

Forum:[Hack Forums](#)

Thread: [Finding Vulnerabilities With Google Dorks \(FREE, No Downloads\)](#)

Hackers - January 7, 2024, 7:17 am

Using "Google Dorks" to find vulnerabilities has been a long-time, known method for finding "hacks". However, I can't stress enough how easy & useful it is to this day. In fact, I just used two dorks to see if this type of method still works. On the 2nd try, I found a site and was in their admin panel within a minute. I will not reveal the site, or use it, because to be honest it was a complete accident - I was just trying to see if my old login details of admin:admin worked, and it did!

What is a Google Dork?

- No, it's not me although I am a bit of a dork who uses Google.

It's a useful way of searching Google for specific info. Here are some examples:

Code inurl:hackforums.net This will only show me links that include "hackforums.net" in it.

Code site:hackforums.net This will only show me links from HF, and no other sites.

Code intitle:"White Hat Hacking" This will only show me pages that have White Hat Hacking in the title.

Let's combine some dorks - let's find a page on only Hackforums.net:

Code site:hackforums.net intitle:"White Hat Hacking" You can see that works here:

Now, how to find hacks? Well, this is only a case of knowing about a vulnerability and then using a Google dork to find it. For example, if we knew that a page titled "My Insecure Admin Demo" is hackable, we could use the dork intitle: "My Insecure Admin Demo" to find websites still hosting that page.

For example, certain admin panels have a default login of admin:admin, and using a dork would be on way to find sites still using that software to check it out:

Spoiler ([Click to View](#))

Dork:

Code intitle:"Sphider Admin Login"

Login with user 'admin', and password 'admin'.

Remember, this is only for educational purposes for your own pentesting, securing your own servers, and helping others secure their servers. How you use this information is up to you, and my intent is for you to learn from this method, not to hack innocent people. Please be kind!

Here are some specific dorks you can use to see if your site is secure or not:
(keep in mind there are many duplicates across these different links)

<https://www.bboxpiper.com/posts/google-dork-list-advisories-and-vulnerabilities>

<https://github.com/TomMalvoRiddle/google-dorks-1/blob/main/Google%20Dorks%20List%20and%20Updated%20Database%20in%202022.txt>

<https://medium.com/@rkpr0xy13/google-dorks-list-and-updated-database-in-2023-1dc6934f9415>

<https://www.bboxpiper.com/posts/google-dork-list>

<https://gbhackers.com/latest-google-dorks-list/>