

Forum:[Hack Forums](#)

Thread: [Find columns name with SQL Injection Help](#)

SecureHatz - November 10, 2019, 12:18 am

Hello everyone.

I find tables name when i using manuel sql injection.

[http://xxx.xx/?id=10171%27and+0+union+select+table_name,2,3,4,5,6,7,8,9,10,11 - Pastebin.com](http://xxx.xx/?id=10171%27and+0+union+select+table_name,2,3,4,5,6,7,8,9,10,11-Pastebin.com)

I've come this far. Table name writes on the screen. But I'm having trouble finding the column names.

When I trying to :

[http://xxx.xx/?id=10171%27and+0+union+select+column_name,2,3,4,5,6,7,8,9,10,11 - Pastebin.com](http://xxx.xx/?id=10171%27and+0+union+select+column_name,2,3,4,5,6,7,8,9,10,11-Pastebin.com)

You have an error in your SQL syntax..

How I can find columns_name ? Anyone can help me?

Thanks

Error22 - November 15, 2019, 8:24 am

drop real site so we check it

powerkami - November 15, 2019, 7:18 pm

did you try sqlmap ,you can get

SecureHatz - November 19, 2019, 11:30 pm

(Nov 15, 2019 09:24 AM)Error22 Wrote: [\[CITE\]](#) drop real site so we check itI sent you pm bro

(Nov 15, 2019 08:18 PM)powerkami Wrote: [\[CITE\]](#) did you try sqlmap ,you can get
I tried but did not

ajkaro_lover - November 21, 2019, 3:29 pm

Poor advice for all. Think through the problem, like the greats used to.

Its clear from your error that you are asking for something that it cannot provide.

Code ... select column_name,2,3,4,5,6,7,8,9,10,11,12 from information_schema.columns where table_schema not like information_schema and table_name='tablenamehere'

...

cleaned up equals

Code SELECT column_name FROM information_schema.columns WHERE table_schema NOT LIKE information_schema AND table_name = 'tablenamehere'

Looking at this statement, we are asking the database to exclude any tables that have 'information_schema' as their table schema and only show the columns for the table 'tablenamehere'.

The issue is that the statement is overkill. Asking the server to only show columns with table_name 'tablenamehere' would effectively complete the job and will not error.

Reference regarding Information_schema - dev.mysql.com/doc/refman/5.7/en/columns-table.html

Top tip - Break down each statement and understand specifically what you are asking for. Do not be scared to try out commands here (sqlfiddle.com/) and read the specs (dev.mysql.com/doc/)

Good luck

SecureHatz - January 19, 2020, 1:45 am

(Nov 21, 2019 04:29 PM)ajkaro_lover Wrote: [\[CITE\]](#) Poor advice for all. Think through the problem, like the greats used to.

Its clear from your error that you are asking for something that it cannot provide.

Code ... select column_name,2,3,4,5,6,7,8,9,10,11,12 from information_schema.columns where table_schema not like information_schema and table_name='tablenamehere'

...
cleaned up equals

Code SELECT column_name FROM information_schema.columns WHERE table_schema NOT LIKE information_schema AND table_name = 'tablenamehere'

Looking at this statement, we are asking the database to exclude any tables that have 'information_schema' as their table schema and only show the columns for the table 'tablenamehere'.

The issue is that the statement is overkill. Asking the server to only show columns with table_name 'tablenamehere' would effectively complete the job and will not _error_.

Reference regarding Information_schema - dev.mysql.com/doc/refman/5.7/en/columns-table.html

Top tip - Break down each statement and understand specifically what you are asking for. Do not be scared to try out commands here (sqlfiddle.com/) and read the specs (dev.mysql.com/doc/)

Good luck

Can you give an example ? Thank you for interest bro. I try some commands but I get syntax error.

Error22 - January 29, 2020, 12:55 am

(Nov 20, 2019 12:30 AM)SecureHatz Wrote: [\[CITE\]](#) I sent you pm bro

I tried but did not
i didnt get ur pm dear drop site