USEFUL Google DORKS IN 2025

Google Dorks:

Google Dorking, also known as Google Hacking, is a technique that uses advanced search operators to find information on the internet that might not be easily available.

Google Dorking uses specialized operators like "site:", "inurl:", "intitle:", "intext:", and "filetype:" to find specific information. For example, you can use the "site:" operator to search for a specific site, or the "inurl:" operator to search for a specific keyword in the URL of a website.

Advantages:

Exact Information Retrieval – It is possible to search for certain information more accurately.

Time E cient – It is possible to instantly shorten search results.

Privacy Protection – Help find potentially disclosed personal or sensitive data.

Vulnerability Assessment – Ethical Assessment of any cyber system without conducting a penetration test.

Index:

Google Dorking can be used for:

Security: Security professionals use Google Dorking to identify vulnerabilities in their systems.

Research: Innocent researchers and journalists can use Google Dorking to find information.

Cybercrime **:** Hackers, cyberstalkers, and cybercriminals can use Google Dorking to uncover sensitive data that has been exposed to the public.

Popular Google Dork operators:

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**

allinurl: it can be used to fetch results whose URL contains all the specified characters.

e.g: **allinurl client area**

filetype: used to search for any kind of file extensions.

e.g: if you want to search for jpg files you can use: **filetype: jpg**

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.

e.g: **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"**

link: will show the list of web pages that have links to the specified URL.

e.g. **link: microsoft.com**

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.

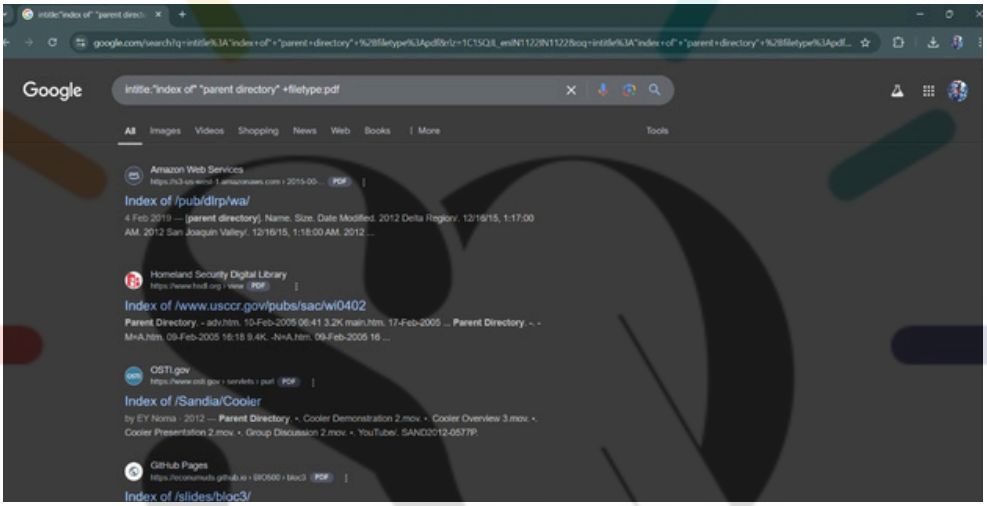
e.g. **security -trails** will show pages that use "security" in their text, but not those

that have the word “trails.”

Basic Dorks:

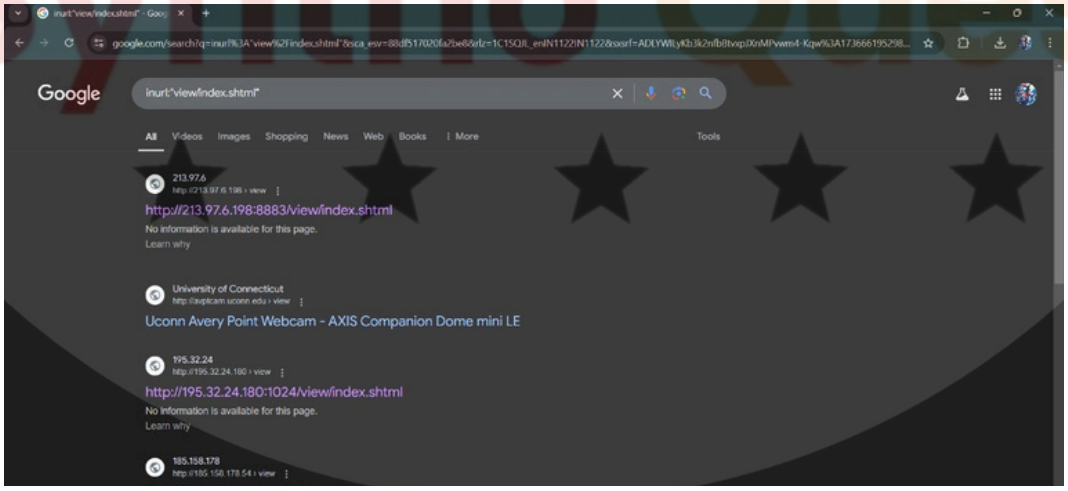
Basic Directory Listing : intitle: Search for published PDF files that are found in unprotected folders. The title of intitle:index of parent directory ascertains web pages that act as raw directory listings.

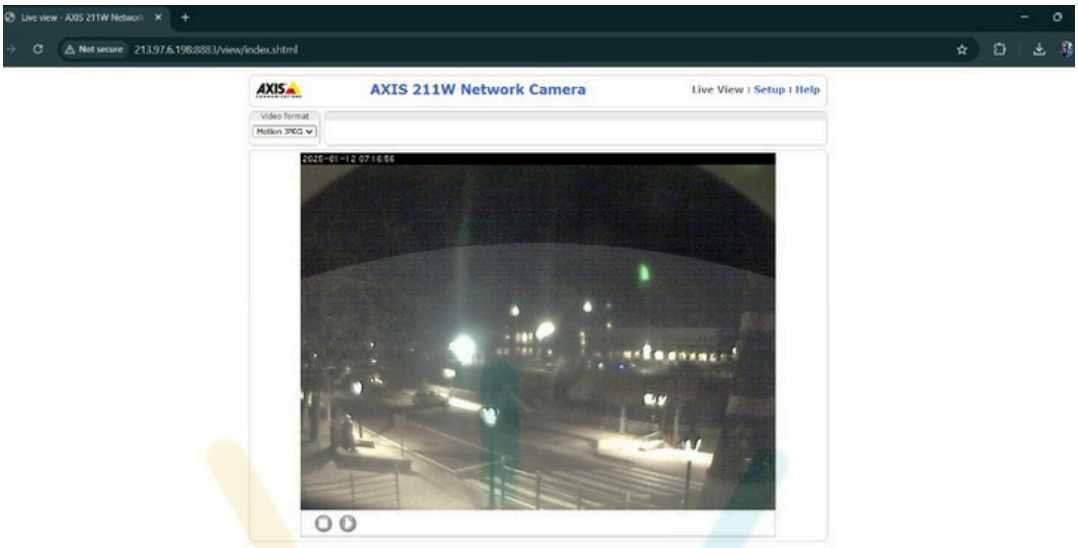
Syntax : intitle:"index of" "parent directory" +filetype:pdf



Discovering Vulnerable Cameras : Find publicly reachable IP cameras that divulge their interfaces without proper safety.

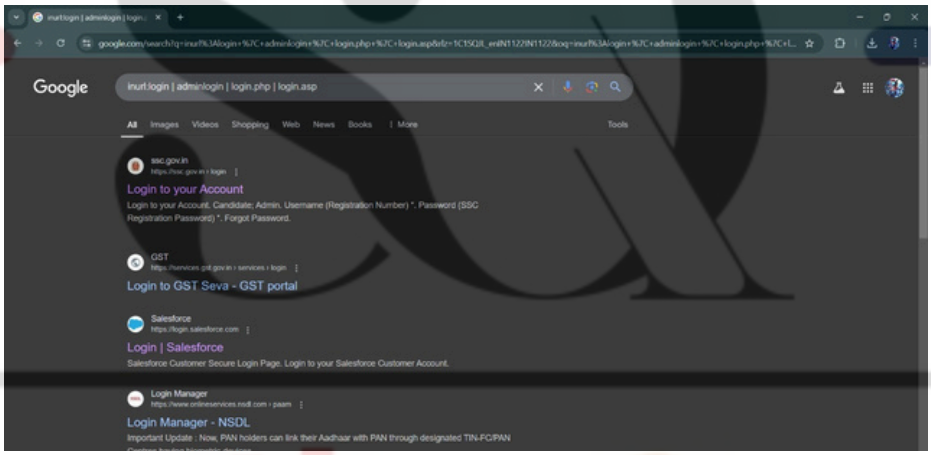
Syntax : inurl:"view/index.Shtml"





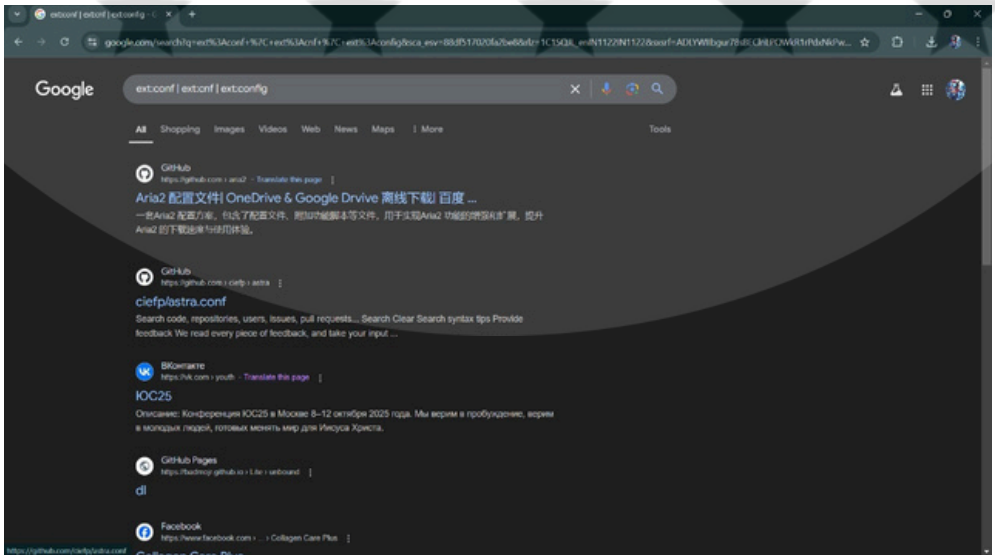
Locating the Login URLs : Search for login screens of di erent websites or applications. This is helpful in finding the login entry points for di erent websites.

Synatx : inurl: login | adminlogin | login.php | login.asp



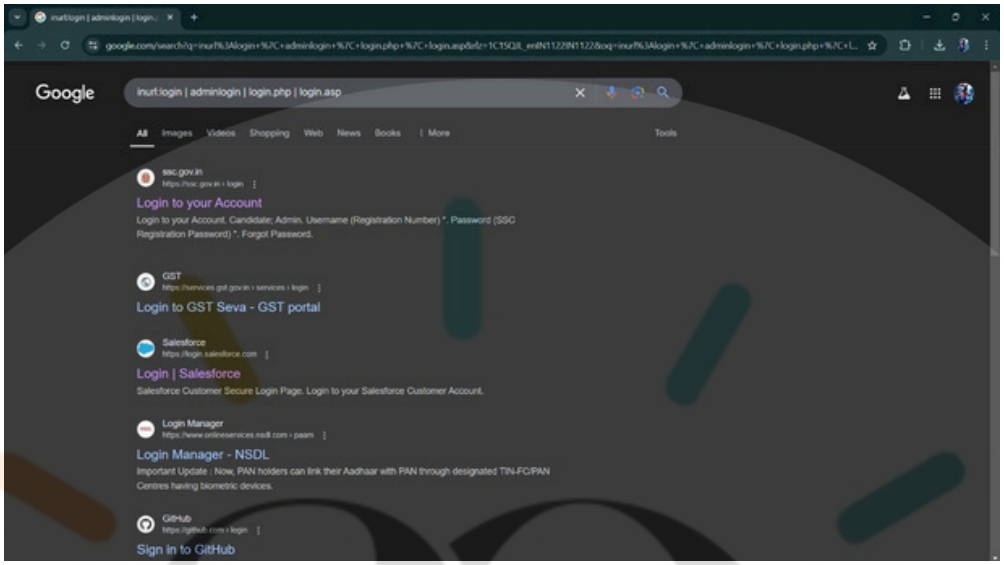
Searching for Configuration Files : Locate configuration files that might contain server settings or other details, useful for auditing server configurations.

Syntax : ext:conf | ext:cnf | ext:config



Database Information Leaks : Identify publicly exposed phpMyAdmin login portals.

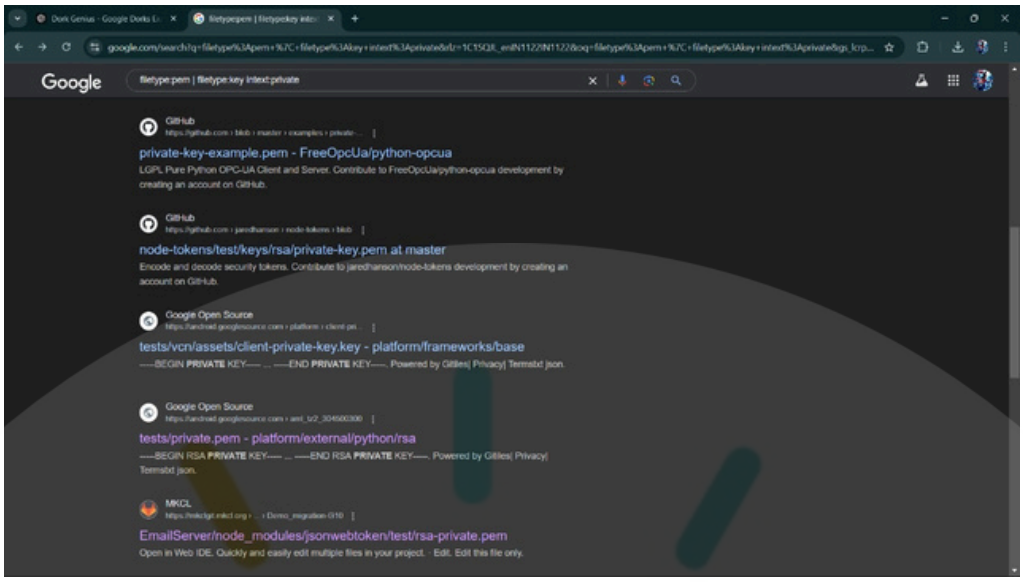
Syntax : inurl:phpmyadmin inurl:login



Sensitive Data Dorks:

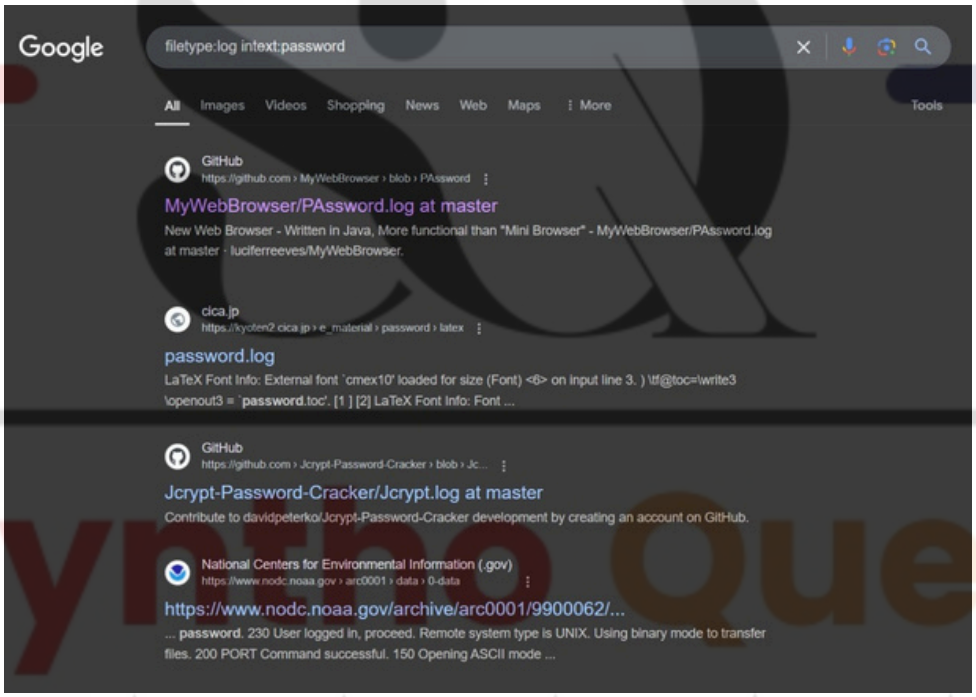
Finding Private Keys : Identifies private key files accidentally exposed online.

Syntax : filetype:pem | filetype:key intext:private



Finding Password Files : Searches for log files that contain passwords.

Syntax : filetype:log intext:password



Discovering Emails : Searches for Excel files containing Gmail addresses.

Syntax : intext:"@gmail.com" filetype:xls