

# Forum:[Hack Forums](#)

Thread: [\[Medium\]--+SQL Challange+--\[Medium\]](#)

?Stark - July 10, 2013, 12:13 pm

[#]Type:Medium

[#]Target:

Code hxxp://thelionpress.com/books.php?cat=9

[#]Proof:

[img]http://s16.postimg.org/coth3yb6t/sqli1.png[/img]

[#]Rules:

[+] Any Method of SQLi

[+] Display Name,Version,Database

[+] Type of sqli that you injected

[+] No need to Send command just Bloor your screenshot....

[#]Winners:

[+] benzi

[+] PuzzuS

[+] DOS482

[+]

[+]

benzi - July 10, 2013, 12:40 pm

thanks for the challenge.

PuzzuS - July 10, 2013, 3:21 pm

Thanks :)

[img]http://www.anonmgur.com/up/eee3e39ca52b80e07b46376034c1574a.png[/img]

666Karma666 - July 10, 2013, 4:04 pm

All people use error based ?

..///

iTackleFatKids - July 10, 2013, 4:10 pm

I will give this a go now :) I am very new to SQLi

666Karma666 - July 10, 2013, 4:13 pm

(Jul 10, 2013 04:10 PM)iTackleFatKids Wrote: [\[CITE\]](#) I will give this a go now :) I am very new to SQLi

If you are new to SQLi, my advice will be to begin with Union based

DOS482 - July 10, 2013, 4:15 pm

thanks for the challange :)

Spoiler ([Click to View](#))

?Stark - July 10, 2013, 9:20 pm

Nice all...

@666karma

ya error based

@itacklefatkids

well you should start from union based...

check here dude::>><https://hackforums.net/showthread.php?tid=2008347>

VipVince - July 11, 2013, 3:13 pm

Thanks.

[img]<http://b81lfq.jpg>[img]

TUNOVATO - July 11, 2013, 4:05 pm

[IMG]<http://www.anonmgur.com/up/f19713e2ad29c6776e8f7f7e824b7858.png>[IMG]

Wild Wolf - July 11, 2013, 4:56 pm

Hi all friends

Please enter commands after the end of the race until we learn to let the answer

133720 - July 11, 2013, 7:45 pm

Thanks for challenge

sweettoow - July 12, 2013, 3:51 am

im noob... n i knw i need to eliminate tht extra \ WAF adding.. but dont understand how.. :( i tried many times..

if anyone can give hint, it will be appreciable, so tht i can try it more.. :)

Processor - July 13, 2013, 2:02 am

Thanks for the challenge

sweettoow - July 14, 2013, 5:37 am

can someone please give me hint how to eliminate that extra \ added by WAF??

im noob but until now i have learned so much, but for me always the hardest part is to find the vulnerability and columns.

?Stark - July 14, 2013, 6:29 am

from where you stuck in problem?

better find from here

[https://www.google.com/search?output=search&client=psy-ab&q=site:hackforums.net+waf&oq=site:hackforums.net+waf&gs\\_l=hp.3...858.7912.0.8038.27.25.2.0.0.0.430.8307.2-2j19j3.24.0.cqgrwrth...0...1.1.19.psy-ab.JUz3G5ncGDU&pbx=1&bav=on.2.or.r\\_cp.r\\_qf.&bvm=bv.48705608,d.d2k&biw=1280&bih=871&ech=1&psi=lafiUZ-EKLCa0QXc24G4Cg.1373808531963.3&emsg=NCSR&noj=1&ei=lafiUZ-EKLCa0QXc24G4Cg](https://www.google.com/search?output=search&client=psy-ab&q=site:hackforums.net+waf&oq=site:hackforums.net+waf&gs_l=hp.3...858.7912.0.8038.27.25.2.0.0.0.430.8307.2-2j19j3.24.0.cqgrwrth...0...1.1.19.psy-ab.JUz3G5ncGDU&pbx=1&bav=on.2.or.r_cp.r_qf.&bvm=bv.48705608,d.d2k&biw=1280&bih=871&ech=1&psi=lafiUZ-EKLCa0QXc24G4Cg.1373808531963.3&emsg=NCSR&noj=1&ei=lafiUZ-EKLCa0QXc24G4Cg)

sweettoow - July 14, 2013, 6:45 am

(Jul 14, 2013 06:29 AM)ax02798 Wrote: [CITE](#) from where you stuck in problem?

better find from here

[https://www.google.com/search?output=search&scient=psy-ab&q=site:hackforums.net+waf&oq=site:hackforums.net+waf&gs\\_l=hp.3...858.7912.0.8038.27.25.2.0.0.0.430.8307.2-2j19j3.24.0.cqrwrth...0...1.1.19.psy-ab.JUz3G5ncGDU&pbx=1&bav=on.2.or.r\\_cp.r\\_qf.&bvm=bv.48705608,d.d2k&biw=1280&bih=871&ech=1&psi=lafiUZ-EKLCa0QXc24G4Cg.1373808531963.3&emsg=NCSR&noj=1&ei=lafiUZ-EKLCa0QXc24G4Cg](https://www.google.com/search?output=search&scient=psy-ab&q=site:hackforums.net+waf&oq=site:hackforums.net+waf&gs_l=hp.3...858.7912.0.8038.27.25.2.0.0.0.430.8307.2-2j19j3.24.0.cqrwrth...0...1.1.19.psy-ab.JUz3G5ncGDU&pbx=1&bav=on.2.or.r_cp.r_qf.&bvm=bv.48705608,d.d2k&biw=1280&bih=871&ech=1&psi=lafiUZ-EKLCa0QXc24G4Cg.1373808531963.3&emsg=NCSR&noj=1&ei=lafiUZ-EKLCa0QXc24G4Cg)

i m stuck at the very beginning, i cant even start, i dont know how many columns are there, when i added ' or " or \ WAF adds extra \

like .php?id=999\

I just cant understand the error.. i just dont understand how do i move ' just after digit 9 so tht query will be legitimate

once i move from this step, i can do all by myself, i know how error based injection works.

If you PM me any how to start in this case, it would be more appreciable.. :)

?Stark - July 14, 2013, 7:24 am

(Jul 14, 2013 06:45 AM)sweetoow Wrote: [\[CITE\]](#) i m stuck at the very beginning, i cant even start, i dont know how many columns are there, when i added ' or " or \ WAF adds extra \

like .php?id=999\

I just cant understand the error.. i just dont understand how do i move ' just after digit 9 so tht query will be legitimate

once i move from this step, i can do all by myself, i know how error based injection works.

If you PM me any how to start in this case, it would be more appreciable.. :)this is hard to bypass...

i think you can not bypass it.

read here about \' character..

this is used for prevention injection.

[https://www.owasp.org/index.php/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet](https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)

sweetoow - July 14, 2013, 8:05 am

(Jul 14, 2013 07:24 AM)ax02798 Wrote: [\[CITE\]](#) this is hard to bypass...

i think you can not bypass it.

read here about \' character..

this is used for prevention injection.

[https://www.owasp.org/index.php/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet](https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)

yeah you are right, i cant bypass it

i will try reading that thread, and if i still stuck somewhere,

ill get back to you.

Thanks ?

?Stark - July 14, 2013, 9:09 am

(Jul 14, 2013 08:05 AM)sweetoow Wrote: [\[CITE\]](#) yeah you are right, i cant bypass it

i will try reading that thread, and if i still stuck somewhere,

ill get back to you.

Thanks ?

Your welcome dude....????

sweetoow - July 14, 2013, 10:24 am

hehe.. got the column count..

i was doing the stupidest mistake.. SPACES.. haha

now next step.. still its hard, but i will figure it out..

whole query is shown in the source code.. wondering why? and how to make it work?

for a newbie like me, its really tough challenge.. :)

