

Forum:[Hack Forums](#)

Thread: [can anyone find the column number of this site](#)

arun hacker - March 14, 2015, 5:45 am

I have got sqli vulnerability in this site but i am not getting the column numbers of this site, can anyone get me the column number of this site and tell me how you go it.

<http://www.agirmedia.de/newsdetail.php?ID=36>

Thanks

Red Lion - March 14, 2015, 6:03 am

Were you able to confirm the SQL injection ?

Because i only get an error message if i submit anything but numbers and whitespaces.

arun hacker - March 14, 2015, 6:11 am

yeah it is sqli vulnerable and i get the same error every time when i use to find the column numbers, even i tried every query. First i simple tried order by n-- and after that i tried ' order by n -- - but then i also i wasn't able to find the column numbers of the site

Red Lion - March 14, 2015, 6:17 am

Can you post a query where you didn't get an error ?

Don't think that this is exploitable, as you don't get anywhere only with numbers.

arun hacker - March 14, 2015, 6:50 am

(Mar 14, 2015 06:17 AM)Red Lion Wrote: [\[CITE\]](#) Can you post a query where you didn't get an error ?

Don't think that this is exploitable, as you don't get anywhere only with numbers.

bro , i have given the site, you can try yourself

<http://www.agirmedia.de/newsdetail.php?ID=36>

Red Lion - March 14, 2015, 7:06 am

As i said, when ID contains something else but numbers, you'll get the error.

id=36s --> error

means if it was vulnerable the SQL query would have to look like

where id=36s

but the error is

Quote: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 " at line 2

The conclusion is id is casted to int before it is inserted into the SQL query.

If id contains a string the cast fails and id is empty.

You get the same error if you submit id=""

Sorry but this parameter is not vulnerable to SQL injection.

hahdbwoannniabs - March 14, 2015, 8:03 am

It's probably something they put there purposely as a honeypot or to ward off hackers.

Uploader.sx - March 14, 2015, 10:04 am

Leave it ... theres no /login or /admin !

Th3PonyWizard - March 14, 2015, 11:47 am

(Mar 14, 2015 08:03 AM)0x0c0c0c0c Wrote: [\[CITE\]](#) It's probably something they put there purposely as a honeypot or to ward off hackers. I feel this is more of a lazy workaround rather than an actual attempt of something, such as forced casting. Like the dude above said, anything not integer is error.

SELECT * FROM `table` where `id` = {(int)\$_GET['ID']};
or something.

(Mar 14, 2015 10:04 AM)RealMafia Wrote: [\[CITE\]](#) Leave it ... theres no /login or /admin !Yeah, who needs database records when there's no clear privileged URL detected! Boo!