

Forum:[Hack Forums](#)

Thread: [\[Janus\]SQLi challenge #10 \[hard\]](#)

JaNuS18 - March 8, 2015, 3:42 pm

Hi folks,

Here is my final challenge (#10 of #10 for M"SQLi circle members (open to others too)). ? Possible other challenges from me WILL NOT be part of Mensa SQLi circle competition any more.... I finished my obligation, waiting for challenges from other M"SQLi members... I expect your revenge ?

Credits for some parts of this challenge go again to ajkaro. Thanx man for all your help and inspiration ?

~ Tasks ~

- display version with your name
- display list of all tables in primary database, sorted descending by number of columns where column name starts with letter j or a or n or u or s
- at tables where such columns exist, graphically display number of them and display them in sorted list in descending order (see proof picture)

~ Site ~

aHR0cDovL3d3dy50cnVjb3JlcGlzYXRlcy5jb20vdHJhaW5lcnMucGhwP3BhZ2VfaWQ9MjU=
(Base64 decode it using online decoder like <https://www.base64decode.org/>)

~ Proof ~

[img]<http://img15.hostingpics.net/pics/111243challenge10.jpg>[/img]

~ Rules ~

- use DIOS. group_concat, order by, group by, html table commands may not be part of your syntax
- use pure SQL (no javascript or anything else)
- your injection should work without knowing anything about databases/tables/columns at that site
- your solution should be generic (it should work at different SQLi vulnerable sites (WAF excluded))

Post your syntax to <https://privnote.com> (it is automatically destroyed after reading) and send me link to PM

Let's SQL knowledge be with you ?

~ Solvers ~

-

Try also my other challenges for advanced injectors:

[janus #1](#)

[janus #2](#)

[janus #3](#)

[janus #4](#)

[janus #5](#)

[janus #6](#)

[janus #7](#)

[janus #8](#)

[janus #9](#)

rawaz karim - September 14, 2017, 4:06 pm

why repeated column look picture

JaNuS18 - September 16, 2017, 5:08 am

(Sep 14, 2017 04:06 PM)rawaz karim Wrote: [\[CITE\]](#) why repeated column look picture

You do something wrong. Local variable with last table name is probably NOT updated properly, so columns from first table are in the ouput...

rawaz karim - September 16, 2017, 9:58 am

(Sep 16, 2017 05:08 AM)JaNuS18 Wrote: [\[CITE\]](#) You do something wrong. Local variable with last table name is probably NOT updated properly, so columns from first table are in the ouput...

thx master janus for helping

JaNuS18 - September 16, 2017, 1:45 pm

(Sep 16, 2017 09:58 AM)rawaz karim Wrote: [\[CITE\]](#) thx master janus for helping

Thanks for doing monkey business behind my back. ??? You are disqualified from all my challenges PERMANENTLY

rawaz karim - September 16, 2017, 2:30 pm

(Sep 16, 2017 01:45 PM)JaNuS18 Wrote: [\[CITE\]](#) Thanks for doing monkey business behind my back. ??? You are disqualified from all my challenges PERMANENTLY

i am not solve your challenge any more and no post picture as on your challenge and show some respect and kick me