Google Dorking for Penetration Testers

What is Google Dork?

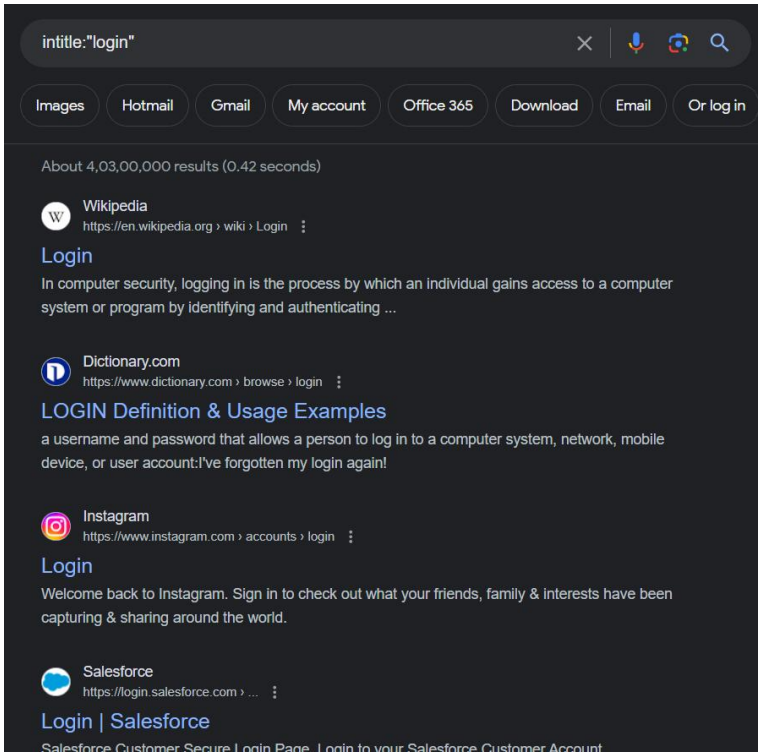
It is basically a search string that uses advanced search query to find information that are not easily available on the websites. It is also regarded as illegal google hacking activity which hackers often uses for purposes such as cyber terrorism and cyber theft.

Special google search operators

Before starting with google dorks, you need to have basic understanding of few special google search operators and also how it functions.

1.intitle:

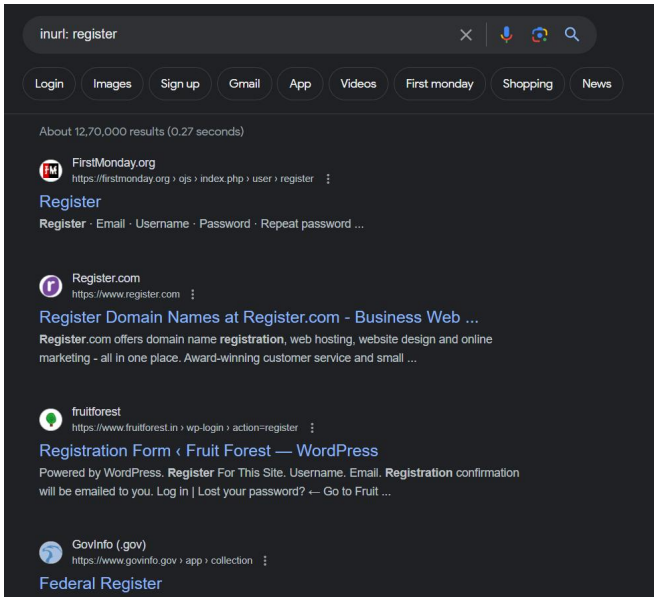
This will ask google to show pages that have the term in their html title



2. inurl:

Searches for specified term in the URL.

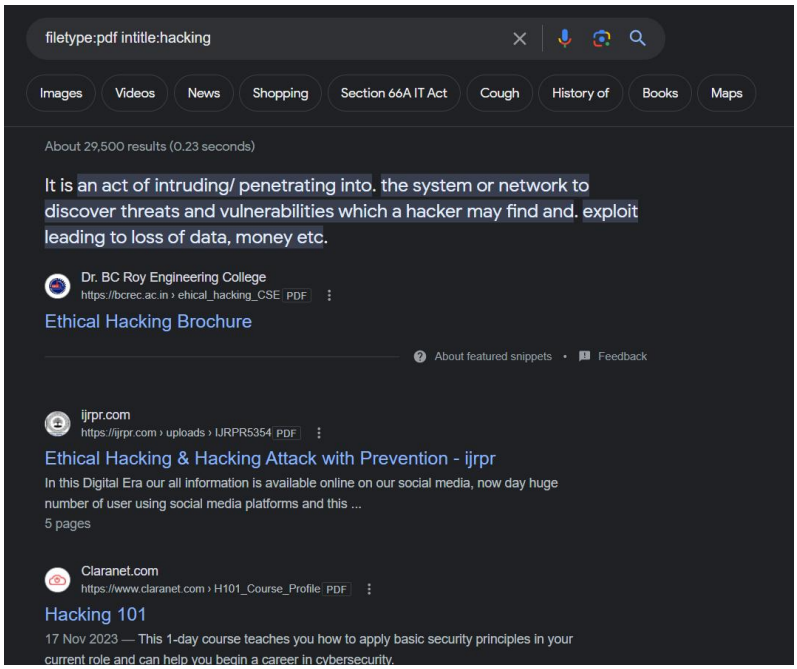
For example: inurl: register



3. filetype:

Searched for certain file type.

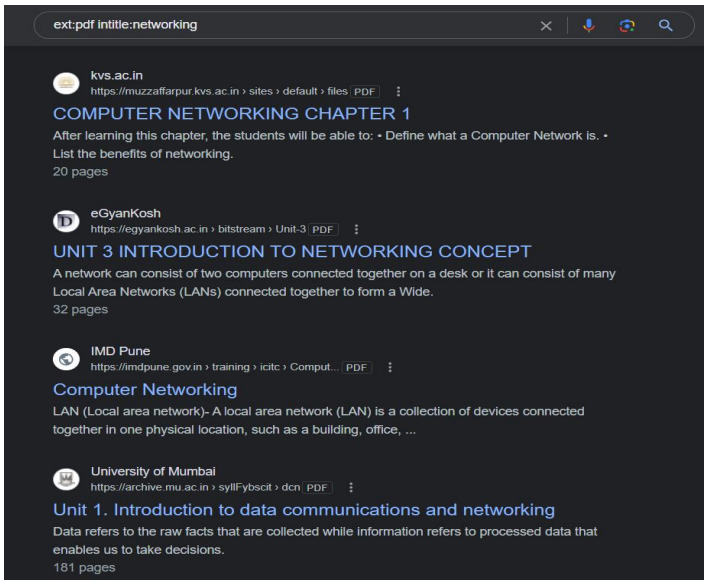
Example: filetype:pdf will search for all the pdf files in the websites.



4. ext:

It works similar to filetype.

Example: ext:pdf finds pdf extension files.



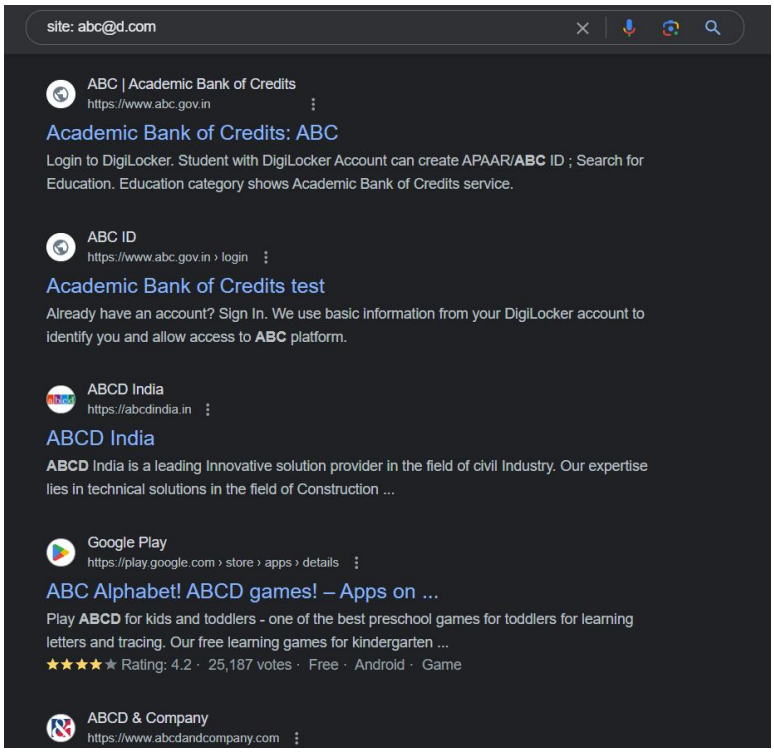
5. intext:

This will search content of the page. This works somewhat like plain google search

6. site:

This limits the search to a specific site only.

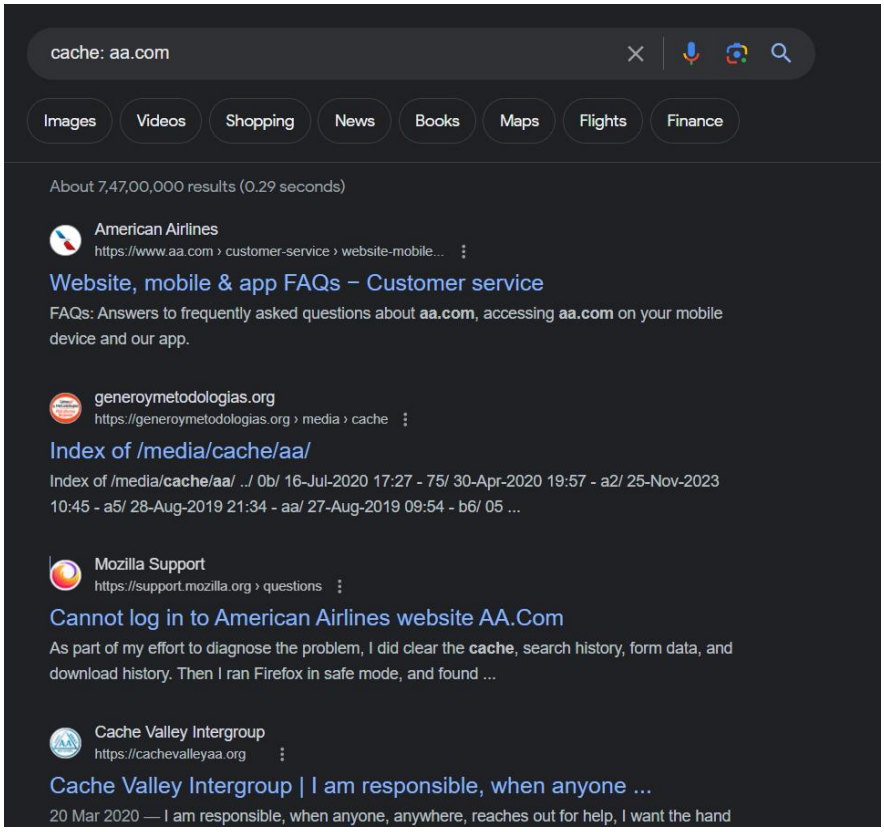
Example: site: abc@d.com will limit search to only abc@d.com.



7. Cache:

This will show you cached version of any website.

Example: *cache: aa.com*



8. *

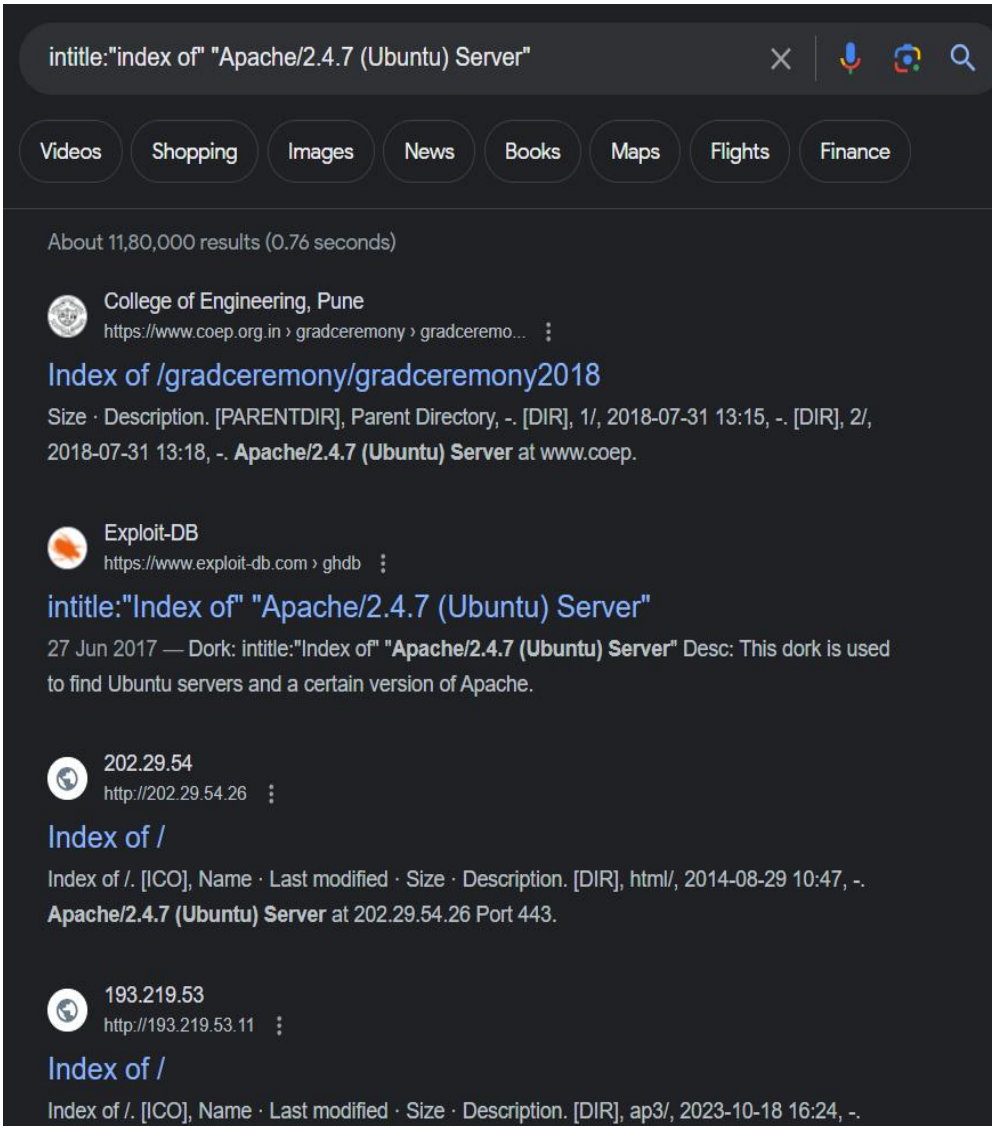
This works like a wildcard.

Example: How to * sites, will show you all the results like *“how to…” design/create/hack, etc… “sites”*

Examples of Google Dorking

1. Finding vulnerable versions of software

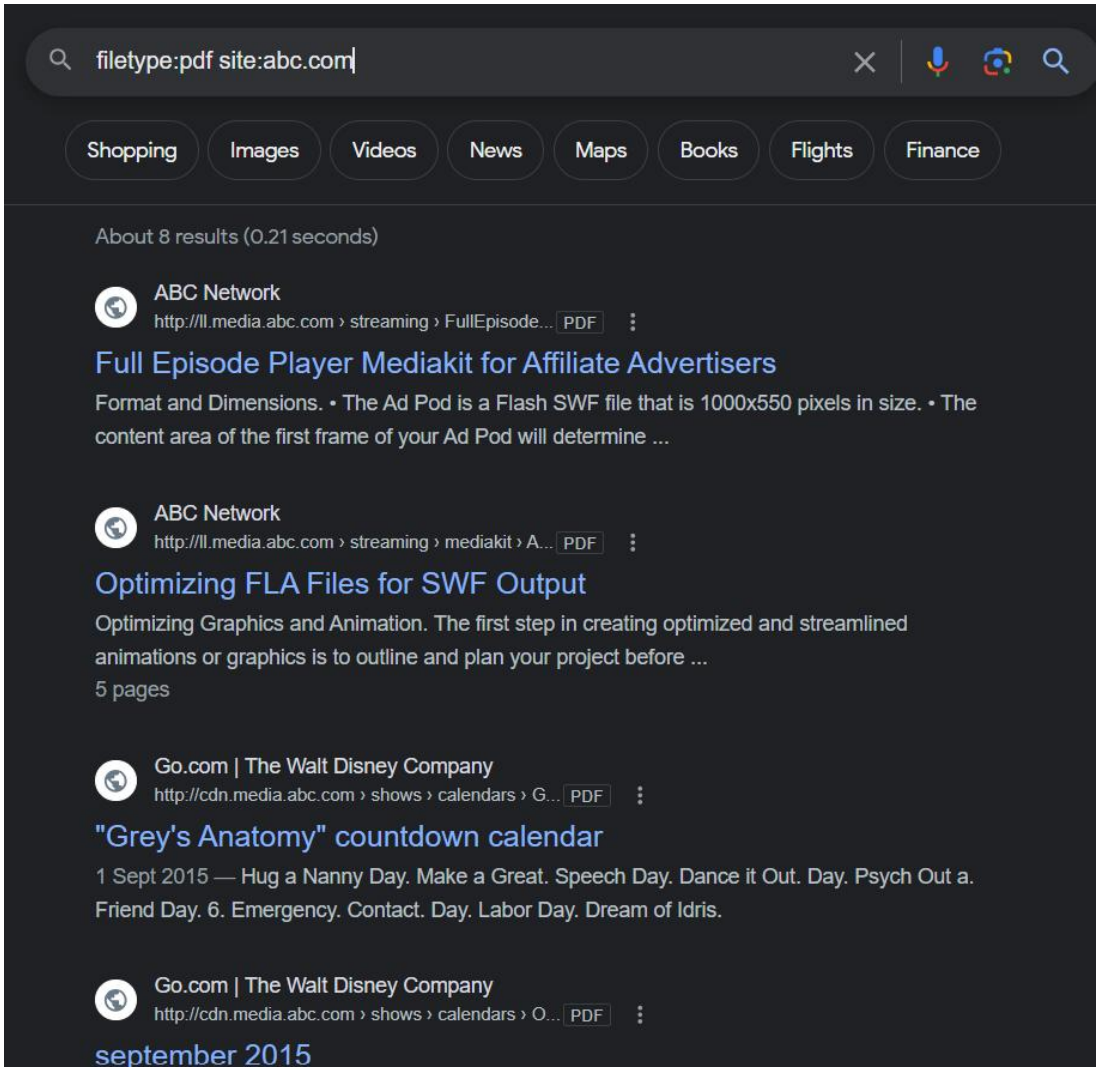
intitle:"index of" "Apache/2.4.7 (Ubuntu) Server"



The Google dork intitle:"index of" "Apache/2.4.7 (Ubuntu) Server" is used to find websites that are running Apache version 2.4.7 on Ubuntu and have an "index of" listing enabled. This can be useful for finding potentially vulnerable websites, as older versions of software may have known vulnerabilities. However, it's important to note that accessing or attempting to access such directories without authorization is illegal and unethical.

2. Finding publicly exposed documents:

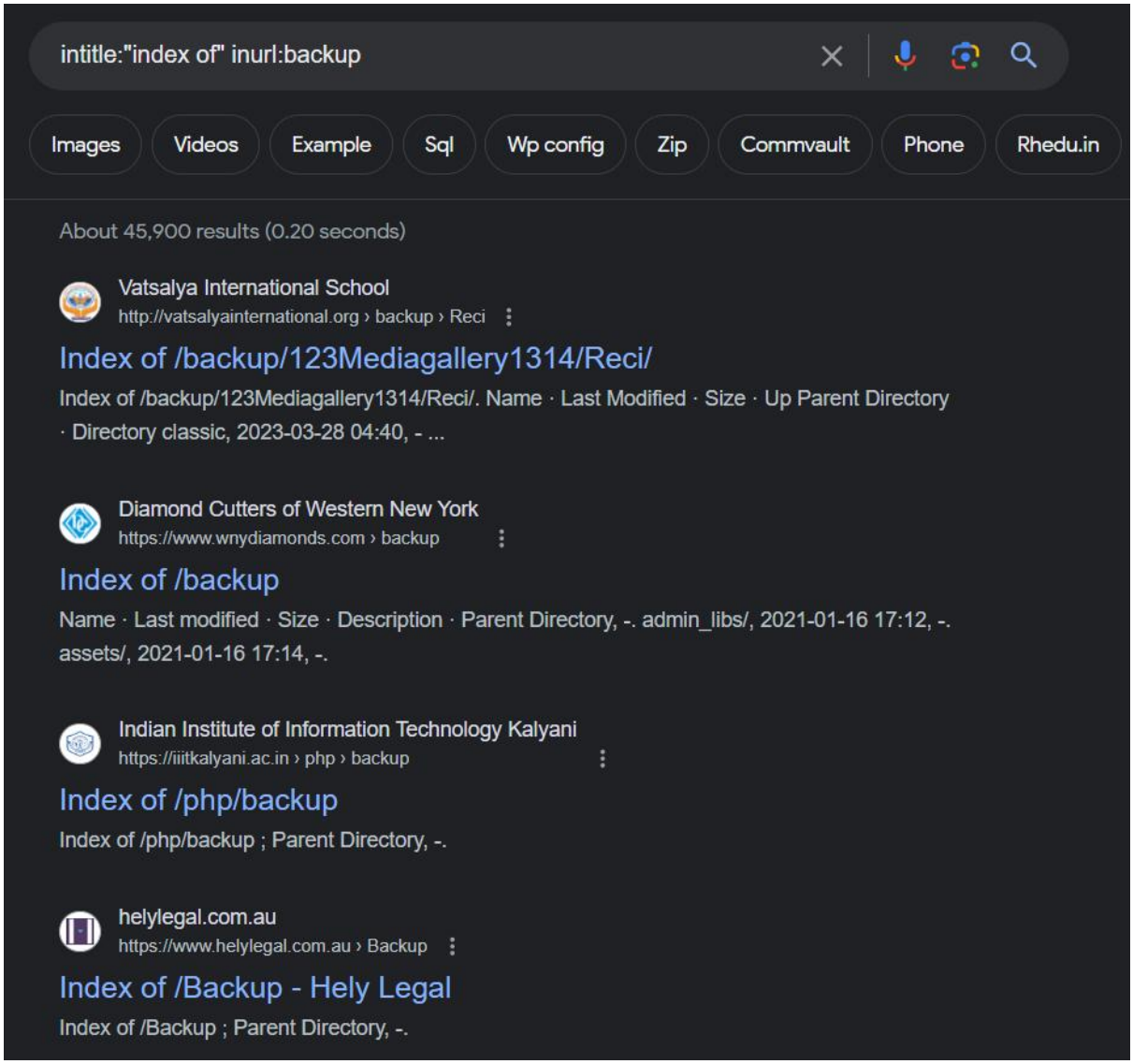
filetype:pdf site: abc.com



The Google dork filetype:pdf site: abc.com is used to find PDF files on a specific website (replace abc.com with the actual domain name). This can be useful for finding publicly accessible PDF documents on a website, which may contain sensitive information that could be useful for a penetration test. However, it's important to use this dork ethically and with permission, as accessing or attempting to access files without authorization is illegal.

3. Finding exposed directories:

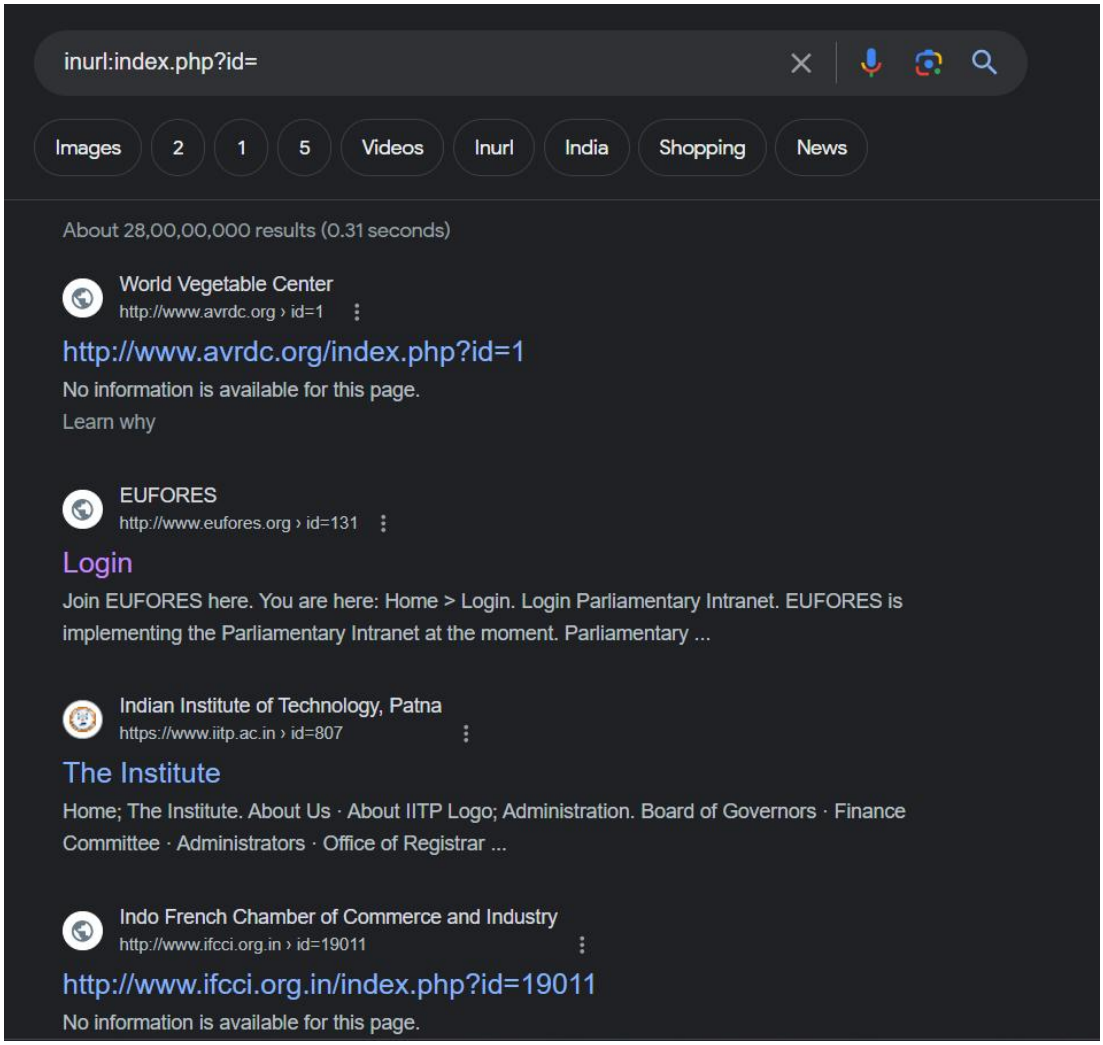
intitle:"index of" inurl:backup



The Google dork intitle:"index of" inurl: backup is used to find websites that have an "index of" listing in directories with "backup" in the URL. This can sometimes reveal backup files or directories that may contain sensitive information. It's important to use this dork ethically and with permission, as accessing or attempting to access such directories without authorization is illegal.

4.Finding SQL injection vulnerabilities:

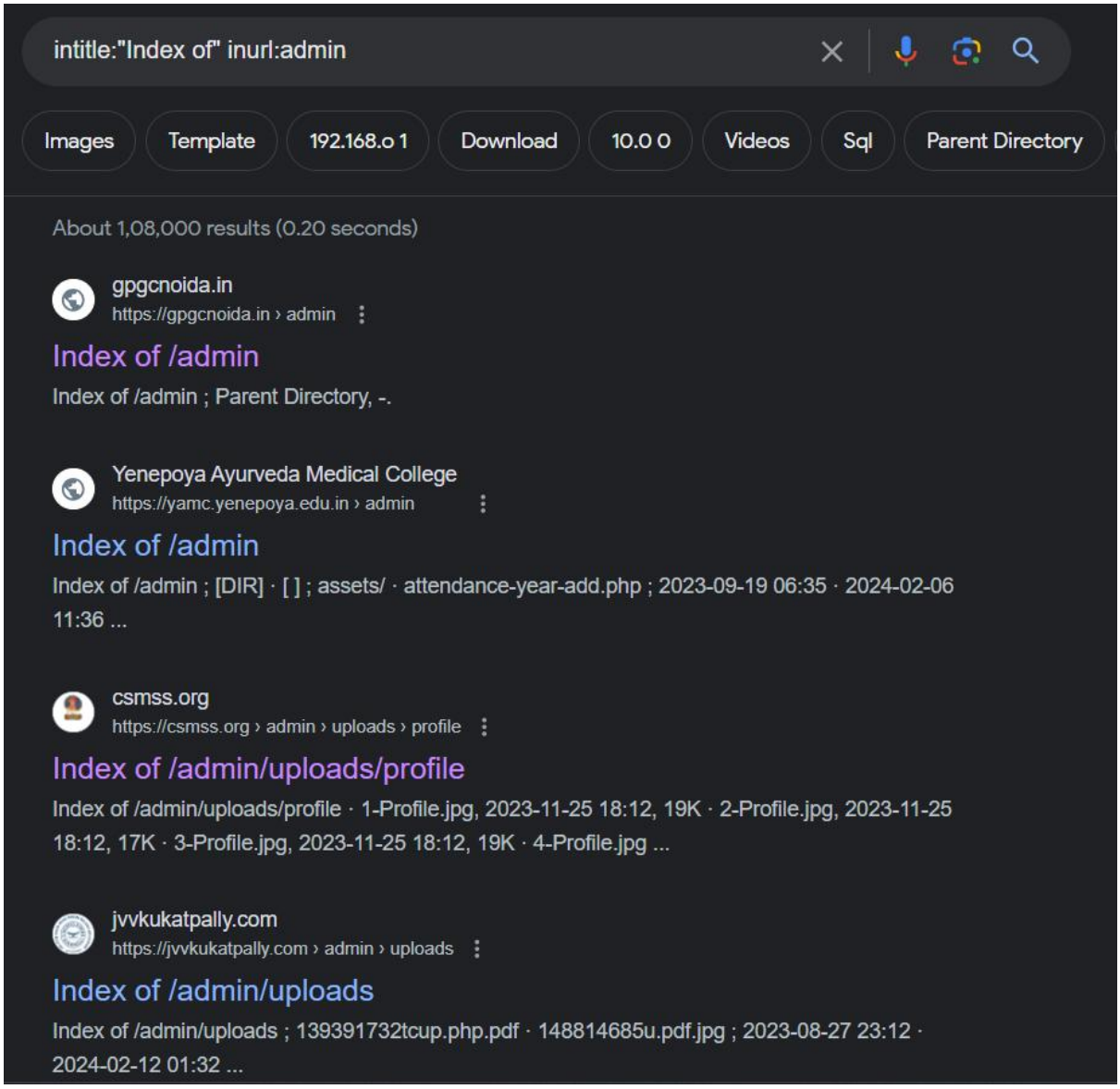
inurl: index.php?id=



The Google dork inurl: index.php?id= is commonly used to search for websites that have URLs containing "index.php?id=". This type of URL structure is often associated with dynamic web pages that use query parameters to retrieve specific content from a database. It can be indicative of websites vulnerable to SQL injection attacks, as attackers may attempt to manipulate the "id" parameter to inject malicious SQL code.

5.Finding sites with exposed directories that may contain sensitive files:

intitle:"Index of" inurl:admin



The Google dork `intitle:"Index of" inurl: admin` is used to find websites that have an "index of" listing in their URL path that includes "admin". This can sometimes reveal directories or files related to administration, which may contain sensitive information or be vulnerable to unauthorized access. However, it's important to use this dork ethically and with permission, as accessing or attempting to access such directories without authorization is illegal.

The Google Hacking Database (GHDB)

Google Hacking Database

Filters | Reset All

Show 15

Quick Search

Date Added	Dork	Category	Author
2024-02-26	"PMB" AND ("changelog.txt" OR inurl:opac_css)	Vulnerable Servers	Wallehazz
2024-02-26	intitle:"Index of /confidential"	Files Containing Juicy Info	Gautam Rawat
2024-02-26	inurl:"/wp-json/oembed/1.0/embed?url="	Files Containing Juicy Info	Jeel Patel
2024-02-16	inurl:* "auditing.txt"	Files Containing Juicy Info	Gautam Rawat
2024-02-16	intext:"index of" web	Files Containing Juicy Info	A.K.M. Mohiuddin
2024-02-16	intitle:"index of" cgi.pl	Files Containing Juicy Info	Gautam Rawat
2024-02-13	inurl:* "encryption.txt"	Files Containing Juicy Info	Naved Ansari
2024-02-06	allintitle:"Bright Cluster Manager" site:.edu	Vulnerable Servers	Thomas Heverin
2024-02-05	intitle:"index of" env.cgi	Files Containing Juicy Info	Wallehazz
2024-02-02	intitle:"Welcome to iTop version" wizard	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-02-02	intitle:"Installation Wizard - PowerCMS v2"	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-02-02	ext:java intext:"executeUpdate"	Files Containing Juicy Info	BULLETMHS
2024-02-02	"Started by upstream project" ext:txt	Files Containing Juicy Info	Nadir Boulacheb (RubX)

The Google Hacking Database (GHDB) is a project that was started to catalog various search queries, known as Google dorks, that can be used to uncover vulnerable or sensitive information on websites. These dorks are used to refine Google searches and find specific types of information that may not be readily accessible through standard searches.

The GHDB includes dorks for finding things like exposed web servers, vulnerable scripts, sensitive directories, and more. It's important to note that while the GHDB can be a useful resource for security professionals and penetration testers, using these dorks for unauthorized access or exploitation is illegal and unethical.

The GHDB is no longer actively maintained as a separate project, but the concept of Google dorks and their use in security testing remains relevant.