

Forum: [Hack Forums](#)

Thread: [\[Janus\] SQLi challenge #20](#)

JaNuS18 - September 25, 2015, 3:50 am

Spoiler ([Click to View](#)) MensaSQLi circle, session 2(3)

Every injector usually wants to dump interesting data from some table. But why not dump data from all columns from all tables (or many of them) at once? Here is a challenge where you can exercise such ultimate DIOS (Dump In One Shot).

~ Tasks ~

- display data from all columns of different tables in primary database (in one shot). As single table can have few thousands records and such picture with few thousands records can't be proof of data from all columns from different tables, display ONLY 3 RECORDS from each table in your proof picture.
- each table should be numbered, with displayed statistics about: records count, columns count, it's column names
- three numbered records in each table should be displayed. Use some divider between columns data (as I used :)

~ Target ~

aHR0cDovL3d3dy5jZWxsdWxhci1zb2x1dGlvbnMuY28udWsvY2FzZXN0dWRpZXMuGhwP2lkPTE0Mw==

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

~ Proof ~

[img]http://img15.hostingpics.net/pics/466284challenge20final.jpg[/img]

Edit:

Site is not vulnerable any more. Use new site below.

aHR0cDovL3d3dy5mb3JndW4ucnUvaW5mb3JtYXRpb24ucGhwP2luZm9faWQ9OQ==

New proof picture (no direct link with HTML IMG tags as picture is big - 983 x 49903)

<https://phify.com/img/WbNNzrIfiTC.jpg>

~ Rules ~

- use DIOS
- your syntax should be generic and work without knowing anything about tables/columns from that database
- don't ask for hints or solution

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

Let SQL knowledge be with you ?

~ Solvers ~
- makman ?

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](#)
[janus #10](#)
[janus #11](#)
[janus #12](#)
[janus #13](#)
[janus #14](#)
[janus #15](#)
[janus #16](#)
[janus #17](#)
[janus #18](#)
[janus #19](#)

Skidy - September 25, 2015, 9:38 am

<http://site.co.uk/casestudies.php?id=143%27+order+by+2>

I don't understand, on some websites using the order+by+ until I can find all the tables works, but its giving an error 100% of the time.

Ruse Reborn - September 25, 2015, 9:56 am

i.imgur.com/zrTSYLP.png

something different :D

krankenstein - September 25, 2015, 12:43 pm

17 columns found, but i have tried all the method

finding in source code

```
+and+false+
+and+0+
+and+true
+div+0+
+div+false+
+div+true+
+and+1=0+
+and+1=2+
=143/0
=14.3
=143/False
=.143
```


krankenstein - September 25, 2015, 1:13 pm

(Sep 25, 2015 12:59 PM)JaNuS18 Wrote: [\[CITE\]](#) krankenstein

this is a challenge!!! Why are you posting code? You want to ruin the challenge? ?
sorry brother, i have wasted 3hours for watching vulnerable column.
i am expressing my failure, ok go ahead,but i quit,hope one day u/others will expose it??
make/send some waf tricks&their behaviors to me/hackforum ?? with copyright protection ? ?

0x00FF - September 26, 2015, 5:29 am

Hi ,

i don't have permission to send private message , (new member)

ps : i use makman DIOS

this is the P0c :

img11.hostingpics.net/pics/392441Capture.png

thank you.

JaNuS18 - September 26, 2015, 8:34 am

(Sep 26, 2015 05:29 AM)0x00FF Wrote: [\[CITE\]](#) Hi ,

i don't have permission to send private message , (new member)

ps : i use makman DIOS

this is the P0c :

img11.hostingpics.net/pics/392441Capture.png

thank you.

Please read the tasks again. You must display data from those columns too... (3 records per table)

0x00FF - September 26, 2015, 9:40 am

(Sep 26, 2015 08:34 AM)JaNuS18 Wrote: [\[CITE\]](#) Please read the tasks again. You must display data from those columns too... (3 records per table)

i will try ?

HAAQ - September 29, 2015, 6:39 am

cellular.*_users:id
cellular.*_users:username
cellular.*_users:password

i'm DONE :D

JaNuS18 - September 30, 2015, 9:29 am

(Sep 29, 2015 06:39 AM)HAAQ Wrote: [\[CITE\]](#) cellular.*_users:id

cellular.*_users:username
cellular.*_users:password

i'm DONE :D

How is your post relevant for this topic (challenge)? ? ?

Report about your private injection post in your thread please.

Thanks ?

0x00FF - September 30, 2015, 10:30 am

Hi ,
the task pure sql?

blingbling - October 1, 2015, 1:47 am

(Sep 30, 2015 10:30 AM)0x00FF Wrote: [\[CITE\]](#) Hi ,
the task pure sql?

I have the same question. Is this pure SQL or can we include some javascript in query results?

HAAQ - October 1, 2015, 5:04 pm

(Sep 30, 2015 09:29 AM)JaNuS18 Wrote: [\[CITE\]](#) How is your post relevant for this topic (challenge)?
? ?

Report about your private injection post in your thread please.

Thanks ?
you had request alot broo for the challenge :(?

i care about my self and my capability :D

check this to make sure that i am right :D > 4:admin:***1982hu**** ?

krankenstein - October 2, 2015, 12:27 am

Thatz all i got ??

JaNuS18 - October 2, 2015, 1:10 am

Guys:

don't change target URL

don't post things I am not asking for in challenge tasks. Challenge is not about "if you can inject there" so I don't see a reason for a post where you give me data about admin

tasks and rules are clear. Don't complicate your life with definition like pure SQL. Is it pure SQL if we use HTML elements in our injection like
, , ???

krankenstein - October 2, 2015, 1:40 am

(Oct 2, 2015 01:10 AM)JaNuS18 Wrote: [\[CITE\]](#) Guys:

don't change target URL

don't post things I am not asking for in challenge tasks. Challenge is not about "if you can inject there" so I don't see a reason for a post where you give me data about admin

tasks and rules are clear. Don't complicate your life with definition like pure SQL. Is it pure SQL if we use HTML elements in our injection like
, , ???

i did not accept your challenge,i just needed to find out the exploit thats all,ur tasks&rules are quite impossible for the newbie like me
matter of fact::no expert will teach but eager to insult::pointing all sql experts ??

JaNuS18 - November 6, 2015, 12:40 pm

(Oct 2, 2015 01:40 AM)krankenstein Wrote: [\[CITE\]](#) matter of fact::no expert will teach but eager to insult::pointing all sql experts ??

Quote me please where did I insult you. ?

Thanks.

P.S.

And I shared many syntax with you, always answering all your questions. So I don't see a reason for your writing (see above) in my thread.

krankenstein - November 6, 2015, 12:48 pm

(Nov 6, 2015 01:40 PM)JaNuS18 Wrote: [\[CITE\]](#) Quote me please where did I insult you. ?

Thanks.

P.S.

And I shared many syntax with you, always answering all your questions. So I don't see a reason for your writing (see above) in my thread.i did not mean you bro.this was for another guy.....

Jin Goddo - December 11, 2015, 1:40 pm

Still no one has figured out this challenge. Time to reveal it maybe? :)

EDIT: And site is no longer vulnerable.

JaNuS18 - December 11, 2015, 2:33 pm

All my challenges remain open, so people can try them any time...

For challenge #20 use new site below.

PHP Code

<?php

aHR0cDovL3d3dy5mb3JndW4ucnUvaW5mb3JtYXRpb24ucGhwP2luZm9faWQ9OQ==

Here is new proof picture (no direct link with HTML IMG tags as picture is big - 983 x 49903)

PHP Code

<?php

<https://phify.com/img/WbNNzrlfiTC.jpg>

Jin Goddo - December 11, 2015, 3:15 pm

(Dec 11, 2015 03:33 PM)JaNuS18 Wrote: [\[CITE\]](#) All my challenges remain open, so people can try them any time...

For challenge #20 use new site below.

PHP Code

```
<?php
```

```
aHR0cDovL3d3dy5mb3JndW4ucnUvaW5mb3JtYXRpb24ucGhwP2luZm9faWQ9OQ==
```

Here is new proof picture (no direct link with HTML IMG tags as picture is big - 983 x 49903)

PHP Code

```
<?php
```

```
https://phify.com/img/WbNNzrlfiTC.jpg
```

Answer me this before I start on the challenge. Are you using javascript in this DIOS?

JaNuS18 - December 12, 2015, 2:42 am

(Dec 11, 2015 04:15 PM)Jin Goddo Wrote: [\[CITE\]](#) Answer me this before I start on the challenge. Are you using javascript in this DIOS?

Challenge has 3 simple rules. Just follow them. ? All three of them!

Slachter - December 30, 2015, 7:14 am

Page could not be found. :(:(

JaNuS18 - December 30, 2015, 9:05 am

(Dec 30, 2015 08:14 AM)Slachter Wrote: [\[CITE\]](#) Page could not be found. :(:(

Please read all messages in topic. HF doesn't allow me to edit first post any more... (I don't have status l33t or ub3r)

See

<https://hackforums.net/showthread.php?tid=4999671&pid=48920551#pid48920551>

spirited_wolf™ - June 3, 2016, 10:25 pm

Janus brother is it still vulnerable ? because the page is showing 404 error :cry:

JaNuS18 - June 4, 2016, 12:29 pm

(Jun 3, 2016 10:25 PM)spirited_wolf Wrote: [\[CITE\]](#) Janus brother is it still vulnerable ? because the page is showing 404 error :cry:

Latest challenge target link is one post above yours. And yes, it is still vulnerable...

spirited_wolf™ - June 5, 2016, 10:02 am

(Jun 4, 2016 12:29 PM)JaNuS18 Wrote: [\[CITE\]](#) Latest challenge target link is one post above yours. And yes, it is still vulnerable...

ohh oks Thanks ? brother