

Forum:[Hack Forums](#)

Thread: [Best tool for sql injection using google dorks?](#)

giorgiomoroder11 - July 16, 2019, 11:35 am

SQL Dumper 8.2 only gets a certain amount of websites and doesn't get any others regardless of the dorks pasted into it.

Are there any other more advanced tools that would get more websites with the same dorks?

Black Day - July 17, 2019, 11:49 am

thank you bro so much nice

BreachingParrot - July 18, 2019, 5:42 am

What works great for me is using sqliv (github.com/the-robot/sqliv) it's a Python Tool which can scan multiple search engines with a provided dork and also does some vulnerable testing on its own..

Another great Tool is V3n0m-Scanner - which is a very fast Scanner that can scan hundreds of Dorks and also does automated vulnerability testing.

I usually also save all URLs that are deemed not vulnerable and explore them with tools like sqlmap. If you really want some big hits tho, you should always go for some manual exploring and invest more time into finding harder to find vulnerabilities.

Another thing that works great is after finding a vulnerable site is looking at the potential creator of the company (e.g. a Website Company) often times they reuse a lot of their stuff and you can break into every customer page of them.

xerox2018 - July 18, 2019, 7:33 am

are these tools you have mentioned freeware?

Sam Cart - July 29, 2019, 10:06 am

There's a tool out there for free that takes Google Dorks as an argument, it's called sqlmap. I'm sure you could hound it down on github or just install it from the linux repository if you happen to have Linux! The best part is you can set it in batch mode, which means it will just automate the process and will NOT require user input. This helps me cause I sell exploits to web servers so I have to deal with the "Quantity over Quality" deal. Let me know if this helps!

Demonik - July 29, 2019, 1:54 pm

(Jul 18, 2019 07:33 AM)xerox2018 Wrote: [\[CITE\]](#) are these tools you have mentioned freeware? Lol its the internet... Everything is free ;)

noupzy - August 2, 2020, 4:07 am

(Jul 18, 2019 05:42 AM)BreachingParrot Wrote: [\[CITE\]](#) What works great for me is using sqliv (github.com/the-robot/sqliv) it's a Python Tool which can scan multiple search engines with a provided dork and also does some vulnerable testing on its own..

Another great Tool is V3n0m-Scanner - which is a very fast Scanner that can scan hundreds of Dorks and also does automated vulnerability testing.

I usually also save all URLs that are deemed not vulnerable and explore them with tools like sqlmap. If you really want some big hits tho, you should always go for some manual exploring and invest more time into finding harder to find vulnerabilities.

Another thing that works great is after finding a vulnerable site is looking at the potential creator of the company (e.g. a Website Company) often times they reuse a lot of their stuff and you can break into every customer page of them.

Thanks for this