

Forum:[Hack Forums](#)

Thread: [\[New Update\] sqlinjector \[C++ | Free | Always Updated\] + Video](#)

dotcppfile - May 7, 2014, 10:44 am

Hello everyone,

sqlinjector v0.2 beta has been released

Updates:

- 1- Made a simple website where people can check updates (because I can't edit the HF thread since I am not L33t...) and download links of all versions: <http://sqlinjector.site88.net/>
- 2- Added an Automatic Version Checker. (makes sure you're using the newest version)

Picture:

Features:

- 1- Only works on Postgre Databases.
- 2- This is capable of doing everything when it comes to Postgre Databases, using Blind Injection, unlike other tools.
- 3- This is much faster than Havij, Sqlmap or similar tools.
- 4- Actually, those tools does barely support Postgre and you can test them yourself on the vulnerable link shared in my [Blind Postgre Sql Injection Tutorial](#) and you'll see that Havij and Sqlmap will fail while sqlinjector v0.1 beta will succeed.
- 5- It's programmed in C++, it works on all Windows Platforms.
- 6- Automatic Version Checker. (makes sure you're using the newest version)
- 7- This is currently just in beta so bare with me....

Upcoming Updates:

- 1- Mysql, Mssql and Oracle will be supported.
 - 2- Linux will be supported. (just let me finish getting rid of those Window's dependencies)
 - 3- It will also be released on Kali Linux.
 - 4- When it's completely done, the source will be released.
- (I will be adding whatever comes to my mind to this tool. If there's anything you want to see in the upcoming updates then just let me know.)

Videos:

[Video: <https://www.youtube.com/watch?v=OIMjyrh9nk>]

Website (so freaking simple):

<http://sqlinjector.site88.net/>

Download Link:

<http://up.ht/1kOMPdJ>

Scan:

<https://www.virustotal.com/en/file/5d1d83615085a53f6aad5a52722f4a52ce77ca6b22787442252ebf213e9ed7e9/analysis/1399555293/>

Know Errors:

Missing msvcp110.dll.

Just download the following: <http://www.microsoft.com/en-au/download/details.aspx?id=30679> and it should be fixed.

An update will be released soon to fix this.

Caution:

I can't update this thread later on because I am not a l33t...

Check the website of sqlinjector for any update or anything similar.

Also, I will be posting all kinds of updates as a normal reply to this thread.

Final words? Yep:

This is for Educational and Personal Use only, I take no responsibility on how you might use sqlinjector.

Special thanks to DownFall since together we worked on some researches related to Postgre.

Special thanks to everyone else who supported me in this thread:

<https://hackforums.net/showthread.php?tid=4212679>

If you like this tool and would like to support it then leaving a nice reply to keep the thread alive would be enough.

If you want to know how this tool does it all then check my tutorial.

Witness Happiness:

<http://www.youtube.com/watch?v=-yINYVIH6ME>

(Only 1 video allowed in a thread)

That's all for now,
dotcppfile.

protocolback - May 7, 2014, 11:07 am

is this open source? are you going to release the source?

#opensauce4life

WACKO - May 7, 2014, 11:15 am

This looks like a really nice tool. Good work dotcppfile.

dotcppfile - May 7, 2014, 11:26 am

(May 7, 2014 11:07 AM)protocolback Wrote: [\[CITE\]](#) is this open source? are you going to release the source?

#opensauce4life

I am not releasing the source right now but I will do so when this tool gets what it deserves and gets on Kali and Linux.

(May 7, 2014 11:15 AM)WACKO Wrote: [\[CITE\]](#) This looks like a really nice tool. Good work dotcppfile.

Thanks a lot WACKO, your support is much appreciated.

-DownFall - May 7, 2014, 11:27 am

Nice job on the release - might want to put some virus scans up on the thread though.

dotcppfile - May 7, 2014, 11:35 am

(May 7, 2014 11:27 AM)-DownFall Wrote: [\[CITE\]](#) Nice job on the release - might want to put some virus scans up on the thread though.

Thanks. Cool, I just added a link to the virus scan.

Kuky - May 7, 2014, 11:39 am

Havij handles PSQl perfectly. Whats another advantage to yours over havij?

dotcppfile - May 7, 2014, 11:40 am

(May 7, 2014 11:39 AM)Kuky Wrote: [\[CITE\]](#) Havij handles PSQl perfectly. Whats another advantage to yours over havij?

Check this out: <https://hackforums.net/showthread.php?tid=4195199> Havij couldn't handle that website... Also, sqlinjector is much much faster than Havij, etc.

jamilbt - May 7, 2014, 11:51 am

[img]http://farm8.staticflickr.com/7370/14132452735_3a7c121f83_b.jpg[/img]

error, why ?

dotcppfile - May 7, 2014, 11:59 am

(May 7, 2014 11:51 AM)jamilbt Wrote: [\[CITE\]](#) [img]<http://www.tase.go.th/tase/upload/13/e.jpg>[/img]

error, why ?

My Avs blocked your image for some reason... www.tase.go.th? Whatever...

Nord - May 7, 2014, 12:22 pm

(May 7, 2014 11:51 AM)jamilbt Wrote: [\[CITE\]](#) [img]<http://www.tase.go.th/tase/upload/13/e.jpg>[/img]

error, why ?

Same error for me, I have downloaded the dll but this msg still here

jamilbt - May 7, 2014, 12:45 pm

(May 7, 2014 11:59 AM)dotcppfile Wrote: [\[CITE\]](#) My Avs blocked your image for some reason... www.tase.go.th? Whatever...

check the image now..... ?

if still blocked, disable your Avs please.

dotcppfile - May 7, 2014, 12:47 pm

I checked the image with no AV and it seems I fucked up in the first version lol.

Anyways to fix this, you have to download the following:

<http://www.microsoft.com/en-au/download/details.aspx?id=30679>

I will release a fix for this soon.

limainfinita - May 8, 2014, 6:52 am

better than sqlmap and havij but only in Postgre Databases ?

thats a big statement to say, i'm really sceptical about this. but i will try it out.
thank you anyway.

dotcppfile - May 8, 2014, 8:51 am

(May 8, 2014 06:52 AM)limainfinita Wrote: [\[CITE\]](#) better than sqlmap and havij but only in Postgre Databases ?

thats a big statement to say, i'm really sceptical about this. but i will try it out.
thank you anyway.

For now it's only postgre, Mysql, mssql and Oracle will soon be added.

The newest version of sqlmap succeeds, the newest version of Havij fails, sqlinjector succeed with a faster speed.

Anyways, it's good you liked the tool.

sqlinjector v0.2 beta has been released

Updates:

- 1- Made a simple website where people can check updates (because I can't edit the HF thread since I am not L33t...) and download links of all versions: <http://sqlinjector.site88.net/>
- 2- Added an Automatic Version Checker. (makes sure you're using the newest version)

sqlinjector v0.3 beta has been released

Updates:

- 1- Mysql V5 is now supported.
 - 2- This has simply become the fastest tool out there. Check the new video out and you'll see (dumped a mysql database using blind sql injection within 30 seconds):
[Video: <https://www.youtube.com/watch?v=dO7QxeK7UUM>]
- And more is yet to come, please keep check of the official shitty(lol) website; it's where all the new updates, information etc will be added: <http://sqlinjector.site88.net/>

If you like this tool and if you want to support it then leaving a nice reply and keeping this thread alive would be enough.

JACK.HAMMER - May 9, 2014, 3:59 pm

nice job man its good tool keep it up pro :)

dotcppfile - May 10, 2014, 5:26 am

(May 9, 2014 03:59 PM)JACK.HAMMER Wrote: [\[CITE\]](#) nice job man its good tool keep it up pro :)
Thanks for the nice reply JACK.HAMMER, appreciated.

New Updates:

Updates:

- 1- Changed the name to CppSqlInjector
- 2- Updated the website to make it better and a little bit more clear.

News:

CppSqlInjector v0.4 beta will be released today with the support of Mssql or Opera(not sure which one to add yet lol)

Th3PonyWizard - May 10, 2014, 6:28 am

You chose one hell of a language to code an injector over, kodus. As for the speed, remember it'll always depend on the server response time target-wise hence at some cases the speed advantage won't matter. This is quite refreshing as a tool though, and good luck with it. I'll keep an eye open.

dotcppfile - May 10, 2014, 9:01 am

(May 10, 2014 06:28 AM)Th3PonyWizard Wrote: [\[CITE\]](#) You chose one hell of a language to code an injector over, kodus. As for the speed, remember it'll always depend on the server response time target-wise hence at some cases the speed advantage won't matter. This is quite refreshing as a tool though, and good luck with it. I'll keep an eye open.

C++ is one of the best languages out there and lets not forget about what it offers me when programming CppSqlInjector. About the speed thing, you're right; it is all about how fast the server responds to the request sent by CppSqlInjector but the power of the functions used in the tool, the way they work, their stability, how they stay in contact with the website and the way they act depending on what is given or received is also a huge fact when it comes to the speed of such tools. Anyways, I appreciate your reply and your interest, thanks.

News:

I did say I want to add a new feature to CppSqlInjector such as the support of Mssql or Opera today so I started working with Mssql on a localhost but it wasn't easy: I am using Xampp with php version >5 and microsoft doesn't really offer support to such versions so I had to use unofficial files to get it to work, I also got phpmsadmin and I set it up the right way.

The bad part is that I am in need of Microsoft Sql Server which is about 2gb(something like that) and I can't really download it today for many reasons related to the need of the full speed of my connection so I might work on this tomorrow or after tomorrow, but I got everything ready as you can see and I wrote a simple vulnerable php script as well.

In the mean while I am working on CppSqlInjector's functions related to Mssql but I can't test anything which means I won't be releasing CppSqlInjector v0.4 today so please bare with me.

dotcppfile - May 11, 2014, 2:03 pm

News:

1- Just got a free domain from co.nr : cppsqlinjector.co.nr and it is set up. I like it, it's much better than that site88.net thingy.

2- I promised you that CppSqlInjector will be supporting Mssql within few days and I will keep my word even though that Microsoft Sql Server is being such a bitch lol.

3- I may start Live Streaming about this for many reasons and one of these reasons is because I start talking to myself when working on CppSqlInjector late at nigh lol, so yeah, this has to stop lol.

Ch1m4zz - May 11, 2014, 2:04 pm

(May 11, 2014 02:03 PM)dotcppfile Wrote: [\[CITE\]](#) News:

1- Just got a free domain from co.nr : cppsqlinjector.co.nr and it is set up. I like it, it's much better than that site88.net thingy.

2- I promised you that CppSqlInjector will be supporting Mssql within few days and I will keep my word even though that Microsoft Sql Server is being such a bitch lol.

3- I may start Live Streaming about this for many reasons and one of these reasons is because I start talking to myself when working on CppSqlInjector late at nigh lol, so yeah, this has to stop lol. When are the Linux support coming? I really want it, and thanks for helping the community:D

dotcppfile - May 12, 2014, 4:33 am

(May 11, 2014 02:04 PM)Ch1m4zz Wrote: [\[CITE\]](#) When are the Linux support coming? I really want it, and thanks for helping the community:D

Not so soon because I am currently working on adding extra features and when it's out of beta I will get rid of those dependencies and put it on linux. Anyways, thanks for your interest, appreciated.

Ch1m4zz - May 12, 2014, 5:04 am

(May 12, 2014 04:33 AM)dotcppfile Wrote: [\[CITE\]](#) Not so soon because I am currently working on adding extra features and when it's out of beta I will get rid of those dependencies and put it on linux. Anyways, thanks for your interest, appreciated.

Ok, thanks for the information. I hope it will come soon I really don't use windows for hacking!):

giannis098 - May 12, 2014, 11:28 am

Im getting this error:

Software error:

Can't exec:

Column 'ip' cannot be null at Modules/DataBase.pm line 55.

dotcppfile - May 12, 2014, 11:11 pm

(May 12, 2014 11:28 AM)giannis098 Wrote: [\[CITE\]](#) Im getting this error:

Software error:

Can't exec:

Column 'ip' cannot be null at Modules/DataBase.pm line 55.

When are you getting this error giannis098?

By the way, who rated 1 star? I would like to know why...

News:

1- I've been lazy but it's all done when it comes to setting up everything related to Microsoft Sql Server. It's all working amazingly and currently I am working on the injection itself so give me sometime and bare with me.

2- I added a new simple feature which will allow CppSqlInjector to take down any vulnerable website(there's many websites that are vulnerable but all those tools out there doesn't realize it for many reasons, well, in CppSqlInjector you shouldn't worry about this anymore, this feature is still in beta but it is tested and it should work just fine).

3- CppSqlInjector v0.4 beta will be released soon.

News:

I already did most of it, it should be released tomorrow if I put some extra hard work into it.

dotcppfile - May 14, 2014, 10:01 am

News:

Okay this is not easy at all. I checked the official website of Havij and I realized that you have to buy the actual tool to get the support of a Blind Mssql Injection and now I know why lol.

So far, the things added are related to:

- 1- Grabbing the length of the version
- 2- Grabbing the version
- 3- Grabbing the length of the current database
- 4- Grabbing the current database
- 5- Grabbing the number of databases found
- 6- Grabbing the length of each found databases
- 7- Grabbing all of these databases

(I actually used some special queries that I will share with everyone sooner or later, those queries were never used before, when it comes to hacking or anything similar, and they should be helpful)

So, I still have to take care of the Tables and Columns and the Data but the Base of this Feature is Now Built and things should start getting a little bit easier for me.

Also, the speed is still the same, it's extremely fast and it does grab all I've stated before within 10 seconds which is nice.

That's all for today, I know I said I will be releasing this few days ago but I'm getting surprised each

and every time so bare with me and that's all.
dotcppfile.

cheatson - May 14, 2014, 11:22 am

(May 14, 2014 10:01 AM)dotcppfile Wrote: [\[CITE\]](#) News:
Okay this is not easy at all. I checked the official website of Havij and I realized that you have to buy the actual tool to get the support of a Blind Mssql Injection and now I know why lol.
So far, the things added are related to:
1- Grabbing the length of the version
2- Grabbing the version
3- Grabbing the length of the current database
4- Grabbing the current database
5- Grabbing the number of databases found
6- Grabbing the length of each found databases
7- Grabbing all of these databases
(I actually used some special queries that I will share with everyone sooner or later, those queries were never used before, when it comes to hacking or anything similar, and they should be helpful)

So, I still have to take care of the Tables and Columns and the Data but the Base of this Feature is Now Built and things should start getting a little bit easier for me.
Also, the speed is still the same, it's extremely fast and it does grab all I've stated before within 10 seconds which is nice.

That's all for today, I know I said I will be releasing this few days ago but I'm getting surprised each and every time so bare with me and that's all.
dotcppfile.Good things come to those who wait. :)

foreveralone1 - May 14, 2014, 12:28 pm

I will try and write a review for u :)

dotcppfile - May 14, 2014, 11:54 pm

(May 14, 2014 12:28 PM)foreveralone1 Wrote: [\[CITE\]](#) I will try and write a review for u :)
That's nice of you, thanks in advance.

(May 14, 2014 11:22 AM)cheatson Wrote: [\[CITE\]](#) Good things come to those who wait. :)
Old but gold. Thanks for the support cheatson.

Updates:

1- Full Mssql Support!
Actually, CppSqlInjector is the only Tool that Supports Blind Mssql Injection in Such Speed and For Free Unlike Havij that makes you Pay about 500\$ to get it or Sqlmap that makes you wait Hours to get your results.

Picture:

New Video:

[Video: <https://www.youtube.com/watch?v=poZpvGW9E9M>]

Download Link:

http://uppit.com/jehc9s1qk7sf/CppSqlInjector_v0.4_beta.rar

Virus Scan:

<https://www.virustotal.com/en/file/2de50b132c113e4db975fd182cb44e4b98df6dcb5aec6854a71046b8b7382409/analysis/1400177136/>

dotcppfile - May 16, 2014, 2:18 pm

Updates:

- 1- Added the Support of String with Blind Sql Injection.
- 2- Many bug Fixes. (Most of them were related to Mysql Blind Injection which Should make it Even Faster)
- 3- CppSqlInjector now has a WideR Connection with the user.
- 4- The Official Website has been updated with new Tabs: Updates Logs and Explanations

Download Link:

http://uppit.com/tl215kr6bref/CppSqlInjector_v0.5_beta.rar

Virus Scan:

<https://www.virustotal.com/en/file/5e46a61ce66f3ba95842f1a3fe973084d3e2d132e423cc928197c547f69512e5/analysis/1400272889/>

Some guy rated the thread 2 stars Without Even downloading CppSqlInjector v0.5 beta. That's awesome lol.

Anyways, I wanna thank everyone who's supporting CppSqlInjector, who's adding me on Skype and being nice because of this tool, who's giving me +rep, etc. I really appreciate all the support I am getting and as long as there's someone out there who's loving CppSqlInjector then this project will never die. Also, greets to Soap from Ubers . org who was supporting me out since the beginning.

Nothing but respect to all of you.

SohnGottes - May 16, 2014, 3:20 pm

(May 16, 2014 02:18 PM)dotcppfile Wrote: [\[CITE\]](#) Some guy rated the thread 2 stars Without Even downloading CppSqlInjector v0.5 beta. That's awesome lol.

Don't worry, there are always people who are childish and bored and probably live in a basement and try to destroy other people's work. I wouldn't really mind about ratings on HF. Sometimes you see an ub3r with like hundreds of +rep that has the intellect and behaviour of a 10 year old... quite common on HF.

I haven't tried your program, but it looks promising so just keep going if you believe in it and don't get irritated by the ratings ?

-DownFall - May 17, 2014, 12:26 am

Someone probably rated your thread low because it's an automated tool, which keep users from learning the right way. Even then, redirected to a "manual SQLi tutorial" doesn't teach them right. Just wish some people would take the time and do things the real manual way - fucking learn PHP and SQL, you wouldn't need to follow a tutorial or even slightly need the use of a tool. No point in ranting, those who do get their worth earned. Those who don't - well you see them everyday in web/forum hacking and the SQLi section making help threads. This is part of the reason I don't mentor users anymore in web hacking - there's just no effort put in. Overall nice tool, though I see

no point or need in using it - I brought your thread up to 3 stars from 1 the other day. Thanks for the effort;

-DownFall

dotcppfile - May 17, 2014, 2:22 am

(May 16, 2014 03:20 PM)SohnGottes Wrote: [\[CITE\]](#) Don't worry, there are always people who are childish and bored and probably live in a basement and try to destroy other people's work. I wouldn't really mind about ratings on HF. Sometimes you see an ub3r with like hundreds of +rep that has the intellect and behaviour of a 10 year old... quite common on HF.

I haven't tried your program, but it looks promising so just keep going if you believe in it and don't get irritated by the ratings ?

Thanks a lot for everything SohnGottes, I really mean that.

(May 17, 2014 12:26 AM)-DownFall Wrote: [\[CITE\]](#) Someone probably rated your thread low because it's an automated tool, which keep users from learning the right way. Even then, redirected to a "manual SQLi tutorial" doesn't teach them right. Just wish some people would take the time and do things the real manual way - fucking learn PHP and SQL, you wouldn't need to follow a tutorial or even slightly need the use of a tool. No point in ranting, those who do get their worth earned. Those who don't - well you see them everyday in web/forum hacking and the SQLi section making help threads. This is part of the reason I don't mentor users anymore in web hacking - there's just no effort put in. Overall nice tool, though I see no point or need in using it - I brought your thread up to 3 stars from 1 the other day. Thanks for the effort;

-DownFall

You're right, people should learn about sql injections and doing it manually is obviously the best choice but after all cppsqlinjector is about Blind Injection and I dont think anyone is a fan of extracting 1000 character from a database manually, it's not even interesting since all you have to do is to change a number or so and thats why CppSqlInjector was created.

Anyways DownFall, I knew someone rated this thread 5 starts right after I posted that old reply, but I never knew it was you, I appreciate that, I really do, thanks.

It seems there's a bug in the Blind and String Sql Injection feature. I will fix it asap.

Updates:

1- Fixed Multiply Bugs related to Blind and String Sql Injection

Download Link:

http://uppit.com/1eojtlu8abl1/CppSqlInjector_v0.6_beta.rar

Virus Scan:

<https://www.virustotal.com/en/file/16aca328f1adee01a96cb85098c90082b2fb7cb7b783cc4da50d565bf7436c9b/analysis/1400331778/>

pthnmj - May 17, 2014, 8:48 am

Uppit doesn't seem to be working.

Software error:

Can't exec:

Column 'ip' cannot be null at Modules/DataBase.pm line 55.

For help, please send mail to this site's webmaster, giving this error message and the time and date of the error.

dotcppfile - May 17, 2014, 1:15 pm

(May 17, 2014 08:48 AM)pthnmj Wrote: [\[CITE\]](#) Uppit doesn't seem to be working.

Software error:

Can't exec:

Column 'ip' cannot be null at Modules/DataBase.pm line 55.

For help, please send mail to this site's webmaster, giving this error message and the time and date of the error.

Uppit is working just fine but it's probably not for you, check your PMs, I will send you another download link.

Trig-Config-Maker - May 18, 2014, 12:03 am

uppit dont work for me either for some reason giving me column "ip" not valid lol

dotcppfile - May 18, 2014, 2:34 am

It seems that Uppit is causing a lot of problems.

Anyways, I will upload the files on the main host and program a simple counter to see how many people are downloading CppSqlInjector. I will start working on this ASAP, it should be done soon.

Updates:

I have updated the website, specifically downloads.html since people were having problems downloading the files from <http://uppit.com/>

I uploaded the files to the current webhost(SPAM) and I used <http://dstats.net/> as a Download Counter. I also added a simple Hit Counter on Index.html using <http://www.hit-counter-download.com> and the counting started from 100 (I know it's useless but it's cool).

News:

I just read that <http://dstats.net/> will record your IP whenever you try to download the file and I know that some people don't like that so screw it. I'll forget about the counters and I will add Direct Links to download the files.

Himanshu09 - May 18, 2014, 4:24 pm

Awesome work mate :D But i try this and MSVCP110D.DLL error i download this dll and put in system32 folder and also in same cppsqlinjector.exe dir folder bt still same error :/

dotcppfile - May 19, 2014, 2:28 am

(May 18, 2014 04:24 PM)Himanshu09 Wrote: [\[CITE\]](#) Awesome work mate :D But i try this and MSVCP110D.DLL error i download this dll and put in system32 folder and also in same cppsqlinjector.exe dir folder bt still same error :/

Do not download the .dll file. Go to cppsqlinjector.co.nr/downloads.html and in there you will find a link that you should download related to fixing this error.

highlyillegal - May 19, 2014, 3:47 am

I'd be interested in having a look at the source code for this project. Will it be released?

dotcppfile - May 19, 2014, 4:45 am

(May 19, 2014 03:47 AM)highlyillegal Wrote: [\[CITE\]](#) I'd be interested in having a look at the source code for this project. Will it be released?

The source wont be released now. It will be released whenever CppSqlInjector starts supporting Linux.

Trig-Config-Maker - May 19, 2014, 10:44 pm

i downloaded it and also the redistributable pack from microsoft and still have same error dll file missing, i have read that if ppl have vs2010 installed and its built with later version or earlier then it wont work properly?

dotcppfile - May 19, 2014, 10:59 pm

(May 19, 2014 10:44 PM)whitehatfriends1 Wrote: [\[CITE\]](#) i downloaded it and also the redistributable pack from microsoft and still have same error dll file missing, i have read that if ppl have vs2010 installed and its built with later version or earlier then it wont work properly?

The error can be easily fixed if you download and install the file related to the link shared on <http://cppsqlinjector.co.nr/downloads.html> This is the only fix for this error and it's 100% working so just make sure you're doing it right.

dotcppfile - May 21, 2014, 3:11 am

News:

I am currently working on an simple but really useful WAF bypassing function. The way it works is pretty neat and it's where the user inputs what he would like CppSqlInjector to use instead of another word such as Select. What CppSqlInjector will be supporting will be each and every word used in it's default queries which will give the user the power to manipulate the whole query. Now this should allow the user to successfully inject a website using CppSqlInjector most of the time. Although CppSqlInjector wont be supporting any kind of Encoding or Encryption or the Usage of a Completely New Query to bypass a WAF because I honestly think that when it comes to bypassing some really advanced WAF then it's time to do it manually even if it's a Blind Sql Injection.

There's also some upcoming plans on using TOR but that's not yet well thought about because I am willing to get CppSqlInjector on Linux first.

Also, nothing is planned yet for the support of Oracle's databases and that's because I never enjoyed working with it lol.

That's all for now,

Dotcppfile.

dotcppfile - June 10, 2014, 8:10 am

Updates:

- 1- Fixed a Huge Bug that was affecting CppSqlInjector's Vulnerability Detector.
- 2- Fixed another Huge Bug that was affecting String Injection.
- 3- Got rid of the "Missing msvcrt110.dll" Error.
- 4- Replaced Wininet by Curl which made things Faster and Better.
- 5- Got rid of Windows's Header File(Windows.h) completely and VERY Soon CppSqlInjector will be Released on Linux.

Download Link:

<http://cppsqlinjector.co.nr/downloads/CppSqlInjector%20v0.7%20Beta.rar>

Virus Scan:

<https://www.virustotal.com/en/file/707f398b8913c591eb84a248b77064c0c115ec5f667cb36617f3147be6895c96/analysis/1402412313/>

Ch1m4zz - June 10, 2014, 10:22 am

(Jun 10, 2014 08:10 AM)dotcppfile Wrote: [\[CITE\]](#) Updates:

- 1- Fixed a Huge Bug that was affecting CppSqlInjector's Vulnerability Detector.

- 2- Fixed another Huge Bug that was affecting String Injection.
- 3- Got rid of the "Missing msvcp110.dll" Error.
- 4- Replaced Wininet by Curl which made things Faster and Better.
- 5- Got rid of Windows's Header File(Windows.h) completely and VERY Soon CppSqlInjector will be Released on Linux.

Download Link:

<http://cppsqlinjector.co.nr/downloads/CppSqlInjector%20v0.7%20Beta.rar>

Virus Scan:

<https://www.virustotal.com/en/file/707f398b8913c591eb84a248b77064c0c115ec5f667cb36617f3147be6895c96/analysis/1402412313/>

YEEESSS

Soon to Linux! Thanks dude I've been waiting forever for this :D

dotcppfile - June 10, 2014, 4:21 pm

(Jun 10, 2014 10:22 AM)Ch1m4zz Wrote: [\[CITE\]](#) YEEESSS

Soon to Linux! Thanks dude I've been waiting forever for this :D

Thanks a lot for your great support m8. And yes, it will be released on linux within 10 days or so. I will work with multithreading first and then focus on Linux.

Ch1m4zz - June 10, 2014, 11:54 pm

(Jun 10, 2014 04:21 PM)dotcppfile Wrote: [\[CITE\]](#) Thanks a lot for your great support m8. And yes, it will be released on linux within 10 days or so. I will work with multithreading first and then focus on Linux.

Am I able to donate in OMC to you because of your great work?

I wish I could code with you but I'm a python coder

dotcppfile - June 11, 2014, 11:32 am

(Jun 10, 2014 11:54 PM)Ch1m4zz Wrote: [\[CITE\]](#) Am I able to donate in OMC to you because of your great work?

I wish I could code with you but I'm a python coder

I really appreciate that m8, thanks a lot for your support but I dont have anything related to OMC yet. Thanks again though.

YOLO - June 11, 2014, 4:37 pm

Looks like a really nice tool, going to download it tomorrow :)!

dotcppfile - June 12, 2014, 7:14 am

(Jun 11, 2014 04:37 PM)YOLO Wrote: [\[CITE\]](#) Looks like a really nice tool, going to download it tomorrow :)!

I am glad you liked it, thanks for your nice reply.

News:

So I will start working on Multi Threading which is something really important and CppSqlInjector is missing that so once it's setuped CppSqlInjector is going to be pretty fast and competitive.

Thanks all for your support, I really appreciate that.

Ch1m4zz - June 16, 2014, 10:12 am

(Jun 12, 2014 07:14 AM)dotcppfile Wrote: [\[CITE\]](#) I am glad you liked it, thanks for your nice reply.

News:

So I will start working on Multi Threading which is something really important and CppSqlInjector is missing that so once it's setuped CppSqlInjector is going to be pretty fast and competitive.

Thanks all for your support, I really appreciate that.

What's the appreciated time until linux version? And I really want this because I have a target to inject ?

Kitty - June 25, 2014, 1:24 pm

i get "... is not a valid win32 program" :(
thanks nonetheless, looks interesting!!~

dotcppfile - June 25, 2014, 1:31 pm

(Jun 25, 2014 01:24 PM)Kitty Wrote: [\[CITE\]](#) i get "... is not a valid win32 program" :(
thanks nonetheless, looks interesting!!~

It's been some time Kitty, how you doing?

Anyways, send me a picture of the error and I will tell you what to do.

casperr - June 25, 2014, 2:57 pm

Looks great ! Thanks for the share I will try .

Th3PonyWizard - June 26, 2014, 3:37 am

You do know who's going to port this beast to C once (and if) you'll release the source, right? I've figured out winsock2. C:

AntiPaste - June 26, 2014, 12:19 pm

Alright, I tested the tool out.

The method used for blind SQL injection is amongst the worst. It's using ASCII-based comparison, which means that it'll iterate over ASCII 126 to 32.

Assuming equal character distribution, this means it takes on average 47 requests for one character . In the worst case of the character being a space, it takes 94 requests for one character.

These numbers are high which makes the tool insanely slow. There are methods that take as little as 7 requests per character.

(May 7, 2014 10:44 AM)dotcppfile Wrote: [\[CITE\]](#) 3- This is much faster than Havij, Sqlmap or similar tools.

I compared the newest version of this tool against sqlmap. I forced sqlmap to be single-threaded to compare apples to apples.

I artificially slowed my connection down to get more accurate results.

The task was to dump a single value, 5 characters.

sqlmap dumped it in 1 minute and 3 seconds.

This tool took on average 1 minute 20 seconds per character. At the end it took this tool 6 minutes 39 seconds to dump 5 characters.

In conclusion, this tool is dreadfully slow. Until it's improved, I suggest you use better tools.

However, it's a good start. It does simple things and it does them without noticeable bugs. You shouldn't state things that aren't true though, e.g. claiming that it's faster than sqlmap.

NOTE: It will NOT take this tool 6 minutes 39 seconds to dump values in the real world. As said, I used an artificially slowed connection to get accurate results.

You should only look at the relative differences, which means that instead of thinking "This tool is 5 minutes 19 seconds slower!" you should think that it's ~498% slower.

dotcppfile - June 26, 2014, 1:37 pm

(Jun 26, 2014 12:19 PM)AntiPaste Wrote: [\[CITE\]](#) Alright, I tested the tool out.

The method used for blind SQL injection is amongst the worst. It's using ASCII-based comparison, which means that it'll iterate over ASCII 126 to 32.

Assuming equal character distribution, this means it takes on average 47 requests for one character. In the worst case of the character being a space, it takes 94 requests for one character.

These numbers are high which makes the tool insanely slow. There are methods that take as little as 7 requests per character.

I compared the newest version of this tool against sqlmap. I forced sqlmap to be single-threaded to compare apples to apples.

I artificially slowed my connection down to get more accurate results.

The task was to dump a single value, 5 characters.

sqlmap dumped it in 1 minute and 3 seconds.

This tool took on average 1 minute 20 seconds per character. At the end it took this tool 6 minutes 39 seconds to dump 5 characters.

In conclusion, this tool is dreadfully slow. Until it's improved, I suggest you use better tools.

However, it's a good start. It does simple things and it does them without noticeable bugs. You shouldn't state things that aren't true though, e.g. claiming that it's faster than sqlmap.

NOTE: It will NOT take this tool 6 minutes 39 seconds to dump values in the real world. As said, I used an artificially slowed connection to get accurate results.

You should only look at the relative differences, which means that instead of thinking "This tool is 5 minutes 19 seconds slower!" you should think that it's ~498% slower.

This took you some time mate, calculations, statistics, colors and stuff lol.

(Jun 26, 2014 12:19 PM)AntiPaste Wrote: [\[CITE\]](#) Alright, I tested the tool out.

The method used for blind SQL injection is amongst the worst. It's using ASCII-based comparison, which means that it'll iterate over ASCII 126 to 32. Well, ASCII Based Sql Injection is actually the best way to perform blind sql injection... Also, CppSqlInjector does it from 126 to 32, you probably used Wireshark to find that out, so good job lol.

(Jun 26, 2014 12:19 PM)AntiPaste Wrote: [\[CITE\]](#) Assuming equal character distribution, this means it takes on average 47 requests for one character. In the worst case of the character being a space, it takes 94 requests for one character.

These numbers are high which makes the tool insanely slow. There are methods that take as little as 7 requests per character. I am not sure what you're trying to say here but I can see that you're good at math which is a good thing lol.

CppSqlInjector goes threw all the characters as simple as that, I am not sure why are you trying to complicate this.

And about the method that uses 7 requests per character, well, it's jut another method and I won't be using it because the one that is currently being used is good enough.

Now for the rest of your post, I am not sure what to say tbh since it's kind of funny. Anyways, you slowed your connection down? to get better results? Well...

Also, CppSqlInjector is not slow at all, it is what it is, it is faster than the others and just because you used your l337 math skills in this, lol, this doesn't mean it's right. I really can't say anything else because then I would be going way too offensive, like calling this whole thing a fail post, something I don't feel like doing right now.

Now, I also would like to add few Extra stuff of CppSqlInjector's defense:

What makes CppSqlInjector actually special and unique would be:

1- The support of Blind MsSql Injection. Tools like Havij doesn't support Blind MsSql, only the premium version does which costs up to 500\$...

2- The fully functional support of Postgresql, Havij and Sqlmap doesn't care much about Postgresql while CppSqlInjector treats Blind Postgre Sql Injection as good as it treats the others. (In one of my old posts, a user, which is now a friend of mine I'm mentoring, couldn't use Blind Postgresql Injection threw Sqlmap, it was simply failing and that's when I decided to create CppSqlInjector v0.1 beta. Later on I decided to share my tool with the public and here it is)

3- CppSqlInjector is being updated all the time and it's still in beta. It's coded in C++ and it works on Windows and within 24 hours it will be released on Linux with Multi Threading which will make it really fast and effective. Unlike other tools like Havij that only works on Windows (that's why very few people uses it) and Sqlmap that has a "fucked up" windows version...

4- It's Free lol. I am not even asking anything in exchange, so if few people doesn't like it then I can't care less because I like it and a lot of people around there does as well...

CppSqlInjector is the best Blind Sql Injection tool out there, enough said, and god knows that all the supporters on skype, so whatever, are getting exactly what they're asking for. I've been updating this based on what's suggested and I'll keep doing that because CppSqlInjector deserves to stay on the top, as simple as that.

Tony S - June 26, 2014, 1:46 pm

(Jun 26, 2014 01:37 PM)dotcppfile Wrote: [\[CITE\]](#) CppSqlInjector is the best Blind Sql Injection tool out there, enough said, and god knows that all the supporters on skype, so whatever, are getting exactly what they're asking for. I've been updating this based on what's suggested and I'll keep doing that because CppSqlInjector deserves to stay on the top, as simple as that.

With an attitude like that to good user feedback it's going to stay anywhere but the top. You've demonstrated your level of ignorance and arrogance towards the community that you spent oh-so-long building this "tool" for, and I for one know that I will never stoop as low as to use a below-par tool such as CppSqlInjector.

Good day.

dotcppfile - June 26, 2014, 1:57 pm

(Jun 26, 2014 01:46 PM)Tony Spilotro Wrote: [\[CITE\]](#) With an attitude like that to good user feedback it's going to stay anywhere but the top. You've demonstrated your level of ignorance and arrogance towards the community that you spent oh-so-long building this "tool" for, and I for one know that I will never stoop as low as to use a below-par tool such as CppSqlInjector.

Good day.

(Jun 26, 2014 01:46 PM)Tony Spilotro Wrote: [\[CITE\]](#) You've demonstrated your level of ignorance and arrogance towards the community

I never did but if it makes you feel better then it's okay lol.

Also, what Anti Paste wrote wasn't really a feedback, it was an offensive post since I have him on skype and he simply told me that he will post this here on purpose so yh...

I talk to members from this community each and every day over skype, and they know I show respect to all of them and all these features were added because they asked for it so please...

Good day to you to lol.

AntiPaste - June 26, 2014, 2:28 pm

(Jun 26, 2014 01:37 PM)dotcppfile Wrote: [\[CITE\]](#) This took you some time mate, calculations, statistics, colors and stuff lol.

I like to research my arguments well and make my posts easy to read.

(Jun 26, 2014 01:37 PM)dotcppfile Wrote: [\[CITE\]](#) Well, ASCII Based Sql Injection is actually the best way to perform blind sql injection...

It's clearly not. It uses more queries, which means it's slow and noisy in logs.

(Jun 26, 2014 01:37 PM)dotcppfile Wrote: [\[CITE\]](#) I am not sure what you're trying to say here but I can see that you're good at math which is a good thing lol.

Actually the post required very little math, but thank you. ~

(Jun 26, 2014 01:37 PM)dotcppfile Wrote: [\[CITE\]](#) Anyways, you slowed your connection down? to get better results? Well...

I actually stated clearly, no less than two times, that I slowed it down to get more accurate results. Since I was running the tests on LAN both tools were completing their dump in seconds, which makes it hard to compare results.

(Jun 26, 2014 01:37 PM)dotcppfile Wrote: [\[CITE\]](#) Also, CppSqlInjector is not slow at all, it is what it is, it is faster than the others and just because you used your l337 math skills in this, lol, this doesn't mean it's right.

It's clearly not faster than sqlmap at least. I just proved it to you using an empirical method.

Also the fact that sqlmap utilises bit shifting while yours does ASCII-based comparison makes it impossible for your tool to be faster.

(Jun 26, 2014 01:37 PM)dotcppfile Wrote: [\[CITE\]](#) 2- The fully functional support of Postgresql, Havij and Sqlmap doesn't care much about Postgresql while CppSqlInjector treats Blind Postgre Sql Injection as good as it treats the others.

Incorrect. sqlmap boasts full PostgreSQL support as stated on their [website](#).

I just tested it on my own server and it worked fine. Perhaps you were using an old version or don't know how to use it?

(Jun 26, 2014 01:57 PM)dotcppfile Wrote: [\[CITE\]](#) Also, what Anti Paste wrote wasn't really a feedback, it was an offensive post since I have him on skype and he simply told me that he will post this here on purpose so yh...

How was that an offensive post?

I never said a single bad thing about your tool except proving your false statements about it's speed.

I even went as far to say this in the middle of my post:

(Jun 26, 2014 12:19 PM)AntiPaste Wrote: [\[CITE\]](#) However, it's a good start. It does simple things and it does them without noticeable bugs. You shouldn't state things that aren't true though, e.g. claiming that it's faster than sqlmap.

My whole post was about proving one of your statements wrong yet you take it as if I just called the entire thing a steaming pile of shit.

I also don't understand why you had to list reasons in the tool's defense when I didn't, in my previous post, question any of the facts you brought up.

dotcppfile - June 26, 2014, 2:51 pm

(Jun 26, 2014 02:28 PM)AntiPaste Wrote: [\[CITE\]](#) It's clearly not faster than sqlmap at least. I just proved it to you using an empirical method.

Also the fact that sqlmap utilises bit shifting while yours does ASCII-based comparison makes it impossible for your tool to be faster. Just because it's using low amount of queries then this doesn't mean it's faster... You're summarizing the whole tool by the queries it's using, it's like the rest of the 123123123 lines of codes are useless... Lol.

(Jun 26, 2014 02:28 PM)AntiPaste Wrote: [\[CITE\]](#) Incorrect. sqlmap boasts full PostgreSQL support as stated on their [website](#).

I just tested it on my own server and it worked fine. Perhaps you were using an old version or don't know how to use it? I am pretty sure using Sqlmap is really hard but I think I managed Lool.

As I said, it's weak, back in the days, a guy wanted to do a Blind Sql Injection on a website that uses Postgre and Havij/Sqlmap failed and that's when I decided to create CppSqlInjector and that's when we tested it on that website and that's when it worked.

Again, you're summarizing a whole topic in a query; just because Sqlmap solved a Sql Injection this doesn't make it better. There's tons of differences between a tool and another so please...

(Jun 26, 2014 02:28 PM)AntiPaste Wrote: [\[CITE\]](#) How was that an offensive post?

I never said a single bad thing about your tool except proving your false statements about it's speed.

I even went as far to say this in the middle of my post:

My whole post was about proving one of your statements wrong yet you take it as if I just called the entire thing a steaming pile of shit.

I also don't understand why you had to list reasons in the tool's defense when I didn't, in my previous post, question any of the facts you brought up.

You're whole post was offensive... You were not proving that one of my statements was wrong, you were trying your best to prove it's bad.

That's not how anyone would give their opinion about anything.

-ZYMOTOM' - June 26, 2014, 3:28 pm

(Jun 26, 2014 02:51 PM)dotcppfile Wrote: [\[CITE\]](#) Just because it's using low amount of queries then this doesn't mean it's faster... You're summarizing the whole tool by the queries it's using, it's like the rest of the 123123123 lines of codes are useless... Lol.

I am pretty sure using Sqlmap is really hard but I think I managed Lool.

As I said, it's weak, back in the days, a guy wanted to do a Blind Sql Injection on a website that uses Postgre and Havij/Sqlmap failed and that's when I decided to create CppSqlInjector and that's when we tested it on that website and that's when it worked.

Again, you're summarizing a whole topic in a query; just because Sqlmap solved a Sql Injection this doesn't make it better. There's tons of differences between a tool and another so please...

You're whole post was offensive... You were not proving that one of my statements was wrong, you were trying your best to prove it's bad.

That's not how anyone would give their opinion about anything.

First of all, he didn't say it only made it faster. Code in other places does not necessarily imply longer wait times either btw.

He ALSO said that it was more noisy in the logs, which it is if there are more queries. If you scroll through the accesslog and see pages and pages of someone making weird queries, well, yea, you'll be caught. On the other hand if you only make a few queries, it might go unnoticed.

Second of all, he did prove you wrong by providing statistics about both tools.

Third of all, how the hell was it offensive? Please, elaborate.

Th3PonyWizard - June 26, 2014, 3:30 pm

>this thread

[img]http://i921.photobucket.com/albums/ad60/moonlit-sonnet0/Animation%20and%20Comics/My%

20Little%20Pony/Friendship%20is%20Magic/Pinkie%20Pie/Popcorn.gif[/img]

no but for real, lets focus on making this thing better instead of debating about stuff we said. ^^

dotcppfile - June 26, 2014, 3:33 pm

(Jun 26, 2014 03:28 PM)-zYMTOM Wrote: [\[CITE\]](#) First of all, he didn't say it only made it faster. Code in other places does not necessarily imply longer wait times either btw.

He ALSO said that it was more noisy in the logs, which it is if there are more queries. If you scroll through the accesslog and see pages and pages of someone making weird queries, well, yea, you'll be caught. On the other hand if you only make a few queries, it might go unnoticed.

Second of all, he did prove you wrong by providing statistics about both tools.

Third of all, how the hell was it offensive? Please, elaborate.

You do realize that in a way or another it will be detected right? So if you use 100 queries instead of 100 then the logs won't be noisy anymore? You serious mate?

Check my old posts if you want to know what's my response for the rest of your reply; I am not typing that again.

(Jun 26, 2014 03:30 PM)Th3PonyWizard Wrote: [\[CITE\]](#) >this thread

[img]http://i921.photobucket.com/albums/ad60/moonlit-sonnet0/Animation%20and%20Comics/My%20Little%20Pony/Friendship%20is%20Magic/Pinkie%20Pie/Popcorn.gif[/img]

no but for real, lets focus on making this thing better instead of debating about stuff we said. ^^

I am not really going to care much anymore since they're just calling each others which is seriously stupid tbh.

Every time I check how this whole discussion started in the first place, it makes me think that I should have ignored Anti Paste in the first place because, right now, he's seriously trying to prove to everyone that he wasn't going offensive but he was giving his opinion.. Too late for that now Lol.

AntiPaste - June 26, 2014, 3:43 pm

(Jun 26, 2014 02:51 PM)dotcppfile Wrote: [\[CITE\]](#) Just because it's using low amount of queries then this doesn't mean it's faster... You're summarizing the whole tool by the queries it's using, it's like the rest of the 123123123 lines of codes are useless... Lol.

The main part of an injector is the method it uses to fetch data.

There's only so much you can optimise in the code before the connection becomes the bottleneck.

I have an average latency of 37 ms to en.wikipedia.org which is low compared to 100+ ms overseas.

The time it takes for the simplest HTTP request to an article to return the data is 255 ms.

I'd like to think that Wikipedia is very well optimised so 255 ms for a request is pretty good.

Lets assume a favourable scenario for your tool. The data that needs to be retrieved is all lowercase a - z, which is ASCII codes 97 - 122.

Because your tool starts at ASCII code 126, no matter what the data is you have to do 4 requests. The alphabet consists of 26 letters.

Assuming equal character distribution, your tool has to perform 17 queries $(4 + 26 / 2)$ per character while the optimal method is 7 queries per character.

Here's a table showing how character count affects the difference in time your tool has to make up for:

Clearly sqlmap's or any reasonable tool's code does not add 10 second overhead to the HTTP requests, looping or processing data.

This means that your tool will inevitably be slower than all the tools out there utilising the optimal 7-queries-per-character method.

(Jun 26, 2014 02:51 PM)dotcppfile Wrote: [\[CITE\]](#) As I said, it's weak, back in the days, a guy wanted to do a Blind Sql Injection on a website that uses Postgre and Havij/Sqlmap failed and that's when I decided to create CppSqlInjector and that's when we tested it on that website and that's when it worked.

Back in the days is how long ago? As I said, perhaps you were using an old version or didn't know how to use it.

I'd argue that sqlmap's support for PostgreSQL is as good as it gets.

Also, for the nth time I'm not saying or complaining about anything other than the speed.

Stop bringing irrelevant points to the topic if you want to discuss this further.

(Jun 26, 2014 02:51 PM)dotcppfile Wrote: [\[CITE\]](#) Again, you're summarizing a whole topic in a query; just because Sqlmap solved a Sql Injection this doesn't make it better. There's tons of differences between a tool and another so please...

I'm not summarising the whole topic in a query.

I'm trying to prove how your tool is not and cannot be faster than sqlmap or other tools utilising the optimal query method.

(Jun 26, 2014 02:51 PM)dotcppfile Wrote: [\[CITE\]](#) You're whole post was offensive... You were not proving that one of my statements was wrong, you were trying your best to prove it's bad.

Please quote one point in my post where I said anything negative about anything other than the speed, for which I had a reason.

The reason being that you claimed this tool is faster than sqlmap or any other tool.

-ZYMOTOM' - June 26, 2014, 3:45 pm

(Jun 26, 2014 03:33 PM)dotcppfile Wrote: [\[CITE\]](#) You do realize that in a way or another it will be detected right? So if you use 100 queries instead of 100 then the logs won't be noisy anymore? You serious mate?

Check my old posts if you want to know what's my response for the rest of your reply; I am not typing that again.

I am not really going to care much anymore since they're just calling each others which is seriously stupid tbh.

Every time I check how this whole discussion started in the first place, it makes me think that I should have ignored Anti Paste in the first place because, right now, he's seriously trying to prove to everyone that he wasn't going offensive but he was giving his opinion.. Too late for that now Lol.

You do realize you never actually responded to either of the last to questions in either of your posts. You only said "just because you have l33t math skills does not mean it's right", nothing actually disproving what he said about yours taking about 5 min.

The other thing you said was he said on skype that he would post it for the purpose of posting it, do you mean for the purpose of going on the offensive?

Other than that, who's calling who?

I do realize there are other ways to detect SQL injection. That is irrelevant though. But, more queries also equals to bigger chance of getting blocked by any protections.

dotcppfile - June 26, 2014, 4:00 pm

I've been replying post after post about the whole thing and you guys just come again and asks the same questions. Seriously, I have no time for this crap. I know that no matter what I write back you will always say the same thing over and over with few extra words that makes you feel better about yourself Lol.

The best way to end this useless and time wasting discussion would be this:

I was wrong, you never offended me or my 2 months work or my code or my queries or anything else, it's just that I feel this way every time someone shares his opinion about this in a huge post that mainly consist on making my work look shit, so please excuse me. Also, clearly CppSqlInjector is completely shitty since a guy with a formal accent and colorful posts is trying to prove that so I think I simply have to believe the fact that I'm not up for such a challenge and I also have to admit that I am a complete idiot because I will no longer be wasting my time trying to defend myself or anyone who chose CppSqlInjector over any other public tool.

I guess that's it. Lol.

-zYMTOM' - June 26, 2014, 4:03 pm

(Jun 26, 2014 04:00 PM)dotcppfile Wrote: [\[CITE\]](#) I've been replying post after post about the whole thing and you guys just come again and asks the same questions. Seriously, I have no time for this crap. I know that no matter what I write back you will always say the same thing over and over with few extra words that makes you feel better about yourself Lol.

The best way to end this useless and time wasting discussion would be this:

I was wrong, you never offended me or my 2 months work or my code or my queries or anything else, it's just that I feel this way every time someone shares his opinion about this in a huge post that mainly consist on making my work look shit, so please excuse me. Also, clearly CppSqlInjector is completely shitty since a guy with a formal accent and colorful posts is trying to prove that so I think I simply have to believe the fact that I'm not up for such a challenge and I also have to admit that I am a complete idiot because I will no longer be wasting my time trying to defend myself or anyone who chose CppSqlInjector over any other public tool.

I guess that's it. Lol.

You must be pretty dense, because you can't seem to understand that no one is telling you that your tool is shit. I give you props for doing what most people on HF can't actually do, which is to code a tool of their own and not just using what ever is advertised the most.

But, what he is doing is giving you genuine feedback and actually is only trying to disprove ONE of your statements, which was that your tool was faster than any others out there.

Also he questioned the statement about it being the best at postgresql, which I do as well but no one has tried to disprove that.

[EDIT]

Here's a tip, take the feedback and instead of just plainly ignoring his very valid posts, switch the method you're using to the most efficient one and from there make it so it's actually faster and better than any other tool out there, then you can be proud to call it "the fastest"

cheatson - June 26, 2014, 4:06 pm

It would be cool once you have the tool optimised dotcppfile to see more data verifying its speed over other established tools. Not to take away anything from the effort you are putting into it which I applaud, but better to take Antipaste's post as feedback. It's expected that claims over established tools like sqlmap would be tested and if the data supports exposed, that's healthy part of peer-review! If someone posted a tool claiming it faster than your own, it would be good to know there are people that care enough to spend there time investigating it :)

dotcppfile - June 26, 2014, 4:11 pm

(Jun 26, 2014 04:06 PM)cheatson Wrote: [\[CITE\]](#) It would be cool once you have the tool optimised dotcppfile to see more data verifying its speed over other established tools. Not to take away anything from the effort you are putting into it which I applaud, but better to take Antipaste's post as feedback. It's expected that claims over established tools like sqlmap would be tested and if the data supports exposed, that's healthy part of peer-review! If someone posted a tool claiming it faster than your own, it would be good to know there are people that care enough to spend there time investigating it :)

You've been supporting and giving opinion and suggestions from the beginning and I respect you mate but I have Anti Paste on my skype Lol, he could have just told me about it on skype and we could have discussed it but he simply wants to make a scene out of it which is seriously pathetic. I am seriously going to ignore any further reply coming from anyone that I think is being offensive and move on because I may not be good enough but I know I'm better then this crap, enough said.

AntiPaste - June 26, 2014, 4:20 pm

(Jun 26, 2014 04:11 PM)dotcppfile Wrote: [\[CITE\]](#) [...] but I have Anti Paste on my skype Lol, he could have just told me about it on skype and we could have discussed it but he simply wants to make a scene out of it which is seriously pathetic.

I did tell you. Your response was this:

[26/06/14 02:50:09] Hayden: If you use bit shifting you get the same result in 7 queries.

[26/06/14 02:51:14] dotcppfile LinuxFTW: there's no point tbh

[26/06/14 02:51:16] dotcppfile LinuxFTW: using ASCII

[26/06/14 02:51:22] dotcppfile LinuxFTW: is the best method for blind

Later...

[26/06/14 20:36:42] Hayden: The point is, your tool is 500% slower than sqlmap.

[26/06/14 20:36:47] dotcppfile LinuxFTW: nope

[26/06/14 20:36:49] Hayden: Yep.

[26/06/14 20:36:55] dotcppfile LinuxFTW: whatever makes you feel better mate

[26/06/14 20:36:56] dotcppfile LinuxFTW: lol

[26/06/14 20:37:23] Hayden: You want me to post a video for proof?

[26/06/14 20:37:34] dotcppfile LinuxFTW: I can't give a single fuck mate

[26/06/14 20:37:35] dotcppfile LinuxFTW: lol

I tried to convince you that your tool is way slower than sqlmap, and will be slower unless you change the query method.

I tried to give you proof on Skype, and I've tried to give you proof in this thread.

You've ignored all the evidence and simply posted non-sense replies. I'm done.

The truth is out there now, proving the statement you claim about this tool false. The users can now make an educated choice of the tool they use.

dotcppfile - June 26, 2014, 4:41 pm

(Jun 26, 2014 04:20 PM)AntiPaste Wrote: [\[CITE\]](#) I did tell you. Your response was this:

[26/06/14 02:50:09] Hayden: If you use bit shifting you get the same result in 7 queries.

[26/06/14 02:51:14] dotcppfile LinuxFTW: there's no point tbh

[26/06/14 02:51:16] dotcppfile LinuxFTW: using ASCII

[26/06/14 02:51:22] dotcppfile LinuxFTW: is the best method for blind

Later...

[26/06/14 20:36:42] Hayden: The point is, your tool is 500% slower than sqlmap.
[26/06/14 20:36:47] dotcppfile LinuxFTW: nope
[26/06/14 20:36:49] Hayden: Yep.
[26/06/14 20:36:55] dotcppfile LinuxFTW: whatever makes you feel better mate
[26/06/14 20:36:56] dotcppfile LinuxFTW: lol
[26/06/14 20:37:23] Hayden: You want me to post a video for proof?
[26/06/14 20:37:34] dotcppfile LinuxFTW: I can't give a single fuck mate
[26/06/14 20:37:35] dotcppfile LinuxFTW: lol

I tried to convince you that your tool is way slower than sqlmap, and will be slower unless you change the query method.

I tried to give you proof on Skype, and I've tried to give you proof in this thread.

You've ignored all the evidence and simply posted non-sense replies. I'm done.

The truth is out there now, proving the statement you claim about this tool false. The users can now make an educated choice of the tool they use.

Man you're literally pathetic, if thats how you start a discussion with someone then you have no manners. Also, thats not how this started at all.

Also, if all my replies were non sense according to you then I have nothing to say anymore lol.

And please stop acting smart you're seriously making us all lol out here.

I would have kept posting and defending myself but again I seriously have no time for this crap.

Anyways, you can feel happy about yourself and pretend that you proved your point but you know...
Lol.

-ZYMOTOM - June 26, 2014, 4:43 pm

(Jun 26, 2014 04:41 PM)dotcppfile Wrote: [\[CITE\]](#) Man you're literally pathetic, if thats how you start a discussion with someone then you have no manners. Also, thats not how this started at all.

Also, if all my replies were non sense according to you then I have nothing to say anymore lol.

And please stop acting smart you're seriously making us all lol out here.

I would have kept posting and defending myself but again I seriously have no time for this crap.

Anyways, you can feel happy about yourself and pretend that you proved your point but you know...
Lol.

Disprove his point, please. Disprove the statistics he posted.

If not, I rest my case.

dotcppfile - June 26, 2014, 5:00 pm

(Jun 26, 2014 04:43 PM)-ZYMOTOM Wrote: [\[CITE\]](#) Disprove his point, please. Disprove the statistics he posted.

If not, I rest my case.

I have nothing to disprove, his statistics are seriously useless and all the numbers and math and colors and shits he used are simply pathetic and I am not going to take that seriously at all. He's just here acting smart trying to prove his point no matter what, just like he tried yesterday in Team Prophetic's group chat were he made himself look like a joke and then left saying that the chat is making him lose braincells and that's when nobody gave a fuck tbh and 1 hour later he started talking to me in private telling me how shitty CppSqlInjector is and how dumb the methods used are and that's why I ignored him and everything you're seeing in this thread right now is probably because he's trying to feel better about himself.

Code Hayden: I don't see how your injector is different from any other.

Hayden: It even uses the dumb ASCII comparison for blind injection.(He clearly wasted his time using wireshark to check how CppSqlInjector works and ended up sending me this which is seriously pathetic)

He's not gonna rest because he can't accept the fact that he was wrong in many places, whether the way he talked about the problem or the way he wrote his posts so, whatever, and I really can't

give a single fuck about that.

It's not because I don't care about what others thinks; check all the posts in this thread and you'll know that I do listen to everything said but the way he's acting is simply stupid.

So again, I have no time for this crap. I am not trying to prove anything to anyone, the tool is here to stay whether you like it or not and whether you're trying to get people to use it or not because as long as there's one person finding it useful I will put it at the top... Enough said.

dotcppfile - June 29, 2014, 7:55 am

Update: CppSqlInjector v0.8 beta - Released

Added a new Version for Linux.

Added TOR Support.

Added an Automatic MultiThreading System.

CppSqlInjector is now Faster.

Fixed lots of Simple Bugs.

Only the Linux Version was Released.

The Windows Version will be Released later Today (I hope).

Also, the Automatic MultiThreading System is now only Available for MySql Injections. (I will be using the same thing for the rest but I am so tired today so it should be done within 2 days or so).

Download Link - Linux: <http://cppsqlinjector.co.nr/downloads/Linux/CppSqlInjector%20v0.8%20beta>

Kitty - June 29, 2014, 8:34 am

also one for win32? :praying: it doesn't run for me, if anyone has a working version plz msg me!!~

dotcppfile - June 29, 2014, 8:39 am

(Jun 29, 2014 08:34 AM)Kitty Wrote: [\[CITE\]](#) also one for win32? :praying: it doesn't run for me, if anyone has a working version plz msg me!!~

The windows version will be released at the end of this day.

I will seriously try to ditch Visual Studio because of all its crap when it comes to multi threading so whatever. I have to update my visual studio to get everything up and running the right way and I can't really do that at the moment so screw it Lol.

Anyways, I Will release the Windows Version today and it should work just fine for you.

mosby88 - June 29, 2014, 9:00 am

looks like a great tool, handsome good

dotcppfile - June 29, 2014, 1:23 pm

(Jun 29, 2014 09:00 AM)mosby88 Wrote: [\[CITE\]](#) looks like a great tool, handsome good
Thanks for support mate, appreciated.

News:

CppSqlInjector v0.8 beta has been just released on Windows, as promised.

I don't think any of you should be having problems running it right now.

It has the same features as the Linux Version.

The Versions are actually 100% Identical when it comes to Performance. (I used libraries available on both OSs by default which wasn't an easy task to deal with but it's worth it)

Update Logs: <http://cppsqlinjector.co.nr/updateslogs.html>

Download Link: <http://cppsqlinjector.co.nr/downloads.html>

Kitty - June 29, 2014, 1:50 pm

(Jun 29, 2014 01:23 PM)dotcppfile Wrote: [\[CITE\]](#) I don't think any of you should be having problems running it right now.

thank you very much but it doesn't work on win32. ?

dotcppfile - June 29, 2014, 2:08 pm

(Jun 29, 2014 01:50 PM)Kitty Wrote: [\[CITE\]](#) thank you very much but it doesn't work on win32. ?

I just fixed that threw Visual Studio so it should work, I think you're the only facing this problem. Add me on skype: dotcppfile

I will take a look at it.

TheNeutron - June 29, 2014, 4:10 pm

This look legit... Nice job sir, gonna check it out surely.

mr_IT21 - June 29, 2014, 6:23 pm

Looks promising! Thanks for the post

-Acid - June 30, 2014, 1:33 am

(Jun 29, 2014 01:23 PM)dotcppfile Wrote: [\[CITE\]](#) Thanks for support mate, appreciated.

News:

CppSqlInjector v0.8 beta has been just released on Windows, as promised.

I don't think any of you should be having problems running it right now.

It has the same features as the Linux Version.

The Versions are actually 100% Identical when it comes to Performance. (I used libraries available on both OSs by default which wasn't an easy task to deal with but it's worth it)

Update Logs: <http://cppsqlinjector.co.nr/updateslogs.html>

Download Link: <http://cppsqlinjector.co.nr/downloads.html> Worked for me ?

Very nice and i must say mate....you really deserves to be VIP member of HF ?

dotcppfile - June 30, 2014, 10:34 am

Great everyone likes it, I appreciate that.

A Rapier Guy - June 30, 2014, 3:09 pm

Will this only work on the postre database?

And how do i check if a site is vulner able?

dotcppfile - June 30, 2014, 3:13 pm

(Jun 30, 2014 03:09 PM)A Rapier Guy Wrote: [\[CITE\]](#) Will this only work on the postre database?

And how do i check if a site is vulner able?

This works on Postgresql, MySql, MsSql, I just cant edit the thread because I am not leet...

Check the official website for more info: cppsqlinjector.co.nr

Also, your second question is pretty weird, you need to learn SqlInjection mate because this question cannot be answered in a simple post.

Anyways, CppSqlInjector will check if your link is vulnerable and if it is, it will start sql injecting automatically, if not, it will ask you to give it another link.

?roxy - June 30, 2014, 8:45 pm

Can't seem to get through to your site.
Anyone else having this issue?

Proxy.

dotcppfile - July 1, 2014, 2:07 am

(Jun 30, 2014 08:45 PM)?roxy Wrote: [\[CITE\]](#) Can't seem to get through to your site.
Anyone else having this issue?

Proxy.

Actually I am using SPAM and for the domain I went for freedomain.co.nr.

If freedomain.co.nr is the problem then access the website threw this: <http://sqlinjector.site88.net/>

AccountsZone - July 1, 2014, 2:24 am

Just a suggestion, Add a Mass Dork Scanner :D

UNKNOWN - July 1, 2014, 1:41 pm

Sorry I'm new to this but

How would you use this program on this vulnerability?

<http://www.exploit-db.com/exploits/18056/>

Brooklyn Nights - July 1, 2014, 9:49 pm

This looks very good, downloading now.

SIM-1073426 - July 1, 2014, 10:08 pm

A Proxy and a Tor option would be nice once the program is finished.

dotcppfile - July 2, 2014, 2:39 am

(Jul 1, 2014 10:08 PM)Birkhoff Wrote: [\[CITE\]](#) A Proxy and a Tor option would be nice once the program is finished.

There is a Tor Option mate, it was added in the last update.

(Jul 1, 2014 01:41 PM)UNKNOWN Wrote: [\[CITE\]](#) Sorry I'm new to this but

How would you use this program on this vulnerability?

<http://www.exploit-db.com/exploits/18056/>

You just have to give it the vulnerable link and it will deal with the rest.

(Jul 1, 2014 09:49 PM)Brooklyn Nights Wrote: [\[CITE\]](#) This looks very good, downloading now.
It's great you liked it, thanks for posting.

mangdiabloz - July 4, 2014, 2:25 am

cool tool, thanx for this.. ill be using this in the future...

dotcppfile - July 6, 2014, 6:10 am

(Jul 4, 2014 02:25 AM)mangdiabloz Wrote: [\[CITE\]](#) cool tool, thanx for this.. ill be using this in the

future...

Great you liked it mate, thanks for posting.

News:

- 1- Automatic Multi Threading System added to Blind Postgre Sql Injection as well.
- 2- Added a Smart Character System which makes CppSqlInjector 5 times faster.
- 3- Automatic WAF Bypassing System is being added. It can bypass most of the WAFs out there. After all it's just a tool and it doesn't change queries or do anything similar advanced to bypass a WAF, it just focuses on UTF8 encoding, the usage of characters in different ways, dealing with spaces, dealing with parantheses and working around with comment tags etc.
- 4- Main Arguments are being implemented even though I never liked this but it's needed since there's a lot of inputs required already and more will be added later.
- 5- Fixing a Huge Bug which was causing a Memory Corruption Error while using CppSqlInjector caused by the Automatic Multi Threading System.

dotcppfile - July 7, 2014, 1:04 pm

Update:

- 1- Added a Smart Character System which makes v0.9 2.15 times faster than v0.8.
- 2- Added an Automatic WAF Bypassing System which is Capable of Bypassing most WAFs out there.
- 3- The Automatic MultiThreading System now supports Postgresql.
- 4- Added Main Arguments which should make the Usage of CppSqlInjector Faster and more Friendly.
- 5- Fixed a HUGE Bug caused by the Automatic MultiThreading System which was causing A Memory Corruption Error.
- 6- Fixed a Small Bug related to Identifying Vulnerable Links.

Picture:

You can find the Download Link at: <http://cppsqlinjector.co.nr/>

TheBob - July 8, 2014, 12:48 am

Thanks op! I will definitely be using this in the future.

saolaithe - July 8, 2014, 5:29 am

This looks like a really nice tool. I will try use it

SIM-1073426 - July 8, 2014, 8:11 am

For some reason OP is closed, anyone know why?

Sky - July 8, 2014, 8:24 am

(Jul 8, 2014 08:11 AM)Sons of Anarchy ?????????? Wrote: [\[CITE\]](#) For some reason OP is closed, anyone know why?

He cracked wise with Omni then came off worse for it.

~Arcane ?

maqu3n3r - July 8, 2014, 11:15 am

When i open the program it suddenly closes, do you know why?

Sky - July 8, 2014, 11:43 am

(Jul 8, 2014 11:15 AM)maqu3n3r Wrote: [\[CITE\]](#) When i open the program it suddenly closes, do you know why?

It uses arguments now. Run it from CMD.

~Arcane ?

maqu3n3r - July 8, 2014, 12:02 pm

(Jul 8, 2014 11:43 AM)Pernicious Arcane Wrote: [\[CITE\]](#) It uses arguments now. Run it from CMD.

~Arcane ?

Oh, thanks a lot for your help!! ?

Kitty - July 9, 2014, 7:26 am

Does anyone use this? Could you help me by PM because it won't work at my place (win32).

Sky - July 9, 2014, 7:29 am

(Jul 9, 2014 07:26 AM)Kitty Wrote: [\[CITE\]](#) Does anyone use this? Could you help me by PM because it won't work at my place (win32).

Run it from CMD, it works fine.

~Arcane ?

Kitty - July 9, 2014, 7:51 am

(Jul 9, 2014 07:29 AM)Pernicious Arcane Wrote: [\[CITE\]](#) Run it from CMD, it works fine.

~Arcane ?

It doesn't open from win32. I just want to get all table names from [here](#) using blind with this program (it's taking too long manually). ?

Cyrqisia - July 9, 2014, 8:21 am

nice job man its a very nice tool keep it up bro :)

lynxtech - July 10, 2014, 8:29 am

can't wait for the Mysql database update to come out for this!

mattybeds - July 27, 2014, 5:47 pm

Update:

Added a New Method; the Quotation Marks method. This method can be used with Multiply Vulnerabilities such as:

[vBulletin 5.1.2 Sql Injection](#) (released 4 days ago)

Added Extra Parameters which allows people to Dump what they're Only Looking For; Databases, Tables related to a Specific Schema, etc...

CppSqlInjector can now deal with "Multi Word" Data If it Exists.

Fixed a Bug in the Linux Version that wasn't allowing anyone to use the Tool Properly.

Fixed a Huge Bug related to getting the Length of Specific Data.

Picture:

News:

I know that a lot of people are waiting for a new version on Linux; I am getting PMs, DMs and Emails about this, but working on the same project twice is hard work indeed. Anyways, CppSqlInjector v1.1 beta Will be released within 24 hours on Linux. The Performance is Exactly the same on both Operating Systems and that's because both versions are using the Exact Same Libraries which also supports the fact that this Tool is Unique unlike any other Injector.

Download Link:

Can be found with a VirusTotal scan on: <http://cppsqlinjector.co.nr/>

Himanshu09 - July 27, 2014, 11:19 pm

bro need help... when i open file its opened and then automatically closed quickly :/ what should i do .. ?

MatiasMunk - July 27, 2014, 11:21 pm

It's a console application that takes arguments.

You have to run it through CMD with the required arguments to use it.

No offense, but if you don't know something as simple as this, you should stay away from hacking.

Himanshu09 - July 27, 2014, 11:44 pm

Mate i already try that.. but still same happens and Mate you looks like leet :D , Do you want try to fix it over TV ?

MatiasMunk - July 27, 2014, 11:51 pm

Please, it's a simple solution.. -.-

But I'm feeling generous today, so here's the solution;

Cmd -> cd PathToFile -> "CppSqlInjector v1.2 beta.exe" <http://www.site.com?search.php?id=1> -qM

Himanshu09 - July 27, 2014, 11:54 pm

COOOL :D I hope i may also help you one day anyway Thankyou so much Mate :D :D : D

MatiasMunk - July 28, 2014, 12:02 am

It's alright, no need to.

Just helping a fellow community member.

Just an advice; Go learn SQL & PHP and SQL Inject manually.

It's much cooler, and you'll become a more respected member if you do so.

Himanshu09 - July 28, 2014, 12:28 am

Yeah sure mate :D and i already learned sqli manually and now just started PHP from last week :D

SERPENT@ - July 28, 2014, 3:22 am

How can i use that with PROXY ???

Thanks

MatiasMunk - July 28, 2014, 10:29 am

@Himanshu09, no you didn't "learn" it already. You've probably memorized the commands for a simple error based SQL Injection Attack.

@Serpent@ You can either use the built in TOR function or you can download and use a VPN.

Tajmonekus - August 2, 2014, 2:36 am

A very useful tool, thank you :D I'm testing it out and comparing it to Havij

mattybeds - August 7, 2014, 7:18 pm

Updates:

Now it Can Inject it POST Requests.

Now it Can Inject in a Specific Parameter.

Now it Can Search for a Specific String while Comparing Pages.

Added the Support of a Mobile's User Agent Usage.

Added a Log Recorder.

Fixed a Huge Bug in the WAF Bypassing System.

Fixed many small but global bugs that were affecting the performance of CppSqlInjector.

Pictures:

Official Website:

<http://cppsqlinjector.co.nr/>

Ch1m4zz - August 8, 2014, 1:06 am

(Aug 7, 2014 07:18 PM)mattybeds Wrote: [\[CITE\]](#) Updates:

Now it Can Inject it POST Requests.

Now it Can Inject in a Specific Parameter.

Now it Can Search for a Specific String while Comparing Pages.

Added the Support of a Mobile's User Agent Usage.

Added a Log Recorder.

Fixed a Huge Bug in the WAF Bypassing System.

Fixed many small but global bugs that were affecting the performance of CppSqlInjector.

Pictures:

<http://cppsqlinjector.co.nr/> Thanks for the update Matty! It's legit and not a virus. I saw the development and he has contact with the original dev!

GOOD WORK , rep+ man , rly nice tool.

Great job and Interested also....may i have pls?? thanks in advance!!

Can't keep telling others to post for me Lol.

(Aug 10, 2014 08:52 PM)moklue Wrote: [\[CITE\]](#) Great job and Interested also....may i have pls?? thanks in advance!!

Thank you all for posting, your support is appreciated.

Updates:

Added "Smart Query Recognizer" which is going to allow CppSqlInjector to check if it's suppose to use ' or " or) or ' or " or)).

CppSqlInjector can now Find and Read PostgreSQL Log Files and Read PostgreSQL Config File.

Added the Power to dump Data from Multiply Columns; Example: username,password,

MsSql support has been removed temporarily, it will we be fully supported again soon.

The WAF Bypassing system has been Updated and now it can Bypass 90% of WAFs out there such as Mod Security etc...

CppSqlInjector is now A Lot Faster specially after BitShifting got Added.

Removed many useless stuff which should make the Shown Data look better.

Fixed many Bugs.

CAUTION: Do not forget to add the Comma from now on when Extracting Data from Columns;
Example: Write Down the Name of the Chosen Columns: passwords,

Pictures:

Official Website:

<http://cppsqlinjector.co.nr/>

robby_j - August 28, 2014, 12:43 pm

Windows 8.1 version 1.4 beta closing upon starting. Anyone have any idea on how to stop this from happening?

Sky - August 28, 2014, 1:31 pm

(Aug 28, 2014 12:43 PM)cl0ck Wrote: [\[CITE\]](#) Windows 8.1 version 1.4 beta closing upon starting. Anyone have any idea on how to stop this from happening?

Run it in CMD, it uses arguments now.

~Arcane ?

dotcppfile3 - September 30, 2014, 10:30 am

Release: CppSqlInjector v1.5 beta (Windows Only - the Linux version will be released soon)

Updates:

Now it can Remove and Add the MySql Comments at the end of every query.

Updated "Smart Query Recognizer" and now it Supports Alias Sql Injection.

Fixed the Simple "comma(,)" issue that was presented in v1.4 beta.

Fixed many Bugs.

Attention: Now you can Forget about this whole "comma(,)" thingy mentioned in v1.4 beta.

HaxingIsCool - October 25, 2014, 5:25 am

CppSqlInjector vs Sqlmap - Speed Test:

[Video: <https://www.youtube.com/watch?v=nk6xCENDL8E>]

zetaBoy - April 13, 2016, 12:08 pm

The link is dead is there anyone with the soft to reupload

sunip99 - December 13, 2018, 12:29 am

dose anyone stil have this ?reupload?