

Forum:[Hack Forums](#)

Thread: [{Beta} FREE SQLi Bot - 10-minute SQLi v1.0](#)

SIM-1725686 - November 16, 2013, 2:19 pm

[img]<http://www.fgopl.tk/images/sqlibot.png>[/img]

SQLi in 10 minutes or less • Noob-friendly • Written in C#

v1.0 - Beta

100% FREE TO YOU!

Hello, everyone. I whipped this thing up today. Essentially, it's a helper that helps you pentest your site for SQLi vulnerabilities (Technically, any site, but this isn't necessarily a BH tool.).

Since this just the first version, and a beta, I'm providing it 100% free.

Features:

Automatic Query Completion

Easy-to-follow ToolTips and Guides

Quick Access to Yashar Shahinzadeh's Admin Finder

You don't pay a penny.

Virus-free

Drastic SQLi time decrease

Much more...!

Drawbacks:Column name and username:password display can not yet be automated

Only supports Windows

Unfortunately cannot perform the whole injection in one step

Virus scan: [Click](#)

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

<https://www.virustotal.com/en/file/3d4a2c71ab637b4c79db2b6cf62932f1371b63df29cedbb8b708a7b46ef7120f/analysis/1384636471/>

[img]<http://www.fgopl.tk/images/virtotal.png>[/img]

Screenshots:

Spoiler ([Click to View](#))

[img]http://www.fgopl.tk/sql/screen1.png[/img]

[img]http://www.fgopl.tk/sql/screen2.png[/img]

This code is obfuscated. No leeching allowed. <3

Download Mirrors:

Tell me if any of these are broken.

4Shared:

Spoiler ([Click to View](#))

http://www.4shared.com/file/EmYAXYjV/Injection_Bot.html

#:

Spoiler ([Click to View](#))

<http://#.com/share/571A67B1BD9C460059AB75A53D09FD39>

Direct Download Link:

Spoiler ([Click to View](#))

http://www.fgopl.tk/sql/Injection_Bot.exe

*If you're not comfortable with this link, give it a scan in your antivirus.

Cecilia - November 16, 2013, 2:33 pm

Does this use webbrowsers or http requests?

I've done a thing thats like this in PHP, yet it does do one query dumps.

SIM-1725686 - November 16, 2013, 2:39 pm

(Nov 16, 2013 03:33 PM)LaPanthere Wrote: [\[CITE\]](#) Does this use webbrowsers or http requests?

I've done a thing thats like this in PHP, yet it does do one query dumps.

This one uses WebBrowsers. They were ideal for this project, in that the form shows you the resulting page from your queries.

UserName - November 16, 2013, 2:41 pm

So all the program does is tells you what to type into the URL when you supply it with the data shown in the browser portion of the program?

SIM-1725686 - November 16, 2013, 2:46 pm

(Nov 16, 2013 03:41 PM)_UserName_ Wrote: [\[CITE\]](#) So all the program does is tells you what to type into the URL when you supply it with the data shown in the browser portion of the program?

Not exactly. It basically lets you perform a query with less characters than usual. Helps to shorten the process. There might be some bugs, but that's why it's a beta.

UserName - November 16, 2013, 4:05 pm

Is their WAF bypassing support?

I created something like this in Python, from the sound of it. Yet, mine didn't look as pretty as yours does.

SIM-1725686 - November 16, 2013, 4:09 pm

(Nov 16, 2013 05:05 PM)_UserName_ Wrote: [CITE](#) Is their WAF bypassing support?

I created something like this in Python, from the sound of it. Yet, mine didn't look as pretty as yours does.

As of now, there's no WAF bypassing. I'll probably include it in a full release. Didn't come to mind while I was writing it.