



PRACTICA 3 NAVEGADORES



Hecho por: Izan Navarro

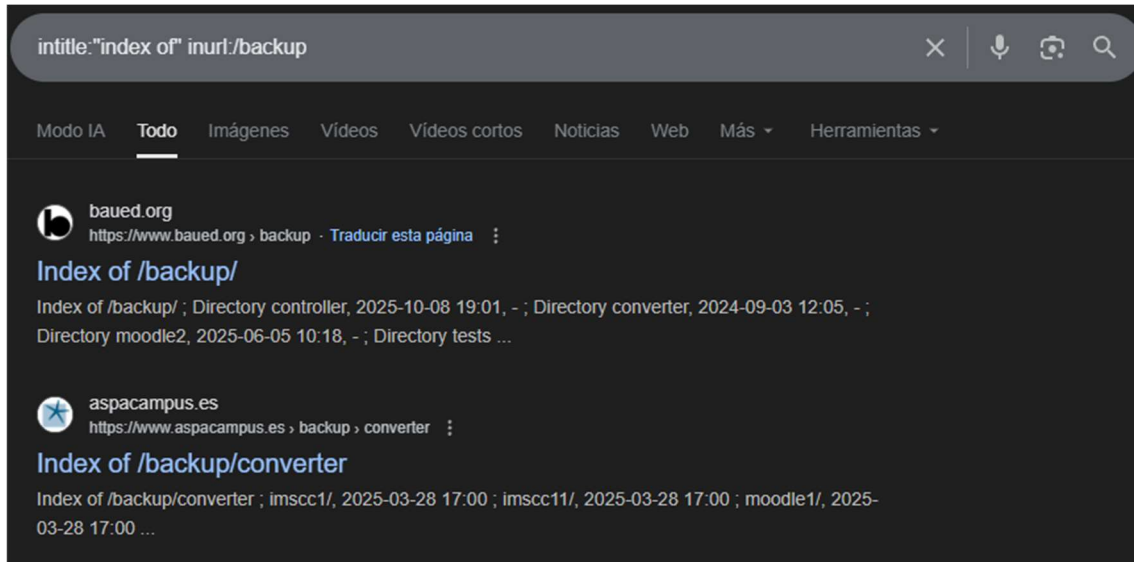


INDICE

Ejercicio 1. Búsqueda de información con GOOGLE	3
Ejercicio 2. Búsqueda de información con BING	9
Ejercicio 3. Búsqueda de información con Shodan	12
Ejercicio 4. Búsqueda de información del dominio de una organización con Robtex	13

Ejercicio 1. Búsqueda de información con GOOGLE

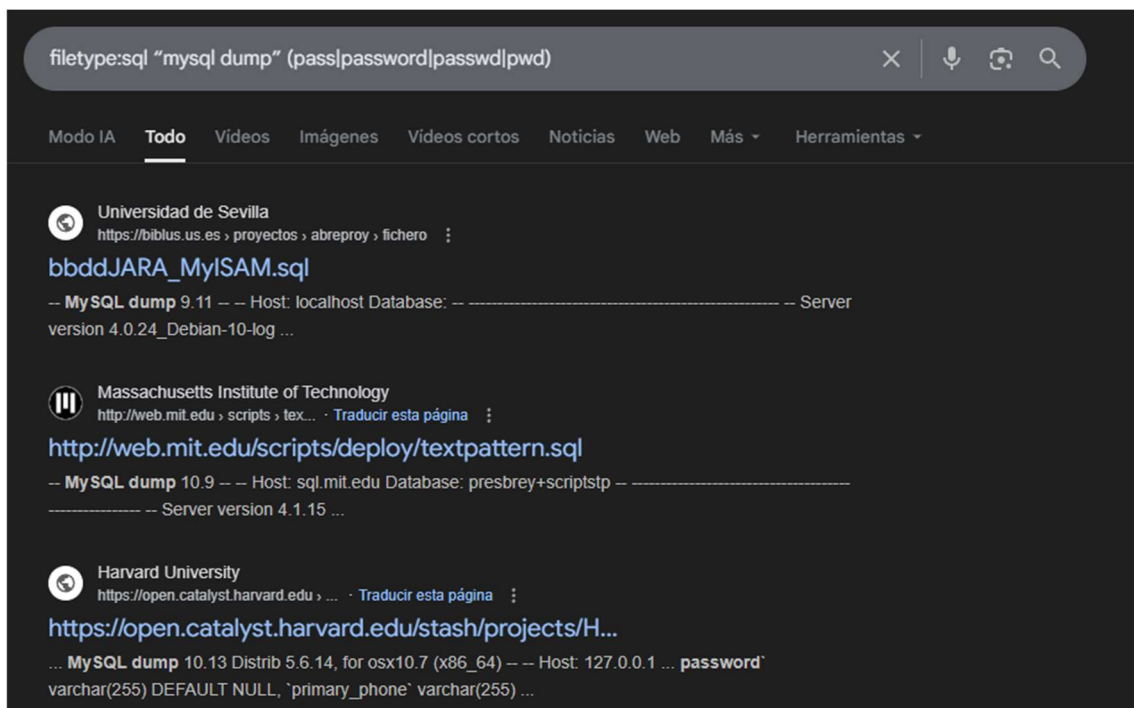
- `intitle:"index of" inurl:/backup:`



-Intitle "index of": Busca páginas cuyo título contenga exactamente "index of"

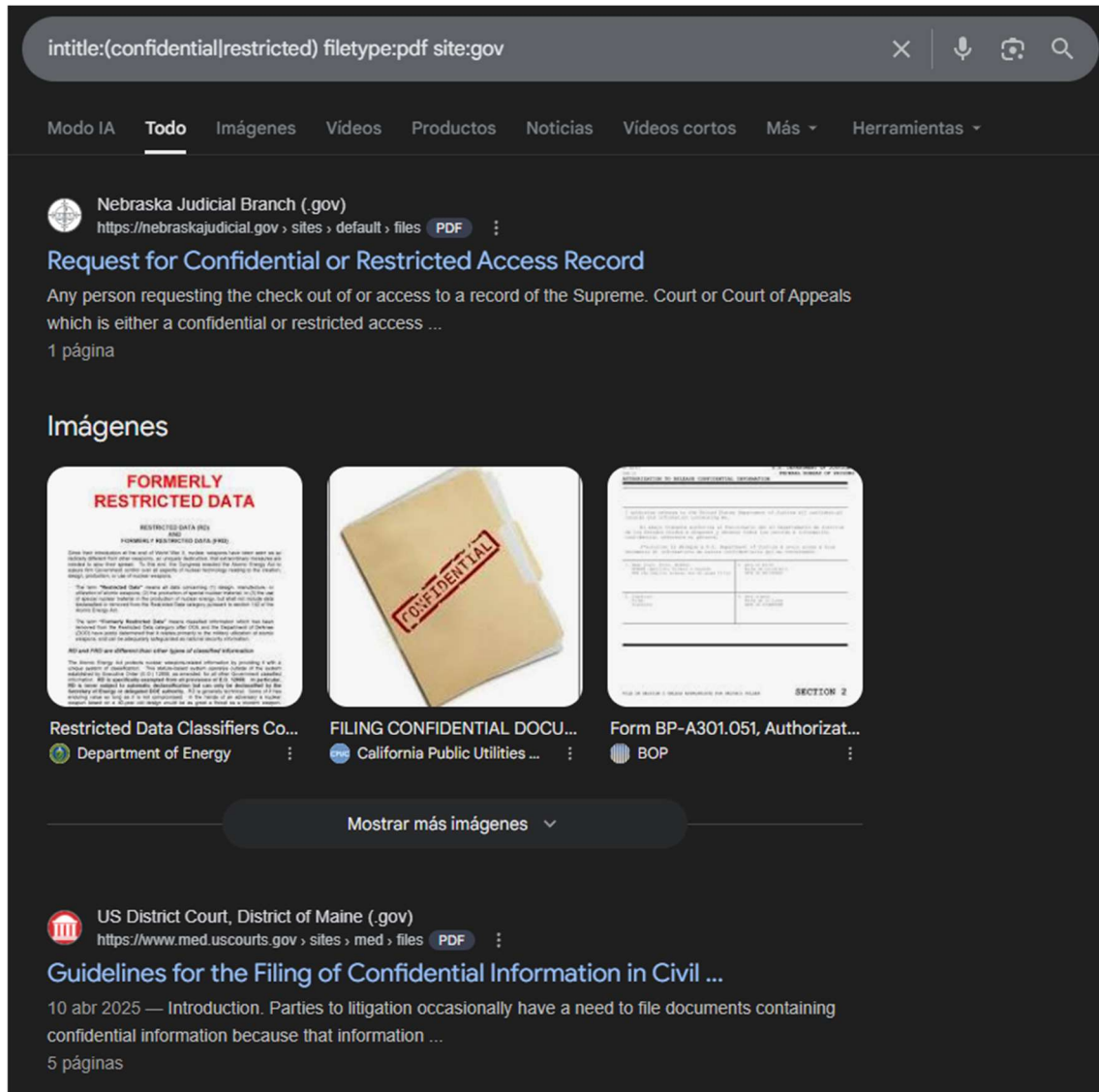
-inurl:/backup: Obliga a que la URL contenga la cadena /backup (directorio llamado backup)

- `filetype:sql "MySQL dump" (pass|password|passwd|pwd):`



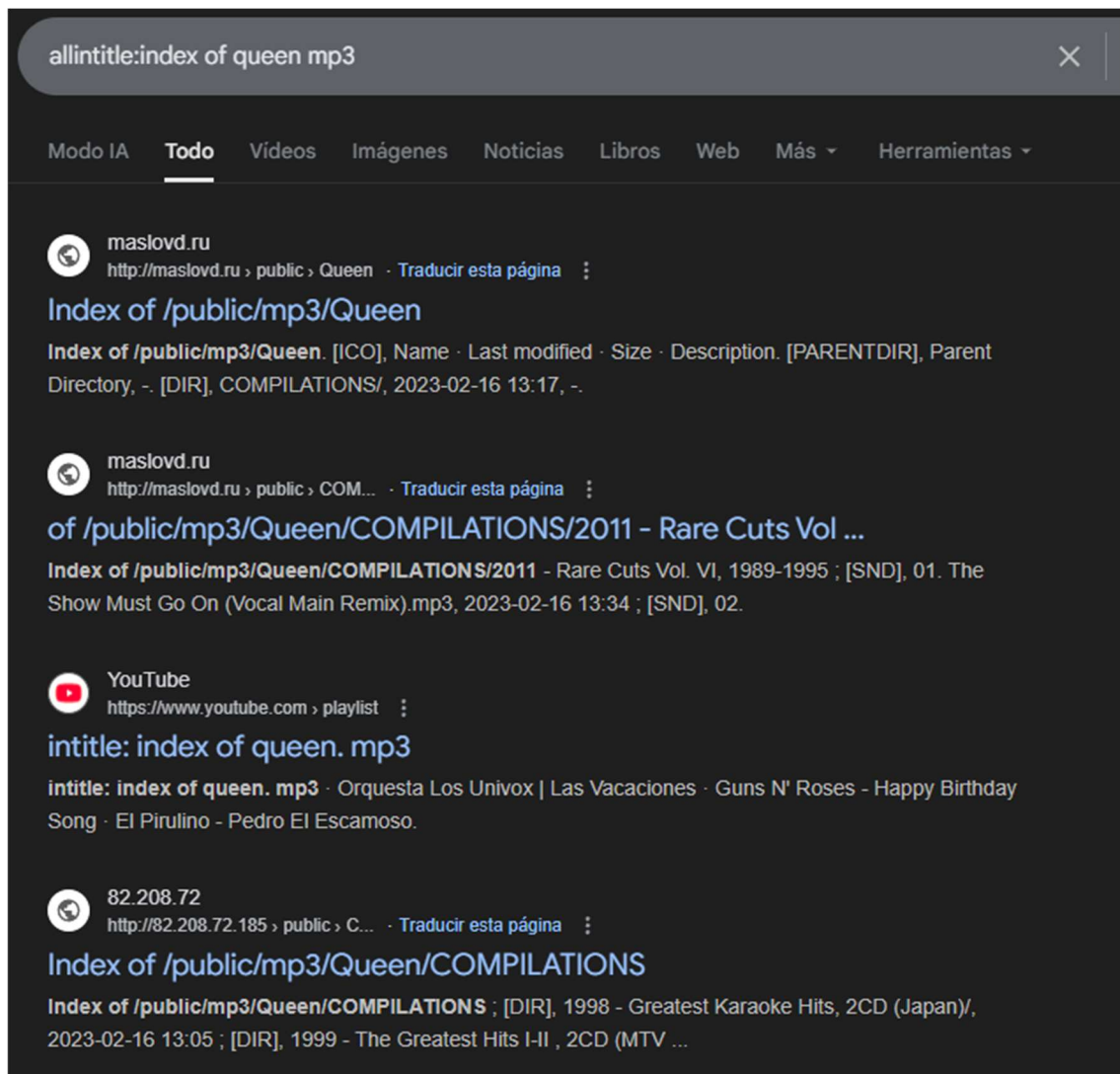
- (pass|password|passwd|pwd) → Busca cualquiera de esas palabras en la página (o en el archivo indexado).

- "MySQL dump" → Frase exacta probablemente presente al comienzo de un volcado generado por mysqldump.
- filetype:sql → Restringe resultados a ficheros con extensión .sql.
- intitle:(confidential|restricted) filetype:pdf site:gov:



- intitle:(confidential|restricted) → el título contiene “confidential” o “restricted” (busca documentos marcados como restringidos).
- filetype:pdf → solo PDFs.
- site:gov → restringe a dominios .gov.

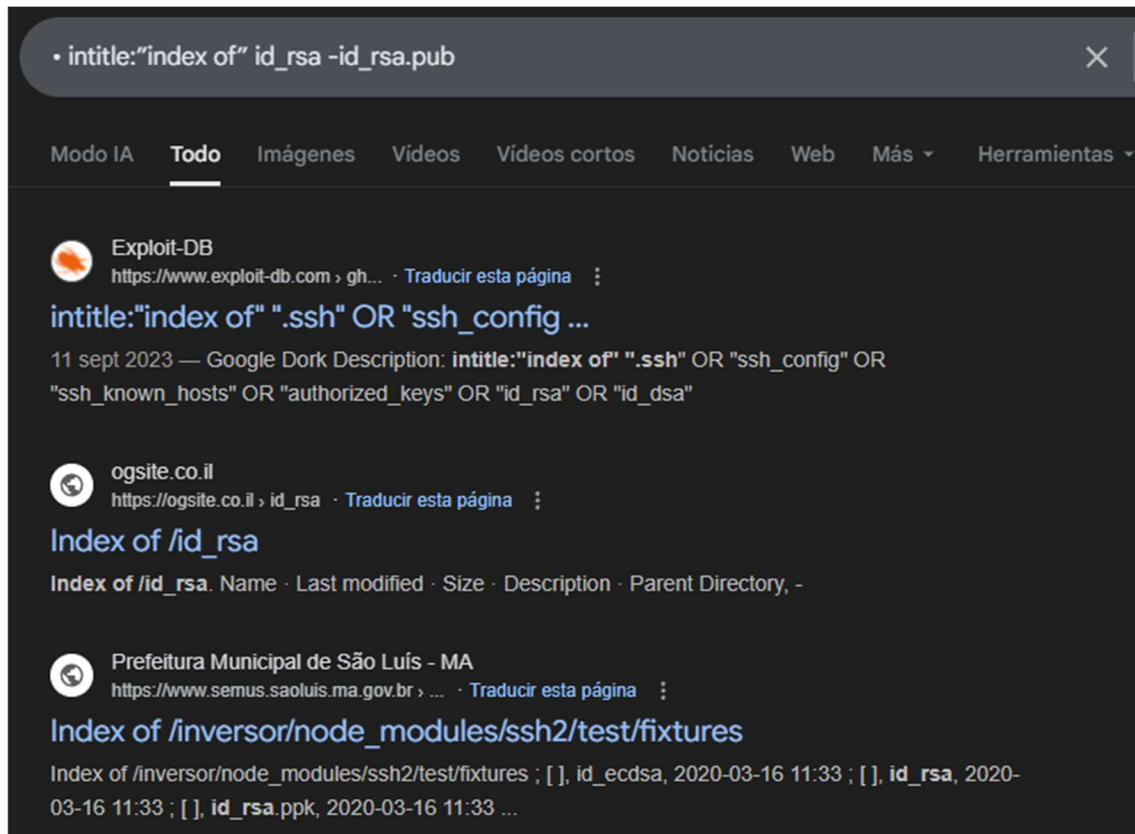
- allintitle:index of queen mp3:



- allintitle: → todos los términos a continuación deben aparecer en el título de la página.

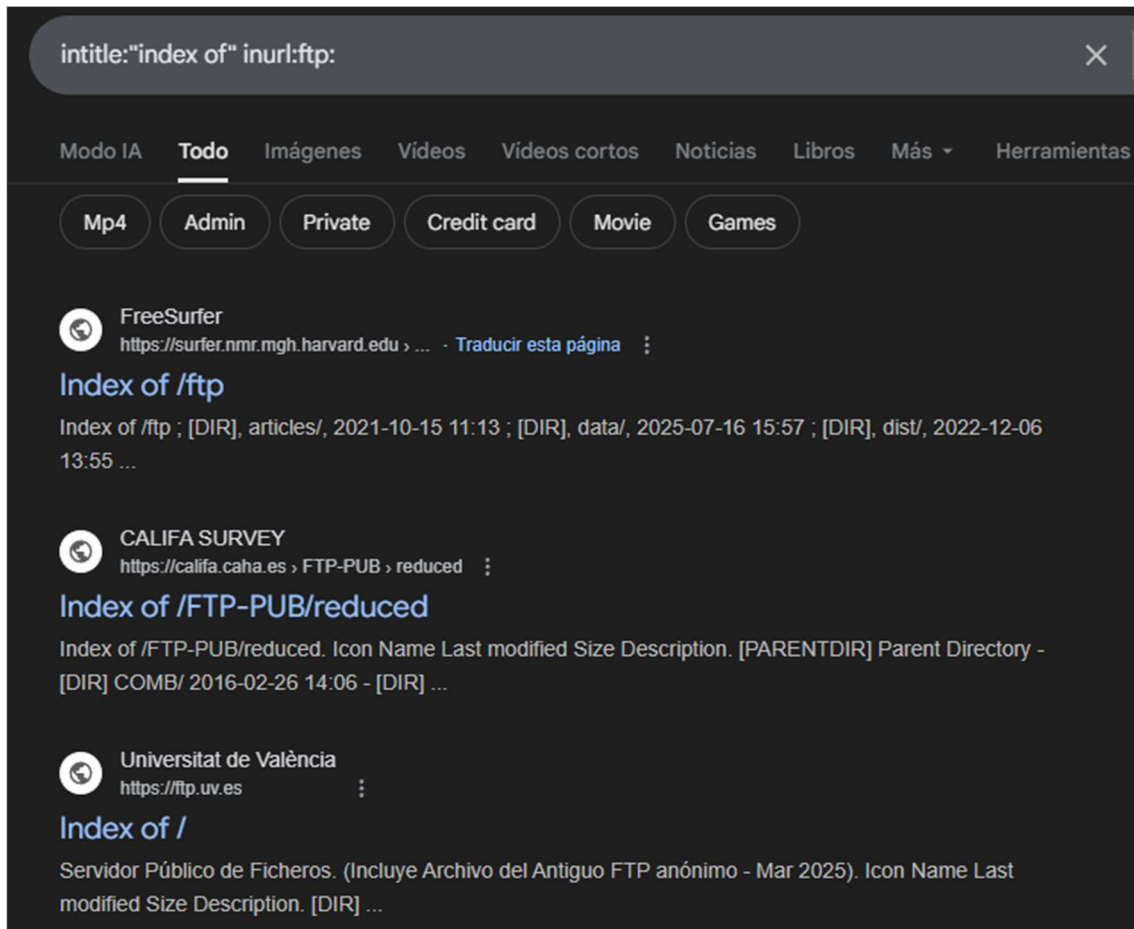
- index of queen mp3 → busca listados de directorio (index) cuyo título contenga las palabras index, of, queen, mp3.

- `intitle:"index of" id_rsa -id_rsa.pub`:



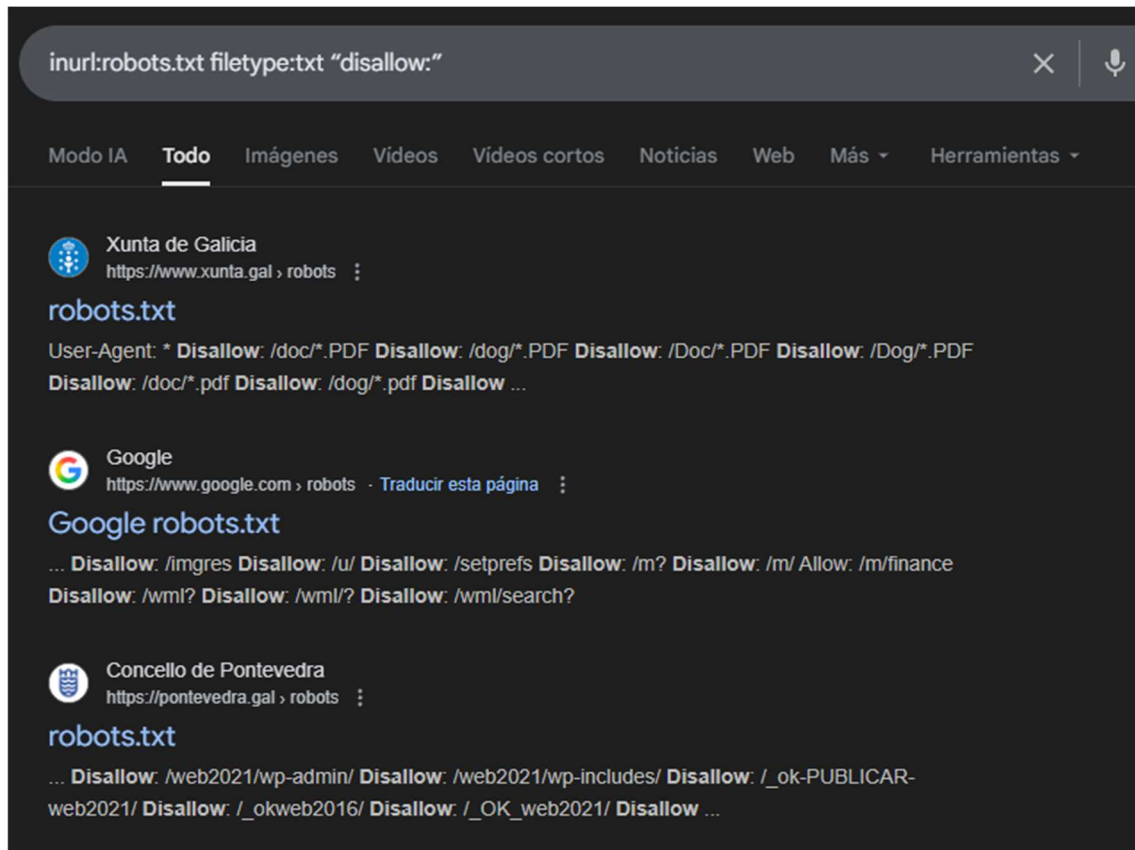
- `intitle:"index of"` → directorio indexado.
- `id_rsa` → busca la presencia de `id_rsa` (clave privada SSH) en la página/archivo.
- `-id_rsa.pub` → excluye resultados que contengan `id_rsa.pub` (la clave pública), porque típicamente si sólo hay `id_rsa.pub` no hay riesgo inmediato; el objetivo aquí es aislar *claves privadas* expuestas.

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



- Igual a los anteriores, pero obliga que la URL contenga ftp → listados expuestos vía servicios FTP o rutas que contienen “ftp”.

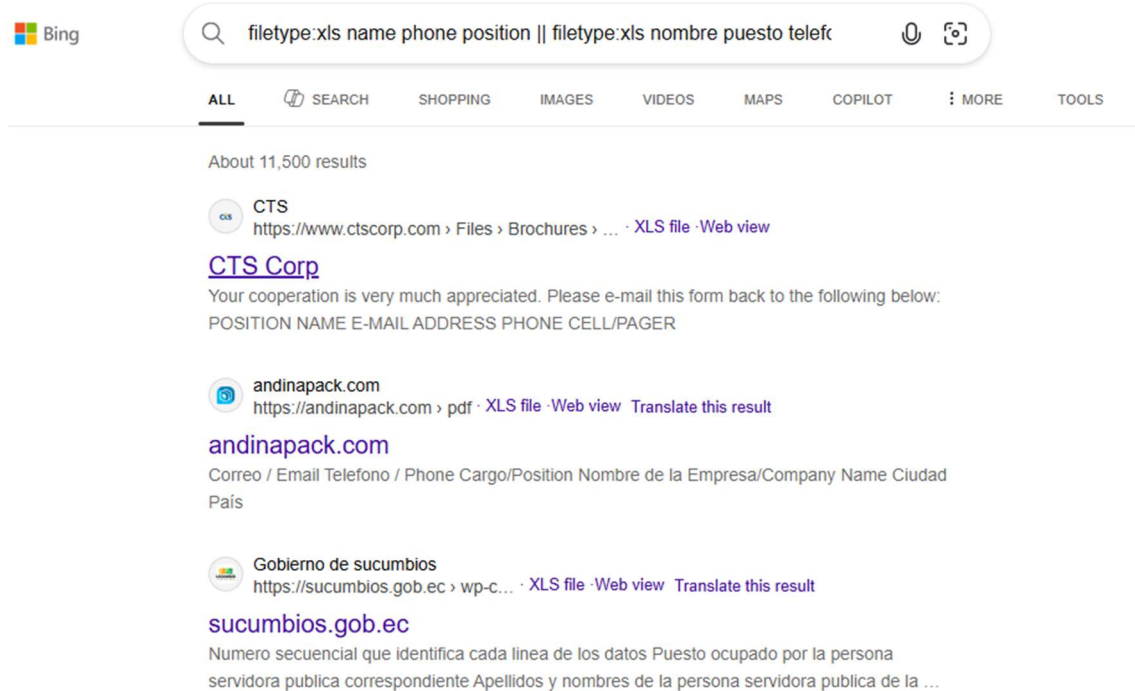
- `inurl:robots.txt filetype:text "disallow:"`:



- `inurl:robots.txt` → URL que termine o contenga robots.txt.
- `filetype:text` → arquivo de texto.
- `"disallow:"` → línea típica de robots.txt.

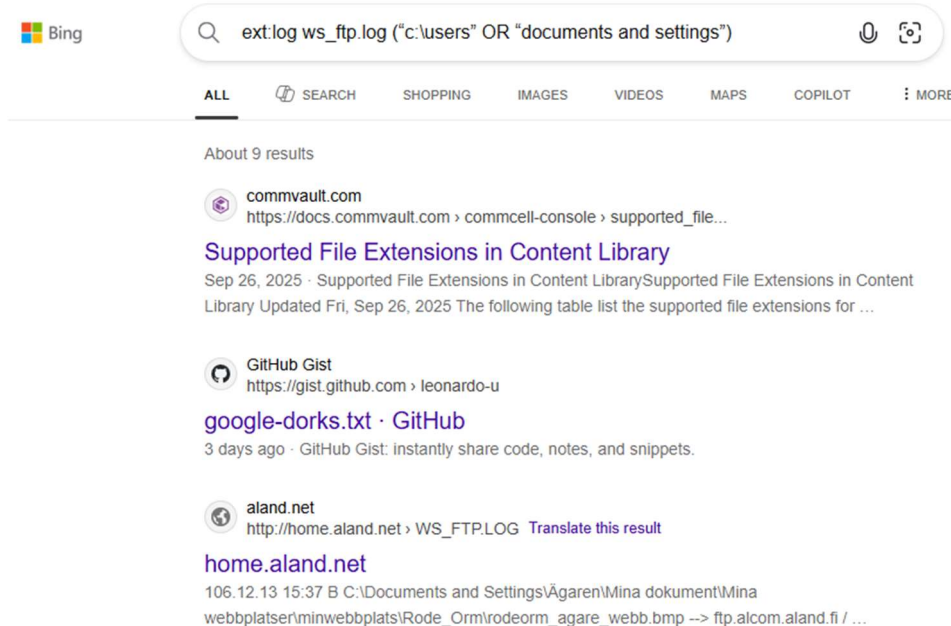
Ejercicio 2. Búsqueda de información con BING

- filetype:xls name phone position o filetype:xls nombre puesto teléfono:



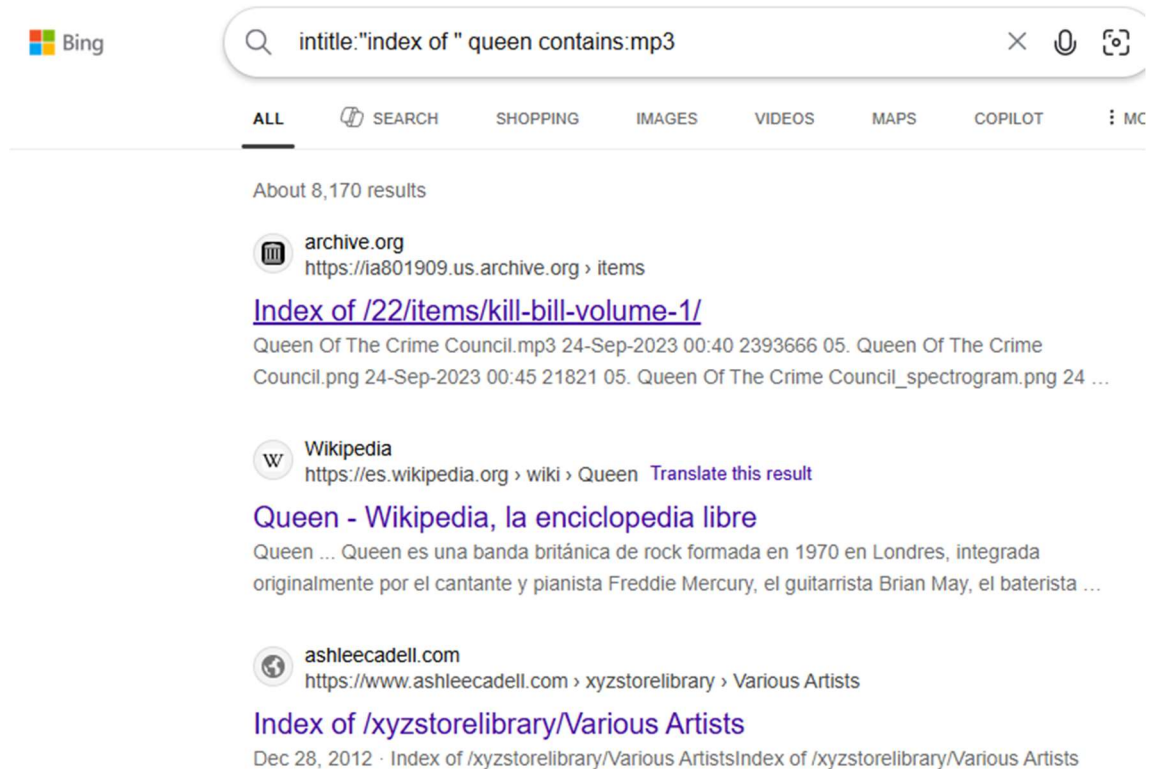
- filetype:xls → ficheros Excel (formato antiguo .xls) indexados.
- Las palabras name phone position (o su traducción) buscan hojas de cálculo que contengan columnas con esos encabezados → típicamente bases de datos de contactos, listados de empleados, etc.

- ext:log ws_ftp.log (“c:\users” OR “documents and settings”):




- ext:log → archivos con extensión .log.

- ws_ftp.log → nombre concreto de log (logs de cliente/servidor WS_FTP).
- ("c:\users" OR "documents and settings") → cadenas Windows típicas que aparecen en logs cuando la ruta local se registra (path de archivos).
- intitle:"index of " queen contains:mp3:




- intitle:"index of " → listados de directorio.
- queen → término buscado.
- contains:mp3 → operador Bing que indica que la página contiene archivos MP3.

- filetype:txt ext:sql insert into password:

 **mit.edu**
<https://scripts-cert.mit.edu> › trac › export › branches › locker-dev › ...


scripts-cert.mit.edu

```
system("mysql -e \"INSERT INTO jos_users VALUES (62, 'Administrator', '$admin_username', '$email', MD5('$admin_password'), 'Super Administrator', 0, 1, 25, NOW(), NOW(), ' ', ' ')\" $sqldb");
```

 **PostgreSQL 正體中文使用手冊**
<https://docs.postgresql.tw> › reference › client-applications ... [Translate this result](#)


docs.postgresql.tw

``--password`` This option is never essential, since `pg_dumpall` will automatically prompt for a password if the server demands password authentication. However, `pg_dumpall` will waste a ...

 **Comprehensive Perl Archive Network**
<https://www.cpan.org> › authors › id › SA › SATOH

www.cpan.org

Unlike `DBIx::Class`, you don't need to have a set of classes that represent a row type (i.e. "result" classes in DBIC terms). In `Teng`, the row objects are blessed into anonymous classes that ...

 **dolthub.com**
<https://docs.dolthub.com> › sql-reference › server › configuration.md

docs.dolthub.com

This is a bit of an advanced option. ``allow_cleartext_passwords`` only affects the ``mysql_clear_password`` auth plugin, which is only used for JSON Web Token (JWT) ...

- filetype:txt ext:sql → busca texto plano con contenido SQL (a veces los volcados .sql se indexan con .txt). ext:sql sería redundante pero apunta a extensiones relacionadas.
- insert into password → busca sentencias SQL INSERT INTO en tablas relacionadas con password (posible volcado o exposición de contraseñas).

Ejercicio 3. Búsqueda de información con Shodan

- Busca máquinas con Windows en Madrid, España:

The screenshot shows the Shodan search interface with the query `os:Windows city:"Madrid" country:"ES"`. The search results are categorized into several sections:

- TOTAL RESULTS:** 43,007
- TOP CITIES:**
 - Madrid: 42,939
 - Las Rozas de Madrid: 41
 - Humanes de Madrid: 27
- TOP PORTS:**
 - 80: 8,404
 - 3389: 7,674
 - 443: 6,000
 - 1433: 1,466
 - 21: 1,360
- TOP ORGANIZATIONS:**
 - TELEFONICA DE ESPAÑA S.A.U.: 5,348
 - IONOS SE: 2,941
 - arsys.es: 2,370
 - Teléfonos de España S.A.U.: 2,288

Two detailed results are shown:

- IIS Windows Server:** IP 82.194.94.93, Hostname `customers.hostalia.com`, Organization `Secigo Limited`. The SSL certificate is issued by `Secigo RSA Domain Validation Secure Server CA`.
- Service:** IP 68.221.232.110, Hostname `gwt.cloudapp.net`, Organization `Microsoft Corporation`. The SSL certificate is issued by `AME Infra CA 03`.

- El comando a ejecutar es: **`os:Windows city:"Madrid" country:"ES"`**

- Busca máquinas en España con Terminal Server abierto (posible ataque con malware BlueKeep):

The screenshot shows the Shodan search interface with the query `port:3389 country:"ES" product:"Microsoft Terminal Services"`. The search results are empty, and a blue banner displays the message: **Note: No results found**.

-El comando a ejecutar es: **`port:3389 country:"ES" product:"Microsoft Terminal Services"`**

- Busca routers Asus RT-AC68U en Portugal (pt):

product:"RT-AC68U" country:"PT"

View Report View on Map Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

85.247.150.111 madds.asuscomm.com bl14-150-111.dsl.telepac.pt PT Comunicacoes S.A. Portugal, Funchal	SSL Certificate Issued By: - Common Name: R10 - Organization: Let's Encrypt Issued To: - Common Name: madds.asuscomm.com	HTTP/1.0 200 OK Server: httpd/2.0 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block Date: Sun, 19 Oct 2025 19:09:39 GMT Content-Type: text/html Connection: close
79.168.170.35 www.asusrepeater.com router.asus.com a79-168-170-35.cpe.netcabo.pt www.asusrouter.com www.asusswitch.com NOS COMUNICACOES S.A. Portugal, São Domingos de Rana self-signed	SSL Certificate Issued By: - Common Name: www.asusrouter.com Issued To: - Common Name: www.asusrouter.com	HTTP/1.0 200 OK Server: httpd/2.0 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block Date: Sun, 19 Oct 2025 14:33:54 GMT Content-Type: text/html Connection: close
62.28.41.246 cegadvogadosmm.asuscomm.com static-wan-bl3-41-246.rev.webside.pt PT Prime - Solucoes Empresariais Portugal, Lisbon	SSL Certificate Issued By: - Common Name: R13 - Organization: Let's Encrypt Issued To: - Common Name: cegadvogadosmm.asuscomm.com	HTTP/1.0 200 OK Server: httpd/2.0 x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block Date: Sun, 19 Oct 2025 13:55:23 GMT Content-Type: text/html Connection: close

-El comando a ejecutar es: **product:"RT-AC68U" country:"PT"**

- Busca servidores Apache versión 2.4.6 en Centos en Francia (fr):

product:Apache version:2.4.6 os:CentOS country:"FR"

Note: No results found

-El comando a ejecutar para poder buscarlo es: **product:Apache version:2.4.6 os:CentOS country:"FR"**

Ejercicio 4. Búsqueda de información del dominio de una organización con Robtex

Accede a Robtex y realiza alguna consulta sobre algún nombre de dominio o alguna dirección IP y adjunta una captura del resultado. Comenta brevemente el tipo de información que te muestra. Para determinado tipo de información, es necesario hacer login. Puedes hacerlo de manera gratuita (aunque limitado como en Shodan) con una cuenta de Google.

·WIKIPEDIA.ORG:

The screenshot shows the Robtex website interface for a DNS lookup of wikipedia.org. The page title is "WWW.ROBTEX.COM - wikipedia.org". The breadcrumb trail is "Home > DNS lookup > org > wikipedia". The search bar contains "wikipedia.org". Below the search bar, there are several buttons for different lookup types: "Discover more", "Reverse DNS lookup", "Email", "reverse DNS", "DNS lookup", "mail", "Message transfer agent", "Robtex", "mail server", and "Reverse DNS Lookup". The results section shows "wikipedia.org checked at 2025-10-19T20:49:37.930Z 885ms 134/134/134 100% R:28". The "AI analysis" section provides additional information: "wikipedia.org is a parent of tpi.wikipedia.org, kv.wikipedia.org, donate.wikipedia.org, ne.wikipedia.org, csb.wikipedia.org and several hundreds other host names." and "wikipedia.org points to two IP numbers: 2a02:ec80:300:ed1a::1 and 185.15.59.224." The "PTR" section shows "mx-in1001.wikimedia.org".

WWW.ROBTEX.COM - wikipedia.org

Home > DNS lookup > org > wikipedia

Search for IP or hostnames:

P/hostname
wikipedia.org

Discover more [Reverse DNS lookup](#) [Email](#) [reverse DNS](#) [DNS lookup](#) [mail](#) [Message transfer agent](#) [Robtex](#) [mail server](#) [Reverse DNS Lookup](#)

wikipedia.org checked at 2025-10-19T20:49:37.930Z 885ms 134/134/134 100% R:28

wikipedia.org

MX [mx-in1001.wikimedia.org](#)

A [2620:0:861:4:208:80:155:102](#)
us [Wikimedia Foundation](#)

PTR [mx-in1001.wikimedia.org](#)

AI analysis

wikipedia.org is a parent of [tpi.wikipedia.org](#), [kv.wikipedia.org](#), [donate.wikipedia.org](#), [ne.wikipedia.org](#), [csb.wikipedia.org](#) and several hundreds other host names.

wikipedia.org points to two IP numbers: [2a02:ec80:300:ed1a::1](#) and [185.15.59.224](#).

Other host names such as [wiktionary.org](#), [text-](#)

Robtex muestra:

- Registros DNS (A, AAAA, CNAME, MX, NS)
- Reverse DNS
- ASN/propietario
- Rutas BGP relacionadas y
- Relaciones entre dominios e IPs.

·IP PÚBLICA:

IP/hostname
93.184.216.34

Cost effective ISO 27001

Grow globally with ISO 27001 compliance. Accelerating ISO 27001 compliance with Sprinto.

93.184.216.34 checked at 2025-10-19T20:52:28.309Z 470ms 38/38/38 100% R:21

PTRs and A-records

A	beacnpaim.com
A	93.184.216.34
A	franciscleary.com
A	93.184.216.34
A	frogpondpottery.com
A	93.184.216.34
A	google-webstore.com
A	93.184.216.34
A	lagrangesystems.com

Robtex muestra:

- Registros A / reverse (Passive DNS)
- Información de Red y Bloque
- Geolocalización e información adicional