



3234



Google Dorking

Explaining how Search Engines work and leveraging them into finding hidden content!

Start AttackBox

Show Split View

Cloud Details

Awards

Help

×

Chart

Scoreboard

Video

Discuss

Writeups

More

Difficulty: Easy

Google Dorking | DarkStar • Jan 16, 2021

Source: YouTube

TryHackMe Google Dorking Official Walkthrough



Active Machine Information

Loading...

Loading...

Loading...


Loading...

75%

- Task 1 ☒ Ye Ol' Search Engine ▼
- Task 2 ☒ Let's Learn About Crawlers ▼
- Task 3 ☐ Enter: Search Engine Optimisation ▼
- Task 4 ☒ Beepboop - Robots.txt ▼
- Task 5 ☒ Sitemaps ▼
- Task 6 ☐ What is Google Dorking? ▼

Using Google for Advanced Searching

As we have previously discussed, Google has a lot of websites crawled and indexed. Your average Joe uses Google to look up Cat pictures (I'm more of a Dog person myself...). Whilst Google will have many Cat pictures indexed ready to serve to Joe, this is a rather trivial use of the search engine in comparison to what it can be used for. For example, we can add operators such as that from programming languages to either increase or decrease our search results - or perform actions such as arithmetic!



12 + 1

🔍

🔍 All

📍 Maps

📰 News

🖼️ Images


🛒 Shopping

⋮ More

⚙️ Settings

🔧 Tools


About 25,270,000,000 results (0.55 seconds)



A privacy reminder from Google

REMIND ME LATER

REVIEW



12 + 1 =

13

Say if we wanted to narrow down our search query, we can use quotation marks. Google will interpret everything in between these quotation marks as exact and only return the results of the exact phrase provided...Rather useful to filter through the rubbish that we don't need as we have done so below:

"american pscho poster"

All

Images

Shopping

News

Videos

More

Settings

Tools

About 46,100 results (0.44 seconds)

Showing results for "american **psycho** poster"

Search instead for "american pscho poster"

Images for "american psycho poster"

minimalist


original

movie

alternative

book

retro



More images for "american psycho poster"

Report images

www.redbubble.com > Wall Art > Poster

American Psycho Posters | Redbubble

patrick bateman, american psycho, phone, cellphone, cell, christian, bale, christian bale, dubs, checkern. Patrick Bateman on Phone (American Psycho) Poster.

Refining our Queries

We can use terms such as “**site**” (such as [bbc.co.uk](#)) and a query (such as “gchq news”) to search the specified site for the keyword we have provided to filter out content that may be harder to find otherwise. For example, using the “site” and “query” of “bbc” and “gchq”, we have modified the order of which Google returns the results.

In the screenshot below, searching for “gchq news” returns approximately 1,060,000 results from Google. The website that we want is ranked behind GCHQ’s actual website:

Google

gchq news

All

News

Maps

Images

Videos

More

Settings

Tools

About 1,060,000 results (0.36 seconds)

www.gchq.gov.uk > section > news > latestnews

Latest News - GCHQ

The latest **news** from **GCHQ**. ... Latest **News**. The latest **news** from **GCHQ**. 130 items. Sort by: Most recent, A-Z, Z-A. Dropdown Icon ...

www.bbc.co.uk > news > topics > gchq

GCHQ - BBC News

BBC Security Correspondent Gordon Corera becomes the first journalist allowed to record inside **GCHQ's** listening station at Bude, which has spied on global ...

But we don’t want that...We wanted “**bbc.co.uk**” first, so let’s refine our search using the “**site**” term. Notice how in the screenshot below, Google returns with much fewer results? Additionally, the page that we didn’t want has disappeared, leaving the site that we did actually want!

Google

site: bbc.co.uk gchq news

All

News

Images

Shopping

Videos

More

Settings

Tools

About 344,000 results (0.42 seconds)

www.bbc.co.uk > news > topics > gchq

GCHQ - BBC News

All the latest **news** about **GCHQ** from the **BBC**. ... Rebel Tory MPs fail to pass their amendment blocking the **company's** involvement in the **UK's** 5G network.

www.bbc.co.uk > news > uk-england-london-47819408

Drab London office block was GCHQ spy base - BBC News

5 Apr 2019 - **GCHQ** acknowledged the location after moving out of its home. Director Jeremy Fleming said the **site** in Palmer Street, used by intelligence ...

Of course, in this case, GCHQ is quite a topic of discussion - so there'll be a load of results regardless.

So What Makes "Google Dorking" so Appealing?

First of all - and the important part - it's legal! It's all indexed, publicly available information. However, what you do with this is where the question of legality comes in to play...

A few common terms we can search and combine include:

Term	Action
filetype:	Search for a file by its extension (e.g. PDF)
cache:	View Google's Cached version of a specified URL
intitle:	The specified phrase MUST appear in the title of the page

For example, let's say we wanted to use Google to search for all PDFs on [bbc.co.uk](#):

site:bbc.co.uk filetype:pdf

Google

site:bbc.co.uk filetype:pdf

🔊 🔍

🔍 All

🖼 Images

📰 News

🛒 Shopping

📍 Maps

⋮ More

Settings

Tools

About 46,300 results (0.34 seconds)

downloads.bbc.co.uk › london

pdf

XXXX Dear XXXX, RE: Freedom of Information Request ... - BBC
5 Jan 2011 - The detailed information on services outside the Top 10, relating to those services and passengers in excess of capacity, that is being withheld ...

downloads.bbc.co.uk › commissioning › site › pascl

PDF

BBC PasC
20 Mar 2002 - PDU PRODUCTIONS (AS ABOVE) ?? State where relevant whether the Producer/Director is Continuing Staff (CS) Guest Staff (GS) or Short ...

downloads.bbc.co.uk › spanish › manual_biodigestor

PDF

[Translate this page](#)

biodigestor - Producción Animal
by RB Bolero - Cited by 72 - Related articles
Se resume la experiencia adquirida por los autores durante la instalación y puesta en funcionamiento de biodigestores del tipo Taiwán (flujo continuo) Estos se.

www.bbc.co.uk › oxford › glyme

PDF

Glyme Valley Way - Oxfordshire Cotswolds
The Glyme Valley Way was devised by BBC Oxford and Oxfordshire County Council's Countryside Service as part of Oxfordshire 2007 which is celebrating a ...

Great, now we've refined our search for Google to query for all publically accessible PDFs on "**bbc.co.uk**" - You wouldn't have found files like this "Freedom of Information Request Act" file from a wordlist!

Here we used the extension **PDF**, but can you think of any other file formats of sensitive nature that **may** be publically accessible? (Often unintentionally!!) Again, what you do with any results that you find is where the legality comes into play - this is why "Google Dorking" is so great/dangerous.

Here is simple directory traversal.

I have blanked out a lot of the below to cover you, me, THM and the owners of the domains:

Google

intitle:index.of

🔊 🔍

🔍 All

🖼 Images

📰 News

📺 Videos

📖 Books

⋮ More

Settings

Tools

[REDACTED]

[REDACTED]

Index of /downloads

[REDACTED]

[REDACTED]

Index of [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Index of /

[REDACTED]

Index of / [REDACTED]

Name	Last modified	Size	Description
Parent Directory		-	
[REDACTED]			

Answer the questions below

What would be the format used to query the site bbc.co.uk about flood defences

Answer format: ****. ***.*.*** *****

Submit

Hint

What term would you use to search by file type?

Answer format: *****:

Submit

What term can we use to look for login pages?

Answer format: *****; *****

Submit

Hint

Created by



cmnatic

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 69672 users are in here and this room is 861 days old.

