

Introduction to Google Dorks

Eyad Eltaher

January 24, 2025

Introduction

- **What is Google Dorking?**

Google Dorking, also known as Google Hacking, involves using advanced search techniques to find information inaccessible through conventional search methods. You can uncover files, sensitive data, and other information that typically remains hidden from standard searches by using specific search operators.

- **How Does Google Dorking Work?**

Google Dorking leverages advanced search operators to uncover hidden or sensitive information on websites indexed by Google. By using specific commands, such as "intitle:" to search within titles, "inurl:" to search within URLs, or "filetype:" to target specific file types like PDFs, users can refine their searches to reveal data often missed by regular search queries.



Google Dorking search Commands

Mastering the right search operators is crucial for effective Google Dorking, as they allow you to filter results and uncover specific information with precision. Here are some key search operators and commands used in Google Dorking:

1. **site:** This operator restricts the search to a specific website or domain. For example, `site:example.com` will show results only from "example.com."
2. **intitle:** This command searches for a keyword within the title of web pages. Example: `intitle:"login"` displays pages with "login" in their title, often revealing login pages.
3. **inurl:** This operator searches for specific words within the URL. For example: `inurl:admin` helps locate URLs with "admin" in them, which might lead to admin panels.
4. **filetype:** This function is used to find specific file types, such as PDFs, Excel sheets, or word documents. For example, `filetype:pdf "confidential"` uncovers potentially sensitive PDF files.
5. **intext:** This command searches for a specific word or phrase within the content of web pages. Example: `intext:"password"` reveals pages containing the word "password," which might expose sensitive data.
6. **allintext, allintitle and allinurl:** If you want to use multiple keywords, then you can use `allintext` and `allintitle`. All the keywords will be separated using a single space between them. Google will consider all the keywords and provide all the pages in the result. Thus, users only get specific results. So, make sure you use the right keywords or else you can miss important information.
Example: `allintext:"username" "password"`
Example: `allintitle:"ip camera" "dvr"`
Example: `allinurl:tesla lambo`
7. **ext:** search for a specific type of document, you can use the `ext` command.
Example: `ext:pdf spanish guide`
8. **@command:** If you want your search to be specific to social media only, use this command. It'll show results for your search only on the specified social media platform.
Example: `mangoes @facebook`
9. **Related:** In some cases, you might want specific data with more than one website with similar content. You can provide the exact domain name with this Google Dorking command: `Related:domainname.com`
10. **before & after:** The `before:` & `after:` commands return documents before and after a date. You must provide year-month-day dates or only a year. You can combine both. For example:
`avengers endgame before:2019`
`avengers endgame after:2019-04-01`
`avengers endgame after:2019-03-01 before:2019-03-05`

Google Dorking search Operators

To narrow down and filter your results, you can use operators for better search. The following are some operators that you might find interesting.

1. **Search term:** You can use this operator to make your search more specific so the keyword will not be confused with something else. For example, if you are specifically looking for “Italian foods,” then you can use the following syntax. “Italian foods”
2. **AND:** This operator will include all the pages containing all the keywords. The keywords are separated by the ‘&’ symbol. You can use the following syntax.
site:facebook.com & site:twitter.com
3. **OR:** Using this operator, you can provide multiple keywords. You will get results if the web page contains any of those keywords. You can separate the keywords using “|” For example.
site:facebook.com | site:twitter.com
4. **Glob Pattern:** You can use the glob pattern (*) when you are unsure what goes there and tell Google to make the search accordingly. For example site:*.com

Tips & tricks

Here are a few Google hacks for you to try:

- Use the “@” symbol to search for information within social media sites. For this, you need to provide the social media name. For example, enter @google:username to search for the term username within Google.
- To get hashtags-related information, you need to use a # sign before your search term. For example, enter #HelloDelhi.
- To search for unknown words, use the asterisk character (*) that will replace one or more words. For example, Daya will move to *.
- You can use the keyword map along with the location name to retrieve the map-based results. For example, enter map:Delhi.