

Forum:[Hack Forums](#)

Thread: [Anyone Retrieving Databases?](#)

TetraHC - March 11, 2019, 2:34 pm

Anyone familiar with the tool dirsearch available on github if you use this please get in touch with me, or anyone who specifically retrieves databases of sites!

bravetoaster - March 12, 2019, 4:12 pm

(Mar 11, 2019 02:34 PM)TetraHC Wrote: [\[CITE\]](#) Anyone familiar with the tool dirsearch available on github if you use this please get in touch with me, or anyone who specifically retrieves databases of sites!

Pretty vague, but what is it specifically?

TetraHC - March 12, 2019, 4:29 pm

(Mar 12, 2019 04:12 PM)bravetoaster Wrote: [\[CITE\]](#) Pretty vague, but what is it specifically? what do you mean abit vague lol what more do you want me to tell you im looking for people who use the tool you obviously dont know what it is so why even comment?

bravetoaster - March 12, 2019, 4:42 pm

(Mar 12, 2019 04:29 PM)TetraHC Wrote: [\[CITE\]](#) what do you mean abit vague lol what more do you want me to tell you im looking for people who use the tool you obviously dont know what it is so why even comment?

Lol I know what it is, I meant its vague asking for anyone who gets DBs from sites. Like I guess I could have said it better, but was asking what the relation of that and DBs is and what you mean by that exactly. Getting DBs in what sense? Dropping tables? Finding them? Selling them? So since I'm here - I've used dirsearch before - and meet the criteria I listed regarding DBs whats up?

TetraHC - March 13, 2019, 6:50 am

(Mar 12, 2019 04:42 PM)bravetoaster Wrote: [\[CITE\]](#) Lol I know what it is, I meant its vague asking for anyone who gets DBs from sites. Like I guess I could have said it better, but was asking what the relation of that and DBs is and what you mean by that exactly. Getting DBs in what sense? Dropping tables? Finding them? Selling them? So since I'm here - I've used dirsearch before - and meet the criteria I listed regarding DBs whats up?

yo thats what im talking about lol why didnt u say this bro, i need put in the right direction on learning how to retrieve db's myself wether thats using the program dirsearch or uploading a shell i want to know how i go about doing this bud im new to it but really interested in learning

(Mar 12, 2019 04:42 PM)bravetoaster Wrote: [\[CITE\]](#) Lol I know what it is, I meant its vague asking for anyone who gets DBs from sites. Like I guess I could have said it better, but was asking what the relation of that and DBs is and what you mean by that exactly. Getting DBs in what sense? Dropping tables? Finding them? Selling them? So since I'm here - I've used dirsearch before - and meet the criteria I listed regarding DBs whats up?

and yes just to give you a better idea its for profit purposes thats what im intending to learn about

bravetoaster - March 14, 2019, 10:06 am

(Mar 13, 2019 06:50 AM)TetraHC Wrote: [\[CITE\]](#) yo thats what im talking about lol why didnt u say this bro, i need put in the right direction on learning how to retrieve db's myself wether thats using the program dirsearch or uploading a shell i want to know how i go about doing this bud im new to it but really interested in learning

and yes just to give you a better idea its for profit purposes thats what im intending to learn about Roger Roger. So that tool, dirbuster, and other fuzzing oriented tools help you find directories. They'll show you where things are they may not always be indexed, advertised, etc. Now to retrieve DBs...I've (no lie) had more success in randomly finding them with Google. You'd be surprised how many "Web Designers" are idiots. I'm a full-stack developer by trade. Lately my freelance work has had me "reparing" wordpress sites. Really what I've been is a fucking demo guy. I wipe the WP off the map because they're bullocks. I re-write the same site from scratch to be as "similar" as possible in my own code. To nick DBs you'll need more than a tool to find folders and a popular route is via SQL vulnerabilities. You can download a DB any way really but I've found more accidentally than on purpose, and most have ben acquired via some form of SQL manipulation. SO I'll go in hard here with some background....

Hacking a Database:

1.) Methods -

a. Password Guessing / brute force:(Tools included here could be Hydra, Burp's intruder, etc.) These would be valuable if you can get to the login page or prompt.

So your Dirsearch would be valuable here as you'd need to know here TO login before you can wrap your mind around HOW to login.

b. Server/System Vulnerabilities:

As I mentioned above you can go about it with SQLi (my preferred first try as databases are usually Oracle, MySQL, SQLITE, etc and relational DBs such as the ones above have a bleeding vulnerability wildly known to hackers - Injection. There are tools like SQLMap and others that can locate vulnerabilities and even exploit them. I prefer doing it by hand because that's half the fun. This occurs when developers or engineers don't validate input (aka sanitization.) As a developer my practicum is "Zero Trust" so I essentially plan for the worst case all the time. If someone can input data on a site you can guran-damn-tee someone is going to try to leverage it against you. Knowing how queries are structured help immensely, but it's not crazy complex. I'd suggest setting up a LAMP server and getting used to querying a database like MYSQL on something like a WordPress installation to get a feel for how it relates to front end processes, how queries work, etc. It help to know how to build something if you intend on breaking it. But short quick, point-and-click methodologies also pay off. If you just want to get your hands dirty start with " ' " - yes one single quotation. Add that to the end of the URL in the browser bar and if you get an ERROR message of any kind - Bob's your uncle. You can find "cheat sheets" online of popular queries and how to carry them out. Basically anywhere you can enter data is a place of interest. Logins and search bars especially. For example a poorly sanitized queery for a login page would allow me to type " admin" as a username and [FIREWALL BLOCKED THIS EXAMPLE ON HF] which would tell the database "[HF FIREWALL BLOCK] which logically is true so the statement returns TRUE as if you entered the proper password. Now there's endless ways to craft these so that's why it helps to know SQL. Know where data is sanitized, how to close off a statement and exploit it to resolve to your desires. This is the most popular way of attacking a database through the internet because it's usually started at a web application or website that the relational database is a backend to - If you want to learn about DBs this is a solid starting point, I have tons of material on it I could provide you if your interested...anyways, I digress

c. Installing a backdoor, malware, or rootkit:

I could write pages on this and if your newer to these topics I won't load you down with lots of confusion. There are libraries written on just this subject alone. You could deliver a payload via a phishing link/page, a JS hook in a crafted webpage to leverage some XSS vulnerabilities to work your way towards the DB, physical access with something like a USB Ducky or other USB delivery

methodology.

d. Windows NTLM authentication challenges can be exploited with MITM access.

The challenge response mechanism is vulnerable by default by all versions of MS use shit configurations and default setups - most people leave them this way. If you leverage MITM access somehow you can leverage that to carry out NTLM MITM attacks. Responder is a tool that can accomplish this (also once again back to the fact that if your newer to these types of terminology/ processes then don't worry to much about it, you'll drive yourself mad trying to learn everything)

SO I'm going to stop with examples there as those cover the most popular suspects in terms of what types, how, etc. If your new to the game I'll brief you on a TL:DR to set you kinda in the right direction here. Focus on SQL Injection if you want to know / nick DBs. It's the most common (the others are usually advanced actors, nation states, and other APTs that have resources, knowledge, and motivation to carry the complex methodologies out) Tool wise - SQL Map will be your friend for these purposes, there's loads of vids online going over how to use it properly. You'll also want to have a good recon technique. If your just randomly looking for things to nick then, my friend Google is your best friend and here's why - There are countless DBs online that aren't secure. They don't exactly need to be. The developers and owners of these things have one-track minds. They think that. "Oh we have secure passwords on the front-end, we're good" WRONG. I can't count the DBs I've come across by using specified google queries when I'm bored. This happens because the idiot "web designers" don't know what a fucking robots.txt page is and how to write one. I mean c'mon, it's not even code, it's fucking english. So what happens is Google crawls their page, and this includes the DBs that are accessed on the front end sometimes. So while their site may be secure - if you know the right URL parameters you can skip the process entirely and go straight shot- right to the baby maker.

I tried to include some example SQLi techniques and queries but upon trying to post I got a HF error page saying I triggered their firewall lol. So hey props to them because I wasn't even trying to break out, it was just amongst the rest of the text...Now I'm curious... Anyways, Look into SQL Injection, I can point you towards some good material, I even have loads myself. Look into Google Dorking, or Google Hacking as it's sometimes called. Basically I'm going to give you just what your asking for here - finding databases. Go to Google and type in the following " intitle:index of / & filetype:sql " the results of the search will be SQL DB dumps, or unsecured and indexable database pages. Be advised though there are plenty of honeynets honeypots and honey fucking everything out there. I am in InfoSec and I know the resources put into setting up 'traps' if you will. So if your going to browse around be smart, be careful, be vigilant of where you are. Don't do this on your main google profile. Make sure you're logged out as Google logs your searches. Make sure the "SYNC" function is off or you're on a different browser user. Use a VPN or a proxy, and don't get too excited if you find something cool and keep your wits about you. Let me know if there's any specifics you'd like me to go over, any resources you need pointed towards, or any you need sent your way. Best of luck mate, Cheers ?