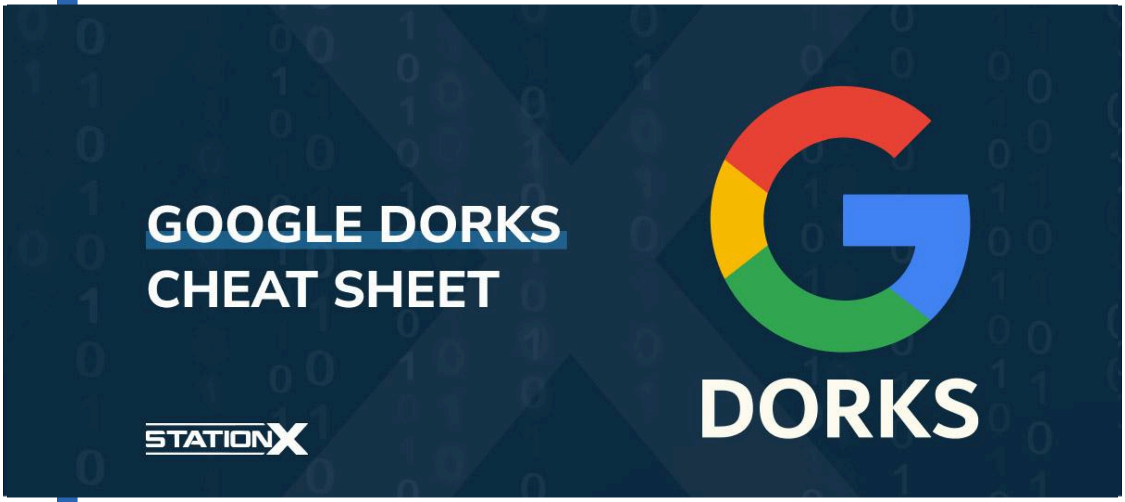
Google Dorks Cheat Sheet



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.

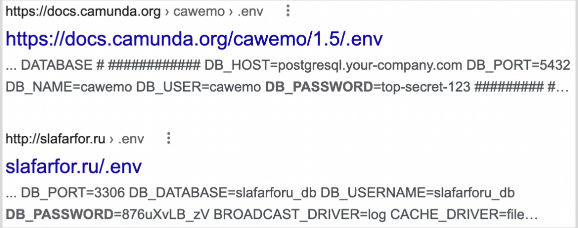
If you know you can’t resist having fun with it (and you will), you could work from Pagodo, which automates Google searching for potentially vulnerable web pages and applications on the Internet. It also lets you automate the rate at which your device issues Google dorks.

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:  https://docs.camunda.org › cawemo › .env https://docs.camunda.org/cawemo/1.5/.env ... DATABASE # ############ DB_HOST=postgresql.your-company.com DB_PORT=5432 DB_NAME=cawemo DB_USER=cawemo **DB_PASSWORD**=top-secret-123 ######### #... http://slafarfor.ru › .env slafarfor.ru/.env ... DB_PORT=3306 DB_DATABASE=slafarforu_db DB_USERNAME=slafarforu_db **DB_PASSWORD**=876uXvLB_zV BROADCAST_DRIVER=log CACHE_DRIVER=file...	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.

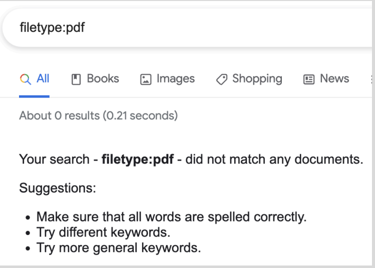
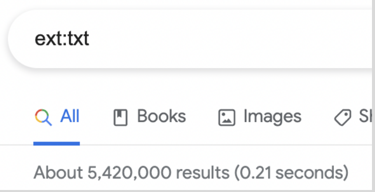
Google Dorking Commands

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.

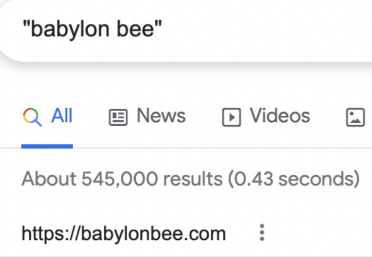
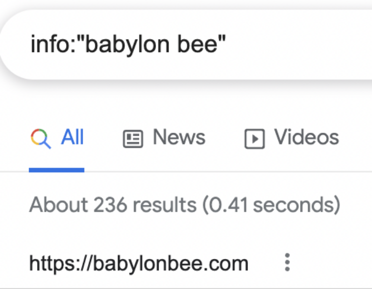
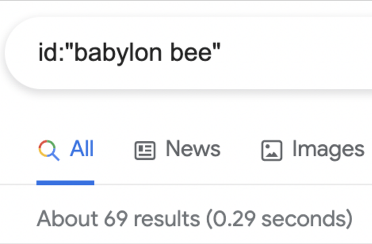
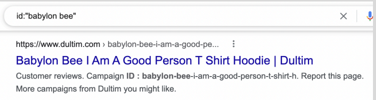
Command	Description	Example usage
site:	Restrict search to a particular website, top-level domain, or subdomain. Additional query items are optional.	site:google.com, site:maps.google.com, site:.org tax return
filetype:, ext:	Restrict the returned web addresses to the designated file type. Unlike most 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 extensions db, log, and html. Nonetheless, searches on mp3 and mp4 with and	filetype:pdf car design, ext:log username Compare with filetype:pdf, ext:txt, etc.  filetype:pdf About 0 results (0.21 seconds) Your search - **filetype:pdf** - did not match any documents. Suggestions: • Make sure that all words are spelled correctly. • Try different keywords. • Try more general keywords.  ext:txt About 5,420,000 results (0.21 seconds)

	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
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:META (Meta), 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:cnn

Informational Dorks

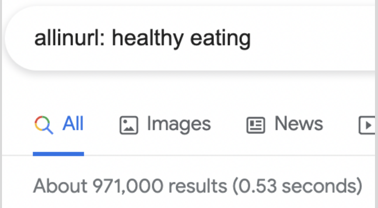
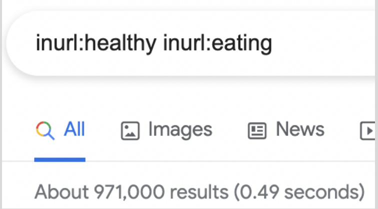
These dorks appear to work best if used as standalone commands, i.e., without additional query items.

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:	Get a map of the given	map:"new york"

	location	
weather:	Get the weather of the given location	weather:london
Usable but possibly deprecated commands		
location:	Find information about a location. Results may be inconsistent. Google now treats “loc” (formerly an abbreviation of “location”) as a search term instead of a dork.	location:NY crime compared with 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. Google now treats “id” (possibly shorthand for “info”) as a search term instead of a dork.	"babylon bee" vs info:"babylon bee": a politically conservative satire website in the US  "babylon bee" About 545,000 results (0.43 seconds) https://babylonbee.com  info:"babylon bee" About 236 results (0.41 seconds) https://babylonbee.com Here’s how id:"babylon bee" treats “id” as a search parameter (bold text) in some results:  id:"babylon bee" About 69 results (0.29 seconds)  id:"babylon bee" https://www.dultim.com › babylon-bee-i-am-a-good-pe... Babylon Bee I Am A Good Person T Shirt Hoodie | Dultim Customer reviews. Campaign **ID : babylon-bee**-i-am-a-good-person-t-shirt-h. Report this page. More campaigns from Dultim you might like.

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.

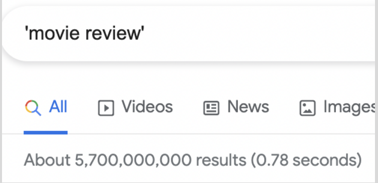
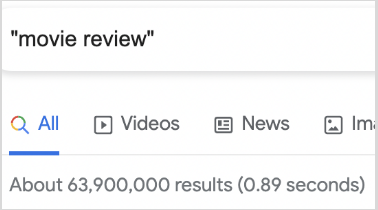
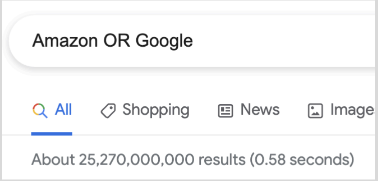
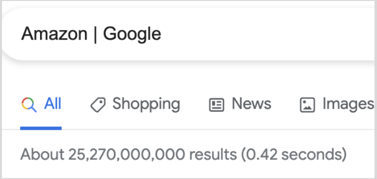
Command	Description	Example usage
intitle:, allintitle:	Look for pages with titles containing the search terms. The dork “intitle:” applies to its search parameter only, while “allintitle:” applies to the entire query string.	intitle:toy story, intitle:"toy story", allintitle:"toy story", allintitle:toy story Compare the above with the number of search results of toy story and "toy story".
inurl:	Find links containing the character string.	inurl:login.php
allinurl:	Find links containing all words following the colon (:). Equivalent to applying “inurl:” to discrete search strings.	Compare allinurl: healthy eating vs inurl:healthy inurl:eating:  allinurl: healthy eating About 971,000 results (0.53 seconds)  inurl:healthy inurl:eating About 971,000 results (0.49 seconds)
Usable but possibly deprecated commands		
intext:, allintext:	Find 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. Look at intext:"Index of /" +.htaccess -intitle:"Index of /" (exclude titles containing the search query) too.

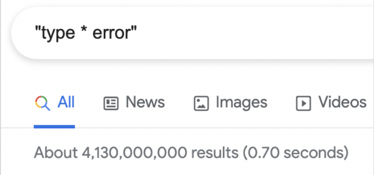
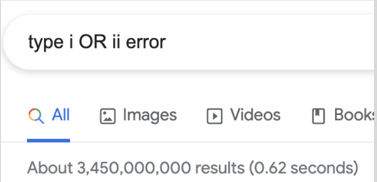
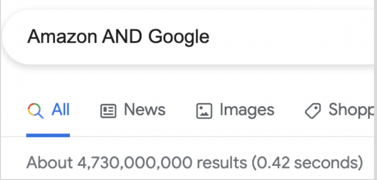
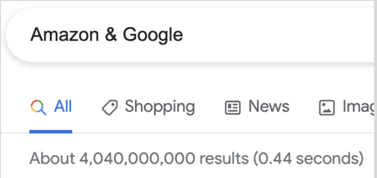
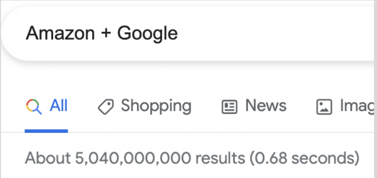
Google Dorks Operators

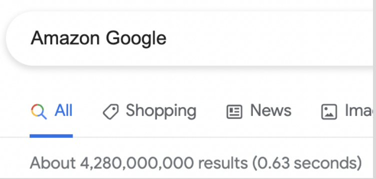
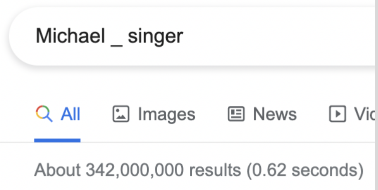
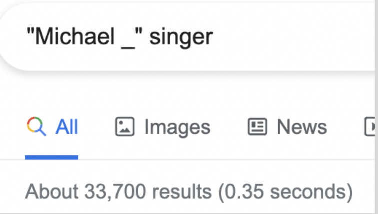
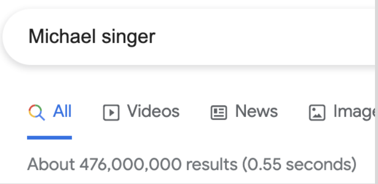
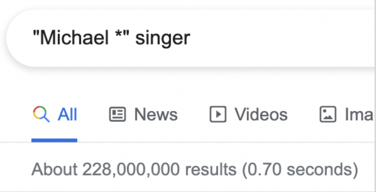
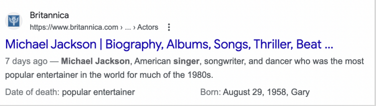
Unlike certain Google Dorking commands, you may include spaces between Google dorking operators and your query items. You may combine as many different operators and commands as are necessary.

Search

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

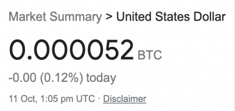
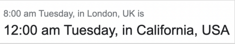
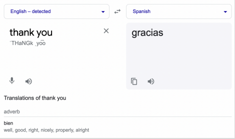
Command	Description	Example usage
" "	Return exact matches of a query string enclosed in the double quotes. Note that these are straight and not curly “” quotation marks. The curly quotes may or may not return similar results as straight quotes. Single quotes don’t work.	"Google dorking commands". Compare 'movie review' and "movie review":  'movie review' All Videos News Images About 5,700,000,000 results (0.78 seconds)  "movie review" All Videos News Ima About 63,900,000 results (0.89 seconds)
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.  Amazon OR Google All Shopping News Image About 25,270,000,000 results (0.58 seconds)  Amazon | Google All Shopping News Images About 25,270,000,000 results (0.42 seconds)
( )	Group multiple Google dork operators as a logical statement	(black OR white) hat hacker
-	Hyphen; exclude search results containing the word or phrase after the hyphen.	Amazon -reviews, "sql injection" -"penetration testing"

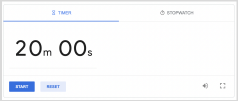
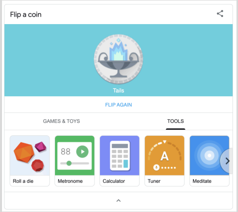
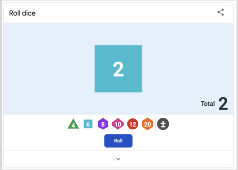
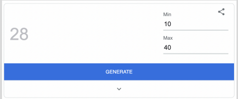
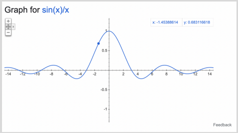
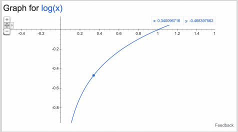
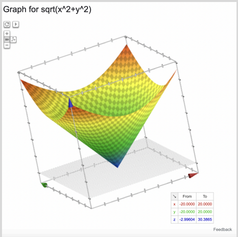
*	Wildcard or glob pattern as a placeholder for query item	"type * error" returns pages on Type I and II errors in statistics. Compare this with the search “type i OR ii error” which doesn’t use this wildcard:  "type * error" About 4,130,000,000 results (0.70 seconds)  type i OR ii error About 3,450,000,000 results (0.62 seconds)
#..#	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 deprecated commands		
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 queries without these dorks. Curiously, the estimated number of search results differs.	Amazon AND Google, Amazon & Google, Amazon + Google. Compare with Amazon Google (no quotes):  Amazon AND Google About 4,730,000,000 results (0.42 seconds)  Amazon & Google About 4,040,000,000 results (0.44 seconds)  Amazon + Google About 5,040,000,000 results (0.68 seconds)

		 Amazon Google About 4,280,000,000 results (0.63 seconds)
_	Wildcard symbol for Google Autocomplete. Google appears to treat this symbol literally if it's inside double quotes.	Suppose you can't recall the name of the late singer Michael Jackson: Michael _ singer, "Michael _" singer.  Michael _ singer About 342,000,000 results (0.62 seconds)  "Michael _" singer About 33,700 results (0.35 seconds) Compare with Michael singer, "Michael *" singer.  Michael singer About 476,000,000 results (0.55 seconds)  "Michael *" singer About 228,000,000 results (0.70 seconds) Only "Michael *" singer has a direct entry about Michael Jackson on the first page of the search results:  Britannica https://www.britannica.com › ... › Actors Michael Jackson | Biography, Albums, Songs, Thriller, Beat ... 7 days ago — **Michael Jackson**, American **singer**, songwriter, and dancer who was the most popular entertainer in the world for much of the 1980s. Date of death: popular entertainer Born: August 29, 1958, Gary

Math

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

Operators	Description	Example usage	Result
+	Addition	3 + 20	23
-	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 = 9, 3**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 =  Market Summary > United States Dollar 0.000052 BTC -0.00 (0.12%) today 11 Oct, 1:05 pm UTC · Disclaimer  8:00 am Tuesday, in London, UK is 12:00 am Tuesday, in California, USA  English – detected ⇄ Spanish thank you ˈTHaNGk ˌyo͞o gracias Translations of thank you adverb bien well, good, right, nicely, properly, alright
sqrt	Square root	sqrt(3)	1.73205080757
i	Imaginary number. 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 integers. (Combinatorics)	6 choose 4	15
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

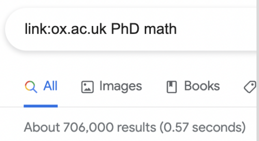
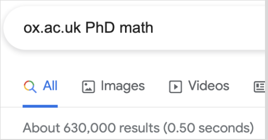
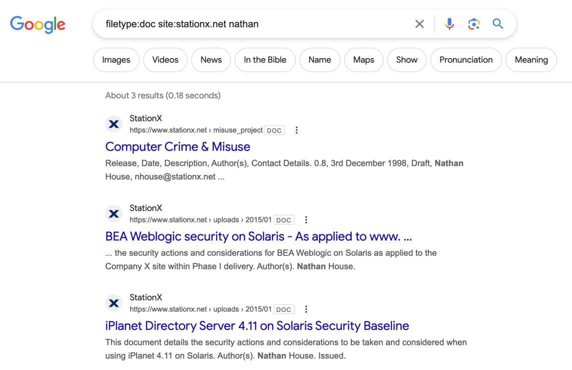
timer	Timer	timer for 20 minutes	
[This has no specific operator]	Generate a random number. Find more on the drop-down dialog box labeled “Tools” on the results page.	flip a coin, roll a dice, show random number from 10 to 40	 Flip a coin Tails FLIP AGAIN GAMES & TOYS TOOLS Roll a die Metronome Calculator Tuner Meditate  
[graph] EXPRESSION [from A to B]	Graph a mathematical EXPRESSION with variables x and y on an (optional) numerical range from A to B. The “graph” keyword is only necessary if Google doesn’t understand your query.	sin(x)/x, graph log(x), sqrt(x^2+y^2) from -20 to 20	  

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
@youtube trending shorts	Find short clips trending on YouTube
@reddit memes -dark	Find memes on Reddit that are not dark
site:cdn.cloudflare.net filetype:pdf	Find PDFs on the *.cdn.cloudflare.net domain
secret in spanish inurl:dict	Translate the word “secret” to Spanish and limit results to URLs containing “dict”
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:  link:ox.ac.uk PhD math About 706,000 results (0.57 seconds)  ox.ac.uk PhD math About 630,000 results (0.50 seconds)
filetype:doc site:stationx.net nathan	StationX with the .doc extension. This looks for legacy Microsoft Word files containing the keyword “nathan” (founder’s name).  filetype:doc site:stationx.net nathan Google Images Videos News In the Bible Name Maps Show Pronunciation Meaning About 3 results (0.18 seconds) StationX https://www.stationx.net › misuse_project DOC Computer Crime & Misuse Release, Date, Description, Author(s), Contact Details. 0.8, 3rd December 1998, Draft, **Nathan** House, nhouse@stationx.net ... StationX https://www.stationx.net › uploads › 2015/01 DOC BEA Weblogic security on Solaris - As applied to www. ... ... the security actions and considerations for BEA Weblogic on Solaris as applied to the Company X site within Phase I delivery. Author(s). **Nathan** House. StationX https://www.stationx.net › uploads › 2015/01 DOC iPlanet Directory Server 4.11 on Solaris Security Baseline This document details the security actions and considerations to be taken and considered when using iPlanet 4.11 on Solaris. Author(s). **Nathan** House. Issued.

How to Prevent Google Dorks

With great power comes great responsibility, and even if you use Google Dorks with the utmost care, other entities may not. Here are some suggestions to avoid becoming the next victim of unwanted 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 nmap, 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.

Conclusion

Ethical and legal considerations abound when using Google dorks. They are such powerful tools for uncovering data and locating vulnerabilities that your intention and frequency in using them are paramount to your Google dorking experience. Google dorking is an invaluable tool for practical cyber security research when used responsibly.

We hope this cheat sheet is helpful to you as a penetration tester, ethical hacker, or someone interested in the security position of your enterprise. 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.