



Google Dorking

¿Qué es Google Dork?

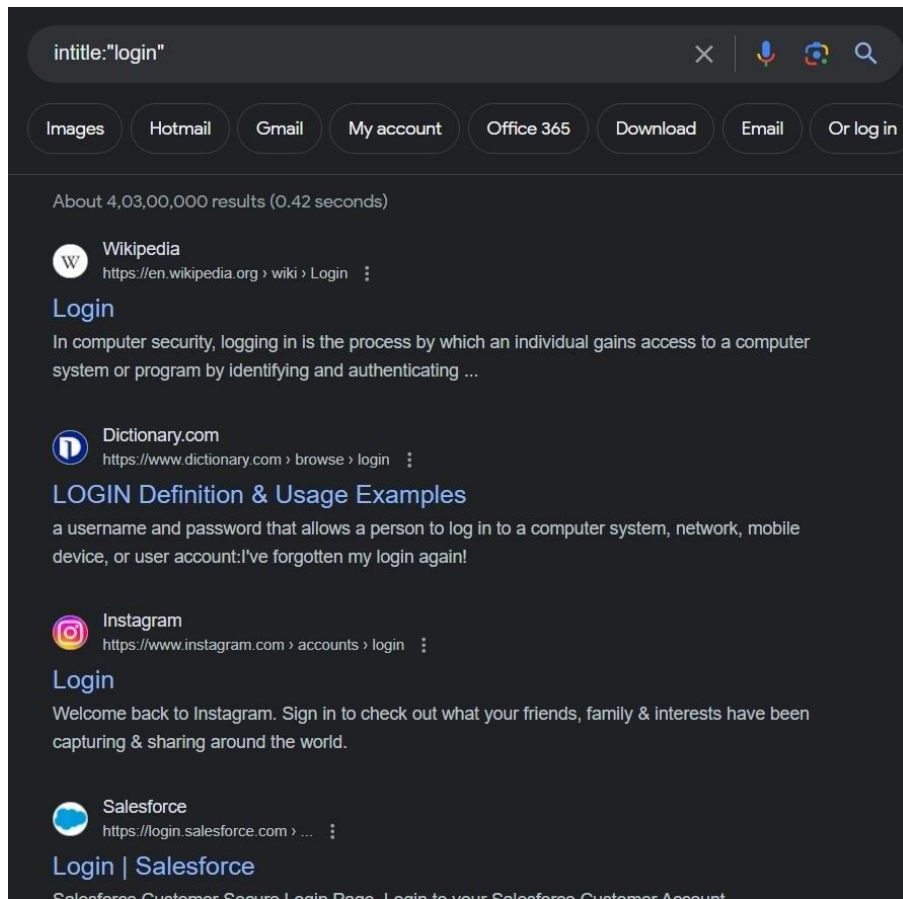
Es básicamente una cadena de búsqueda que utiliza una consulta de búsqueda avanzada para encontrar información que no está fácilmente disponible en los sitios web. También se considera una actividad ilegal de piratería de Google, que los piratas informáticos a menudo utilizan con fines como el terrorismo cibernético y el robo cibernético.

Operadores de búsqueda especiales de Google

Antes de comenzar con Google Dorks, debe tener una comprensión básica de algunos operadores de búsqueda especiales de Google y también cómo funciona.

1.intitle:

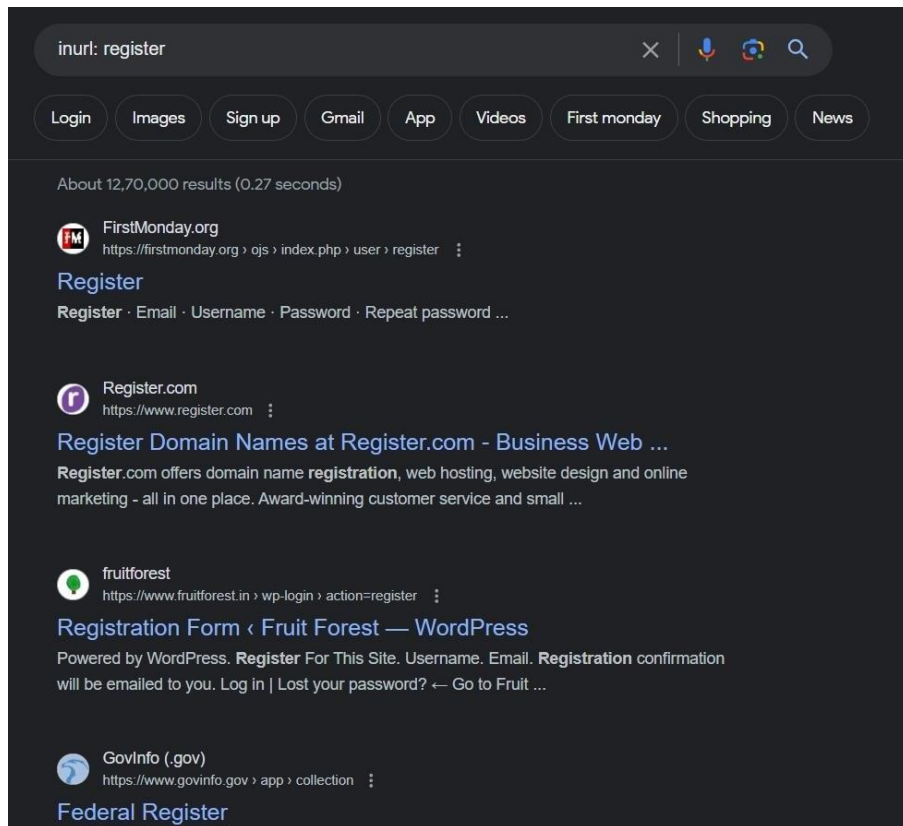
Esto le pedirá a Google que muestre las páginas que tienen el término en su título html



2. inurl:

Busca el término especificado en la dirección URL.

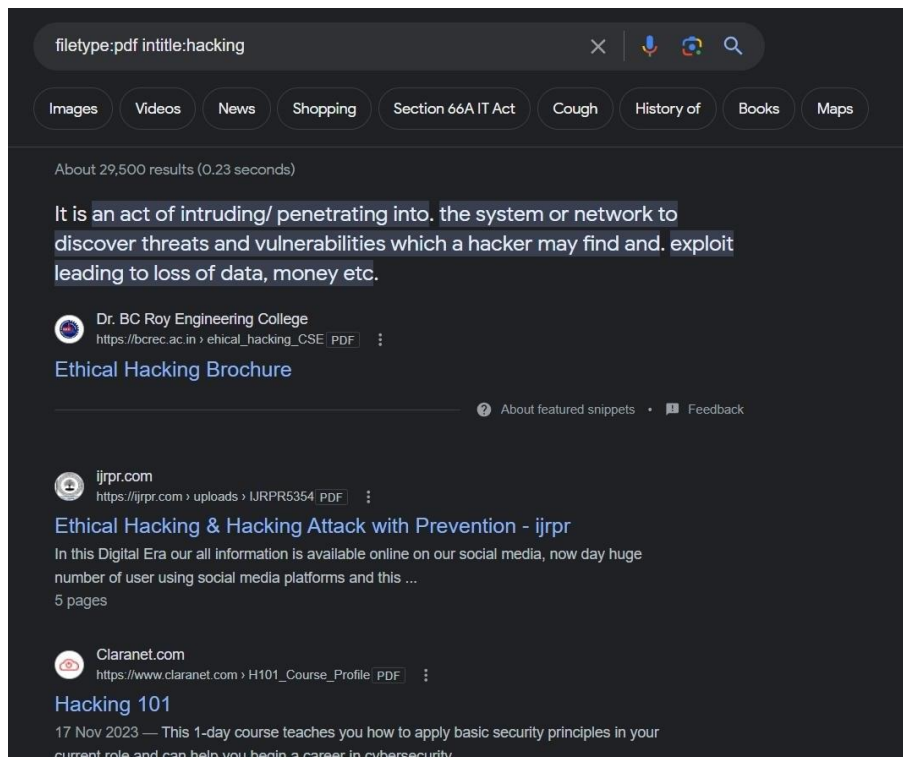
Por ejemplo: inurl: register



3. filetype:

Se ha buscado un determinado tipo de archivo.

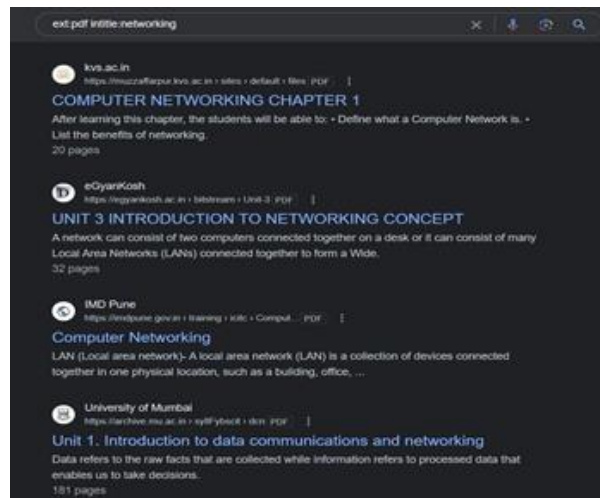
Ejemplo: filetype:pdf will search for all the pdf files in the websites.



4. ext:

Funciona de manera similar al tipo de archivo.

Ejemplo: ext:pdf Busca archivos de extensión PDF.



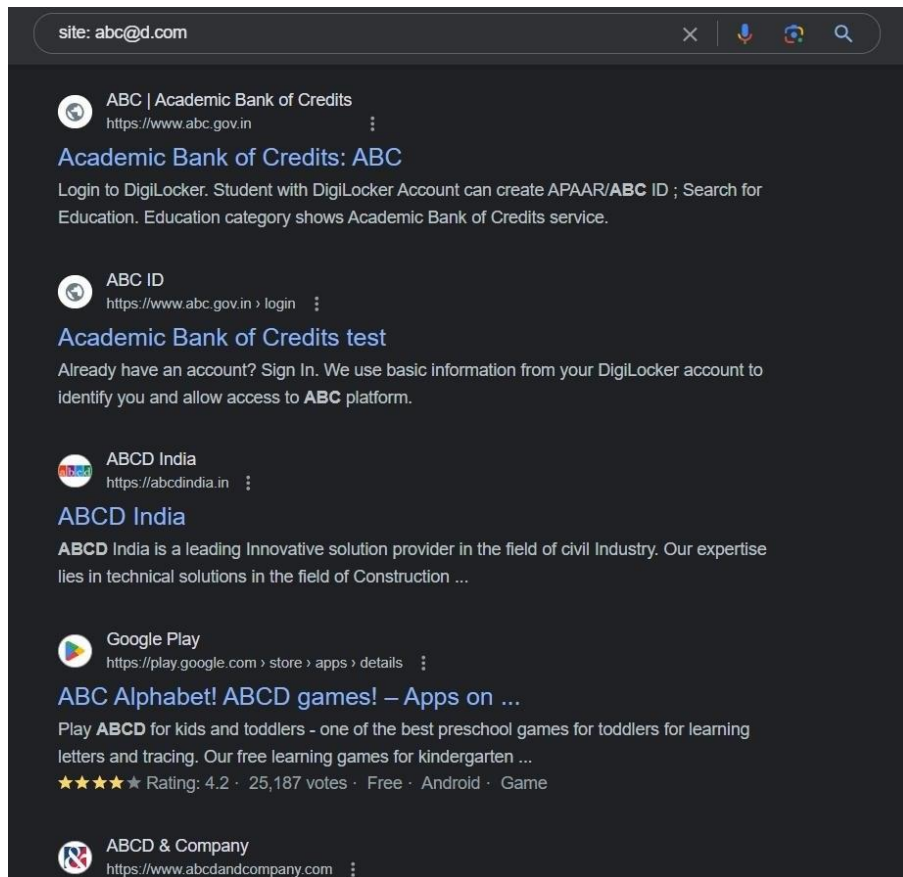
5. intext:

Esto buscará el contenido de la página. Esto funciona de alguna manera como una simple búsqueda en Google

6. site:

Esto limita la búsqueda solo a un sitio específico.

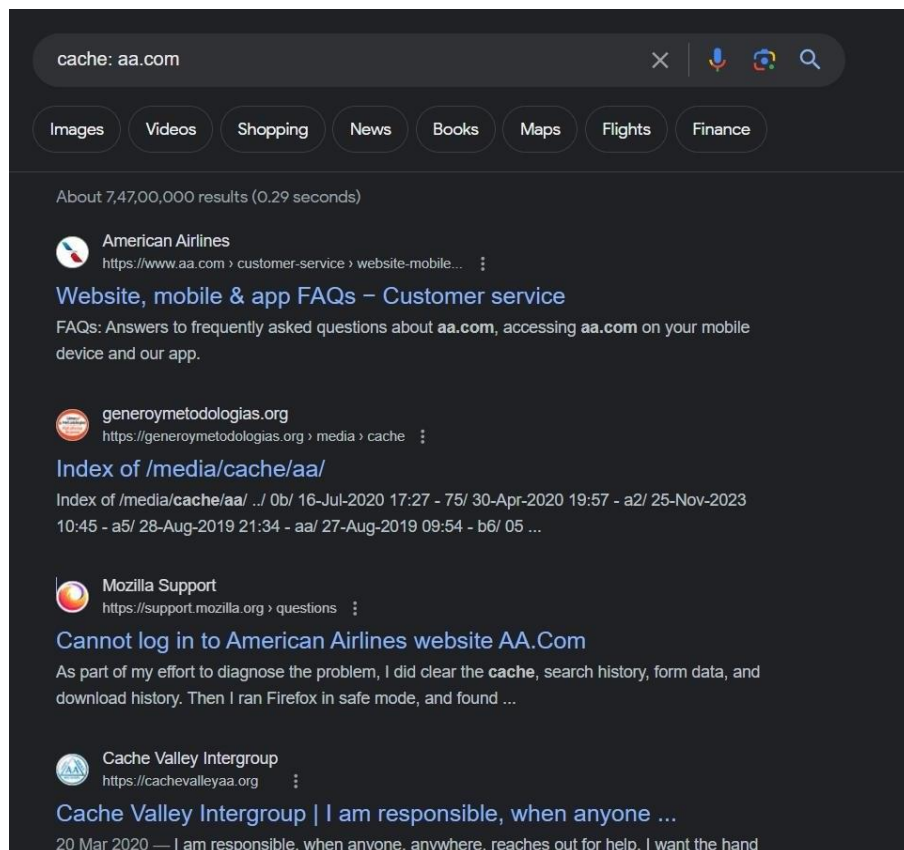
Ejemplo: site: abc@d.com limitará la búsqueda a solo abc@d.com.



7. Cache:

Esto le mostrará la versión en caché de cualquier sitio web.

Ejemplo: cache: aa.com



8. *

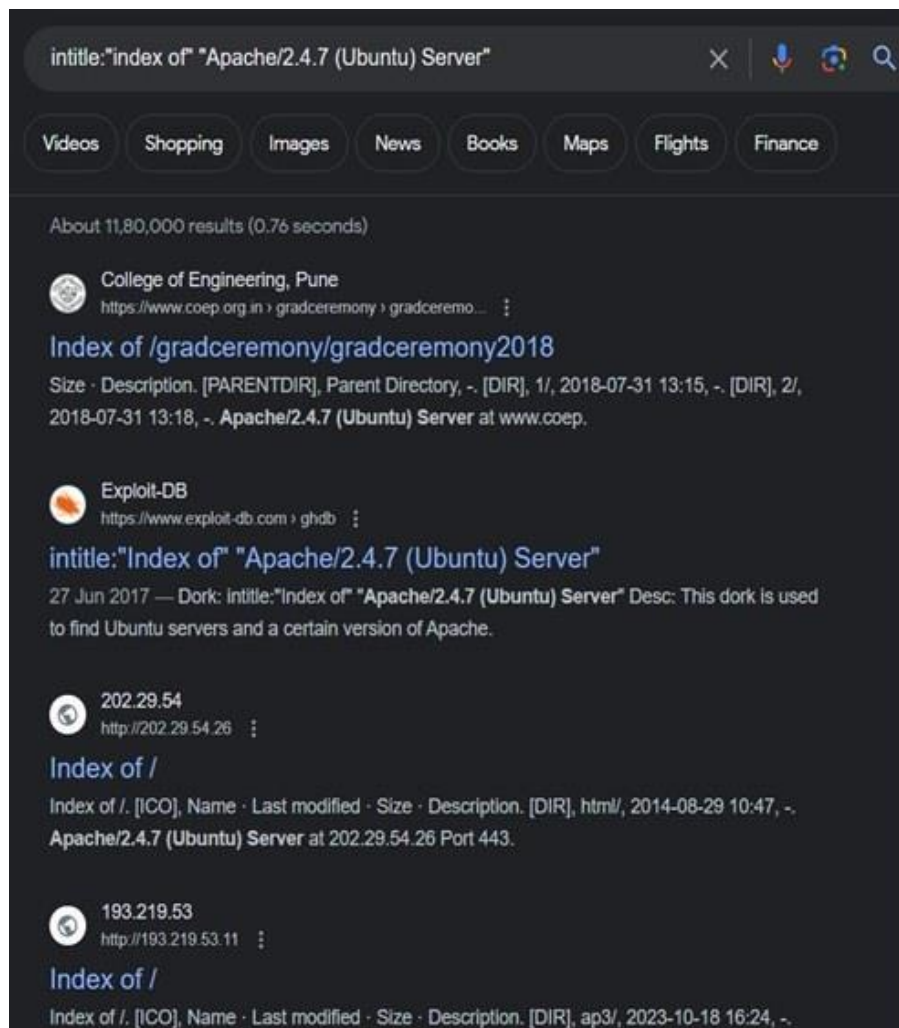
Esto funciona como un comodín.

Ejemplo: Cómo * sites, te mostrará todos los resultados como ***“how to...”***
design/create/hack, etc... “sites”

Ejemplos de Google Dorking

1. Encontrar versiones vulnerables del software

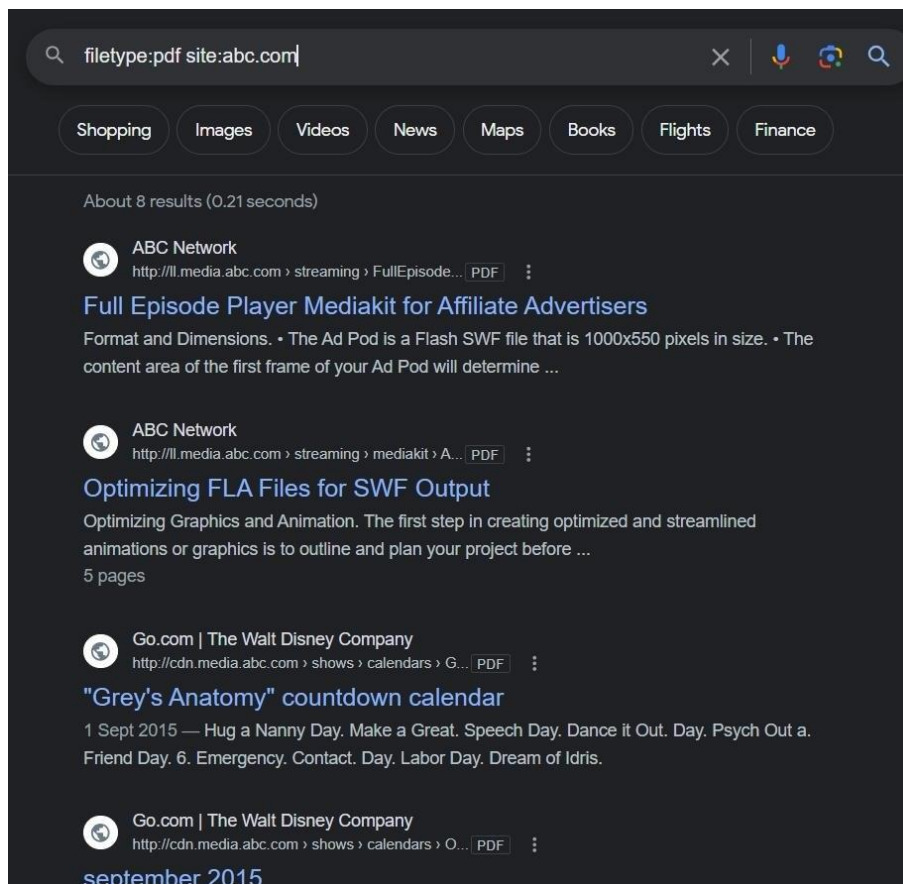
intitle:"index of" "Apache/2.4.7 (Ubuntu) Server"



El dork de Google `intitle:"index of" "Apache/2.4.7 (Ubuntu) Server"` se utiliza para encontrar sitios web que ejecutan Apache versión 2.4.7 en Ubuntu y tienen habilitada la lista de "índice de". Esto puede ser útil para encontrar sitios web potencialmente vulnerables, ya que las versiones anteriores del software pueden tener vulnerabilidades conocidas. Sin embargo, es importante tener en cuenta que acceder o intentar acceder a dichos directorios sin autorización es ilegal y poco ético.

Búsqueda de documentos expuestos públicamente:

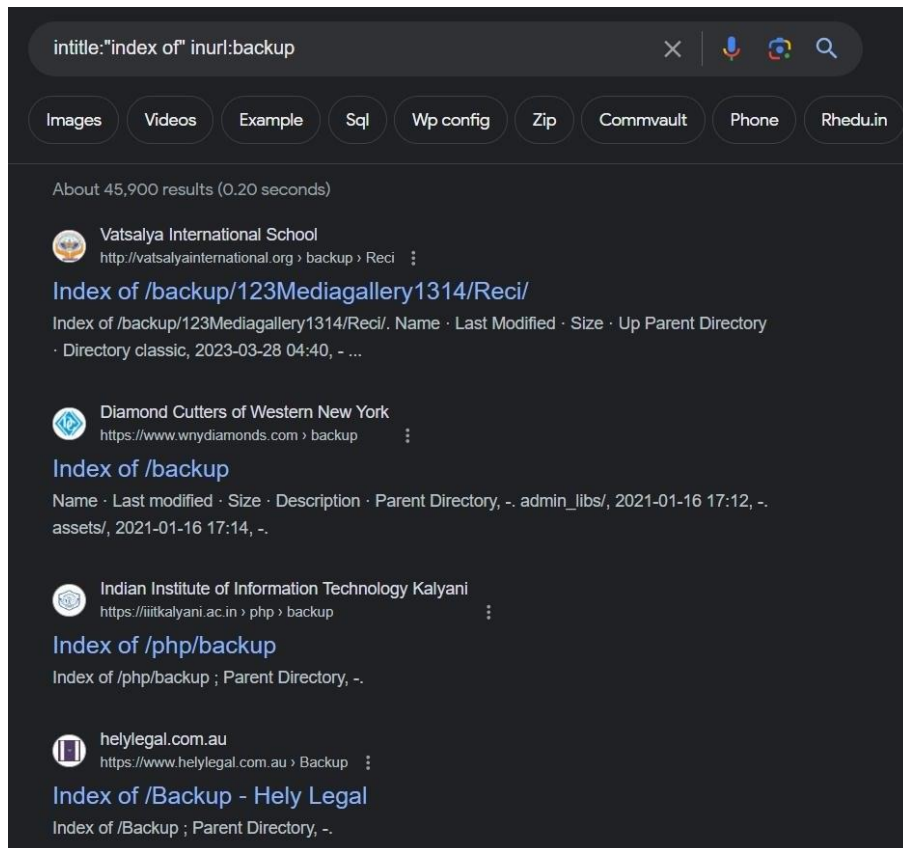
filetype:pdf site: abc.com



El abc.com Google dork filetype:pdf site: se utiliza para encontrar archivos PDF en un sitio web específico (reemplace abc.com con el nombre de dominio real). Esto puede ser útil para encontrar documentos PDF de acceso público en un sitio web, que pueden contener información confidencial que podría ser útil para una prueba de penetración.

Búsqueda de directorios expuestos:

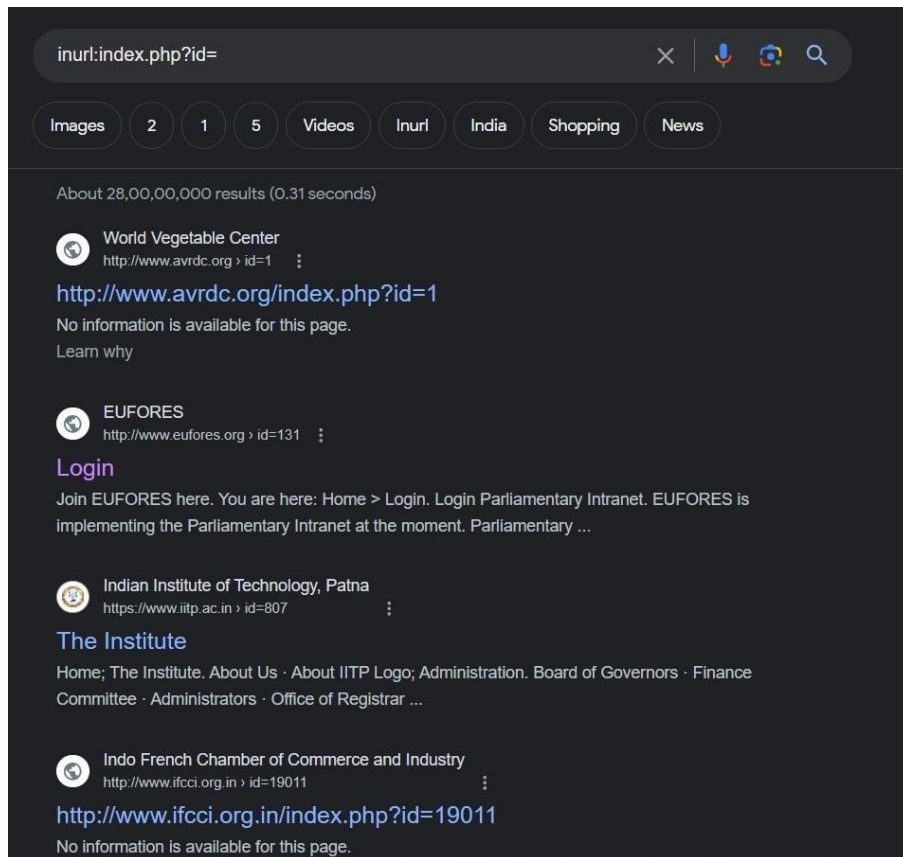
intitle:"index of" inurl:backup



El dork de Google `intitle:"index of" inurl: backup` se utiliza para encontrar sitios web que tienen un listado de "índice de" en directorios con "backup" en la URL. Esto a veces puede revelar archivos de copia de seguridad o directorios que pueden contener información confidencial.

4. Encontrar vulnerabilidades de inyección SQL:

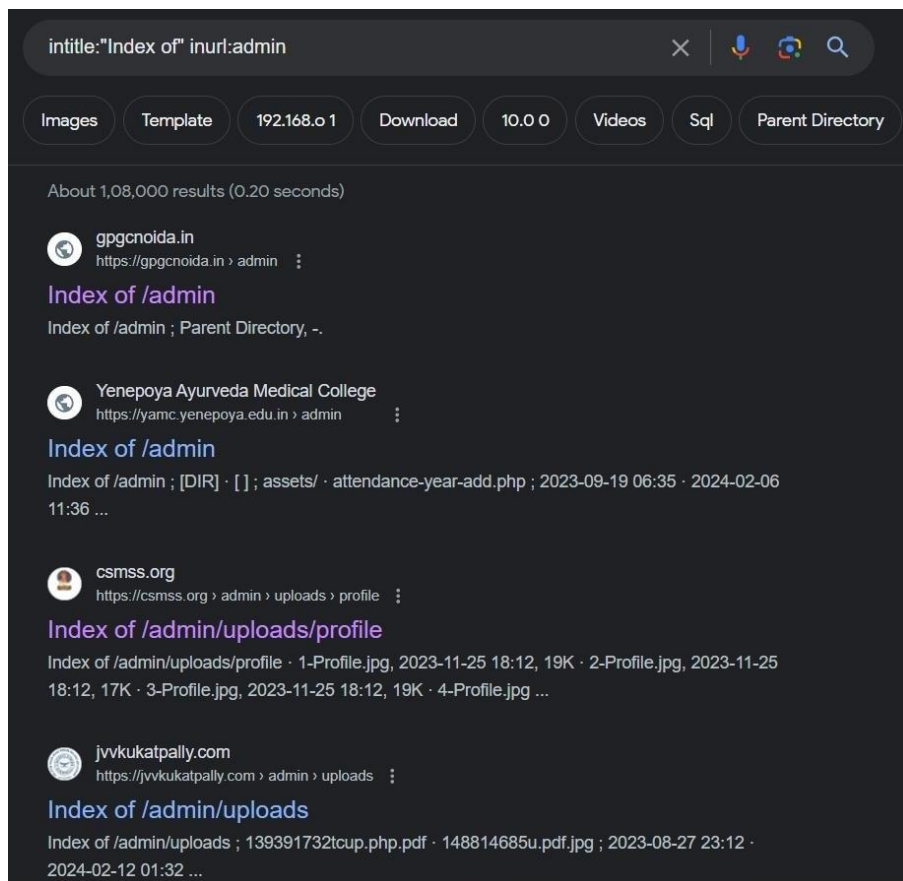
inurl: index.php?id=



El inurl de Google dork: `index.php?id=` se usa comúnmente para buscar sitios web que tienen URL que contienen "`index.php?id=`". Este tipo de estructura de URL a menudo se asocia con páginas web dinámicas que usan parámetros de consulta para recuperar contenido específico de una base de datos. Puede ser indicativo de sitios web vulnerables a ataques de inyección SQL, ya que los atacantes pueden intentar manipular el parámetro "id" para inyectar código SQL malicioso.

5.Encontrar sitios con directorios expuestos que puedan contener archivos confidenciales:

intitle:"Index of" inurl:admin



El dork de Google 'intitle:"Index of" inurl: admin' se utiliza para encontrar sitios web que tienen una lista de "índice de" en su ruta URL que incluye "admin". Esto a veces puede revelar directorios o archivos relacionados con la administración, que pueden contener información confidencial o ser vulnerables al acceso no autorizado.

Google Hacking Database (GHDB)

Date Added	Dork	Category	Author
2024-02-26	"PMW" AND ("changes.txt" OR "urlinfo.txt")	Vulnerable Servers	Wallehaz
2024-02-26	intitle:"index of /confidential"	Files Containing Juicy Info	Gautam Rawat
2024-02-26	intitle:"wp-content/uploads/1/downloads.txt"	Files Containing Juicy Info	Jeel Patel
2024-02-16	intitle:"auditing.txt"	Files Containing Juicy Info	Gautam Rawat
2024-02-16	intitle:"index of /web"	Files Containing Juicy Info	A.K.M. Mohuddin
2024-02-16	intitle:"index of /cgi.pl"	Files Containing Juicy Info	Gautam Rawat
2024-02-13	intitle:"encryption.txt"	Files Containing Juicy Info	Naved Arisan
2024-02-06	allintitle:"Bright Cluster Manager" site:.edu	Vulnerable Servers	Thomas Haverh
2024-02-05	intitle:"index of /enc.cgi"	Files Containing Juicy Info	Wallehaz
2024-02-02	intitle:"Welcome to rTop version" intext:and	Vulnerable Servers	Nadir Bouachet (HuX)
2024-02-02	intitle:"Installation Wizard - PowerCMS v2"	Vulnerable Servers	Nadir Bouachet (HuX)
2024-02-02	ext:java intext:"executables"	Files Containing Juicy Info	BULLETNIGHT
2024-02-02	"Started by upstream project" ext:txt	Files Containing Juicy Info	Nadir Bouachet (HuX)

La Google Hacking Database (GHDB) es un proyecto que se inició para catalogar varias consultas de búsqueda, conocidas como Google dorks, que se pueden utilizar para descubrir información vulnerable o sensible en sitios web. Estos dorks se utilizan para refinar las búsquedas de Google y encontrar tipos específicos de información a los que no se puede acceder fácilmente a través de las búsquedas estándar.

El GHDB incluye dorks para encontrar cosas como servidores web expuestos, scripts vulnerables, directorios confidenciales y más. Es importante tener en cuenta que, si bien el GHDB puede ser un recurso útil para los profesionales de la seguridad y los probadores de penetración, el uso de estos idiotas para el acceso o la explotación no autorizados es ilegal y poco ético.

El GHDB ya no se mantiene activamente como un proyecto separado, pero el concepto de los dorks de Google y su uso en las pruebas de seguridad sigue siendo relevante.

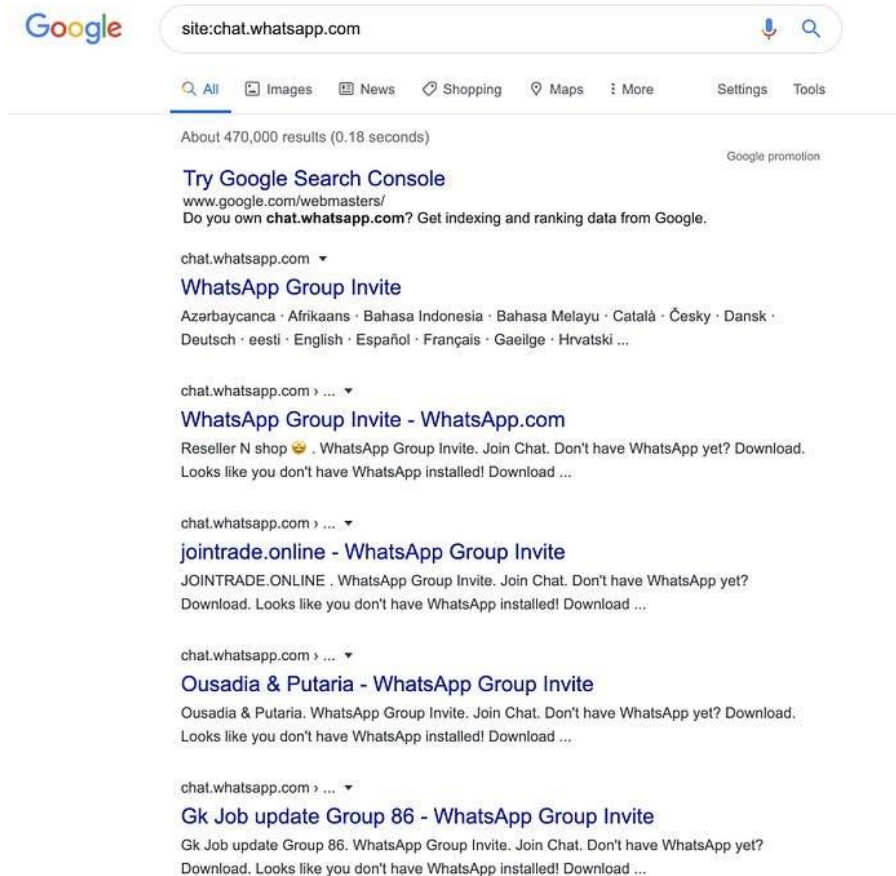
Dorking WhatsApp y Telegram

Es posible enumerar a los grupos de WhatsApp con un poco [de Google Dorking](#). El dork aprovecha los Grupos que ha permitido **"Invitar a Grupo a través de la función Enlace"**.

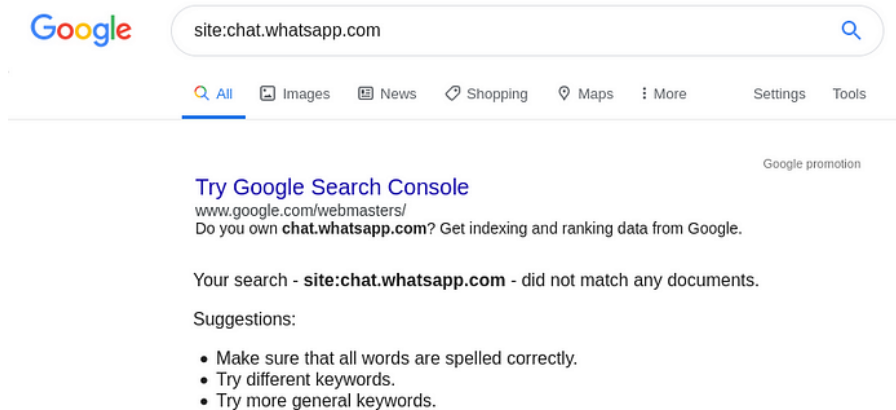
Un administrador de grupo puede entonces generar un vínculo público compartido con el grupo para que otros se unan. Esta característica permite que los grupos sean indexados por Google y muchos otros motores de búsqueda que hace que esté disponible a través de Internet. Esto fue considerado inicialmente como una configuración errónea en WhatsApp, ya **"noindex"** que la indexación podría haberse evitado mediante el uso de la etiqueta meta , pero Facebook no lo aceptó como un error de seguridad.

Google ha eliminado la indexación de los enlaces de WhatsApp después de que el tuit se hiciera viral sin embargo otros motores de búsqueda no lo hicieron.

Google Dork: `sitio:chat.whatsapp.com`



Antes de que Google eliminó la indexación



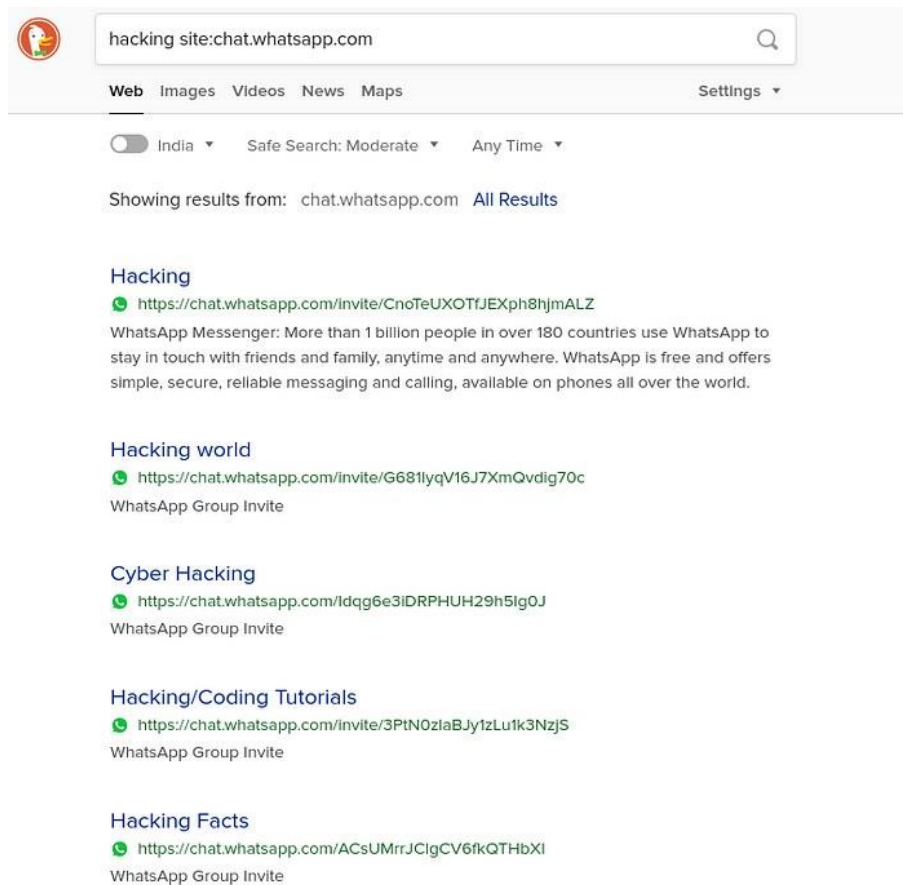
Tras la eliminación de la indexación

Sin embargo, estos todavía están presentes en otros motores de búsqueda como DuckDuck Go, Bing, Yahoo, etc. Para explotar esto podemos adjuntar el término de búsqueda ya sea en el prefijo o sufijo del idioma para enumerar los grupos que tienen nombre relacionado.

site:chat.whatsapp.com - hackeo - bitcoin - familia

(o)

sitio de hacking:chat.whatsapp.com



The screenshot shows a search engine interface with a search bar containing the text "hacking site:chat.whatsapp.com". Below the search bar, there are tabs for "Web", "Images", "Videos", "News", and "Maps", with "Web" selected. To the right of the tabs is a "Settings" dropdown menu. Below the tabs, there are filters for "India", "Safe Search: Moderate", and "Any Time". The search results are displayed below the filters, starting with "Showing results from: chat.whatsapp.com" and a link to "All Results". The results are categorized into several sections: "Hacking", "Hacking world", "Cyber Hacking", "Hacking/Coding Tutorials", and "Hacking Facts". Each section contains a list of links to WhatsApp chat groups, each preceded by a green WhatsApp icon. The links are: "https://chat.whatsapp.com/invite/CnoTeUXOTfJEXph8hjmALZ", "https://chat.whatsapp.com/invite/G681lyqV16J7XmQvdig70c", "https://chat.whatsapp.com/ldqg6e3IDRPHUH29h5Ig0J", "https://chat.whatsapp.com/invite/3PtN0ziaBJy1zLu1k3NzjS", and "https://chat.whatsapp.com/ACsUMrrJCigCV6fkQTHbXI". Each link is followed by the text "WhatsApp Group Invite".

hacking site:chat.whatsapp.com

Web Images Videos News Maps Settings

India Safe Search: Moderate Any Time

Showing results from: chat.whatsapp.com All Results

Hacking

WhatsApp Messenger: More than 1 billion people in over 180 countries use WhatsApp to stay in touch with friends and family, anytime and anywhere. WhatsApp is free and offers simple, secure, reliable messaging and calling, available on phones all over the world.

Hacking world

WhatsApp Group Invite

Cyber Hacking

WhatsApp Group Invite

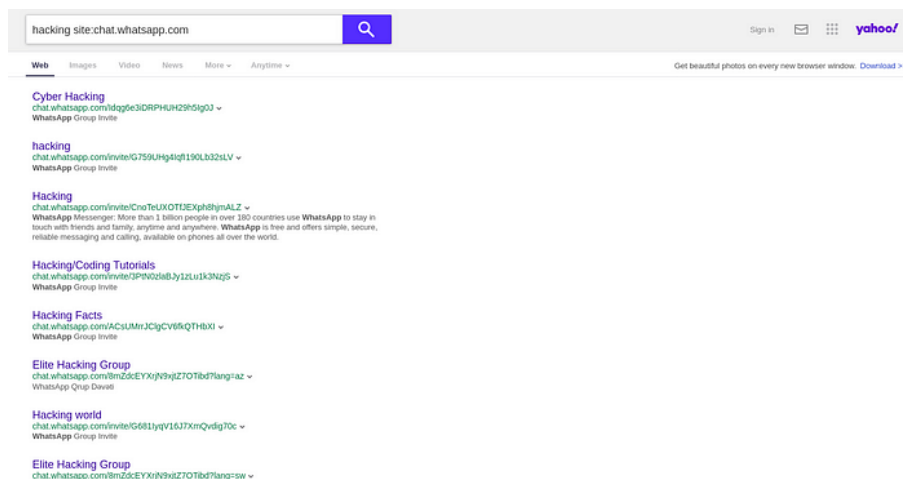
Hacking/Coding Tutorials

WhatsApp Group Invite

Hacking Facts

WhatsApp Group Invite

DuckDuckGo



The screenshot shows a search engine interface with a search bar containing the text "hacking site:chat.whatsapp.com". Below the search bar, there are tabs for "Web", "Images", "Video", "News", "More", and "Anytime", with "Web" selected. To the right of the tabs is a "Sign in" button and a "yahoo/" link. Below the tabs, there are filters for "India", "Safe Search: Moderate", and "Any Time". The search results are displayed below the filters, starting with "Showing results from: chat.whatsapp.com" and a link to "All Results". The results are categorized into several sections: "Cyber Hacking", "hacking", "Hacking", "Hacking/Coding Tutorials", "Hacking Facts", "Elite Hacking Group", "Hacking world", and "Elite Hacking Group". Each section contains a list of links to WhatsApp chat groups, each preceded by a green WhatsApp icon. The links are: "https://chat.whatsapp.com/ldqg6e3IDRPHUH29h5Ig0J", "https://chat.whatsapp.com/invite/G759UHq4q1190lb32sLV", "https://chat.whatsapp.com/invite/CnoTeUXOTfJEXph8hjmALZ", "https://chat.whatsapp.com/invite/3PtN0ziaBJy1zLu1k3NzjS", "https://chat.whatsapp.com/ACsUMrrJCigCV6fkQTHbXI", "https://chat.whatsapp.com/invite/8m2dcEYX0N9vZ7OTbd7angraz", "https://chat.whatsapp.com/invite/G681lyqV16J7XmQvdig70c", and "https://chat.whatsapp.com/invite/8m2dcEYX0N9vZ7OTbd7angraz". Each link is followed by the text "WhatsApp Group Invite".

hacking site:chat.whatsapp.com

Web Images Video News More Anytime

Sign in yahoo/

Showing results from: chat.whatsapp.com All Results

Cyber Hacking

WhatsApp Group Invite

hacking

WhatsApp Group Invite

Hacking

WhatsApp Messenger: More than 1 billion people in over 180 countries use WhatsApp to stay in touch with friends and family, anytime and anywhere. WhatsApp is free and offers simple, secure, reliable messaging and calling, available on phones all over the world.

Hacking/Coding Tutorials

WhatsApp Group Invite

Hacking Facts

WhatsApp Group Invite

Elite Hacking Group

WhatsApp Group Invite

Hacking world

WhatsApp Group Invite

Elite Hacking Group

WhatsApp Group Invite

Yahoo

The screenshot shows a Bing search results page for the query "hacking site:chat.whatsapp.com". The search bar at the top contains the query. Below the search bar, there are tabs for "ALL", "IMAGES", "VIDEOS", "MAPS", and "NEWS". The "ALL" tab is selected. Below the tabs, there are filters for "11 Results", "Date", "Language", and "Region". The search results are displayed in a list format. The first result is titled "Hacking Course - New results - Get All Results" and includes a link to "https://search.visymo.com/hacking course". Below the link, there is a snippet: "(Ad) 99% Match on Hacking Course. Start searching with Visymo.com. Always Facts - Unlimited Access - The Best Resources Services: Best Results, #1 Search, Explore Now, Best Sources". To the right of the snippet, there are two buttons: "99% Match" and "100's of Results". Below the first result, there is a second result titled "Hacking Course - Search Hacking Course | izito.co.in" and a link to "https://www.izito.co.in/hacking course/quality_results". Below the link, there is a snippet: "(Ad) Get Hacking Course. Discover Millions Of Results Here Discover Quality Results - Find Related Results Now Types: News, Video, Images, Web, Wiki". To the right of the snippet, there are two buttons: "Better Results" and "Search Efficiently". Below the second result, there is a third result titled "WhatsApp Group Invite" and a link to "https://chat.whatsapp.com/DkdwoZML1VmDjPsv0Vv5Tq". Below the link, there is a snippet: "WhatsApp Group Invite". To the right of the snippet, there are two buttons: "Search Smarter" and "Find Fast". Below the third result, there is a fourth result titled "hacking" and a link to "https://chat.whatsapp.com/invite/G759UHG4lqf190Lb32sLV". Below the link, there is a snippet: "WhatsApp Group Invite". To the right of the snippet, there are two buttons: "Search Efficiently" and "Find Fast". Below the fourth result, there is a fifth result titled "Hacking world" and a link to "https://chat.whatsapp.com/invite/G681lyqV16J7XmQvdig70c". Below the link, there is a snippet: "WhatsApp Group Invite". To the right of the snippet, there are two buttons: "Search Smarter" and "Find Fast". Below the fifth result, there is a sixth result titled "Cyber Hacking" and a link to "https://chat.whatsapp.com/ldqg6e3iDRPHUH29h5ig0J". Below the link, there is a snippet: "WhatsApp Group Invite". To the right of the snippet, there are two buttons: "Search Smarter" and "Find Fast". Below the sixth result, there is a seventh result titled "Hacking/Coding Tutorials".

Bing

Incluso los Grupos de Telegram están siendo indexados de la misma manera que provocando que los Grupos cotizaran de la misma manera.

site:t.me/joinchat

Es importante tener en cuenta que incluso si no es un problema crítico, pero muchos datos de los usuarios se pueden recuperar.

Búsquedas

🔑 1. Encontrar archivos con contraseñas:

filetype:txt intext:"password"

📹 2. Cámaras de seguridad accesibles:

inurl:"view.shtml"

3. Paneles de administración vulnerables

intitle:"Admin Login" inurl:adminlogin

4. Servidores FTP sin seguridad

intitle:"index of" inurl:ftp

5. Documentos confidenciales filtrados

filetype:pdf "confidential"