OSINT – Google dorks

OsintItalia
ASSOCIAZIONE di PROMOZIONE SOCIALE

Alessia Gianaroli

Mirko LAPI

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

This presentation is licensed under the Creative Commons BY-NC License

To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

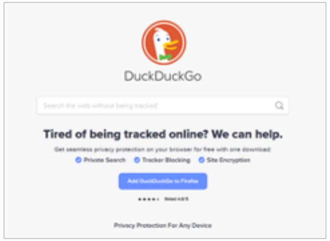
- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Outline

- Search engines overview
- Google
- Dorks
- Exploit-DB
- Dorksearch

Search Engines

Search engines are one of the most common and easy method of utilizing OSINT



DuckDuckGo

Search the web without being tracked

Tired of being tracked online? We can help.

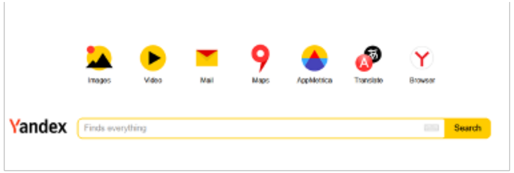
Get seamless privacy protection on your browser for free with one download:

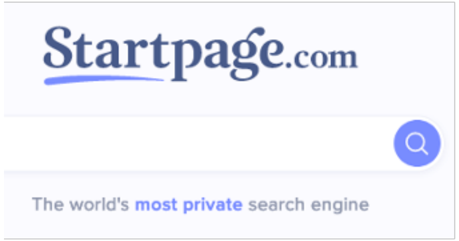
Private Search Tracker Blocking Site Encryption

Add DuckDuckGo to Firefox

★★★★☆ Rated 4.6/5

Privacy Protection For Any Device





Startpage.com

The world's **most private** search engine

This website uses cookies to ensure you get the best search experience. More information

I Agree

eTools

Search

Welcome to eTools.ch, the transparent Metasearch Engine from Switzerland

Google

In October 2019 Google introduced the Bidirectional Encoder Representations from Transformers (BERT)

With this system the search considers the full context of the query (surrounding and directional words)

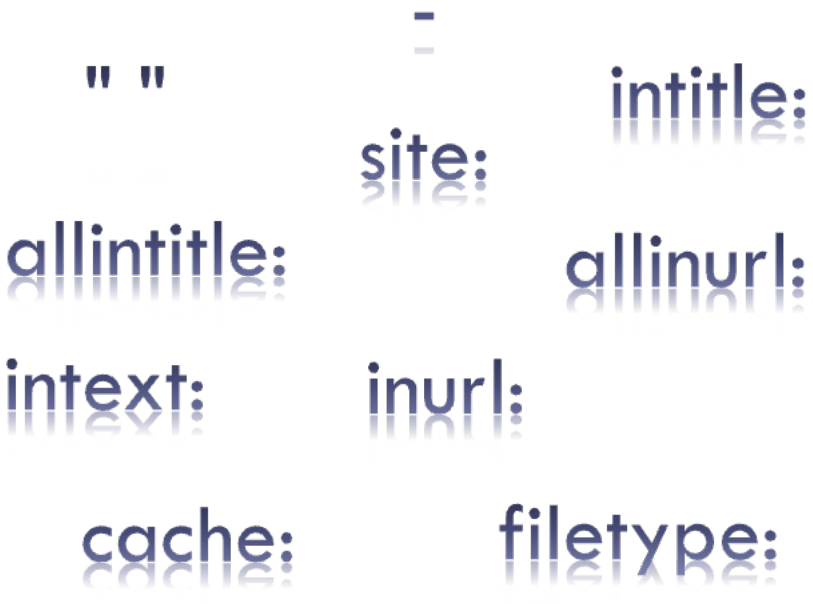
Dorks

Google Dork queries can be used to find

- XSS, SQLi, and other parameter-based vulnerabilities in web applications
- Confidential information from websites, such as usernames, passwords, and other forms of personally identifiable information (PII)
- Information on printers, video cameras, and types of IOT devices
- any other type of research…

Basic search dorks

This part will focus on the absolute essential search modifiers that we need learn and memorize



OR

- The "OR" used between two words or expressions will bring back all the links containing one or the other of these words or expressions
- This saves our time because we don't need to conduct multiple queries

Quotation marks

- Insert a search term in quotation marks will match the exact text we are looking for
- For example, if we conducted a search for "live view" without quotes, the result is about 11,560,000,000 results because all these pages do not have these two words right next to each other
- Searching for the term "live view", including quotes, reduces the search results to about 8,810,000 pages
- While to add "camera system" reduces our results to about 291,000 pages

site:

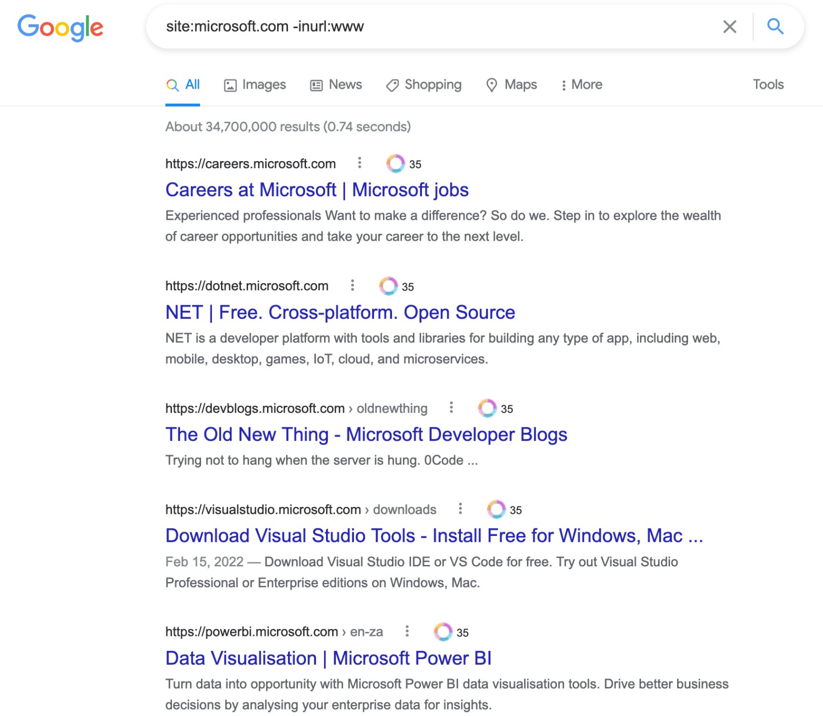
The site: search operator will return search results only on the specified website

- **site**:www.salute.gov.it→ to search all pages of a domain
- **site**:salute.gov.it→ to find all urls including subdomains
- **site**:salute.gov.it/portale/ministro → to search from a directory
- **site**:it → all pages of a top-level domain (e.g.: com, gov, edu, etc…)

The minus sign -

- The hyphen tells most search engines and social network to exclude the text immediately following from any results
- It is important to never include a space between the hyphen and filtered text

site:microsoft.com -inurl:www



About 34,700,000 results (0.74 seconds)

https://careers.microsoft.com 35

Careers at Microsoft | Microsoft jobs

Experienced professionals Want to make a difference? So do we. Step in to explore the wealth of career opportunities and take your career to the next level.

https://dotnet.microsoft.com 35

NET | Free. Cross-platform. Open Source

NET is a developer platform with tools and libraries for building any type of app, including web, mobile, desktop, games, IoT, cloud, and microservices.

https://devblogs.microsoft.com › oldnewthing 35

The Old New Thing - Microsoft Developer Blogs

Trying not to hang when the server is hung. 0Code ...

https://visualstudio.microsoft.com › downloads 35

Download Visual Studio Tools - Install Free for Windows, Mac ...

Feb 15, 2022 — Download Visual Studio IDE or VS Code for free. Try out Visual Studio Professional or Enterprise editions on Windows, Mac.

https://powerbi.microsoft.com › en-za 35

Data Visualisation | Microsoft Power BI

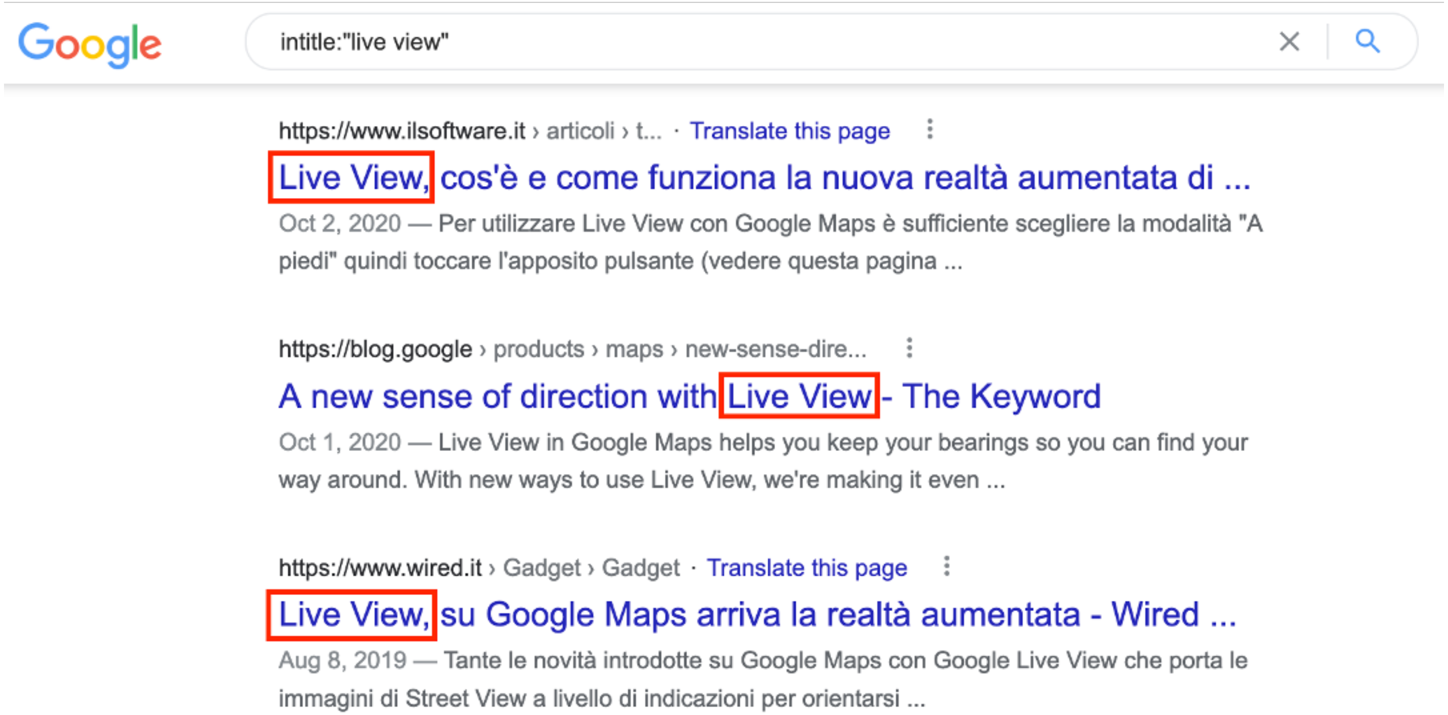
Turn data into opportunity with Microsoft Power BI data visualisation tools. Drive better business decisions by analysing your enterprise data for insights.

The intitle: & allintitle:

- The intitle: operator give us results that show only those pages that have the specified search term in their page/HTML title. The following search term will return all sites with Microsoft in their title
- The allintitle: operator allow us to simplify our query. Google will only show us search results where all the search words are contained in the title of a page

Example `intitle:index of contacts.txt`

The intitle:



intitle:"live view"

https://www.ilsoftware.it › articoli › t... · Translate this page

Live View, cos'è e come funziona la nuova realtà aumentata di ...

Oct 2, 2020 — Per utilizzare Live View con Google Maps è sufficiente scegliere la modalità "A piedi" quindi toccare l'apposito pulsante (vedere questa pagina ...

https://blog.google › products › maps › new-sense-dire...

A new sense of direction with Live View - The Keyword

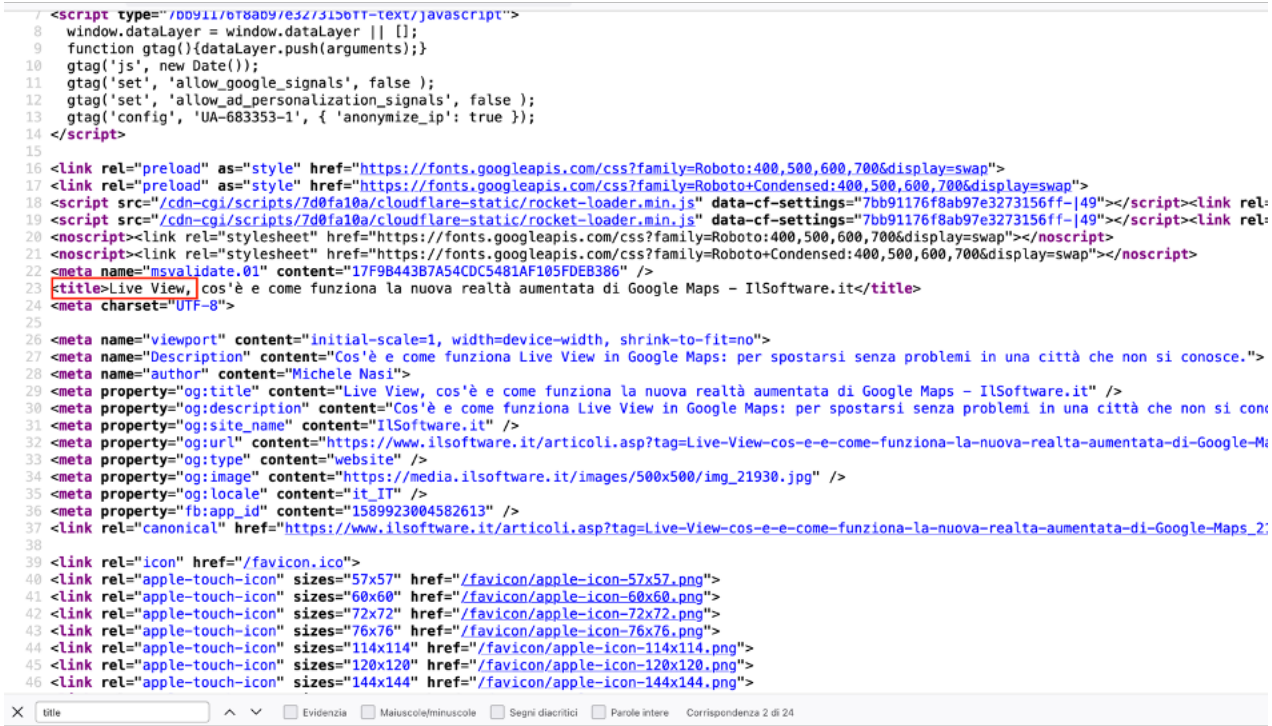
Oct 1, 2020 — Live View in Google Maps helps you keep your bearings so you can find your way around. With new ways to use Live View, we're making it even ...

https://www.wired.it › Gadget › Gadget · Translate this page

Live View, su Google Maps arriva la realtà aumentata - Wired ...

Aug 8, 2019 — Tante le novità introdotte su Google Maps con Google Live View che porta le immagini di Street View a livello di indicazioni per orientarsi ...

The intitle:



```
<script type="7bb91176f8ab97e3273156ff-text/javascript">
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());
  gtag('set', 'allow_google_signals', false );
  gtag('set', 'allow_ad_personalization_signals', false );
  gtag('config', 'UA-683353-1', { 'anonymize_ip': true });
</script>

<link rel="preload" as="style" href="https://fonts.googleapis.com/css?family=Roboto:400,500,600,700&display=swap">
<link rel="preload" as="style" href="https://fonts.googleapis.com/css?family=Roboto+Condensed:400,500,600,700&display=swap">
<script src="/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js" data-cf-settings="7bb91176f8ab97e3273156ff-|49"></script><link rel=
<script src="/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js" data-cf-settings="7bb91176f8ab97e3273156ff-|49"></script><link rel=
<noscript><link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:400,500,600,700&display=swap"></noscript>
<noscript><link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto+Condensed:400,500,600,700&display=swap"></noscript>
<meta name="msvalidate.01" content="17F9B443B7A54CDC5481AF105FDEB386" />
<title>Live View, cos'è e come funziona la nuova realtà aumentata di Google Maps - IlSoftware.it</title>
<meta charset="UTF-8">

<meta name="viewport" content="initial-scale=1, width=device-width, shrink-to-fit=no">
<meta name="Description" content="Cos'è e come funziona Live View in Google Maps: per spostarsi senza problemi in una città che non si conosce.">
<meta name="author" content="Michele Nasi">
<meta property="og:title" content="Live View, cos'è e come funziona la nuova realtà aumentata di Google Maps - IlSoftware.it" />
<meta property="og:description" content="Cos'è e come funziona Live View in Google Maps: per spostarsi senza problemi in una città che non si conc
<meta property="og:site_name" content="IlSoftware.it" />
<meta property="og:url" content="https://www.ilsoftware.it/articoli.asp?tag=Live-View-cos-e-e-come-funziona-la-nuova-realta-aumentata-di-Google-Ma
<meta property="og:type" content="website" />
<meta property="og:image" content="https://media.ilsoftware.it/images/500x500/img_21930.jpg" />
<meta property="og:locale" content="it_IT" />
<meta property="fb:app_id" content="158992300458261З" />
<link rel="canonical" href="https://www.ilsoftware.it/articoli.asp?tag=Live-View-cos-e-e-come-funziona-la-nuova-realta-aumentata-di-Google-Maps_2

<link rel="icon" href="/favicon.ico">
<link rel="apple-touch-icon" sizes="57x57" href="/favicon/apple-icon-57x57.png">
<link rel="apple-touch-icon" sizes="60x60" href="/favicon/apple-icon-60x60.png">
<link rel="apple-touch-icon" sizes="72x72" href="/favicon/apple-icon-72x72.png">
<link rel="apple-touch-icon" sizes="76x76" href="/favicon/apple-icon-76x76.png">
<link rel="apple-touch-icon" sizes="114x114" href="/favicon/apple-icon-114x114.png">
<link rel="apple-touch-icon" sizes="120x120" href="/favicon/apple-icon-120x120.png">
<link rel="apple-touch-icon" sizes="144x144" href="/favicon/apple-icon-144x144.png">
```

✕ title ∧ ∨ □ Evidenzia □ Maiuscole/minuscole □ Segni diacritici □ Parole intere Corrispondenza 2 di 24

The filetype:

- The filetype: operator is useful when we are looking for specific types of files, such as PDF, DOC, CSV, XLS, etc…
- To search for a list file on a particular website, we would use the following query:

```
Example list filetype:xls site:sitename.com
```

inurl:

- The inurl: operator give us results with our search term specifically in the URL
- This does not have to be the domain name, but it can include the path or even the filename.

Example `filetype:xls inurl:passwd`

intext:

- The intext: operator will search for your specific words in the text of a web page
- This operator may seem superfluous, but it is not because intext: can be used to scan pages for any text we need, such as an email address, full name, PIL, or even keywords from an admin login screen

```
Example intext:"Real-time IP Camera Monitoring System"
```

cache:

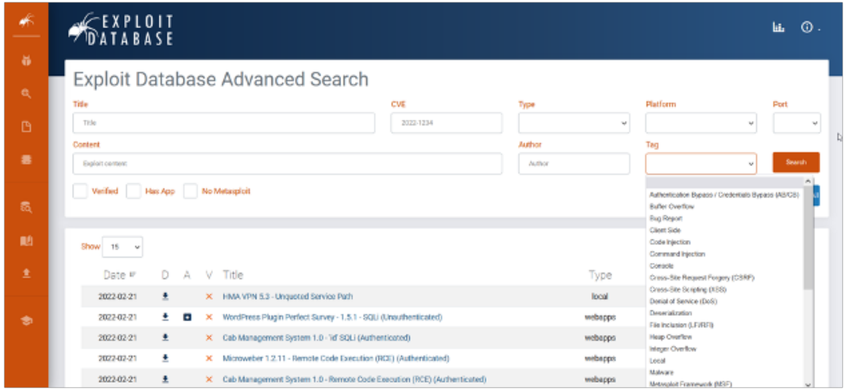
- The cache: operator is an important dork because it will let you search for pages in Google's cache
- Pages and sites come and go, and sometimes it can be necessary to look for a page or file that has been removed

```
Example cache:domain.com "search term"
```

Exploit-DB

https://www.exploit-db.com/google-hacking-database

It is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers

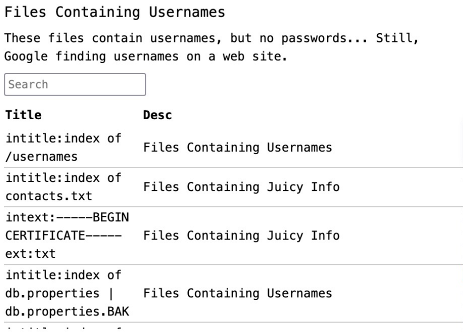


Date	D	A	V	Title	Type
2022-02-21	⬇		✗	HMA VPN 5.3 - Unquoted Service Path	local
2022-02-21	⬇	▣	✗	WordPress Plugin Perfect Survey - 1.5.1 - SQLi (Unauthenticated)	webapps
2022-02-21	⬇		✗	Cab Management System 1.0 - 'id' SQLi (Authenticated)	webapps
2022-02-21	⬇		✗	Microweber 1.2.11 - Remote Code Execution (RCE) (Authenticated)	webapps
2022-02-21	⬇		✗	Cab Management System 1.0 - Remote Code Execution (RCE) (Authenticated)	webapps

Dorksearch

https://www.dorksearch.com/

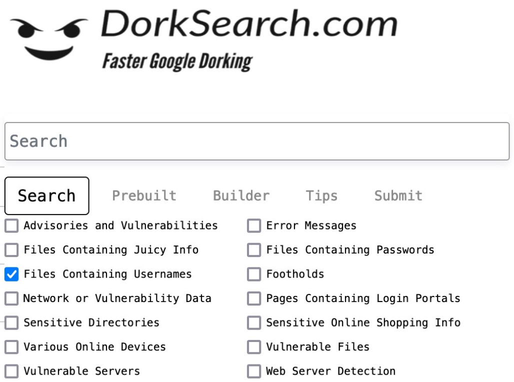
For educational purposes only. Misuse of Google Dorking can be viewed as hacking in some countries.



Files Containing Usernames

These files contain usernames, but no passwords... Still, Google finding usernames on a web site.

Title	Desc
intitle:index of /usernames	Files Containing Usernames
intitle:index of contacts.txt	Files Containing Juicy Info
intext:-----BEGIN CERTIFICATE----- ext:txt	Files Containing Juicy Info
intitle:index of db.properties | db.properties.BAK	Files Containing Usernames



- ☐ Advisories and Vulnerabilities
- ☐ Files Containing Juicy Info
- ☑ Files Containing Usernames
- ☐ Network or Vulnerability Data
- ☐ Sensitive Directories
- ☐ Various Online Devices
- ☐ Vulnerable Servers
- ☐ Error Messages
- ☐ Files Containing Passwords
- ☐ Footholds
- ☐ Pages Containing Login Portals
- ☐ Sensitive Online Shopping Info
- ☐ Vulnerable Files
- ☐ Web Server Detection

Thank you for your attention

OsintItalia
ASSOCIAZIONE di PROMOZIONE SOCIALE

Alessia Gianaroli

Mirko LAPI

CYBER
CHALLENGE.IT

CYBERSECURITY
NATIONAL
LABORATORY

cini

https://cybersecnatlab.it