Google Dorks an Easy Way of Hacking

Shanzida Anika Mim Follow
Sep 13 · 7 min read

“Where should I start learning how to hack ?” Personally Google is one of my best friends in Hacking, and I’m sure Google will be yours too after reading this article.

All you need to carry out to move further with **“Google Dork”**, is a computer, an internet connection and knowledge of the appropriate search syntax. A number of examples are given down below and if you need more, you can visit Github, a large number of Google Dork can be found.

HOW IT ALL STARTED?

The concept of **“Google Hacking”** dates back to 2002, when Johnny Long began to collect interesting Google search queries that uncovered vulnerable systems and sensitive information, labeling

them Google Dorks.

“In the years I’ve spent as a professional hacker, I’ve learned that the simplest approach is usually the best. As hackers, we tend to get down into the weeds, focusing on technology, not realizing there may be non-technical methods at our disposal that work as well or better than their high-tech counterparts. I always kept an eye out for the simplest solution to advanced challenges ~ Johnny Long 2011.

WHAT DATA CAN WE FIND USING GOOGLE DORKS?

- Username and passwords
- Admin login pages
- Sensitive documents
- Govt/military data
- Email lists
- Bank account details
- Vulnerable websites
- So much more …

A Google Dork is just a search that uses one or more of these advanced techniques to reveal something interesting. Something important to keep in mind, the web can be crawled by anyone. Google automatically indexes a website, and unless sensitive information is

explicitly blocked from indexing (nofollow, robots.txt), all of the content can be searched via Dorks or advanced search operators.

Most of the time, users might post the link, not realizing what they've shared. This information will be exposed in the "referrer" header. Consider a web page: "wp-content/uploads/private"", if the browser needs to make a request to another domain to render this web page (for instance, to download an image), a header will be included: "Referer: http://yourdomain.com/wp-content/uploads/private".

HOW TO USE THE DORKS?

cache: Google will highlight words within the cached document. For instance, [cache:www.google.com] web will show the cached content with the word "web" highlighted. This functionality is also accessible by clicking on the "Cached" link on Google's main results page. The query [cache:] will show the version of the web page that Google has in its cache.

link: The query [link:] will list web pages that have links to the specified web page. For instance, [link:www.google.com] will list web pages that have links pointing to the Google homepage. Note there can be no space between the "link:" and the web page URL.

related: The query [related:] will list web pages that are "similar" to a specified web page. For instance, [related:www.google.com] will

list web pages that are similar to the Google homepage. Note there can be no space between the “related:” and the web page URL.

info: The query [info:] will present some information that Google has about that web page. For instance, [info:www.google.com] will show information about the Google homepage.

define: The query [define:] will provide a definition of the words you enter after it, gathered from various online sources. The definition will be for the entire phrase entered (i.e., it will include all the words in the exact order you typed them).

stocks: If you begin a query with the [stocks:] operator, Google will treat the rest of the query terms as stock ticker symbols, and will link to a page showing stock information for those symbols. For instance, [stocks:intc yhoo] will show information about Intel and Yahoo. (Note you must type the ticker symbols, not the company name.)

site: If you include [site:] in your query, Google will restrict the results to those websites in the given domain. For instance, [help site:www.google.com] will find pages about help within www.google.com. [help site:com] will find pages about help within “.com” URL.

allintitle: If you start a query with [allintitle:], Google will restrict the results to those with all of the query words in the title. For

instance, [allintitle:google search] will return only documents that have both “google” and “search” in the title.

intitle: If you include [intitle:] in your query, Google will restrict the results to documents containing that word in the title. For instance, [intitle:google search] will return documents that mention the word “google” in their title, and mention the word “search” anywhere in the document (title or no).

inurl: If you include [inurl:] in your query, Google will restrict the results to documents containing that word in the url. For instance, [inurl:google search] will return documents that mention the word “google” in their url, and mention the word “search” anywhere in the document (url or no). Note there can be no space between the “inurl:” and the following word. Putting “inurl:” in front of every word in your query is equivalent to putting “allinurl:” at the front of your query: [inurl:google inurl:search] is the same as [allinurl:google search].

SOME SMALL EXAMPLES OF GOOGLE DORKS

- intitle:the title you are looking
- inurl:the website URL you are targeting

As per the examples mentioned above, you can use the same way the Google Dork as follow :

- site:
- phonebook:
- maps:
- book:
- info:
- movie:
- weather:
- link:

Finding PDF Files with Google Dorks

```
inurl:(htm|html|php) intitle:"index of" + "last modified"
+"parent directory" +description +size +(pdf) "hacking"
inurl:(htm|html|php) intitle:"index of" + "last modified"
+"parent directory" +description +size +(pdf) "python"
```

```
"whoops! there was an error." "db_password"
```

Personally I highly recommended you to never put your **.env** files in the web-server directory. As you can see, this can cause serious damage.

```
db_password filetype:env
```

```
db_password ===
```

With this Dork search you can find website information as per the below screenshot. It’s something very common to find passwords, website credentials details and even login of payment systems such as PayPal.

BUDGETS ON THE US SECURITY WEBSITE

```
budget filetype:xls
budget filetype:xlsx OR budget filetype:csv
site:nasa.gov filetype:pdf
budget site:dhs.gov filetype:xls
```

FINDING DIRECTORY

Finding a directories can be something very interesting when auditing, since in them you can find files with sensitive information. Through **Google Dork**, you can find a directory indexed in google that otherwise would go unnoticed.

```
intitle:index of "parent directory"
intitle:index of name size
intitle:index.of.admin
inttitle:index.of inurl:admin
filetype:log inurl:ws_ftp log
intitle:index.of "server at"
intitle:index.of "Apache/1.3.27 Server at"
```

PROTECT YOUR PRIVACY

In August 2014, the United States Department of Homeland Security (DHS), the FBI and the National Counter terrorism Center issued a bulletin warning agencies to guard against the potential for Google Dork on their sites.

If you're using **Google Dork** in a country with heavy internet surveillance, it's possible that your searches could be recorded and used against you in the future. As protection, we recommend using the Tor Browser or any Anon Surf when you're using Google Dork. **Tor** masks your internet traffic and block webpages accessing informations about your machine.

GOOGLE IS BLOCKING ME

If you start getting HTTP 503 errors, Google has rightfully detected you as a bot and will block your IP for a set period of time. The solution is to use **proxychains**.

INSTALL PROXYCHAINS4 ON DEBIAN AND DERIVATED DISTRIBUTIONS

```
sudo apt install proxychains4 -y
```

COPY

Output

Edit the **/etc/proxychains4.conf** configuration file to round robin the look ups through different proxy servers. In the example below, 2 dynamic **socks** proxies have been set up with different local listening ports (9050 and 9051).

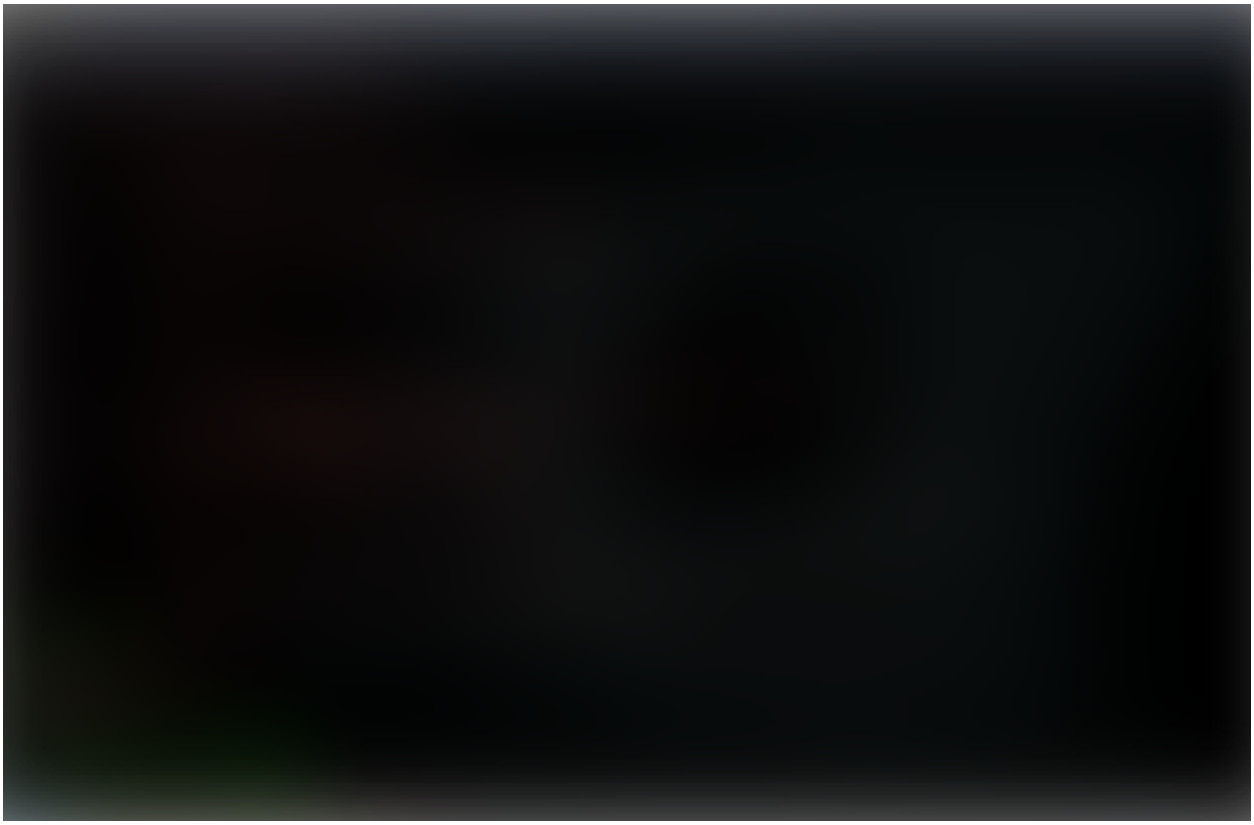
```
vim /etc/proxychains4.conf
```

COPY

Or

```
nano /etc/proxychains4.conf
```

COPY



IMPORTANT THINGS TO REMEMBER

- This article was written for educational purpose and pen-test only.
- The author can not be held responsible for damages caused by the

use of these resources.

- You will not misuse the information to gain unauthorized access.
- This information shall only be used to expand knowledge and not for causing malicious or damaging attacks.
- Performing any hacks without written permission is illegal.

Finally

There is so much to tell about Google Dork and it's so much fun and great. I really hope you have learned something from this article so that you can apply it.