

Forum: [Hack Forums](#)

Thread: [\[Janus\] SQLi challenge #4](#)

JaNuS18 - December 20, 2014, 10:16 am

Hi folks,

This is my challenge #4. Again, it will be a little harder than previous ones ?

~ Task ~

- display all tables in primary database
- under each table (displayed only once) display numbered list (use roman numbers) of columns in that table (with their length in characters) sorted by column length descending
- display only column names with more than 6 characters in its name (hide all shorter ones)
- make a statistics about records in each table, number of columns and number of hidden columns (those shorter than 6 characters in column_name) in each table - see proof picture

~ Site ~

aHR0cDovL3d3dy5ldmVuZW1lbnRpZWwtZnJhbmNILmNvbS90YXJpZi1ldC1kZXZpcy10YXJpZnMu
cGhwP2lkYXBwZWw9NjA1MA==

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

~ Proof ~

[img]<http://img15.hostingpics.net/pics/98313178c1.jpg>[/img]

~ Rules ~

- complete injection must be done in one vulnerable column
- don't use group_concat, limit and substring_index (use pure DIOS)
- your command should work without knowing anything about tables/columns on that site...

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 ~

- S-x-S
- Inject0r Killer
- 7h3_Ph3n0m

P.S.

Don't harm the site. ? I choose it only for challenge...

Try also my other challenges for advanced injectors:

[janus #1](#)

[janus #2](#)

[janus #3](#)

RAi Jee - December 23, 2014, 8:58 pm

hey bro update the link u provided it cannot be decoded in base64

JaNuS18 - December 24, 2014, 1:44 am

(Dec 23, 2014 09:58 PM)RAi Jee Wrote: [\[CITE\]](#) hey bro update the link u provided it cannot be decoded in base64
It decodes fine. ?

Just don't use hackbar (bug in decoding) but site I suggested - <https://www.base64decode.org/>

?

RAi Jee - December 24, 2014, 3:36 am

(Dec 24, 2014 02:44 AM)JaNuS18 Wrote: [\[CITE\]](#) It decodes fine. ?

Just don't use hackbar (bug in decoding) but site I suggested -

?

yup but most people here use hackbar ,

JaNuS18 - December 25, 2014, 5:26 pm

(Dec 24, 2014 04:36 AM)RAi Jee Wrote: [\[CITE\]](#) yup but most people here use hackbar ,
I am using hackbar too. But there are bugs in hackbars (problems with decoding)...

What do you think why did I put that link for decoding target URL? ?

Lamer - December 25, 2014, 5:56 pm

Bugs are from myBB (what a shitty cms)

S-x-S - July 6, 2016, 12:01 am

[img]http://img15.hostingpics.net/pics/86738152147852.png[/img]

JaNuS18 - July 6, 2016, 2:56 am

(Jul 6, 2016 12:01 AM)S-x-S Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#)
[img]http://img15.hostingpics.net/pics/86738152147852.png[/img]

Great work S-x-S. ? Congrats. ?

Please add missing part (see PM)

gn0m3 - July 7, 2016, 1:10 am

I've been blocked by their security master JanuS can you pm me your Solution?

S-x-S - July 19, 2016, 2:39 am

[img]http://img15.hostingpics.net/pics/7213597775222777.png[/img]

Master, thanks for the challenge
????

JaNuS18 - July 19, 2016, 3:19 pm

(Jul 19, 2016 02:39 AM)S-x-S Wrote: [\[CITE\]](#) ...

Master, thanks for the challenge
????

Great ??

Added you to solvers ?

Kashmiri Hunter - August 3, 2016, 10:21 am

(Jul 19, 2016 03:19 PM)JaNuS18 Wrote: [\[CITE\]](#) Great ??

Added you to solvers ?

CHeck PM Related To This CHallenge ?

JaNuS18 - August 5, 2016, 1:44 pm

(Aug 3, 2016 10:21 AM)Kashmiri Hunter Wrote: [\[CITE\]](#) CHeck PM Related To This CHallenge ?
Sorry, you should do all tasks.

?

Inject0r Killer - August 19, 2016, 5:14 am

<http://prntscr.com/c7pkfw>

Check Pm ?

JaNuS18 - August 19, 2016, 6:02 am

(Aug 19, 2016 05:14 AM)Inject0r Killer Wrote: [\[CITE\]](#) <http://prntscr.com/c7pkfw>

Check Pm ?

Nice. ?

See all tasks carefully again. You didn't follow all tasks. Your proof picture differs from mine.

Also your output has big problems with tables at the end... Last details are not visible any more.

You are close. Good luck ?

7h3_Ph3n0m - August 19, 2016, 7:51 am

I'm unable to do roman numbering ,other task done?

JaNuS18 - August 19, 2016, 8:39 am

(Aug 19, 2016 07:51 AM)7h3_Ph3n0m Wrote: [\[CITE\]](#) I'm unable to do roman numbering ,other task done?

That part is the easiest.

If you are really so close I will brake my own rule and give you a solution for that ?

http://www.w3schools.com/html/html_lists.asp

?

Dgameman1 - August 20, 2016, 2:05 am

Quick question.

What do I do after I find out it's vulnerable?

Cause the order by doesn't seem to work for this website?

Inject0r Killer - August 20, 2016, 4:06 am

<http://prntscr.com/c8379y>

Thanks For Challenge Master ?

JaNuS18 - August 20, 2016, 4:43 am

(Aug 20, 2016 04:06 AM)Inject0r Killer Wrote: [\[CITE\]](#) <http://prntscr.com/c8379y>

Thanks For Challenge Master ?

Accepted. Congrats ?

Error:

Inject0r Killer has reached their private message quota so your message could not be sent.

Clean your PMs. I can't send you PM...

(Aug 20, 2016 02:05 AM)Dgameman1 Wrote: [\[CITE\]](#) Quick question.

What do I do after I find out it's vulnerable?

Cause the order by doesn't seem to work for this website?

copy/paste from other thread:

Hey, it is a challenge, so everyone should try to solve it alone ? Please follow some fair play rules with challenges.

If you have other site(s) where do you have problems, ask in forum or by PM and we will be glad to help you... ?

Inject0r Killer - August 20, 2016, 5:43 am

(Aug 20, 2016 04:43 AM)JaNuS18 Wrote: [\[CITE\]](#) Accepted. Congrats ?

Error:

Inject0r Killer has reached their private message quota so your message could not be sent.

Clean your PMs. I can't send you PM...

Cleaned ? (send me Urs Syntax Master)