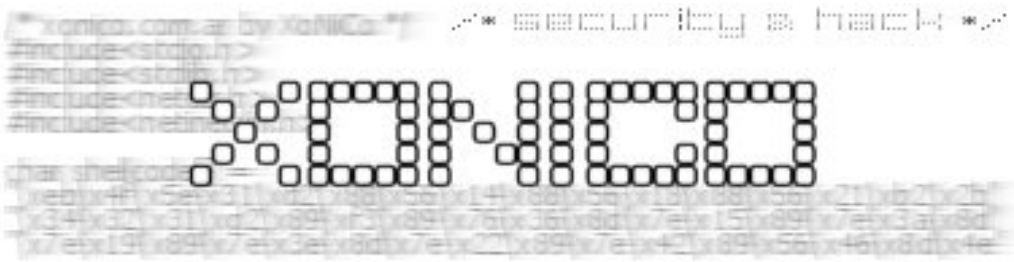
Hackeando con Google

17/09/2003



http://www.xonico.com.ar
xonico@gmail.com
by xonico

Google.com es el motor de búsqueda más popular del mundo y para muchos el mejor, posee una gran variedad de comandos que hacen de nuestra busque más fácil y eficaz, mas que un buscador es un amigo, con el podremos encontrar todo el material necesario para aprender sobre cualquier tema que nos sea de interés. En este articulo debido a la amplitud del tema solo me basare en la utilización de google como una herramienta para localizar contraseñas, base de datos, archivos privados, vulnerabilidades, y algunas cosas de interes general. El objetivo de este articulo es familiarizarse con los procedimientos de búsqueda y adoptar una estrategia de búsqueda.

Antes de empezar, google no diferencia minúsculas de mayúsculas y acentos, para él buscador es lo mismo que pongas exploit que Exploit o que pongos programación o programacion, a continuación voy a explicar los diferentes operadores de google.

- Puedes buscar una frase exacta usando las comillas “palabra1 palabra2...“ ejemplo:
  “programacion en c”

- Si tu lo que quieres es encontrar una palabra u otra podrías utilizar el operador OR, o con el simbolo |, puedes hacer mas efectiva tu búsqueda agregando paréntesis para agrupar palabras... ejemplo:
  programacion (manual OR tutorial)
  programacion (manual | tutorial)

- Otro es el operador + que nos incluye palabras que google no las toma por defecto como (de, la, las, los, etc.), también se escribe para indicar que esa palabra es necesaria en la búsqueda... ejemplo:
  +la programacion
  programacion delphi +fuentes

- Puedes excluir palabras en la búsqueda con el símbolo – (menos) ejemplo:
  programacion -pascal

- Existe también el asterisco * para reemplazar por palabras ejemplo:
  *“programacion en *”*

Ahora que ya sabemos los operadores básicos comenzaremos con algo mas divertido. Si tu sitio contiene información confidencial o no esta bien configurado, con solo entrar a google estarías vulnerable a cualquier persona. Pareciera que no es cierto pero es asi... Entonces prueba lo siguiente. Frontpage permite añadir formularios para capturar el feedback de los visitantes, en los cuales podrían añadirse campos como: nombre, dirección, número de teléfono y otros datos importantes. De forma predeterminada, esto se almacena en _private\form_results.txt La carpeta _private debería tener permisos que limiten su acceso, pero a veces la gente se olvida de ellos. Para comprobar hasta qué punto puedes llegar utilizando google prueba con:
allinurl:"form_results.txt"

Allinurl: busca páginas que tengan el término en alguna parte del URL (la dirección web).
Inurl: es lo mismo pero se puede combinar algunos operadores.

allinurl:passwd.txt

Esto nos mostraría las paginas que contengan en su url passwd.txt, usando un poco la imaginación este comando nos seria de gran utilidad. Por ejemplo si conocemos una falla de php-nuke de sql injection en las contraseñas del admin, y si sabemos que la falla se encuentra en los archivos admin.php podremos buscar *allinurl:admin.php*

Podemos restringir mas la búsqueda con el comando **Site**:

allinurl:admin.php site:.edu

Restringe buscando solo en los sitios .edu

Filetype: busca archivos .pdf, .ps, .doc, .xls, .txt, .ppt, .rtf, .asp, .wpd...

filetype:xls password site:.mil

Buscaría archivos con extensión exel en los sitios militares, que contengan la palabra password

Otra manera para encontrar archivo es usando las comillas “archivo.ext” ejemplo:
“config.inc.php” OR “mysql.cfg”

Index of: Uno de los tipos de búsqueda que nos permite hacer google es mostrar directorios poniendo en un índice, debido a la mala configuración del webmaster podemos encontrar cosas muy interesantes. Ejemplos:

"Index of /admin"
"Index of /root"
"Index of /password"
"Index of /" +passwd

Allintitle e **Intitle**: restringe la búsqueda únicamente al título de la página web (aquello que está entre las etiquetas).

allintitle: "index of/admin"
allintitle: restricted filetype:doc site:gov
intitle:"index of private"

Cache: con este comando podemos ver paginas o textos ya borrados, esto si googlebot (el robot de google) pasó por la web y la indexó antes de ser borrada la pagina.

cache:http://www.elhost.com/pass.txt

Los comandos **link, related, info**... tal vez no sean de utilidad como herramientas de hack pero seria bueno saber para que sirven.

link: para buscar webs que pongan un enlace a cierta web

related: páginas relacionadas o parecidas con la página de inicio de aquella web que usemos como referencia.

info: muestra la información que google tiene de nuestra página de inicio o principal.

Algunos ejemplos de búsqueda que podemos realizar con lo aprendido.

Algunas que otras contraseñas:
allinurl:auth_user_file.txt
intitle:"Index of" config.php
intitle:index.of.etc
filetype:xls username password email
intitle:"Index of" ".htpasswd" "htgroup" -intitle:"dist" -apache -htpasswd.c
intitle:"Index of" ".htpasswd" htpasswd.bak
inurl:config.php dbuname dbpass
intitle:"Index of" master.passwd
intitle:"Index of" .mysql_history
intitle:"index of" trillian.ini
intitle:"Index of" spwd.db passwd -pam.conf
intitle:"Index of" pwd.db
intitle:"Index of" secring.bak
intitle:"Index of" "people.lst"
intitle:"Index of..etc" passwd
intitle:"Index of" passwd passwd.bak
intitle:index.of passlist

Buscando usuarios:
intitle:"Index of" .bash_history
intitle:"Index of" .sh_history

Ninguna contraseña ni usuarios pero unas que otras cosas interesantes:
site:edu grades admin
filetype:htaccess basic
intitle:"Index of" finances.xls
"This report was generated by WebLog"
"phpinfo.php" –manual
intitle:Index.of robots.txt

Mensajes de error que dicen mucho:
"Chatologica MetaSearch" "stack tracking:"
"Error Diagnostic Information" intitle:"Error Occurred While"
"supplied argument is not a valid MySQL result resource"

Existen muchisimos archivos vulnerables que google puede encontrar:
intitle:"Index of" _vti_inf.html
intitle:"Index of" service.pwd
intitle:"Index of" shtml.dll
intitle:"Index of" shtml.exe
intitle:"Index of" fpcount.exe
intitle:"Index of" default.asp
intitle:"Index of" htimage.exe
intitle:"Index of" default.asp
intitle:"Index of" AT-admin.cgi
intitle:"Index of" glimpse

intitle:"Index of" guestbook.cgi
intitle:"Index of" perl
intitle:"Index of" show
intitle:"Index of" index.html~
intitle:"Index of" stats.html
inurl:shop "Hassan Consulting's Shopping Cart Version 1.18"

Encontrando algunes servidores con determinados servicios y sistemas operativos
intitle:"Welcome to Windows 2000 Internet Services"
intitle:"Welcome to IIS 4.0"
"powered by openbsd" +"powered by apache"
"Powered by phpBB 2.0.0"

Otros google's, algunos útiles otros no, que si utilizan un poco la imaginación les podrían ser útiles.

http://images.google.com/
Buscador de imágenes.

http://groups.google.com/
Buscador dentro de los grupos de 'news' (newsgroups). Contiene el archivo de DejaNews, adquirida por Google.

http://directory.google.com/
Utiliza la tenología de Google para buscar dentro de las categorías del OpenDirectory - DMOZ- (www.dmoz.org)

http://news.google.com/
Buscador de noticias, en más de 4.000 medios de comunicación de Internet.

http://froogle.google.com/froogle
Es un buscador de información de productos online. Google no es el que vende, simplemente se aprovecha de su motor de búsqueda para reconocer los sitios web que ofrecen productos online y crear una base de datos con sus datos y sus URLs.

http://catalogs.google.com/
Buscador de productos, dentro de los catálogos de venta por correo de cientos de empresas.

http://labs.google.com/
Servidor de pruebas de Google, donde se pueden hacer búsquedas de significado de palabras, conjuntos de términos, búsqueda por voz, y búsqueda avanzada por el teclado.

http://answers.google.com/
Cientos de usuarios realizan sus preguntas, y ofrecen recompensa por las respuestas.

http://toolbar.google.com/
Integración de una barra de búsqueda de Google dentro del navegador web. Solamente disponible para MS IExplorer sobre MS Windows. Otros navegadores web incluyen una

herramienta similar. Por ejemplo, para Mozilla se ha desarrollado http://googlebar.mozdev.org/

http://www.google.com/unclesam
Busca en los servidores cuyos dominios son .gov, .mil ó .us

http://www.google.com/linux
Busca términos relacionados con el Sistema Operativo Linux.

http://www.google.com/bsd
Busca términos relacionados con los Sistema Operativo BSD*.

http://www.google.com/mac
Busca dentro de todo lo relacionado con Apple y Macintosh.

http://www.google.com/microsoft
Busca términos relacionados con la compañía Microsoft.

http://www.google.com/options/universities.html
Las Universidades de todo el mundo pueden añadir su propio Google.

http://www.google.com/wml
Versión WAP de Google.

http://translate.google.com/translate_t
Traduce páginas webs entre varios idiomas (inglés, español, alemán, francés, ...).

http://www.googlestore.com/
Camisetas, bolígrafos, gorras, ... Todo relacionado con Google.

Conclusión
Espero que de ahora en adelante no dependas de nadie para encontrar algo que te interese y comiences a divertirte con google.

Referencias:
http://google.dirson.com
http://www.vnunet.com/News/1127162
http://johnny.ihackstuff.com/
http://www.oreilly.com/catalog/googlehks/