

Forum:[Hack Forums](#)

Thread: [Extracting data from SQL database knowing tables and columns](#)

jackjohn - March 8, 2016, 9:56 am

well say theoretically that I have found a vulnerable website, found the number of columns, found the vulnerable column and finally found the names of both the tables and the columns...how the hell I extract data like passwords or anything else ? I mean what query should I use ? Please help

JaNuS18 - March 8, 2016, 2:56 pm

Using DIOS syntax (no limitation with output)

or using group_concat (possible output limitation as output is limited to 1024 characters).

See syntax :

<http://pastie.org/private/de9jfl89op1hdvskpjpf7a>

kolinn - March 9, 2016, 4:22 am

hello bro! where can i get more DIOS code?

Frosteh - March 9, 2016, 5:12 am

(Mar 9, 2016 05:22 AM)kolinn Wrote: [\[CITE\]](#) hello bro! where can i get more DIOS code?

I have a tutorial blog post which goes in depth regarding DIOS, specifically used for dumping the entire DB struct. But it's fairly easy to modify these queries to pull out the actual data.

<http://frostyhacks.blogspot.co.uk/2014/10/one-sqli-to-rule-them-all.html>

Anti0Day - March 9, 2016, 9:47 am

Maybe column is empty.....

Use SqlMap tool to try.

jackjohn - March 9, 2016, 9:48 am

thank you so much, I'll take a look to the DIOS tutorial

jackjohn - March 23, 2016, 11:12 am

Hi guys!!! Now say theoretically that I've been able to watch all the data in all the columns of all the tables...is it possible that there's not sensible data ?? I mean there's no trace of passwords or mails or telephone numbers ! In this case is the sql injection totally useless ??

JaNuS18 - March 23, 2016, 11:51 am

(Mar 23, 2016 11:12 AM)jackjohn Wrote: [\[CITE\]](#) Hi guys!!! Now say theoretically that I've been able to watch all the data in all the columns of all the tables...is it possible that there's not sensible data ?? I mean there's no trace of passwords or mails or telephone numbers ! In this case is the sql injection totally useless ??

Did you check all databases for passwords?

If passwords are not stored in database that doesn't mean SQLi is generally useless. SQLi can't give you something that isn't stored in database(s).

jackjohn - March 23, 2016, 1:38 pm

yes it is what I was trying to say :) I meant it is useless in this particular case isn't it ? so is it possible that passwords are not stored anywhere ?

Forum Developer - *March 23, 2016, 8:12 pm*

If you're using sqlmap hmu.

jackjohn - *March 24, 2016, 3:48 am*

No I'm doing it "manually"