

Forum:[Hack Forums](#)

Thread: [The Challenge N 02 medium >> The challenge is closed and solution in <<](#)

BlackRoas - September 9, 2017, 3:16 pm

Hi my friend's how are you to all this challenge Number 02 medium

target

PHP Code

<?php

redwoodbank.co.uk/inside-redwood/meet-the-team/staff-detail/?id=5

Task & Rules

1- Union Based && GET Method

2- Your User Name , Version , Database Name , All Tables

3- User Name + Version + Database Name >>> Show them all with table >> View_CMS_User

4- Send Your Query

5- complete injection should be in the same column <<< This condition is optional

6- Don't Use In Your Query >> convert , int , and this method

Proof

Solution

I use select top 1 clause Because it's Windows so it's useful on large tables with thousands of records. Returning a large number of records can impact on performance.

and I used COLLATE SQL_Latin1_General_CP1_CI_AS >>> Because Is a clause that can be applied to a database definition or a column definition to define the collation, or to a character string expression to apply a collation cast so The collate bit follows the column name, basically

More

PHP Code

<?php

<https://docs.microsoft.com/en-us/sql/t-sql/statements/collations>

InjectorBoy - September 9, 2017, 4:50 pm

I have tried a lot but it is very difficult only the @@version Just what I can get out ,I will wait for the end of the challenge to know the solution

rawaz karim - September 9, 2017, 5:46 pm

thx for challenge

my proof :

BlackRoas - September 9, 2017, 7:57 pm

(Sep 9, 2017 05:46 PM)rawaz karim Wrote: [\[CITE\]](#) thx for challenge

my proof :

I use variable = 5 and your solution have variable = 14 and By looking at google I found a solution identical to yours with a change in your character and with same variable = 14 so !

PHP Code

<?php

<https://pastebin.com/sPuehmLV>

The challenge is closed because is there a solution in google

Regards

pishicat - September 13, 2017, 3:36 am

ok! why should in your solution you use :

top 1

and '::'

SQL_Latin1_General_CP1_CI_AS?

that i used it ? there are 200000000000 collation why this ?

it's hf's 100th time that copy and past from our forums ????

HF is low???

don't repeat and learn from your masters in HF ?

(Sep 9, 2017 03:16 PM)BlackRoas Wrote: [\[CITE\]](#) I use select top 1 clause Because it's Windows so it's useful on large tables with thousands of records. Returning a large number of records can impact on performance.I said this in my post ! tables are not too many..

[hxxp://s9.picofile.com/file/8306334326/123.JPG](http://s9.picofile.com/file/8306334326/123.JPG)

and said to your student that they do not ask challenge of a master to master !

rawaz karim - September 13, 2017, 3:47 am

i am member in a forum i saw this site before and i found it there not by search google

Inject0r Killer - September 13, 2017, 7:14 am

(Sep 13, 2017 03:36 AM)pishicat Wrote: [\[CITE\]](#) it's hf's 100th time that copy and past from our forums ????

Most of people are doing that stuff here ?

pishicat - *October 18, 2017, 11:38 pm*

pishicat_injector as ghtvbr in our forums put this target as question and i answered to him...

after it i commed here and see he puts solution full copy off my posts..i don't said that only i solved it .. but i'm sure blackrose doesn't solved it ..

this should be close of hf's admins ...

and when i posted here he said in ashiyane that my name is pishicat so i'm sure that blackrose = pishicat_injector..