

Forum:[Hack Forums](#)

Thread: [Dead Simple SQL Injection Tutorial \(With Havij\)](#)

Crypto™ - March 17, 2012, 3:49 pm

This is my short SQLi tutorial.

Please comment if you found it helpful!!!

[Download Havij](#). (There's both a free and paid version, but unless you're bound and determined to hack every site you find, go with the free version. It'll get the job done)

Find an injectible site. (Here's my method. Go to Google and type in `inurl:".php?id="`. This is what's known as a "dork". You can find/craft your own. :))

Test its injectability. (A lot of sites aren't injectible. Here's a quick trick for a preliminary check. Throw in a single quote. ' If it returns an error, it might be injectible.)

Throw the link into Havij. There's a box at the top (v1.15) for the URL.

Click analyze. (Simple enough)

Wait to see what it throws back. If it says the site isn't injectible, move on. Or if you know how, go for tactics like Blind SQL injection. (Not my style, too much hassle)

If it returns a DB name, click on the tab called "Tables".

Next, you can either look for more DBs (Click on Get DBs), or you can go straight to the tables of the current DB (Click on Get Tables).

Once you get down to tables for a specific DB, choose one and click on Get Columns.

Once you get down to columns, select the ones you want, and click Get Data.

You now have successfully SQLi'd a site (the n00b way, but it works)

ErrataIf you're retrieving passwords, they may be MD5'd. Luckily, Havij comes with a tool to try and crack them (It's a one way encryption standard with no known exploitable weaknesses). Copy down (Ctrl + C) the md5 of the password, then open the tab labeled "MD5". Paste it into the box and hit start. If it returns nothing, you have three options. One, give up. Two, Google it (recommended course of action). Three, spend hours/days/months/years obsessing over it attempting to find a way to crack it, including generating your own rainbow tables.

The URL you are attacking must already have a variable specified in it. E.g.
<http://www.site.com/something.php?id=1> This red part is the variable specification.

Not all variables make SQL requests, therefore, not all variables will work.

Links [Havij](#)

Lots of dorks for you [here](#), [here](#), [here](#), [here](#), and [here](#).

A great tut on how to find your own dorks and vulnerabilities: [here](#).

[Google](#)

Notes: For the sake of legality, I'll say I don't support any hacking except for educational purposes on systems you own. Yada yada yada FBI yada blah yada hacking yada yada yada big white van.

I'll add pictures to this eventually.

Razor96 - September 14, 2012, 8:00 am

Thanks for the info. I injected into the database of a local university.

Illicit - September 14, 2012, 8:11 am

Great TUT for...

[img]<http://t1.gstatic.com/images?q=tbn:ANd9GcSMld6-GxgTxAACoY-FiEzS9FQzTIH1PqpKi-tUtrV0Z7FbL3Lx/>[img]

keyloggerv3 - September 14, 2012, 8:15 am

Good tutorial for those who are 2 lazy to do sqli by hand.

I would highly suggest that you learn sqli by hand first so you get a good understanding of what havij is doing.

if you will just go and use havij from the start you're NOT a hacker, you are a skid.

Also remember that havij leaves alot more logs than you would do by doing the injection urself.

Elderum - October 12, 2012, 4:03 pm

really need to learn this sql malarky!

Crypto™ - October 13, 2012, 11:47 pm

If you want to learn how to do it the hard way, check out this guy's tuts.

<https://hackforums.net/showthread.php?tid=93224>

Sought - October 14, 2012, 12:12 pm

Nice tut but as many people say learn how to do it manually its much better

Smorgasbord_ - October 14, 2012, 1:05 pm

This program is great, i have used it for a while, i dont really understand why people think its nooby, why make it hard when its easy :)

jaycity23 - November 25, 2012, 10:55 am

I am having a bit of trouble doing this becuae i am using a mac. Could you please help me figure out how to use havij on a mac.

Thanks

zombiehacker - November 25, 2012, 10:56 am

Only skids like you use tools to hack, stop it.

phlow - November 25, 2012, 11:04 am

(Nov 25, 2012 11:55 AM)jaycity23 Wrote: [\[CITE\]](#) I am having a bit of trouble doing this becuae i am using a mac. Could you please help me figure out how to use havij on a mac.

Thanks

Learn to SQL Inject manually. You'd be doing yourself a favor.

j4rkill - November 25, 2012, 11:05 am

very very old 1337 Skill Tutorial ;)

jaycity23 - November 25, 2012, 11:10 am

(Nov 25, 2012 12:04 PM)EarlWolf Wrote: [\[CITE\]](#) Learn to SQL Inject manually. You'd be doing yourself a favor.

How would i go about learning how to do it manually? i would love to learn it and yes i am a noob

omiboss - November 25, 2012, 11:47 am

good tut...nice but can u upload videoo

Wú Yifán - November 25, 2012, 12:25 pm

Nice tut. Not much use to me or anyone else that's not a script kiddie. :P

MikoulFR - November 27, 2012, 10:29 am

Good Programm and tutoriel thank you ;)

midiiyawenyo - November 27, 2012, 11:02 am

This is not a good way to sqlinject, this is for skiddies.