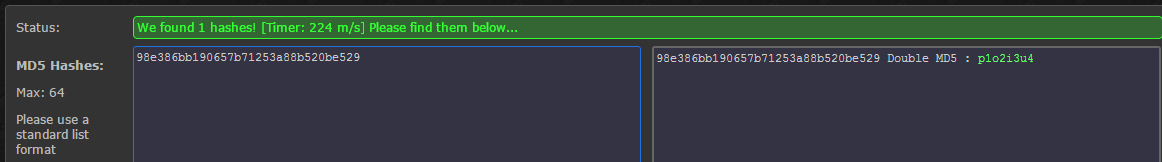
**Step 5: List usernames and Password from target columns of target table of selected database:-**

**C:\Users\user\Pictures\Screenshots\Screenshot from 2015-10-19 21_38_51.png**

****

**Step 6: Decrypting hash:-**

Decrypting the hash code using Online Decrypter at <http://www.hashkiller.co.uk/>



**Hence Using SQL Injection We can get Username/Email-id & Password of any SQL vulnerable Site Now we can Easily access any Account Or even Destroy them.**