

Forum:[Hack Forums](#)

Thread: [Script that finds vulnerable sites and outputs urls to file?](#)

DoxM3 - April 29, 2017, 5:49 pm

All that would be needed is an option to input a dork and it should go to google, input `inurl:*dork here*` and go to every url, add a ', and search the webpage that's loaded after inputting the ' for sql and if sql is a word on the page it be output to a file.

At least that's how I'd think it should work, I'm sure there is something like this around right? I tried googling but didn't find much.. I'm sure it could be done wit imacros or something right? I know a little python and c but I doubt that would be useful when it comes to something like this.

pomwtin - April 29, 2017, 5:55 pm

(Apr 29, 2017 05:49 PM)DoxM3 Wrote: [\[CITE\]](#) All that would be needed is an option to input a dork and it should go to google, input `inurl:*dork here*` and go to every url, add a ', and search the webpage that's loaded after inputting the ' for sql and if sql is a word on the page it be output to a file.

At least that's how I'd think it should work, I'm sure there is something like this around right? I tried googling but didn't find much.. I'm sure it could be done wit imacros or something right? I know a little python and c but I doubt that would be useful when it comes to something like this.

Python and curl (pycurl) would do just fine. Fairly easy to implement

Triops - April 29, 2017, 5:59 pm

(Apr 29, 2017 05:55 PM)pomwtin Wrote: [\[CITE\]](#) Python and curl (pycurl) would do just fine. Fairly easy to implement

Any idea if I could make a script in Python that'd exploit websites that have an XPath Error Based vulnerability?

DoxM3 - April 30, 2017, 11:54 am

(Apr 29, 2017 05:55 PM)pomwtin Wrote: [\[CITE\]](#) Python and curl (pycurl) would do just fine. Fairly easy to implement

PM'd you but I don't really know how to do things like this I just know functions and general stuff with python.

Clutch - April 30, 2017, 12:42 pm

Just use Sqlmap. It lets you input a Google dork instead of a URL.

DoxM3 - April 30, 2017, 12:44 pm

(Apr 30, 2017 12:42 PM)Clutch Wrote: [\[CITE\]](#) Just use Sqlmap. It lets you input a Google dork instead of a URL.

I didn't know that was an option on SQLMap, thanks, man!