Google Hacking o Dorks son técnicas para hackear páginas web o servidores usando la búsqueda avanzada de Google como herramienta. Habitualmente, cuando escribo trucos para ser el 1º en Google, Google es bueno, te ayuda y es tu amigo. Pero aquí verás cómo Google puede ser tu peor enemigo. El proceso que sigue un hacker tiene 7 pasos:

1. Localizar objetivo
2. Recopilar información sobre objetivo
3. Identificar vulnerabilidades
4. Explotar vulnerabilidades y acceder
5. Ataque
6. Borrado de huellas
7. Mantener el acceso, para futuras ocasiones

Google les ayuda directamente en los pasos 1, 2, 3 y 7. E indirectamente en los pasos 4, 5 y 6, porque pueden buscar en Google cómo llevarlos a cabo.

Búsqueda avanzada de Google: comandos y trucos

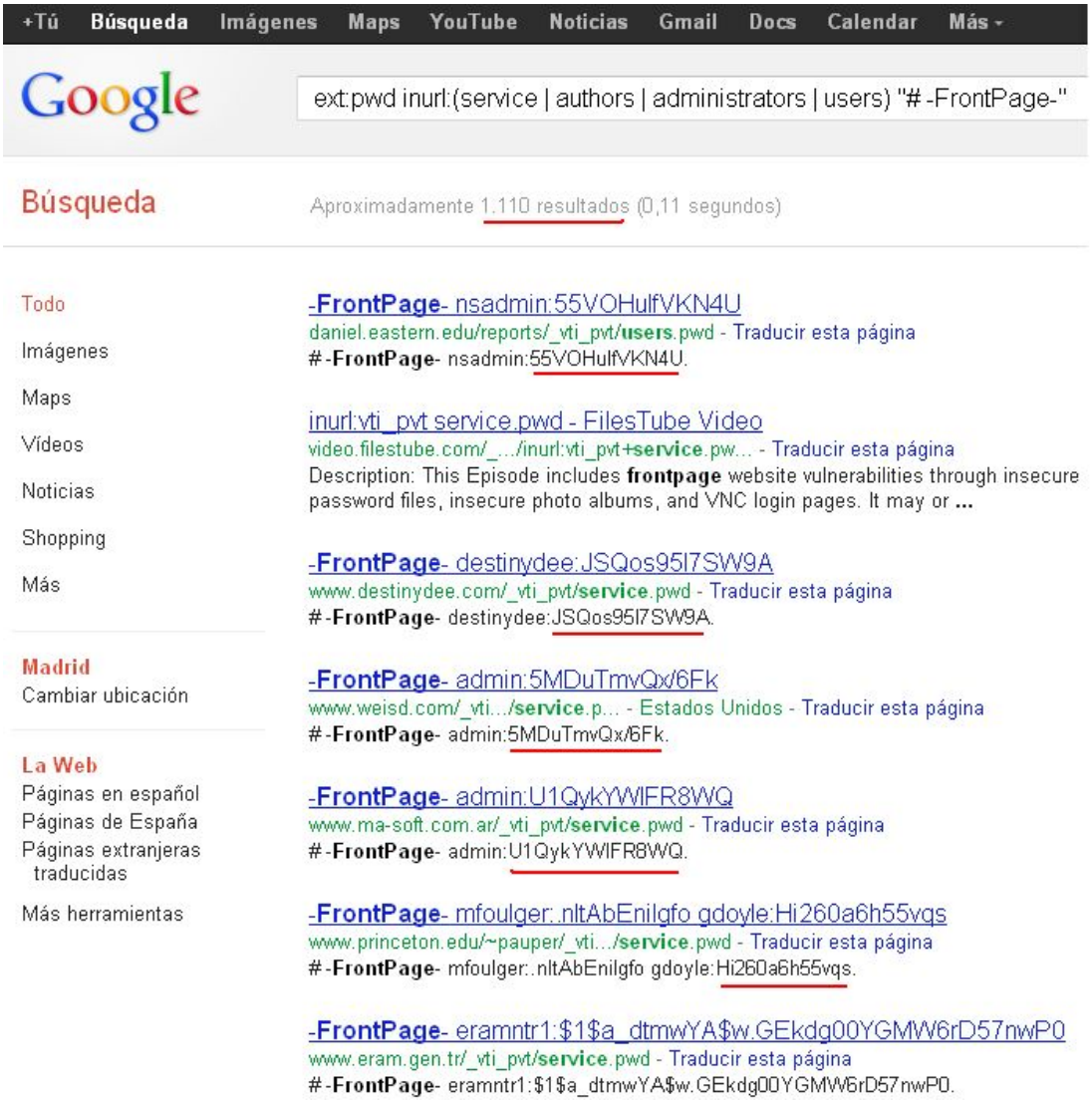
Para hacer Google Hacking, tienes que conocer los operadores avanzados de búsqueda de Google o comandos de búsqueda avanzada de Google, que se pueden incluir en el recuadro normal de búsquedas individualmente o combinados entre sí. Luego pondré ejemplos reales de esto, no te preocupes si no lo entiendes ahora. Además, tienes más información en la guía de Google sobre sus comandos de búsqueda avanzada de Google. Aquí van los principales comandos de búsqueda avanzada Google:

” ” (comillas): buscar frase exacta
and or **not**: operadores lógicos “y” o “no”
+ y **-**: incluir y excluir. Ej: jaguar -coches: busca la palabra “jaguar”, pero omite las webs con la palabra “coches”
***** (asterisco): comodín, cualquier palabra, pero una sóla palabra
. (punto): comodín, cualquier palabra, una o muchas
intitle o allintitle: la expresión buscada está en el título
inurl o allinurl: la expresión buscada está en la url
site: sólo busca resultados dentro de la web que va detrás de “site:”
filetype: sólo busca archivos de un tipo (doc, xls, txt…)
link: sólo busca en páginas que tienen un link a una determinada web
inanchor: sólo busca en páginas que tienen en el texto de enlace la expresión buscada
cache: muestra el resultado en la caché de Google de una página web
related: busca webs relacionadas con una determinada

Combinando estos operadores, el hacker puede obtener 7 tipos de información. A continuación describo los grupos de información y pongo en cursiva los códigos que hay que meter en el rectángulo de búsquedas de Google:

1) Ficheros con usuarios y contraseñas: lo que permite al hacker entrar directamente en tu web. Ejemplos:

- **ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-"** Usuarios y claves de administradores, para modificar la web. Se ven directamente en Google, sin necesidad de entrar en la página. Hay más de 1.100 claves así en Google

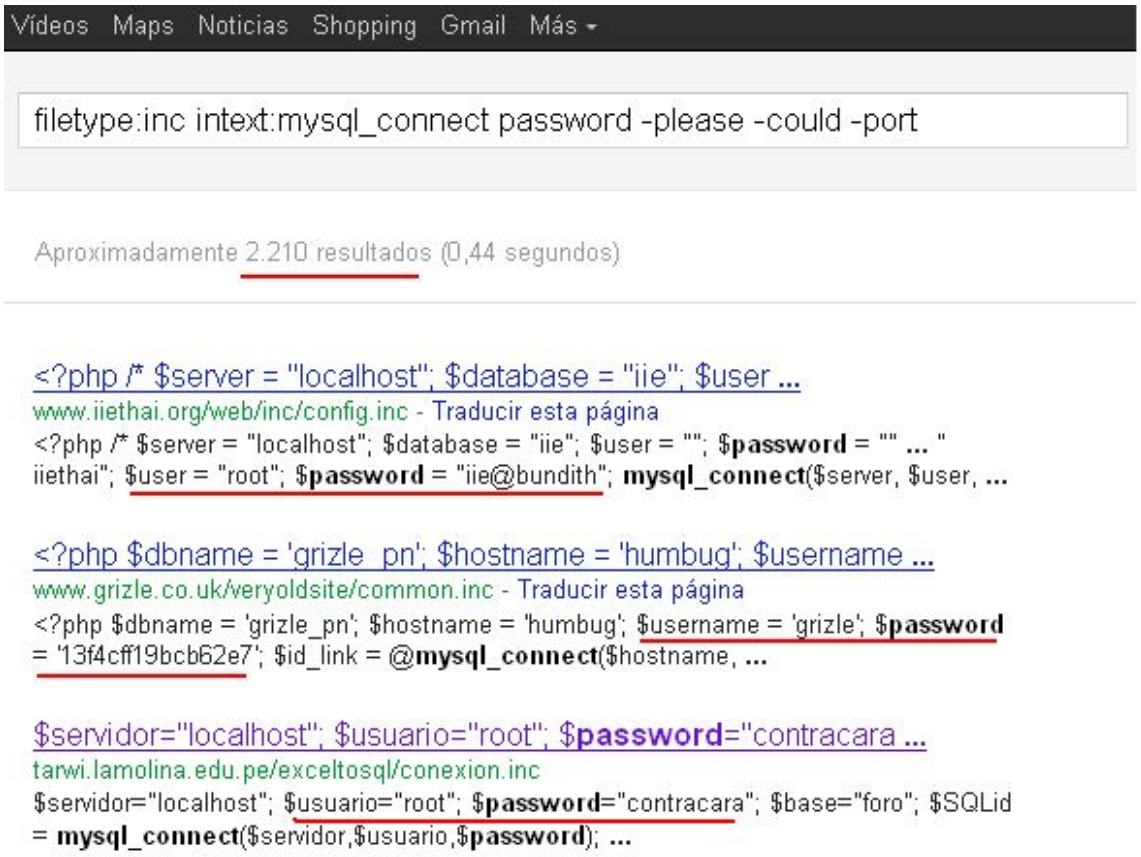


- **filetype:sql "# dumping data for table" "`PASSWORD` varchar"** Bases de datos sql volcadas completas, tienen datos de usuarios y contraseñas. Se pueden hacer modificaciones en la cadena de búsqueda, para sacar otros tipos de información. Aquí un ejemplo de contraseñas de la Universidad de Vigo. Las contraseñas van encriptadas en md5, pero basta buscar en Google la contraseña y el hacker encontrará un foro donde alguien la ha desencriptado y sale la original. Pongo un recuadro negro en los e-mails

```
#
# Table structure for table 'USUARIO'
#

# DROP TABLE IF EXISTS USUARIO;
CREATE TABLE `USUARIO` (
  `ID` bigint(20) NOT NULL AUTO_INCREMENT,
  `TIPO_USUARIO` varchar(20) DEFAULT NULL,
  `EMAIL` varchar(255) DEFAULT NULL,
  `ULTIMOACCESO` date DEFAULT NULL,
  `LOGIN` varchar(255) DEFAULT NULL,
  `FECHAALTA` date DEFAULT NULL,
  `PASSWORD` varchar(255) DEFAULT NULL,
  `VERSION` int(11) DEFAULT NULL,
  `NOMBRE` varchar(255) DEFAULT NULL,
  `APELLIDOS` varchar(255) DEFAULT NULL,
  `CODPOSTAL` varchar(255) DEFAULT NULL,
  `LOCALIDAD` varchar(255) DEFAULT NULL,
  `NIF` varchar(255) DEFAULT NULL,
  `DOMICILIO` varchar(255) DEFAULT NULL,
  `TELEFONO` varchar(255) DEFAULT NULL,
  `PROVINCIA` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`ID`)
) ENGINE=MyISAM AUTO_INCREMENT=5 DEFAULT CHARSET=latin1;

#
# Dumping data for table 'USUARIO'
#

INSERT INTO USUARIO VALUES (1,'administrador'[redacted],'2011-01-24','ana','2011-01-24','MwB+aDVFLGv1afWMderst9h2TCAxAaix',1,'Ana','Pére
INSERT INTO USUARIO VALUES (2,'administrador'[redacted],'2011-01-24','eva','2011-01-24','yjP8Y4Z5UX65i6w1CI9piwdy9gHQN7eI',1,'Eva','Garc
INSERT INTO USUARIO VALUES (3,'cliente','luis[redacted]11-01-24','luis','2011-01-24','W69Hv5nCOyjnFHaadauDgLOE47gBWyum',1,'Luis','Fernár
INSERT INTO USUARIO VALUES (4,'cliente','marc[redacted],'2011-01-24','marcos','2011-01-24','5ZahAjai59+WHaOWqUX+WngwHk3mn2Uy',1,'Marcos'
```

- **intitle:"index of" "Index of /" password.txt** Servidores con un archivo llamado password.txt. Se puede centrar por países con site:.es o por páginas educativas con **site:.edu**

- **filetype:inc intext:mysql_connect password -please -could -port** Google nos da más de 2.000 usuarios y contraseñas de bases de datos MySQL



- **filetype:sql "MySQL dump" (pass|password|passwd|pwd)** Más contraseñas disponibles en bases de datos
- **"there are no administrators accounts yet"** "create the Super User" inurl:admin.php Instalaciones de php nuke a mitad de proceso, que nos piden que elijamos la contraseña de administrador.

2) Páginas con formularios de acceso (típica ventana que te pide usuario y contraseña, para entrar): lo que les permite realizar un ataque de diccionario (con listas de usuarios y contraseñas más frecuente combinados). Y si no consigue entrar por ahí usará la fuerza bruta: probando contraseñas con un programa, hasta conseguir entrar. El hacker puede usar Brutus u otros programas similares, para sacar las contraseñas. Tienes más detalles sobre esto en: ¿Cómo robar contraseñas de wifi, windows, hotmail, gmail, tuenti, msn, facebook, twitter o yahoo?. Ejemplos:

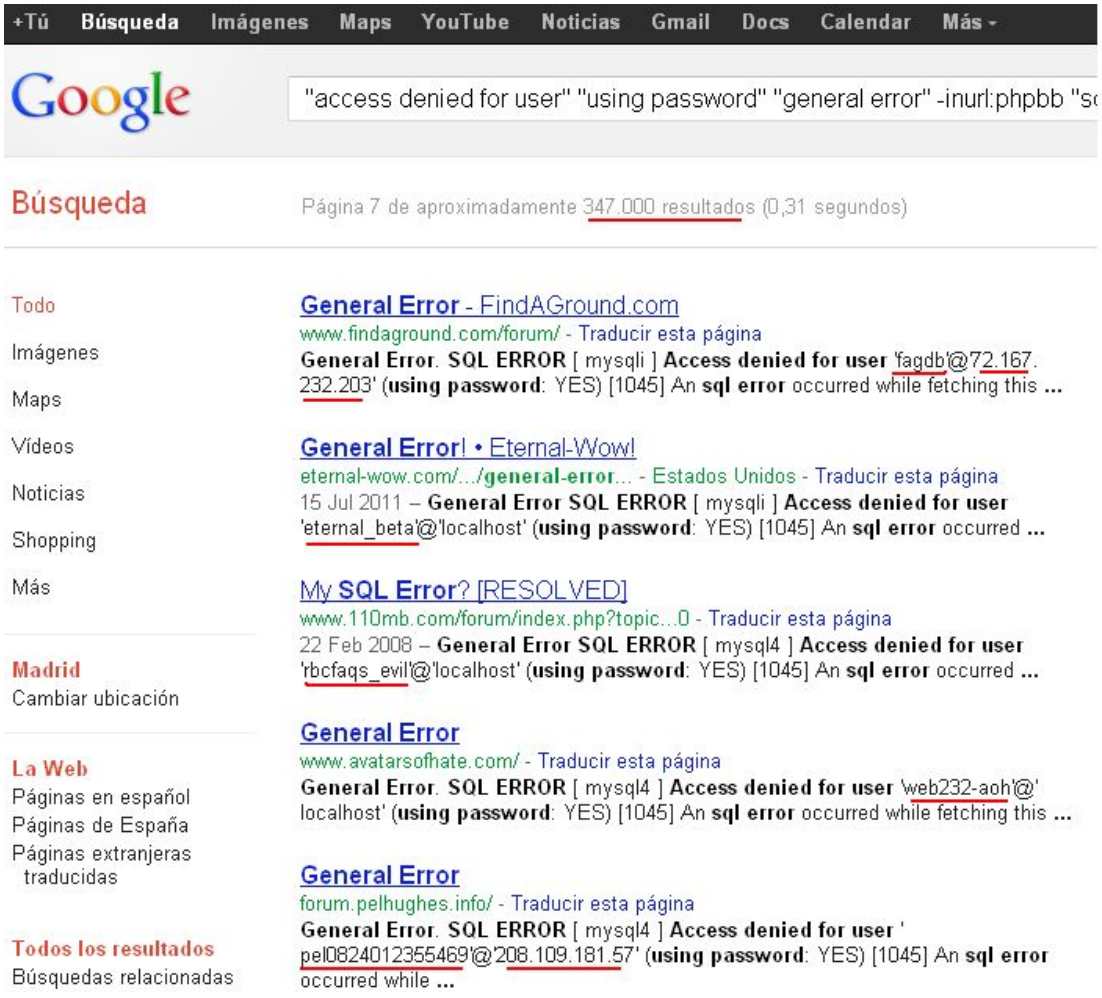
- **"You have requested access to a restricted area of our website. Please authenticate yourself to continue."** Puerta de entrada a la administración de la web. Casi 7.000 webs salen en Google al hacer esta búsqueda.
- **inurl:":10000" webmin** Webmin es un programa que permite administrar vía web remotamente un servidor linux por el puerto 10000, esta búsqueda nos da más de 5.000 servidores que lo tienen activado. Al pinchar nos pide usuario y contraseña
- **"VNC Desktop" inurl":5800"** VNC es un programa, que permite administrar remotamente la web y corre en el puerto 5800 por defecto. Similar al anterior.
- **intitle:"vnc viewer for java"** otra forma de acceder a gente que tiene instalado VNC. Google muestra 4.000 ordenadores listos para administrar remotamente.
- **inurl:/admin/login.asp** Da al hacker 8 millones de páginas diferentes donde hacer login

- **allintitle:Outlook Web Access Logon Login**, que permite al hacker ver los correos de una empresa
- **“best idea is to create the super user” “now by clicking here”** Instalación de php nuke a medias, que nos pide clave de administrador y lleva a formulario de acceso. Más de 100.000 están disponibles en Google.

Y el hacker puedes obtener millones de logins en sitios con WordPress yendo a la carpeta /wp-admin o en Joomla yendo a la carpeta /administrator, que son las carpetas que viene por defecto y casi nadie cambia

3) Ficheros con nombres de usuario o mensajes de error que revelan el nombre de usuario: esto se lo pone más sencillo al hacker para atacar con diccionarios o con Brutus, ya sólo tiene que sacar la contraseña para entrar, porque saben el usuario. Ejemplos:

“access denied for user” “using password” “general error” -inurl:phpbb “sql error” Foros phpbb que dan errores. Nos dan el nombre del usuario y a veces también la IP del servidor. En Google aparecen más de 340.000 foros vulnerables.



4) Detección de la versión servidor de la web o versiones productos vulnerables: si el servidor web, o alguno de los programas instalados en el mismo, no son la última versión, casi siempre tienen agujeros de seguridad. Las versiones habitualmente salen para actualizar agujeros de seguridad. Basta buscar en Google el exploit, para poder entrar en el servidor. Un exploit es un “programa” o una manera de explotar la vulnerabilidad: hay millones en internet. El hacker encontrará los exploits buscando en

Google, en Exploit Database o dejando que MetaSploit Framework los descubra y ejecute directamente. Ejemplos:

- **“SquirrelMail version 1.4.4” inurl:src ext:php** Una versión muy mala y fácilmente hackeable del gestor de correo. En Goolge aparecen 1940 empresas con ese gestor de correo, es como si dicen: “hackeame, mira mis correos”
- **“Powered by MercuryBoard [v1”** Versión antigua y con agujeros de seguridad de este software para envío de boletines. 188.000 resultados nos da Google.
- **intitle:”Welcome to Windows Small Business Server 2003″** Google muestra 17.000 servidores con esta versión anticuada de Windows Server, el hacker no sabe por cuál empezar…
- **intitle:index.of “Apache/*” “server at”** Da más de 500 millones de resultados en Google. Busca servidores Apache. Poniendo en lugar del * una versión con vulnerabilidades, el hacker sabe en qué servidores puede entrar.
- **intitle:index.of “Microsoft-IIS/* server at”** Igual que el anterior, aunque este muestra “sólo” 600.000 servidores, con sus versiones correspondientes.

5) Dispositivos hardware online (ver webcams y cámaras de vigilancia o manejar impresoras remotamente). Con ellos puedes espiar remotamente, dar sustos imprimiendo archivos en impresoras ajenas, ver qué se imprime en una empresa, manejar los sistemas de calefacción remotamente a tu antojo, etc. Ejemplos:

- **Camera linksys inurl:main.cgi** 700 cámaras disponibles para que un hacker nos vea. No hace falta contraseña, para entrar
- **inurl:”ViewerFrame?Mode=”** 83.000 cámaras disponibles para espiar sin necesidad de contraseña
- **“active webcam page” inurl:8080** Más cámaras disponibles en el puerto 8080
- **intitle:”toshiba network camera – User Login”** 15.000 cámaras más
- **intitle:”ivista main page”** más cámaras
- **intitle:”i-catcher console” “please visit”** y más todavía
- **inurl:webarch/mainframe.cgi** Impresoras listas para administrar remotamente
- **intitle:”network print server” filetype:shtm** y más impresoras esperando a hackers

6) Ficheros con información sensible o directorios sensibles de un servidor. Ejemplos:

- **“phone * * *” “address *” “e-mail” intitle:”curriculum vitae”** Obtenemos teléfono, nombre, mail y dirección postal de más de 573.000 personas. También se podría hacer el equivalente en español.
- **filetype:ctt** Archivos con listas de e-mails. Más de 4.000 archivos disponibles en Google.
- **“robots.txt” “disallow:” filetype:txt** En el archivo robots.txt el webmaster dice qué partes de su web no quiere que Google muestre, es decir, la información más confidencial de la web, que es lo 1º que quiere mirar un hacker. Haciendo la búsqueda anterior, Google muestra más de 2 millones de webs con archivos robots.txt, que indican al hacker su información más delicada.
- **allintitle:restricted filetype:doc site:gov** Encontrar información “interesante” en sitios de Gobiernos. Se puede cambiar “restricted” por “top secret” o “confidential”. Y “doc” por “pdf” o “txt”. O “gov” por “mil”, para sitios del ejército…

- **passwords|contraseñas|login|contraseña filetype:txt site:"web".com** Busca contraseñas y logins en documentos txt de la web web.com. Se puede ir cambiando el filetype o la web, para tener resultados diferentes.
- **inurl:intranet filetype:doc** confidential Igual que los 2 anteriores, admite variaciones
- **"Index of" / "chat/logs"** Logs de chats almacenados en servidores
- **index.of.dcim** 300.000 páginas con carpetas con fotos para descargar gratis. DCIM significa Digital Camera Image Dumps, y es el nombre que viene por defecto en las carpetas de fotos de las cámaras digitales. Esta búsqueda muestra personas que han subido las carpetas de fotos a una web tal cual, sin cambiar siquiera el nombre.
- **intitle:index.of "parent directory"** Listado de directorios de un servidor, para ver las carpetas y explorarlas. Son los más clásicos. Otros con funciones similares son:
- **intitle:"index of" "Index of /"**
- **intitle:"index of" inurl:"admin"**
- **intitle:index.of passwd** Permite navegar por el servidor y encontrar archivos de contraseñas. Con frecuencia no funciona, porque la gente ha hecho webs con virus para salir arriba en esa búsqueda y que los "lammers" piquen y pinchen los links, por eso no lo pongo en el apartado 1 de esta recopilación…

7) Información de apoyo al acceso. Ejemplos:

- **"Microsoft (R) Windows * (TM) Version * DrWtsn32 Copyright (C)" ext:log** Procesos ejecutándose en el servidor, para saber qué antivirus tiene, si tiene firewall…
- i**nurl:":8080" -intext:8080** Servidores que ejecutan servicios en el puerto 8080. A veces sólo con pinchar la url se entra directamente, a veces pide login, a veces es información "confidencial", o a veces son webs normales. Hay más de 1 millón de resultados en Google.
- **intitle:index.of ws_ftp.log** Logs de acceso por FTP, que incluyen las rutas locales de los archivos que se suben y horas de subida. Más de 1 millón de logs disponibles en Google.
- **site:sitio.com -site:"www.sitio.com"** Sirve para conocer subdominios, intranets, dominios para la gestión del correo, etc. Suele producir varias ventanas de login.
- **intitle:"the page cannot be found" "please * * following" "Internet * Services"** Permite saber el tipo de servidor.

Esto era sólo un resumen, sin ánimo de ser exhaustivo. Hay bases de datos de Google dorks, que así se llaman estos "fallos" de Google en: Exploit Database Google Dorks y Google Hacking Database. Hay Google Dorks para cada plugin o módulo de WordPress o Joomla que tienen vulnerabilidades. Los Google Dorks permiten encontrarlos y hackear las webs con plugins no actualizados.

Por último, hay programas que permiten probar automáticamente todas las vulnerabilidades de un sitio web que muestra Google, para no tener que ir buscando una a una. Algunos de los programas que hacen esto son:

- Site Digger: recomendado, es el que yo uso más a menudo para pruebas de seguridad de mis clientes
- Wikto
- SearchDiggit
- Athena (de snakeoillabs.com): no recomendable porque viola política de Google, porque no usa Google Api para las peticiones
- Gooscan: no recomendable por lo mismo que el anterior

Gonzalez, A. (2021, 14 enero). *Google Hacking & Dorks (46 ejemplos): cómo conseguir un hacker contraseñas usando sólo Google. Google puede ser tu peor enemigo.* | *14 de enero de 2021 Limpiar Reputación Online y SEO Google*. Limpiar Reputación Online y SEO Google | Me llamo Antonio González, tengo 15 años de experiencia como consultor SEO: posicionamiento web primero en Google, y «limpiar» tu reputación en Google. Dirijo el Ranking de Reputación Online y la agencia Trei.es, agencia SEO en Madrid, con clientes en toda España y resto del mundo. Clientes: CNN, Google, Telefónica, Movistar, ABC, EuropaPress, Banco ING, Banco Popular, Terra, Comunidad de Madrid, 6 Universidades, 4 clínicas estéticas... CONTACTO: antonio@trei.es.
https://antoniogonzalezm.es/google-hacking-46-ejemplos-hacker-contrasenas-usando-google-enemigo-peor/