

Forum:[Hack Forums](#)

Thread: [\[SQLi challenge #2\] pick your dreamgirl \[/SQLi challenge #2\]](#)

t.pro - February 14, 2014, 1:18 pm

CHALLENGE CLOSED - SITE IS DOWN!

Hey guys,
here a new challenge from Mr.TechProspect ?

TARGET:

Code xxx.mat[HF]chukr[HF]aine.co[HF]m

LEVEL:

medium (a lil bit to do / but basic injection)

good training for n00bs that read the HF-HQ-Tuts-carefully

RULES:pic a girl and show: ID, NAME, CITY, ENG, VK or EMAIL

Dreamgirl limitation:

you have to pic a girl with either email or VK-Link

*check tasks or proofpic for meaning of rule

Dont use: concat() or group_concat() for both use your brain instead ?

Hardcode limitation:

your command should work without knowing anything from database except the datapart of your "dreamgirl" (of course you can type in name of columns ONLY FOR THAT PART)

Cut off either VK-Link or email from girl (see my proof VK-Link, for email cut off after @) USE SQL FOR CUT OFF!

Dont ask for hints, please dont share anything until challenge is closed!

MAIN-TASKS:

show USER,DB,VERSION and Count DB'S without MySQL-Tables

pic your favourite girl and display your fav. picture of her

(you are allowed to hardcode img tag, and column names of "girlTable" but NOT the DATA itself)

Display a numbered list of all tables in primary DB with a numbered list of columns for each table

PROOF:

[img]http://s25.postimg.org/ov187mtz3/image.jpg[/img]

Send me command via PM (use <https://privnote.com/> for that)
post proof!

SOLVERS:

Ajkaro

Renegade18

133720

cheers and have fun ?

CHALLENGE CLOSED - SITE IS DOWN!

ajkaro - February 14, 2014, 2:20 pm

[img]<http://www.anonmgur.com/up/18f097e72a9ef25b5fabb8f44057db56.jpg>[/img]

Thanks for the challenge ?

t.pro - February 14, 2014, 2:34 pm

Please see the cutoff rule AND the no concat() rule my friend!

ajkaro - February 14, 2014, 3:02 pm

(Feb 14, 2014 03:34 PM)t.pro Wrote: [\[CITE\]](#) Please see the cutoff rule AND the no concat() rule my friend!

I sent you new syntax with cut off and without concat()

?

t.pro - February 14, 2014, 3:07 pm

(Feb 14, 2014 04:02 PM)ajkaro Wrote: [\[CITE\]](#) I sent you new syntax with cut off and without concat() that's exactly what i wanted to see! ?

Renegade18 - February 15, 2014, 7:56 am

[img]<http://anonmgur.com/up/8f28d5567c8ed3bb222ad448640df469.png>[/img]

t.pro - February 15, 2014, 9:39 am

Great work guys. u both choosed a hot girl!

?

@all

Renegades Girl has neither a VK Link or Email link (but it is a rule to pick a girl with either email or vk)

He had a query-soloution to inject the data by changing the ID. (btw. nice solution)

That means with renegades query i can click between the id's and data change automatically.

Thats why his proof pic isnt important (or not wrong)!

hackersallin - February 17, 2014, 1:45 am

I am not Good at SQL that much :/

Specially when it comes to these challenges... I cant understand what you guys do to make it write all the tables and stuff.

[img]<http://anonmgur.com/up/3e9e17913ad20d4af0f2243254b3bbd7.png>[/img]

I could only do this much....

I know the challenge is not complete for me but can you PM me the syntax used to i can learn how to do it?

I will PM you my Syntax.

Thanks for the challenge!

133720 - February 18, 2014, 4:25 pm

Thanks for challenge ?

t.pro - February 19, 2014, 1:21 am

(Feb 18, 2014 05:25 PM)133720 Wrote: [\[CITE\]](#) Thanks for challenge ?

Congratiolations, added to solvers ?

CHALLENGE CLOSED - SITE IS DOWN!

.