APRIL 4, 2023 / #PENETRATION TESTING

Google Dorking for Penetration Testers — A Practical Tutorial

Manish Shivanandhan

Every day, Google processes over 8.5 billion searches. We know how much we use Google daily.

With the crawling capabilities of Google, it can also be a powerful tool for pen testers. Google can help us find exposed files, scripts and other critical resources in web applications.

Google Dorks are special search terms that help locate information which is not found through regular web searches.

In this article, we will look at what Google Dorks are and how they can help us in penetration testing.

What are Google Dorks?

A Google Dork is a special search term. These terms, when used with regular search keywords, can help us discover hidden resources crawled by Google.

These resources include sensitive information such as usernames, passwords, credit card numbers, email addresses, shell scripts, user accounts, and so on.

These Dorks are not limited to Google. We can also use them with search engines like Bing and Yahoo. The results might vary, but they still serve the same purpose.

To harness the full potential of Google Dorking, we'll need to master some specialized search operators. These operators will fine-tune our search results and help us find exactly what we are looking for.

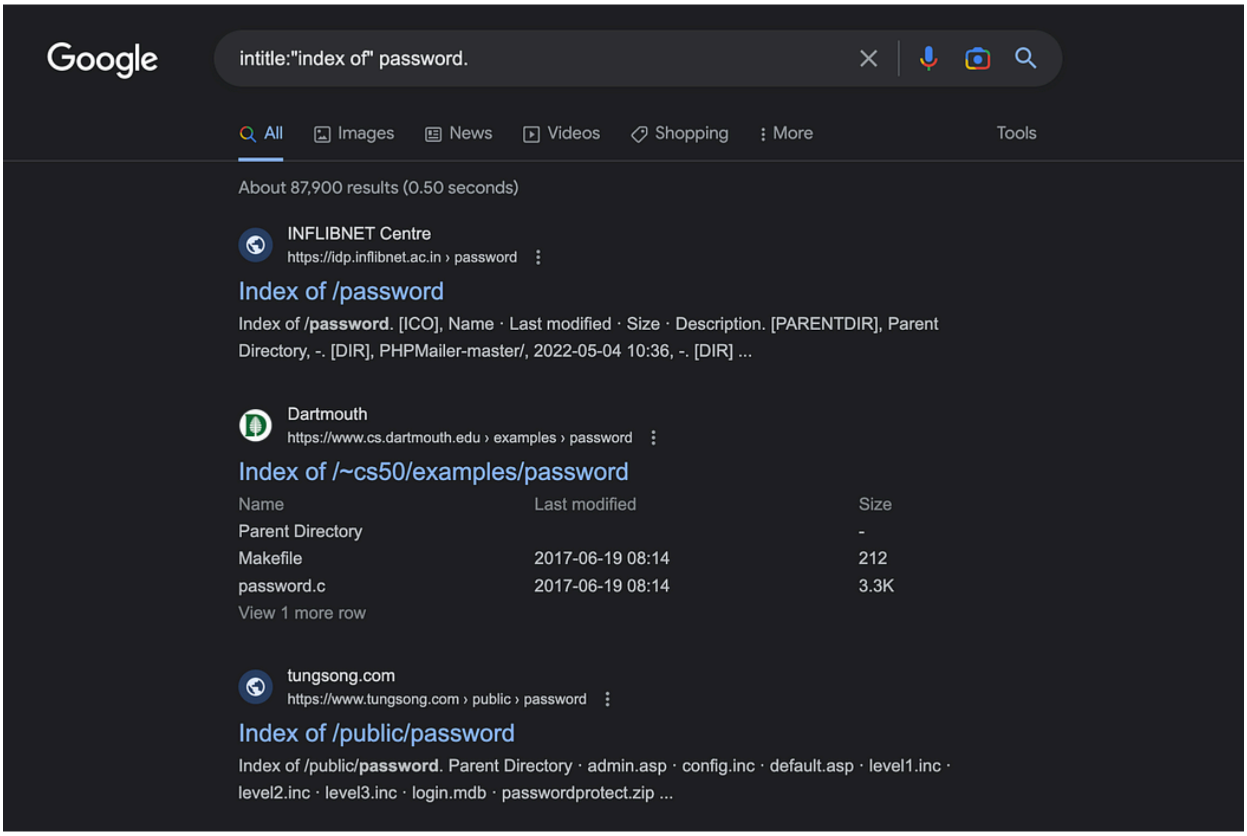
Let's try a few Google dorks.

Common Google Dorks

Some of the common query operators in Google Dorking include search modifiers. These search modifiers allow us to find specific information that may not be accessible through traditional search methods.

Intitle operator

The “**intitle**” operator searches for web pages with specific words or phrases in the title tag. For instance, if you’re looking for pages that contain the phrase “password” and have “index of” in the title, you would use the search term:intitle:”index of” password.



About 87,900 results (0.50 seconds)

INFLIBNET Centre
https://idp.inflibnet.ac.in › password

Index of /password

Index of /**password**. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], PHPMailer-master/, 2022-05-04 10:36, -. [DIR] ...

Dartmouth
https://www.cs.dartmouth.edu › examples › password

Index of /~cs50/examples/password

Name	Last modified	Size
Parent Directory		-
Makefile	2017-06-19 08:14	212
password.c	2017-06-19 08:14	3.3K

View 1 more row

tungsong.com
https://www.tungsong.com › public › password

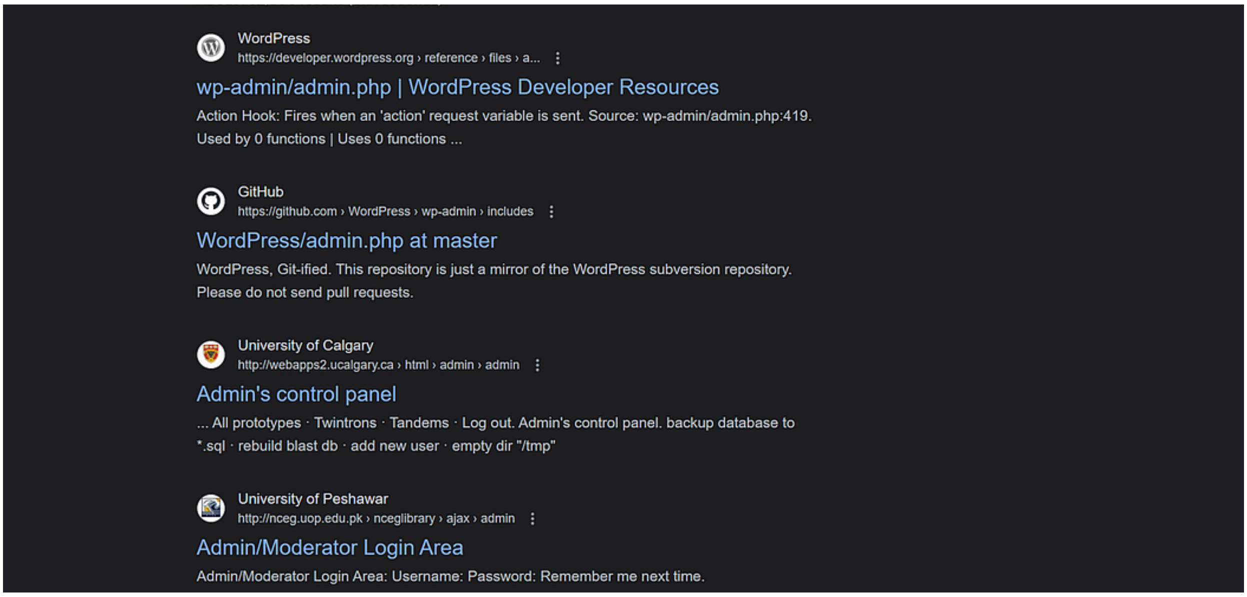
Index of /public/password

Index of /public/**password**. Parent Directory · admin.asp · config.inc · default.asp · level1.inc · level2.inc · level3.inc · login.mdb · passwordprotect.zip ...

In title. Image by the author.

Inurl operator

The “**inurl**” operator searches for web pages that contain specific words or phrases in the URL. For example, if you’re looking for pages that contain “admin.php” in the URL, you would use the search term:inurl:admin.php.



WordPress
https://developer.wordpress.org › reference › files › a...

wp-admin/admin.php | WordPress Developer Resources

Action Hook: Fires when an 'action' request variable is sent. Source: wp-admin/admin.php:419. Used by 0 functions | Uses 0 functions ...

GitHub
https://github.com › WordPress › wp-admin › includes

WordPress/admin.php at master

WordPress, Git-ified. This repository is just a mirror of the WordPress subversion repository. Please do not send pull requests.

University of Calgary
http://webapps2.ucalgary.ca › html › admin › admin

Admin's control panel

... All prototypes · Twintrons · Tandems · Log out. Admin's control panel. backup database to *.sql · rebuild blast db · add new user · empty dir "/tmp"

University of Peshawar
http://nceg.uop.edu.pk › nceglibrary › ajax › admin

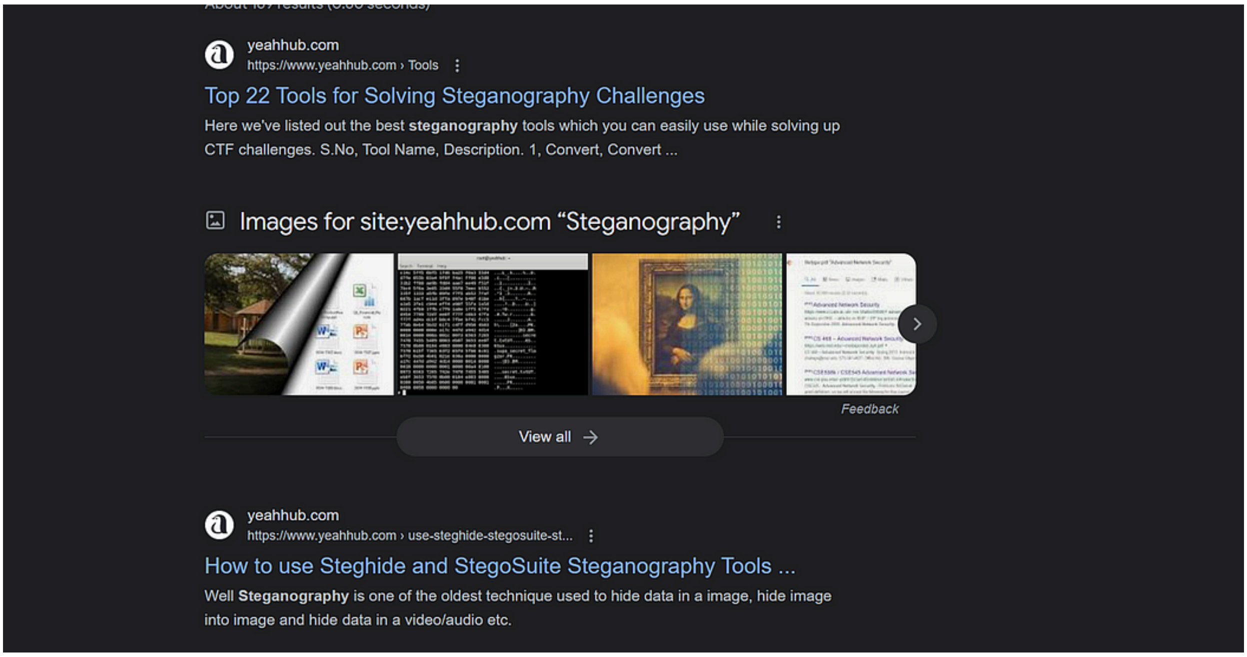
Admin/Moderator Login Area

Admin/Moderator Login Area: Username: Password: Remember me next time.

In url. Image by the author.

Site operator

The “**site**” operator allows you to search within a specific website or domain. For instance, if you’re looking for pages on the example.com domain that contain the word “Steganography”, you would use the search term:site:yeahhub.com “Steganography”



yeahhub.com
https://www.yeahhub.com › Tools

Top 22 Tools for Solving Steganography Challenges

Here we've listed out the best **steganography** tools which you can easily use while solving up CTF challenges. S.No, Tool Name, Description. 1, Convert, Convert ...

Images for site:yeahhub.com "Steganography"

yeahhub.com
https://www.yeahhub.com › use-steghide-stegosuite-st...

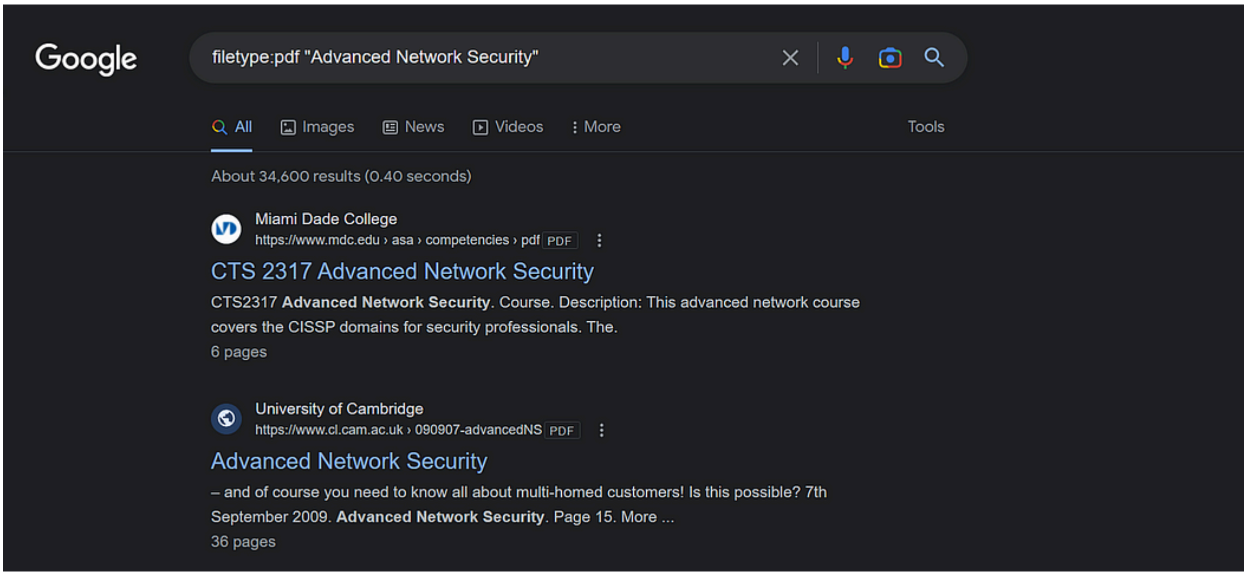
How to use Steghide and StegoSuite Steganography Tools ...

Well **Steganography** is one of the oldest technique used to hide data in a image, hide image into image and hide data in a video/audio etc.

In site. Image by the author.

Filetype operator

The "**filetype**" operator allows you to search for specific file types, such as PDFs or Word documents. For example, if you're looking for PDF files that contain the phrase "confidential report", you would use the search term:filetype:pdf "Advanced Network Security"



filetype:pdf "Advanced Network Security"

About 34,600 results (0.40 seconds)

Miami Dade College
https://www.mdc.edu › asa › competencies › pdf PDF

CTS 2317 Advanced Network Security

CTS2317 **Advanced Network Security**. Course. Description: This advanced network course covers the CISSP domains for security professionals. The.
6 pages

University of Cambridge
https://www.cl.cam.ac.uk › 090907-advancedNS PDF

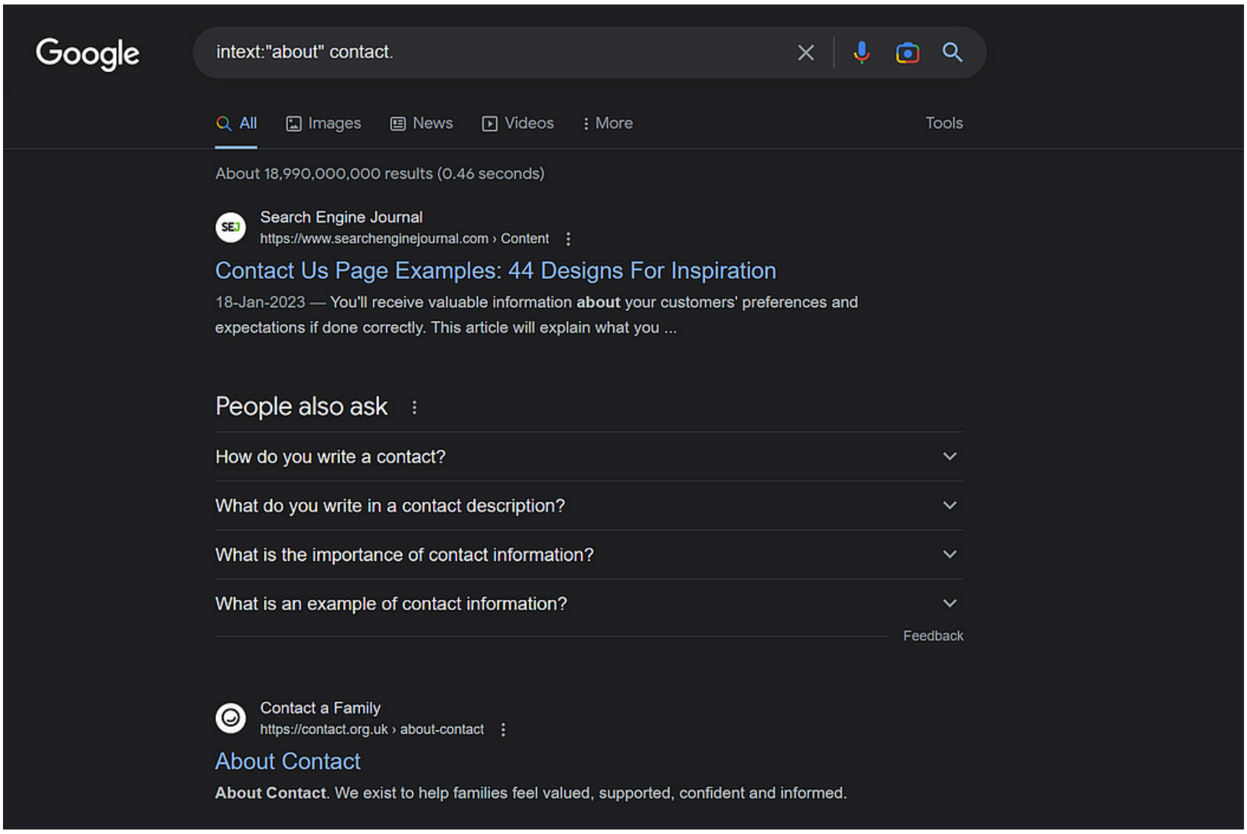
Advanced Network Security

– and of course you need to know all about multi-homed customers! Is this possible? 7th September 2009. **Advanced Network Security**. Page 15. More ...
36 pages

Filetype. Image by the author.

intext operator

The “**intext**” operator searches for pages that contain specific words or phrases within the body of the page. For instance, if you’re looking for pages that contain both the words “login” and “password” within the body of the page, you would use the search term:intext:"about" contact.



About 18,990,000,000 results (0.46 seconds)

Search Engine Journal
https://www.searchenginejournal.com › Content

Contact Us Page Examples: 44 Designs For Inspiration

18-Jan-2023 — You'll receive valuable information **about** your customers' preferences and expectations if done correctly. This article will explain what you ...

People also ask

How do you write a contact?

What do you write in a contact description?

What is the importance of contact information?

What is an example of contact information?

Feedback

Contact a Family
https://contact.org.uk › about-contact

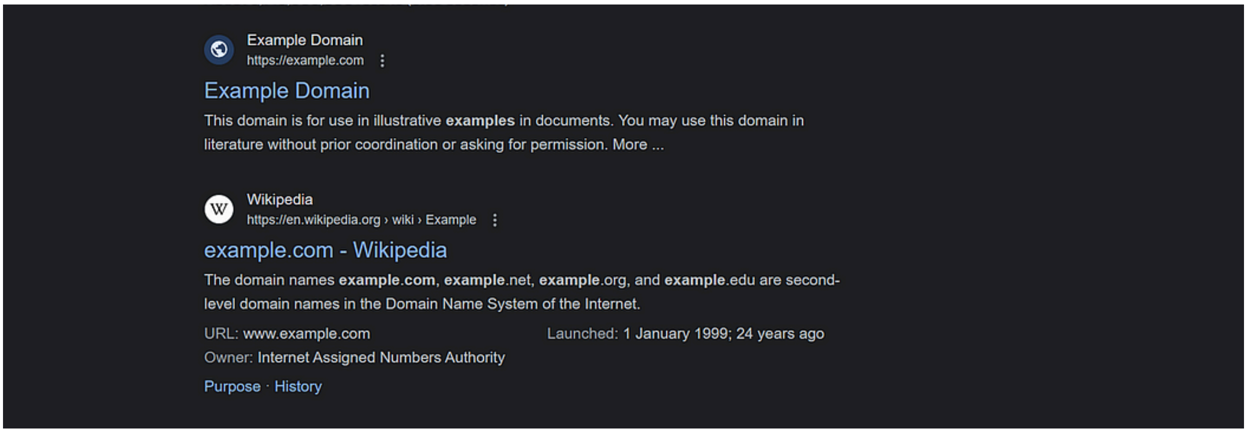
About Contact

About Contact. We exist to help families feel valued, supported, confident and informed.

In text. Image by the author.

Link operator

The “**link**” operator searches for web pages that link to a specific URL. For example, if you’re looking for web pages that link to the example.com domain, you would use the search term:link:”example.com”



Example Domain
https://example.com

Example Domain

This domain is for use in illustrative **examples** in documents. You may use this domain in literature without prior coordination or asking for permission. More ...

Wikipedia
https://en.wikipedia.org › wiki › Example

example.com - Wikipedia

The domain names **example.com**, **example**.net, **example**.org, and **example**.edu are second-level domain names in the Domain Name System of the Internet.

URL: www.example.com Launched: 1 January 1999; 24 years ago
Owner: Internet Assigned Numbers Authority

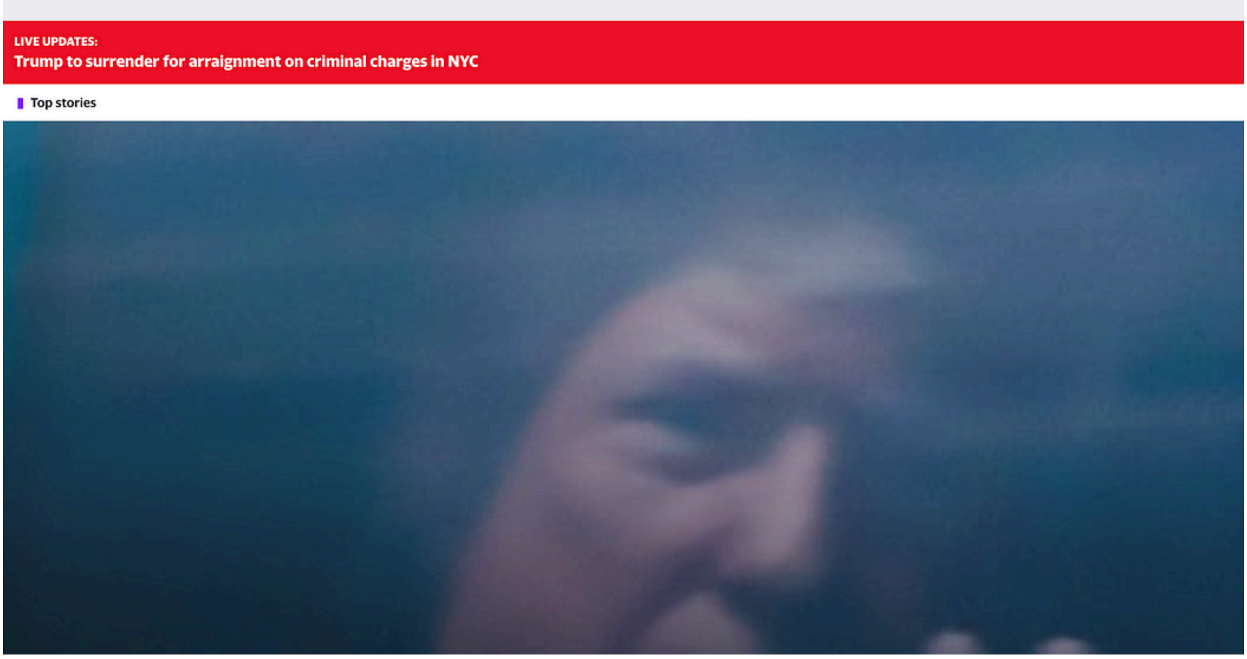
Purpose · History

Link operator. Image by the author.

Cache operator

The "**cache**" operator is used to retrieve the cached version of a web page. When you search for a website using Google, Google creates a cached version of that page in its system. This version can be useful if the original website is temporarily down or if you want to view an older version of the website.

Here is the syntax to find the cached version of yahoo.com.cache:https://www.yahoo.com

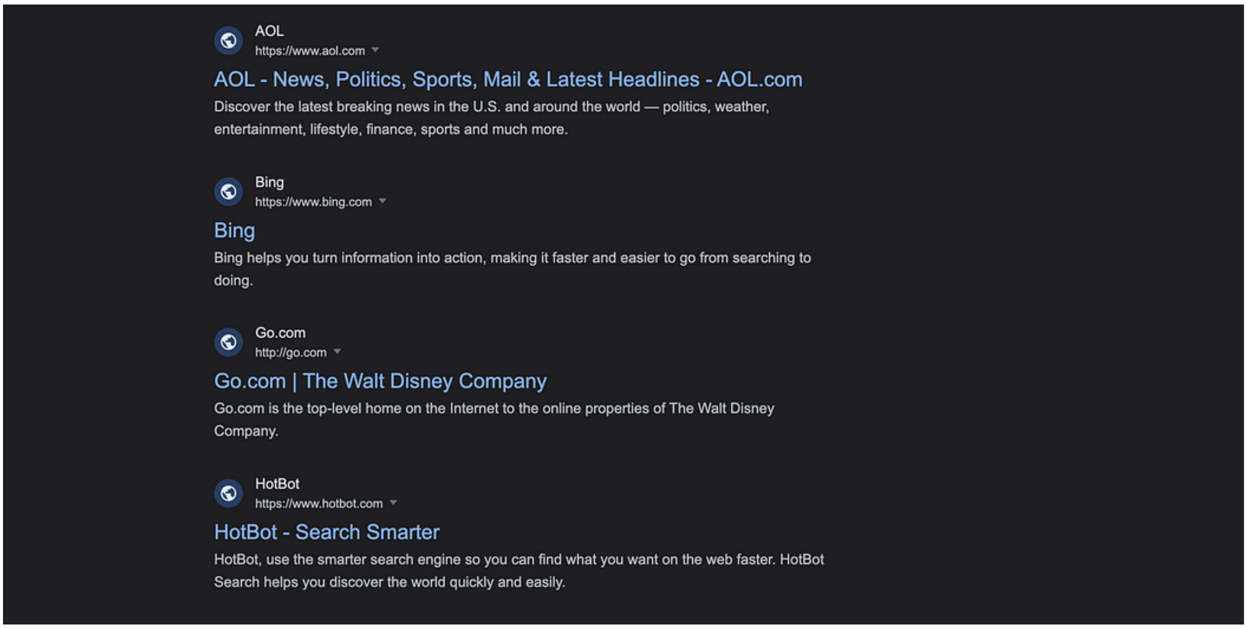


LIVE UPDATES:
Trump to surrender for arraignment on criminal charges in NYC

Cached version of yahoo.com. Image by author.

Related operator

The “**related**” operator is used to find web pages that are related to a specific URL. Here is the syntax to use the “related” operator to find sites similar to yahoo.com.



AOL
https://www.aol.com
AOL - News, Politics, Sports, Mail & Latest Headlines - AOL.com
Discover the latest breaking news in the U.S. and around the world — politics, weather, entertainment, lifestyle, finance, sports and much more.

Bing
https://www.bing.com
Bing
Bing helps you turn information into action, making it faster and easier to go from searching to doing.

Go.com
http://go.com
Go.com | The Walt Disney Company
Go.com is the top-level home on the Internet to the online properties of The Walt Disney Company.

HotBot
https://www.hotbot.com
HotBot - Search Smarter
HotBot, use the smarter search engine so you can find what you want on the web faster. HotBot Search helps you discover the world quickly and easily.

Related operator. Image by author.

By combining these operators in creative ways, you can find specific types of information on the web that can be useful for penetration testing and other purposes.

Structure of Query Operators

Google Dorking query operators have a structure similar to regular Google search query operators. This technique involves using advanced operators and search queries to uncover information that is not typically available through regular searches.

The general structure of query operators in Google Dorking includes three elements:

1. **Operator**: A specific keyword or symbol that instructs Google what to search for. For instance, the "**inurl**" operator searches for pages that contain a particular keyword in their URL.

keyword.

3. **Modifier:** An additional search parameter that you can use to further refine your search. For example, the “**filetype**” modifier searches for a specific file type, such as a PDF.

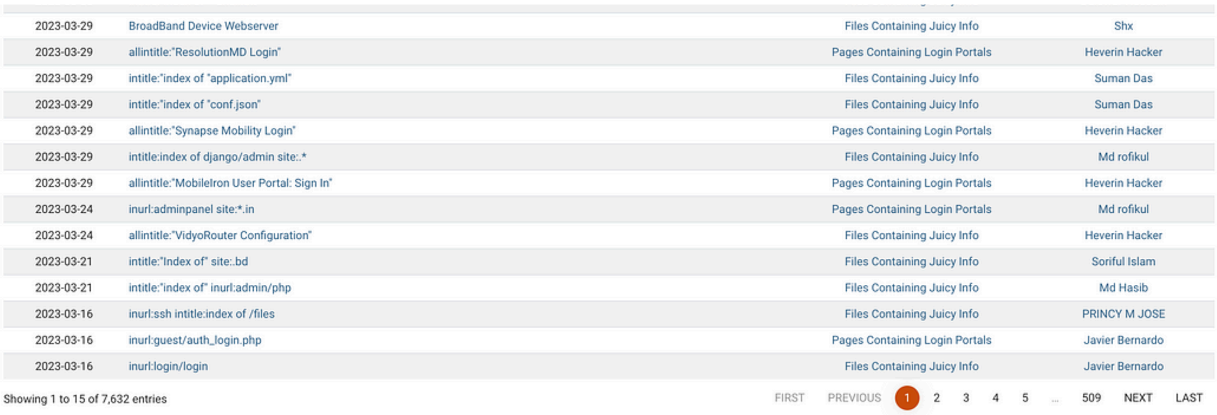
Here’s an example of a query operator structure in Google Dorking: intitle: “index of” site:example.com password filetype:pdf

This query uses the “**intitle**” operator to search for pages with “index of” in their title, the “site” operator to search within the example.com domain, the keyword “password,” and the “filetype” modifier to search for PDF files.

By utilizing query operators in Google Dorking, we can find useful and often vulnerable information that might not be accessible through regular searches.

Google Hacking Database (GHDB)

The Google Hacking Database (GHDB) is a compilation of search queries and query operators that help us in Google Dorking.



2023-03-29	BroadBand Device Webserver	Files Containing Juicy Info	Shx
2023-03-29	allintitle:"ResolutionMD Login"	Pages Containing Login Portals	Heverin Hacker
2023-03-29	intitle:"index of "application.yml"	Files Containing Juicy Info	Suman Das
2023-03-29	intitle:"index of "conf.json"	Files Containing Juicy Info	Suman Das
2023-03-29	allintitle:"Synapse Mobility Login"	Pages Containing Login Portals	Heverin Hacker
2023-03-29	intitle:index of django/admin site:.*	Files Containing Juicy Info	Md rofikul
2023-03-29	allintitle:"MobileIron User Portal: Sign In"	Pages Containing Login Portals	Heverin Hacker
2023-03-24	inurl:adminpanel site:*.in	Pages Containing Login Portals	Md rofikul
2023-03-24	allintitle:"VidyoRouter Configuration"	Files Containing Juicy Info	Heverin Hacker
2023-03-21	intitle:"Index of" site:.bd	Files Containing Juicy Info	Soriful Islam
2023-03-21	intitle:"index of" inurl:admin/php	Files Containing Juicy Info	Md Hasib
2023-03-16	inurl:ssh intitle:index of /files	Files Containing Juicy Info	PRINCY M JOSE
2023-03-16	inurl:guest/auth_login.php	Pages Containing Login Portals	Javier Bernardo
2023-03-16	inurl:login/login	Files Containing Juicy Info	Javier Bernardo

Showing 1 to 15 of 7,632 entries

Google hacking database. Image generated by author.

Johnny Long, a well-known security researcher and author, established the GHDB. It has since become a valuable resource for security engineers like you and me.

The GHDB has several search queries and operators that can uncover numerous sensitive files, vulnerable web servers, and applications. It can also discover default login pages and credentials, as well as network and security devices that may be prone to attack.

GHDB is arranged into categories such as "Files containing passwords" "Vulnerable servers" "Footholds" and "Error Messages". Each category contains several search queries and operators crafted to reveal specific information about a target.

Please note that search queries and operators in the GHDB might produce false positives or outdated information. Always verify the information obtained through these search operators.

A Dorking Scenario

Let's assume you have to conduct a pentesting audit for a client. Here is a sample dorking scenario.