

Forum:[Hack Forums](#)

Thread: [{TUT} How to SQLi ComboLists](#)

nondescriptoldie - December 4, 2014, 11:25 am

Due to the amount of people nagging me and others saying "How to get Combo?" "How to crack accounts?" I have made this Tutorial dedicated to SQLing Combos.

REQUIRMENTS:

- 1) SQLi Dumper v.7.0(Sorry, you will need to find the program on google.
- 2) Google Dorks list. Find them here on HF or in my threads for some
- 3) VPN or RDP/VPS. I would get a RDP as they are fast, and have great internet.

How to do it:

Import your dorks into the top box and all all of your dorks.

Once you have added your dorks you have to click "Start Scanner"

The program will make and compile a LONG list of websites. (I recommend you leave it overnight)

Once you have the URLs loaded move to the "EXPLOITABLES TAB" and click "Start Exploitation" and I recommend you wait till it has finished ALL of the URLs.

Now move to the next tab called "Injectables" and do the same as before. Once you have a large amount of Injectable sites you need to Right click in a website in the list and click "Go to Dumper" and when you do this a Database will come up and click on the Database and click "Get Tables" once you get the tables look for where the users might be stored. Usually it would be "Users" or "Customers". Once you found the users click on it and click "Get Columns" and check the boxes next to "User and Pass" or "Email and Pass", then click DUMP DATA and you should see User names and Passwords coming up and then export the data! :) ?

NOTE:

Sometimes you might get a big website and they usually will get "Hashed Passwords" I would recommend you leave it although if you really want it use a cracker. Most of the time they will use MD5. Or they might use Salt although I wouldn't bother doing anything to these....yet.....

THANKS FOR READING AND ENJOY! :)

DontRep4Rep - December 4, 2014, 11:27 am

Thanks for this thread aha helped me out!!

nondescriptoldie - December 4, 2014, 11:28 am

(Dec 4, 2014 12:27 PM)Pinkponyprancer Wrote: [\[CITE\]](#) Thanks for this thread aha helped me out!!It is an easy method and I hope I helped you one step further with Sentry cracking! :) ? Wrote it just for you! ?

Bumper Sticker - December 4, 2014, 11:30 am

Thanks for the read, is this just like another Havij but with more websites?

nondescriptoldie - December 4, 2014, 11:37 am

(Dec 4, 2014 12:30 PM)Bumper Sticker Wrote: [\[CITE\]](#) Thanks for the read, is this just like another Havij but with more websites?It is used for combo lists and is like Havij in a way and is simpler and can be used automatically and finds websites for you! :)

ProblemSolva - December 6, 2014, 3:40 am

why you dont use sqlmap man ? its alot better then then these gui tools.
you can also use the tamper scripts to bypass WAF and IDS.

nondescriptoldie - December 6, 2014, 7:10 am

(Dec 6, 2014 04:40 AM)ProblemSolva Wrote: [\[CITE\]](#) why you dont use sqlmap man ? its alot better then then these gui tools.

you can also use the tamper scripts to bypass WAF and IDS.I can use SQLmap. I just wanted to share "this" method to others not the SQLmap method. ?

Although, I thank for your appreciation and reply to this thread! ?

Elena Gilbert - December 6, 2014, 8:31 am

So this is how we make wordlists for sentry MBA

nondescriptoldie - December 6, 2014, 10:19 am

(Dec 6, 2014 09:31 AM)DarkySoul Wrote: [\[CITE\]](#) So this is how we make wordlists for sentry MBA Pretty much bud, as loads of people requested me for this and wanted to share on how easy it is to SQL Combolists! ?

YoloSlime - September 18, 2015, 12:12 pm

hmm , i cant find dorks , cold you please link me ? tnx for tutorial !

nondescriptoldie - September 18, 2015, 12:32 pm

(Sep 18, 2015 12:12 PM)YoloSlime Wrote: [\[CITE\]](#) hmm , i cant find dorks , cold you please link me ? tnx for tutorial !Really?

You cannot find dorks? They are everywhere, go on google and type SQL dorks site:pastebin.com or just go on my threads and get some. ?

spirited_wolf™ - October 10, 2015, 9:15 pm

Thabkz bro my problem is solved now

but can you plz tell me how can i descrypt saltbased md5 hash

nondescriptoldie - October 11, 2015, 7:23 am

(Oct 10, 2015 09:15 PM)spirited_wolf Wrote: [\[CITE\]](#) Thabkz bro my problem is solved now

but can you plz tell me how can i descrypt saltbased md5 hashUse online and GPU.

And I would not waste time decrypting hashes unless its a big website. ?

nondescriptoldie - May 22, 2016, 2:52 am

(May 21, 2016 06:34 AM)JustDayo Wrote: [\[CITE\]](#) ... I got a website with 170k users, but the emails are obfuscated...obfuscated

Can you specify more on what you mean?

If you mean hashed, PM me, I can maybe help you out.

170k isn't that big, but we wil see what we can do