HACKING

SECURITYTRAILS BLOG · LAST UPDATED ON MAR 29 2021 · BY ESTEBAN BORGES

Top 20 Google Hacking Techniques

Reading time: 15 minutes

Facebook Twitter LinkedIn

Some time ago we wrote an interesting post about the OSINT concept and its importance in the security researching world, showing how easy it is to get information from publicly available sources on the Internet.

Last week one of our developers shared an interesting link he found — one that was exposing many supposedly "private" resources from different websites.

That's when someone from our team suggested a post about this kind of data exposure issue. We've mentioned this type of security problem in previous posts, as it's a common source for security researchers to find valuable private information about any website.

Today we are going to dig into Google hacking techniques, also known as Google Dorks.

TABLE OF CONTENTS

What is a Google Dork?

A Google Dork, also known as Google Dorking or Google hacking, is a valuable resource for security researchers. For the average person, Google is just a search engine used to find text, images, videos, and news. However, in the infosec world, Google is a useful hacking tool.

How would anyone use Google to hack websites?

Well, you can't hack sites directly using Google, but as it has tremendous web-crawling capabilities, it can index almost anything within your website, including sensitive information. This means you could be exposing too much information about your web technologies, usernames, passwords, and general vulnerabilities without even knowing it.

In other words: Google "Dorking" is the practice of using Google to find vulnerable web applications and servers by using native Google search engine capabilities.

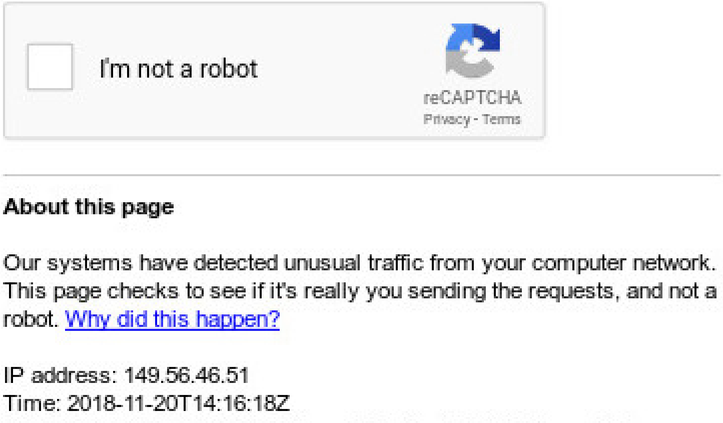
Unless you block specific resources from your website using a robots.txt file, Google indexes all the information that is present on any website. Logically, after some time any person in the world can access that information if they know what to search for. You can also access the Google Hacking Database (GHDB) which is the full Google dork list containing all Google dorking commands.

Important note: while this information is publicly available on the Internet, and it is provided and encouraged to be used by Google on a legal basis, people with the wrong intentions could use this information to harm your online presence.

Be aware that Google also knows who you are when you perform this kind of query. For this reason and many others, it's advised to use it only with good intentions, whether for your own research or while looking for ways to defend your website against this kind of vulnerability.

While some webmasters expose sensitive information on their own, this doesn't mean it's legal to take advantage of or exploit that information. If you do so you'll be marked as a cybercriminal. It's pretty easy to track your browsing IP, even if you're using a VPN service. It's not as anonymous as you think.

Before reading any further, be aware that Google will start blocking your connection if you connect from a single static IP. It will ask for captcha challenges to prevent automated queries.



About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

IP address: 149.56.46.51
Time: 2018-11-20T14:16:18Z

Popular Google Dork operators

Google's search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.

Let's look at the most popular Google Dorks and what they do.

- `cache` : this dork will show you the cached version of any website, e.g. `cache:securitytrails.com`
- `allintext` : searches for specific text contained on any web page, e.g. `allintext: hacking tools`
- `allintitle` : exactly the same as allintext, but will show pages that contain titles with X characters, e.g. `allintitle:"Security Companies"`
- `allinurl` : it can be used to fetch results whose URL contains all the specified characters, e.g: `allinurl:clientarea`
- `filetype` : used to search for any kind of file extensions, for example, if you want to search for pdf files you can use: `email security filetype: pdf`
- `inurl` : this is exactly the same as `allinurl` , but it is only useful for one single keyword, e.g. `inurl:admin`
- `intitle` : used to search for various keywords inside the title, for example, `intitle:security tools` will search for titles beginning with "security" but "tools" can be somewhere else in the page.
- `inanchor` : this is useful when you need to search for an exact anchor text used on any links, e.g. `inanchor:"cyber security"`

- `intext` : useful to locate pages that contain certain characters or strings inside their text, e.g. `intext:"safe internet"`
- `site` : will show you the full list of all indexed URLs for the specified domain and subdomain, e.g. `site:securitytrails.com`
- `*` : wildcard used to search pages that contain "anything" before your word, e.g. `how to * a website` , will return "how to…" design/create/hack, etc… "a website".
- `|` : this is a logical operator, e.g. `"security" "tips"` will show all the sites which contain "security" or "tips," or both words.
- `+` : used to concatenate words, useful to detect pages that use more than one specific key, e.g. `security + trails`
- `–` : minus operator is used to avoiding showing results that contain certain words, e.g. `security -trails` will show pages that use "security" in their text, but not those that have the word "trails."

If you're looking for the complete set of Google operators, you can follow this SEJ post which covers almost every known dork available today.

Google Dork examples

Let's take a look at some practical examples of the best Google hacks. You'll be surprised how easy is to extract private information from any source just by using Google hacking techniques.

Log files

Log files are the perfect example of how sensitive information can be found within any website. Error logs, access logs and other types of application logs are often discovered inside the public HTTP space of websites. This can help attackers find the PHP version you're running, as well as the critical system path of your CMS or frameworks.

For this kind of dork we can combine two Google operators, allintext and filetype, for example:

```
allintext:username filetype:log
```

This will show a lot of results that include username inside all *.log files.

In the results we discovered one particular website showing an SQL error log from a database server that included critical information:

```
MyBB SQL Error
SQL Error: 1062 - Duplicate entry 'XXX' for key 'username'
Query:
INSERT
INTO XXX (`username`,`password`,`salt`,`loginkey`,`email`,`postnum`,`avatar`,`avatartype`
VALUES ('XXX','XXX','XXX','XXX','XXX','0','','','5','','0','','1389074395','1389074395','
```

This Google hack example exposed the current database name, user login, password and email values to the Internet. We've replaced the original values with "XXX".

Vulnerable web servers

The following Google Dork can be used to detect vulnerable or hacked servers that allow appending "/proc/self/cwd/" directly to the URL of your website.

```
inurl:/proc/self/cwd
```

As you can see in the following screenshot, vulnerable server results will appear, along with their exposed directories that can be surfed from your own browser.

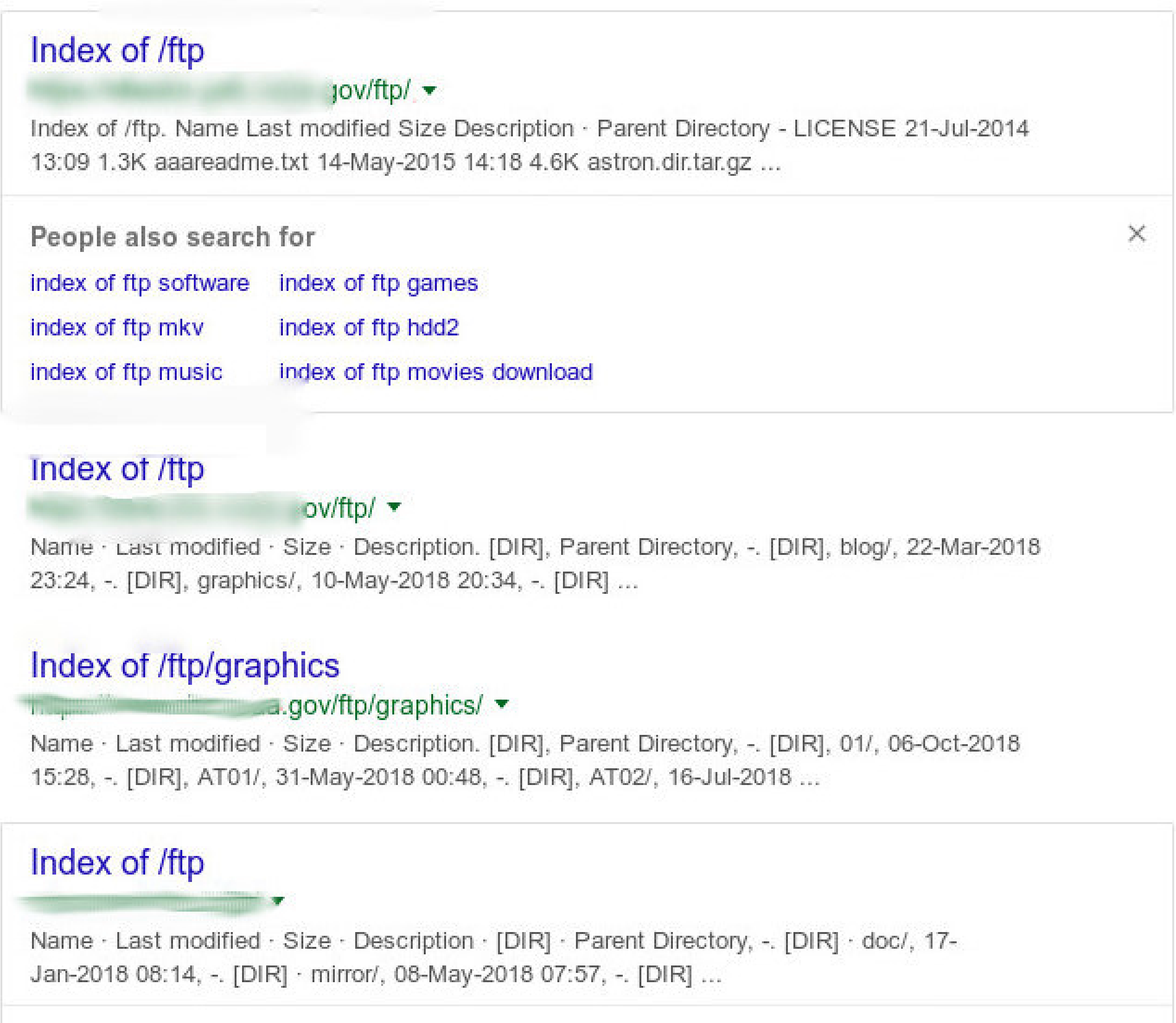
Open FTP servers

Google does not only index HTTP-based servers, it also indexes open FTP servers.

With the following dork, you'll be able to explore public FTP servers, which can often reveal interesting things.

```
intitle:"index of" inurl:ftp
```

In this example, we found an important government server with their FTP space open. Chances are that this was on purpose — but it could also be a security issue.



Index of /ftp

[redacted]jov/ftp/ ▾

Index of /ftp. Name Last modified Size Description · Parent Directory - LICENSE 21-Jul-2014 13:09 1.3K aaareadme.txt 14-May-2015 14:18 4.6K astron.dir.tar.gz ...

People also search for

index of ftp software	index of ftp games
index of ftp mkv	index of ftp hdd2
index of ftp music	index of ftp movies download

Index of /ftp

[redacted]ov/ftp/ ▾

Name · Last modified · Size · Description. [DIR], Parent Directory, -. [DIR], blog/, 22-Mar-2018 23:24, -. [DIR], graphics/, 10-May-2018 20:34, -. [DIR] ...

Index of /ftp/graphics

[redacted]a.gov/ftp/graphics/ ▾

Name · Last modified · Size · Description. [DIR], Parent Directory, -. [DIR], 01/, 06-Oct-2018 15:28, -. [DIR], AT01/, 31-May-2018 00:48, -. [DIR], AT02/, 16-Jul-2018 ...

Index of /ftp

[redacted] ▾

Name · Last modified · Size · Description · [DIR] · Parent Directory, -. [DIR] · doc/, 17-Jan-2018 08:14, -. [DIR] · mirror/, 08-May-2018 07:57, -. [DIR] ...

ENV files

.env files are the ones used by popular web development frameworks to declare general variables and configurations for local and online dev environments.

One of the recommended practices is to move these .env files to somewhere that isn't publicly accessible. However, as you will see, there are a lot of devs who don't care about this and insert their .env file in the main public website directory.

As this is a critical dork we will not show you how do it; instead, we will only show you the critical results:

.

You'll notice that unencrypted usernames, passwords and IPs are directly exposed in the search results. You don't even need to click the links to get the database login details.

SSH private keys

SSH private keys are used to decrypt information that is exchanged in the SSH protocol. As a general security rule, private keys must always remain on the system being used to access the remote SSH server, and shouldn't be shared with anyone.

With the following dork, you'll be able to find SSH private keys that were indexed by uncle Google.

intitle:index.of id_rsa -id_rsa.pub

Let's move on to another interesting SSH Dork.

If this isn't your lucky day, and you're using a Windows operating system with PUTTY SSH client, remember that this program always logs the usernames of your SSH connections.

In this case, we can use a simple dork to fetch SSH usernames from PUTTY logs:

```
filetype:log username putty
```

Here's the expected output:

Email lists

It's pretty easy to find email lists using Google Dorks. In the following example, we are going to fetch excel files which may contain a lot of email addresses.

```
filetype:xls inurl:"email.xls"
```

We filtered to check out only the .edu domain names and found a popular university with around 1800 emails from students and teachers.

```
site:.edu filetype:xls inurl:"email.xls"
```

Remember that the real power of Google Dorks comes from the unlimited combinations you can use. Spammers know this trick too, and use it on a daily basis to build and grow their spamming email lists.

Live cameras

Have you ever wondered if your private live camera could be watched not only by you but also by anyone on the Internet?

The following Google hacking techniques can help you fetch live camera web pages that are not restricted by IP.

Here's the dork to fetch various IP based cameras:

```
inurl:top.htm inurl:currenttime
```

To find WebcamXP-based transmissions:

```
intitle:"webcamXP 5"
```

And another one for general live cameras:

```
inurl:"lvappl.htm"
```

There are a lot of live camera dorks that can let you watch any part of the world, live. You can find education, government, and even military cameras without IP restrictions.

If you get creative you can even do some white hat penetration testing on these cameras; you'll be surprised at how you're able to take control of the full admin panel remotely, and even re-configure the cameras as you like.

MP3, Movie, and PDF files

Nowadays almost no one downloads music after Spotify and Apple Music appeared on the market. However, if you're one of those classic individuals who still download legal music, you can use this dork to find mp3 files:

```
intitle: index of mp3
```

The same applies to legal free media files or PDF documents you may need:

```
intitle: index of pdf   intext: .mp4
```

Weather

Google hacking techniques can be used to fetch any kind of information, and that includes many different types of electronic devices connected to the Internet.

In this case, we ran a dork that lets you fetch Weather Wing device transmissions. If you're involved in meteorology stuff or merely curious, check this out:

```
intitle:"Weather Wing WS-2"
```

The output will show you several devices connected around the world, which share weather details such as wind direction, temperature, humidity and more.

Zoom videos

"Zoom-bombing" became a popular means of disrupting online meetings in 2020 during the initial lockdown. The company has since placed some restrictions to make it harder to find/disrupt Zoom meetings, but long as a URL is shared, a Zoom meeting can still be found:

```
inurl:zoom.us/j and intext:scheduled for
```

The only drawback to this is the speed at which Google indexes a website. By the time a site is indexed, the Zoom meeting might already be over.

SQL dumps

Misconfigured databases are one way of finding exposed data. Another way is to look for SQL dumps that are stored on servers and accessible via a domain/IP.

Sometimes, these dumps appear on sites through incorrect backup mechanisms used by site admins who store backups on web servers (assuming that they aren't indexed by Google). To find a zipped SQL file, we use:

```
"index of" "database.sql.zip"
```

We've omitted screenshots to avoid exposing any possible data breaches.

WordPress Admin

The view on whether to obfuscate your WordPress login page has arguments on both sides. Some researchers say it's unnecessary and using tools like a web application firewall (WAF) can prevent attacks much better than obfuscation would.

Finding WP Admin login pages is not too difficult with a dork:

```
intitle:"Index of" wp-admin
```

Apache2

This can be considered a subset of "vulnerable web servers" mentioned above, but we're discussing Apache2 specifically because:

- LAMP (Linux, Apache, MySQL, PHP) is a popular stack for hosted apps/websites
- These Apache servers could be misconfigured/forgotten or in some stage of being setup, making them great targets for botnets

Find Apache2 web pages with the following dork:

```
intitle:"Apache2 Ubuntu Default Page: It works"
```

phpMyAdmin

Another risky yet frequently discovered tool on LAMP servers is phpMyAdmin software. This tool is another method of compromising data, as phpMyAdmin is used for the administration of MySQL over the web. The dork to use is:

```
"Index of" inurl:phpmyadmin
```

JIRA/Kibana

Google dorks can also be used to find web applications hosting important enterprise data (via JIRA or Kibana).

```
inurl:Dashboard.jspa intext:"Atlassian Jira Project Management Software"
inurl:app/kibana intext:Loading Kibana
```

An easier way to find JIRA instances is to use a tool like SurfaceBrowser™, which can identify subdomains as well as the applications on those subdomains (besides JIRA, there are many other applications).

cPanel password reset

Another dork that can be used as the first step in reconnaissance is to hosted cPanels and then exploit various weaknesses in password resets to take over the cPanel (along with all the websites hosted on it). The dork for this purpose is:

```
inurl:_cpanel/forgotpwd
```

Government documents

Sensitive government documents are the last thing that should be exposed on the internet, but with dorks they aren't too hard to find, as shown below:

```
allintitle: restricted filetype:doc site:gov
```

Preventing Google Dorks

There are a lot of ways to avoid falling into the hands of a Google Dork.

These measures are suggested to prevent your sensitive information from being indexed by search engines.

- Protect private areas with a user and password authentication and also by using IP-based restrictions.
- Encrypt your sensitive information (user, passwords, credit cards, emails, addresses, IP addresses, phone numbers, etc).
- Run regular vulnerability scans against your site, these usually already use popular Google Dorks queries and can be pretty effective in detecting the most common ones.
- Run regular dork queries against your own website to see if you can find any important information before the bad guys do. You can find a great list of popular dorks at the Exploit DB Dorks database.
- If you find sensitive content exposed, request its removal by using Google Search Console.
- Block sensitive content by using a robots.txt file located in your root-level website directory.

Using robots.txt configurations to prevent Google Dorking

One of the best ways to prevent Google dorks is by using a robots.txt file. Let's see some practical examples.

The following configuration will deny all crawling from any directory within your website, which is pretty useful for private access websites that don't rely on publicly-indexable Internet content.

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

You can also block specific directories to be excepted from web crawling. If you have an /admin area and you need to protect it, just place this code inside:

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

This will also protect all the subdirectories inside.

Restrict access to specific files:

```
User-agent: *
Disallow: /privatearea/file.htm
```

Restrict access to dynamic URLs that contain '?' symbol

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

To restrict access to specific file extensions you can use:

```
User-agent: *
Disallow: /*.php$/
```

In this case, all access to .php files will be denied.

Final thoughts

Google is one of the most important search engines in the world. As we all know, it has the ability to index everything unless we explicitly deny it.

Today we learned that Google can be also used as a hacking tool, but you can stay one step ahead of the bad guys and use it regularly to find vulnerabilities in your own websites. You can even integrate this and run automated scans by using custom third-party Google SERPs APIs.

If you're a security researcher it can be a practical tool for your cybersecurity duties when used responsibly.

While Google Dorking can be used to reveal sensitive information about your website that is located and indexable via HTTP protocol, you can also perform a full DNS audit by using the SecurityTrails toolkit.

If you're looking for a way to do it all from a single interface—analyze your DNS records, zones, server IP map, related domains, subdomains as well as SSL Certificates—take a look into your SurfaceBrowser tool, request a demo with us today, or sign up for a free API account.

ESTEBAN BORGES

Esteban is a seasoned cybersecurity specialist, and marketing manager with nearly 20 years of experience. Since joining SecurityTrails in 2017 he's been our go-to for technical server security and source intelligence info.

Related Posts:

Top GitHub Dorks and Tools Used to Scan GitHub Repositories for Sensitive Data

Find the top GitHub Dorks, tools and tips to scan GitHub repositories for credentials, access keys, tokens, password, and more.

Information Gathering: Concept, Techniques and Tools explained

Discover what is information gathering in cybersecurity, the most important techniques, tools and tips to perform a successful intel-recon task.

PRODUCTS

Attack Surface Intelligence™

SecurityTrails API™

SurfaceBrowser™

SecurityTrails Feeds™

Pricing

COMPANY

Blog