

Forum:[Hack Forums](#)

Thread: [\[EASY\] Fast and Easy SQL Injection Method \[EASY\]](#)

Cabin Fever - March 17, 2010, 4:30 pm

Hey guys, I thought I would contribute a little to the community, so here is my guide on how to test for SQLi vulnerable sites and then doing the actual injecting. This method is extremely fast, and requires about 2-3 things of copy and pasting, so here we go.

Programs Needed:

SQLi Helper v2.7
SQLi Scanner
Admin Page Finder

Download [HERE](#)

Credits to [\[color\]Zarabyte.com\[/color\]](#), Internet Security Research Team.

All programs are clean.

STEP 1

First, open up your Vulnerability Scanner, and type in a dork such as "inurl:index.php?articleid=". There are THOUSANDS more, but this is the one I am using. Just do a search on here for "Google Dorks", and you'll find 'em ;). Type in your Dork into the area designated for it, and make sure the box for "SQLi Based Error" is the only one checked, then click "Scan Sites". Your screen should look more or less like the picture, depending on the Dork you use.

Spoiler ([Click to View](#))

STEP 2

After you do that, a list of sites should appear on the left side of the screen. These are the sites that were found using the Google Dork. Now what you need to do is click the button NEXT to the "Scan Sites" button, marked "Test Sites". Once you click this, a smaller list of sites should appear on the right side. These are the Vulnerable sites picked out of the sites found by the Dork. Again, your picture should look more or less like mine.

Spoiler ([Click to View](#))

STEP 3

Now, open up your SQLi Helper v2.7.

In the target area of the SQLi Helper, you will put the links you have found on the Vulnerable Sites part of the Scanner. Please note that you can only test one site at a time.

Alright, now the site I will be testing is one I found earlier, Taleempk.com.

Put the Vulnerable site link into the Target area, and click "Inject".

Yet again, your screen should look similar to mine.

Spoiler ([Click to View](#))



STEP 4

Now on to the next step. If the SQL version is below 5.0, then it's better to go on to the next site. Ok, now click "Get Database". A couple of things should show up, sometimes more. Just a little side note, don't use information_schema. It's useless. For this one, I'll click on "taleempk_data" and then click "Get Tables". Once you do that, the Tables should show up, and if you're lucky, the Admin or Users tables will show. Luckily this one did. Click on the word Admin and press "Get Columns" and the words Username and Password show up, yay! Now, click on "Username" then hold CTRL and click on "Password", then click "Dump Now". It might not always work if you try to do both of them at the same time, so if it doesn't, then just do one at a time. Now when you do this, the Username and Password will show up. (PLEASE NOTE THAT EVERYTHING YOU SEE WILL BE DIFFERENT FOR EACH SITE, JUST USE YOUR COMMON SENSE)

Spoiler ([Click to View](#))

STEP 5

Now that you have the Admins Username and Password, you'll need to find out where to enter it in at.

Open up your Admin Page Finder, and type in the name of the website you are Injecting, and click Scan, and the admin page links should show up in the Directory part, just double click on them to be automatically linked to it.

Now just type in the Username and Password, and there you go! Instant Admin Access from only a few button clicks!

Here are some notes to clarify a few things.

This won't work on all sites.

If the version is 4.0 and not 5, move along to the next one.

Even if it's vulnerable, the Admin columns still might not show up.

Even if the Admin Columns do show up, the password might be crypted.

Identify the type of hash it is, then find the a decrypter that works on that type of hash.

Even if you find a decrypter it still might not be crackable.

The End.

I worked on this tutorial for about an hour, if you liked it, please leave feedback! Thanks for reading! Nobody wants to write a review? Damn.

-mothered- - March 17, 2010, 5:07 pm

Mate, this Is awesome. A very well detailed, Illustrated and elaborated tut. Will definitely be trying It. Thanks mate for the share.

Cabin Fever - March 17, 2010, 5:16 pm

(Mar 17, 2010 05:07 PM)mothered Wrote: ([CITE](#)) Mate, this Is awesome. A very well detailed, Illustrated and elaborated tut. Will definitely be trying It.

Thanks mate for the share.

No problem :)

It saves you a lot of time finding the Vulnerable sites and a lot of time with the auto injecting :)
Try it out and let me know what you think man.

jasontest - March 17, 2010, 5:36 pm

Awesome guide, the "Google Dork" you used is the only one I found to give results. However all the URL's are non vulnerable. Any tips?

Never mind, got it working. One of the best guides I read so far on these forums. (I dont read many tho--yours was just very neat and easy)

peek - March 17, 2010, 5:40 pm

When I downloaded SQLihelper it came up as a virus. Is that normal, lol?

jasontest - March 17, 2010, 5:50 pm

None of them are working for me... :|

Why are none of the collums popping up

Cabin Fever - March 17, 2010, 6:19 pm

(Mar 17, 2010 05:40 PM)#CyberGate Wrote: [\[CITE\]](#) When I downloaded SQLihelper it came up as a virus. Is that normal, lol?

Yeah, it happens to me too, no worries, it's from Zarabyte so I don't think it's backdoored, lol.

? Elektrisk ? - March 17, 2010, 6:21 pm

Admin page finder link is down. I rar'd all 3 programs.

<http://www.sendspace.com/file/bywylt>

Thanks for taking the time to write this.

Cabin Fever - March 17, 2010, 6:24 pm

(Mar 17, 2010 06:21 PM)Elektrisk Wrote: [\[CITE\]](#) Admin page finder link is down. I rar'd all 3 programs.

<http://www.sendspace.com/file/bywylt>

Thanks for taking the time to write this.

Thanks for RARing them, I'll add them to the tutorial instead of the seperate links.

BlueBit - March 17, 2010, 6:36 pm

Got loads of trojan warnings on the SQLiHelper

Cabin Fever - March 17, 2010, 6:37 pm

(Mar 17, 2010 06:36 PM)FillUp Wrote: [\[CITE\]](#) Got loads of trojan warnings on the SQLiHelper

Yeah same here I'm pretty sure it's not backdoored, I think it was just how it's made or maybe it's a false positive. Run it and Sandboxie and scan it on VirusTotal, see what it is.

designedBy - March 17, 2010, 6:40 pm

You can never be sure with virus checks as it could be crypted.

I'm going to imagine it's a false positive.

SQLi Helper seems legit.

BlueBit - March 17, 2010, 6:43 pm

I'd rather not take the chance, sorry.

Once more people verify it's false positive, I'll probably download it.

Cabin Fever - March 17, 2010, 6:45 pm

(Mar 17, 2010 06:40 PM)fear Wrote: [\[CITE\]](#) You can never be sure with virus checks as it could be crypted.

I'm going to imagine it's a false positive.

SQLi Helper seems legit.

Scan it on VirusTotal, it will be detected when you do that.

Friedrich Schiller - March 17, 2010, 6:55 pm

Very very helpful tutorial however its also good if people learn to SQL manually without tools to understand what they are actually doing

but overall a VERY handy and effective tutorial

keep up the good work

Cabin Fever - March 17, 2010, 7:05 pm

(Mar 17, 2010 06:55 PM)The Black Hat Wrote: [\[CITE\]](#) Very very helpful tutorial however its also good if people learn to SQL manually without tools to understand what they are actually doing

but overall a VERY handy and effective tutorial

keep up the good work

Thanks for your feedback, feedback is always appreciated! :)

designedBy - March 17, 2010, 7:11 pm

Know if there is a mac version of this?

Internet is down on my desktop and my mactop is currently stealing the neighbor's WiFi.. only way I can get on the Internet right now. Hah.

? Elektrisk ? - March 17, 2010, 7:20 pm

(Mar 17, 2010 07:11 PM)fear Wrote: [\[CITE\]](#) Know if there is a mac version of this?

Internet is down on my desktop and my mactop is currently stealing the neighbor's WiFi.. only way I can get on the Internet right now. Hah.

There isn't.

Use Bootcamp.

Cabin Fever - March 17, 2010, 7:26 pm

Yeah just use Bootcamp, was going to say it but he got to it first :D

designedBy - March 17, 2010, 7:34 pm

Yeah I more than likely will.

To the ones concerned, you could probably just sandboxie this for safety.

fubu1 - March 17, 2010, 7:37 pm

"Get Database" doesnt work ? is that cause site isnt vuln?

Cabin Fever - March 17, 2010, 7:46 pm

(Mar 17, 2010 07:37 PM)fubu1 Wrote: [\[CITE\]](#) "Get Database" doesnt work ? is that cause site isnt vuln?

Yes.

? Elektrisk ? - March 17, 2010, 8:02 pm

(Mar 17, 2010 07:37 PM)fubu1 Wrote: [\[CITE\]](#) "Get Database" doesnt work ? is that cause site isnt vuln?

Make sure the program says "Url is vulnerable" and not "Url is not vulnerable". Sometimes, the site scanner (to find vulnerable sites) finds sites that aren't vulnerable on accident.

SIM-74411 - March 17, 2010, 8:07 pm

Awesome tutoriat :) will give it a try ;)

Cabin Fever - March 17, 2010, 8:10 pm

(Mar 17, 2010 08:07 PM)thalada Wrote: [\[CITE\]](#) Awesome tutoriat :) will give it a try ;)

Please do, let me know how it works out for you :)

raponi - March 17, 2010, 8:16 pm

OMG THANK YOUUUUU

bahhhhhh how do i give reps ?

Friedrich Schiller - March 17, 2010, 8:18 pm

only HF 1337 can give +rep

I'm pretty sure at least lol

Cabin Fever - March 17, 2010, 8:23 pm

(Mar 17, 2010 08:16 PM)raponi Wrote: [\[CITE\]](#) OMG THANK YOUUUUU

bahhhhhh how do i give reps ?

Only l33t can give reps buddy, it costs \$15 to upgrade to one.

CharlieSheen - March 17, 2010, 9:06 pm

i think im detecting a virus or my computer just thinks its a virus but im kinda worried now. posting a pic in a sec could someone please help??

Cabin Fever - March 17, 2010, 9:07 pm

(Mar 17, 2010 09:06 PM)dylmyster22 Wrote: [\[CITE\]](#) i think im detecting a virus or my computer just thinks its a virus but im kinda worried now. posting a pic in a sec could someone please help??

It's a false positive, run it on Sandboxie if you don't trust it.

CharlieSheen - March 17, 2010, 9:07 pm

[IMG]<http://i646.photobucket.com/albums/uu188/dylmyster666/wtf.jpg>[IMG]

eXemist - March 17, 2010, 9:08 pm

This is an awesome release thank you!

Cabin Fever - March 17, 2010, 9:08 pm

(Mar 17, 2010 09:07 PM)dylmyster22 Wrote: [\[CITE\]](#)

[IMG]<http://i646.photobucket.com/albums/uu188/dylmyster666/wtf.jpg>[IMG]

Thank you for your concern. It's a false positive, meaning that some parts of the code are the same pattern as the virus that it detects it as. It's not a virus, and it's not backdoored.

Alright that's what i figured i just wanted to make sure. just recently got a virus off my computer, didn't want another one back on haha

Eh... No offense but this takes the "Fun" out of it. It's less rewarding mentally if you don't do it yourself. And you lose bragging rights.

sweet well ima try this tut out. ill post some pics if i get anything to work.

Oh, and all the SQLHelpers, even the legitimate ones are detected as viruses cause so many faggots binded viruses to them.

(Mar 17, 2010 09:10 PM)Oblakastouf Wrote: [\[CITE\]](#) Eh... No offense but this takes the "Fun" out of it. It's less rewarding mentally if you don't do it yourself. And you lose bragging rights.

Well, I do defacements for the fun of it, and to show off sometimes ;).

I already know how to do SQLi manually, so this is a Godsend that I found this out, makes my job a lot easier.

sqli 2.7 wont open for me. i double click, right click and open and nothing. i can open the other ones just fine though

Well the other ones are essentially the same, so go ahead and use those.

(Mar 17, 2010 09:09 PM)dylmyster22 Wrote: [\[CITE\]](#) Alright that's what i figured i just wanted to make sure. just recently got a virus off my computer, didn't want another one back on haha

Please use spoiler tags when embedding images in a post in the future, unless it's small. To do this, do:

`[spoiler][img] [/img] [/spoiler]`

It's not a rule, but it's nicer for people with slower connections :)

Also, as for it not opening, what is your OS? I'm using XP and it works fine.

(Mar 17, 2010 09:10 PM)Oblakastouf Wrote: [\[CITE\]](#) Eh... No offense but this takes the "Fun" out of it. It's less rewarding mentally if you don't do it yourself. And you lose bragging rights.

I'm content knowing I could do it myself. It's easier to do it with a tool. It's like experienced web designers using Dreamweaver to make it easier for them.

(Mar 17, 2010 09:16 PM)Elektrisk Wrote: [\[CITE\]](#) (Mar 17, 2010 09:10 PM)Oblakastouf Wrote: [\[CITE\]](#)
Eh... No offense but this takes the "Fun" out of it. It's less rewarding mentally if you don't do it yourself. And you lose bragging rights. I'm content knowing I could do it myself. It's easier to do it with a tool. It's like experienced web designers using Dreamweaver to make it easier for them.

Took the words right out of my head, I just couldn't get them out of my mouth in the right format lol

x1029 - March 17, 2010, 9:29 pm

(Mar 17, 2010 09:23 PM)The Phlegethon Wrote: [\[CITE\]](#) I'm content knowing I could do it myself. It's easier to do it with a tool. It's like experienced web designers using Dreamweaver to make it easier for them.

Took the words right out of my head, I just couldn't get them out of my mouth in the right format lol
[/quote]

I mean if you're in a jam and need it done fast... I guess... Other than that :\... It just defies all basic hacker instinct :\

Cabin Fever - March 17, 2010, 9:31 pm

(Mar 17, 2010 09:29 PM)Oblakastouf Wrote: [\[CITE\]](#) Took the words right out of my head, I just couldn't get them out of my mouth in the right format lol

I mean if you're in a jam and need it done fast... I guess... Other than that :\... It just defies all basic hacker instinct :\

[/quote]

Well it's just a pain in the ass going through all the sites and most of them aren't even vulnerable.

CharlieSheen - March 17, 2010, 9:35 pm

im running XP to oh well its cool. i used the example the OP used that taleempk site and i got pass and user ut cant find a working admin page.

? Elektrisk ? - March 17, 2010, 9:35 pm

Quote:I mean if you're in a jam and need it done fast... I guess... Other than that :\... It just defies all basic hacker instinct :\

That's like saying we shouldn't use calculators because we could do math on paper.

MySocksAreWet - March 17, 2010, 9:36 pm

This is actually a really good fucking tutorial.

Good job bro.

Cabin Fever - March 17, 2010, 9:38 pm

(Mar 17, 2010 09:36 PM)MySocksAreWet Wrote: [\[CITE\]](#) This is actually a really good fucking tutorial.

Good job bro.

Thank you for your feedback. I appreciate it.

Eweshi - March 17, 2010, 9:38 pm

Thanks alot of tut :D

CharlieSheen - March 17, 2010, 9:39 pm

any help on trying to get the site? i have the pass and username but when i go to the control panel and type it in it says login attempt failed

Cabin Fever - March 17, 2010, 9:42 pm

Yeah I changed it, it's just for practice.

HighSpeed - March 17, 2010, 9:43 pm

It doesnt return the version on any of the links I've tried with the SQLi Helper, anyone have the same issue?

CharlieSheen - March 17, 2010, 9:44 pm

what did you change?

Cabin Fever - March 17, 2010, 9:46 pm

(Mar 17, 2010 09:43 PM)HighSpeed Wrote: [\[CITE\]](#) It doesnt return the version on any of the links I've tried with the SQLi Helper, anyone have the same issue?

How many links have you tried?

HighSpeed - March 17, 2010, 9:47 pm

about 15 so far, does it normally take awhile for it to publish the results?

? Elektrisk ? - March 17, 2010, 9:49 pm

(Mar 17, 2010 09:44 PM)dylmyster22 Wrote: [\[CITE\]](#) what did you change?

Are you trying the website used in the tutorial? If so, then the OP changed the admin's password already.

Cabin Fever - March 17, 2010, 9:49 pm

(Mar 17, 2010 09:44 PM)dylmyster22 Wrote: [\[CITE\]](#) what did you change?

The password for the cPanel

(Mar 17, 2010 09:47 PM)HighSpeed Wrote: [\[CITE\]](#) about 15 so far, does it normally take awhile for it to publish the results?

Depends on your computer.

HighSpeed - March 17, 2010, 9:53 pm

Im using it on a core 2, not the fastest computer but it seems to be handling the program just fine. It has been on Check No. of Columns for awhile now, am I missing something here?

? Elektrisk ? - March 17, 2010, 9:53 pm

(Mar 17, 2010 09:53 PM)HighSpeed Wrote: [\[CITE\]](#) Im using it on a core 2, not the fastest computer but it seems to be handling the program just fine. It has been on Check No. of Columns for awhile now, am I missing something here?

I've noticed that some websites lag like that. Are you sure the URL is vulnerable?

CharlieSheen - March 17, 2010, 9:54 pm

aww darn wanted to test it out. see what things i could come up with

HighSpeed - March 17, 2010, 9:55 pm

Ya, pretty much every site I have tried so far has said "URL is Vulnerable" I will let it run for awhile longer and see what happens.

(Mar 17, 2010 09:53 PM)Elektrisk Wrote: [\[CITE\]](#) I've noticed that some websites lag like that. Are you sure the URL is vulnerable?

CharlieSheen - March 17, 2010, 9:57 pm

i have tried a bunch of dorks and no results yet =/

i wanna do angrymarks but afraid they would come beat me up if they caught me XD lol

it says the sites are vulnerable but then checks for columns and then takes forever =/

Cabin Fever - March 17, 2010, 10:05 pm

(Mar 17, 2010 09:57 PM)dylmyster22 Wrote: [\[CITE\]](#) i have tried a bunch of dorks and no results yet =/

i wanna do angrymarks but afraid they would come beat me up if they caught me XD lol

it says the sites are vulnerable but then checks for columns and then takes forever =/

The ones that do that aren't going to work, move on to the next one.

CharlieSheen - March 17, 2010, 10:06 pm

aww darn how long should it normally take to finish injecting?

Cabin Fever - March 17, 2010, 10:08 pm

About 30 seconds at the most, if it goes past, just move on.

CharlieSheen - March 17, 2010, 10:08 pm

sweet it said that checking for columns is finished now searching for largest text visible column. working?

Cabin Fever - March 17, 2010, 10:10 pm

Yep! Just post again if you have anymore problems.

CharlieSheen - March 17, 2010, 10:13 pm

nothing is working for me ><

HighSpeed - March 17, 2010, 10:13 pm

I had the same thing searching for larger text visble columns, no luck still searching though

CharlieSheen - March 17, 2010, 10:14 pm

ya im still trying but with no luck.

Cabin Fever - March 17, 2010, 10:18 pm

Well I don't know what to tell you guys, it works PERFECTLY for me.

CharlieSheen - March 17, 2010, 10:20 pm

it could be the sql version differences.

do you have t.v.? if so maybe you could tell me if im doing anything wrong

HighSpeed - March 17, 2010, 10:20 pm

Do u think u can find a url that is working for u perfectly so I can see if it works for me too or if it is just my computer? please?

Maybe it is my version of the SQLi Helper, I noticed in ur screeshots u have 2.7 running but what I got from the DL was 2.6. I doubt that would matter much though but I'm not sure why its not working for me.

CharlieSheen - March 17, 2010, 10:25 pm

you got 2.6 working? i could only get 2.5 to work =/

HighSpeed - March 17, 2010, 10:28 pm

ya 2.6 running right now

CharlieSheen - March 17, 2010, 10:35 pm

i think its my av that is blocking the programs yo open =/

Cabin Fever - March 17, 2010, 10:36 pm

(Mar 17, 2010 10:35 PM)dylmyster22 Wrote: [\[CITE\]](#) i think its my av that is blocking the programs yo open =/

I think you're right.

? Elektrisk ? - March 17, 2010, 10:38 pm

(Mar 17, 2010 10:35 PM)dylmyster22 Wrote: [\[CITE\]](#) i think its my av that is blocking the programs yo open =/

It should give you a notification if that's the case. Any good AV would. Which do you use?

CharlieSheen - March 17, 2010, 10:40 pm

cuz everytime i go to open the file, it gives me a pop up then when i click ignore it just closes it. and the others are to remove th infection and remove all unhealed infections. im running avg free 8.5 i can choose heal, move to vault, or ignore. the first two just deletes the program and ignore just does nothing.

Cabin Fever - March 17, 2010, 10:41 pm

Turn it off and it should work fine.

HighSpeed - March 17, 2010, 10:42 pm

I just can't get the database name to show up, after the

Object reference not set to an instance of an object.

Check if supports union

Object reference not set to an instance of an object.

Check if database version

thats the most i've seen so far after the visble text part

? Elektrisk ? - March 17, 2010, 10:42 pm

(Mar 17, 2010 10:40 PM)dylmyster22 Wrote: [\[CITE\]](#) cuz everytime i go to open the file, it gives me a pop up then when i click ignore it just closes it. and the others are to remove th infection and remove all unhealed infections. im running avg free 8.5

i can choose heal, move to vault, or ignore. the first two just deletes the program and ignore just does nothing.

AVG is very annoying when handling malware (as in, you are the handler). Switch to avast. It's very simple to disable, whereas AVG has no simple way of disabling it.

(Mar 17, 2010 10:41 PM)The Phlegethon Wrote: [\[CITE\]](#) Turn it off and it should work fine.

You can't easily turn off AVG.

Cabin Fever - March 17, 2010, 10:46 pm

Just get MalwareBytes instead.

CharlieSheen - March 17, 2010, 10:47 pm

ya gonna switch soon

? Elektrisk ? - March 17, 2010, 10:48 pm

(Mar 17, 2010 10:46 PM)The Phlegethon Wrote: [\[CITE\]](#) Just get MalwareBytes instead.

MalwareBytes is NOT an antivirus. It's an anti-malware scanner. MalwareBytes and an antivirus (such as avast) would be ideal, as well as a firewall, such as Online Armor or ZoneAlarm. Howevre, I've noticed that firewalls tend to be annoying to people who dab into malware often, 'cause they have to make sure their firewall isn't blocking ports, the program's access to the internet, and so on.

Cabin Fever - March 17, 2010, 10:52 pm

(Mar 17, 2010 10:48 PM)Elektrisk Wrote: [\[CITE\]](#) MalwareBytes is NOT an antivirus. It's an anti-malware scanner. MalwareBytes and an antivirus (such as avast) would be ideal, as well as a firewall, such as Online Armor or ZoneAlarm. Howevre, I've noticed that firewalls tend to be annoying to people who dab into malware often, 'cause they have to make sure their firewall isn't

blocking ports, the program's access to the internet, and so on.
Ahh, thanks for the correction. My mistake.

CharlieSheen - March 17, 2010, 10:53 pm

are the upgrade codes for avast good to be used multiple times or would i have to get a unique code to upgrade?

? Elektrisk ? - March 17, 2010, 10:54 pm

(Mar 17, 2010 10:53 PM)dylmyster22 Wrote: [\[CITE\]](#) are the upgrade codes for avast good to be used multiple times or would i have to get a unique code to upgrade?

Afaik, they can be used multiple times. However, the free version should be good enough. If not, just search warez-bb or serials.ws.

(Mar 17, 2010 10:52 PM)The Phlegethon Wrote: [\[CITE\]](#) Ahh, thanks for the correction. My mistake. Np. It's a common misconception.

CharlieSheen - March 17, 2010, 10:57 pm

finally got rid of avg and now i can open 2.7 =]

Cabin Fever - March 17, 2010, 10:59 pm

(Mar 17, 2010 10:57 PM)dylmyster22 Wrote: [\[CITE\]](#) finally got rid of avg and now i can open 2.7 =]
I knew it! :)

CharlieSheen - March 17, 2010, 11:00 pm

lol i had a feeling but ok its scanning again now in 2.7 so well see if it works now

Cabin Fever - March 17, 2010, 11:10 pm

Alright well thanks for posting your feedback and all. Glad I could help. Anyone else?

CharlieSheen - March 17, 2010, 11:25 pm

ugh this doesnt like me. will get all the way through, then in the end it wont let me get database. im gonna try this again in the morning. night

crack_that - March 17, 2010, 11:28 pm

very nice tut bro thank you very much

HighSpeed - March 17, 2010, 11:30 pm

yea same here, still can't get the database info to show up. Does it matter what OS it's on? I'm running it on vista.

? Elektrisk ? - March 17, 2010, 11:31 pm

(Mar 17, 2010 11:30 PM)HighSpeed Wrote: [\[CITE\]](#) yea same here, still can't get the database info to show up. Does it matter what OS it's on? I'm running it on vista.

It shouldn't matter. It works on XP. If you have an XP machine, I suggest trying on that.

Cabin Fever - March 17, 2010, 11:47 pm

(Mar 17, 2010 11:28 PM)crack_that Wrote: [\[CITE\]](#) very nice tut bro thank you very much
No problem, thank you for your feedback

Any suggestions on how I can make this tutorial better are also welcome.
Thanks.

Big.Eye - March 17, 2010, 11:48 pm

Wow this is awesome. ty dude

? Elektrisk ? - March 17, 2010, 11:51 pm

(Mar 17, 2010 11:47 PM)The Phlegethon Wrote: [\[CITE\]](#) No problem, thank you for your feedback

Any suggestions on how I can make this tutorial better are also welcome.

Thanks.

You should firstly spoiler your images. Also, you should declare each new step. For example:

Step #1:

First, you do this ...

Step #2:

Then, you do this ...

Also, put some color in the tutorial. Don't go crazy with it. Make sure the colors contrast well with the background and surrounding font colors. Also, use some italics/bold where necessary.

Also, use more line breaks. Keep sentences together so they are all relevant to each other in the same paragraph. Sentences that don't relate to other sentences should not be in the same paragraphs, if you get what I mean.

Good luck!

Cabin Fever - March 17, 2010, 11:52 pm

(Mar 17, 2010 11:51 PM)Elektrisk Wrote: [\[CITE\]](#) You should firstly spoiler your images. Also, you should declare each new step. For example:

Step #1:

First, you do this ...

Step #2:

Then, you do this ...

Also, put some color in the tutorial. Don't go crazy with it. Make sure the colors contrast well with the background and surrounding font colors. Also, use some italics/bold where necessary.

Also, use more line breaks. Keep sentences together so they are all relevant to each other in the same paragraph. Sentences that don't relate to other sentences should not be in the same paragraphs, if you get what I mean.

Good luck!

Thank you very much, I'll get to work organizing it right now!

SIM-209986 - March 18, 2010, 6:28 am

Thank you its very good! But 1. Question. Can i be traced while SQLI injection? I dont mean with defacement just with SQL?

? Elektrisk ? - March 18, 2010, 6:34 am

(Mar 18, 2010 06:28 AM)V~I~R~U~S Wrote: [\[CITE\]](#) Thank you its very good! But 1. Question. Can i be traced while SQLI injection? I dont mean with defacement just with SQL?

Technically, yes, since your IP is logged once you connect to the site. However, I don't think they'll be able to detect you doing anything wrong, as long as you don't change anything. Basically what you are doing when you get the password is exploiting the SQL vulnerability, and since they don't know that it exists (obviously), I doubt they are gonna notice.

Cabin Fever - March 18, 2010, 7:37 am

(Mar 18, 2010 06:28 AM)V~I~R~U~S Wrote: [\[CITE\]](#) Thank you its very good! But 1. Question. Can i be traced while SQLI injection? I dont mean with defacement just with SQL?

Yes, but they won't do anything (if they even think of doing anything) unless you log into the Admin account or upload a shell (if they are lucky enough to detect you before that). Once you upload the shell, delete the logs because your IP will stay in there, although it wouldn't matter if you're chaining proxies.

I_Learning_I - March 18, 2010, 7:54 am

This is a good tutorial, but you forgot to mention most websites will have the password hashed and many times even salted.

Which means it could be hard to get the real password, even those websites which have 13 billions passwords hashed probably have 0 passwords salted.

Other than that, it is nice, I sometimes use it, when I'm busy being lazy :P

Cabin Fever - March 18, 2010, 8:04 am

(Mar 18, 2010 07:54 AM)I_Learning_I Wrote: [\[CITE\]](#) This is a good tutorial, but you forgot to mention most websites will have the password hashed and many times even salted.

Which means it could be hard to get the real password, even those websites which have 13 billions passwords hashed probably have 0 passwords salted.

Other than that, it is nice, I sometimes use it, when I'm busy being lazy :P

No I didn't, it's at the bottom of the post. Thanks for your feedback.

hxkd - March 18, 2010, 11:01 am

Very good man.

hxkd

Cabin Fever - March 18, 2010, 12:37 pm

thank you :)

Did you try it out?

designedBy - March 18, 2010, 2:52 pm

Code Get Server Info

Check if URL is Vulnerable

URL is Vulnerable

Check No. of Columns

That loads, and it just stalls there until I hit stop. When I hit stop it shows some info, but no database.

Is it supposed to take a long time?

Cabin Fever - March 18, 2010, 3:09 pm

(Mar 18, 2010 02:52 PM)fear Wrote: [\[CITE\]](#) Code Get Server Info

Check if URL is Vulnerable

URL is Vulnerable

Check No. of Columns

That loads, and it just stalls there until I hit stop. When I hit stop it shows some info, but no database.

Is it supposed to take a long time?

Sometimes it takes a long time and sometimes it doesn't.

designedBy - March 18, 2010, 3:16 pm

When entering the URL for example:

<http://www.<sitehere>.com/index.php?page='11>

Should I leave it with the ' before the number, take the ' out, or put:

<http://www.<sitehere>.com/index.php?page=%2711>

(%27 being ')

Cabin Fever - March 18, 2010, 3:29 pm

(Mar 18, 2010 03:16 PM)fear Wrote: [\[CITE\]](#) When entering the URL for example:

<http://www.<sitehere>.com/index.php?page='11>

Should I leave it with the ' before the number, take the ' out, or put:

<http://www.<sitehere>.com/index.php?page=%2711>

(%27 being ')

Take 'em out.

designedBy - March 18, 2010, 3:30 pm

Alright thanks very much! :)

I'd rep you but I'm not sure I can.

designedBy - March 18, 2010, 4:39 pm

"Could not get no. of columns for unknown reasons, if you entered a 'true keyword' and nothing, get the columns manually"

Keep getting that on every one I do.

Any ideas?

? **Elektrisk ?** - March 18, 2010, 4:53 pm

(Mar 18, 2010 03:30 PM)fear Wrote: [\[CITE\]](#) Alright thanks very much! :)

I'd rep you but I'm not sure I can.

Only L33Ts and UB3Rs can rep.

(Mar 18, 2010 04:39 PM)fear Wrote: [\[CITE\]](#) "Could not get no. of columns for unknown reasons, if you entered a 'true keyword' and nothing, get the columns manually"

Keep getting that on every one I do.

Any ideas?

What are you entering for the target site? Give me the full URL.

designedBy - March 18, 2010, 5:02 pm

Nevermind, I tried another site and got it to work. Canceled after I got about 100 tables just in the letter a.

? **Elektrisk ?** - March 18, 2010, 5:03 pm

(Mar 18, 2010 05:02 PM)fear Wrote: [\[CITE\]](#) Nevermind, I tried another site and got it to work.

Canceled after I got about 100 tables just in the letter a.

LOL. I can think of few reasons why you would call a column 'a'. Someone needs to take a web development class?

Cabin Fever - March 18, 2010, 5:14 pm

(Mar 18, 2010 05:03 PM)Elektrisk Wrote: [\[CITE\]](#) LOL. I can think of few reasons why you would call a column 'a'. Someone needs to take a web development class?

Lol very true. After going through some of those sites and the way their databases are it has no order or anything lol

BroTard - March 18, 2010, 5:41 pm

Yea, Reiluke tools are pretty bitchen.

Cabin Fever - March 18, 2010, 5:44 pm

(Mar 18, 2010 05:41 PM)BroTard Wrote: [\[CITE\]](#) Yea, Reiluke tools are pretty bitchen.

Very much so ?

hacc - March 18, 2010, 5:45 pm

(Mar 17, 2010 06:36 PM)FillUp Wrote: [\[CITE\]](#) Got loads of trojan warnings on the SQLiHelper this.

and it shouldnt be like that its not a trojan builder or anything.

I dont recommend downloading these.

? Elektrisk ? - March 18, 2010, 5:46 pm

(Mar 18, 2010 05:45 PM)hac Wrote: [\[CITE\]](#) this.

and it shouldnt be like that its not a trojan builder or anything.

I dont recommend downloading these.

Wait, you're saying that a tool used to exploit vulnerabilities in a website and gain illegal access to their database is going to show up as malicious? NO WAY!

Cabin Fever - March 18, 2010, 5:50 pm

(Mar 18, 2010 05:45 PM)hac Wrote: [\[CITE\]](#) this.

and it shouldnt be like that its not a trojan builder or anything.

I dont recommend downloading these.

What a retard.. lol.

Plkdrmmr - March 18, 2010, 7:27 pm

wow using tools is for noobs

learn to do it yourself

Cabin Fever - March 18, 2010, 7:36 pm

(Mar 18, 2010 07:27 PM)Plkdrmmr Wrote: [\[CITE\]](#) wow using tools is for noobs

learn to do it yourself

LMAO, I've been knowing how to do this manually for years. Come back when you've grown up and had some common sense implanted in you.

? Elektrisk ? - March 18, 2010, 7:39 pm

(Mar 18, 2010 07:27 PM)Plkdrmmr Wrote: [\[CITE\]](#) wow using tools is for noobs learn to do it yourself
This has been addressed. Find your way out of the thread, thanks.

DID THE PORTAL WORK? - March 18, 2010, 7:40 pm
awesome tutorial man keep up the not so amazing work

? **Elektrisk ?** - March 18, 2010, 7:43 pm
(Mar 18, 2010 07:40 PM)DID THE PORTAL WORK? Wrote: [\[CITE\]](#) awesome tutorial man keep up the not so amazing work
I don't understand. So, do you think the tutorial is awesome or not?

Cabin Fever - March 18, 2010, 7:47 pm
(Mar 18, 2010 07:40 PM)DID THE PORTAL WORK? Wrote: [\[CITE\]](#) awesome tutorial man keep up the not so amazing work
Um, alright. It seems you have some mixed emotions there.

RiotousMind - March 18, 2010, 9:23 pm
When I click get columns, the windows stay blank. Any help?

MySocksAreWet - March 18, 2010, 9:26 pm
The injection tool is a little fucked, been scanning this link for 20min, should it take that long?

Cabin Fever - March 18, 2010, 9:29 pm
(Mar 18, 2010 09:26 PM)MySocksAreWet Wrote: [\[CITE\]](#) The injection tool is a little fucked, been scanning this link for 20min, should it take that long?
Lol I wouldn't wait more than 30 seconds.

MySocksAreWet - March 18, 2010, 9:30 pm
(Mar 18, 2010 09:29 PM)The Phlegethon Wrote: [\[CITE\]](#) Lol I wouldn't wait more than 30 seconds. I'll re-download and post results.

Cabin Fever - March 18, 2010, 9:40 pm
Alright I'll be here.

RobotzInDisguise - March 18, 2010, 9:53 pm
Everytime i test scan, nothing shows up in the right box:/

Cabin Fever - March 18, 2010, 10:12 pm
That seems to be happening with almost everyone but me.. it works perfectly for me.

CharlieSheen - March 18, 2010, 10:52 pm
give us some of the working links please. i cant get any working ones

xman111 - March 18, 2010, 11:26 pm
Got loads of trojan warnings on the SQLiHelper

Cabin Fever - March 18, 2010, 11:28 pm
(Mar 18, 2010 11:26 PM)xman111 Wrote: [\[CITE\]](#) Got loads of trojan warnings on the SQLiHelper
Lol, everyone did. Welcome to the club, it's a false-positive.

CharlieSheen - March 18, 2010, 11:30 pm
ugh i was so close. can you scan tis site? i tried in the exploit scanner and came up then i put in sqli

helper and it scas then stops again. sites

http://www.tulsaworld.com/news/article.aspx?subjectid=11&articleid=20100228_11_A21_JimGil721446

or tell us some ways you get so many working sites?

Cabin Fever - March 18, 2010, 11:32 pm

I don't know dude I don't do anything special, I do everything that you do lol

CharlieSheen - March 18, 2010, 11:34 pm

what dorks do you use?

Cabin Fever - March 18, 2010, 11:37 pm

look up google dorks in the search bar.

CharlieSheen - March 18, 2010, 11:57 pm

ok well still nothing =/

Drafted - March 19, 2010, 12:11 am

Might use this.. I wanted to learn how to deface.

pkdemon - March 23, 2010, 5:59 am

wow this is kewl

i like this method instead of all the dang typing :D

uchiha--itachi - March 23, 2010, 9:16 am

Well SQL is one of the best way

pROPER - March 23, 2010, 9:37 am

(Mar 17, 2010 06:21 PM)Elektrisk Wrote: [\[CITE\]](#) Admin page finder link is down. I rar'd all 3 programs.

<http://www.sendspace.com/file/bywylt>

Thanks for taking the time to write this.

Thanks ?

VizuaL - March 23, 2010, 10:26 am

S
K
I
D

Tutorial much? Do it the harder way and feel like you accomplished somethnig.

z3pt0seC - March 23, 2010, 10:36 am

if i could i would +rep you

Awesome tut

10/10

thanks

Cabin Fever - March 23, 2010, 10:56 am

(Mar 23, 2010 10:26 AM)VizuaL Wrote: [\[CITE\]](#) S

K

I
D

Tutorial much? Do it the harder way and feel like you accomplished somethnig.
Skid?

LOLLLLLLLLLLLLLOLLLLLLLLLLLLLOLLLLLLLLLLLLLOOOOOOOLLLLLLLLLLLLLLLLLLOLLLLLLLLLLLLLOLLL
LLLLLLLLLOLLLLLLLLLLLLLOLLLLLLLL

Why would I want to do it the hard way? That's like walking a far distance when I can just drive. You hypocrite, why don't you walk to school everyday instead of taking the bus? I'm assuming you're 12 by the way from your comments. And yes this is a tutorial, if you don't like it, gtfo.

th3 Loh1 - March 23, 2010, 11:06 am
thanks mate.....i will try it :) tahts for sure

? Elektrisk ? - March 23, 2010, 5:02 pm
(Mar 23, 2010 10:26 AM)VizuaL Wrote: [\[CITE\]](#) S
K
I
D

Tutorial much? Do it the harder way and feel like you accomplished somethnig.
That's like saying people should do math on paper instead of using a calculator. If someone knows how to do SQL injections manually, what is the harm in them using tools to automate the process? It's not like using the tools is going to make them magically lose the knowledge.

Bonza - April 1, 2010, 8:47 pm
Love it! thanks mate.

notahacker - April 3, 2010, 12:15 am
why does it always freeze up at "looking for largest visible text column"?

UnknownEdition - April 3, 2010, 12:32 am
Fast and noob SQL Injection!
If you do not know do manualy SQL Injection, you never not know do it!
Please this thread is for this section [SQL Injection Attacks](#)

notahacker - April 3, 2010, 12:44 am
How do you "get the columns manually"?
(Apr 3, 2010 12:32 AM)UnknownEdition Wrote: [\[CITE\]](#) Fast and noob SQL Injection!
If you do not know do manualy SQL Injection, you never not know do it!
Please this thread is for this section [SQL Injection Attacks](#)
Who cares, if it works?

UnknownEdition - April 3, 2010, 1:06 am
(Apr 3, 2010 12:44 AM)notahacker Wrote: [\[CITE\]](#) How do you "get the columns manually"?

Who cares, if it works?We must learn to do SQL injection, I do not think it is very difficult to learn it!

paw - April 3, 2010, 1:45 am
Nice post mate;p Really helpful REP+

ACDC - April 3, 2010, 1:41 pm

ive tried over 10 sites they all say there vunverable and does everything right and says succesful and at the end it says "Could not get no. of columns for unknown reasons, if you entered a 'true keyword' and nothing, get the columns manually" and when i click get columns nothing happens any help?

notahacker - April 4, 2010, 2:23 am

I'm having the same problem andy :(
sometimes it freezes up at "looking for largest visible text column" as well

demnas - April 4, 2010, 3:04 am

nice info brother.....!!!
i like this tool.....!!!

anythingga - April 15, 2010, 10:27 am

i cant open sqli helper 2.7 it says that i have innapropriate acces

tipliedown - April 15, 2010, 1:36 pm

doing manually is best to do

silvercola - April 15, 2010, 2:57 pm

before downloading it bitdefender cried virus

djovani - April 15, 2010, 4:19 pm

Nice, thanks for sharing bro

.Eli - May 3, 2010, 1:19 pm

This is a very very good tutorial, i didnt know hacking was so simple :)

Cabin Fever - June 1, 2010, 10:31 pm

(May 3, 2010 01:19 PM).Eli Wrote: [\[CITE\]](#) This is a very very good tutorial, i didnt know hacking was so simple :)

It can be this simple if people would only use their brain.

Suicidal Thoughts - June 2, 2010, 12:29 am

Nice tut man easy for beginners.
Keep it up.

My Life - June 2, 2010, 1:18 am

Nice one but its best when you doing it manually !

Cabin Fever - June 2, 2010, 11:58 am

(Jun 2, 2010 01:18 AM)WesternGuy Wrote: [\[CITE\]](#) Nice one but its best when you doing it manually !
Not if you already know how to do it.

Sector9 - June 2, 2010, 4:41 pm

I meant to say thanks for the tools.

Cabin Fever - June 3, 2010, 8:24 pm

(Jun 2, 2010 05:08 PM)PaNiK Wrote: [\[CITE\]](#) This tutorial sucks dick. Also, jackass OP tried to nominate it when the rules clearly state the tutorial should be from the last 30 days.
Why are you so upset? Lol.

illLusion - June 3, 2010, 8:48 pm

You guys, The SQIHelper given in here (I think) is a virus.

I will upload one that is not detected as a virus and is clean. I have gotten it a long time ago.

<http://www.mediafire.com/download.php?jdzmwmngd2u>

OP Feel free to put this in your download. :)

I'm 70% Sure the other has some sort of malware. mine zipped is only 123kb

The one in download is 348kb...

GL with your thread :D Thanks alot helped me.

axmetmcl - June 3, 2010, 9:50 pm

i think its the best sql injection tutorial ever in this HF.

Cabin Fever - June 3, 2010, 10:05 pm

(Jun 3, 2010 09:50 PM)axmetmcl Wrote: [\[CITE\]](#) i think its the best sql injection tutorial ever in this HF.

Lol, thanks for your feedback.

Mallow360 - June 4, 2010, 7:33 am

This works. Thank you so much.

I almost had a hard time following some other ones. But yours was simple for me.

Novatic - June 5, 2010, 3:36 pm

SQLi helper comes out as a virus, and look at your rep, no thank you.

darkcast - June 5, 2010, 4:03 pm

great tut. i was into the part were we are supposed to test the sites but i took more than 10 minutes and nothing was showing up. i this usual ?

VampyD - June 5, 2010, 5:20 pm

I wouldnt download this stuff -45 rep?

sopranosmohit - June 5, 2010, 11:20 pm

dude when i put any one of the sites from the vulnerability list, to the sql helper everytime it says the URL is not vulnerable. why>. Give me some site name or url which i can check this method on....

T 2 - June 13, 2010, 11:12 am

thanks mate, i just hacked a university website minute ago
its fucking easy

david316 - June 13, 2010, 11:17 am

Looks good,

I hope I wont mess up?

Im2Psychotic - June 13, 2010, 11:53 am

Wow why would you ever use this it takes all the fun out of SQLi not that its hard or very fun to begin with but i just don't get why people use this shit prove you're skill don't use skid tools.

Cabin Fever - June 13, 2010, 12:50 pm

(Jun 13, 2010 11:53 AM)Im2Psychotic Wrote: [\[CITE\]](#) Wow why would you ever use this it takes all the fun out of SQLi not that its hard or very fun to begin with but i just don't get why people use this

shit prove you're skill don't use skid tools.

Another dumbass who thinks he's l33t because he wastes his time doing something that he already knows how to do 10x slower.

Fucking idiot.

I proved my skill, I know how to do SQL, and I don't want to type in a whole bunch of shit that I already know how to do over and over again.

Get a fucking brain, kid.

(Jun 5, 2010 05:20 PM)VampyD Wrote: [\[CITE\]](#) I wouldent download this stuff -45 rep?
Haha, I was +30 rep when I made it.

DerekHubbard3000 - June 15, 2010, 12:06 am

it always says not vulnerable why

elvin4o - June 18, 2010, 3:58 am

thx .. for the malware inside. fuckin asshole

Cabin Fever - June 19, 2010, 7:14 pm

(Jun 18, 2010 03:58 AM)elvin4o Wrote: [\[CITE\]](#) thx .. for the malware inside. fuckin asshole
It's not Malware fucktard, it's a false positive.

Jesus 4k views, I am god!