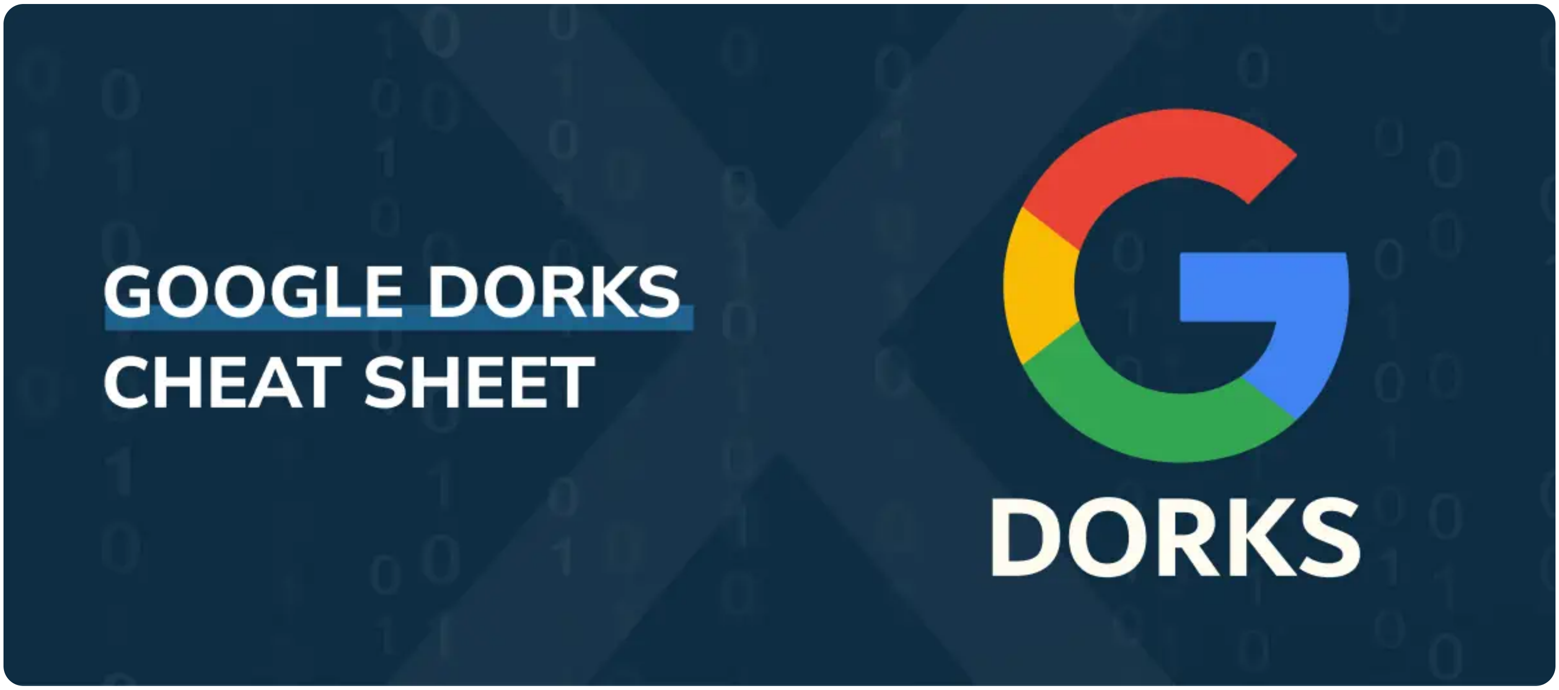
Google Dorks Cheat Sheet 2023: How to Hack using Google

January 4, 2023 / By Cassandra Lee



Listen to the article

Learning about Google dorks is fundamental to a practical understanding of cyber security, especially penetration testing and ethical hacking. Ingeniously constructed Google queries can uncover leaked passwords and sensitive data, let you view neighborhoods from unsecured cameras, access files not meant for you, and more.

Google dorks are challenging to master for three non-technical reasons:

1. Valid dorks change often;
2. Misuse can lead to serious legal repercussions;
3. The dangers of accidentally inappropriate Google dorking discourage explorers from achieving mastery.

This Google dorks cheat sheet will cover the dorking commands and operators, search parameters, their combinations, questionable dorks, and how to prevent others from Google dorking your online resources.

Google traces every search back to the device issuing it, so take care in handling the clickable examples in this Google dorking cheat sheet, which you may download **here**.

When you're ready, let's dive in.

What Is a Google Dork?

A "Google dork" is an advanced Google search technique. "Google dorking" (aka "Google hacking") is the activity of performing advanced searches on Google. You can combine different Google dorks to comb data otherwise inaccessible to ordinary users of Google search.

On a browser, if you make too many Google searches in a short time, Google requires that you unscramble garbled letters in an image called a captcha before you can proceed. Captcha completion can frustrate end users like you, but Google servers must nip denial-of-service cyberattacks in the bud.

Unlike most cheat sheets, we cannot guarantee that the commands below will remain unchanged in perpetuity. Google updates its dorks continually, so deprecated techniques don't appear here, even if you can find them elsewhere on the Internet.

Before You Begin Google Dorking

Google dorking is not a playground where you can flood commands to your heart's content:

- Google limits your Google search rate from a single device.
- It may ban your IP if you issue too many queries.
- Abuse of dorks may have legal repercussions.

No, you're not immune even if you're working from a virtual machine toying with **sqlmap**.

If you know you can't resist having fun with it (and you will), you could work from **Pagodo**, which automates Google searching for potentially vulnerable web pages and applications on the Internet. It also lets you **automate the rate** at which your device issues Google dorks.

Regardless of how you use Google dorks, respect Google's **Terms of Service**. Be careful.

Examples of Creepy Dorks

These dorks reveal vulnerabilities in websites, and their contents may be newsworthy depending on the zeitgeist.

For details on how the following commands work, refer to **Text dorks**, **Google Dorks Operators**, and **Scope-Restricting Dorks**.

EXAMPLES	DESCRIPTION
inurl:”view.shtml” “Network Camera”,“Camera Live Image”, **inurl:”guestimage.html”**,**intitle:”webcamXP 5’”**	Get web applications showing live webcam (online camera) footage.
“Not for Public Release” + “Confidential” ext:pdf | ext:doc | ext:xlsx	Get links to documents meant to be classified. Some come from governmental websites.
site:.hk & inurl:wp-login	Get login pages of WordPress sites ending in the notoriously **unsafe domain** “.hk”
”index of” inurl:ftp secret	Get FTP servers you want to access containing the keyword “secret”
Critical dorks performed on .env files yielding results such as:	Popular web development frameworks use .env files to declare general variables and configurations for local and online dev environments, often including passwords. The dork used to produce the screenshot exposes database passwords. Hence it’s vital to keep .env files from being publicly accessible. (If you’ve read this cheat sheet in its entirety, you will be able to guess the dork used here.)

This often-updated exploit database contains other Google dorks that expose sensitive information. Proceed with caution.

Google Dorks Search Parameters

A search parameter in a Google dork is the text string payload affixed to or used with the Google dorking command or operator. Without a suitable search parameter, Google treats the dork keyword as an ordinary query keyword at best and returns zero results at worst.

For example, in the search **site:stationx.net**, the domain “stationx.net” is the parameter. In **(psychology OR computer science) AND design**, the three subjects of psychology, computer science, and design are the parameters. In **16 F to C** (converting a temperature from degrees Fahrenheit to Celsius), 16 is the parameter.

Search parameters include web domains, file extensions, numbers, and character strings with or without quotes.

Google Dorking Commands

As Google's internal documentation on dorks frequently changes, the following is not an exhaustive list but a list of commands known to return meaningful results. Some of the given commands may be obsolete because they return similar results as a dork-free search. Deprecated commands don't appear below.

Scope-Restricting Dorks

These help specify your target range of websites or data types. For example, in hunting for e-books, the Google dork "filetype:pdf" is indispensable.

If a command listed below ends with a symbol, include no space between the command and the parameter. The correct way to use each command is in the "Example usage" column. Otherwise, Google will treat the command as an ordinary search keyword rather than a dork.

COMMAND	DESCRIPTION	EXAMPLE USAGE
`site:`	Restrict search to a particular website, top-level domain, or subdomain. Additional query items are optional.	**site:google.com**,**site:maps.google.com**, **site:.org tax return**
`filetype:, ext:`	Restrict the returned web addresses to the designated file type. Unlike most other dorks, this **requires additional keywords** in the search bar or will return no results. Here is Google's **official list** of common file types it can search. Google also supports the file	**filetype:pdf car design**,**ext:log username** Compare with**filetype:pdf**, **ext:txt**, etc.

COMMAND	DESCRIPTION	EXAMPLE USAGE
	extensions **db**, **log**, **html**, **mpeg**, **mov**, and **flv**. Nonetheless, searches on mp3 and mp4 with and without additional search terms have yielded no results.	
`@`	Restrict search to a particular social platform. It supports popular platforms such as Facebook, Twitter, YouTube, and Reddit. A downside is it’s not as precise as the “site:” dork.	**@twitter pentest**,**@youtube google dorking**
`imagesize:(height)x(width)`	Restrict image search results to those of the specified dimensions	You can use these images as desktop wallpapers or video thumbnails: **imagesize:1920×1080**
`define:`	Return definitions of a word or phrase	Compare **define:privacy** and a plain search on **privacy**.
`stocks:`	Check the financial activity of a particular stock	**stocks:TWTR** (Twitter), **stocks:gm** (General Motors), **stocks:pfizer**
`movie:`	Return information about any movie with the given title	Compare **movie:”phantom of the opera”** and **“phantom of the opera”**.
`source:`	Find reports from a Google News source.	**source:npr**

Informational Dorks

These dorks appear to work best if used as standalone commands, i.e., without additional query items.

COMMAND	DESCRIPTION	EXAMPLE USAGE
`$`	Search for prices in USD ($). This also works for Euro (€), but not GBP (£) or Yen (¥).	**ipad $329**,**iphone €239**
`cache:`	Get Google's last saved version of a particular website. A website snapshot like this is called "cache".	**cache:news.yahoo.com**
`link:`	Find pages linking to the given domain	**link:stationx.net**
`related:`	Return websites related to the given website	**related:harvard.edu**, **related:bbc.co.uk**
`map:`	Gets a map of the given location	**map:"new york"**
`weather:`	Gets the weather of the given location	**weather:london**
Usable but possibly deprecated commands		
`location:, loc:`	Find information about a location. Results may be inconsistent.	**location:NY crime**,**loc:NY crime**
`info:, id:`	Return pages that convey information about the given website. Finding queries that gave different results with and without the "info:" / "id:" command was difficult. This command could still help you find the canonical, indexed version of a URL.	**"babylon bee"** vs **info:"babylon bee"**: a politically conservative satire website in the US

COMMAND	DESCRIPTION	EXAMPLE USAGE
		Also, **id:"babylon bee"** treats "id" as a search parameter (bold text) in some results:

Text Dorks

These are helpful if you want to look for web pages containing certain text strings or follow particular patterns. For example, those familiar with the URLs of webcam apps, for example, use Google dorks similar to the first entry in **this table** to find camera footage to watch.

COMMAND	DESCRIPTION	EXAMPLE USAGE
`intitle:`, `allintitle:`	Look for pages with titles containing the search terms. The dork "intitle:" applies to its	**intitle:toy story**, **intitle:"toy story"**Compare the above with the number of search results of **toy story** and **"toy**

COMMAND	DESCRIPTION	EXAMPLE USAGE
	search parameter only, while "allintitle:" applies to the entire query string.	**story"**. **allintitle:"toy story"**.Compare with **intitle:"toy story"** — both have the same number of search results.
`inurl:`	Finds links containing the character string.	**inurl:login.php**
`allinurl:`	Finds links containing all words following the colon (:). Equivalent to applying "inurl:" to discrete search strings.	Compare **allinurl: healthy eating** vs **inurl:healthy inurl:eating**:

COMMAND	DESCRIPTION	EXAMPLE USAGE
Usable but possibly deprecated commands		
`intext:`, `allintext:`	Finds websites containing the payload. The dork “intext:” applies to its search parameter only, while “allintext:” applies to the entire query string. The websites displayed in the results appear similar to a search without either command.	Compare **intext:”Index of /” +.htaccess**, **allintext:”Index of /” +.htaccess**, and **“Index of /” +.htaccess**.

Google Dorks Operators

Unlike certain Google Dorking commands, you may include spaces between Google dorking operators and your query items. You may combine as many different operators and commands as are necessary.

Search

These refine the search and constrain the results to follow the rules of logic. Most of the following are logical operators.

COMMAND	DESCRIPTION	EXAMPLE USAGE
`" "`	Return exact matches of a query string enclosed in the double quotes. Note that these are straight and not curly	**“Google dorking commands”**. Compare **‘movie review’** and **“movie review”**:

COMMAND	DESCRIPTION	EXAMPLE USAGE
	“” quotation marks. The curly quotes may or may not return similar results as straight quotes. Single quotes don’t work.	
`OR, |`	Return sites containing either query item joined by OR or the pipe character |. This is an inclusive OR.	**Amazon OR Google** yields the same number of results as **Amazon | Google**.
`( )`	Groups multiple Google dork operators as a logical statement	**(black OR white) hat hacker**
`-`	Hyphen; excludes search results containing the word or phrase after the hyphen.	**Amazon -reviews**, **“sql injection” -“penetration testing”**

COMMAND	DESCRIPTION	EXAMPLE USAGE
`*`	Wildcard or glob pattern as a placeholder for query item	**“type * error”** returns pages on Type I and II errors in statistics. Compare this with the search **“type i OR ii error”** which doesn’t use this wildcard:
`#..#`	Search a numerical range specified by the two endpoints # inclusive	**2006..2008** finds all pages that include 2006, 2007, or 2008 in them.
`AROUND(N)`	Match pages containing the search terms separated by at most N other words	**read AROUND(2) book**, **read AROUND(3) book**
Usable but possibly		
`AND, &, +`	Concatenation; return sites containing both query items joined by AND, the ampersand symbol & or the plus sign +. Google seems to assume you’re using this dork whenever you have multiple search items in one query. This is because the websites in the dorked search results are similar to	**Amazon AND Google**, **Amazon & Google**, **Amazon + Google**.Compare with**Amazon Google** (no quotes):

COMMAND	DESCRIPTION	EXAMPLE USAGE
	queries without these dorks. Curiously, the estimated number of search results differs.	
_	Wildcard symbol for Google Autocomplete. Google appears to treat this symbol	Suppose you can’t recall the name of the late singer Michael Jackson:**Michael _ singer**, **“Michael _” singer**.

COMMAND	DESCRIPTION	EXAMPLE USAGE
		Compare with **Michael singer**, **“Michael *” singer**. Only **“Michael *” singer** has a direct entry about Michael Jackson on the first page of the search results:

Math

The following are mathematical operations that you can perform on Google.

OPERATORS	DESCRIPTION	EXAMPLE USAGE	RESULT
+	Addition	**3 + 20**	23

OPERATORS	DESCRIPTION	EXAMPLE USAGE	RESULT
–	Subtraction	**3 – 20**	-17
*	Multiplication	**3 * 20**	60
/	Division	**3 / 20**	0.15
% of	Percentage	**33% of 400**	6.6
X^Y, X**Y	Raise X to the power of Y. Both operators ^ and ** perform the same operation.	**3^2**,**3**2**	3^2 = 93**2 = 9
in, to	Convert a quantity from a given unit to another. Translate words into another language.	**6 ft 2 inches in cm**,**140 lbs in kg**,**100 USD to bitcoin**,**8 am London time to California time**,**thank you in spanish**	6 ft 2 inches = 187.96 cm,140 lbs = 63.5029 kg,100 USD =
i	Use it with other mathematical operations to see it in action.	**i^2**	-1
N choose R	Find how many combinations are possible from N items taken R at a time, where N and R are	**6 choose 4**	15

00:00 00:00 1

OPERATORS	DESCRIPTION	EXAMPLE USAGE	RESULT
	integers. (Combinatorics)		
sin, cos, tan	Trigonometric functions. You may specify the formula using symbols and natural language.	**sin(pi/6)**,**sin 30 degrees**	sin(pi/6) = 0.5,sin 30 degrees = 0.5
timer	**Timer**	**timer for 20 minutes**	
[This has no specific operator]	**Generate a random number**. Find more on the drop-down dialog box labeled “Tools” on the results page.	**flip a coin**,**roll a dice**,**show random number from 10 to 40**	
[graph]	Graph a mathematical numerical range from A to B. The “graph” keyword is only necessary if Google doesn’t understand your query.	**sin(x)/xgraph**	

00:00 00:00 1

OPERATORS	DESCRIPTION	EXAMPLE USAGE	RESULT

Google also supports other scientific calculator operations on its **calculator**. This **website** features additional examples of mathematical operations you can perform on Google.

Examples of Complex Google Dorks

You can combine Google dorking commands and operations for specific results.

COMMAND	DESCRIPTION
`inurl:zoom.us/j intext:scheduled`	Get links to publicly shared Zoom meetings you may want to access.
`"index of" "database.sql.zip"`	Get unsecured SQL dumps. Data from improperly configured SQL servers will show up on this page.
`filetype:yaml inurl:cassandra`	Get YAML configuration files specific to **Apache Cassandra databases**
`@reddit memes -dark`	Find memes on Reddit that are not dark
`site:twitter.com filetype:pdf`	Find PDFs on the **twitter.com** domain
`imagesize:1920x1080 clouds`	Find cloud images of dimensions 1920 pixels by 1080 pixels
`secret in spanish inurl:dict`	Translate the word “secret” to Spanish and limit results to URLs containing “dict”

COMMAND	DESCRIPTION
`link:ox.ac.uk PhD math`	Find information on “PhD” and “math” that link to the University of Oxford’s official website. Compare with **ox.ac.uk PhD math**:
`filetype:html site:rumble.com james`	Rumble video pages end in “.html”. This looks for Rumble video URLs containing the keyword “james”.

How to Prevent Google Dorks

Google Dorking.

- Implement IP-based restrictions and password authentication to protect private areas. Securing your login portals discourages unauthorized access.
- Encrypt all sensitive information, like usernames, passwords, email addresses, phone numbers, and physical addresses. This way, in the event of data leakage, the original data remains unexposed.
- Run vulnerability scans to find and disable Google dorks. Examples of vulnerability scanners are Nessus and Qualys.
- Run regular dork queries on your website to discover loopholes and sensitive information before attacks occur. **Sqlmap** is a helpful tool.

- If you find sensitive content exposed on your website and you've exhausted all other means of removing it (such as changing your passwords or renaming your login pages), request its removal through **Google Search Console**.
- Be judicious in the use of `robots.txt`. Read the **warning** below.

A Word of Caution

Other websites mentioning Google Dorks typically recommend using robots.txt to conceal sensitive content or to stop Google from indexing specific parts of your website. On your website server, you can find `robots.txt` in the root-level directory, such as `/public_html`.

What seems like a simple, good-faith solution to eliminate complex reconnaissance via Google Dorks is, to an intelligent hacker, a treasure trove and a cash cow. Instead of backing off, they'll attack your website by targeting the items listed in `robots.txt`.

Hence, it's best to adopt this measure cautiously. The most prudent use of `robots.txt` is instructing Google to exclude one's entire website, as follows:

```
User-agent: *Disallow: /
```

Such a robots.txt file compels visitors looking for information to use the search function inside the website. A well-built internal search function may have safeguards against Google dorking, SQL injection, and other hacking techniques. These safeguards protect the website better than allowing external search engines such as Google to index the website.

Summary

paramount to your Google dorking experience. Google dorking is an invaluable tool for practical cyber security research when used responsibly.

We hope this Google dorking cheat sheet is helpful to you. You can read our **full guide on Google dorking specific websites here**. Remember: with great power comes great responsibility. More important than enjoying Google dorking, stay safe.

Frequently Asked Questions

⊖ What can you do with Google Dorking?

You can filter websites with greater precision, unearth information ordinarily inaccessible to the public, and discover vulnerabilities in websites. As Google records your search history, be careful with searches on sensitive data; you risk Google flagging you as a threat or even legal action from external parties.

⊕ Is it legal to use Google Dorks?

⊕ What are the Google Dorking commands?

⊕ What are the two elements of a Google dork?

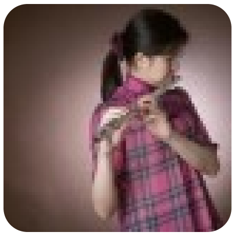
⊕ What are Google dork operators?

⊕ Which Google dork restricts the search results to the websites under the given domain?

00:00 00:00 1

FIND OUT MORE

CATEGORIES CHEAT SHEETS HACKING



Cassandra Lee

I make connections across disciplines: cyber security, writing/journalism, art/design, music, mathematics, technology, education, psychology, and more. I've been advocating for girls and women in STEM since the 2010s, having written for Huffington Post, International Mathematical Olympiad 2016, and Ada Lovelace Day, and I'm honored to join StationX. You can find me on **LinkedIn** and **Linktree**.

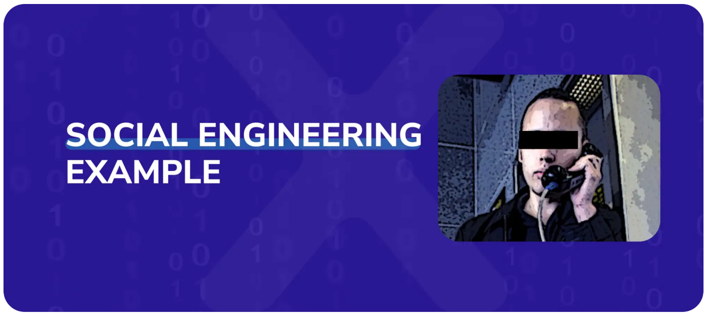
Related Articles

Nmap Cheat Sheet 2023: All the Commands, Flags & Switches

Read More »

Linux Command Line Cheat Sheet: All the Commands You Need

Read More »



Social Engineering Example

Read More »

Movies for Hackers to Watch

Read More »

INFO

- Affiliates
- Legal Notices
- Privacy Policy
- Site Map

SECURITY ASSESSMENT

- Penetration Testing
- Vulnerability
- Source Code Review
- Social Engineering

CONSULTING

- Audit & Compliance
- Incident Response
- Risk Assessment
- Security Training

00:00

00:00

1

00:00 00:00 1