Google Dorks

John Bocook Follow
Sep 21, 2016 · 2 min read

I have a system administrator friend that asked if there was an easy way to compile a list of companies that use a specific online platform and how we could go about finding them. My response … **Google Dorks**!

Google Dork?

A Google Dork involves using advanced operators in the Google search engine to locate specific strings of text within search results. Most people call this Google hacking and use these searches to find specific versions of vulnerable Web applications.

Calling these searches *hacking* is the same as saying you drive a Cadillac when really it’s a 1980s Oldsmobile. Sure they both have chassis auto-leveling and sirrea grain leather but it’s still an Oldsmobile and your still not a hacker.

Search Modifiers

So—Now that you know *what* a google dork search is, how can we use these to find what we are looking for? Well Young Padawan, it all depends on what your searching for. For my buddy, we needed to find any **college university** that is using the **Edvance360 Learning Management System** (LMS) kicking us off by only needing .edu domain names. This is accomplished by using the **site:** search modifier. **site:edu** commands almighty google to search *only* inside results for domain names ending in edu.

We are now limiting to only educational websites. Next is to find who out of .edu list runs the e360 platform. Hello **intitle:**, you sexy seven letter fox. Adding intitle: to the search will only return results that contain the text we are looking for. Combined with site: our search is now super focused. Using multiple modifiers or swapping modifiers out for others will return different search results allowing you to build your list.

> Complete search returning .edu sites that have a page containing "edvance360"
> **site:edu intitle:"edvance360"**

To get the best results think about what the system in question gives you. Would the organization have specific text on a page linking to the system - **intext:”edvancee360"**.

How about standardized footer text?
- **intext:”powered by mailgust”**

Sensitive Directories?
- **inurl:trash%20intitle:index.of**

Additional Resources

A few resources to begin your journey. You can use modifiers to search for filetypes, directory names, and pretty much anything else you can think of.

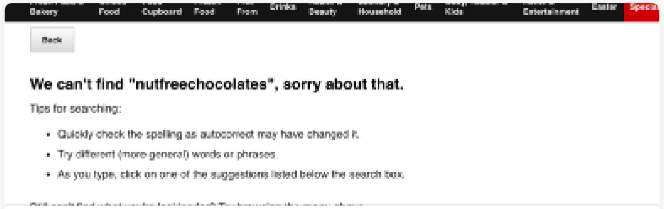
10 Clever Google Search Tips
SQL Injection Examples
Google Hacking Database

Search Google Query Hacking Security

John Bocook

I’m a Christian, Husband and Father. Oh and I write code for a living.

Follow



Back

We can't find "nutfreechocolates", sorry about that.

Tips for searching:

- Quickly check the spelling as autocorrect may have changed it.
- Try different (more general) words or phrases.
- As you type, click on one of the suggestions listed below the search box.

Also tagged Search ★

Query Segmentation and Spelling Correction

Sonu Sharma

Apr 23 · 8 min read ★

1

Also tagged Query ★

Implementing GraphQL: A Journey to the Underworld

Nisha Chatterjee

Apr 18 · 4 min read ★

243

Top on Medium ★

The Price We Pay for Multitasking at Work

David Staab

Apr 22 · 8 min read

3.6K

Responses

Write a response…