

Forum:[Hack Forums](#)

Thread: [Asking for help from masters in sql](#)

Berry White - October 10, 2017, 10:44 pm

Hey guys, im not strange with sql, but there is some injections i cant inject but im sure they are vulnerable on union based... If some masters like janus can help me to inject this one site, i would be grateful

Many thanks in advance

Gardener Jim - October 10, 2017, 11:33 pm

Post the site and we might be able to help you.

Use: <https://www.base64encode.org/>

Berry White - October 10, 2017, 11:35 pm

Here it is mate,

aHR0cDovL3d3dy5zbG9ib2Rub3NycHNraS5jb20vaW5kZXgucGhwP2plemlrPXYm1lbmlfbGlua19pZD0yMA==
meni_link_id parameter is vulnerable

c0sm1k - October 11, 2017, 6:00 am

You have to use %23 to end the comments with or screen goes blank..

Code id=20' order by 13%23 sql error on screen

id=20' order by 14%23 screen goes blank

hope this helps ?

JaNuS18 - October 11, 2017, 11:47 am

(Oct 10, 2017 10:44 PM)Berry White Wrote: [\[CITE\]](#) Hey guys, im not strange with sql, but there is some injections i cant inject but im sure they are vulnerable on union based... If some masters like janus can help me to inject this one site, i would be grateful

Many thanks in advance

use:

PHP Code

<?php

syntax deleted by request

version: 5.5.55-cli

P.S:

OP contact me by PM when you will have rights to do it...

pishicat_Injector - October 11, 2017, 12:48 pm

(Oct 10, 2017 11:35 PM)Berry White Wrote: [\[CITE\]](#) Here it is mate,

aHR0cDovL3d3dy5zbG9ib2Rub3NycHNraS5jb20vaW5kZXgucGhwP2plemlrPXYm1lbmlfbGlua19pZD0yMA==

meni_link_id parameter is vulnerable

WOW, I notice this post now, it's a hot site, I will write a lesson explaining the method of injecting this site after a little special to you dear ?

JaNuS18 - October 11, 2017, 1:43 pm

(Oct 11, 2017 12:48 PM)pishicat_Injector Wrote: [\[CITE\]](#) WOW, I notice this post now, it's a hot site, I will write a lesson explaining the method of injecting this site after a little special to you dear ?

Sure, after I posted my syntax, you will explain it ? ??? Story of your life...

P.S.

My syntax was later removed by request as it is used in a challenge

pishicat_Injector - October 11, 2017, 1:53 pm

(Oct 11, 2017 01:43 PM)JaNuS18 Wrote: [\[CITE\]](#) Sure, after I posted my syntax, you will explain it ? ??? Story of your life...

P.S.

My syntax was later removed by request as it is used in a challenge

first: mr JaNuS18 I swear I have not seen your syntax, I am a Muslim and I never lie ?

Second: mr JaNuS18 wait to see my work to see it's not your work ?

I hope not only between us except good work

Regards Mr JaNuS18 ?

Berry White - October 11, 2017, 2:35 pm

(Oct 11, 2017 11:47 AM)JaNuS18 Wrote: [\[CITE\]](#) use:

PHP Code

<?php

syntax deleted by request

version: 5.5.55-cli

P.S:

OP contact me by PM when you will have rights to do it...

Janus can u pm me ?

(Oct 11, 2017 12:48 PM)pishicat_Injector Wrote: [\[CITE\]](#) WOW, I notice this post now, it's a hot site, I will write a lesson explaining the method of injecting this site after a little special to you dear ?

Thank you

(Oct 11, 2017 06:00 AM)c0sm1k Wrote: [\[CITE\]](#) You have to use %23 to end the comments with or screen goes blank..

Code id=20' order by 13%23 sql error on screen

id=20' order by 14%23 screen goes blank

hope this helps ?

Well I found 13 columns too, but that's not problem...

I found 6 columns too with ;%00

But no output or The used SELECT statements have a different number of columns, that's the problem xD but thanks for trying, I appreciate that mate <3

pishicat_Injector - October 11, 2017, 5:57 pm

(Oct 10, 2017 10:44 PM)Berry White Wrote: [\[CITE\]](#) Hey guys, I'm not strange with sql, but there is

some injections i cant inject but im sure they are vulnerable on union based... If some masters like janus can help me to inject this one site, i would be grateful

Many thanks in advance

Here You Go My Frind The Solution For You My Dear?

PHP Code

<?php

<https://hackforums.net/showthread.php?tid=5735331>

Berry White - October 11, 2017, 7:42 pm

(Oct 11, 2017 05:57 PM)pishicat_Injector Wrote: [\[CITE\]](#) Here You Go My Frind The Solution For You My Dear?

Well, thanks but u shouldnt type real site name, because probably someone will use it for bad purposes...

I was curious for solution, but somebody is going to be skiddie and deface site... you should set just something like example[dot]com,but thanks anyhow

PS:

Also, can u add when exactly are we supposed to use NULLIF ? Thanks in advance

pishicat_Injector - October 11, 2017, 8:09 pm

(Oct 11, 2017 07:42 PM)Berry White Wrote: [\[CITE\]](#) Well, thanks but u shouldnt type real site name, because probably someone will use it for bad purposes...

I was curious for solution, but somebody is going to be skiddie and deface site... you should set just something like example[dot]com,but thanks anyhow

PS:

Also, can u add when exactly are we supposed to use NULLIF ? Thanks in advance

why you don't say that to me in facebook in account Berry White Or here when I say to you I will make tut for you, if I do that now what about the Image the site in my Image so what you need from me now I delet my tut, that Which took me a great time to prepare for you? ?

Berry White - October 11, 2017, 8:14 pm

(Oct 11, 2017 08:09 PM)pishicat_Injector Wrote: [\[CITE\]](#) why you don't say that to me in facebook when I say to you I will make tut for you, if I do that now what about the Image the site in my Image so what you need from me now I delet my tut, that Which took me a great time to prepare for you? ?

Dude first of all i didnt expect that u will type real website name...

Second, u didnt wrote this for me, u wrote it because yourself on some way :)

And third, i dont need you to delete tut, i just asked to remove website name

pishicat_Injector - October 11, 2017, 8:46 pm

Berry White - October 11, 2017, 8:57 pm

(Oct 11, 2017 08:46 PM)pishicat_Injector Wrote: [\[CITE\]](#) who you say that ?

I don't need your site to add tut here in this section I have six Tutorial written for this section already, Just a matter of time on publication .

I spent a lot of time writing the subject just to help you not to my self ? as you say

Any way cuz you see this Tut It's for my self not for you my brother , I love to say to you I don't need it ? cuz I know all thing that Posted in this topic, So this Tut Is Deleted

Regards ?

You have? Then why u didnt set other website name, but this?

U could just change website name because its same injection method..

And i mean, its not specificaly for you tutorial, but for others , so you gain rep+

pishicat_Injector - October 11, 2017, 10:23 pm

(Oct 11, 2017 08:57 PM)Berry White Wrote: [\[CITE\]](#) You have? Then why u didnt set other website name, but this?

U could just change website name because its same injection method..

And i mean, its not specificaly for you tutorial, but for others , so you gain rep+

look what you say my brother

so what about my image in this tut I delet it to ? , there more of 5 or 7 image that's have the real site and If I deleted this image this tut it will be sucks, so I deleted all

BTW I have copy of this tut if you need just ask and I will pm to you CUZ all my work here it just for help you Not for personal gain

regards

Berry White - October 11, 2017, 10:34 pm

(Oct 11, 2017 10:23 PM)pishicat_Injector Wrote: [\[CITE\]](#) look what you say my brother

so what about my image in this tut I delet it to ? , there more of 5 or 7 image that's have the real site and If I deleted this image this tut it will be sucks, so I deleted all

BTW I have copy of this tut if you need just ask and I will pm to you CUZ all my work here it just for help you Not for personal gain

regards

Well man, u said u have more websites with same injection method, just make tutorial with that websites...

Yes i need it buddy, thank you a lot, i hope u didnt take all this wrong, but i just dont want some skiddie deface this website, thats all, i really appreciate ur work <3

pishicat_Injector - October 11, 2017, 11:54 pm

(Oct 11, 2017 10:34 PM)Berry White Wrote: [\[CITE\]](#) Well man, u said u have more websites with same injection method, just make tutorial with that websites...

Yes i need it buddy, thank you a lot, i hope u didnt take all this wrong, but i just dont want some skiddie deface this website, thats all, i really appreciate ur work <3
who say that I have more websites with same injection method ?

I say I have 6 tut ready to post here in HF not need to your sit to do it a tut

that's what I say

regards

Berry White - October 12, 2017, 1:02 am

(Oct 11, 2017 08:46 PM)pishicat_Injector Wrote: [\[CITE\]](#)

Here u wrote, but now u edited...
Really man, u kidding me ?

pishicat_Injector - October 12, 2017, 1:33 am

(Oct 12, 2017 01:02 AM)Berry White Wrote: [\[CITE\]](#) Here u wrote, but now u edited...
Really man, u kidding me ?

no my friend but I get many ask to back my tut, so I do it, not kidding you I don't need to do that with you, I hope you learning some thing new This is great do not forget it

Berry White - October 12, 2017, 2:24 am

(Oct 12, 2017 01:33 AM)pishicat_Injector Wrote: [\[CITE\]](#) no my friend but I get many ask to back my tut, so I do it, not kidding you I don't need to do that with you, I hope you learning some thing new This is great do not forget it
Write your tutorial, but dont use website which i asked for help

pishicat_Injector - October 12, 2017, 11:03 pm

I forgot to tell you You are posting a site name here That's why everyone knows it, and You tell me not to publish his name in my tut Really stupid person

Berry White - October 13, 2017, 12:19 am

(Oct 12, 2017 11:03 PM)pishicat_Injector Wrote: [\[CITE\]](#) I forgot to tell you You are posting a site name here That's why everyone knows it, and You tell me not to publish his name in my tut Really stupid person
I just asked for help, nobody asked you to write tutorial about it, i just needed help ...

Second, if you pmed me with solution, and if u didnt wrote that u will make tutorial for me, and then write tutorial about this injection, probably nobody would know that this site is involved... especially not some skiddie who wants only to deface..

Third, if you say that this tutorial is for me, then i guess you should respect my requests about tutorial and dont put website name, am i right?

And fourth, but most important, learn english better please, i can barely understand you, like you use some hash algorithm to talk/write lol

linhtinh - October 14, 2017, 12:13 pm

(Oct 11, 2017 06:00 AM)c0sm1k Wrote: [\[CITE\]](#) You have to use %23 to end the comments with or screen goes blank..

Code id=20' order by 13%23 sql error on screen
id=20' order by 14%23 screen goes blank
hope this helps ?

aHR0cDovL3d3dy5qYXBhbmVzZWNhcnRyYWwRILmNvbS9zdG9ja19saXN0LnBocD90eXBIX2lkPTIxIGhhdmZyAwIHVuaW9uIHNIbGVjdCAXMTEtMS0t

Can u give me the way to sqli with this site ?Vulnerale column is true but show only number

JaNuS18 - October 14, 2017, 3:26 pm

(Oct 14, 2017 12:13 PM)linhtinh Wrote: [\[CITE\]](#)

aHR0cDovL3d3dy5qYXBhbmVzZWNhcnRyYWwRILmNvbS9zdG9ja19saXN0LnBocD90eXBIX2lkPTIxIGhhdmZyAwIHVuaW9uIHNIbGVjdCAXMTEtMS0t

Can u give me the way to sqli with this site ?Vulnerale column is true but show only number
Follow forum rules and open new thread for your problem. Don't overtake thread from OP.

Regarding your URL with interesting problem:

DB: japanese_jctdb

version: 5.1.73-cll

Contact me by PM.

P.S.

I won't post syntax any more. Last time I did that (in exactly this thread) pishicat_injector saw it (but didn't understand it) and wrote the worst and most useless tutorial (new method ? ?) I've seen in my life. To prevent next such misery I will help you linhtinh only by PM.

•^v^-[bLacKn3x]-^v^• - October 14, 2017, 3:48 pm

(Oct 14, 2017 12:13 PM)linhtinh Wrote: [\[CITE\]](#)

aHR0cDovL3d3dy5qYXBhbmVzZWVhcnRyYWVhcnRyYWRILmNvbS9zdG9ja19saXN0LnBocD90eXBIX2lkPTI
xIGhhdmluZyAwIHVuaW9uIHNIbGVjdCAxMTExMS0t

Can u give me the way to sqli with this site ?Vulnerale column is true but show only number

pm me if you need help with that site

edit: fuck got problems

Berry White - October 14, 2017, 4:19 pm

Can i get solution for that site? if linthin agree

linhtinh - October 15, 2017, 1:29 am

(Oct 14, 2017 04:19 PM)Berry White Wrote: [\[CITE\]](#) Can i get solution for that site? if linthin agree
Yes u can , i cant pm anyone bcos im new member :((

(Oct 14, 2017 03:26 PM)JaNuS18 Wrote: [\[CITE\]](#) Follow forum rules and open new thread for your problem. Don't overtake thread from OP.

Regarding your URL with interesting problem:

DB: japanese_jctdb

version: 5.1.73-cll

Contact me by PM.

P.S.

I won't post syntax any more. Last time I did that (in exactly this thread) pishicat_injector saw it (but didn't understand it) and wrote the worst and most useless tutorial (new method ? ?) I've seen in my life. To prevent next such misery I will help you linhtinh only by PM. Sorry im new member so i cant pm anyone ,where orther way can i pm u ?Thanks

Berry White - October 15, 2017, 2:38 am

(Oct 15, 2017 01:29 AM)linhtinh Wrote: [\[CITE\]](#) Yes u can , i cant pm anyone bcos im new member :((

Sorry im new member so i cant pm anyone ,where orther way can i pm u ?Thanks

Thank you man

•^v^-[bLacKn3x]-^v^• - October 15, 2017, 9:41 am

(Oct 15, 2017 01:29 AM)linhtinh Wrote: [\[CITE\]](#) Yes u can , i cant pm anyone bcos im new member :((

Sorry im new member so i cant pm anyone ,where orther way can i pm u ?Thanks

<https://pastebin.com/0tnYvUq2>

you have to hex your output --> delete comma and decode your hex value :))

linhtinh - October 15, 2017, 12:43 pm

(Oct 15, 2017 09:41 AM)•^v^-[bLacKn3x]-^v^• Wrote: [\[CITE\]](#) you have to hex your output --> delete comma and decode your hex value :))

output of hex not only number :((,im thinking about binary but i dont know how to convert output

kmhacker - October 15, 2017, 12:51 pm

(Oct 15, 2017 12:43 PM)linhtinh Wrote: [\[CITE\]](#) output of hex not only number :((,im thinking about binary but i dont know how to convert output

this number show on the page so remove comma and add 0x before and decode hex

6,163,636,573 = 0x6163636573 decode hex output = acces

linhtinh - October 15, 2017, 1:05 pm

(Oct 15, 2017 12:51 PM)kmhacker Wrote: [\[CITE\]](#) 6,163,636,573 = 0x6163636573 decode hex output = acces

And version: 5.1.73-cll > 0x352e312e37332d636c6c >352e312e37332d636c6c ? How to show this string ?

•^v^-[bLacKn3x]-^v^• - October 15, 2017, 1:07 pm

You can't change our output as char or anything because value from that parameter is converted to number and only number will work here .

So we can't print text or speciaal signs directly here

yes you can use binary then output --> numbers .
this works too

kmhacker - October 15, 2017, 1:09 pm

(Oct 15, 2017 01:07 PM)•^v^-[bLacKn3x]-^v^• Wrote: [\[CITE\]](#) You can't change our output as char or anything because value from that parameter is converted to number and only number will work here .

So we can't print text or speECIAL signs here directly here

yes you can use binary then output --> numbers .
this works too
bro can you post version query pastebin

•^v^-[bLacKn3x]-^v^• - October 15, 2017, 1:21 pm

i think you can select from information_schema.global_variables

but version is not important. you need tables and columns ;)

LD_PRELOAD - October 15, 2017, 1:25 pm

You use `/*!12345*/` to identify version.

linhtinh - October 15, 2017, 1:27 pm

(Oct 15, 2017 01:09 PM)kmhacker Wrote: [\[CITE\]](#) bro can you post version query pastebin some problem not right here my friend , im used double hex like `hex(hex(version()))` ,im sure with double hex make output show only number ,but not right when i decode value hex :-s

c0sm1k - October 15, 2017, 4:52 pm

(Oct 15, 2017 09:41 AM)•^v^-[bLacKn3x]-^v^• Wrote: [\[CITE\]](#) `https://pastebin.com/0tnYvUq2` you have to hex your output --> delete comma and decode your hex value :))
Wow It took me a second to see what was going on ! ??