



Le piratage via Google

« Google Hacking »

Mai 2005

Profil



- Président et co-propriétaire de GoSecure Inc., fondée en Mai 2002
- Possède plus de 10 années d'expérience dans le domaine de la sécurité de l'information
- Grande expertise de consultation auprès d'organisations oeuvrant dans différents secteurs d'activités tels que:
 - Gouvernements
 - Banques
 - Entreprises (petite, moyenne et de grande envergure)
 - Police et sécurité publique

Agenda



Aperçu

- Technique de recherche - Google
- Opérateurs de base - Google
- Opérateurs avancés - Google
- Le piratage via Google :
 - Explorer à la recherche de “vulnérabilités en or”
 - Identifier les systèmes d’exploitation
 - Effectuer des balayages de vulnérabilités
 - « Proxying »
- Protéger vos informations contre Google

Technique de recherche - Google

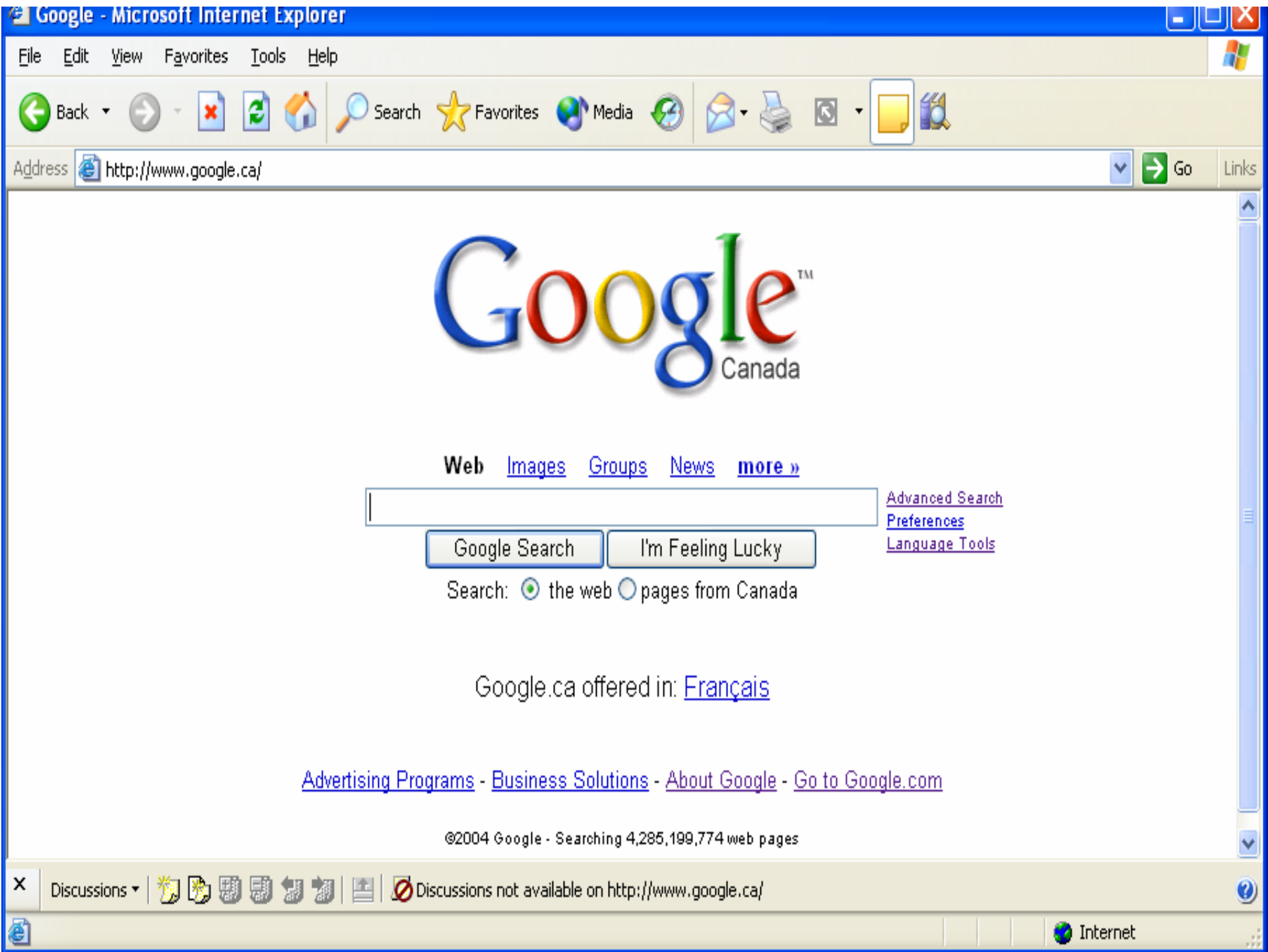
- Technique de recherche :
 - Seulement inscrire un mot et effectuer une recherche
- Vous devez vérifier votre présence Internet :
 - Google est une base de données qui possède presque tout !
- Une des plus puissantes bases de données au monde
- Consolide beaucoup de renseignements
- Google est utilisé par :
 - Les étudiants ...
 - Les entreprises ...
 - Al'Qaeda ...
 - Google est un magasin général idéal pour préparer une attaque et trouver des informations telles que des cartes géographiques, plans, adresses, photos et informations techniques MAPS.GOOGLE.COM
 - Exemple : On peut coordonner une attaque dans un pays étranger à partir de cartes satellites, plans des réseaux de transports publics, horaires, caméras de surveillance des réseaux routiers. De plus, on peut trouver les plans et guides d'utilisation d'explosifs et des détonateurs de classe civil et militaire.

Technique de recherche - Google

- Que peut faire Google pour un pirate ? :
 - Rechercher des informations sensibles comme le livre de paie, le # NAS et même la boîte de courriel personnelle
 - Effectuer des balayages de vulnérabilités
 - Proxy transparent

Technique de recherche - Google

- Google, ami ou ennemi ? :
 - Google est le meilleur ami de chacun (le vôtre et celui des pirates)
 - La cueillette d'information et l'identification des vulnérabilités sont les premières étapes d'un scénario typique de piratage
 - Passif, furtif et contient une immense collection de données
 - Google est beaucoup plus qu'un moteur de recherche
 - Avez-vous utilisé Google pour vérifier votre organisation aujourd'hui ?



Technique de recherche - Google

- Recherche avancée Google :
 - Un peu plus sophistiqué



Advanced Search

[Advanced Search Tips](#) | [About Google](#)

Find results

with **all** of the words 10 results

with the **exact phrase**

with **at least one** of the words

without the words

Language Return pages written in

File Format return results of the file format

Date Return web pages updated in the

Occurrences Return results where my terms occur

Domain return results from the site or domain

 e.g. google.com, .org [More info](#)

SafeSearch No filtering Filter using [SafeSearch](#)

Opérateurs de base - Google

- Opérateurs de Google :
 - Les opérateurs sont utilisés pour raffiner les résultats et maximiser la valeur d'une recherche. Ils sont vos outils de même que des armes pour les pirates
- Opérateurs de base :
+, -, ~ , .. , * , “” , |, OU
- Opérateurs avancés :
 - allintext:, allintitle:, allinurl:, bphonebook:, cache:, define:, filetype:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, rphonebook:, site:, numrange:, daterange

Opérateurs de base - Google

- Opérateurs de base - Google ? :
 - (+) inclusion forcée d'un mot commun
 - Google ignore par défaut les mots communs (exemple : où, comment, chiffre, lettre singulière, etc.) :
 - Exemple : StarStar Wars Episode +l
 - (-) exclut un terme de recherche
Exemple : apple –red
 - (“ ”) Utiliser les guillemets au début et à la fin d'une expression pour une recherche exacte :
Exemple : “Robert Masse”
 - Robert masse sans guillemets “ ” obtient 309,000 résultats, mais “robert masse” avec guillemets “ ” obtient seulement 927 résultats, Réduisant de 99% les résultats qui ne sont pas pertinents

Opérateurs de base - Google

- Opérateurs de base :
 - (~) recherche de synonyme :
Exemple: ~food
 - Affiche tous les résultats qui s'associent à la nourriture, aux recettes, à la nutrition et à toutes autres informations connexes à ce terme
 - (.) recherche toutes les possibilités avec un caractère simple « wildcard » :
Exemple: m.trix
 - Affiche tous les résultats de : M@trix, ma**tr**ix, me**tr**ix.....
 - (*) recherche toutes les possibilités avec n'importe quel mot « wildcard »

Opérateurs avancés - Google

- Opérateurs avancés : “site:”
 - Site: Domain_name
 - Permet de trouver seulement les pages Web du domaine spécifié. Si nous recherchons un site spécifique, nous obtenons habituellement la structure Web du domaine
 - Exemples :
 - site:ca
 - site:gosecure.ca
 - site:www.gosecure.ca

Google Search: site:gosecure.ca - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail Stop

Address <http://www.google.ca/search?hl=en&ie=UTF-8&q=site%3Agosecure.ca&meta=> Go Links

Google site:gosecure.ca Search Web PageRank 1 blocked Auto

Google Web Images Groups News more »

site:gosecure.ca Search [Advanced Search](#) [Preferences](#)

Search: the web pages from Canada

Web Results 1 - 10 of about 295 from **gosecure.ca** for . (0.36 seconds)

[usr/bin/perl ## Runs a number of concurrent nmap processes and ...](#)
#/usr/bin/perl ## Runs a number of concurrent nmap processes and stores the results in # a specified directory in xml, human and machine formats. ...
www.gosecure.ca/SecInfo/tools/multimap.pl - 10k - [Cached](#) - [Similar pages](#)

[GoSecure: Information Security Experts](#)
VULNERABILITIES & EXPLOIS DETAILS. Multiple Browsers Frame Injection Vulnerability. Source: <http://secunia.com/advisories/11978/> Date: 2004-07-21. Summary. ...
www.gosecure.ca/cgi-bin/detailvul_flash.cgi?id=244 - 17k - [Cached](#) - [Similar pages](#)

[GoSecure: Information Security Experts](#)
VULNERABILITIES & EXPLOIS DETAILS. SSH URI Handler Code Execution. Source: <http://www.securiteam.com/securitynews/archive.html> Date: 2004-06-22. Summary. ...
www.gosecure.ca/cgi-bin/detailvul_flash.cgi?id=221 - 18k - [Cached](#) - [Similar pages](#)

www.gosecure.ca/cgi-bin/detailvul_flash.cgi?id=209
[Similar pages](#)

Discussions Discussions not available on <http://www.google.ca/>

Internet

Opérateurs avancés - Google

- Opérateurs avancés : “filetype:”
 - Filetype : extension_type
 - Permet de trouver les documents contenant des extensions spécifiques
 - Les extensions supportées sont :
 - HyperText Markup Language (html)
 - Adobe Portable Document Format (pdf)
 - Adobe PostScript (ps)
 - Lotus 1-2-3
(wk1, wk2, wk3, wk4, wk5, wki, wks, wku)
 - Lotus WordPro (lwp)
 - MacWrite (mw)
 - Text (ans, txt)
 - Microsoft PowerPoint (ppt)
 - Microsoft Word (doc)
 - Microsoft Works (wks, wps, wdb)
 - Microsoft Excel (xls)
 - Microsoft Write (wri)
 - Rich Text Format (rtf)
 - Shockwave Flash (swf)
 - Note: Nous pouvons aussi rechercher des fichiers asp, php et cgi, à condition que le texte soit compatible
Exemple: Budget filetype: xls

Opérateurs avancés - Google

- Opérateurs avancés
 - Un fichier de budget que nous avons trouvé.....

Microsoft Internet Explorer

File Edit View Insert Format Tools Data Go To Favorites Help

Back Forward Stop Refresh Home Search Favorites Media

Address Go Links

Google budget filetype:xls Search Web PageRank 1 blocked AutoFill Options

B4 317.1

	A	B	C	D	E	F	G	H	I
1	Table 8.8—OUTLAYS FOR DISCRETIONARY PROGRAMS IN CONSTANT (FY 2000) DOLLARS: 1962–2009								
2	(in billions of dollars)								
3	Category and Program	1962	1963	1964	1965	1966	1967	1968	1969
5	Nondefense:								
6	International affairs	33.1	29.9	25.1	24.7	25.9	26.7	23.6	18.5
7	General science, space and technology:								
8	General science and basic research	3.0	3.0	4.2	4.1	4.4	4.5	4.5	4.2
9	Space and other technology	7.4	14.3	22.5	26.4	29.9	26.7	22.3	18.5
10	Total General science, space and technology	10.3	17.4	26.7	30.6	34.3	31.1	26.8	22.7
11	Energy	3.9	3.7	3.7	4.4	3.8	4.2	5.0	4.6
12	Natural resources and environment	13.7	14.4	14.5	14.9	16.0	16.4	16.5	15.4
13	Agriculture	2.2	2.6	2.7	2.8	3.1	3.4	3.8	3.5
14	Commerce and housing credit	8.1	7.8	6.4	8.6	9.5	11.2	10.2	4.7
15	Transportation:								
16	Ground transportation	0.4	0.4	0.4	0.4	0.5	0.6	0.8	1.4
17	Air transportation	4.4	4.4	4.4	4.6	4.6	4.9	5.0	5.4
18	Water and other transportation	3.7	3.6	3.4	3.7	3.4	3.7	4.0	3.8
19	Total Transportation	8.6	8.4	8.1	8.6	8.5	9.3	9.8	10.6
20	Community and regional development	2.6	3.0	5.0	5.7	5.5	5.3	6.6	7.2
21	Education, training, employment and social services:								
22	Education	3.8	4.3	4.5	5.4	11.7	17.2	19.2	17.5
23	Training, employment and social services	1.7	1.9	2.3	4.2	9.2	12.3	14.6	14.2
24	Total Education, training, employment and social services	5.6	6.2	6.8	9.6	20.9	29.5	33.8	31.7

Table 1.1













Discussions not available on

Done Unknown Zone

Opérateurs avancés - Google

- Opérateurs avancés : “intitle:”
 - Intitle: search_term
 - Permet de trouver le terme de recherche à l’intérieur du titre d'une page Web
 - Allintitle: search_term1 search_term2 search_term3
 - Permet de trouver de multiples termes de recherche qui inclut tous ces mots à l’intérieur du titre d’une page Web
 - Ces opérateurs sont particulièrement utiles pour trouver des listes de répertoire
 - Exemple :
Find directory list:
Intitle: Index.of “parent directory”

Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	29-Jul-2004 16:36	-	
 Actions/	12-Dec-2003 14:44	-	
 Animation/	07-Aug-2004 12:18	-	
 Balls/	12-Dec-2003 14:44	-	
 Box/	12-Dec-2003 14:44	-	
 ButSmall/	12-Dec-2003 14:44	-	
 Buttons/	12-Dec-2003 14:44	-	
 Diamonds/	12-Dec-2003 14:44	-	
 FancyLines/	12-Dec-2003 14:44	-	
 Icons/	12-Dec-2003 14:44	-	
 Images.html	12-Dec-2003 14:30	10k	
 Images.m4	16-Apr-2002 20:25	14k	

Opérateurs avancés - Google

- Opérateurs avancés : “inurl:”
 - Inurl: search_term
 - Permet de trouver le terme de recherche dans l’adresse Web d’un document
 - Allinurl: search_term1 search_term2 search_term3
 - Permet de trouver de multiples termes de recherche dans l’adresse Web d’un document
 - Exemples :
 - Inurl: cgi-bin
 - Allinurl: cgi-bin password


[Web](#) [Images](#) [Groups](#) [News](#) [more »](#)

[Advanced Search](#)
[Preferences](#)

Search: the web pages from Canada

Web Results 1 - 10 of about 44,400 for allinurl:cgi-bin password. (0.68 seconds)

[Index of /dda/cgi-bin/password](#)

Index of /dda/cgi-bin/password. Name Last modified
Size Description Parent directory Empty directory

[www.cib.nig.ac.jp/dda/cgi-bin/password](#) - 1k - [Cached](#) - [Similar pages](#)

[Password protector dirs free web hosting cgi-bin at ncsn.org](#)

More search results. Password protector dirs free web hosting cgi-bin info. ... Lot of information about dirs hosting protector password cgi-bin web free. ...

[www.ncsn.org/.../password-protector-dirs-free-web-hosting-cgi-bin.html](#) - 4k - [Cached](#) - [Similar pages](#)

Opérateurs avancés - Google

- Opérateurs avancés : “intext:”
 - Intext: search_term
 - Permet de trouver un terme de recherche dans le corps du texte d’un document
 - Allintext: search_term1 search_term2 search_term3
 - Permet de trouver de multiples termes de recherche dans le corps du texte d’un document
 - Exemples :
 - Intext: Administrator login
 - Allintext: Administrator login



Address Go Links >>

Google intext:Administrator Login Search Web 57 blocked AutoFill Options Administrator Login

Administrator login

Username

password

Opérateurs avancés - Google

- Opérateurs avancés : “cache”:
 - Cache: URL
 - Permet de trouver l’ancienne version dans la mémoire tampon de Google
 - Parfois, même après la mise à jour d’un site, l’ancienne information peut être trouvée dans la mémoire tampon
 - Exemple :
Cache: www.gosecure.com



Address <http://www.google.ca/search?sourceid=navclient&ie=UTF-8&q=cache%3Awww%2Egosecure%2Eca> Go Links

Google cache:www.gosecure.ca Search Web PageRank 1 blocked AutoFill Options

This is Google's cache of <http://www.gosecure.ca/> as retrieved on 31 Jul 2004 00:41:33 GMT. Google's cache is the snapshot that we took of the page as we crawled the web. The page may have changed since that time. Click here for the [current page](#) without highlighting. This cached page may reference images which are no longer available. Click here for the [cached text](#) only. To link to or bookmark this page, use the following url: <http://www.google.com/search?sourceid=navclient&ie=UTF-8&q=cache%3Awww.gosecure.ca>

Google is not affiliated with the authors of this page nor responsible for its content.



Security that drives business results.

> ENTER

La sécurité au service de vos objectifs d'affaires.

> ENTREZ

Opérateurs avancés - Google

- Opérateurs avancés :
 - <number1>..<number2>
 - Permet d'effectuer une recherche avec une série de numéro en spécifiant deux numéros, séparés par deux points, sans espaces. Assurez-vous de spécifier une unité de mesure ou tout autre indicateur de ce que la série de numéro représente
 - Exemples :
 - Computer \$500..1000
 - DVD player \$250..350

Eagle computer
SaveAtEagle.com

Same day shipping on most orders before 4pm CST
Call Toll-Free 800-845-6471

Free shipping on orders \$250 or more
click here for details >>

Search:

SHOW ORD INFO HOME TESTIMONI

Join our e-mail list

Sharednet's **LiveRep**

- Symantec
- Veritas
- Software
- Computers
- Laptops

Home > Laptops, Notebooks, PDA's, New, Factory Refurbished, Used / Refurbished, Dell Latitude, IBM Thinkpad, Compaq Presario / EVO, HP Pavilion / Omnibook, Gateway Solo, Toshiba Tecra / Satellite, Sony Vaio, Apple Powerbook, Averatec Sotec > \$800 to \$999

\$800 to \$999



Batteries running down?

Camcorders, Laptops, Cell Phones, Digital Cameras
Cordless Phones battery replacements at great prices!

YAHOO! SHOPPING TOP SERVICE (5 stars)

ScanAlert! HACKER SAFE
TESTED 10-AUG

Top Sellers

ICOPYDVDS2 Retail Box DVD Copying Software DVD copy, i copy dvds 21315340 like 321 studios xcopy	\$39.95
NEC ND-2510A DVD/RW Writer (8x/4x/12x DVD+RW, 8x/4x/12x DVD- RW, 32x/16x/40x CD-RW), NEW OEM	\$79.00

Opérateurs avancés - Google

- Opérateurs avancés : “daterange:”
 - Daterange: <start_date>-<end date>
 - Permet de trouver les pages Web pour une période comprise entre deux dates
 - Note: start_date & end date utilisez la date Julienne
 - La date Julienne est calculée à partir du nombre de jours depuis le 01 janvier 4713 ac. Par exemple la date Julienne pour le 01 Août 2201 est 2452122
- Exemples :
- 2004.07.10=2453196
- 2004.08.10=2453258
- Représente en date julienne: 2453196-2453258



Web Images Groups News more »

Vulnerabilities daterange:2453196-2453258

Search

Advanced Search Preferences

Search: the web pages from Canada

Web

Results 1 - 10 of about 880,000 for Vulnerabilities daterange:2453196-2453258. (0.50 seconds)

Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) is a list or dictionary that provides common names for publicly known information security vulnerabilities and ...

www.cve.mitre.org/ - 13k - 8 Aug 2004 - Cached - Similar pages

SANS Top 20 Vulnerabilities - The Experts Consensus

... Pentagon hacking incident and the easy and rapid spread of the Code Red and NIMDA worms can be traced to exploitation of unpatched vulnerabilities on this list ...

www.sans.org/top20/ - 101k - 8 Aug 2004 - Cached - Similar pages

{ PivX Solutions, LLC }

... It tries to exploit 7 different vulnerabilities to infect Windows machines, ranging from the Messenger Service buffer overrun, the uPnP overflow, LSASS as well ...

www.pivx.com/larholm/unpatched/ - 7k - 8 Aug 2004 - Cached - Similar pages

Sponsored Links

Vulnerability Database

Easy-to-use & validated info. Free and updated daily. www.secunia.com

DIGEV 2004

1st International Digital Evidence Web Conference. You're invited! www.digev2004.com

Network Security

Free info on network security, software, and enterprise solutions

Opérateurs avancés - Google

- Opérateurs avancés : “link:”
 - Link: URL
 - Permet de trouver des pages Web possédant un lien au URL spécifiée
 - Related: URL
 - Permet de trouver des pages Web similaires à la page Web spécifiée
 - info: URL
 - Présente certaine information que Google possède au sujet de cette page Web
 - Define: search_term
 - Permet de fournir une définition des mots recueillis à partir de diverses sources en ligne
 - Exemples :
 - Link: gosecure.ca
 - Related: gosecure.ca
 - Info: gosecure.ca
 - Define: Network security

Breaking News

Tech Home @Work Reviews @Play

globeandmail.com Business Insight Centre

Resources

Encyclopedia Tech Alert Tech Books Tech Events Troubleshooter Special Reports

EDC Protect your

TECHNOLOGY

POSTED AT 8:34 AM EDT

Monday, Feb 23, 2004

Tech Home | @Work | Reviews | @Play | Today's Paper | Investor

Information security is about people



By Robert Masse Special to Globe and Mail Update

Front Lines is a guest viewpoint section offering perspectives on current issues and events from people working on the front lines of Canada's technology industry. Robert Masse is the president of GoSecure Inc., a Montreal information security services firm, and a former security consultant for KPMG.

One morning I pulled on hat and sweater bearing the logo of a well-known telecom company, printed up a fake work order, and headed off to the offices of one of my clients.

E-mail this Article Print this Article

Tech Poll

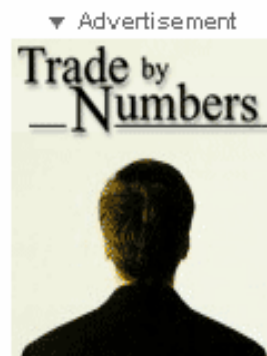
Should government fund programs to ensure small communities have broadband Internet access?

Yes No

Vote

Results & Past Polls

Sign up for Tech Alerts





Web Images Groups News more »

related:www.gosecure.ca/

Search

Advanced Search Preferences

Search: the web pages from Canada

Web

Results 1 - 10 of about 28 similar to www.gosecure.ca/. (0.34 seconds)

[GoSecure](#)

[www.gosecure.ca/](#) - 2k - [Cached](#) - [Similar pages](#)

[LQT Systems | Linux Québec Technologies](#)

[www.linuxquebec.com/](#) - 4k - [Cached](#) - [Similar pages](#)

[SourceForge.net: CVS Repository](#)

SourceForge.net Home, My Favorites. ...

[sourceforge.net/cvs/?group_id=60358](#) - 34k - [Cached](#) - [Similar pages](#)

[Chronoss-devel Info Page](#)

Chronoss-devel --. About Chronoss-devel. To see the collection of prior postings to the list, visit the Chronoss-devel Archives. Using Chronoss-devel. ...

[lists.sourceforge.net/lists/listinfo/chronoss-devel](#) - 5k - [Cached](#) - [Similar pages](#)

[Chronoss-user Info Page](#)

Chronoss-user --. About Chronoss-user. To see the collection of prior postings to the list visit the Chronoss-user Archives. Using Chronoss-user ...



Web [Images](#) [Groups](#) [News](#) [more »](#)

info:www.gosecure.ca

Search

[Advanced Search](#)
[Preferences](#)

Search: the web pages from Canada

Web

Showing web page information for www.gosecure.ca

[GoSecure](http://www.gosecure.ca)

Google can show you the following information for this URL:

- Show [Google's cache](#) of www.gosecure.ca
- Find web pages that are [similar to](#) www.gosecure.ca
- Find web pages that [link to](#) www.gosecure.ca
- Find web pages that [contain the term](#) "www.gosecure.ca"



Web Images Groups News more »

define:"network security"

Search

Advanced Search Preferences

Search: the web pages from Canada

Web

Tip: Try removing quotes from your search to get more results.

Definitions of **Network Security** on the Web:

Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects. Network security includes providing for data integrity.

www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html

Security procedures and controls that protect a network from: (a) unauthorized access, modification, and information disclosure; and (b) physical impairment or destruction.

www.ciao.gov/ciao_document_library/glossary/N.htm

Managing the physical and logical accessibility of your network resources. Physical includes safeguarding the actual equipment; logical includes controlling customers' access to network resources.

www.thinkhdi.com/publications/glossary.asp

Opérateurs avancés - Google

- Opérateurs avancés : “phonebook:”
 - Phonebook
 - Recherche au complet l’annuaire téléphonique de Google
 - rphonebook
 - Recherche seulement les listes résidentielles
 - bphonebook
 - Recherche seulement les listes d’entreprises
 - Exemples :
 - Phonebook: robert las vegas (robert à Las Vegas)
 - Phonebook: (702) 944-2001 (recherche inverse, peu ne pas fonctionner)
 - Cette fonction se limite au EU

Google Search: robert las vegas - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail Stop

Address <http://www.google.ca/search?hl=en&ie=UTF-8&pb=f&q=robert+las+vegas&pb=f> Go Links

Google robert las vegas Search Web PageRank 2 blocked AutoFill Options

Google PhoneBook Search PhoneBook Search the Web Preferences

Business Phonebook Results 1 - 5 of about 219 for robert las vegas. (0.31 seconds)

Century Vision Center, **Robert** Pearson Od - (702) 944-2001 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Eob, Head Start Centers, **Robert** Jones Gardens - (702) 438-3770 - 1750 Marion Dr, Las Vegas, NV 89115 - [Yahoo! Maps](#) - [MapQuest](#)

Clark County Of, Constable **Robert** Bobby G Gronauer - (702) 385-2436 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Clark County Of, Constable **Robert** Bobby G Gronauer, Las Vegas Township - (702) 455-4099 - 309 S 3rd St, Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

American Family Insurance, Career Opportunities, Harrison **Robert** - (702) 732-4708 - 3993 Howard Hughes Pkwy, Las Vegas, NV 89109 - [Yahoo! Maps](#) - [MapQuest](#)

[More business listings...](#) ([Removal Info](#))

Residential Phonebook Results 1 - 5 of about 7 for robert las vegas. (0.31 seconds)

I **Robert** - (702) 433-6314 - 3890 S Nellis Blvd, Las Vegas, NV 89121 - [Yahoo! Maps](#) - [MapQuest](#)

Enrique **Robert** - (702) 792-9312 - 2700 S Valley View Blvd, Las Vegas, NV 89102 - [Yahoo! Maps](#) - [MapQuest](#)

F S **Robert** - (702) 631-2034 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Howard **Robert** - (702) 260-6696 - Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Discussions Discussions not available on <http://www.google.ca/>

Done Internet



Web Images Groups News more »

(702) 944-2001

Search PhoneBook

Search the Web

Preferences

Business Phonebook

Results 1 - 8 of 8 for (702) 944-2001 . (0.03 seconds)

Century Vision Center, Robert Pearson Od - (702) 944-2001 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Century Vision Center, Ronald Dutton Od - (702) 944-2001 - , Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Century Vision Center - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Century Vision Center, Michael Crutchfield Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Cohen David B MD - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Crutchfield Michael Od - (702) 944-2001 - 8230 W Sahara Ave Infocus, Las Vegas, NV 89101 - [Yahoo! Maps](#) - [MapQuest](#)

Dutton Ronald Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Somers William Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - [Yahoo! Maps](#) - [MapQuest](#)

Le piratage via Google

A decorative header image showing red mechanical components, possibly a microscope or similar scientific instrument, with a dark background.

- Salaire :
 - Salary filetype: xls site: edu

1 Based on 7/1/02 Salary Schedule		SALARY INCREASE CALCULATOR			
2 Desired Salary Action	Enter Base Salary	Timebase or Adjustment	Adjusted Salary	Comments	
3 Full-Time to Part-time AY	\$6,000	1	\$3,600.00	Base Salary X Timebase	
4 Full-Time to Part-Time 12 month	\$6,900	1	\$4,140.00	Base Salary X Timebase	
5 AY to 12 Month (15% Increase)	\$6,000	+15.0%	\$6,900.00	Base Salary X 1.15	
6 12 Month to AY (Minus 15%)	\$6,900	-15.0%	\$6,000.00	Base Salary divided by 1.15	
7 Difference-in-Pay Leave (7/1/02)	\$6,000	-\$3035	\$2,965.00	Base Salary minus minimum of Rank 2	

Le piratage via Google

- Numéro d'assurance social :
 - Intitle: Payroll intext: ssn filetype: xls site: edu

5				Regular	Overtime		Federal	State	
6			Pay	Hours	Hours	Gross	Withhold	Withhold	
7	Name	SSN	Rate	Worked	Worked	Pay	Tax	Tax	F
8	-	-	-	-	-	-	-	-	-
9	Kristy Cole	874-72-1000	12.50	26.0	0.0	325.00			
10	Jose Herrera	831-32-6407	11.75	40.0	3.0	522.88			
11	Brooke Hoover	433-25-7700	14.20	22.0	0.0	312.40			

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Numéro d'assurance social :
 - Payroll intext: Employee intext: ssn iletype: xls

			Employee # 1	Time Card		Employee # 4	
			Pay Period Ending: July 27, 2000	Pay Period Ending: July 27, 2000			
			Social Security Number: 502-52-3612	Social Security Number: 502-52-3612			
			Marital Status: Single	Exemptions: 0	Marital Status: Single	Exemptions: 1	
			Deductions: Hospital: \$15.00 Other: \$25.00	Special Deductions:	Hospital: none	Other: \$10.00	

Le piratage via Google

- Information financière :
 - Filetype: xls “checking account” “credit card” - intext: Application -intext: Form only 39 results

4	1619	7/6/99	Mortgage payment	1350.00		11150.00
5	1620	7/6/99	car insur	1236.82		9913.18
6		7/10/99	OTC Deposits		345.00	10258.18
7	1621	7/13/99	Internet Connection	16.00		10242.18
8	1622	7/13/99	Pedernales electric	211.36		10030.82
9		7/13/99	OTC Deposits		985.56	11016.38
10	1623	7/14/99	SW Bell Tel	54.21		10962.17
11	1624	7/15/99	Flying trip to New Orleans 7 hrs @ \$45	315.00		10647.17

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Information financière :
 - Intitle: "Index of" finances.xls (9)

File Edit View Insert Format Tools Data Go To Favorites Help

Back Forward Stop Home Search Favorites Media

Address <http://www.personal.psu.edu/users/b/j/bjg181/Finances.xls> Go




















Google intitle:"Index of" finances.xls Search Web PageRank 16 blocked AutoFill Options Index of finances xls

	A	B	C	D	E	F	G	H	I
2	Date	Description	Amount	Type	Note		Item breakdown		
3							Grocery	\$0.00	
4		Summer 2004					Apartment	\$705.00	
5	5.27	Car service for flashing lights	\$69.50	Debit	Temporary Payment		Books	\$0.00	
6	5.27	Dad's repayment for car service		Check	Reimbursement		School	\$0.00	
7	5.30	Shampoo and fish tank tubing	\$4.60	Cash	Personal		Transportation	\$300.20	
8	5.31	First Pres offering through May	\$150.00	Check	Personal		Personal	\$236.80	
9	6.1	Gas for Rachel's car	\$25.00	Debit	Transportation		Dining	\$40.50	
10	6.5	Dinner at Brat Stop w/ Mom and Dad	\$27.00	Debit	Dining		Gifts	\$0.00	
11	6.7	Kitten supplies	\$35.20	Debit	Personal		Non-PSU	\$0.00	
12	6.8	Plane ticket to NYC	\$255.20	Debit	Transportation		Misc	\$7,244.00	
13	6.9	PSU account refund (general deposit)	-\$50.00	Deposit			Total	\$8,526.50	
14	6.10	Reservation deposit for Tuckaway Heights	\$100.00	Check	Apartment				
15	6.12	Metra ticket to Chicago	\$5.00	Cash	Transportation				
16	6.12	Food at Blues Fest	\$3.50	Cash	Dining				
17	6.12	Blues Fest keychain	\$3.00	Cash	Personal				
18	6.12	Dinner at Giordano's w/ Joy, Neighbor, Vince	\$10.00	Cash	Dining				
19	6.12	Gas for Rachel's car	\$15.00	Debit	Transportation				
20	6.13	Garage sale proceeds from Mom	-\$25.00	Cash	Gift				
21	6.15	Initial shots for Chat	\$99.00	Check	Cat				
22	6.15	Deposit for Tuckaway Heights (minus reserv. dep.)	\$605.00	Check	Apartment				
23	6.16	2-year Vine Line subscription renewal	\$44.00	Check	Personal				
24									
25		Check reimbursement is still a deposit							
26		withdrawal considered part of deposit when cash back is taken							
27									
28									
29		Separate PSFCU and 5/3 somehow!!!							
30									

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Boîte de courriel personnelle :
 - Intitle: Index.of inurl: Inbox (456) (mit mailbox)

Name	Last modified	Size	Description
 Parent Directory	17-Mar-2004 15:00	-	
 #1	17-Mar-2004 14:21	2k	
 #10	17-Mar-2004 14:45	2k	
 #11	17-Mar-2004 14:45	3k	
 #12	17-Mar-2004 14:45	3k	
 #13	17-Mar-2004 14:45	2k	
 #14	17-Mar-2004 14:34	10k	
 #15	17-Mar-2004 14:45	3k	
 #16	17-Mar-2004 14:34	51k	
 #17	17-Mar-2004 15:16	2k	
 #18	17-Mar-2004 15:16	2k	
 #19	17-Mar-2004 15:16	3k	
 #2	17-Mar-2004 14:21	2k	
 #20	17-Mar-2004 15:16	3k	
 #21	17-Mar-2004 15:16	2k	
 #22	17-Mar-2004 14:58	10k	
 #23	17-Mar-2004 15:16	3k	
 #24	17-Mar-2004 14:58	51k	
 #25	17-Mar-2004 15:26	2k	

Le piratage via Google

A decorative header image showing red mechanical components, possibly gears or parts of a machine, set against a dark background.

- Boîte de courriel personnelle :
 - Après plusieurs clics, nous avons obtenu les messages électroniques privés



Return-Path: <kspivey1p@x400gate.ada.at>
Delivered-To: mws+@ux1.sp.cs.cmu.edu
Received: from EDRC.CMU.EDU ([128.2.203.42]) by ux1.sp.cs.cmu.edu id aal8148;
17 Mar 2004 7:15 EST
Received: from MX5.andrew.cmu.edu ([128.2.10.115]) by edrc.cmu.edu id aa04183;
17 Mar 2004 7:14 EST
Received: from med.toho-u.ac.jp (c-67-166-49-63.client.comcast.net [67.166.49.63])
by mx5.andrew.cmu.edu (8.12.10/8.12.10) with SMTP id i2HCE0mN017771
for <mws@andrew.cmu.edu>; Wed, 17 Mar 2004 07:14:09 -0500
Message-ID: <97df01c40c9f\$735656f0\$a9bc03d3@med.toho-u.ac.jp>
From: "Kelvin Spivey" <kspivey1p@x400gate.ada.at>
To: mws@andrew.cmu.edu
Subject: More efficient than via-gra
Date: Wed, 17 Mar 2004 23:12:27 -0500
MIME-Version: 1.0
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
X-MIME-Autoconverted: from 8bit to quoted-printable by mx5.andrew.cmu.edu id i2HCE0mN017771
X-UIDL: becff044e73425d3d94cda6ea8b477f3

<HTML><BODY>
<P>Generic cialis (Regalis), at cheap prices.

Most places charge \$20, we charge \$5. Quite a difference.

Cialis is known as a Super-V=EDagra or Weekend-V=EDagra because its effec=
ts start sooner and last much longer.
</P><P>Shipped worldwide.

Your easy-to-use solution=
is here: http://www.mega-health.ne=
t/cia/?oxygen
</P><P>-----

The link below is for those who hate spam...

http://www.mega-health.net/o=
ff.html
=3D=3D-
</P></BODY></HTML>

Le piratage via Google



- Fichiers confidentiels :
 - “not for distribution” confidential (1,760)

Confidential - **Not for distribution**

1

Page 2

A ONCE Network Proposal to CN

Proposal: "Executive Summit Series" focused on the Business Implications of Web Services.

SUMMARY

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Fichiers confidentiels :
 - “not for distribution” confidential filetype: pdf (marketing info) (456)

An Introduction to AIMMS

Clearing the US Energy Market

part II/II

Gertjan de Lange
Chief Commercial Officer

Peter Nieuwesteeg
AIMMS Consultant at Areva

Le piratage via Google







- Détection du système d'exploitation
- Utilise le mot-clé par défaut de la page d'installation du serveur Web pour faire une recherche
- Utilise le titre pour faire une recherche
- Utilise le bas de page dans le répertoire de la page d'index

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, set against a dark background.

- Détection du système d'exploitation - Windows:
 - “Microsoft-IIS/5.0 server at”

Index of /legislacoes/parecer_jurid_arquivos

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	08-Mar-2004 16:37	-	
 filelist.xml	03-Oct-2002 10:10	1k	
 header.htm	03-Oct-2002 10:10	4k	
 image001.gif	03-Oct-2002 10:10	11k	

Microsoft-IIS/5.0 Server at [www.legis.gov.br](#) Port 80

Le piratage via Google



- Recherche de mots de passe :
 - Recherche des noms de fichier bien connus pour des mots de passe dans les URL
 - Recherche des fichiers de connexion de la base de données ou des fichiers de configuration pour trouver un mot de passe et un nom d'utilisateur
 - Recherche un fichier de nom d'utilisateur spécifique pour un produit spécifique

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Recherche de mots de passe :
 - Inurl: etc inurl: passwd

MiniUnix/etc/passwd

Find at most related files.
 including files from this version of Unix.

```
root::0:1::/:  
sys::2:1::/usr/sys:  
bin::3:1::/bin:  
c::10:1::/usr/c:  
man::3:1::/usr/man:  
adm::3:1::/usr/adm:  
s1::3:1::/src/source/s1:  
s2::3:1::/src/source/s2:  
s3::3:1::/src/source/s3:  
s4::3:1::/src/source/s4:  
s5::3:1::/src/source/s5:  
s6::3:1::/src/source/s6:  
s7::3:1::/src/source/s7:  
s8::3:1::/src/source/s8:
```



```
# $FreeBSD: src/etc/master.passwd,v 1.39 2004/08/01 21:33:47 markm Exp $
#
root::0:0::0:0:Charlie &:/root:/bin/csh
toor:*:0:0::0:0:Bourne-again Superuser:/root:
daemon:*:1:1::0:0:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5::0:0:System &:/usr/sbin/nologin
bin:*:3:7::0:0:Binaries Commands and Source:/usr/sbin/nologin
tty:*:4:65533::0:0:Tty Sandbox:/usr/sbin/nologin
kmem:*:5:65533::0:0:KMem Sandbox:/usr/sbin/nologin
games:*:7:13::0:0:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8::0:0:News Subsystem:/usr/sbin/nologin
man:*:9:9::0:0:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22::0:0:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25::0:0:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26::0:0:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53::0:0:Bind Sandbox:/usr/sbin/nologin
proxy:*:62:62::0:0:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflodg:*:64:64::0:0:pflodg privsep user:/var/empty:/usr/sbin/nologin
uucp:*:66:66::0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6::0:0:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80::0:0:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
nobody:*:65534:65534::0:0:Unprivileged user:/nonexistent:/usr/sbin/nologin
```

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Recherche de mots de passe :
 - Intitle: "Index of..etc" passwd

Index of /etc - Microsoft Internet Explorer






File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address <http://ftp.cs.concordia.ca/etc/> Go Links

Google intitle:"Index of..etc" passwd Search Web PageRank 15 blocked AutoFill Option: >>

Index of /etc

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	01-Nov-2002 15:40	-	
 group	31-Oct-2002 16:48	1k	
 localtime	30-Oct-2002 15:26	1k	
 nsswitch.conf	31-Oct-2002 16:52	2k	
 passwd	31-Oct-2002 16:49	1k	

Apache/1.3.24 Server at ftp.cs.concordia.ca Port 80

Discussions Discussions not available on <http://ftp.cs.concordia.ca/>

Internet

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Recherche de mots de passe :
 - Inurl: admin.pwd filetype: pwd



```
mdneauto:DglNlhTHy9Sis:2025:100:Michael Floodman:/home/mdneauto:/bin/false
```

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar device, with a dark background.

- Recherche de mots de passe ::
 - Filetype: inc dbconn



```
var $ERR_DESC; //Oracle Error Desc.
var $str;

function my_conn() { //Create database connection using bg-id
    $this->i = 0;
    $this->c = @OCIplogon ("poweroftwo", "fourby16", "prod") or die ("Could not connect");
}

function my_err() {
    $err = OCIError($this->sqlstmt);
    $this->ERR = $err["code"];
    $this->ERR_DESC = $err["message"];
}
```



Web Images Groups News Froogle more »

filetype:log inurl:"password.log"

Search

Advanced Search Preferences

Web

Results 1 - 10 of about 23 for filetype:log inurl:"password.log". (0.21 seconds)

[name: = "jbhunt"; password: = "jbhunt"; URL: = "http://home.nc.rr. ...](#)

name: = "jbhunt"; password: = "jbhunt"; URL: = "http://home.nc.rr.com/clay123/ref23.html";

Beth Haas name: = "BHaas"; password: = "Beth Haas"; URL: = "http ...

[home.nc.rr.com/clay123/password.log - 2k - Supplemental Result - Cached - Similar pages](#)

[name: = "tad"; password: = "homepage"; URL: = "<a href="http://www ...](#)

name: = "tad"; password: = "homepage"; URL: = "http://www.dob.com.tw";

END_FILE

[dob.tnc.edu.tw/authorHD/1/password.log - 1k - Cached - Similar pages](#)

[name: = "momo"; password: = "momo"; URL: = "password.htm" ...](#)

name: = "momo"; password: = "momo"; URL: = "password.htm"; END_FILE

[jason123.uhome.net/password.log - 1k - Supplemental Result - Cached - Similar pages](#)

[name: = "23202"; password: = "ilgf"; URL: = "address.htm"; name ...](#)

name: = "23202"; password: = "ilgf"; URL: = "address.htm"; name: = "23203"; password:

= "ilgf"; URL: = "address.htm"; name: = "23204"; password: = "ilgf"; URL ...

[www.lib.nchu.edu.tw/groups/group21/password.log - 9k - Cached - Similar pages](#)

[name: = "admin"; password: = "computer"; URL: = "http://members. ...](#)

name: = "admin"; password: = "computer"; URL: = "http://members.tripod.de/Rick_Cooper/fr.htm";

name: = "paul"; password: = "papst"; URL: = "http://members ...

[mitglied.lycos.de/Rick_Cooper/mbr/password.log - 2k - Supplemental Result - Cached - Similar pages](#)

[cc.nyu.edu/tul...00/2/password.log](#)

Le piratage via Google

- Syntaxe des témoins « cookies »:
 - Filetype: inc inc intext: setcookie -cvs -examples -sourceforge -site: php.net (120) (cookie schema)



Address Go Links

Google Search Web PageRank 16 blocked AutoFill Options

```
<?
//Cookie for name, web and email in news-tnk v1.2.2 tnka@linux-sottises.net
if($param_name && $save!="1"){
$name=$param_name;
$email=$param_email;
$web=$param_web;
}elseif($save=="1"){
setcookie("param_name", "", time()-100000);
setcookie("param_email", "", time()-100000);
setcookie("param_web", "", time()-100000);
setcookie("param_name", $name, time()+315360000);
setcookie("param_email", $email, time()+315360000);
setcookie("param_web", $web, time()+315360000);
}
```

Le piratage via Google







- Listes de répertoires sensibles :
 - Mots clés qui représentent des atouts critiques : Index of
 - Recherche des noms de répertoires de vulnérabilités bien connus

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Listes de répertoires sensibles :
 - “index of cgi-bin” (3590)

Index of /cgi-bin/

Name	Last modified	Size	Description
 Parent Directory			
 forum-admin.pl	18-Jan-2000 10:24	13K	
 forum.pl	18-Jan-2000 10:24	18K	
 tutkimus/	16-Oct-2002 09:36	4K	

Le piratage via Google



- Listes de répertoires sensibles :
 - Intitle: "Index of" cfide (coldfusion directory)



Index of /CFIDE/

Application.cfm	199	05/19/02	07:39	PM
administrator/	dir	08/21/03	06:07	PM
classes/	dir	08/21/03	06:07	PM
componentutils/	dir	08/21/03	06:07	PM
debug/	dir	08/21/03	06:07	PM
install.cfm	4038	05/19/02	07:39	PM
probe.cfm	8061	05/19/02	07:39	PM
scripts/	dir	08/21/03	06:07	PM

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Listes de répertoires sensibles :
 - Intitle: index.of.winnt















Index of /winnt - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address Go Links

Google intitle:index.of.winnt Search Web PageRank 15 blocked AutoFill Options

Name	Last modified	Size	Description
 Parent Directory	27-Jul-2004 17:15	-	
 NT4_PlainPassword.reg	11-Oct-2001 15:48	1k	
 Win2000_PlainPasswor..>	11-Oct-2001 15:48	1k	
 Win95_PlainPassword.reg	11-Oct-2001 15:48	1k	
 Win98_PlainPassword.reg	11-Oct-2001 15:48	1k	
 Win9X-CacheHandling.reg	11-Oct-2001 15:48	1k	
 WindowsTerminalServe..>	11-Oct-2001 15:48	1k	
 apache/	17-Mar-2003 18:26	-	
 hotfixes-postSP3/	29-Aug-2001 19:54	-	
 nocache.reg	02-Oct-2002 10:04	1k	
 optionspack4NTwork/	29-Aug-2001 19:54	-	
 optionspack4ntserver/	29-Aug-2001 19:54	-	
 optionspack4win95/	29-Aug-2001 19:54	-	
 smhcrvnt/	10-Mar-2003 14:02	-	

Discussions Discussions not available on http://afrodite.upf.tche.br/ Internet

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Listes de répertoires sensibles :
 - Intitle: "index of" iissamples (dangeous iissamples)
(32)



Address <http://home.ec.rr.com/glides/iissamples/homepage/>

Google

Search Web PageRank 15 blocked AutoFill Options

Index of /glides/iissamples/homepage

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory	13-Nov-2003 11:56	-	
WS_FTP.LOG	13-Jan-2001 18:31	4k	
bullet.gif	13-Jan-2001 18:31	1k	
default.asp	13-Jan-2001 18:31	1k	
file.gif	13-Jan-2001 18:31	1k	
global.asa	13-Jan-2001 18:31	1k	
guestbk.asp	13-Jan-2001 18:31	6k	
myfiles.asp	13-Jan-2001 18:31	4k	
signbook.asp	13-Jan-2001 18:31	7k	
sub.inc	13-Jan-2001 18:31	9k	
theme.inc	13-Jan-2001 18:31	1k	
themes/	13-Nov-2003 11:56	-	

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Listes de répertoires sensibles :
 - Inurl: iissamples (1080)



Web Images Groups News more »

inurl:iissamples

Search

Advanced Search

Preferences

Search: the web pages from Canada

Web

Results 11 - 20 of about 1,080 for inurl:iissamples . (0.21 seconds)

www.shadey.com/iissamples/exair/howitworks/codebrws.asp

[Similar pages](#)

[File /iissamples/iissamples/oop/qfullhit.htw. The template file ...](#)

File /iissamples/iissamples/oop/qfullhit.htw. The template file specified in CiTemplate cannot be found.

dcnr.nv.gov/.../iissamples/iissamples/oop/qfullhit.htw&CiRestriction=none&CiHiliteType=Full - 1k - [Cached](#) - [Similar pages](#)

[This text is coming from HeaderInfo.asp.](#)

This text is coming from HeaderInfo.asp.

floti.bell.ac.uk/iis/iissamples/sdk/asp/simple/HeaderInfo.asp - 1k - [Cached](#) - [Similar pages](#)

floti.bell.ac.uk/iis/iissamples/sdk/asp/docs/toolbar.asp

[Similar pages](#)

[[More results from floti.bell.ac.uk](#)]

[The format of QUERY_STRING is invalid.](#)

The format of QUERY_STRING is invalid.

Le piratage via Google

A decorative header image showing red mechanical components, possibly from a machine or engine, set against a dark background.

- Manipulation de la base de données :
 - Chaque application de la base de données laisse une signature unique sur les fichiers de la base de données

Le piratage via Google



- Manipulation de la base de données :
 - “Welcome to phpMyAdmin” AND “Create new database” -intext: “No Privilege” (pour trouver une page ayant les privilèges de mises à jour mysql)

Welcome to phpMyAdmin 2.5.7-pl1

MySQL 3.23.49 running on localhost as seven@localhost

MySQL

↳ Create new database [[Documentation](#)]

↳ [Show processes](#) [[Documentation](#)]

↳ [Databases](#)

↳ [Export](#)

phpMyAdmin

↳ Language (🇬🇧):

↳ [phpMyAdmin documentation](#)

↳ [Official phpMyAdmin Homepage](#)
 [[ChangeLog](#)] [[CVS](#)] [[Lists](#)]

The `$cfg['PmaAbsoluteUri']` directive **MUST be set in your configuration file!**

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Manipulation de la base de données :
 - “Welcome to phpMyAdmin” AND “Create new database” (ce qui nous donne le résultat suivant)

Structure

SQL

Export

Search

Query

Field :	<input type="text"/>	<input type="text"/>	<input type="text"/>
Sort :	<input type="text"/>	<input type="text"/>	<input type="text"/>
Show :	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Criteria :	<input type="text"/>	<input type="text"/>	<input type="text"/>
Ins : <input type="checkbox"/> And : <input type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Del : <input type="checkbox"/> Or : <input checked="" type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Modify :	Or : <input type="radio"/> And : <input checked="" type="radio"/> Ins <input type="checkbox"/> Del <input type="checkbox"/>	Or : <input type="radio"/> And : <input checked="" type="radio"/> Ins <input type="checkbox"/> Del <input type="checkbox"/>	Or : <input type="radio"/> And : <input checked="" type="radio"/> Ins <input type="checkbox"/> Del <input type="checkbox"/>

Use Tables :

- account
- author
- category
- comment
- compilation
- document
- format

Add/Delete Criteria Row : 0

Add/Delete Field Columns : 0

Update Query

Submit Query

SQL-query on database avbase2:

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Manipulation de la base de données :
 - “Select a database to view” intitle: “filemaker pro”
(94) Filemaker

FileMaker Pro Web Companion - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Stop

Address <http://150.146.2.34/> Go Links

Google "Select a database to view" intitle:"filemaker pro" Search Web PageRank 16 blocked AutoFill Options

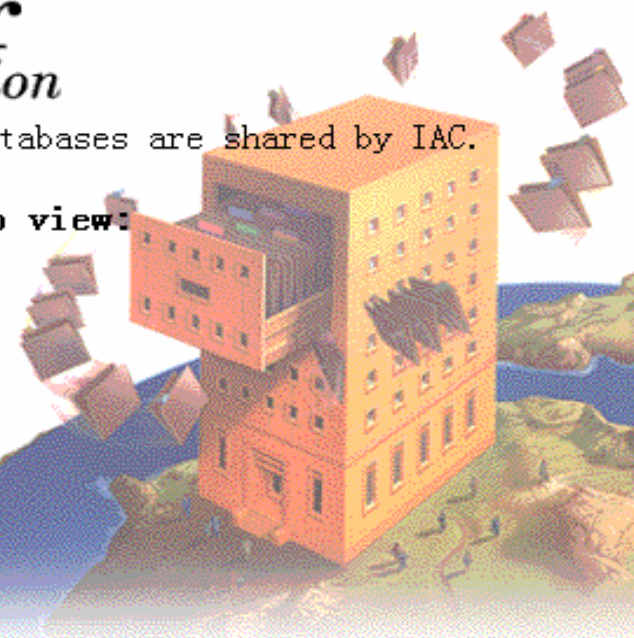
?

FileMaker^{PRO} Web Companion

These FileMaker Pro databases are shared by IAC.

Select a database to view:

- [piconelectures.FP3](#)
- [DIPENDENTIAC.FP3](#)
- [newcnr.FP3](#)
- [preprintdb.FP3](#)
- [preprintiac.fp3](#)
- [pizzaiac.FP3](#)
- [Staff2.FP3](#)
- [financestaff.FP3](#)
- [registro.FP3](#)
- [tecnoareastaff.FP3](#)
- [SCIENTIFICCOMMITTEE.FP3](#)
- [STAFF.FP3](#)
- [preprintdb.FP3](#)
- [seminari.FP3](#)
- [quadernifinale.fp3](#)



Discussions Discussions not available on <http://150.146.2.34/>

Done Internet

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Manipulation de la base de données :
 - Après plusieurs clics, vous pouvez rechercher des informations dans la table

Database: **staff.fp3**

Viewing record range 1-25 of 36

	Nome	Cognome	telefono	email	paginaw
1	Rita	Abbondanza	+39-0688470276	abbondanza@iac.rm.cnr.it	
2	Massimiliano	Adamo	+39-0688470235	adamo@iac.rm.cnr.it	www.iac.rm.cnr.i
3	Piero	Barone	+39-0688470237	barone@iac.rm.cnr.it	www.iac.rm.cnr.i
4	Massimo	Bernaschi	+39-0688470229	massimo@iac.rm.cnr.it	www.iac.rm.cnr.i
5	Michiel	Bertsch	+39-064402627	bertsch@iac.rm.cnr.it	www.iac.rm.cnr.i
6	Stefano	Bianchini	+39-0688470255	bianchin@iac.rm.cnr.it	www.iac.rm.cnr.i
7	Massimiliano	Caramia	+39-0688470222	caramia@iac.rm.cnr.it	www.iac.rm.cnr.i
8	Giuliana	Caringi	+39-0688470205	direzio@iac.rm.cnr.it	

Record range:

1-25

Total records: 36

Sorted

Le piratage via Google

- Manipulation de la base de données :
 - “# Dumping data for table (username|user|users|password)” -site: mysql.com – cvs (289) (données de sauvegarde mysqldump)

http://216.239.39.104/search?q=cache:Uuoa7Sgg4BAJ:typo3.sunsite.dk/LAMP/24.ahversion/mysql.sql4 - Mi...
File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail Stop

Address | Go

Google | le (username|user|users|password)" -site:mysql.com -cvs Search Web PageRank 16 blocked AutoFill Op

```
Process_priv enum('N','Y') NOT NULL default 'N',
File_priv enum('N','Y') NOT NULL default 'N',
Grant_priv enum('N','Y') NOT NULL default 'N',
References_priv enum('N','Y') NOT NULL default 'N',
Index_priv enum('N','Y') NOT NULL default 'N',
Alter_priv enum('N','Y') NOT NULL default 'N',
Show_db_priv enum('N','Y') NOT NULL default 'N',
Super_priv enum('N','Y') NOT NULL default 'N',
Create_tmp_table_priv enum('N','Y') NOT NULL default 'N',
Lock_tables_priv enum('N','Y') NOT NULL default 'N',
Execute_priv enum('N','Y') NOT NULL default 'N',
Repl_slave_priv enum('N','Y') NOT NULL default 'N',
Repl_client_priv enum('N','Y') NOT NULL default 'N',
ssl_type enum('', 'ANY', 'X509', 'SPECIFIED') NOT NULL default '',
ssl_cipher blob NOT NULL,
x509_issuer blob NOT NULL,
x509_subject blob NOT NULL,
max_questions int(11) unsigned NOT NULL default '0',
max_updates int(11) unsigned NOT NULL default '0',
max_connections int(11) unsigned NOT NULL default '0',
PRIMARY KEY (Host,User)
) TYPE=MyISAM COMMENT='Users and global privileges':

--
-- Dumping data for table `user`
--

INSERT INTO user VALUES ('localhost','root','','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y','Y',
INSERT INTO user VALUES ('localhost','typo3','','N','N','N','N','N','N','N','N','N','N','N','N','N','N','N','N',
```

Discussions | Discussions not available on http://216.239.39.104/

Done Internet

Le piratage via Google

- Manipulation de la base de données :
 - “# Dumping data for table
(username|user|users|password)” –site: mysql.com
-CVS



```
-- MySQL dump 8.22
--
-- Host: localhost    Database: cis233j
-----
-- Server version 3.23.51-max-nt

Drop Database if exists cis233j;
Create Database cis233j;
use cis233j;

--
-- Table structure for table 'users'
--

CREATE TABLE users (
  UserKey int(9) NOT NULL auto_increment,
  UserName varchar(15) NOT NULL default '',
  Password varchar(15) NOT NULL default '',
  Active tinyint(1) default '1',
  PRIMARY KEY (UserKey)
) TYPE=MyISAM;

--
-- Dumping data for table 'users'
--

INSERT INTO users VALUES (1,'Greg','biffle',1);
INSERT INTO users VALUES (2,'Doug','pbmaster',1);
INSERT INTO users VALUES (3,'Stevn','linuxmaster',1);
INSERT INTO users VALUES (4,'Skip','vpmaster',1);
```

Le piratage via Google



- Information sensible du système :
 - Les rapports de sécurité du réseau contiennent une liste des vulnérabilités de votre système
 - Les fichiers de configuration contiennent souvent l'inventaire des paramètres d'application

Le piratage via Google



- Rapport de sécurité du réseau (ISS) :
 - “Network Host Assessment Report” “Internet Scanner”
(iss report) (13)

Network Host Assessment Report

Sorted by DNS

4/19/00

Name

Report Description

This report provides detailed network host configuration and vulnerability information. It identifies all services and vulnerabilities associated with each assessible system.

Session Name: R & D Section 6
File Name: Session2_000413
Comment: Weekly Scan

Session ID: 13
Template: Comprehensive
Termination Status: Finished

Scan Summary Information

Hosts Scanned: 3
Hosts Active: 3
Hosts Inactive: 0

Scan Start: 2000/04/13 18:15:20
Scan End: 2000/04/13 18:17:02
Elapsed: 00:01:42

Le piratage via Google



- Rapport de sécurité du réseau (ISS) :
 - “Host Vulnerability Summary Report” (ISS report) (25)

Host Vulnerability Summary Report

Sorted by DNS Name

4/19/00

Report Description

This report displays summary information detailing the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggests corrective action. Vulnerabilities are classified as high, medium and low. High risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network.

Session Name: R & D Section 6
File Name: Session2_000413
Comment: Weekly Scan

Session ID: 13
Template: Comprehensive
Termination Status: Finished

Scan Summary Information

Hosts Scanned: 3
Hosts Active: 3
Hosts Inactive: 0

Scan Start: 2000/04/13 18:15:20
Scan End: 2000/04/13 18:17:02
Elapsed: 00:01:42

DNS Name	Host IP Address	Operating System	Vulnerability Name	Severity
----------	-----------------	------------------	--------------------	----------

Le piratage via Google



- Rapport de sécurité du réseau (Nessus) :
 - “This file was generated by Nessus” ||
intitle:”Nessus Scan Report” -site:nessus.org (185)



Address Go Links

Google by Nessus" || intitle:"Nessus Scan Report" -site:nessus.org Search Web PageRank 16 blocked AutoFill Options

Host List	
Host(s)	Possible Issue
charlemagne.dyndns.org	Security hole(s) found

[\[return to top \]](#)

Analysis of Host		
Address of Host	Port/Service	Issue regarding Port
charlemagne.dyndns.org	discard (9/tcp)	No Information
charlemagne.dyndns.org	daytime (13/tcp)	Security warning(s) found
charlemagne.dyndns.org	ftp (21/tcp)	Security warning(s) found
charlemagne.dyndns.org	telnet (23/tcp)	Security warning(s) found
charlemagne.dyndns.org	smtp (25/tcp)	Security notes found
charlemagne.dyndns.org	time (37/tcp)	Security notes found
charlemagne.dyndns.org	finger (79/tcp)	Security warning(s) found
charlemagne.dyndns.org	www (80/tcp)	Security hole found
charlemagne.dyndns.org	pop3 (110/tcp)	Security notes found
charlemagne.dyndns.org	sunrpc (111/tcp)	Security notes found
charlemagne.dyndns.org	general/tcp	Security hole found
charlemagne.dyndns.org	general/icmp	Security warning(s) found

Le piratage via Google



- Rapport de balayage du réseau (Snort) :
 - “SnortSnarf alert page” (15,500)



SnortSnarf alert page

Source: *218.191.177.52*: overview

[SnortSnarf v020516.1](#)

[Signature section \(3371\)](#) [Top 20 source IPs](#) [Top 20 dest IPs](#)

2558 such alerts found using input module SnortFileInput, with sources:

- /var/log/auth.log

Earliest: **04:04:21** on 6/6/2004

Latest: **07:34:21** on 6/7/2004

19 different signatures are present for *218.191.177.52* as a source

- 1 instances of *TNRO FTP Bad Login*

Le piratage via Google

- Rapport de sécurité du réseau (Snort) :
 - Intitle: "Analysis Console for Intrusion Databases" +intext:"by Roman Danyliw" (13 results, acid alert database) inurl:acid/acid_main.php

Analysis Console for Intrusion Databases

Added 40 alert(s) to the Alert cache

Queried on : Thu August 12, 2004 17:10:13

Database: snort@ (schema version: 106)

Time window: [2004-06-22 16:04:56] - [2004-08-12 17:10:03]

Sensors: 1

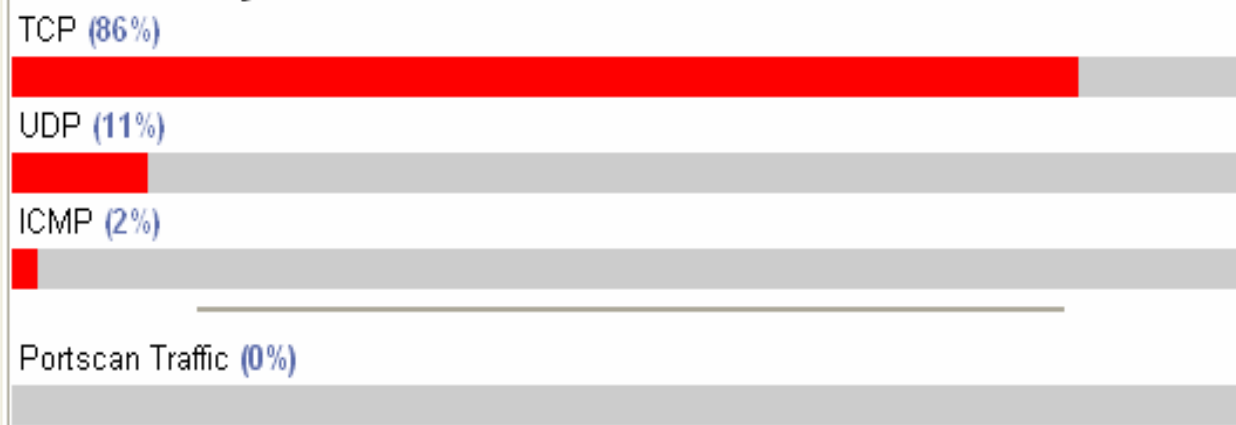
Unique Alerts: 116 (17 categories)

Total Number of Alerts: 5550

- Source IP addresses: 997
- Dest. IP addresses: 135
- Unique IP links 1138

- Source Ports: 3333
 - TCP (3126) UDP (254)
- Dest. Ports: 21

Traffic Profile by Protocol



Le piratage via Google



- Fichiers de configuration (robots.txt) :
 - (inurl: “robot.txt” | inurl: “robots.txt”) intext:disallow filetype:txt
 - Robots.txt signifie qu’il protège votre vie privée contre les spiders « crawlers »
 - Il permet cependant de déterminer l’architecture du système de fichier !



Address Go Links

Google "robot.txt" | inurl:"robots.txt") intext:disallow filetype:txt Search Web PageRank 16 blocked AutoFill Options

```
User-agent: *
Disallow: /cgi-bin
Disallow: /search
Disallow: /query.html
Disallow: /help
Disallow: /360pics/iraq
Disallow: /360pics/text
Disallow: /911/911day/iraq
Disallow: /911/911day/text
Disallow: /911/heroes/iraq
Disallow: /911/heroes/text
# ...
```

Discussions Discussions not available on http://www.████████.gov/



Address Go Links

Google filetype:log inurl:"password.log" Search Web PageRank 15 blocked AutoFill Options password log



Web Images Groups News Froogle more »

filetype:log inurl:"password.log"

Search

[Advanced Search](#)
[Preferences](#)

Web

Results 1 - 10 of about 23 for filetype:log inurl:"password.log". (0.21 seconds)

[name: = "jbhunt"; password: = "jbhunt"; URL: = "http://home.nc.rr. ...](#)

name: = "jbhunt"; password: = "jbhunt"; URL: = "http://home.nc.rr.com/clay123/ref23.html";

Beth Haas name: = "BHaas"; password: = "Beth Haas"; URL: = "http ...

[home.nc.rr.com/clay123/password.log - 2k - Supplemental Result - Cached - Similar pages](#)

[name: = "tad"; password: = "homepage"; URL: = "<a href="http://www ...](#)

name: = "tad"; password: = "homepage"; URL: = "http://www.dob.com.tw";

END_FILE

[dob.tnc.edu.tw/authorHD/1/password.log - 1k - Cached - Similar pages](#)

[name: = "momo"; password: = "momo"; URL: = "password.htm" ...](#)

name: = "momo"; password: = "momo"; URL: = "password.htm"; END_FILE

[jason123.uhome.net/password.log - 1k - Supplemental Result - Cached - Similar pages](#)

[name: = "23202"; password: = "ilgf"; URL: = "address.htm"; name ...](#)

name: = "23202"; password: = "ilgf"; URL: = "address.htm"; name: = "23203"; password:

= "ilgf"; URL: = "address.htm"; name: = "23204"; password: = "ilgf"; URL ...

[www.lib.nchu.edu.tw/groups/group21/password.log - 9k - Cached - Similar pages](#)

[name: = "admin"; password: = "computer"; URL: = "http://members. ...](#)

name: = "admin"; password: = "computer"; URL: = "http://members.tripod.de/Rick_Cooper/fr.htm";

name: = "paul"; password: = "papst"; URL: = "http://members ...

[mitglied.lycos.de/Rick_Cooper/mbr/password.log - 2k - Supplemental Result - Cached - Similar pages](#)

[cc.nyu.edu/tuf.../password.log](#)

Discussions not available on http://www.google.com/



Address Go Links

Google Search Web PageRank 16 blocked AutoFill Options

```
<?
//Cookie for name, web and email in news-tnk v1.2.2 tnka@linux-sottises.net
if($param_name && $save!="1"){
$name=$param_name;
$email=$param_email;
$web=$param_web;
}elseif($save=="1"){
setcookie("param_name", "", time()-100000);
setcookie("param_email", "", time()-100000);
setcookie("param_web", "", time()-100000);
setcookie("param_name", $name, time()+315360000);
setcookie("param_email", $email, time()+315360000);
setcookie("param_web", $web, time()+315360000);
}
```







Address <http://omy.utu.fi/cgi-bin/>

Go Links

Google "index of cgi-bin" Search Web PageRank 15 blocked AutoFill Options

Index of /cgi-bin/

Name	Last modified	Size	Description
 Parent Directory			
 forum-admin.pl	18-Jan-2000 10:24	13K	
 forum.pl	18-Jan-2000 10:24	18K	
 tutkimus/	16-Oct-2002 09:36	4K	

Discussions Discussions not available on <http://omy.utu.fi/>

Done

Internet















Index of /winnt - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address Go Links

Google intitle:index.of.winnt Search Web PageRank 15 blocked AutoFill Options

Name	Last modified	Size	Description
 Parent Directory	27-Jul-2004 17:15	-	
 NT4_PlainPassword.reg	11-Oct-2001 15:48	1k	
 Win2000_PlainPasswor..>	11-Oct-2001 15:48	1k	
 Win95_PlainPassword.reg	11-Oct-2001 15:48	1k	
 Win98_PlainPassword.reg	11-Oct-2001 15:48	1k	
 Win9X-CacheHandling.reg	11-Oct-2001 15:48	1k	
 WindowsTerminalServe..>	11-Oct-2001 15:48	1k	
 apache/	17-Mar-2003 18:26	-	
 hotfixes-postSP3/	29-Aug-2001 19:54	-	
 nocache.reg	02-Oct-2002 10:04	1k	
 optionspack4NTwork/	29-Aug-2001 19:54	-	
 optionspack4ntserver/	29-Aug-2001 19:54	-	
 optionspack4win95/	29-Aug-2001 19:54	-	
 smbrvnt/	10-Mar-2003 14:02	-	

Discussions Discussions not available on http://afrodite.upf.tche.br/ Internet

Index of /glides/iissamples/homepage

Name Last modified Size Description

Parent Directory	13-Nov-2003 11:56	-	
WS_FTP.LOG	13-Jan-2001 18:31	4k	
bullet.gif	13-Jan-2001 18:31	1k	
default.asp	13-Jan-2001 18:31	1k	
file.gif	13-Jan-2001 18:31	1k	
global.asa	13-Jan-2001 18:31	1k	
guestbk.asp	13-Jan-2001 18:31	6k	
myfiles.asp	13-Jan-2001 18:31	4k	
signbook.asp	13-Jan-2001 18:31	7k	
sub.inc	13-Jan-2001 18:31	9k	
theme.inc	13-Jan-2001 18:31	1k	
themes/	13-Nov-2003 11:56	-	



Web Images Groups News more »

inurl:iissamples

Search

Advanced Search

Preferences

Search: the web pages from Canada

Web

Results 11 - 20 of about 1,080 for inurl:iissamples . (0.21 seconds)

www.shadey.com/iissamples/exair/howitworks/codebrws.asp

[Similar pages](#)

[File /iissamples/iissamples/oop/qfullhit.htw. The template file ...](#)

File /iissamples/iissamples/oop/qfullhit.htw. The template file specified in CiTemplate cannot be found.

dcnr.nv.gov/.../iissamples/iissamples/oop/qfullhit.htw&CiRestriction=none&CiHiliteType=Full - 1k - [Cached](#) - [Similar pages](#)

[This text is coming from HeaderInfo.asp.](#)

This text is coming from HeaderInfo.asp.

floti.bell.ac.uk/iis/iissamples/sdk/asp/simple/HeaderInfo.asp - 1k - [Cached](#) - [Similar pages](#)

floti.bell.ac.uk/iis/iissamples/sdk/asp/docs/toolbar.asp

[Similar pages](#)

[[More results from floti.bell.ac.uk](#)]

[The format of QUERY_STRING is invalid.](#)

The format of QUERY_STRING is invalid.

Welcome to phpMyAdmin 2.5.7-pl1

MySQL 3.23.49 running on localhost as seven@localhost

MySQL

↳ Create new database [[Documentation](#)]

↳ [Show processes](#) [[Documentation](#)]

↳ [Databases](#)

↳ [Export](#)

phpMyAdmin

↳ Language (🇬🇧):

↳ [phpMyAdmin documentation](#)

↳ [Official phpMyAdmin Homepage](#)
 [[ChangeLog](#)] [[CVS](#)] [[Lists](#)]

The `$cfg['PmaAbsoluteUri']` directive **MUST be set in your configuration file!**

Structure SQL Export Search Query

Field :	<input type="text"/>	<input type="text"/>	<input type="text"/>
Sort :	<input type="text"/>	<input type="text"/>	<input type="text"/>
Show :	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Criteria :	<input type="text"/>	<input type="text"/>	<input type="text"/>
Ins : <input type="checkbox"/> And : <input type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Del : <input type="checkbox"/> Or : <input checked="" type="radio"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Modify :	Or : <input type="radio"/> And : <input checked="" type="radio"/> Ins <input type="checkbox"/> Del <input type="checkbox"/>	Or : <input type="radio"/> And : <input checked="" type="radio"/> Ins <input type="checkbox"/> Del <input type="checkbox"/>	Or : <input type="radio"/> And : <input checked="" type="radio"/> Ins <input type="checkbox"/> Del <input type="checkbox"/>

Use Tables :

- account
- author
- category
- comment
- compilation
- document
- format

Add/Delete Criteria Row : 0

Add/Delete Field Columns : 0

Update Query

Submit Query

SQL-query on database avbase2:

Le piratage via Google



- Exemple de balayage d'une cible vulnérable :
 - Obtenez les nouvelles vulnérabilités à partir d'un bulletin consultatif
 - Trouvez la signature dans le site Web du vendeur
 - Faites une recherche Google pour trouver des cibles
 - Effectuez des actions qui seront encore plus malveillantes

Secunia Advisories

- ◆ [Secunia Advisories](#)
- ◆ [Historic Advisories](#)
- ◆ [Listed By Product](#)
- ◆ [Listed By Vendor](#)
- ◆ [Statistics](#)
- ◆ [About Advisories](#)
- ◆ [Contact Form](#)

Virus Information

- ◆ [Virus Information](#)
- ◆ [Chronological List](#)
- ◆ [Last 10 Virus Alerts](#)
- ◆ [Statistics](#)
- ◆ [About Virus Info](#)

Mailing Lists

- ◆ [Secunia Advisories](#)
- ◆ [Weekly Summary](#)
- ◆ [Secunia Virus Alerts](#)

Info / Contact

- [Products](#)
- [Secunia Testzone](#)
- [Languages](#)
- [Customer Area](#)

Smart Guest Book Database Content Disclosure Security Issue

Secunia Advisory: SA12401
Release Date: 2004-08-30

Critical:  Moderately critical
Impact: Exposure of sensitive information
Where: From remote
Solution Status: Unpatched

Software: [Smart Guest Book 2.x](#)

Select a product and view a complete list of all Patched/Unpatched Secunia advisories affecting it.

Description:
A security issue has been reported in Smart Guest Book, which may allow malicious people to gain knowledge of sensitive information.

The problem is that the database file "SmartGuestBook.mdb" by default is accessible by anyone. This may disclose various information including the administrative username and password by downloading the file from an affected web site.

Solution:
Place the database file in a separate database directory and restrict access to it.

Provided and/or discovered by:
Security .Net Information

Please note: The information, which this Secunia Advisory is based upon, comes from third party unless stated otherwise.

Secunia collects, validates, and verifies all vulnerability reports issued by security research groups, vendors, and others.

Send Feedback to Secunia:

Search

Secunia News

2004-08-23
New at Secunia.com:
* Improved product pages
* Extra Statistics
* Feedback system
* All Secunia advisories now include "Solution Status"

2004-08-16
A new [spoofing vulnerability](#) has been found in Internet Explorer 6. A test is available [here](#).

2004-07-01
Many browsers are vulnerable to the [Frame Injection Vulnerability](#). Test your browser [here](#).

Secunia Feeds

Secunia Advisories
Get the RSS feed or

Le piratage via Google

A close-up photograph of red mechanical components, possibly a pump or engine part, with various bolts and circular flanges. The lighting is dramatic, highlighting the metallic texture and the vibrant red color.

- Information du manufacturier – Site Web

Installing Free Smart Guest Book 2.0 for Access Database

A. Contents of the zip file

[Free Smart Guest Book](#) [MS SQL Server Installation](#)

You will find the following files:

- ➔ SmartGuestbook.mdb (Access Database)
- ➔ SmartGuestbook.swf (Flash Interface)
- ➔ SmartGuestbook.asp (ASP file where the Flash interface is placed)
- ➔ SmartGuestbookCode.asp (ASP file accessed by the .swf file)
- ➔ scripts.js (Javascript code)
- ➔ badwordfilter.txt (comma delimited bad words list)
- ➔ CloseWindow.htm (to automatically close the window)
- ➔ Readme.txt (content similar to this page section)

Note: If you have your own site and want a quick installation just follow the 1st and 3rd steps. That's It!

B. Installation steps

1. **Important:** Place all the above files in a folder called **SmartGuestBook** under your site root.
Very Important : Please give the folder write permission (If you don't know how to do this, please contact your site administrator).
2. If your site is being hosted by another site i.e. your site is a freely hosted site, you would have to most probably place the access database file in a specified database folder as assigned by your service provider. You will thus need to make a few changes to the pages to give the correct path to the SmartGuestBook files :

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Recherche Google.....:
 - Inurl: smartguestbook.asp




Address <http://www.google.ca/search?hl=en&ie=UTF-8&q=inurl%3Asmartguestbook.asp&meta=>



Google inurl:smartguestbook.asp Search Web 57 blocked AutoFill Options smartguestbook asp

[Web](#)
[Images](#)
[Groups](#)
[News](#)
[more »](#)



[Advanced Search](#)
[Preferences](#)

Search: the web pages from Canada

Web

Results 1 - 10 of about 26 for inurl:smartguestbook.asp. (0.52 seconds)

Le piratage via Google

- Site Web de la victime :

Guest - Book

[New Entry](#)

Dated Apr 15, 2004

Name

Saen

E-mail Address

sean@gemdigi.com

Comments 'n' suggestions

Wow

Entry 25 Of 25

[Reset](#) [Previous](#) [Next](#) [Exit](#)

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, set against a dark background.

- Téléchargement de la base de donnéeéchec et mat !!!

Guest-Book - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail New Tab

Address <http://www.localhost.com/SmartGuestBook/SmartGuestbook.mdb> Go Links

Google inurl:smartguestbook.asp Search Web 57 blocked AutoFill Options smartguestbook asp

Guest - Book

New Entry ▼

Name
Saen

E-mail Address
sean@gemdigi.com

Comments 'n' suggestions
Wow

Entry 25 Of 25

Reset Previous Next Exit

File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: SmartGuestbook.mdb
File type: Microsoft Office Access Application
From: www.localhost.com

⚠ This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

Always ask before opening this type of file

Start downloading from site: <http://www.localhost.com/SmartGuestBook/SmartGuestbook.mdb> Internet

start 2 Microso... m3 - defau... Microsoft E... 3 Interne... 2 Windo... Microsoft P... Document... EN 11:32 AM

Le piratage via Google

- **Le Proxy transparent :**
 - Surf normal sur : www.myip.nu

myip.nu - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Mail Print W Links

Address <http://www.myip.nu/> Go Links

Google inurl:smartguestbook.asp Search Web 57 blocked AutoFill Options smartguestbook.asp

www.myip.nu

Your IP address : [REDACTED] **126.55**

Your Country are : CA Canada


You Browser is: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)

Tuesday 7th September, 2004

You are the 37615th visitor since 11 May 2003

[ip-atlas](#)
[Network Query Tool](#)
[Network utils](#)
[Subnet Calculator](#)
[Who Is](#)

.nudomain: is your .nu name still available?
www.



Done Internet

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, with a dark background.

- Le proxy transparent :
 - Lorsque nous utilisons l'outil de traduction Google pour surfer sur : www.myip.nu



Address http://translate.google.com/translate?u=http%3A%2F%2Fwww.myip.nu&langpair=en%7Cen&hl=en&ie=UTF-8&oe=UTF-8&prev=%2Flanguage_tools Go Links >>

Google inurl:smartguestbook.asp Search Web 57 blocked AutoFill Options smartguestbook asp



This page has been [automatically translated](#) from English.

[View Original Web Page](#)

Printable Version
 Back to Language Tools

www.myip.nu

Your IP address : 216.239.39.5

Your Country are : US United States

You Browser is: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322),gzip(gfe) (via translate.google.com)

Tuesday 7th September, 2004

You are the 37610th visitor since 11 May 2003

- [ip-atlas](#)
- [Network Query Tool](#)
- [Network utils](#)
- [Subnet Calculator](#)
- [Who Is](#)

.nudomain: is your .nu name still available?
WWW.

Le piratage via Google



- Outils automatisés - Google :
 - SiteDigger
 - SiteDigger recherche dans la mémoire tampon de Google pour des vulnérabilités, des erreurs, des problèmes de configuration, de l'informations confidentielles et pour tout autres fragments intéressants qui concerne la sécurité que l'on retrouve sur les sites Web. Voir :
<http://www.foundstone.com>

Foundstone SiteDigger v1.0



File Options Help About

Foundstone | SiteDigger

Results | Signatures

Please enter a domain

Search

Stop

Clear

Export Results

Connecting to Foundstone.com....
Downloading file Schema.xml from Foundstone.com
Downloaded file saved at C:\Program Files\Foundstone\SiteDigger
Signatures successfully updated.....

Enter Google license key:

E980ISBQFHK1K9zQjxzKi5iwJ37HA8lf

Le piratage via Google



- Matériels - Google :
 - Googledorks
 - Le fameux site Web de piratage Google, qui contient plusieurs exemples différents à propos de choses incroyables :
<http://johnny.ihackstuff.com>.

Navigate

- Home
- Who's Johnny?
- Search Engine
- Hacking Forum
- downloads
- Google Hacking Database (GHDB)
- photos/art
- web links
- search

Latest Googledorks

- #530: filetype:reg "Terminal Server Client"
- #529: filetype:rdp rdp
- #528: WebAPP directory traversal
- #527: inurl:snitz_forums_2000.mdb
- #526: "Powered by Ikonboard 3.1.1"
- #525: Snitz! forums db path error
- #524: link:http://www.toastforums.com/
- #523: inurl:"plog/register.php"
- #521: filetype:qbb qbb
- #522: filetype:bkf bkf

Welcome to the Google Hacking Database (GHDB)!

We call them 'googledorks' (gOO gÃ´l'DÃ´rk, noun, slang) : An inept or foolish person as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe! Stop by our forums to see where the magic happens!

Entries by Category

Error Messages (50)

Really retarded error messages that say WAY too much! **new**

Files containing juicy info (125)

No usernames or passwords, but interesting stuff none the less. **new**

Files containing passwords (73)

PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

Files containing usernames (13)

These files contain usernames, but no passwords... Still, google finding usernames on the web..

Footholds (5)

Examples of queries that can help gain a foothold into a web server

Pages containing login portals (46)

These are login pages for various services. Consider them the front door of a site's more sensitive functions.

Pages containing network or vulnerability data (14)

These pages contain such things as firewall logs, network information, IDS logs... all sorts of fun stuff!

Sensitive Directories (27)

Google's collection of sites sharing sensitive directories. The files contained in here will vary from sensitive to uber-secret!

Sensitive Online Shopping Info (3)

Examples of queries that can reveal online shopping info like customer data, suppliers, orders, credit info, etc

Various Online Devices (17)

This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.

Vulnerable Files (25)

HUNDREDS of vulnerable files that Google can find on web servers... **new**

Vulnerable Servers (28)

These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.

Web Server Detection (37)

These links demonstrate Google's awesome ability to profile web servers..

10 most popular entries

- 1) index.of.password
- 2) "access denied for user" "using password"
- 3) auth_user_file.txt
- 4) The Master List
- 5) allinurl: admin mdb
- 6) "A syntax error has occurred" filetype:ihtml
- 7) passlist.txt (a better way)
- 8) ORA-00921: unexpected end of SQL command
- 9) Look in my backup directories! Please?
- 10) config.php

10 most recent entries

- 1) intitle:"Object not found!" intext:"Apache/2.0.* (Linux/SuSE)"
- 2) inurl:netw_tcp.shtml
- 3) intitle:"WebJeff - FileManager" intext:"login" intext:Pass|PAsse
- 4) intitle:"EMUMAIL - Login" "Powered by EMU Webmail"
- 5) intitle:"Open WebMail" "Open WebMail version (2.20|2.21|2.30) "
- 6) intitle:"error 404" "From RFC 2068 "
- 7) intitle:"Directory Listing, Index of /*/"
- 8) "Powered by Caudium Webserver" -caudium.net
- 9) intitle:"IBM HTTP Server" "Use the Administration Server to configure"
- 10) intitle:"Lotus Domino Go Webserver:" "Tuning your webserver" -site:ibm.com

Protéger vos informations contre Google

- Recommandations pour vous aider à protéger vos données :
 - Appliquez les programmes de correction / rustine aux systèmes et aux applications
 - **Ne gardez aucunes** informations ou autres données sensibles sur le Web et implanter une procédure d'authentification (RSA, Radius, Safeword)
 - Désactivez les répertoires de navigation
 - Piratez votre site Web avec Google
 - Pensez à enlever votre site de l'index Google :
<http://www.google.com/remove.html>.
 - Utilisez le fichier robots.txt contre les spiders Web « crawlers » :
<http://www.robotstxt.org>.

Outils pour vous aider à vérifier vos applications Web

Google APIS:

www.google.com/apis

Remove:

<http://www.google.com/remove.html>

Googledorks:

<http://johnny.ihackstuff.com/>

O'reilly Google Hack:

<http://www.oreilly.com/catalog/googlehks/>

Google Hack Presentation, Johnny Long:

<http://johnny.ihackstuff.com/modules.php?op=modload&name=ownloads&file=index&req=viewdownload&cid=1>

“Autism: Using google to hack:

www.smart-dev.com/texts/google.txt

“Google: Net Hacker Tool du Jour:

<http://www.wired.com/news/infostructure/0,1377,57897,00.html>

Le piratage via Google

A decorative header image showing red mechanical components, possibly a camera lens or a similar optical device, set against a dark background.

MERCI!

rmasse@gosecure.ca