

Forum: [Hack Forums](#)

Thread: [\[NOOB FRIENDLY\] Make Your Own Combos: SQLi Dumper Tutorial \[PICTURES\]](#)

prosperhaven - July 14, 2020, 4:16 pm

Requirements:

A copy of SQLi Dumper

Download: https://anonfiles.com/Tdj5ibE9o9/SQLi_Du...PC-RET_zip
[WARNING POSSIBLY INFECTED]

A dork list. You do not need all of them; 1,000 is more than enough

Gaming Dorks: <https://throwbin.io/N0aaEgJ>

Shopping Dorks: <https://throwbin.io/n5U8wS5>

1) Once you have your dork list you can open up SQLi Dumper. Below is what it looks like:

In the picture you can see "inurl:" which is where you copy and paste your chosen dorks. If this is your first time using the program then the second part of the program where you see "https://" in a list will be blank for you, this is normal.

2) Now you are ready to start scanning, so in the bottom left of the program where it says "Start Scanner" with a big green play button, you hit it

Depending on how many dorks you have chosen to use and how many threads you set along with the internet speed and overall power of your PC this may take some time. You can leave it for a couple of hours to a couple of days.

3) You will have noticed that your 'Scanner' option on the left hand side has started to go up as mine does in the image below showing 23K links.

4) Click into your SQL Injection tab on the left hand side. Set the threads (I usually use 200) and click "Start Exploiter"

5) You will eventually see websites starting to fill up in the SQL Injection section of SQLi Dumper

Again the speed of this process completely depends on your internet speed and overall performance of your PC. Once this has finished running and checking all of the sites from your "scanner" list you can either double click any of the websites or right click and then click "Go Dumper"

6) You will be taken to the dumper module, which looks like this:

In your list you will see the database name for the MYSQL database the website you are exploiting

is using. You need to click the database name and then click the "Get columns" button.

This will start to pull through all the tables within that specific database. You are usually going to be looking for something along the lines of "users" "customers" "members" "logins" that type of thing. Some/a lot of websites/stores, etc will use prefixes too such as "pvt_users" "forum_members" etc.

7) When you have generated all the tables for your chosen website, you will then presented with something that looks similar to this:

Notice how I have already highlighted and found the "ns_users" table. This is the most likely place that the "email" and "password" columns will be stored and if we are looking to make a combo list that's exactly what we want.

Highlight over your chosen table and click "Get columns"

Now some websites may store their emails separately from the passwords (eg a forum that requires login via username and only stores emails for a newsletter) but this is still fine and User:Pass combo lists are still insanely useful. The website I have chosen is a User:Pass type of website.

Now you select the data you want to dump like the picture above and click the "dump data" button.

This will change your data dumper screen a little when it starts to gather the data from the columns. You should end up with something that looks like this:

For websites that have multiple tables (this has over 60) you will need to go through and keep searching until you find the one that is storing the user information. This table I have stumbled across appears to be for some type of admin login either with their CMS, shopping system or forum/blog. If you want to go down the route of exploiting their admin panel you certainly can and could even potentially gain access to the site and root the server and use for your own purposes along with being able to then strip the data of every other website hosted on that server.

This should get you moving with the basics of SQLi Dumper

Alieno539 - November 19, 2020, 2:53 pm

thank you soo much this guide is so complete