

Forum:[Hack Forums](#)

Thread: [help to exploit sql injection](#)

MR-XX - February 16, 2017, 2:50 am

how can exploit a sql injection vuln ending with word not a number ?

SQL Injection/Exploit :

http : // localhost /index.php?option=com_joomblog&task=tag&tag=Ihsan_Sencan[SQL]

Dutisto - February 16, 2017, 3:23 am

I don't see where it's different whether you got words or numbers for your injection

MR-XX - February 16, 2017, 5:57 am

(Feb 16, 2017 04:23 AM)Dutisto Wrote: [\[CITE\]](#) I don't see where it's different whether you got words or numbers for your injection

Thank you man for your answer

but i will give example:

you see that link is vulnerable to SQL injection but i wasn't able to exploit it

http: //www .alexkincaid. com/index.php?option=com_joomblog&task=tag&tag=hack'

DelziumTheProudWhale_temp - February 16, 2017, 5:58 am

(Feb 16, 2017 06:57 AM)MR-XX Wrote: [\[CITE\]](#) Thank you man for your answer

but i will give example:

you see that link is vulnerable to SQL injection but i wasn't able to exploit it

http: //www .alexkincaid. com/index.php?option=com_joomblog&task=tag&tag=hack'

use havij

MR-XX - February 16, 2017, 6:06 am

Same probleme

WAppEx 2.0 Analyze :

Analyzing bla bla bla..

Can't find keyword but let me do a try!

Can't find injection type... Trying Integer type if failed, retry with String type

Can't find db server type! But maybe there be some chances! [-o

Finding Injection Method...

Trying Mssql error based method...

I think i was wrong about injection type trying String type!

Trying union based method...

Finding columns count...

Can't find Columns count!

Trying Mysql error based method...

Dutisto - February 16, 2017, 7:44 am

Do you succeed to got at least a SQL error or something ? How do you know that this link is vulnerable ?

PM if u want

MR-XX - February 16, 2017, 9:56 am

(Feb 16, 2017 08:44 AM)Dutisto Wrote: [\[CITE\]](#) Do you succeed to got at least a SQL error or something ? How do you know that this link is vulnerable ?

PM if u want

visit that link and will give you sql error

[http://www.alexkincaid.com/index.php?option=com_joomblog&task=tag&tag=hack'](http://www.alexkincaid.com/index.php?option=com_joomblog&task=tag&tag=hack)

Dutisto - February 16, 2017, 10:47 am

Alright, i was able to inject whatever i want in this site. As i said, number or word doesn't matter^^

DelziumTheProudWhale_temp - February 16, 2017, 12:11 pm

(Feb 16, 2017 11:47 AM)Dutisto Wrote: [\[CITE\]](#) Alright, i was able to inject whatever i want in this site. As i said, number or word doesn't matter^^

may i ask you how you did it?

i tried to do it however no luck

Dutisto - February 16, 2017, 12:12 pm

I can guide you in the right direction, pm me^^

DelziumTheProudWhale_temp - February 16, 2017, 12:12 pm

(Feb 16, 2017 01:12 PM)Dutisto Wrote: [\[CITE\]](#) I can guide you in the right direction, pm me^^
you wont be able to reply to my pm tho

Dutisto - February 16, 2017, 1:41 pm

(Feb 16, 2017 01:12 PM)DelziumTheProudWhale_temp Wrote: [\[CITE\]](#) you wont be able to reply to my pm tho

Oups, forgot about this. Alright, show some injections you tried, and i'll correct you^^

MR-XX - February 16, 2017, 3:04 pm

Guys , how about to show us here in public ?

Dutisto - February 16, 2017, 3:09 pm

That's what we gonna do ;)

MR-XX - February 17, 2017, 1:38 am

(Feb 16, 2017 04:09 PM)Dutisto Wrote: [\[CITE\]](#) That's what we gonna do ;)
Then where is it?

Dutisto - February 17, 2017, 5:09 am

(Feb 17, 2017 02:38 AM)MR-XX Wrote: [\[CITE\]](#) Then where is it?

I just wait for you to show me some injections you tried ! There is no point to just give you the answer

Gee4rce - February 17, 2017, 8:10 am

(Feb 16, 2017 03:50 AM)MR-XX Wrote: [\[CITE\]](#) how can exploit a sql injection vuln ending with word not a number ? (Feb 16, 2017 04:23 AM)Dutisto Wrote: [\[CITE\]](#) I don't see where it's different whether you got words or numbers for your injection

What you guys are facing here is the difference between an integer(represented by numbers) and String(represented by text) based injection.

While for integer, you do not use ' or " to close the injection, it is common for string injection to close

the String with ' or " or even ").

Imagine this SQL query (requesting integer):

<http://pastebin.com/AXf2mejY>

..now same query (but this time requesting a string):

<http://pastebin.com/y71nr4hU>

Do you see the difference?

Therefore when you have an SQLi with String injection type, you have an open clause that needs to be closed, when SQL injecting, otherwise the query would be erroneous like this:

<http://pastebin.com/hEsuPM0a>

Now, same query with closed string:

<http://pastebin.com/47QgQsk5>

The reason for this is that in coding, integers are numerical values (not a string), and therefore in most cases do not need to be enquoted with ' or ".

For strings, this is different, they're treated with ' or " (note that there is a difference between ' and ").

Hope that helps,
cheers Gee.

Dutisto - February 17, 2017, 10:20 am

That's really well explained ! nice

MR-XX - February 17, 2017, 2:58 pm

Nice explanation and easy to understand

Thank you :)

Dutisto - February 17, 2017, 3:33 pm

(Feb 17, 2017 03:58 PM)MR-XX Wrote: [\[CITE\]](#) Nice explanation and easy to understand

Thank you :)

Did you success to do your injection now ?

Gee4rce - February 17, 2017, 8:25 pm

No problem guys,

and yes, i'd also be interested if the injection is working now.

Cheers, Gee.

Dutisto - February 18, 2017, 2:30 am

The injection is working from the beginning for me, as I already know what you said. So if he understood what you said, his should work too^^

MR-XX - February 18, 2017, 6:49 am

(Feb 17, 2017 04:33 PM)Dutisto Wrote: [\[CITE\]](#) Did you success to do your injection now ?

That's kinda weird but i got the result display in <title></title> tag

[http:// alexkincaid.](http://alexkincaid.com/index.php?option=com_joomblog&task=tag&tag=hack%27+UnIoN+SeLeCt+version()--%20-)

[com/index.php?option=com_joomblog&task=tag&tag=hack%27+UnIoN+SeLeCt+version\(\)--%20-](http://alexkincaid.com/index.php?option=com_joomblog&task=tag&tag=hack%27+UnIoN+SeLeCt+version()--%20-)

Dutisto - February 18, 2017, 10:42 am

Yeah, but this is not your fault^^

Btw, you can just use the regular 'union select' no need to capitalize letters