
GoSecure

Hacking with Google for fun and profit!

October 2004

Robert Masse & Jian Hui Wang

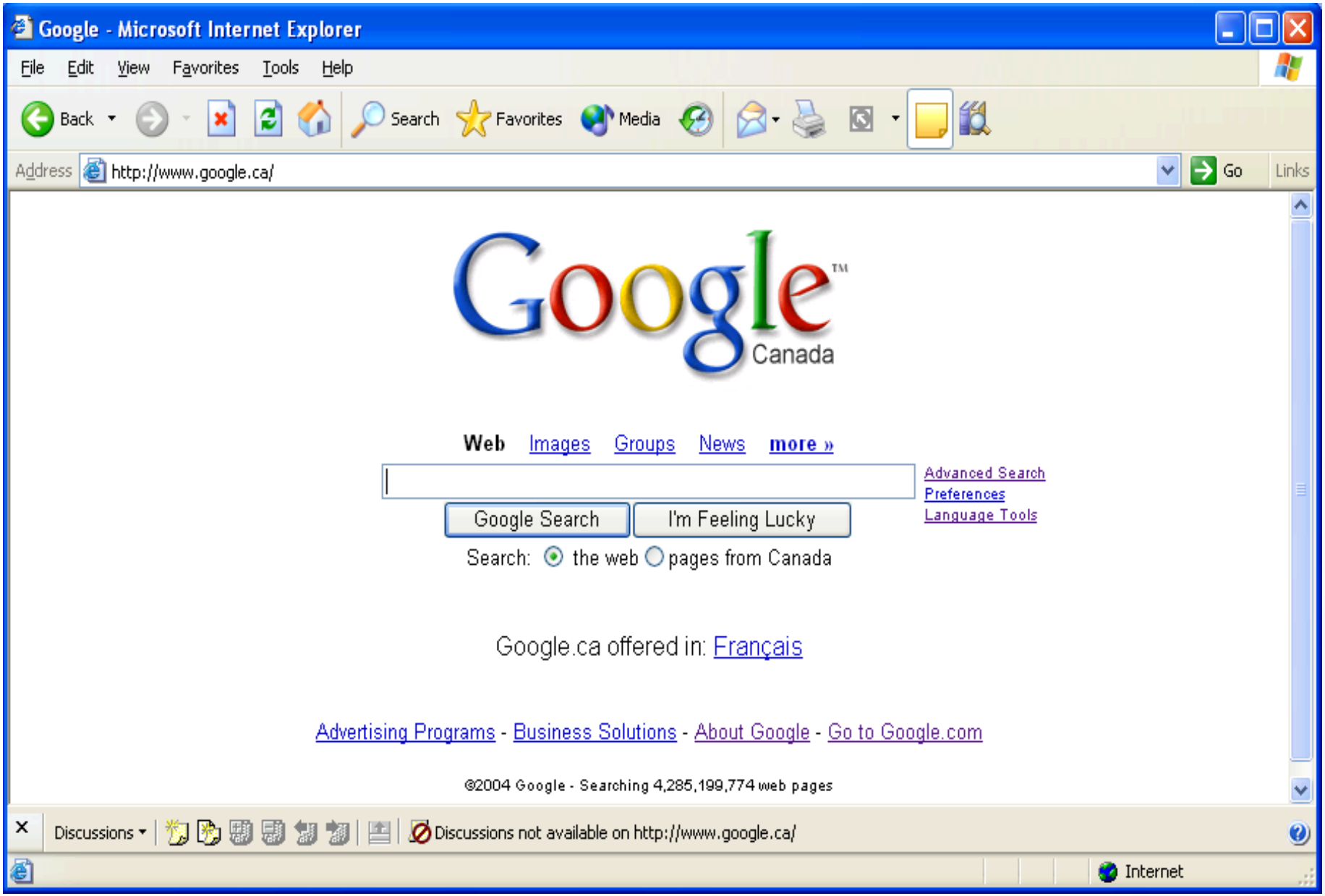
GoSecure Inc.

Agenda

- Google Introduction & Features
- Google Search Technique
- Google Basic Operators
- Google Advanced Operators
- Google Hacking
  - Digging for “vulnerability gold”
  - Identifying operating systems
  - Vulnerability scanning
  - Proxying
- Protect your information from Google

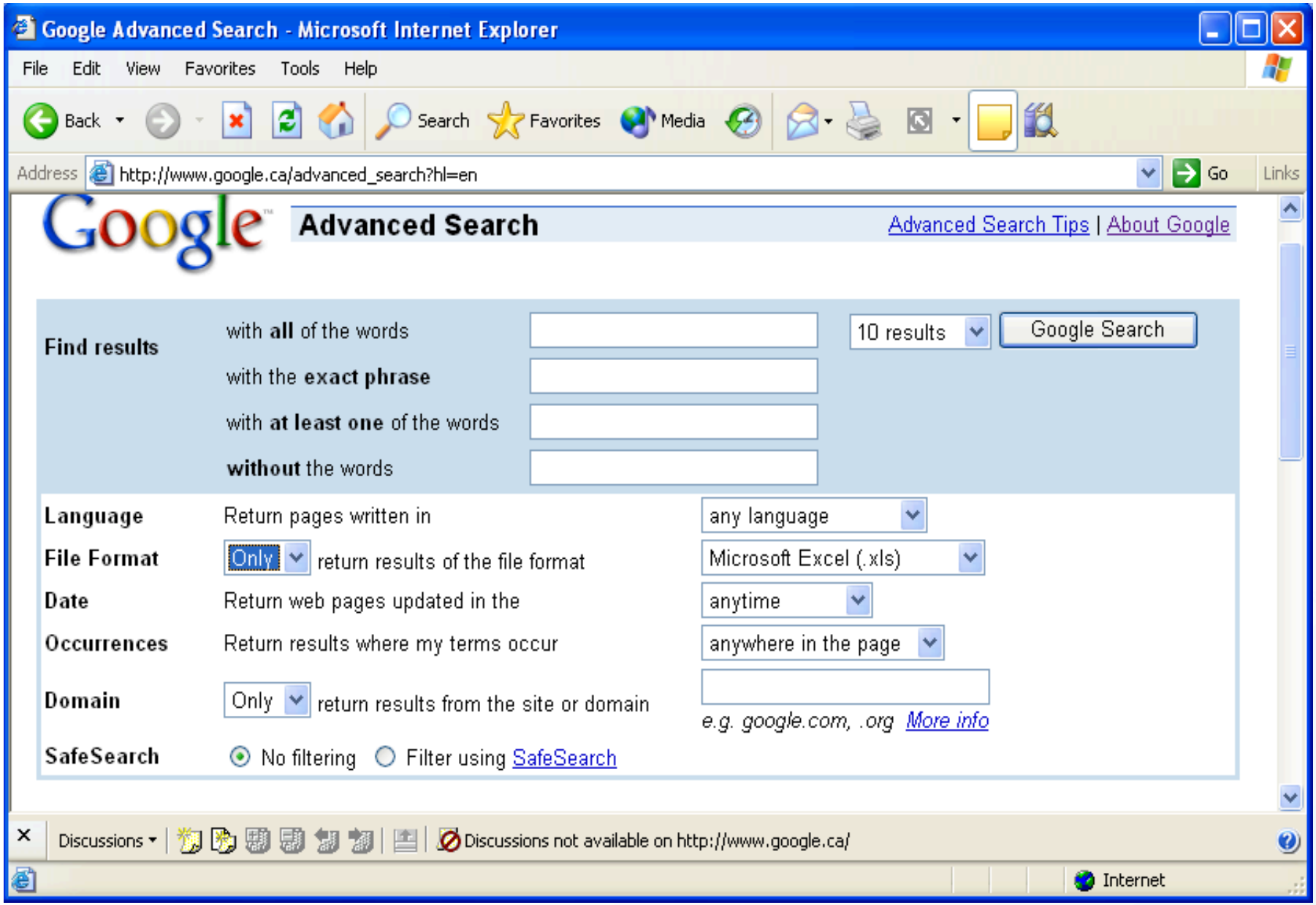
Google Hacking

- Google Search Technique
  - Just put the word and run the search
- You need to audit your Internet presence
  - One database, Google almost has it all!
- One of the most powerful databases in the world
- Consolidate a lot of info
- Usage:
  - Student …
  - Business …
  - Al'Qaeda …
    - One stop shop for attack, maps, addresses, photos, technical information


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/
Go Links
Google™
Canada
Web Images Groups News more »
Advanced Search
Preferences
Language Tools
Google Search
I'm Feeling Lucky
Search: the web pages from Canada
Google.ca offered in: Français
Advertising Programs - Business Solutions - About Google - Go to Google.com
©2004 Google - Searching 4,285,199,774 web pages
Discussions
Discussions not available on http://www.google.ca/
Internet

Google Hacking

- Google Advance Search
  - A little more sophisticated ……


Google Advanced Search - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/advanced_search?hl=en
Go Links
Google
Advanced Search
Advanced Search Tips | About Google
Find results
with all of the words
with the exact phrase
with at least one of the words
without the words
10 results
Google Search
Language
Return pages written in
any language
File Format
Only
return results of the file format
Microsoft Excel (.xls)
Date
Return web pages updated in the
anytime
Occurrences
Return results where my terms occur
anywhere in the page
Domain
Only
return results from the site or domain
e.g. google.com, .org More info
SafeSearch
No filtering
Filter using SafeSearch
Discussions
Discussions not available on http://www.google.ca/
Internet

Google Hacking

- Google Operators:
  - Operators are used to refine the results and to maximize the search value. They are your tools as well as hackers' weapons
- Basic Operators:

  +, -, ~ , ., *, "", |, OR
- Advanced Operators:
  - allintext:, allintitle:, allinurl:, bphonebook:, cache:, define:, filetype:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, rphonebook:, site:, numrange:, daterange

Google Hacking

- Basic Operators
  - (+) force inclusion of something common
  - Google ignores common words (where, how, digit, single letters) by default:

    Example: StarStar Wars Episode +I
  - (-) exclude a search term

    Example: apple –red
  - (“) use quotes around a search term to search exact phrases:

    Example: “Robert Masse”
  - Robert masse without “” has the 309,000 results, but “robert masse” only has 927 results. Reduce the 99% irrelevant results

Google Hacking

- Basic Operators
  - (~) search synonym:

    Example: ~food
  - Return the results about food as well as recipe, nutrition and cooking information
  - (.) a single-character wildcard:

    Example: m.trix
  - Return the results of M@trix, matrix, metrix…….
  - (*) any word wildcard

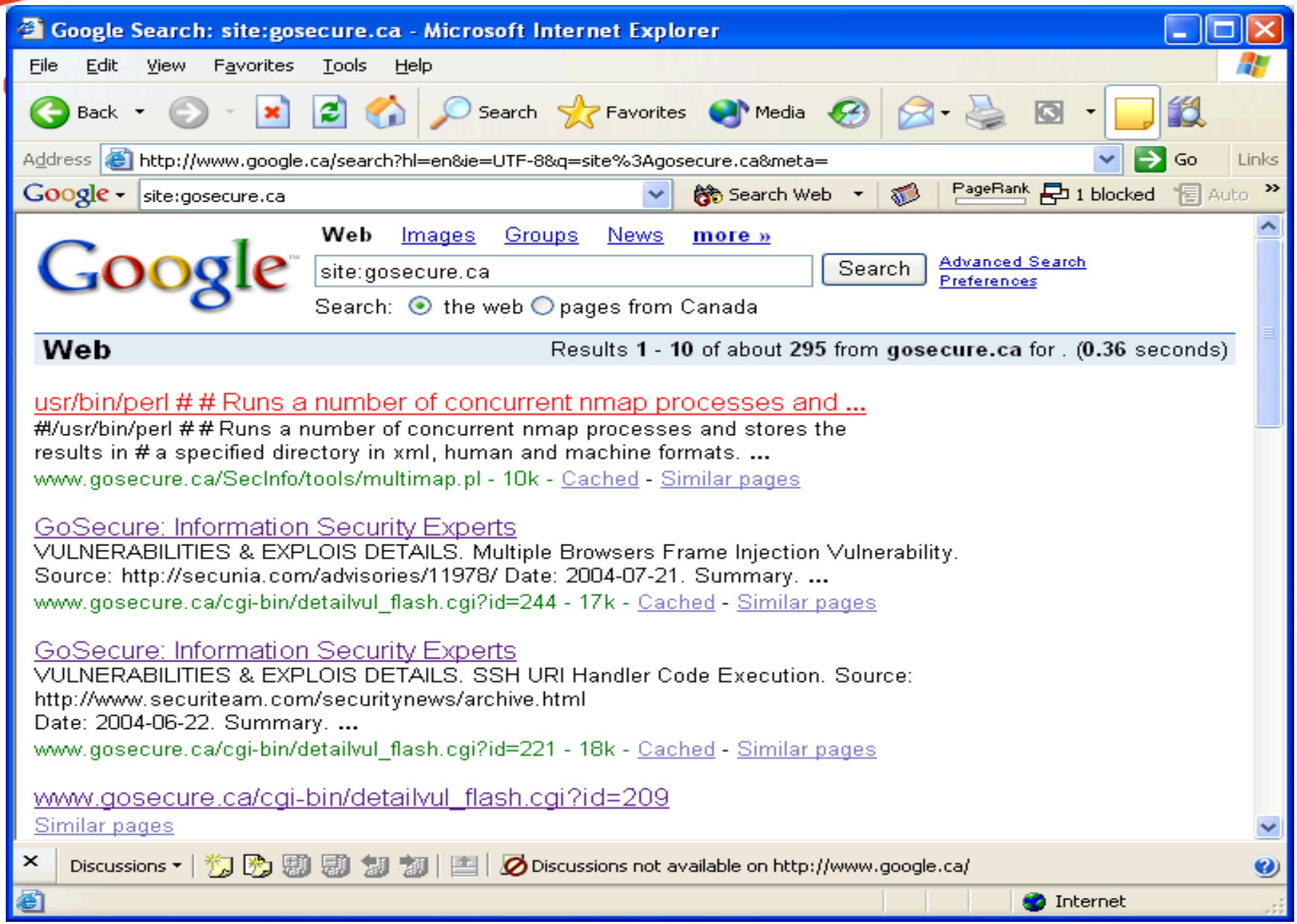
Google Hacking

- Advanced Operators: “Site:”
  - Site: Domain_name
  - Find Web pages only on the specified domain. If we search a specific site, usually we get the Web structure of the domain
  - Examples:

    site:ca

    site:gosecure.ca

    site:www.gosecure.ca


Google Search: site:gosecure.ca - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
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

Google Hacking

- Advanced Operators: “Filetype:”
  - Filetype: extension_type
  - Find documents with specified extensions
  - The supported extensions are:

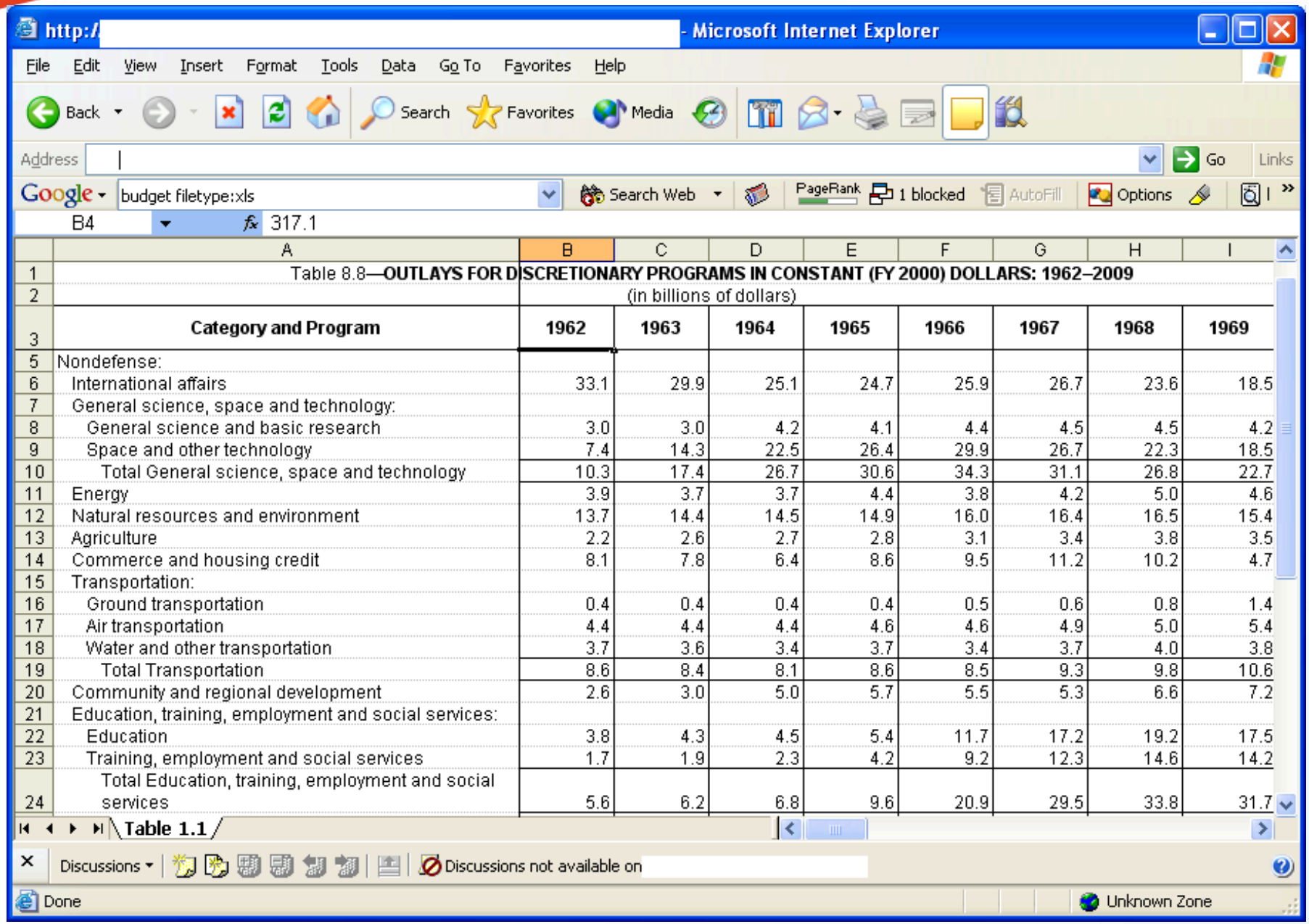
- HyperText Markup Language (html)
- Adobe Portable Document Format (pdf)
- Adobe PostScript (ps)
- Lotus 1-2-3 (wk1, wk2, wk3, wk4, wk5, wki, wks, wku)
- Lotus WordPro (lwp)
- MacWrite (mw)
- Text (ans, txt)
- Microsoft PowerPoint (ppt)
- Microsoft Word (doc)
- Microsoft Works (wks, wps, wdb)
- Microsoft Excel (xls)
- Microsoft Write (wri)
- Rich Text Format (rtf)
- Shockwave Flash (swf)

  - Note: We actually can search asp, php and cgi, pl files as long as it is text-compatible.

    Example: Budget filetype: xls

Google Hacking

- Advanced Operators
  - A budget file we found …….



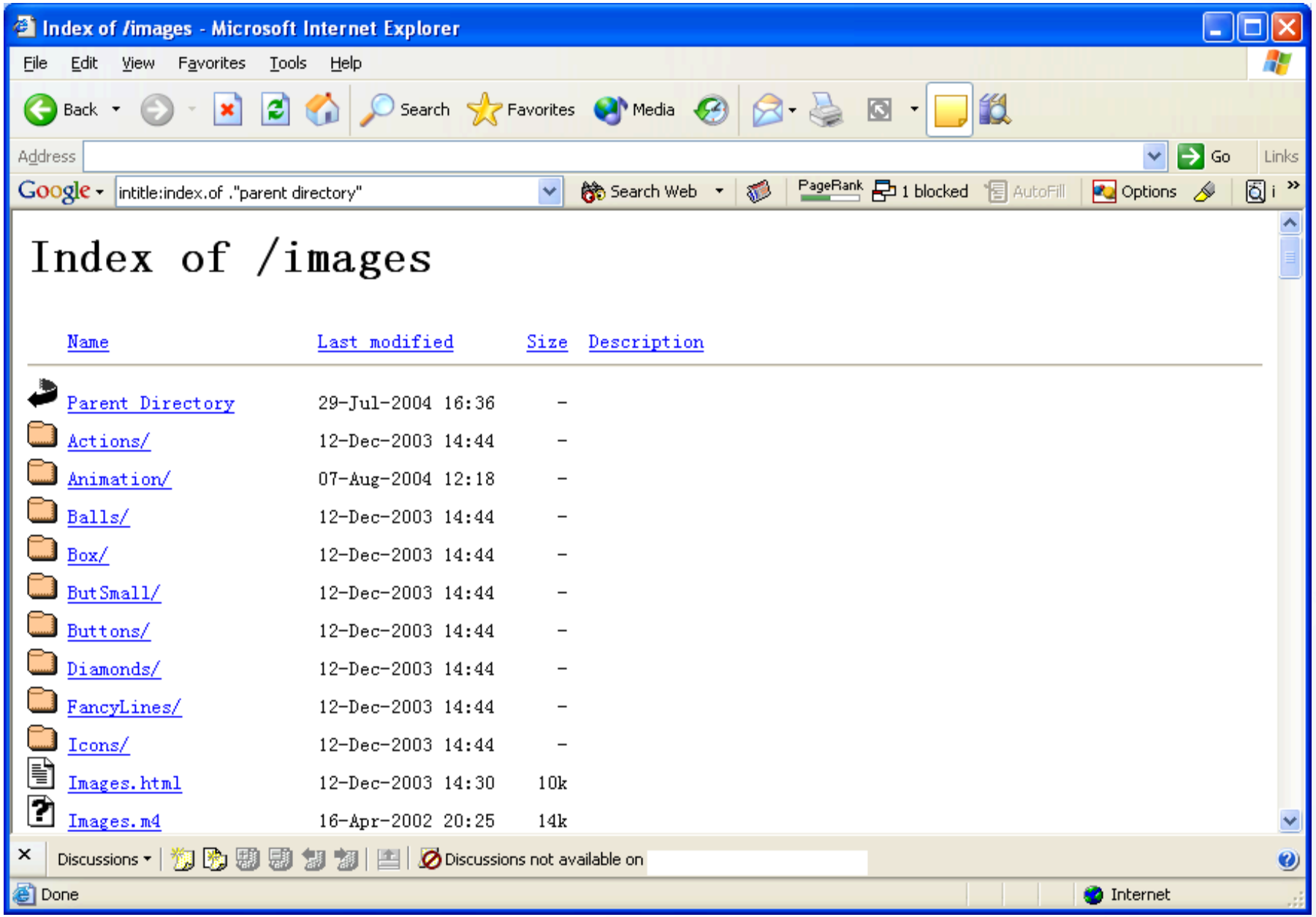
	A	B	C	D	E	F	G	H	I
1	Table 8.8—**OUTLAYS FOR DISCRETIONARY PROGRAMS IN CONSTANT (FY 2000) DOLLARS: 1962–2009**								
2	(in billions of dollars)								
3	**Category and Program**	**1962**	**1963**	**1964**	**1965**	**1966**	**1967**	**1968**	**1969**
5	Nondefense:								
6	International affairs	33.1	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

Google Hacking

- Advanced Operators “Intitle:”
  - Intitle: search_term
  - Find search term within the title of a Webpage
  - Allintitle: search_term1 search_term2 search_term3
  - Find multiple search terms in the Web pages with the title that includes all these words
  - These operators are specifically useful to find the directory lists
  - Example:

    Find directory list:

    Intitle: Index.of “parent directory”

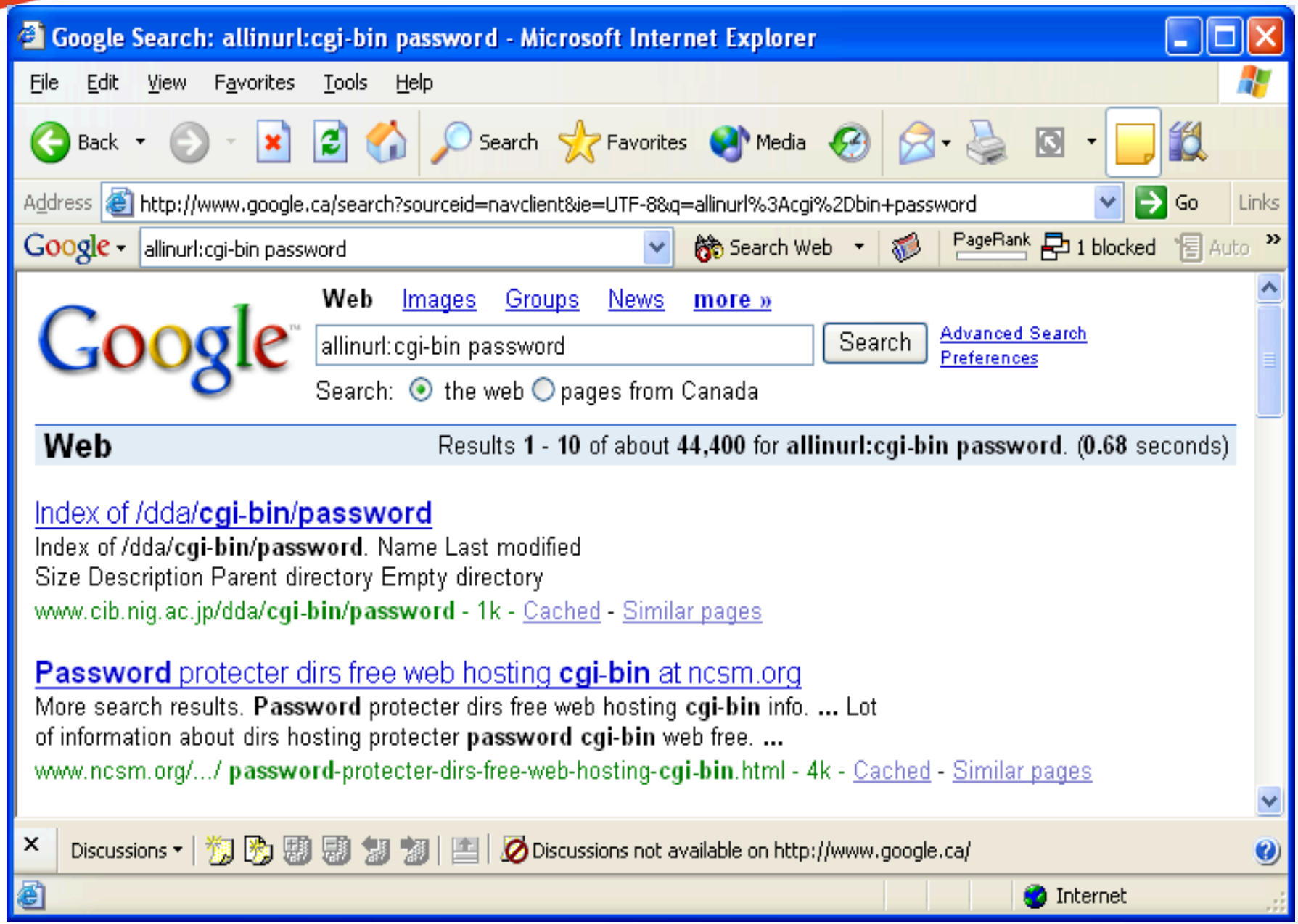

Index of /images - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google intitle:index.of ."parent directory"
Search Web PageRank 1 blocked AutoFill Options
Index of /images
Name Last modified Size Description
Parent Directory 29-Jul-2004 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
Discussions Discussions not available on
Done
Internet

Google Hacking

- Advanced Operators “Inurl:”
  - Inurl: search_term
  - Find search term in a Web address
  - Allinurl: search_term1 search_term2 search_term3
  - Find multiple search terms in a Web address
  - Examples:

    Inurl: cgi-bin

    Allinurl: cgi-bin password

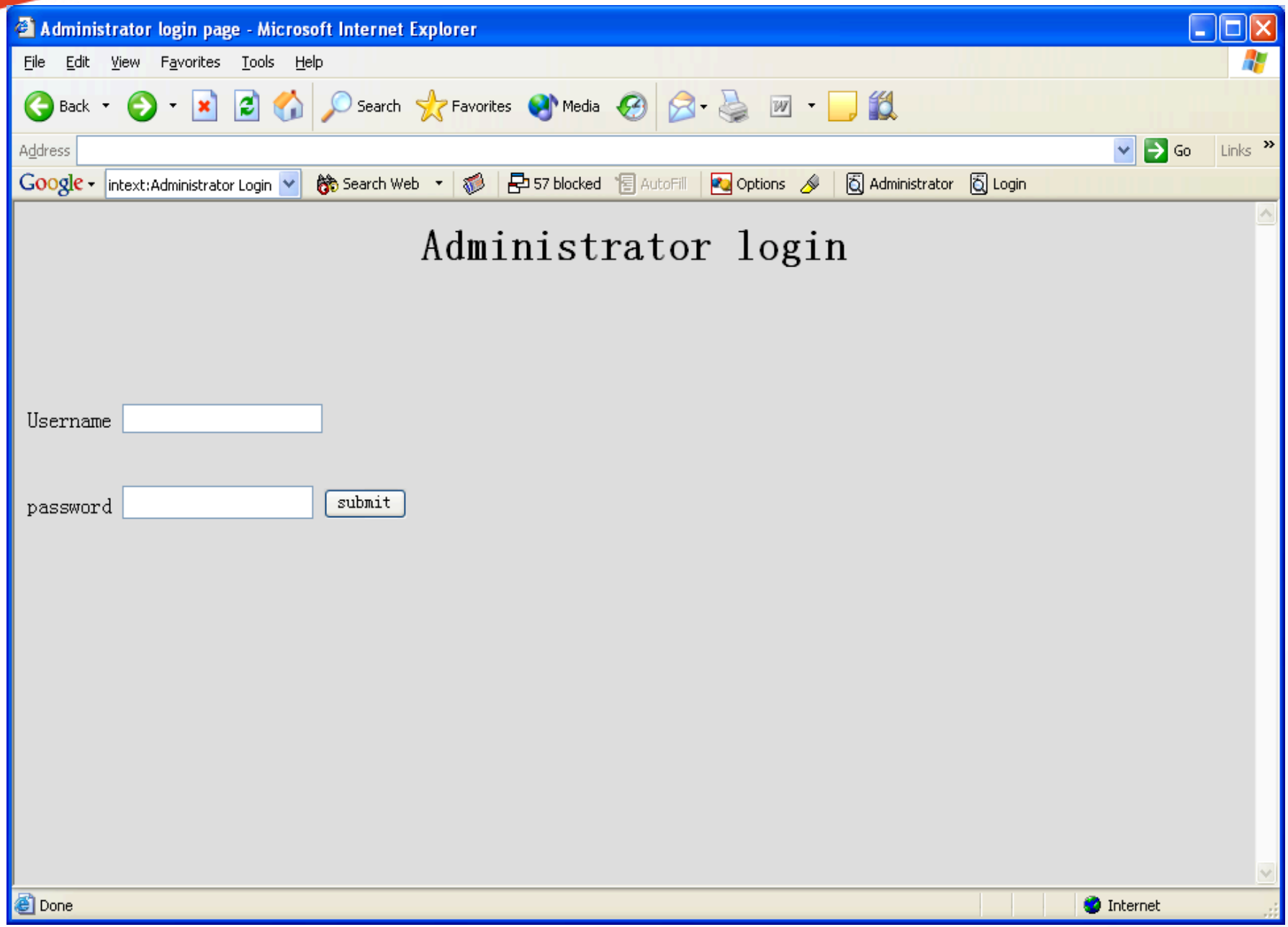

Google Search: allinurl:cgi-bin password - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?sourceid=navclient&ie=UTF-8&q=allinurl%3Acgi%2Dbin+password
Go Links
Google allinurl:cgi-bin password
Search Web PageRank 1 blocked Auto
Web Images Groups News more »
Google
allinurl:cgi-bin password
Search
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 protecter dirs free web hosting cgi-bin at ncsm.org
More search results. Password protecter dirs free web hosting cgi-bin info. ... Lot
of information about dirs hosting protecter password cgi-bin web free. ...
www.ncsm.org/.../ password-protecter-dirs-free-web-hosting-cgi-bin.html - 4k - Cached - Similar pages
Discussions
Discussions not available on http://www.google.ca/
Internet

Google Hacking

- Advanced Operators “Intext;”
  - Intext: search_term
  - Find search term in the text body of a document.
  - Allintext: search_term1 search_term2 search_term3
  - Find multiple search terms in the text body of a document.
  - Examples:

    Intext: Administrator login

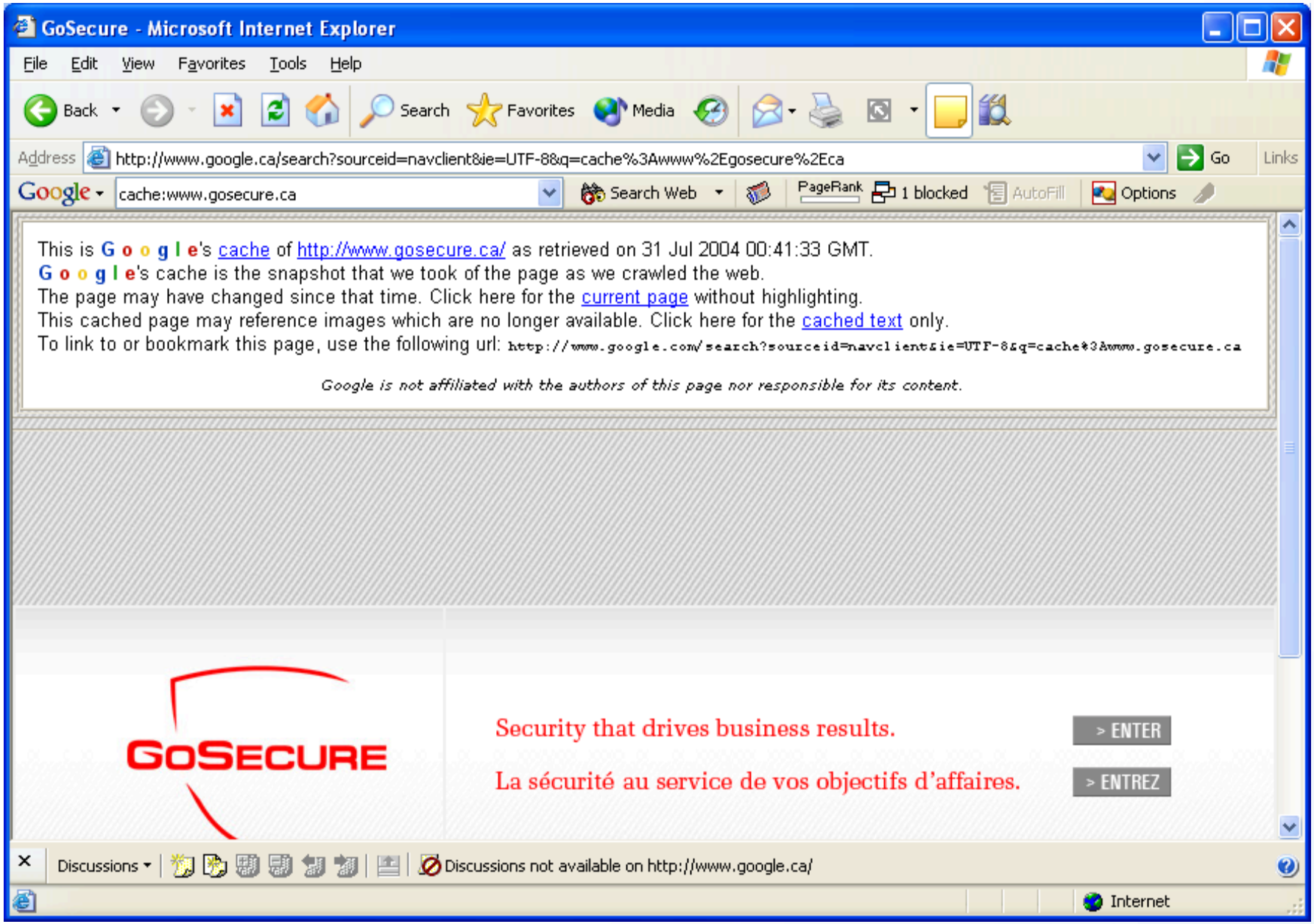
    Allintext: Administrator login


Administrator login page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google intext:Administrator Login Search Web 57 blocked AutoFill Options Administrator Login
Administrator login
Username
password
submit
Done
Internet

Google Hacking

- Advanced Operators: “Cache:”
  - Cache: URL
  - Find the old version of Website in Google cache
  - Sometimes, even the site has already been updated, the old information might be found in cache
  - Examples:

    Cache: www.gosecure.com

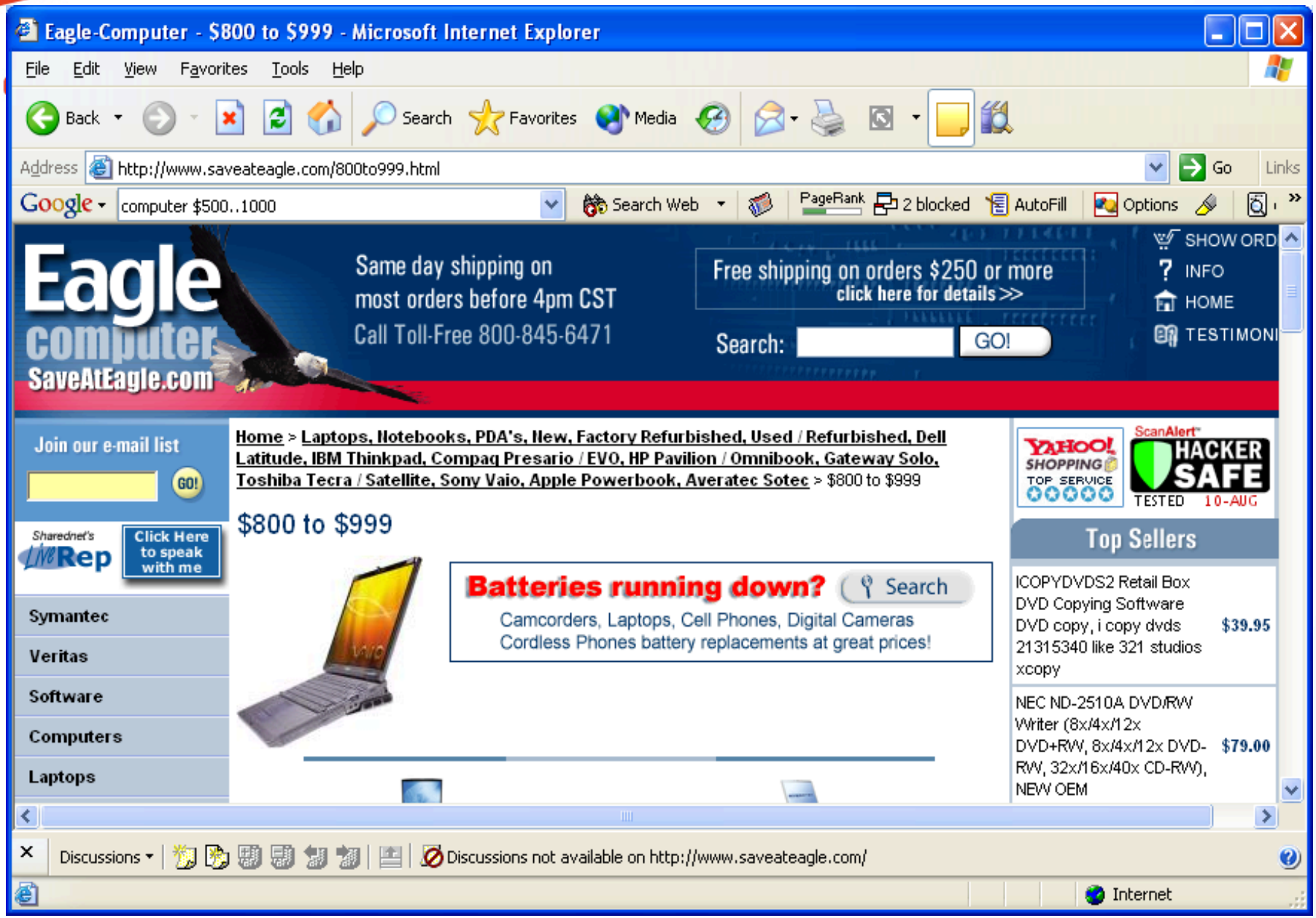

GoSecure - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?sourceid=navclient&ie=UTF-8&q=cache%3Awww%2Egosecure%2Eca
Go Links
Google cache:www.gosecure.ca
Search Web PageRank 1 blocked AutoFill Options
This is Google's cache 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.
GoSecure
Security that drives business results.
> ENTER
La sécurité au service de vos objectifs d'affaires.
> ENTREZ
Discussions
Discussions not available on http://www.google.ca/
Internet

Google Hacking

- Advanced Operators
  - <number1>..<number2>
  - Conduct a number range search by specifying two numbers, separated by two periods, with no spaces. Be sure to specify a unit of measure or some other indicator of what the number range represents
  - Examples:

    Computer $500..1000

    DVD player $250..350

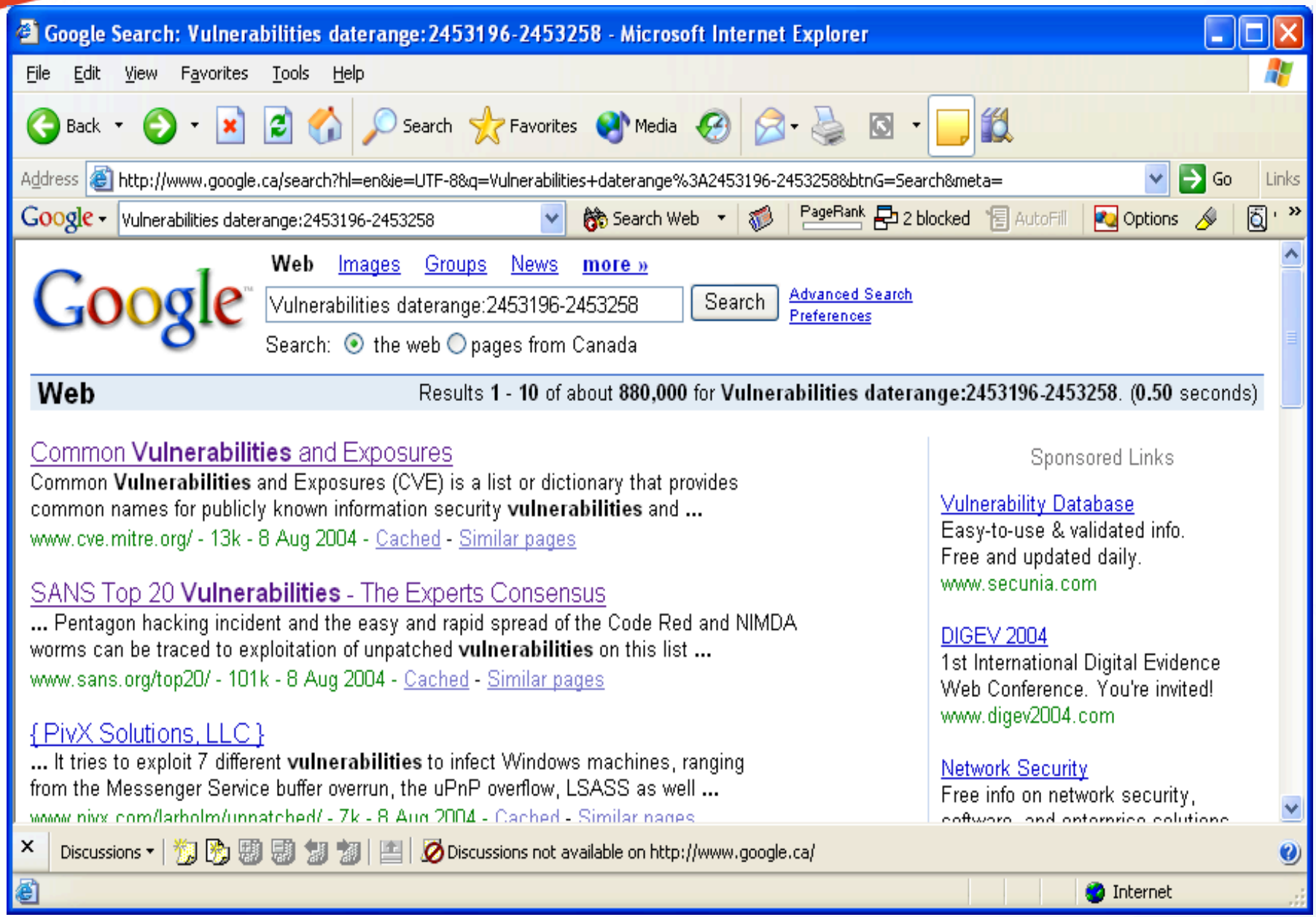

Eagle-Computer - $800 to $999 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.saveateagle.com/800to999.html
Go Links
Google computer $500..1000
Search Web PageRank 2 blocked AutoFill Options
Eagle computer SaveAtEagle.com
Same day shipping on most orders before 4pm CST
Call Toll-Free 800-845-6471
Free shipping on orders $250 or more
click here for details >>
Search: GO!
SHOW ORD
INFO
HOME
TESTIMONI
Join our e-mail list
GO!
Sharednet's LiveRep
Click Here to speak with me
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?
Search
Camcorders, Laptops, Cell Phones, Digital Cameras
Cordless Phones battery replacements at great prices!
YAHOO! SHOPPING TOP SERVICE
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
Discussions
Discussions not available on http://www.saveateagle.com/
Internet

Google Hacking

- Advanced Operators: “Daterange:”
  - Daterange: <start_date>-<end date>
  - Find the Web pages between start date and end date
  - Note: start_date and end date use the Julian date
  - The Julian date is calculated by the number of days since January 1, 4713 BC. For example, the Julian date for August 1, 2001 is 2452122
  - Examples:

    2004.07.10=2453196

    2004.08.10=2453258
  - Vulnerabilities date range: 2453196-2453258


Google Search: Vulnerabilities daterange:2453196-2453258 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?hl=en&ie=UTF-8&q=Vulnerabilities+daterange%3A2453196-2453258&btnG=Search&meta=
Go Links
Google Vulnerabilities daterange:2453196-2453258
Search Web PageRank 2 blocked AutoFill Options
Google
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 ...
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,
Discussions
Discussions not available on http://www.google.ca/
Internet

Google Hacking

- Advanced Operators "Link:"
  - Link: URL
  - Find the Web pages having a link to the specified URL
  - Related: URL
  - Find the Web pages that are "similar" to the specified Web page
  - info: URL
  - Present some information that Google has about that Web page
  - Define: search_term
  - Provide a definition of the words gathered from various online sources
  - Examples:

    Link: gosecure.ca

    Related: gosecure.ca

    Info: gosecure.ca

Globetechnology - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://www.globetechnology.com/servlet/story/RTGAM.20040223.gtflmassefeb23/BNStory/Technology/ Go Links

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

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

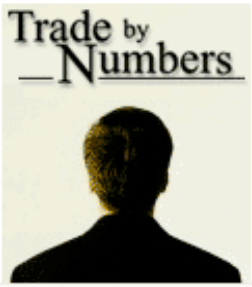
By Robert Masse
Special to Globe and Mail Update

E-mail this Article
Print this Article

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.

Advertisement



Tech Poll

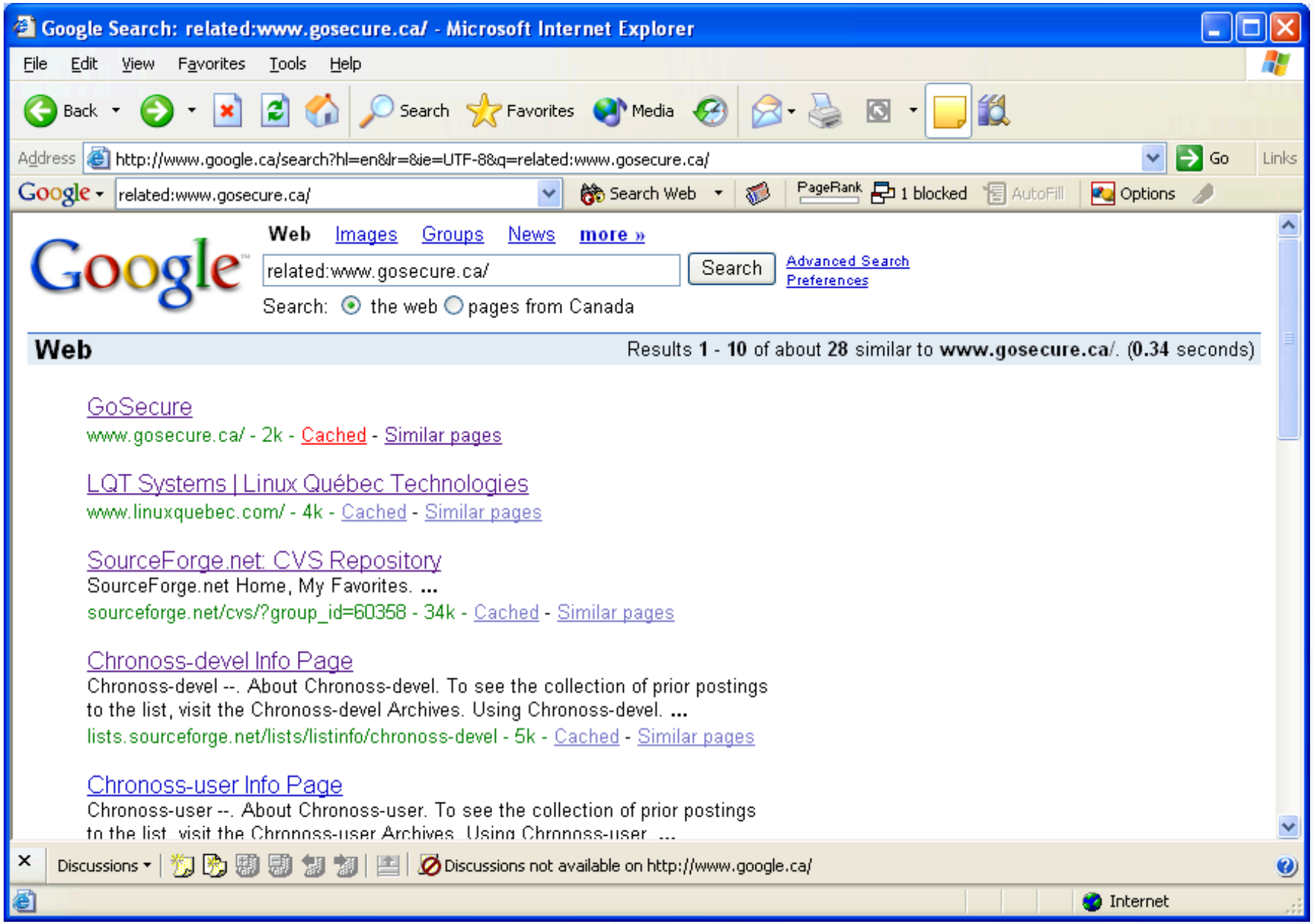
Should government fund programs to ensure small communities have broadband Internet access?

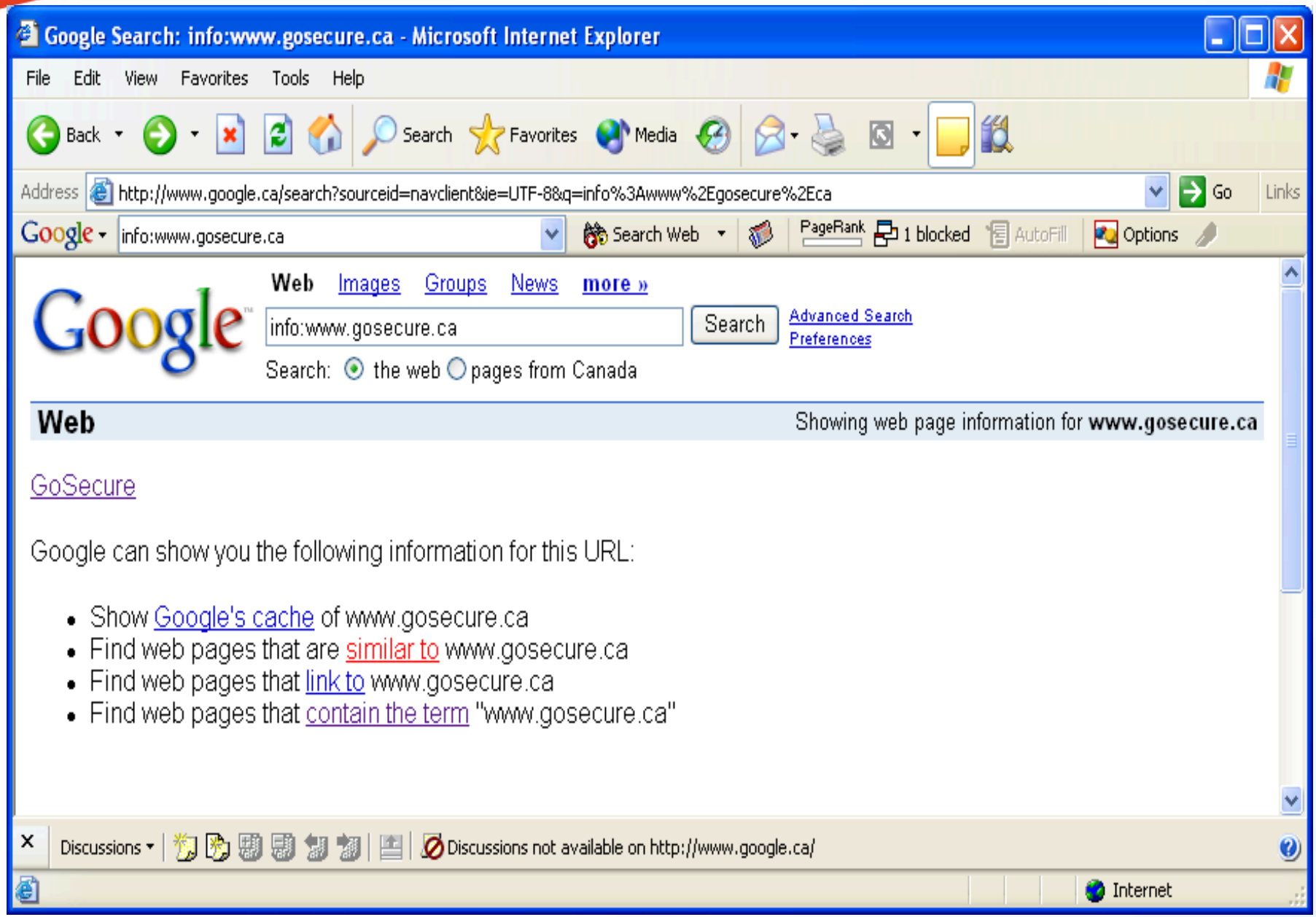
Yes
No
Vote
Results & Past Polls

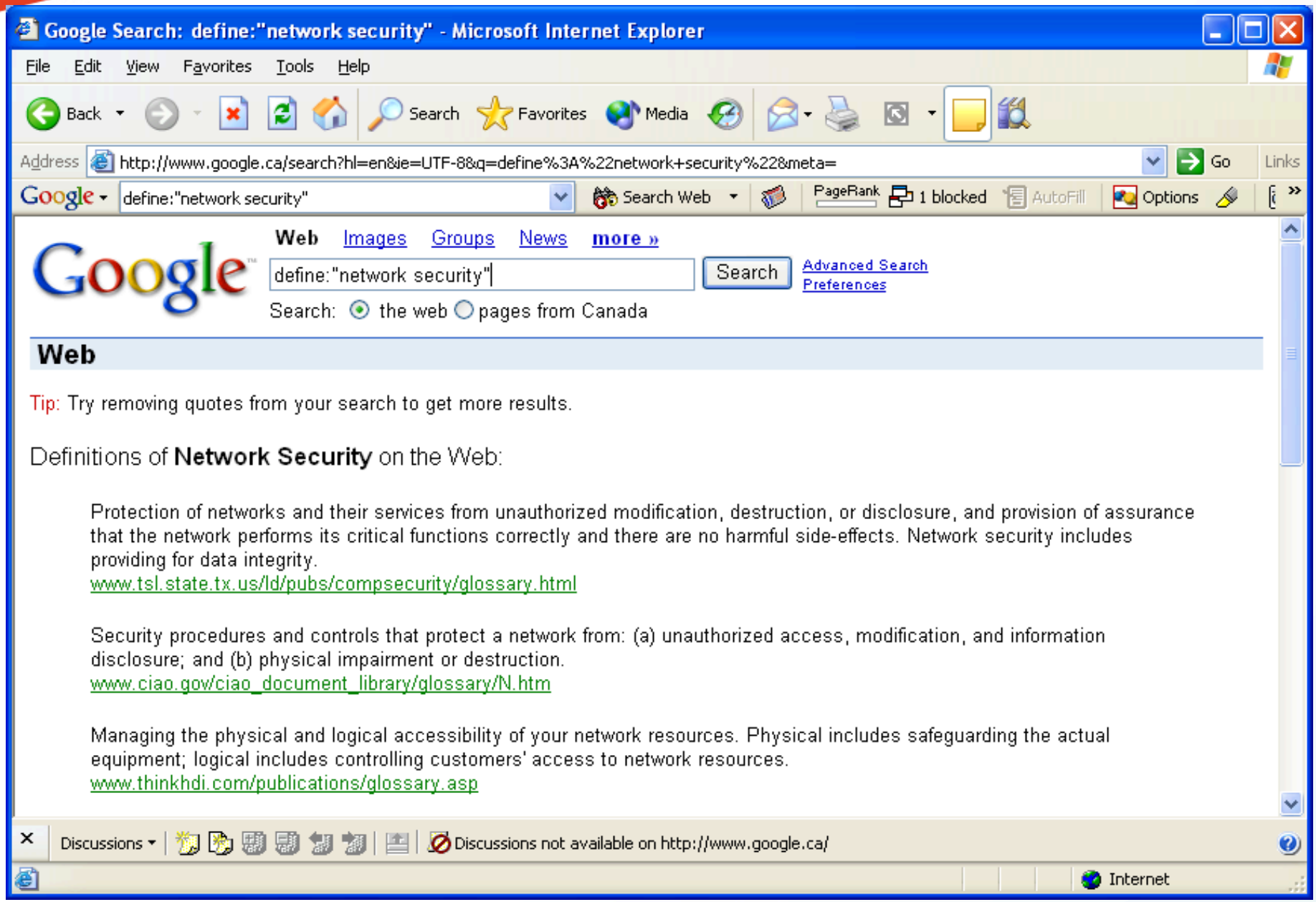
Sign up for Tech Alerts

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

Internet


Google Search: related:www.gosecure.ca/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?hl=en&lr=&ie=UTF-8&q=related:www.gosecure.ca/
Go Links
Google related:www.gosecure.ca/
Search Web PageRank 1 blocked AutoFill Options
Web Images Groups News more »
Google
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
Discussions
Discussions not available on http://www.google.ca/
Internet


Google Search: info:www.gosecure.ca - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?sourceid=navclient&ie=UTF-8&q=info%3Awww%2Egosecure%2Eca
Go Links
Google info:www.gosecure.ca
Search Web PageRank 1 blocked AutoFill Options
Web Images Groups News more »
Google
info:www.gosecure.ca
Search
Advanced Search
Preferences
Search: the web pages from Canada
Web
Showing web page information for www.gosecure.ca
GoSecure
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"
Discussions
Discussions not available on http://www.google.ca/
Internet


Google Search: define:"network security" - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?hl=en&ie=UTF-8&q=define%3A%22network+security%22&meta=
Go Links
Google define:"network security"
Search Web PageRank 1 blocked AutoFill Options
Web Images Groups News more »
Google
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
Discussions
Discussions not available on http://www.google.ca/
Internet

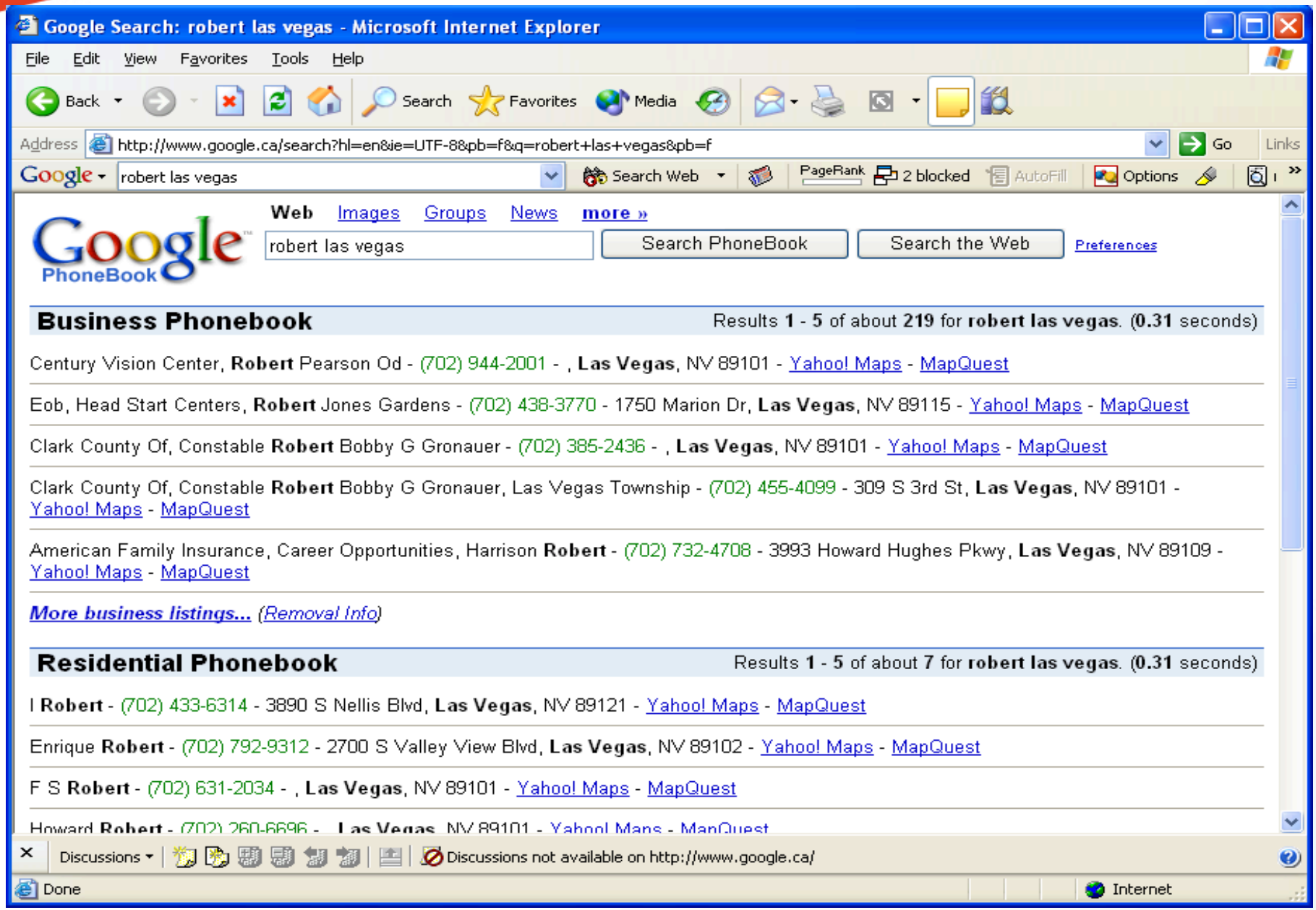
Google Hacking

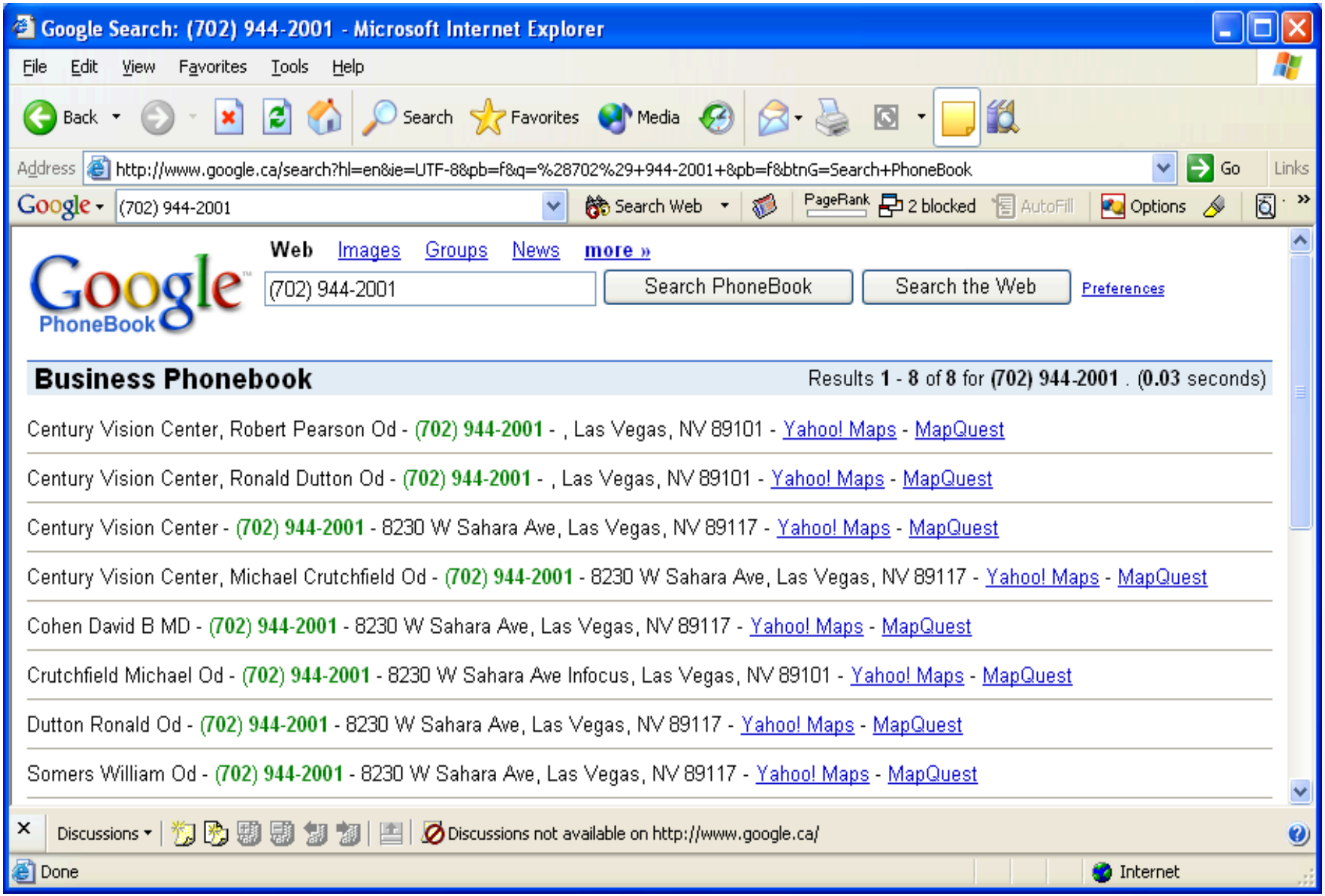
- Advanced Operators “phonebook:”
  - Phonebook
  - Search the entire Google phonebook
  - rphonebook
  - Search residential listings only
  - bphonebook
  - Search business listings only
  - Examples:

    Phonebook: robert las vegas (robert in Las Vegas)

    Phonebook: (702) 944-2001 (reverse search, not always work)

    The phonebook is quite limited to U.S.A


Google Search: robert las vegas - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
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
Web Images Groups News more »
Google PhoneBook
robert las vegas
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


Google Search: (702) 944-2001 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?hl=en&ie=UTF-8&pb=f&q=%28702%29+944-2001+&pb=f&btnG=Search+PhoneBook
Go Links
Google (702) 944-2001
Search Web PageRank 2 blocked AutoFill Options
Web Images Groups News more »
Google PhoneBook
(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
Discussions
Discussions not available on http://www.google.ca/
Done
Internet

Google Hacking

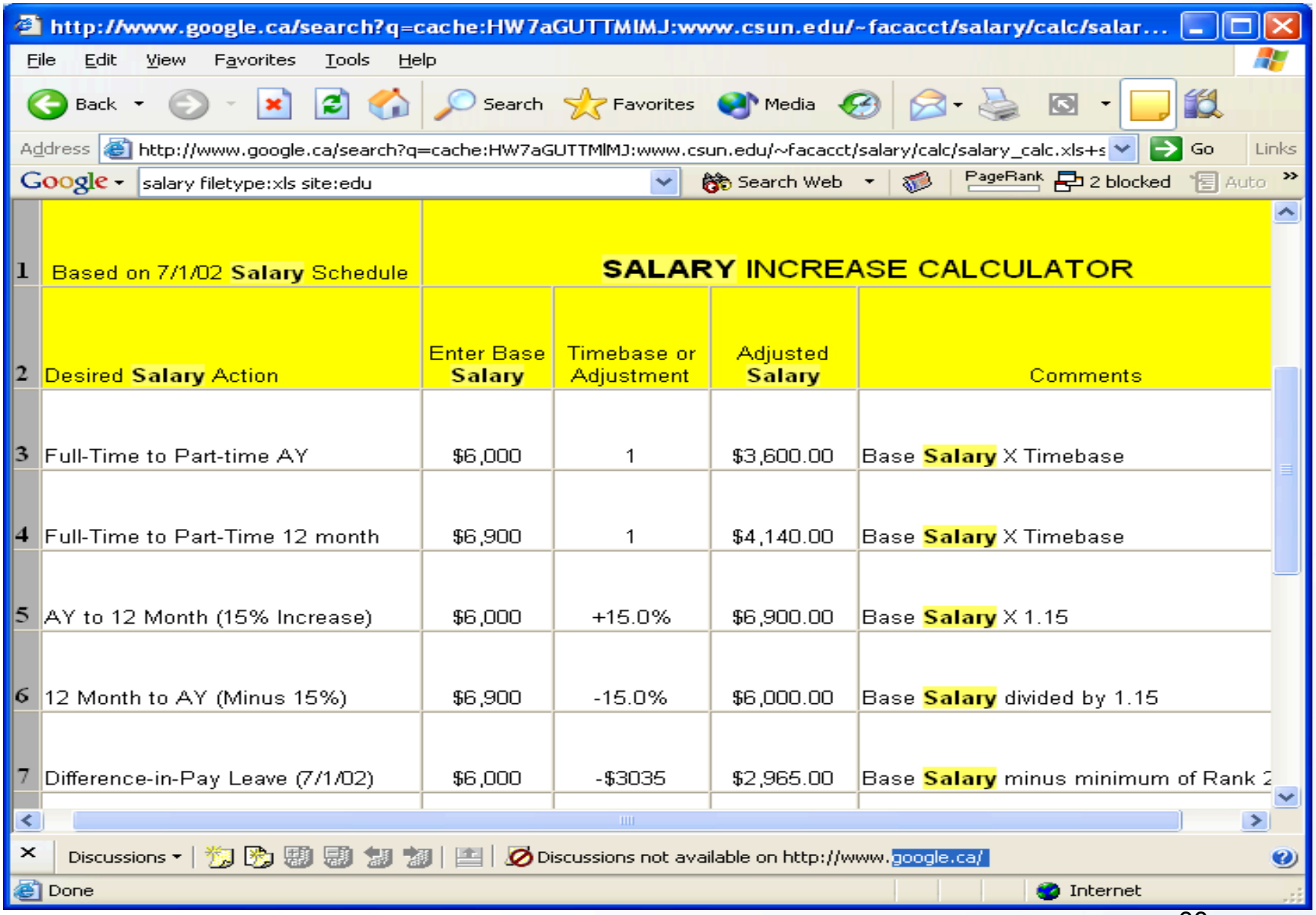
- Google, Friend or Enemy?
  - Google is everyone's best friend (yours or hackers)
  - Information gathering and vulnerability identification are the tasks in the first phase of a typical hacking scenario
  - Passitive, stealth and huge data collection
  - Google can do more than search
  - Have you used Google to audit your organization today?

Google Hacking

- What can Google can do for a hacker?
  - Search sensitive information like payroll, SIN, even the personal email box
  - Vulnerabilities scanner
  - Transparent proxy

Google Hacking

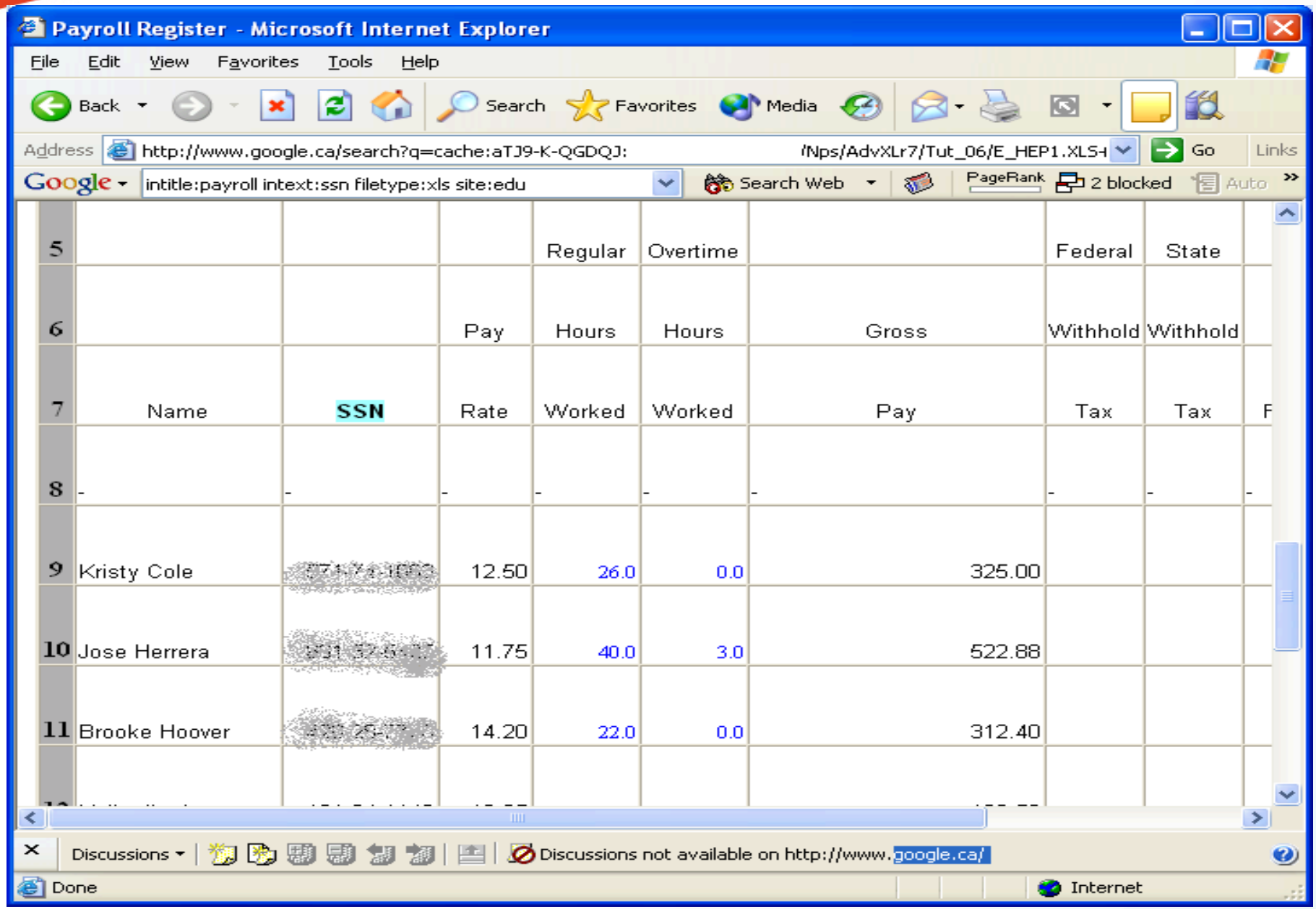
- Salary
  - Salary filetype: xls site: edu



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

Google Hacking

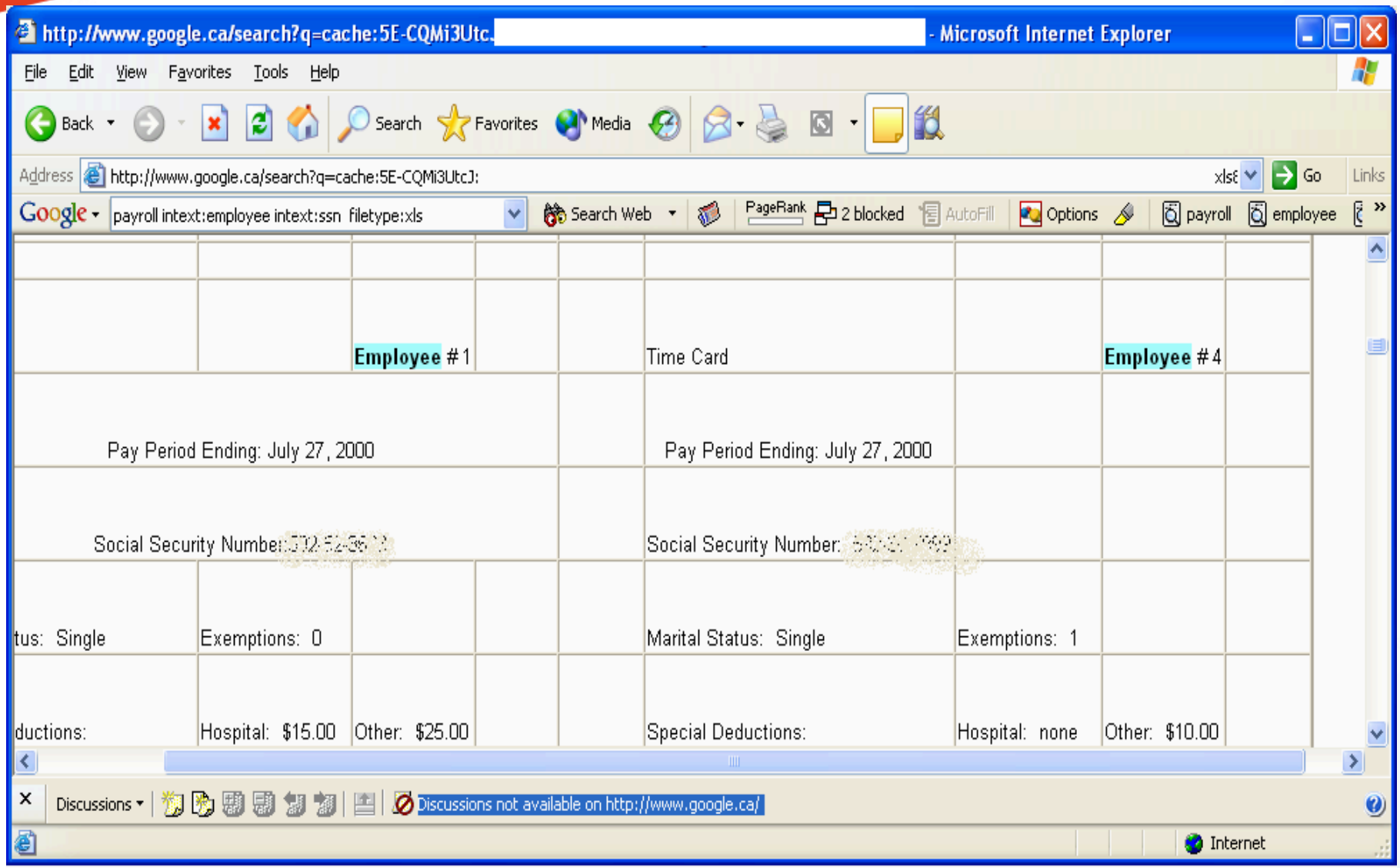
- Security social insurance number
  - Intitle: Payroll intext: ssn filetype: xls site: edu



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	[illegible]	12.50	26.0	0.0	325.00			
10	Jose Herrera	[illegible]	11.75	40.0	3.0	522.88			
11	Brooke Hoover	[illegible]	14.20	22.0	0.0	312.40			

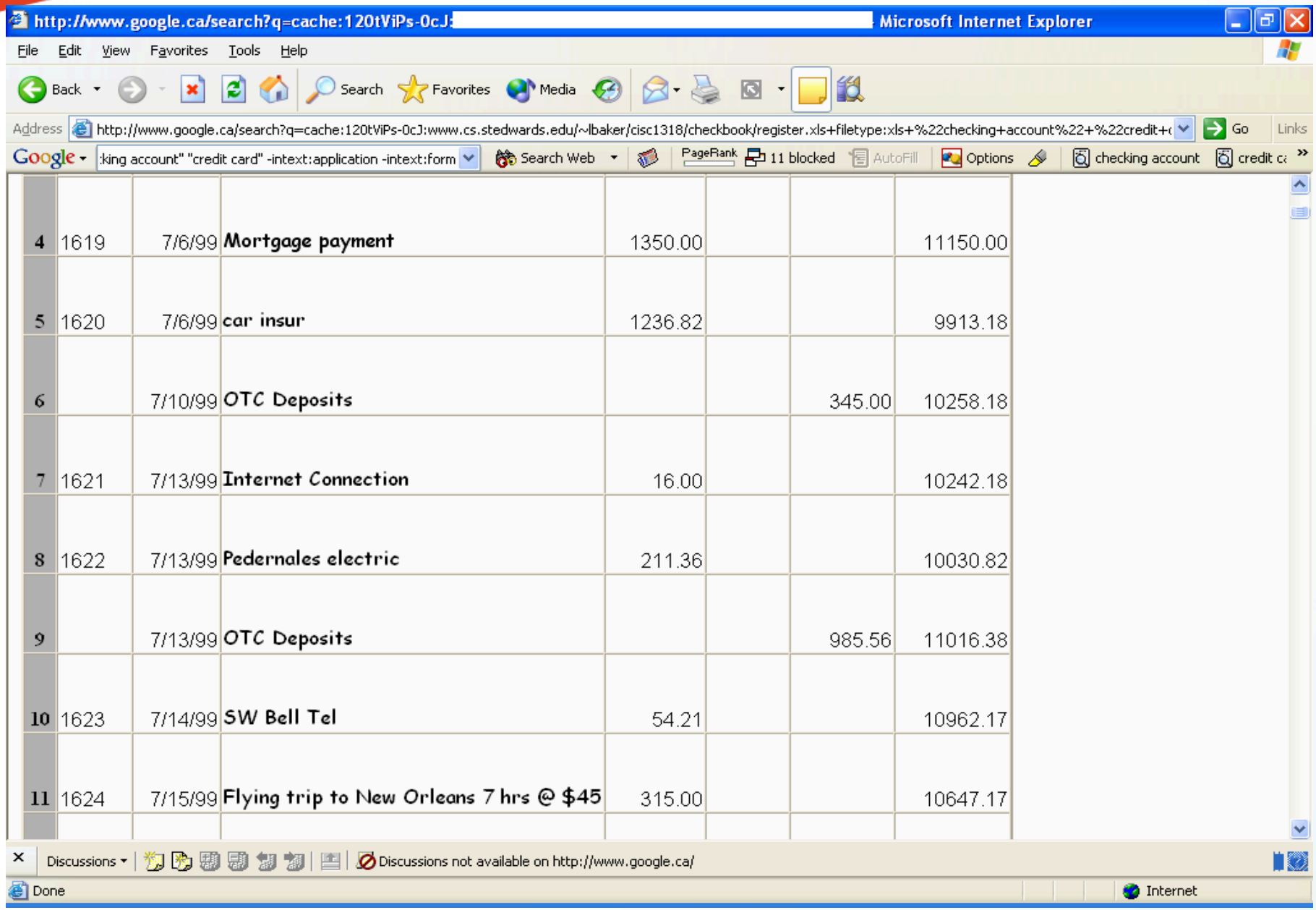
Google Hacking

- Security Social Insurance Number
  - Payroll intext: Employee intext: ssn iletype: xls


http://www.google.ca/search?q=cache:5E-CQMi3Utc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?q=cache:5E-CQMi3UtcJ:
Go Links
Google payroll intext:employee intext:ssn filetype:xls
Search Web PageRank 2 blocked AutoFill Options payroll employee
Employee #1
Time Card
Employee #4
Pay Period Ending: July 27, 2000
Pay Period Ending: July 27, 2000
Social Security Numbe
Social Security Number:
tus: Single
Exemptions: 0
Marital Status: Single
Exemptions: 1
ductions:
Hospital: $15.00
Other: $25.00
Special Deductions:
Hospital: none
Other: $10.00
Discussions
Discussions not available on http://www.google.ca/
Internet

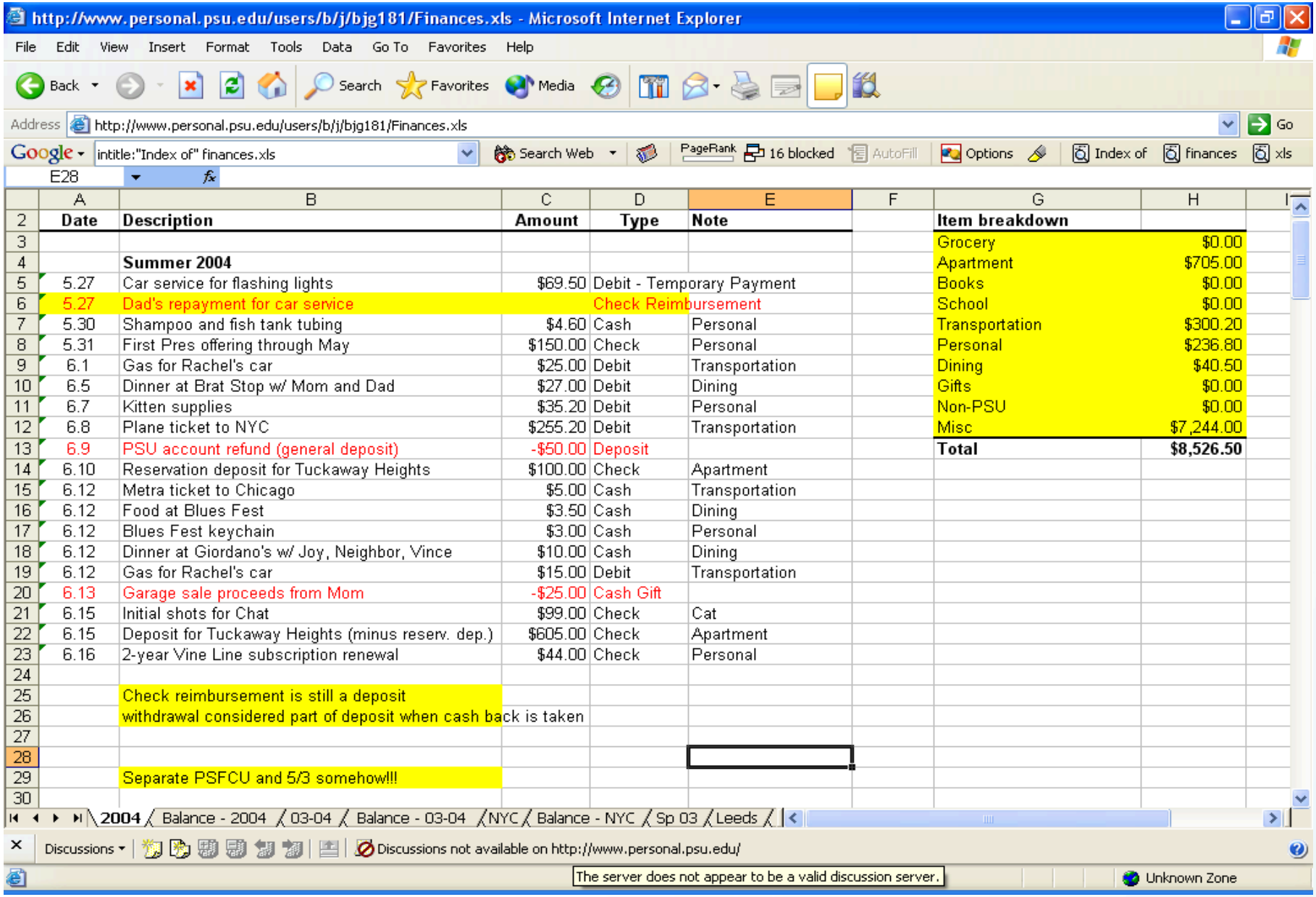
Google Hacking

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


http://www.google.ca/search?q=cache:120tViPs-0cJ: Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?q=cache:120tViPs-0cJ:www.cs.stedwards.edu/~lbaker/cisc1318/checkbook/register.xls+filetype:xls+%22checking+account%22+%22credit+c
Go Links
Google :king account" "credit card" -intext:application -intext:form
Search Web PageRank 11 blocked AutoFill Options checking account credit c
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
Discussions Discussions not available on http://www.google.ca/
Done
Internet

Google Hacking

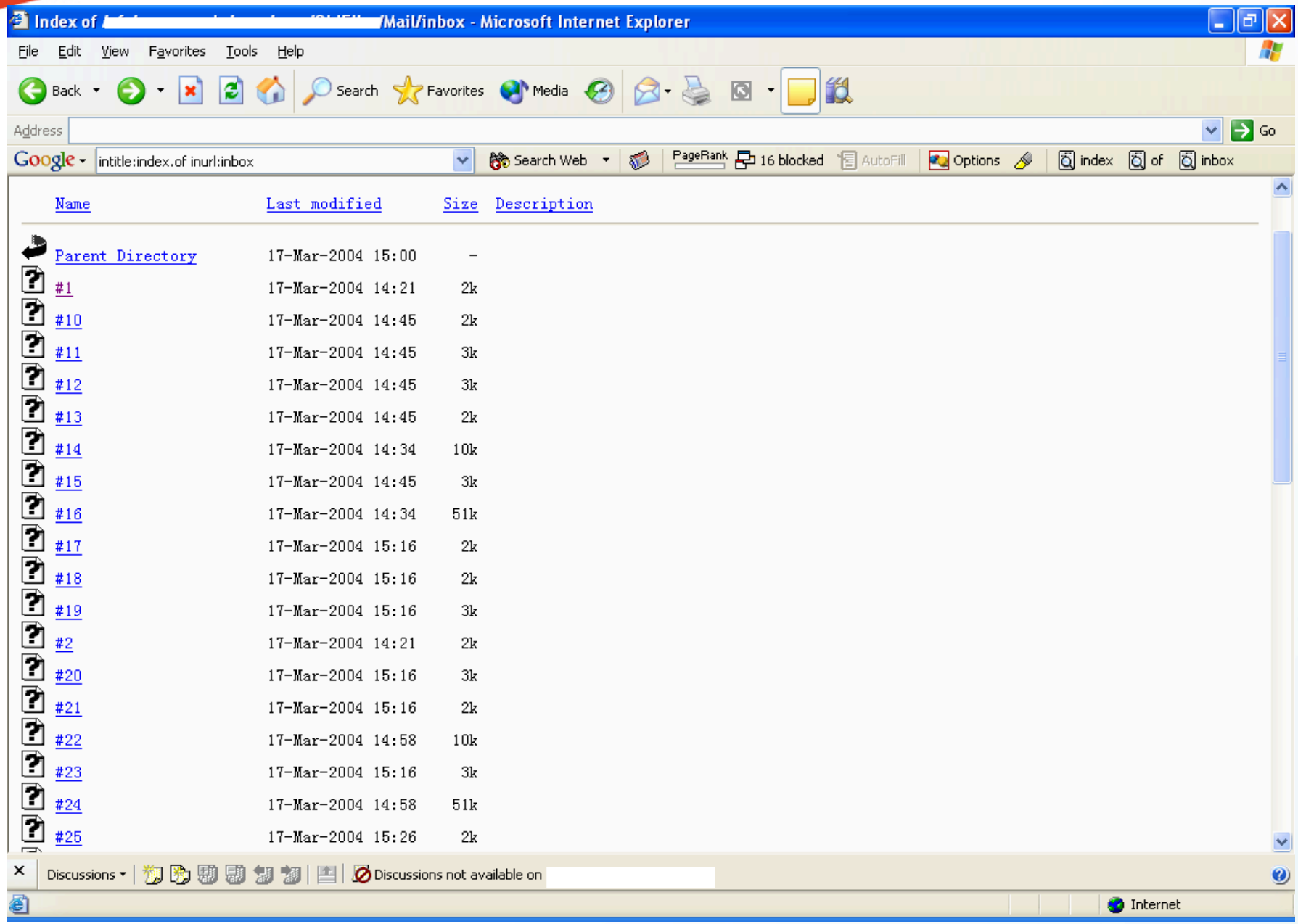
- Financial Information
  - Intitle: “Index of” finances.xls (9)



	A	B	C	D	E	F	G	H
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								

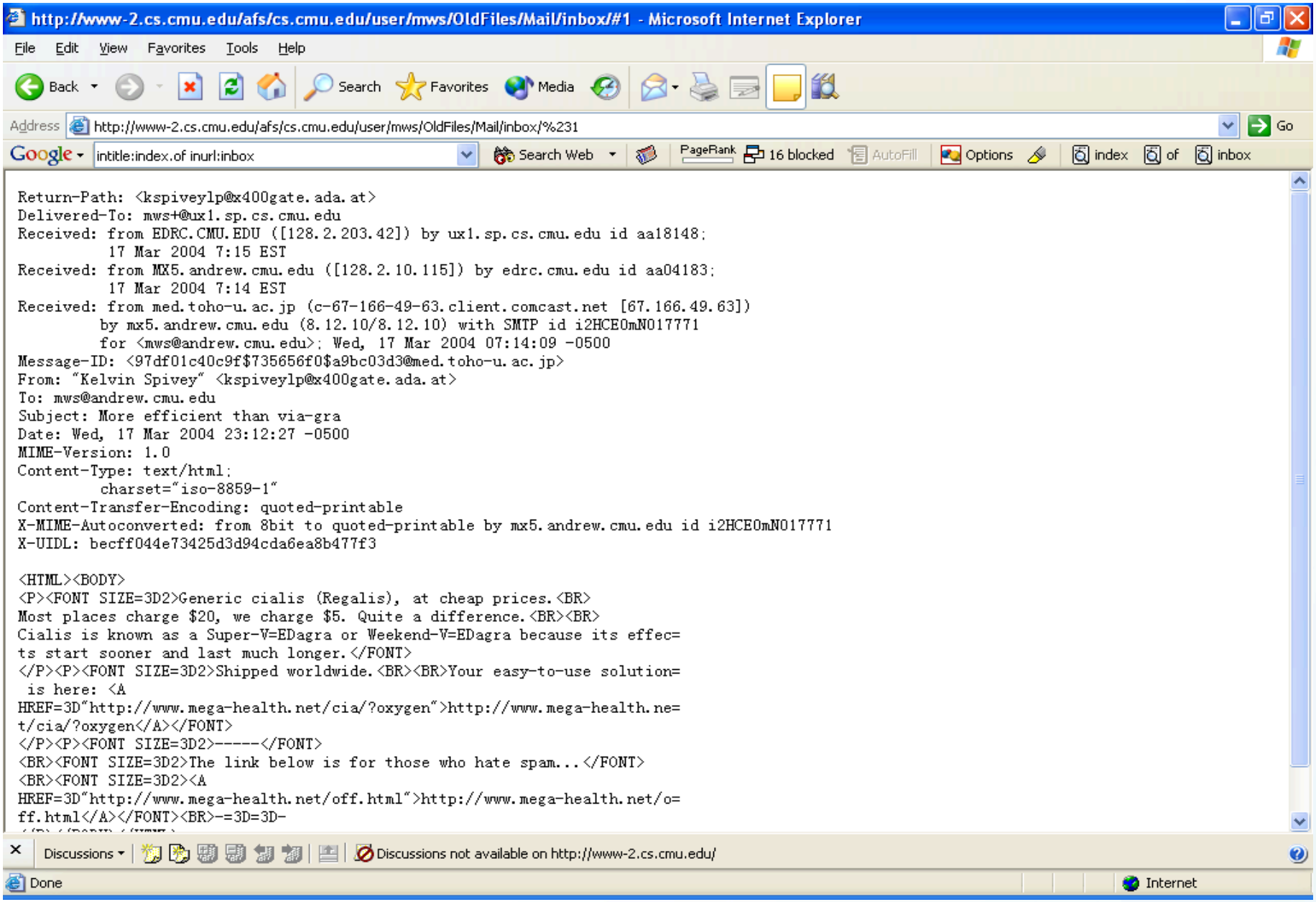
Google Hacking

- Personal Mailbox
  - Intitle: Index.of inurl: Inbox (456) (mit mailbox)


Index of [redacted]/Mail/inbox - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Google intitle:index.of inurl:inbox
Search Web PageRank 16 blocked AutoFill Options index of inbox
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
Discussions Discussions not available on
Internet

Google Hacking

- Personal Mailbox
  - After several clicks , got the private email messages


http://www-2.cs.cmu.edu/afs/cs.cmu.edu/user/mws/OldFiles/Mail/inbox/#1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www-2.cs.cmu.edu/afs/cs.cmu.edu/user/mws/OldFiles/Mail/inbox/%231
Go
Google intitle:index.of inurl:inbox
Search Web PageRank 16 blocked AutoFill Options index of inbox
Return-Path: <kspiveylp@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 aa18148;
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" <kspiveylp@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><FONT SIZE=3D2>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.</FONT>
</P><P><FONT SIZE=3D2>Shipped worldwide.

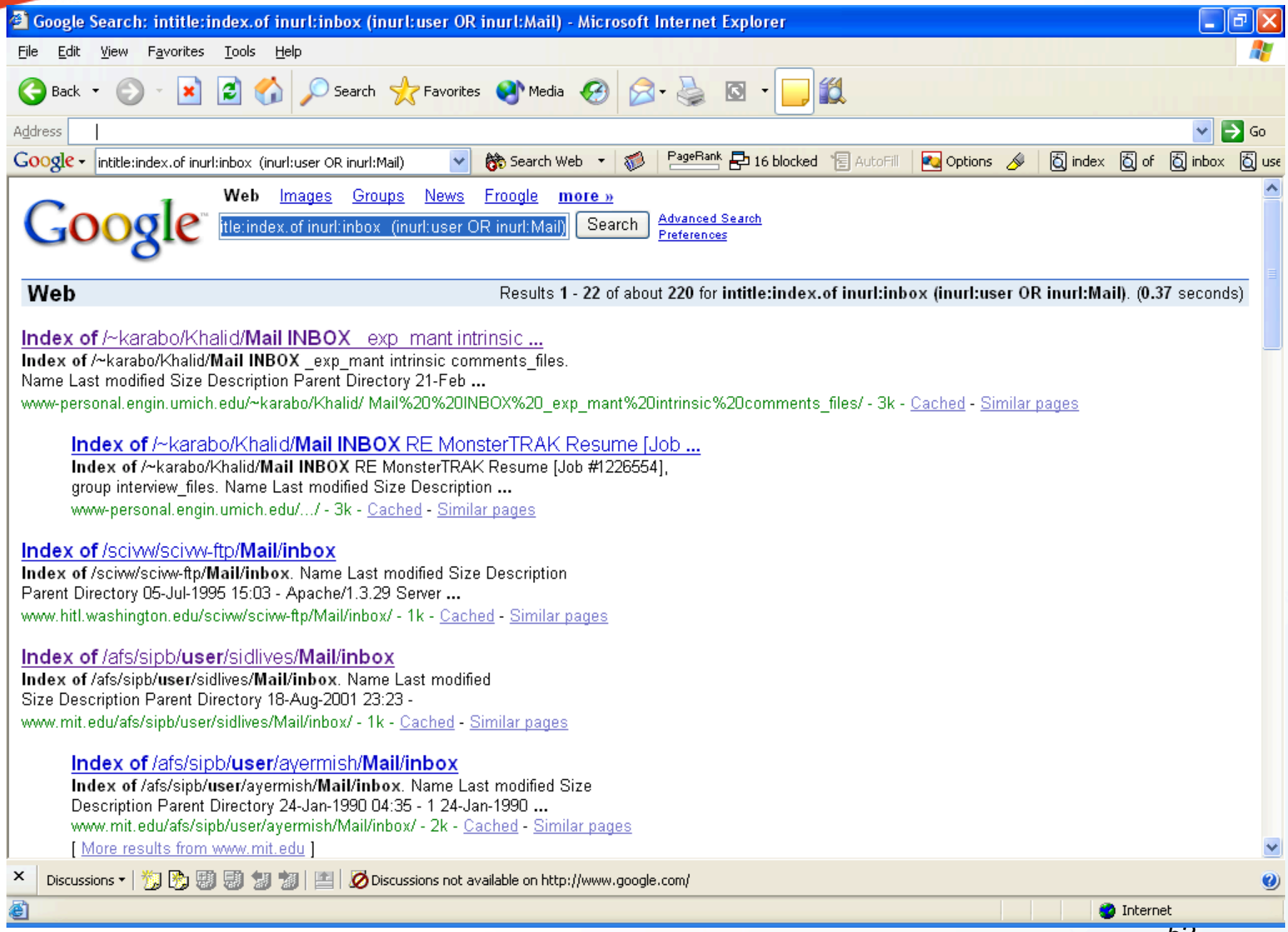
Your easy-to-use solution=
is here: <A
HREF=3D"http://www.mega-health.net/cia/?oxygen">http://www.mega-health.ne=
t/cia/?oxygen</A></FONT>
</P><P><FONT SIZE=3D2>-----</FONT>

<FONT SIZE=3D2>The link below is for those who hate spam...</FONT>

<FONT SIZE=3D2><A
HREF=3D"http://www.mega-health.net/off.html">http://www.mega-health.net/o=
ff.html</A></FONT>
-=3D=3D-
Discussions Discussions not available on http://www-2.cs.cmu.edu/
Done
Internet

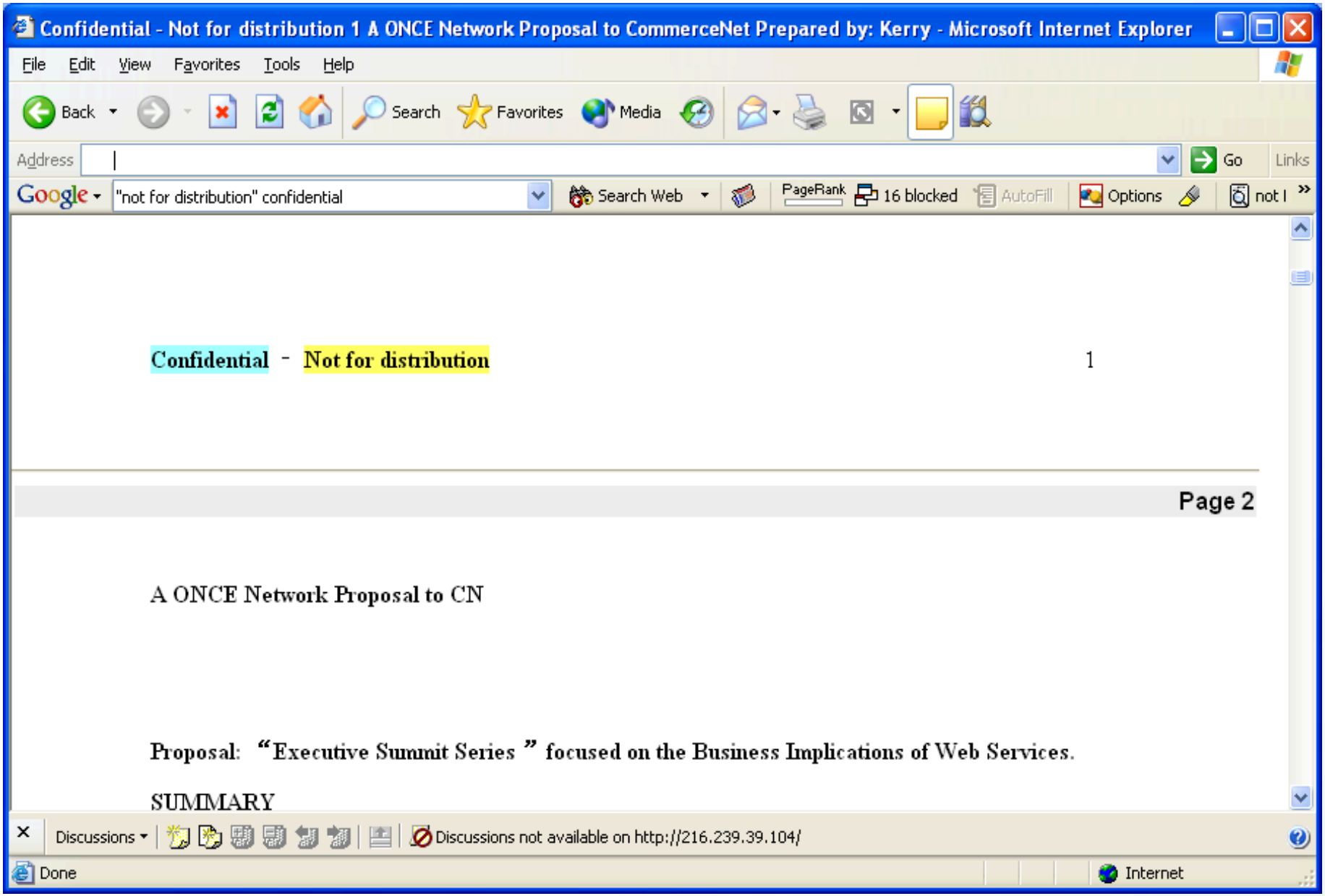
Google Hacking

- Personal Mailbox
  - Intitle: Index.of inurl: Inbox (inurl: User OR inurl: Mail) (220)


Google Search: intitle:index.of inurl:inbox (inurl:user OR inurl:Mail) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Google intitle:index.of inurl:inbox (inurl:user OR inurl:Mail)
Search Web PageRank 16 blocked AutoFill Options index of inbox use
Google
Web Images Groups News Froogle more »
tle:index.of inurl:inbox (inurl:user OR inurl:Mail)
Search
Advanced Search
Preferences
Web
Results 1 - 22 of about 220 for intitle:index.of inurl:inbox (inurl:user OR inurl:Mail). (0.37 seconds)
Index of /~karabo/Khalid/Mail INBOX exp mant intrinsic ...
Index of /~karabo/Khalid/Mail INBOX _exp_mant intrinsic comments_files.
Name Last modified Size Description Parent Directory 21-Feb ...
www-personal.engin.umich.edu/~karabo/Khalid/ Mail%20%20INBOX%20_exp_mant%20intrinsic%20comments_files/ - 3k - Cached - Similar pages
Index of /~karabo/Khalid/Mail INBOX RE MonsterTRAK Resume [Job ...
Index of /~karabo/Khalid/Mail INBOX RE MonsterTRAK Resume [Job #1226554],
group interview_files. Name Last modified Size Description ...
www-personal.engin.umich.edu/.../ - 3k - Cached - Similar pages
Index of /sciww/sciww-ftp/Mail/inbox
Index of /sciww/sciww-ftp/Mail/inbox. Name Last modified Size Description
Parent Directory 05-Jul-1995 15:03 - Apache/1.3.29 Server ...
www.hitl.washington.edu/sciww/sciww-ftp/Mail/inbox/ - 1k - Cached - Similar pages
Index of /afs/sipb/user/sidlives/Mail/inbox
Index of /afs/sipb/user/sidlives/Mail/inbox. Name Last modified
Size Description Parent Directory 18-Aug-2001 23:23 -
www.mit.edu/afs/sipb/user/sidlives/Mail/inbox/ - 1k - Cached - Similar pages
Index of /afs/sipb/user/ayermish/Mail/inbox
Index of /afs/sipb/user/ayermish/Mail/inbox. Name Last modified Size
Description Parent Directory 24-Jan-1990 04:35 - 1 24-Jan-1990 ...
www.mit.edu/afs/sipb/user/ayermish/Mail/inbox/ - 2k - Cached - Similar pages
[More results from www.mit.edu]
Discussions
Discussions not available on http://www.google.com/
Internet

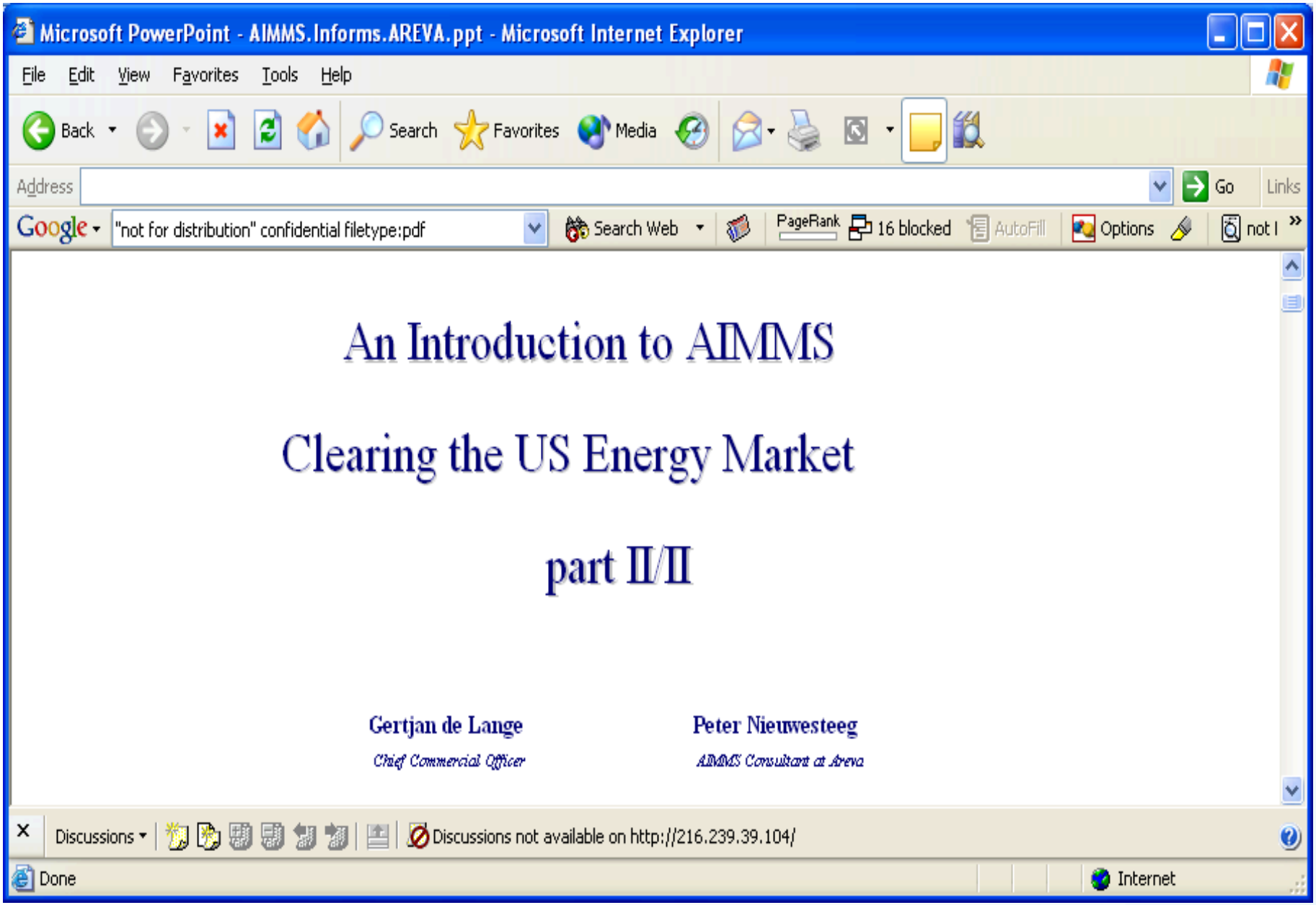
Google Hacking

- Confidential Files
  - “not for distribution” confidential (1,760)


Confidential - Not for distribution 1 A ONCE Network Proposal to CommerceNet Prepared by: Kerry - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "not for distribution" confidential
Search Web PageRank 16 blocked AutoFill Options not I
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
Discussions Discussions not available on http://216.239.39.104/
Done
Internet

Google Hacking

- Confidential Files
  - “not for distribution” confidential filetype: pdf (marketing info) (456)

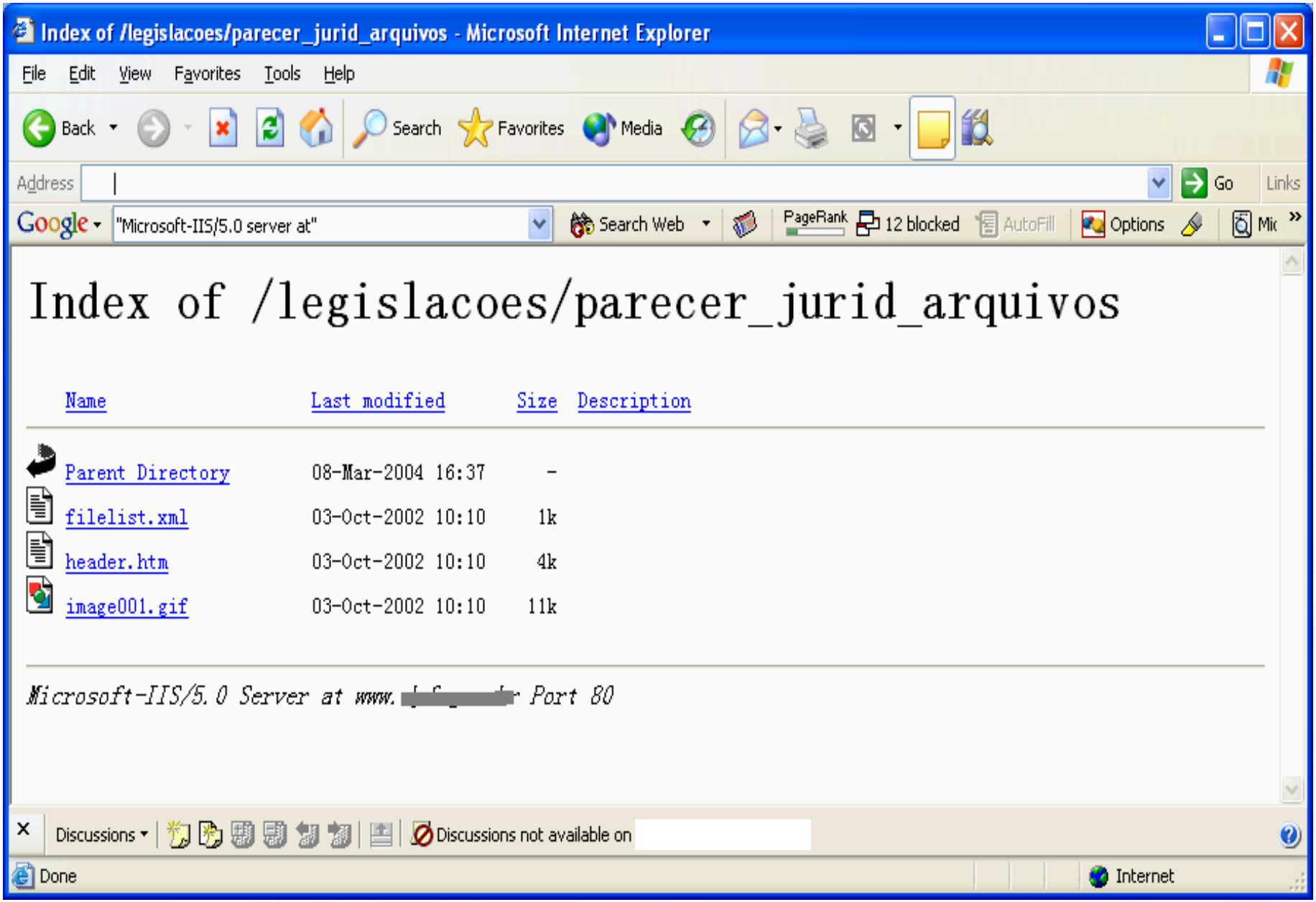

Microsoft PowerPoint - AIMMS.Informs.AREVA.ppt - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address Go Links
Google "not for distribution" confidential filetype:pdf Search Web PageRank 16 blocked AutoFill Options not I
An Introduction to AIMMS
Clearing the US Energy Market
part II/II
Gertjan de Lange
Chief Commercial Officer
Peter Nieuwesteeg
AIMMS Consultant at Areva
Discussions Discussions not available on http://216.239.39.104/
Done
Internet

Google Hacking

- OS Detection
- Use the keywords of the default installation page of a Web server to search.
- Use the title to search
- Use the footer in a directory index page

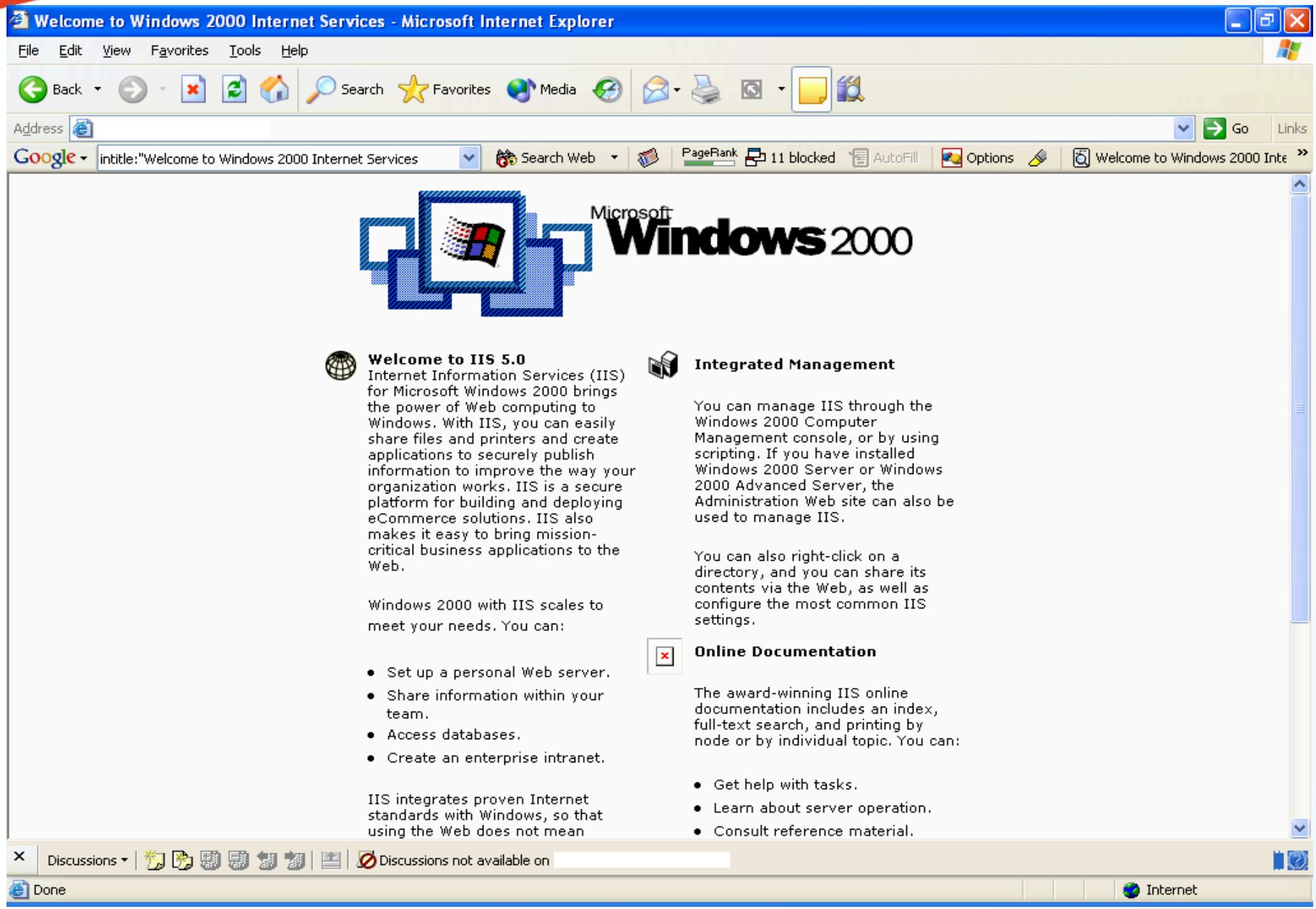
Google Hacking

- OS Detection-Windows
  - "Microsoft-IIS/5.0 server at"


Index of /legislacoes/parecer_jurid_arquivos - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "Microsoft-IIS/5.0 server at"
Search Web PageRank 12 blocked AutoFill Options
Index of /legislacoes/parecer_jurid_arquivos
Name Last modified Size Description
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. Port 80
Discussions Discussions not available on
Done
Internet

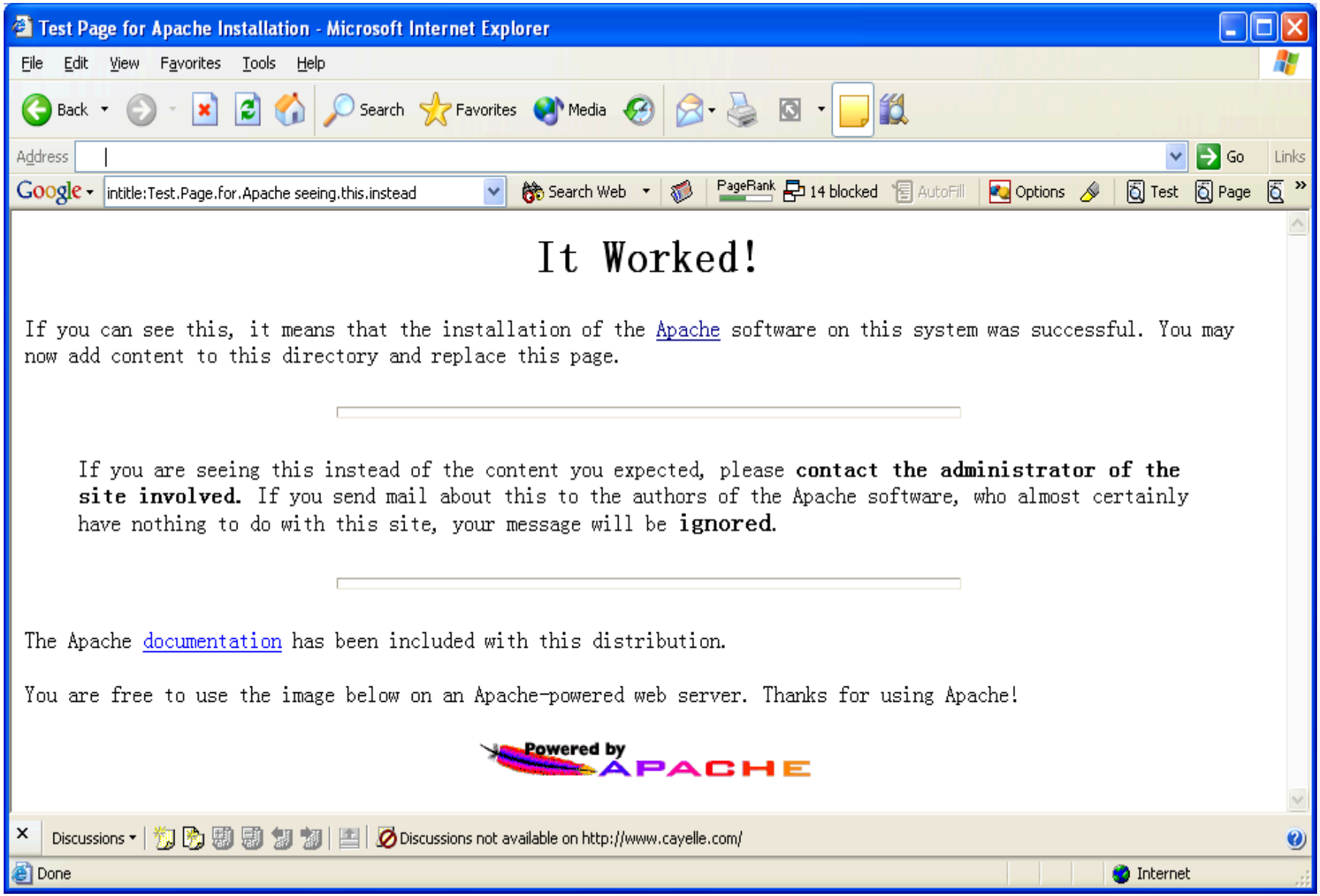
Google Hacking

- OS Detection - Windows
  - Default web page?
  - Intitle: “Welcome to Windows 2000 Internet Services”


Welcome to Windows 2000 Internet Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google intitle:"Welcome to Windows 2000 Internet Services
Search Web PageRank 11 blocked AutoFill Options Welcome to Windows 2000 Inte
Microsoft Windows 2000
Welcome to IIS 5.0
Internet Information Services (IIS) for Microsoft Windows 2000 brings the power of Web computing to Windows. With IIS, you can easily share files and printers and create applications to securely publish information to improve the way your organization works. IIS is a secure platform for building and deploying eCommerce solutions. IIS also makes it easy to bring mission-critical business applications to the Web.
Windows 2000 with IIS scales to meet your needs. You can:
Set up a personal Web server.
Share information within your team.
Access databases.
Create an enterprise intranet.
IIS integrates proven Internet standards with Windows, so that using the Web does not mean
Integrated Management
You can manage IIS through the Windows 2000 Computer Management console, or by using scripting. If you have installed Windows 2000 Server or Windows 2000 Advanced Server, the Administration Web site can also be used to manage IIS.
You can also right-click on a directory, and you can share its contents via the Web, as well as configure the most common IIS settings.
Online Documentation
The award-winning IIS online documentation includes an index, full-text search, and printing by node or by individual topic. You can:
Get help with tasks.
Learn about server operation.
Consult reference material.
Discussions Discussions not available on
Done
Internet

Google Hacking

- OS Detection –Apache 1.3.11-1.3.26
  - Intitle: Test.Page.for.Apache seeing.this.instead


Test Page for Apache Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google intitle:Test.Page.for.Apache seeing.this.instead
Search Web PageRank 14 blocked AutoFill Options Test Page
It Worked!
If you can see this, it means that the installation of the Apache software on this system was successful. You may now add content to this directory and replace this page.
If you are seeing this instead of the content you expected, please contact the administrator of the site involved. If you send mail about this to the authors of the Apache software, who almost certainly have nothing to do with this site, your message will be ignored.
The Apache documentation has been included with this distribution.
You are free to use the image below on an Apache-powered web server. Thanks for using Apache!
Powered by APACHE
Discussions
Discussions not available on http://www.cayelle.com/
Done
Internet

Google Hacking

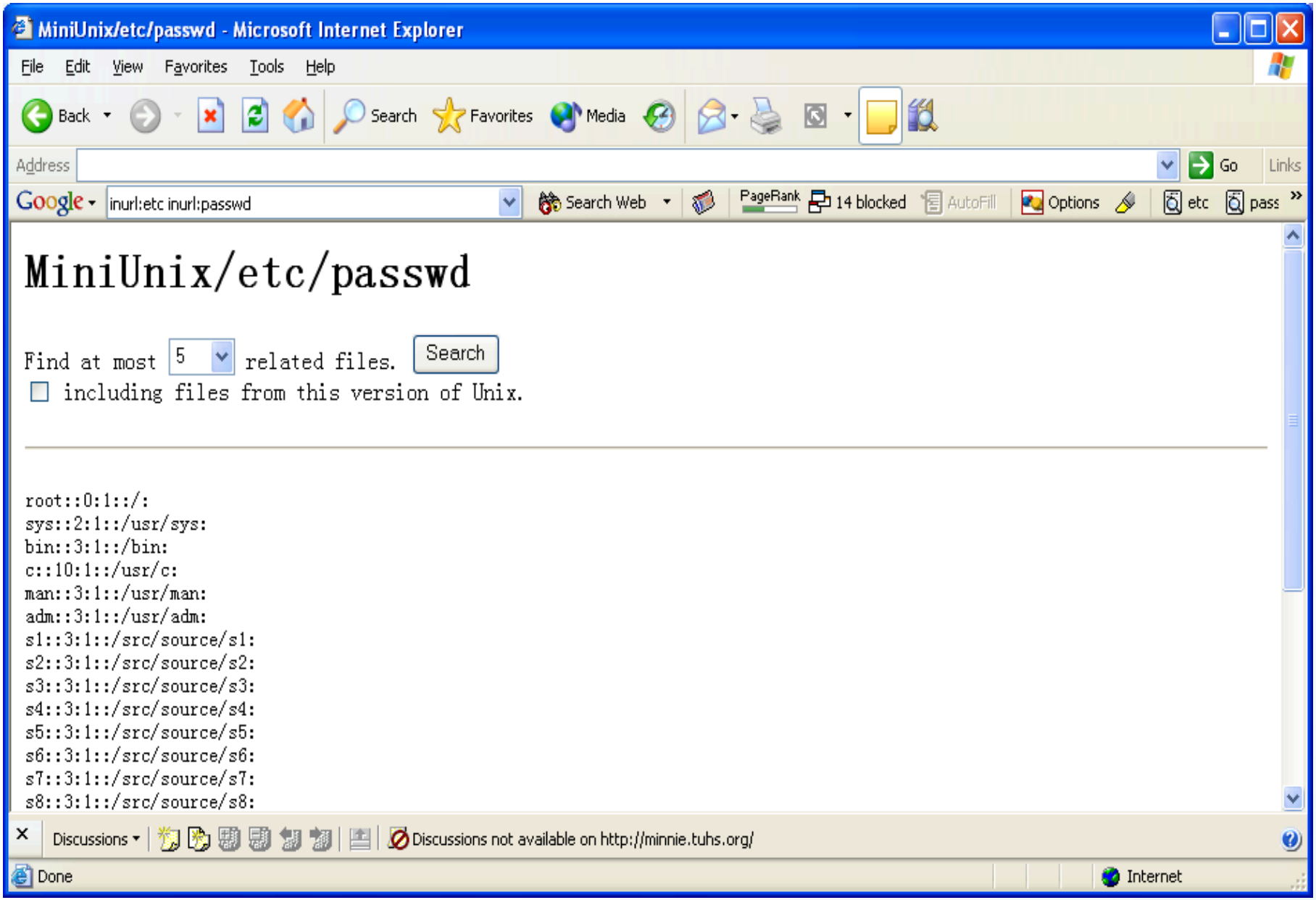
- OS Detection-Apache SSL enable
  - Intitle: Test.page “SSL/TLS-aware” (127)

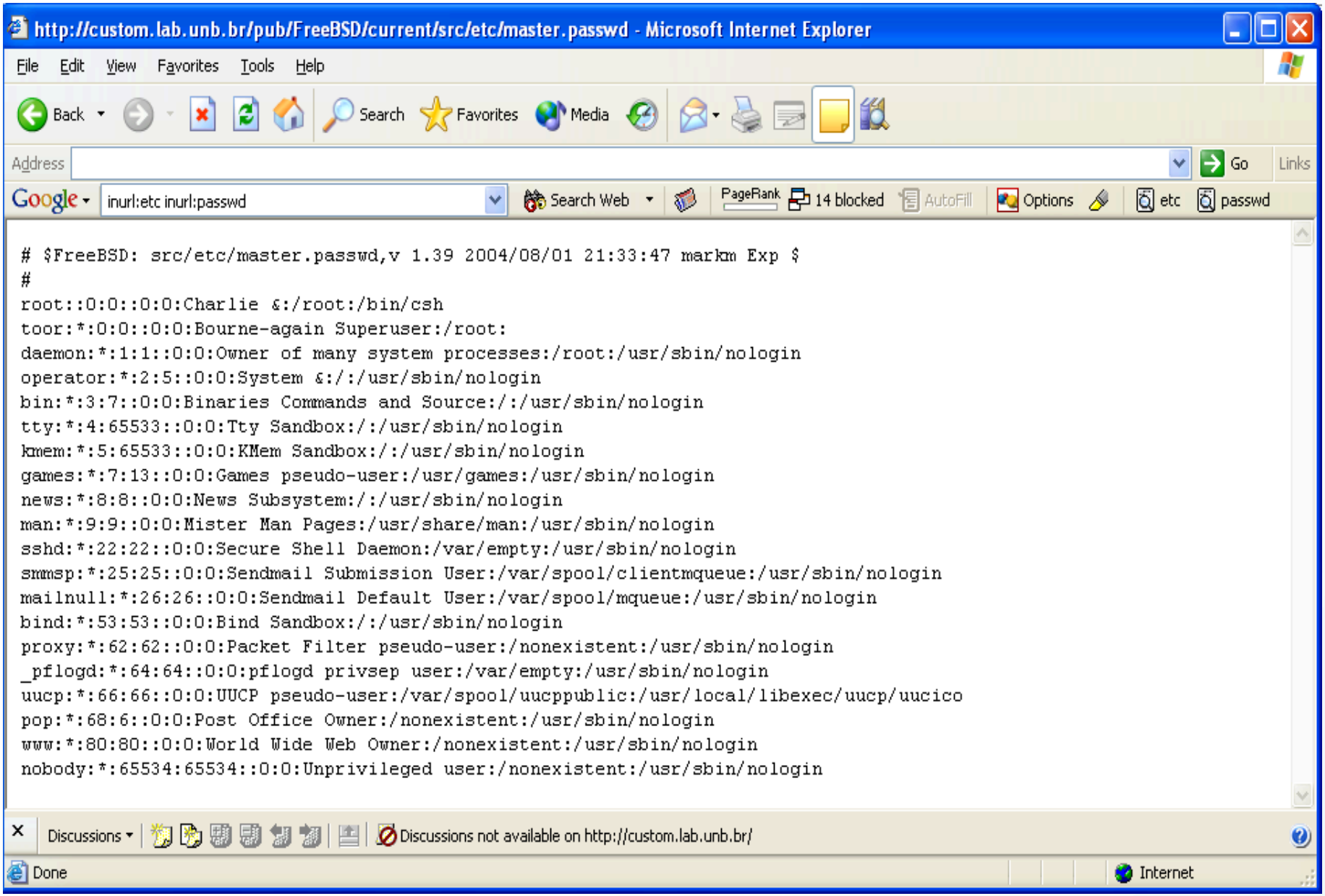

wow my Test Page for the SSL/TLS-aware Apache Installation on Web Site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google intitle:test.page "SSL/TLS-aware"
Search Web PageRank 14 blocked AutoFill Options test page
Hey, it worked !
The SSL/TLS-aware Apache webserver was successfully installed on this website.
If you can see this page, then the people who own this website have just installed the Apache Web server software and the Apache Interface to OpenSSL (mod_ssl) successfully. They now have to add content to this directory and replace this placeholder page, or else point the server at their real content.
ATTENTION!
If you are seeing this page instead of the site you expected, please contact the administrator of the site involved. (Try sending mail to <webmaster@domain>.)
Although this site is running the Apache software it almost certainly has no other connection to the Apache Group, so please do not send mail about this site or its contents to the Apache authors. If you do, your message will be ignored.
The Apache online documentation has been included with this distribution.
Especially also read the mod_ssl User Manual carefully.
Your are allowed to use the images below on your SSL-aware Apache Web server.
Discussions
Discussions not available on http://ww3.freebsddiary.org/
Done
Internet

Google Hacking

- Search Passwords
  - Search the well known password filenames in URL
  - Search the database connection files or configuration files to find a password and username
  - Search specific username file for a specific product

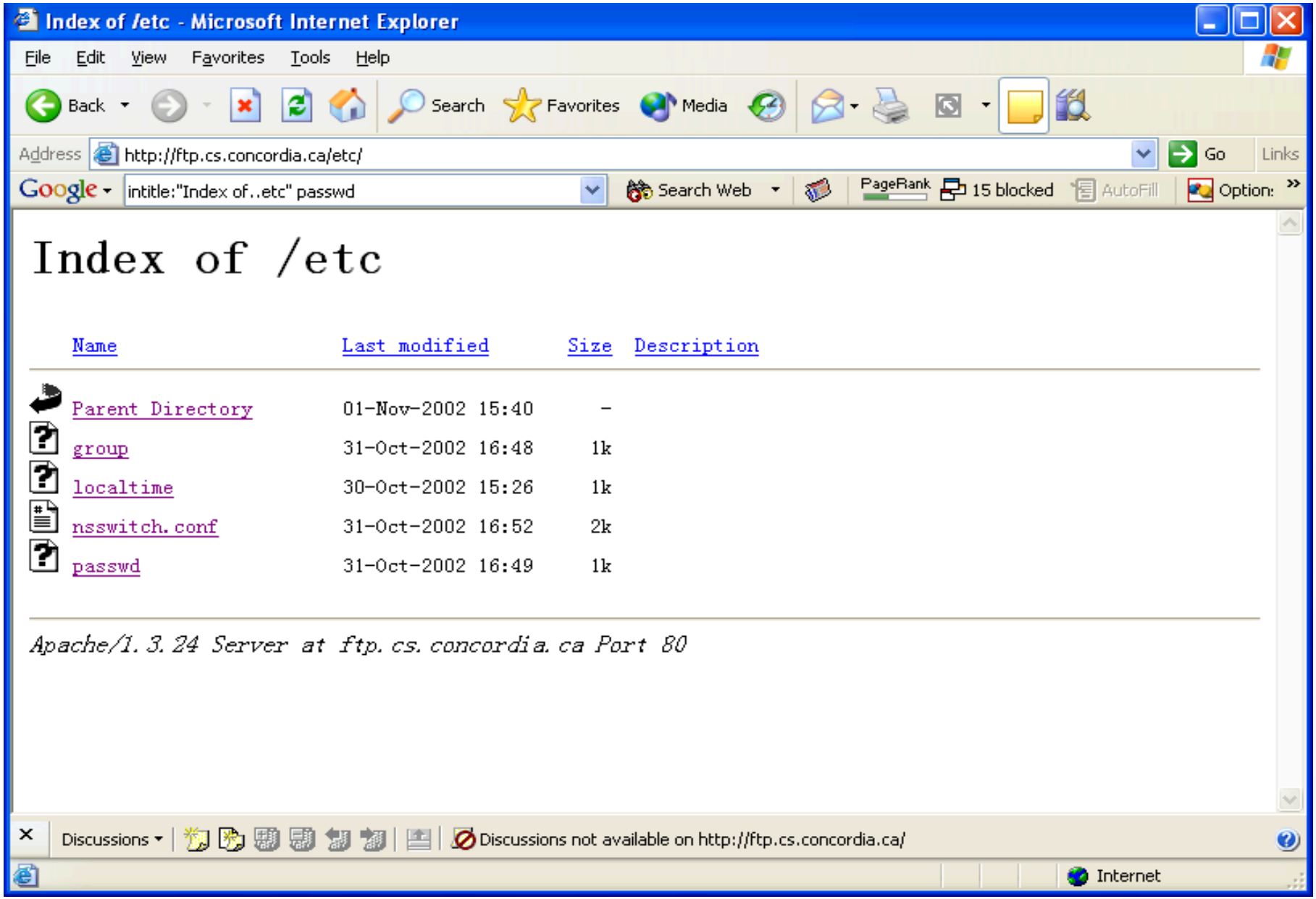
- Search Passwords
  - Inurl: etc inurl: passwd


MiniUnix/etc/passwd - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google inurl:etc inurl:passwd
Search Web PageRank 14 blocked AutoFill Options etc pass
MiniUnix/etc/passwd
Find at most 5 related files. Search
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:
Discussions
Discussions not available on http://minnie.tuhs.org/
Done
Internet


http://custom.lab.unb.br/pub/FreeBSD/current/src/etc/master.passwd - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google inurl:etc inurl:passwd
Search Web PageRank 14 blocked AutoFill Options etc passwd
$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
_pflogd:*:64:64::0:0:pflogd 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
Discussions Discussions not available on http://custom.lab.unb.br/
Done
Internet

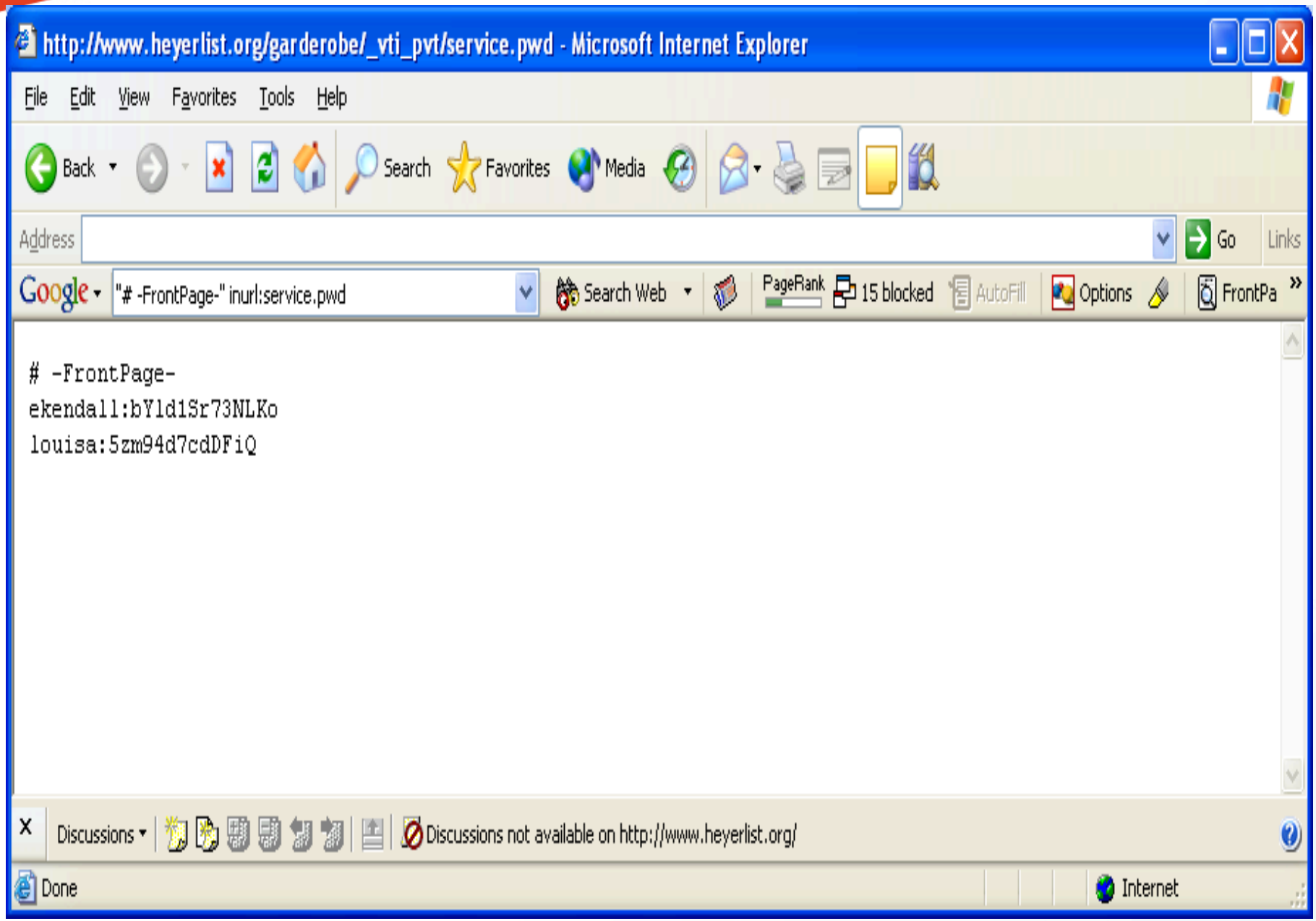
Google Hacking

- Search Passwords
  - Intitle: “Index of..etc” passwd


Index of /etc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back 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
Name Last modified Size Description
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

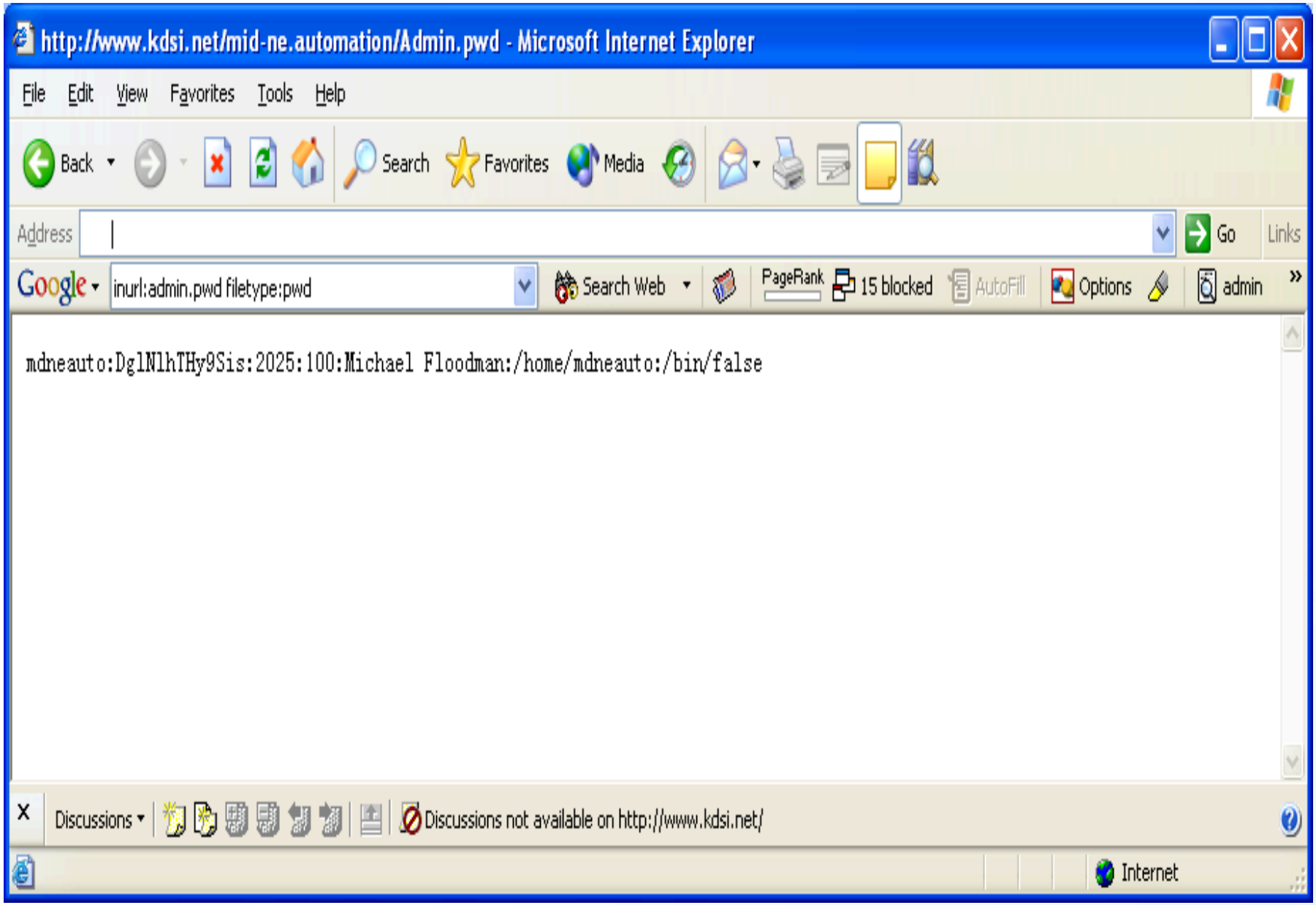
Google Hacking

- Search Passwords
  - "# -FrontPage-" inurl: service.pwd (then crack it)


http://www.heyerlist.org/garderobe/_vti_pvt/service.pwd - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "# -FrontPage-" inurl:service.pwd
Search Web PageRank 15 blocked AutoFill Options FrontPa
-FrontPage-
ekendall:bYld1Sr73NLKo
louisa:5zm94d7cdDFiQ
Discussions Discussions not available on http://www.heyerlist.org/
Done
Internet

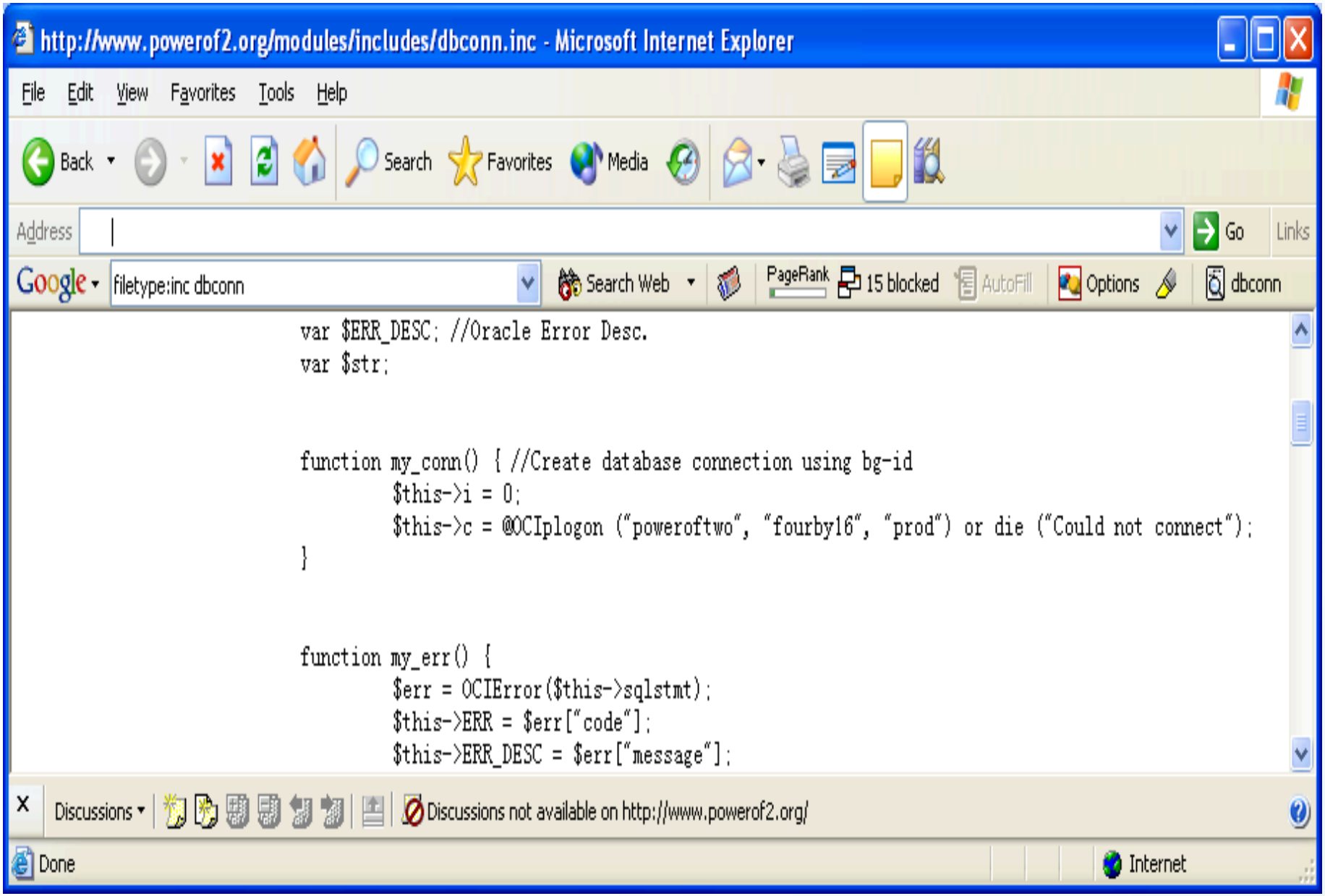
Google Hacking

- Search Passwords
  - Inurl: admin.pwd filetype: pwd


http://www.kdsi.net/mid-ne.automation/Admin.pwd - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google inurl:admin.pwd filetype:pwd
Search Web PageRank 15 blocked AutoFill Options admin
mdneauto:DglNlhTHy9Sis:2025:100:Michael Floodman:/home/mdneauto:/bin/false
Discussions
Discussions not available on http://www.kdsi.net/
Internet

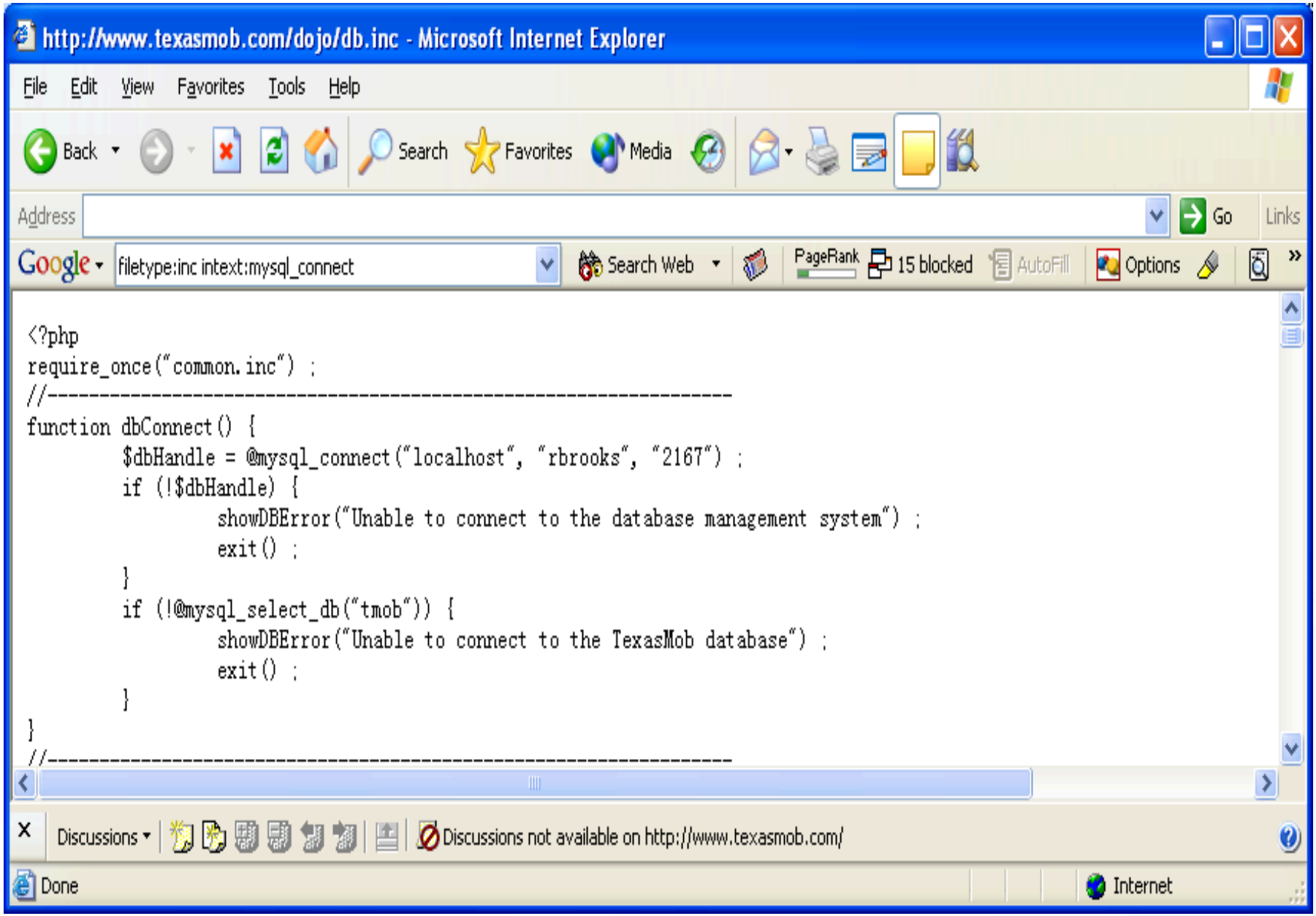
Google Hacking

- Search Passwords
  - Filetype: inc dbconn


http://www.powerof2.org/modules/includes/dbconn.inc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google filetype:inc dbconn
Search Web PageRank 15 blocked AutoFill Options 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"];
Discussions
Discussions not available on http://www.powerof2.org/
Done
Internet

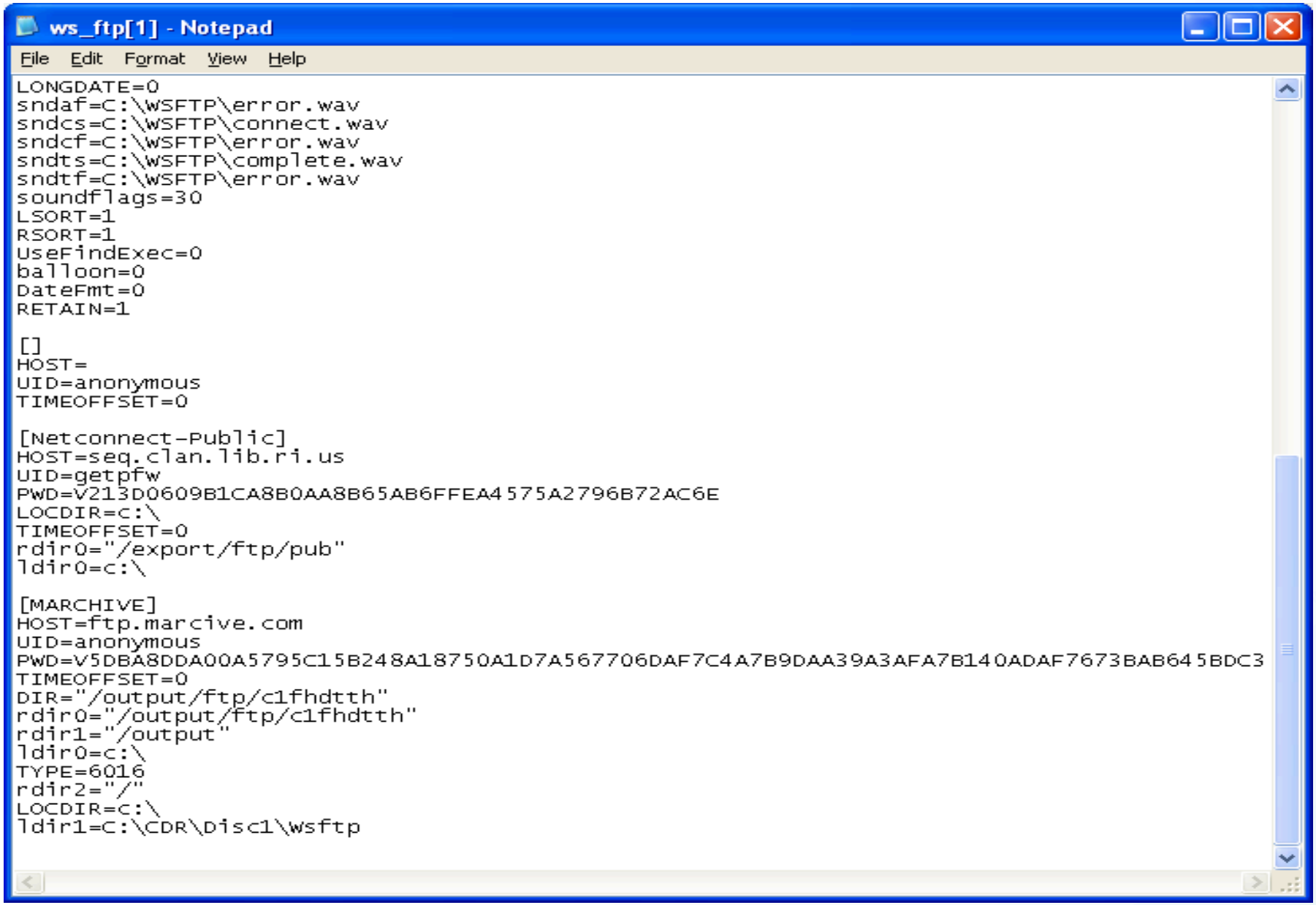
Google Hacking

- Search Passwords
  - Filetype: inc intext: mysql_connect


http://www.texasmob.com/dojo/db.inc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google filetype:inc intext:mysql_connect
Search Web PageRank 15 blocked AutoFill Options
<?php
require_once("common.inc") ;
//--
function dbConnect() {
$dbHandle = @mysql_connect("localhost", "rbrooks", "2167") ;
if (!$dbHandle) {
showDBError("Unable to connect to the database management system") ;
exit() ;
}
if (!@mysql_select_db("tmob")) {
showDBError("Unable to connect to the TexasMob database") ;
exit() ;
}
}
//--
Discussions
Discussions not available on http://www.texasmob.com/
Done
Internet

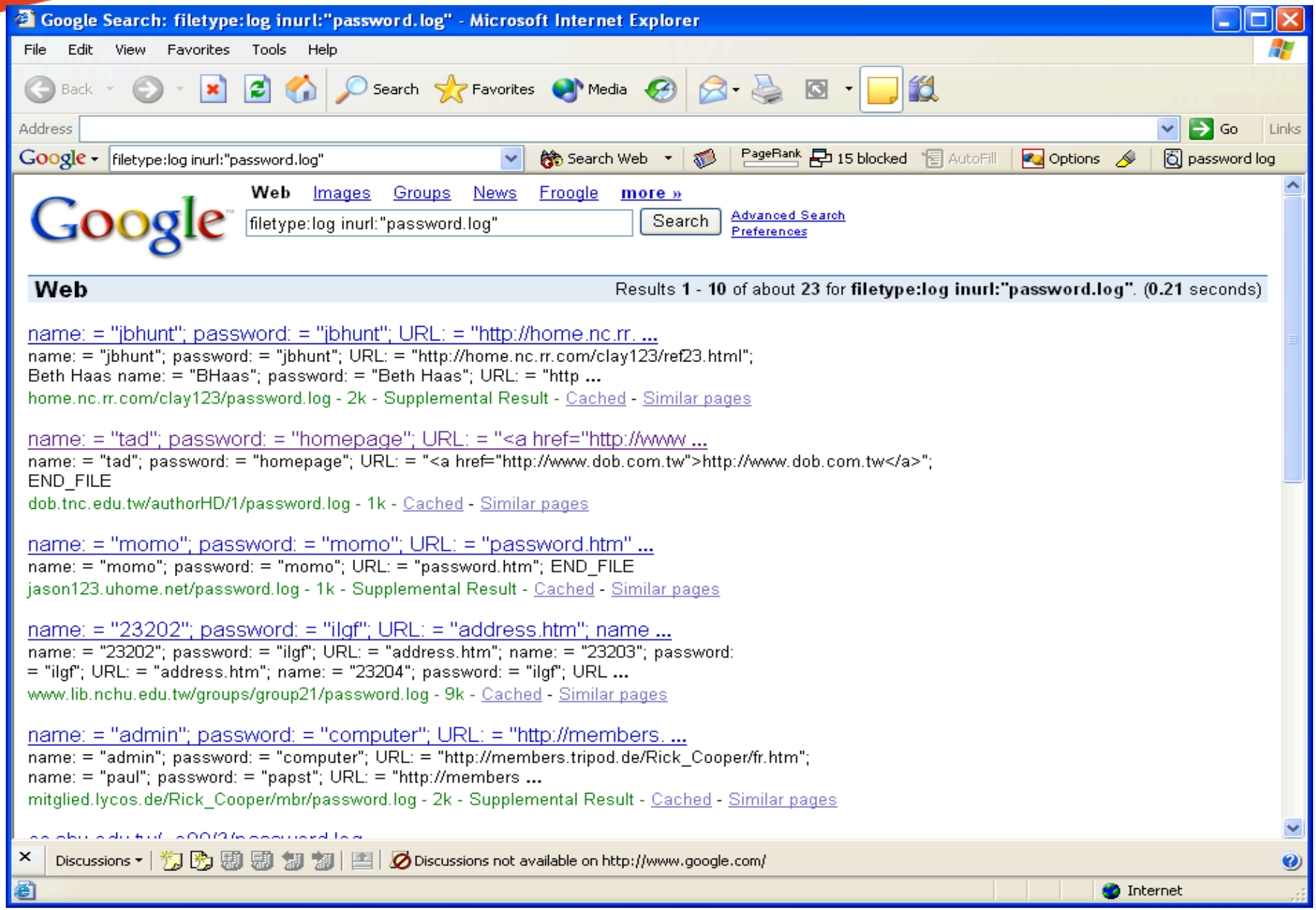
Google Hacking

- Search Passwords
  - Filetype: ini +ws_ftp +pwd (get the encrypted passwords)


ws_ftp[1] - Notepad
File Edit Format View Help
LONGDATE=0
sndaf=C:\WSFTP\error.wav
sndcs=C:\WSFTP\connect.wav
sndcf=C:\WSFTP\error.wav
sndts=C:\WSFTP\complete.wav
sndtf=C:\WSFTP\error.wav
soundflags=30
LSORT=1
RSORT=1
UseFindExec=0
balloon=0
DateFmt=0
RETAIN=1
[]
HOST=
UID=anonymous
TIMEOFFSET=0
[Netconnect-Public]
HOST=seq.clan.lib.ri.us
UID=getpfw
PWD=V213D0609B1CA8B0AA8B65AB6FFEA4575A2796B72AC6E
LOCDIR=c:\
TIMEOFFSET=0
rdir0="/export/ftp/pub"
ldir0=c:\
[MARCHIVE]
HOST=ftp.marcive.com
UID=anonymous
PWD=V5DBA8DDA00A5795C15B248A18750A1D7A567706DAF7C4A7B9DAA39A3AFA7B140ADAF7673BAB645BDC3
TIMEOFFSET=0
DIR="/output/ftp/c1fhdtth"
rdir0="/output/ftp/c1fhdtth"
rdir1="/output"
ldir0=c:\
TYPE=6016
rdir2="/"
LOCDIR=c:\
ldir1=C:\CDR\Disc1\wsftp

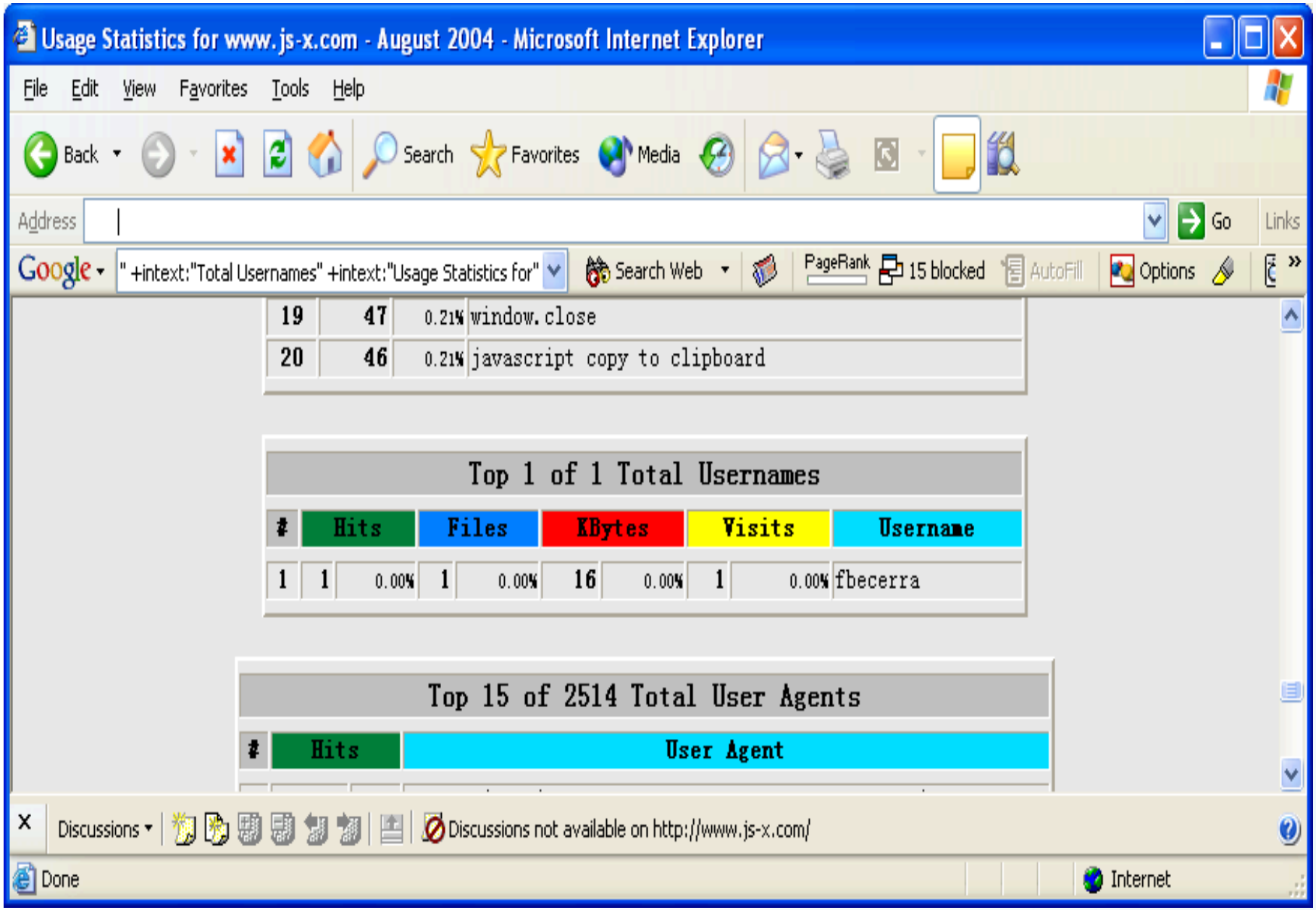
Google Hacking

- Search Passwords
  - Filetype: log inurl: “password.log”


Google Search: filetype:log inurl:"password.log" - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google filetype:log inurl:"password.log"
Search Web PageRank 15 blocked AutoFill Options password log
Google
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
Discussions
Discussions not available on http://www.google.com/
Internet

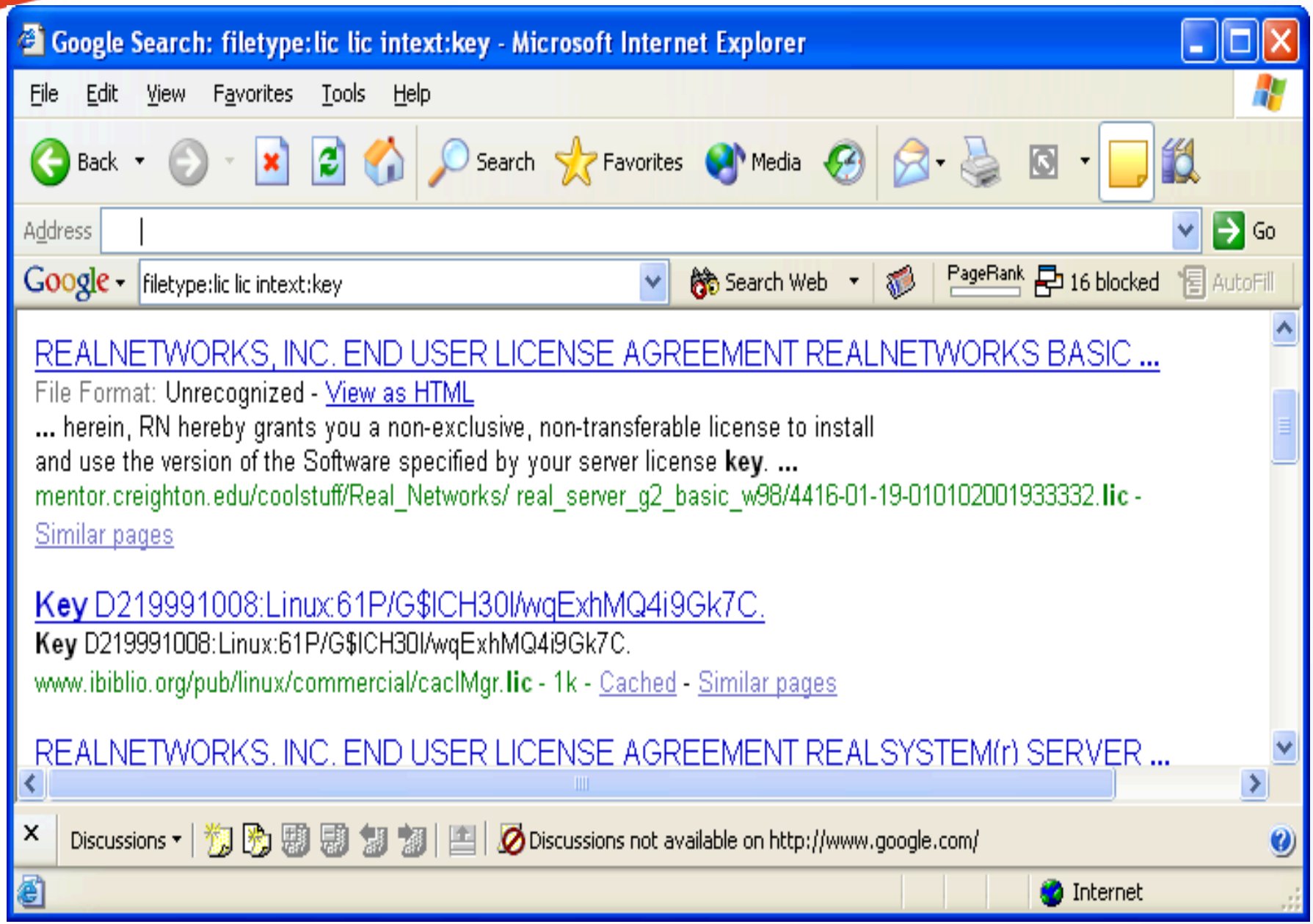
Google Hacking

- Search Username
  - +intext: "webalizer" +intext: “Total Usernames” +intext: “Usage Statistics for”


Usage Statistics for www.js-x.com - August 2004 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google " +intext:"Total Usernames" +intext:"Usage Statistics for" Search Web PageRank 15 blocked AutoFill Options
19 47 0.21% window.close
20 46 0.21% javascript copy to clipboard
Top 1 of 1 Total Usernames
Hits Files KBytes Visits Username
1 1 0.00% 1 0.00% 16 0.00% 1 0.00% fbecerra
Top 15 of 2514 Total User Agents
Hits User Agent
Discussions
Discussions not available on http://www.js-x.com/
Done
Internet

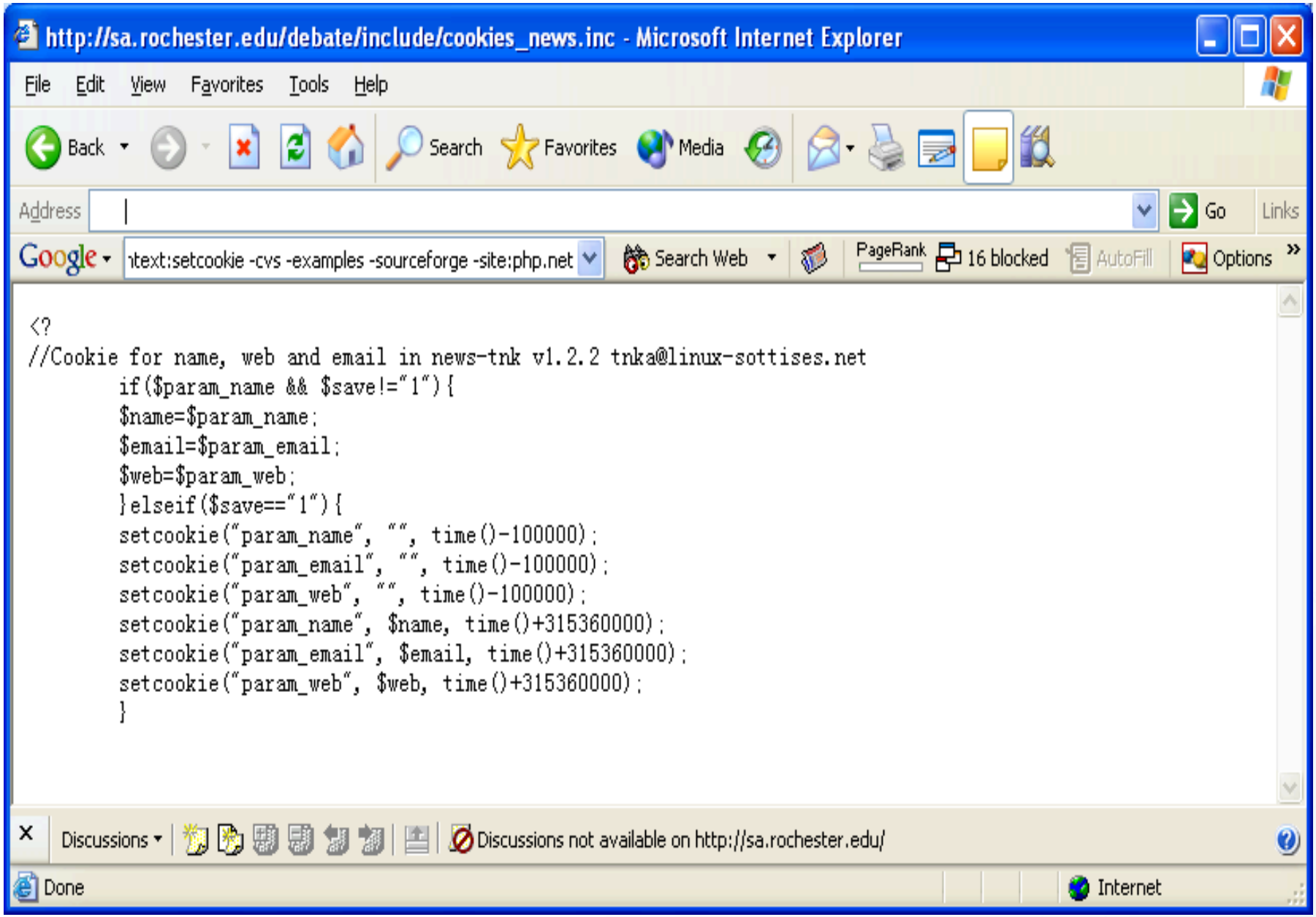
Google Hacking

- License Key
  - Filetype: lic lic intext: key (33) (license key)


Google Search: filetype:lic lic intext:key - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Google filetype:lic lic intext:key
Search Web PageRank 16 blocked AutoFill
REALNETWORKS, INC. END USER LICENSE AGREEMENT REALNETWORKS BASIC ...
File Format: Unrecognized - View as HTML
... herein, RN hereby grants you a non-exclusive, non-transferable license to install and use the version of the Software specified by your server license key. ...
mentor.creighton.edu/coolstuff/Real_Networks/ real_server_g2_basic_w98/4416-01-19-010102001933332.lic - Similar pages
Key D219991008:Linux:61P/G$ICH30l/wqExhMQ4i9Gk7C.
Key D219991008:Linux:61P/G$ICH30l/wqExhMQ4i9Gk7C.
www.ibiblio.org/pub/linux/commercial/caclMgr.lic - 1k - Cached - Similar pages
REALNETWORKS, INC. END USER LICENSE AGREEMENT REALSYSTEM(r) SERVER ...
Discussions
Discussions not available on http://www.google.com/
Internet

Google Hacking

- Cookies Syntax
  - Filetype: inc inc intext: setcookie -cvs -examples -sourceforge -site: php.net (120) (cookie schema)

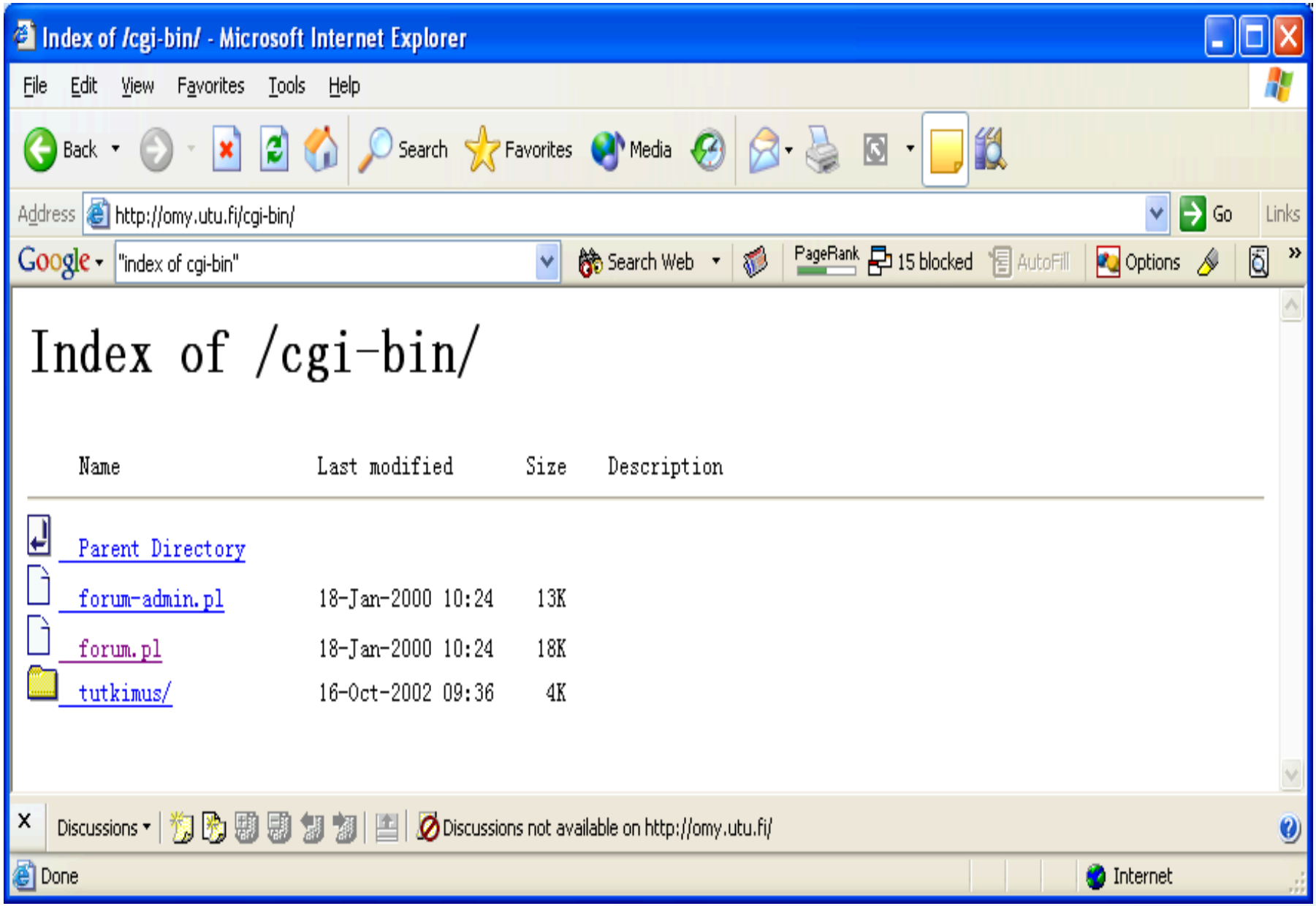

http://sa.rochester.edu/debate/include/cookies_news.inc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google
text:setcookie -cvs -examples -sourceforge -site:php.net
Search Web
PageRank
16 blocked
AutoFill
Options
<?
//Cookie for name, 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);
}
Discussions
Discussions not available on http://sa.rochester.edu/
Done
Internet

Google Hacking

- Sensitive Directories Listing
  - Powerful buzz word: Index of
  - Search the well known vulnerable directories names

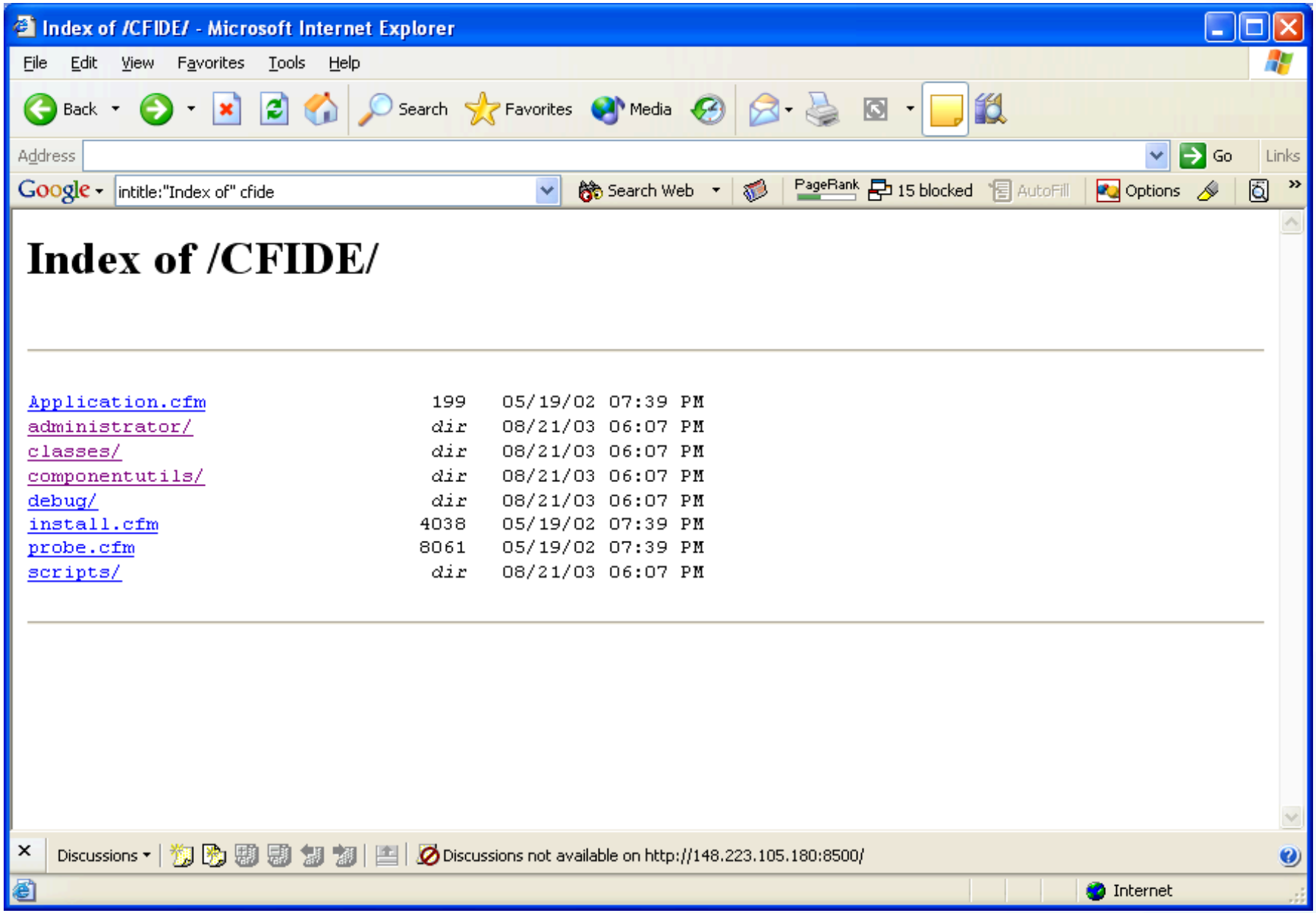
Google Hacking

- Sensitive Directories Listing
  - "index of cgi-bin" (3590)


Index of /cgi-bin/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
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

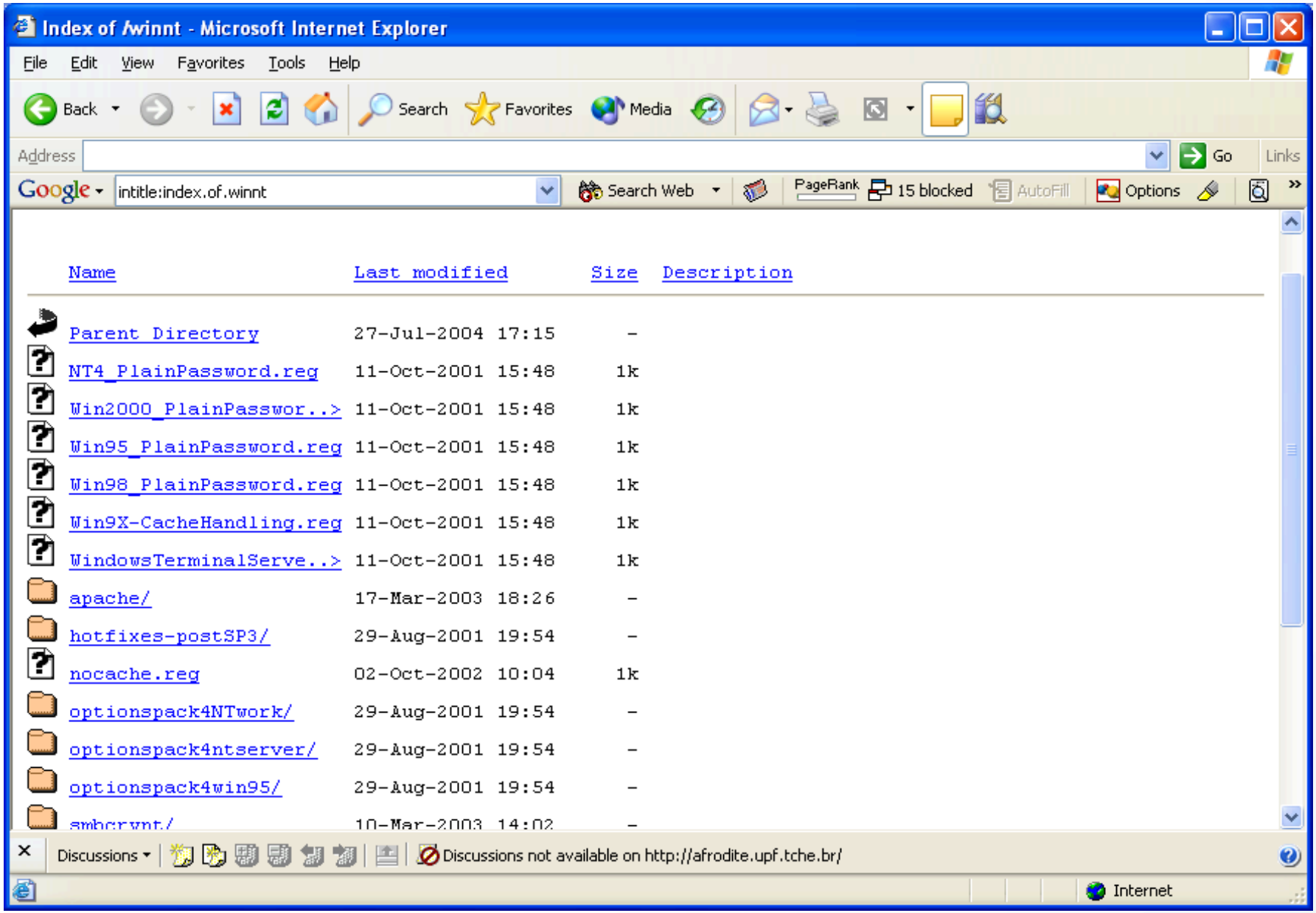
Google Hacking

- Sensitive Directories Listing
  - Intitle: “Index of” cfide (coldfusion directory)


Index of /CFIDE/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google intitle:"Index of" cfide
Search Web PageRank 15 blocked AutoFill Options
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
Discussions
Discussions not available on http://148.223.105.180:8500/
Internet

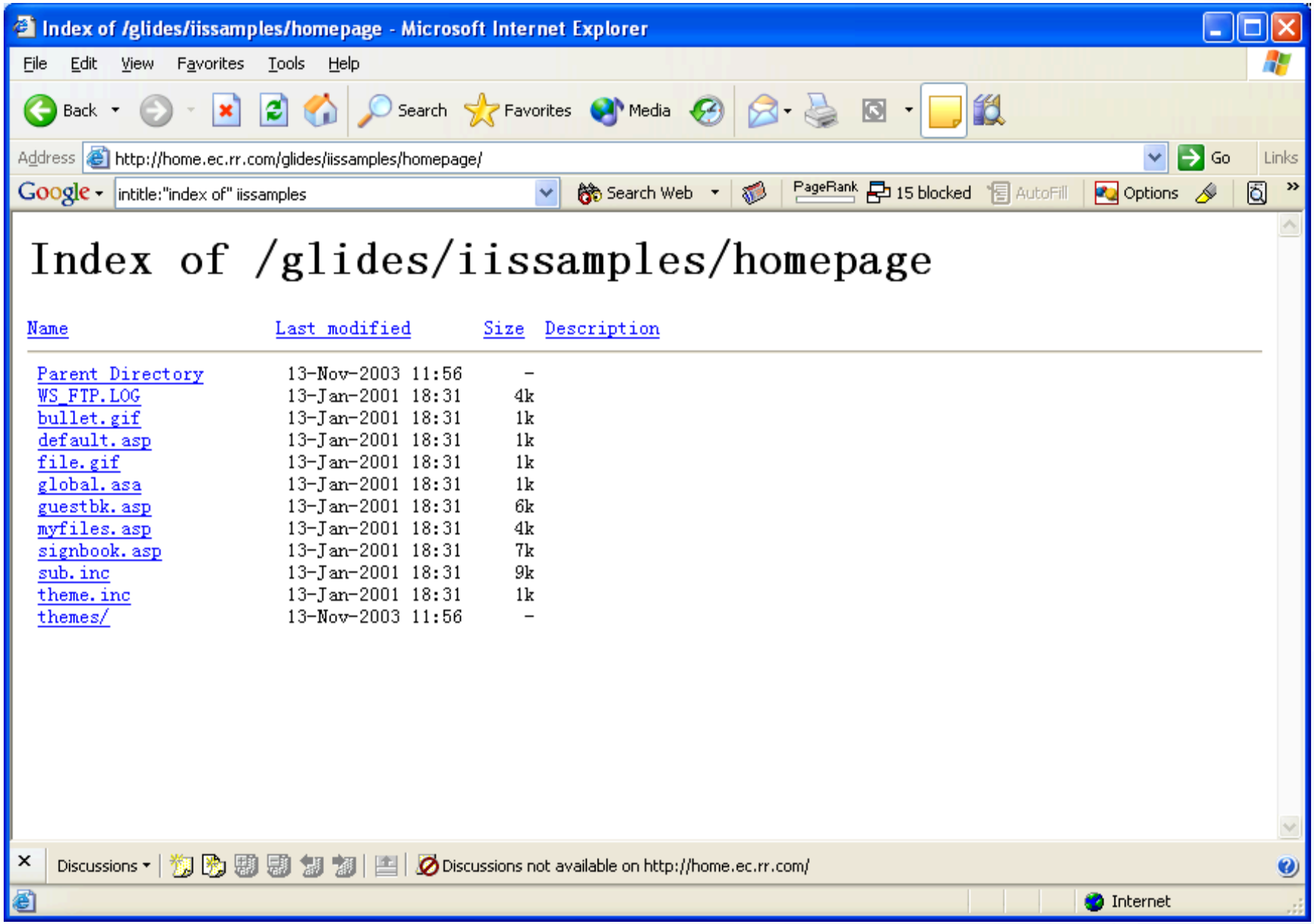
Google Hacking

- Sensitive Directories Listing
  - Intitle: index.of.winnt


Index of /winnt - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back 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 -
smbcrypt/ 10-Mar-2003 14:02 -
Discussions
Discussions not available on http://afrodite.upf.tche.br/
Internet

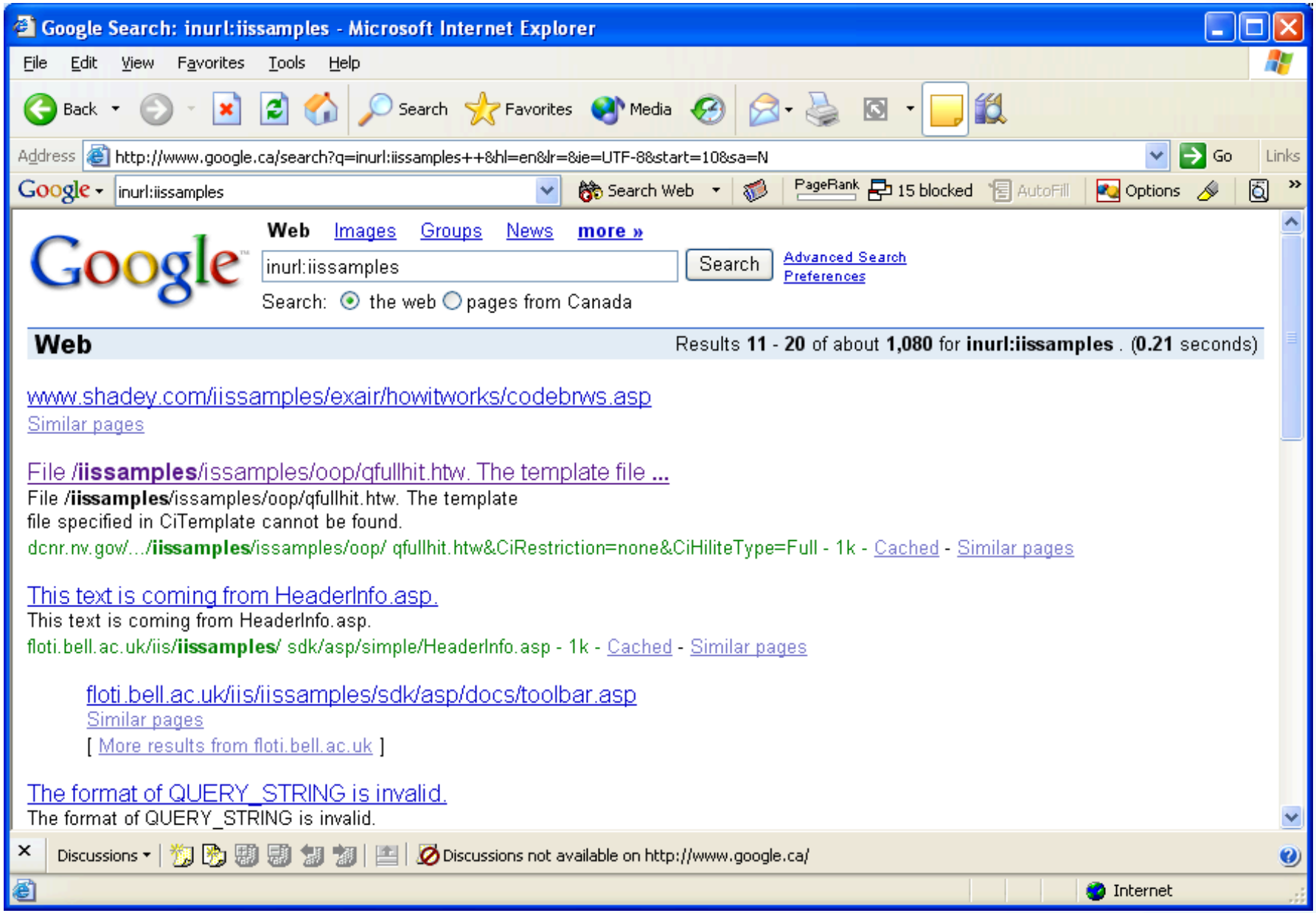
Google Hacking

- Sensitive Directories Listing
  - Intitle: “index of” iissamples (dangeous iissamples) (32)


Index of /glides/iissamples/homepage - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://home.ec.rr.com/glides/iissamples/homepage/
Go Links
Google intitle:"index of" iissamples
Search Web PageRank 15 blocked AutoFill Options
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 -
Discussions
Discussions not available on http://home.ec.rr.com/
Internet

Google Hacking

- Sensitive Directories Listing
  - Inurl: iissamples (1080)

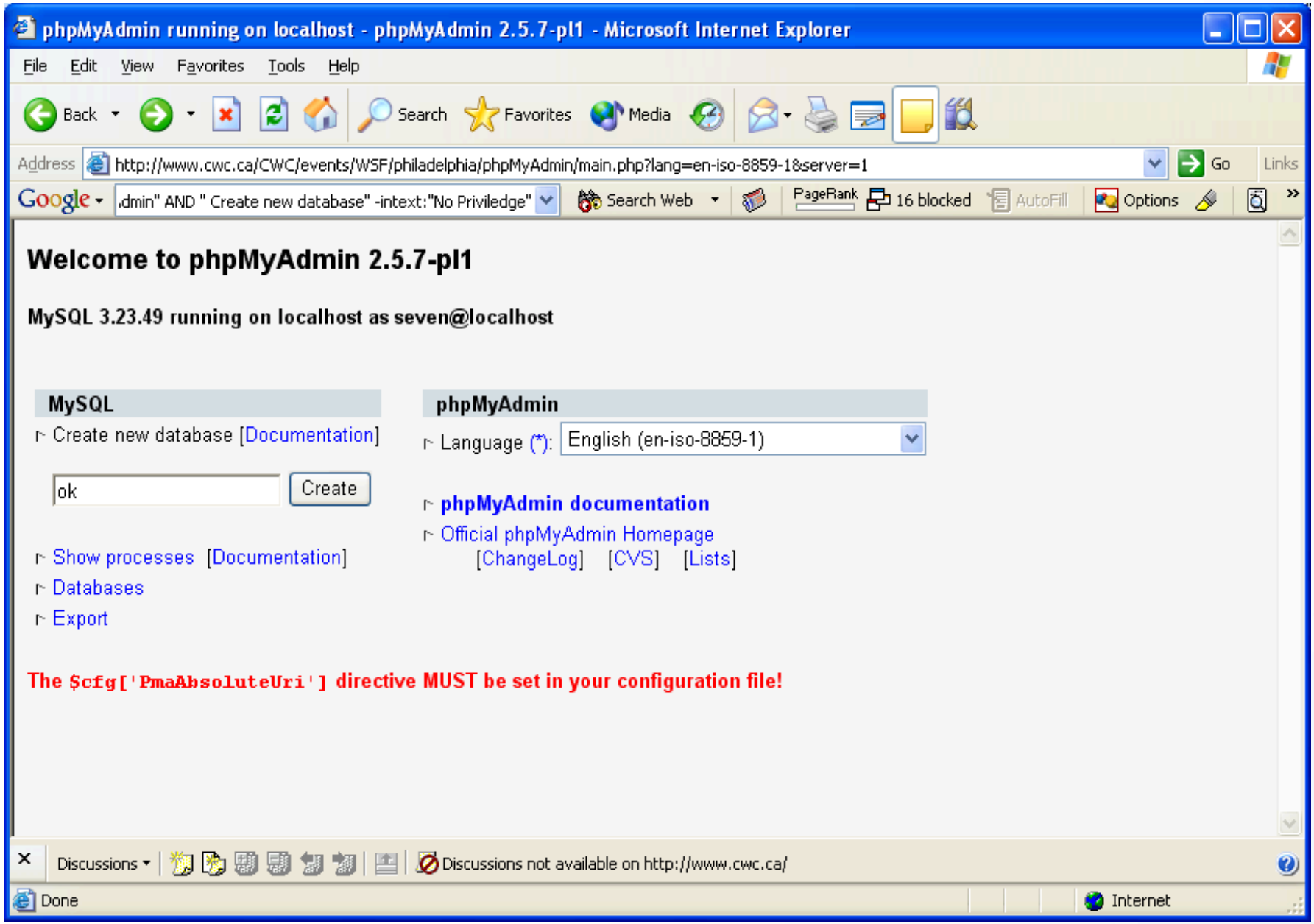

Google Search: inurl:iissamples - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?q=inurl:iissamples++&hl=en&lr=&ie=UTF-8&start=10&sa=N
Go Links
Google inurl:iissamples
Search Web PageRank 15 blocked AutoFill Options
Web Images Groups News more »
Google
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/issamples/oop/qfullhit.htw. The template file ...
File /iissamples/issamples/oop/qfullhit.htw. The template
file specified in CiTemplate cannot be found.
dcnr.nv.gov/.../iissamples/issamples/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.
Discussions
Discussions not available on http://www.google.ca/
Internet

Google Hacking

- Database Manipulation
  - Different database applications leave different signatures on the database files

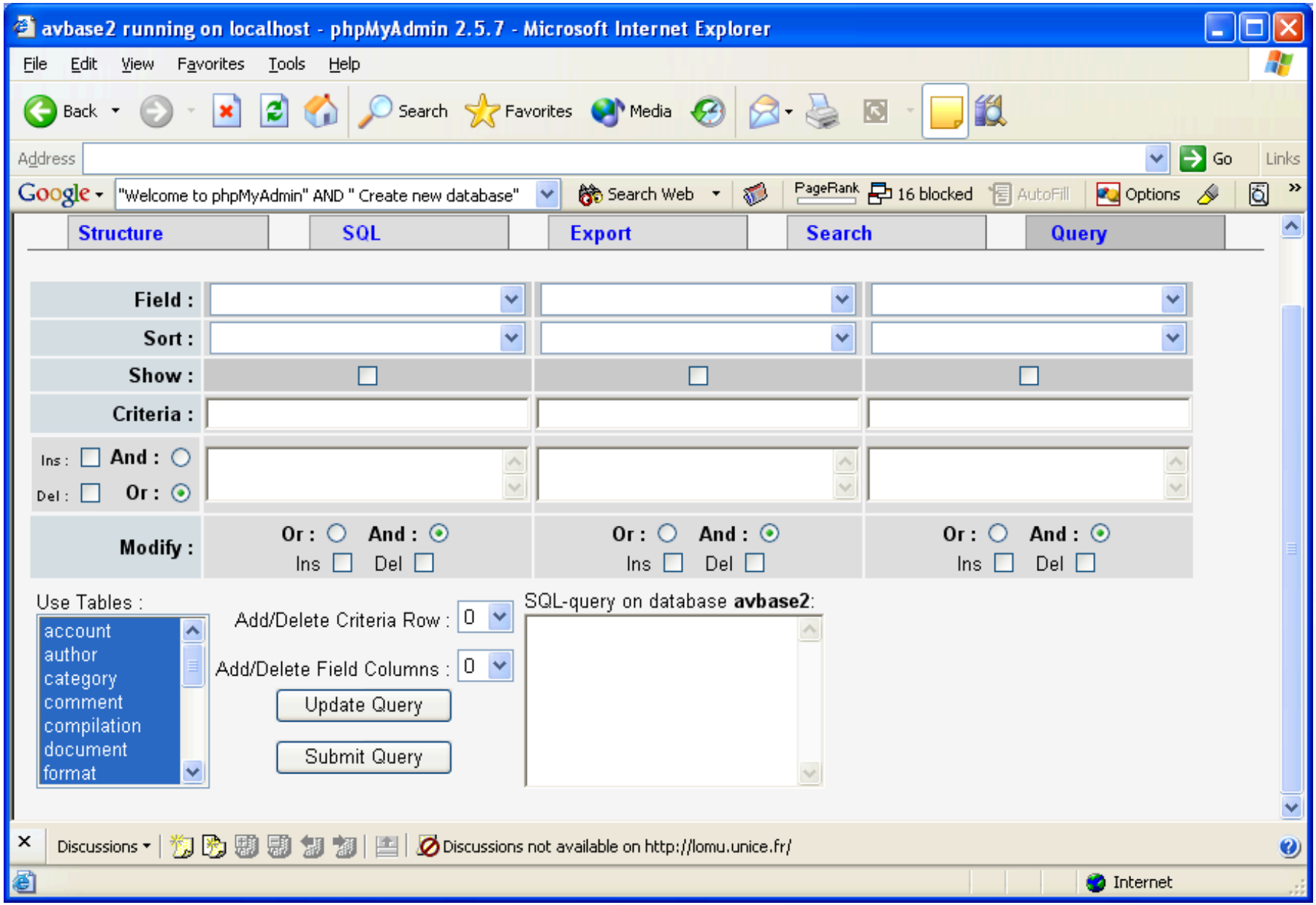
Google Hacking

- Database Manipulation
  - “Welcome to phpMyAdmin” AND “Create new database” -intext: “No Priviledge” (find a page that might have privilege to update mysql)


phpMyAdmin running on localhost - phpMyAdmin 2.5.7-pl1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.cwc.ca/CWC/events/WSF/philadelphia/phpMyAdmin/main.php?lang=en-iso-8859-1&server=1
Go Links
Google ,dmin" AND " Create new database" -intext:"No Priviledge"
Search Web PageRank 16 blocked AutoFill Options
Welcome to phpMyAdmin 2.5.7-pl1
MySQL 3.23.49 running on localhost as seven@localhost
MySQL
Create new database [Documentation]
ok
Create
Show processes [Documentation]
Databases
Export
phpMyAdmin
Language (*): English (en-iso-8859-1)
phpMyAdmin documentation
Official phpMyAdmin Homepage
[ChangeLog] [CVS] [Lists]
The $cfg['PmaAbsoluteUri'] directive MUST be set in your configuration file!
Discussions
Discussions not available on http://www.cwc.ca/
Done
Internet

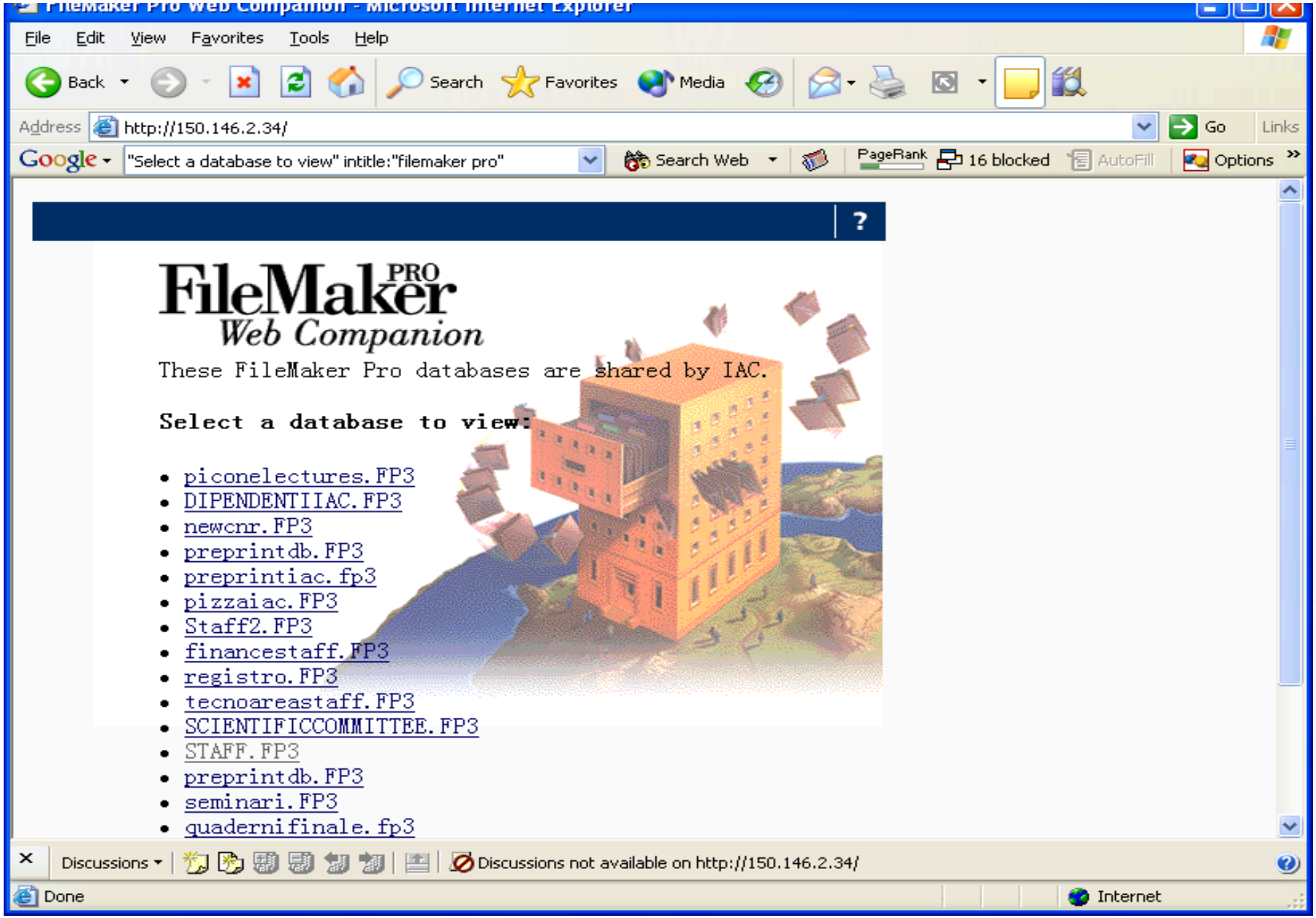
Google Hacking

- Database Manipulation
  - "Welcome to phpMyAdmin" AND "Create new database" (after several hits, we got this)


avbase2 running on localhost - phpMyAdmin 2.5.7 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "Welcome to phpMyAdmin" AND " Create new database" Search Web PageRank 16 blocked AutoFill Options
Structure SQL Export Search Query
Field :
Sort :
Show :
Criteria :
Ins : And :
Del : Or :
Modify :
Or : And :
Ins Del
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:
Discussions
Discussions not available on http://lomu.unice.fr/
Internet

Google Hacking

- Database Manipulation
  - "Select a database to view" intitle: "filemaker pro" (94) Filemaker


FileMaker Pro Web Companion - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
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
DIPENDENTIIAC.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

Google Hacking

- Database Manipulation
  - After several clicks and you can query the table

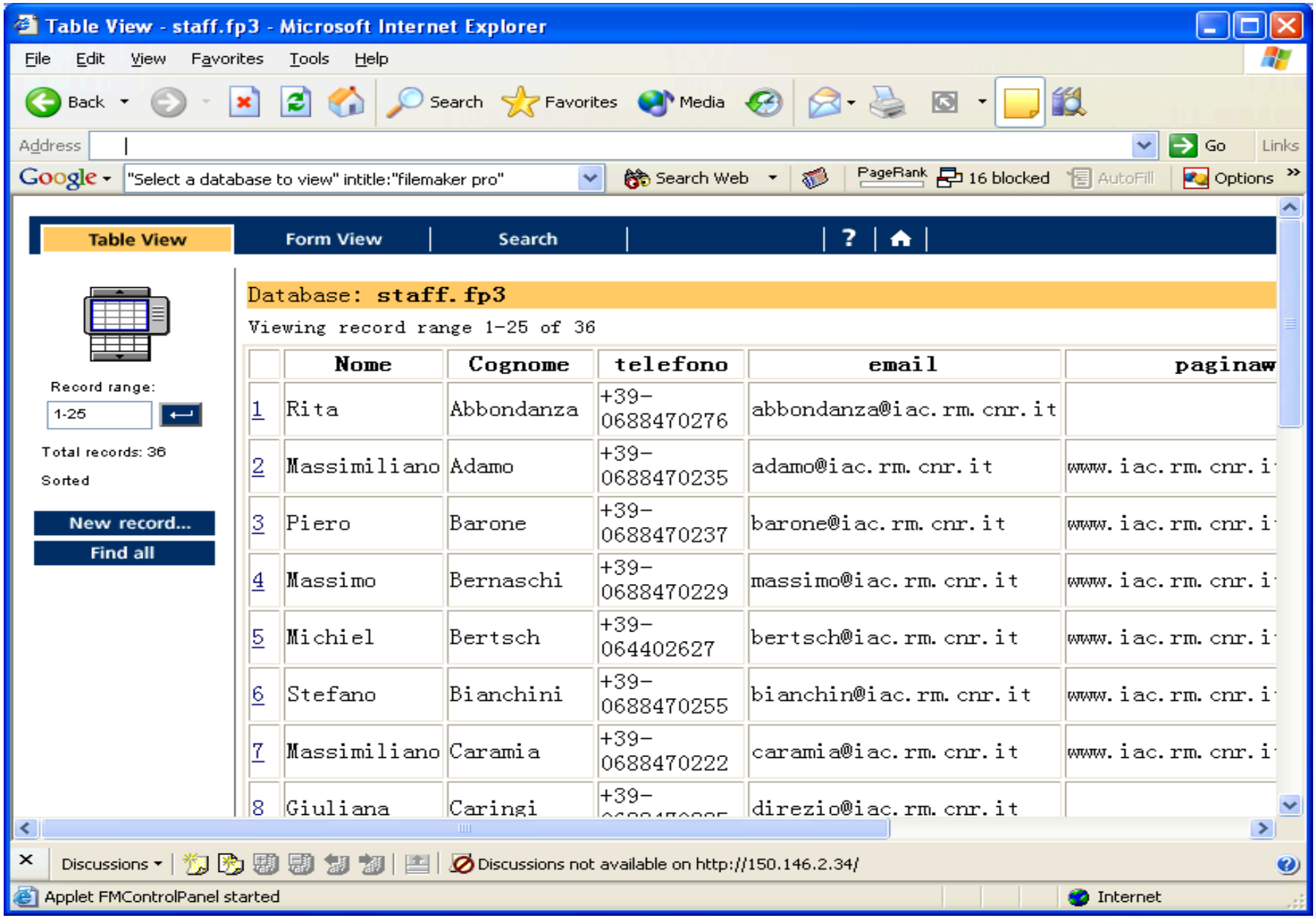
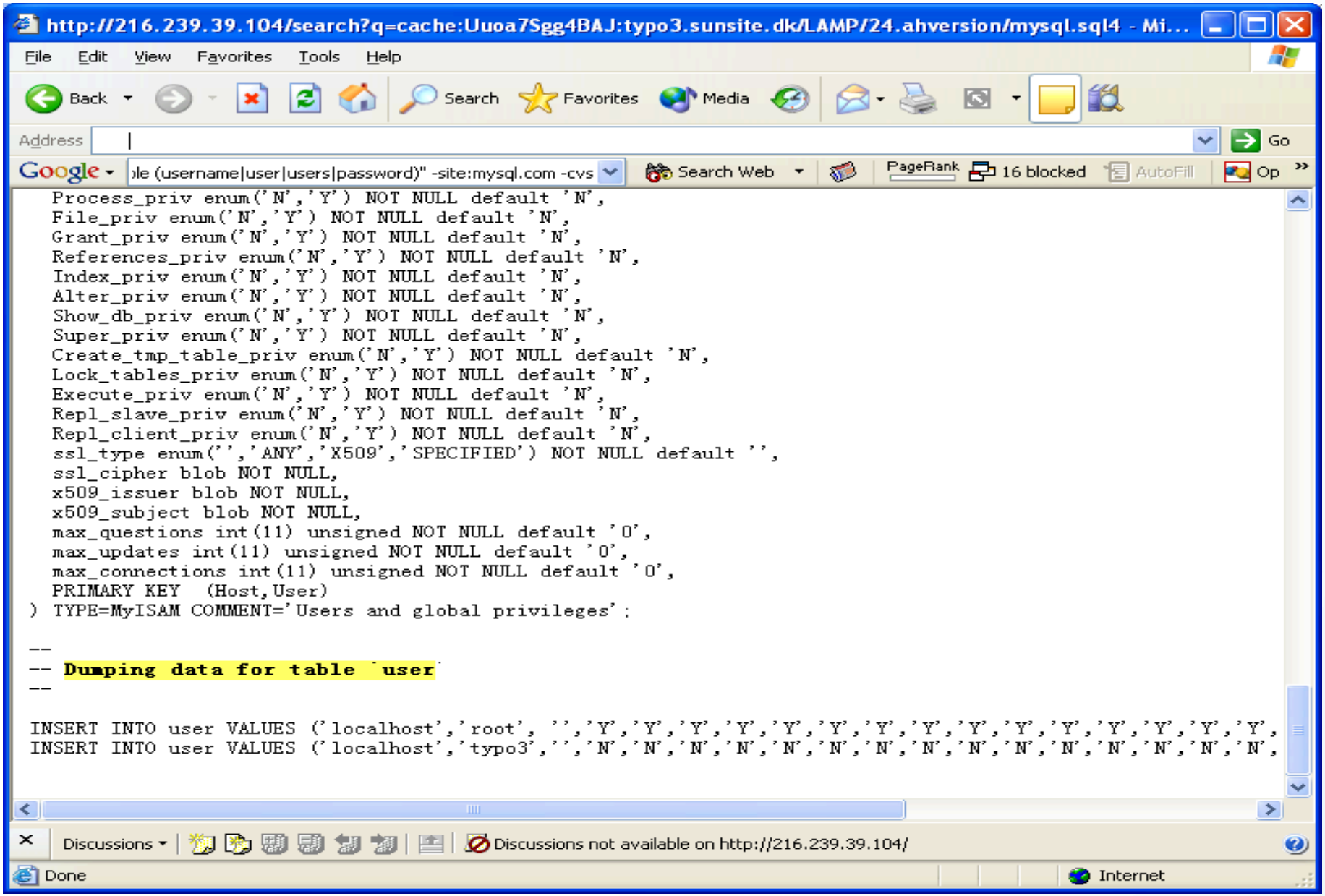


Table View - staff.fp3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "Select a database to view" intitle:"filemaker pro"
Search Web PageRank 16 blocked AutoFill Options
Table View
Form View
Search
Record range:
1-25
Total records: 36
Sorted
New record...
Find all
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 direzio@iac.rm.cnr.it
Discussions Discussions not available on http://150.146.2.34/
Applet FMControlPanel started
Internet

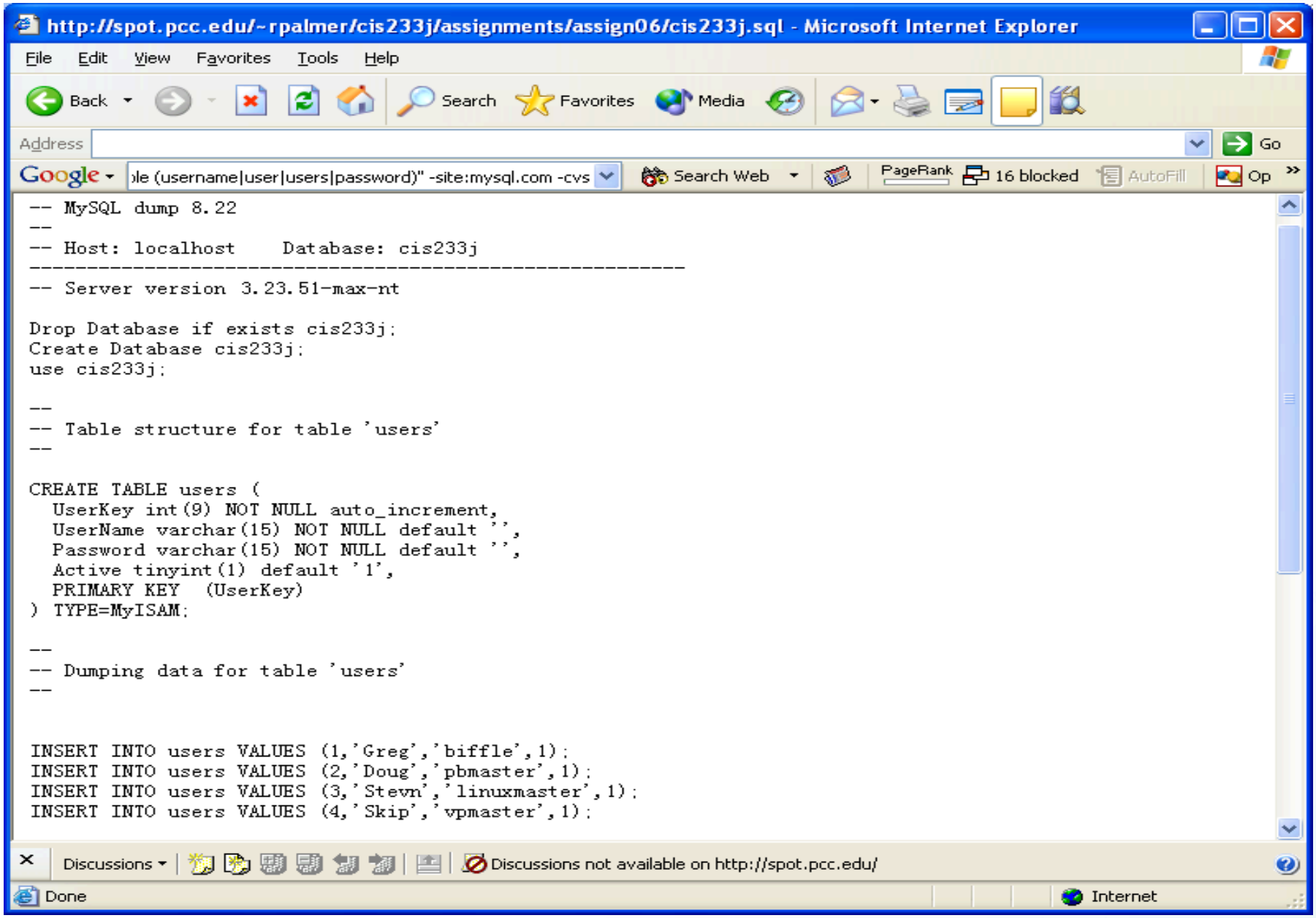
Google Hacking

- Database Manipulation
  - "# Dumping data for table (username|user|users| password)" -site: mysql.com –cvs (289) (backup data of 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 Search Favorites Media
Address
Go
Google
ble (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','Y',
INSERT INTO user VALUES ('localhost','typo3','','N','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

Google Hacking

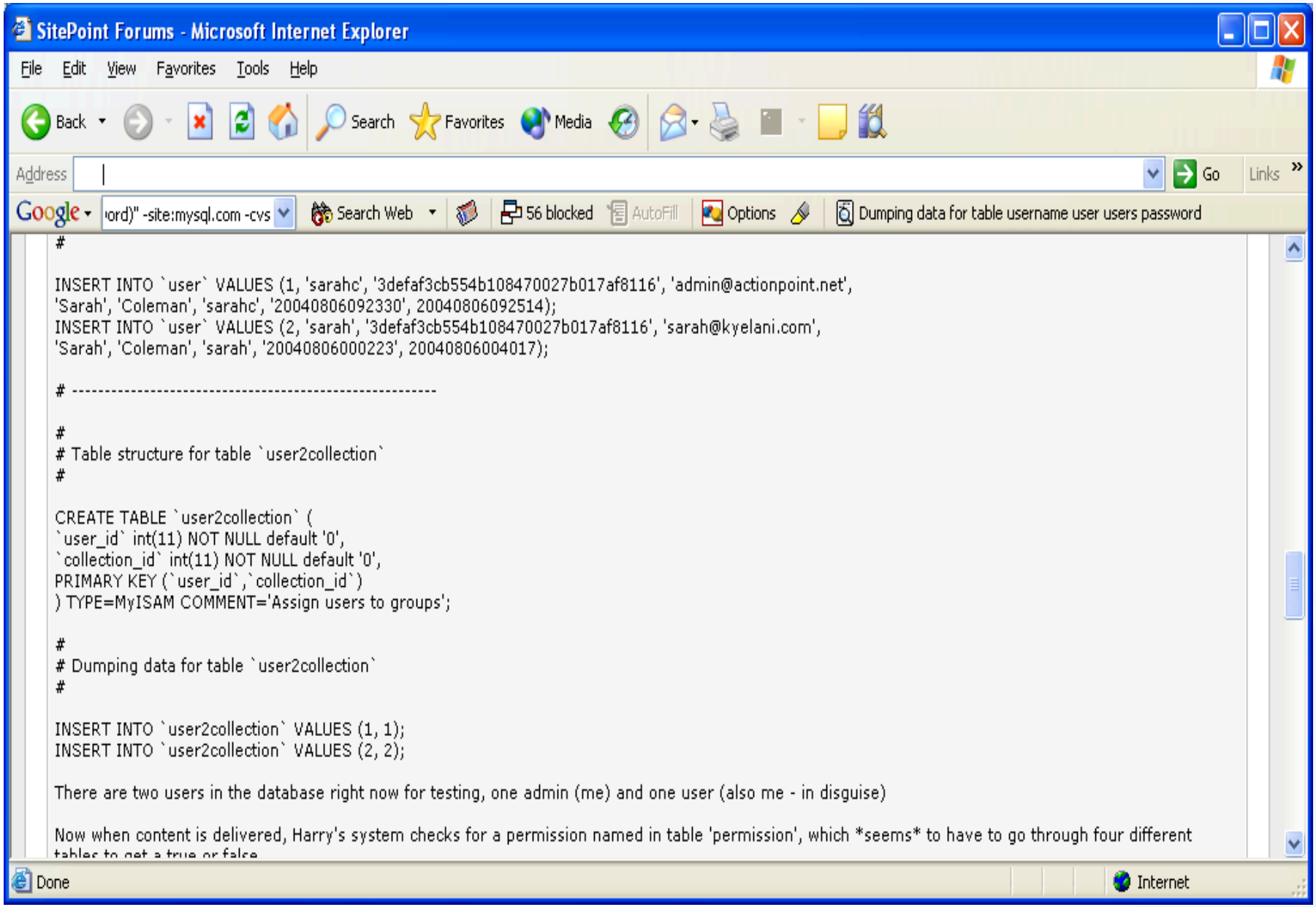
- Database Manipulation
  - "# Dumping data for table (username|user|users|password)" –site: mysql.com -cvs


http://spot.pcc.edu/~rpalmer/cis233j/assignments/assign06/cis233j.sql - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Google
ble (username|user|users|password)" -site:mysql.com -cvs
Search Web
PageRank
16 blocked
AutoFill
Op
-- 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);
Discussions
Discussions not available on http://spot.pcc.edu/
Done
Internet

Google Hacking

- Database Manipulation
  - “# Dumping data for table (username|user|users| password)” -site: mysql.com –cvs

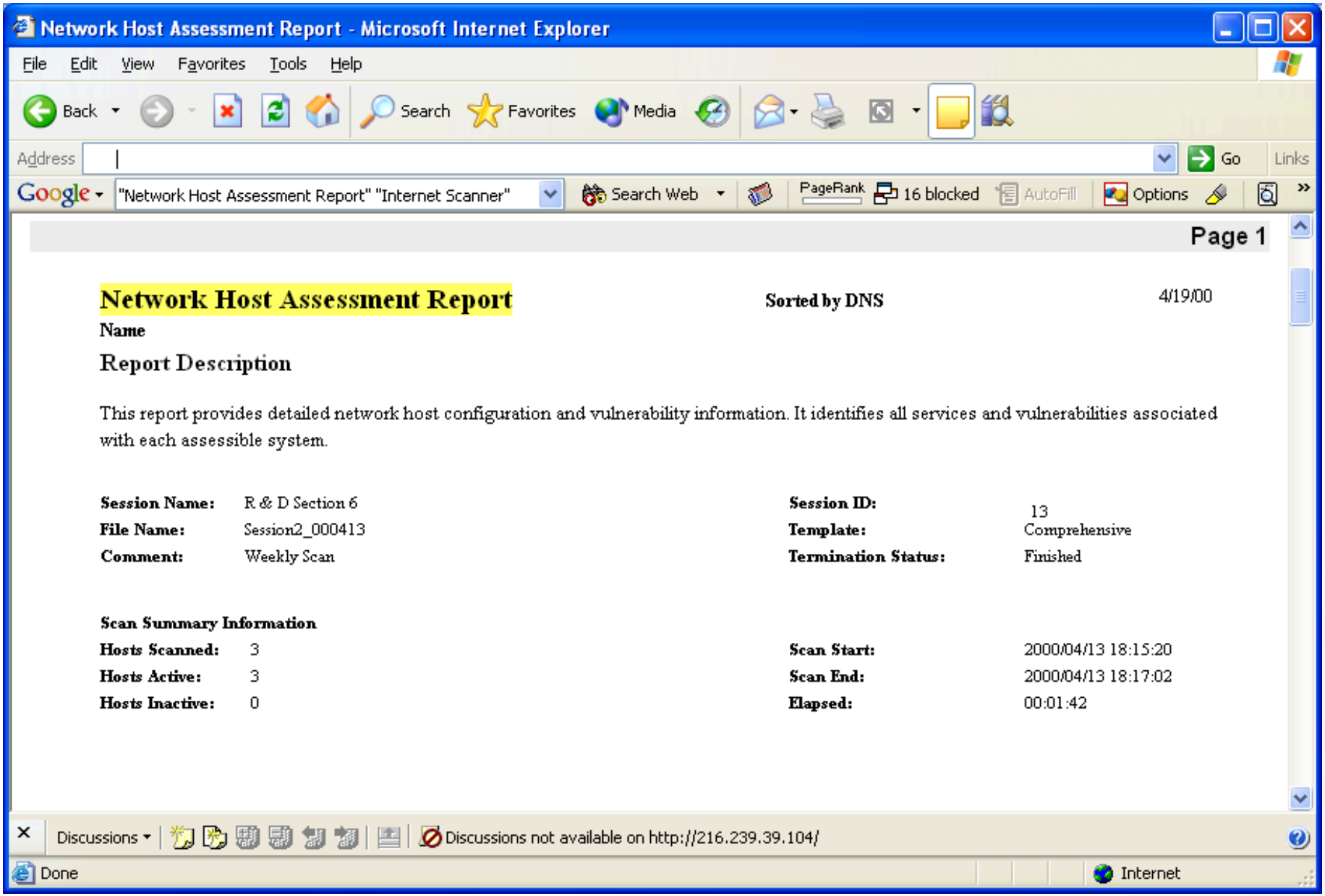

SitePoint Forums - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google
ord)" -site:mysql.com -cvs
Search Web
56 blocked
AutoFill
Options
Dumping data for table username user users password
#
INSERT INTO `user` VALUES (1, 'sarahc', '3defaf3cb554b108470027b017af8116', 'admin@actionpoint.net',
'Sarah', 'Coleman', 'sarahc', '20040806092330', 20040806092514);
INSERT INTO `user` VALUES (2, 'sarah', '3defaf3cb554b108470027b017af8116', 'sarah@kyelani.com',
'Sarah', 'Coleman', 'sarah', '20040806000223', 20040806004017);
--
#
Table structure for table `user2collection`
#
CREATE TABLE `user2collection` (
`user_id` int(11) NOT NULL default '0',
`collection_id` int(11) NOT NULL default '0',
PRIMARY KEY (`user_id`,`collection_id`)
) TYPE=MyISAM COMMENT='Assign users to groups';
#
Dumping data for table `user2collection`
#
INSERT INTO `user2collection` VALUES (1, 1);
INSERT INTO `user2collection` VALUES (2, 2);
There are two users in the database right now for testing, one admin (me) and one user (also me - in disguise)
Now when content is delivered, Harry's system checks for a permission named in table 'permission', which *seems* to have to go through four different
Done
Internet

Google Hacking

- Sensitive System Information
  - Network security reports have lists of vulnerabilities for your system
  - Configuration files often contain the application parameters inventory

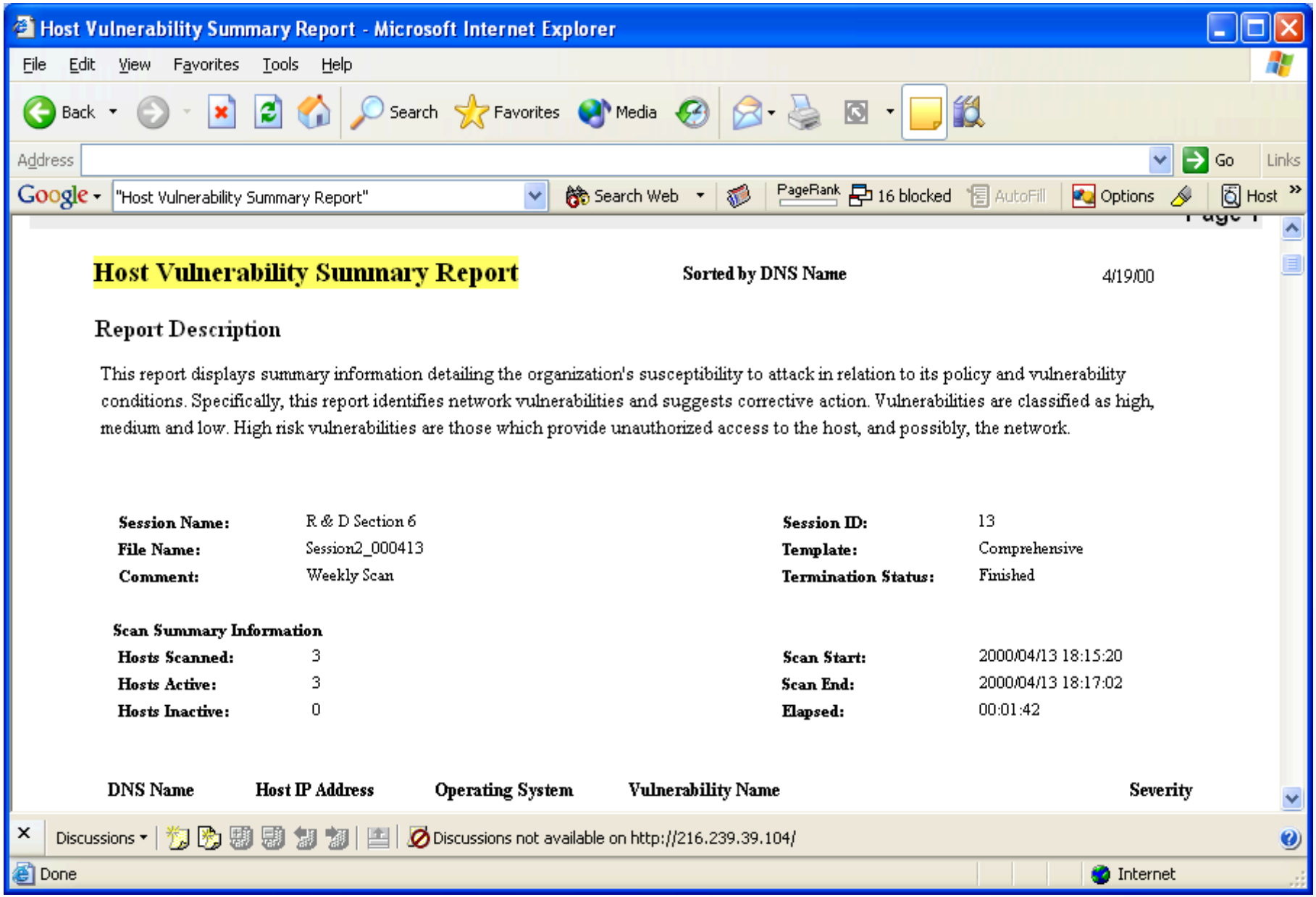
Google Hacking

- Network Security Report (ISS)
  - "Network Host Assessment Report" "Internet Scanner" (iss report) (13)


Network Host Assessment Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "Network Host Assessment Report" "Internet Scanner"
Search Web PageRank 16 blocked AutoFill Options
Page 1
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
Discussions
Discussions not available on http://216.239.39.104/
Done
Internet

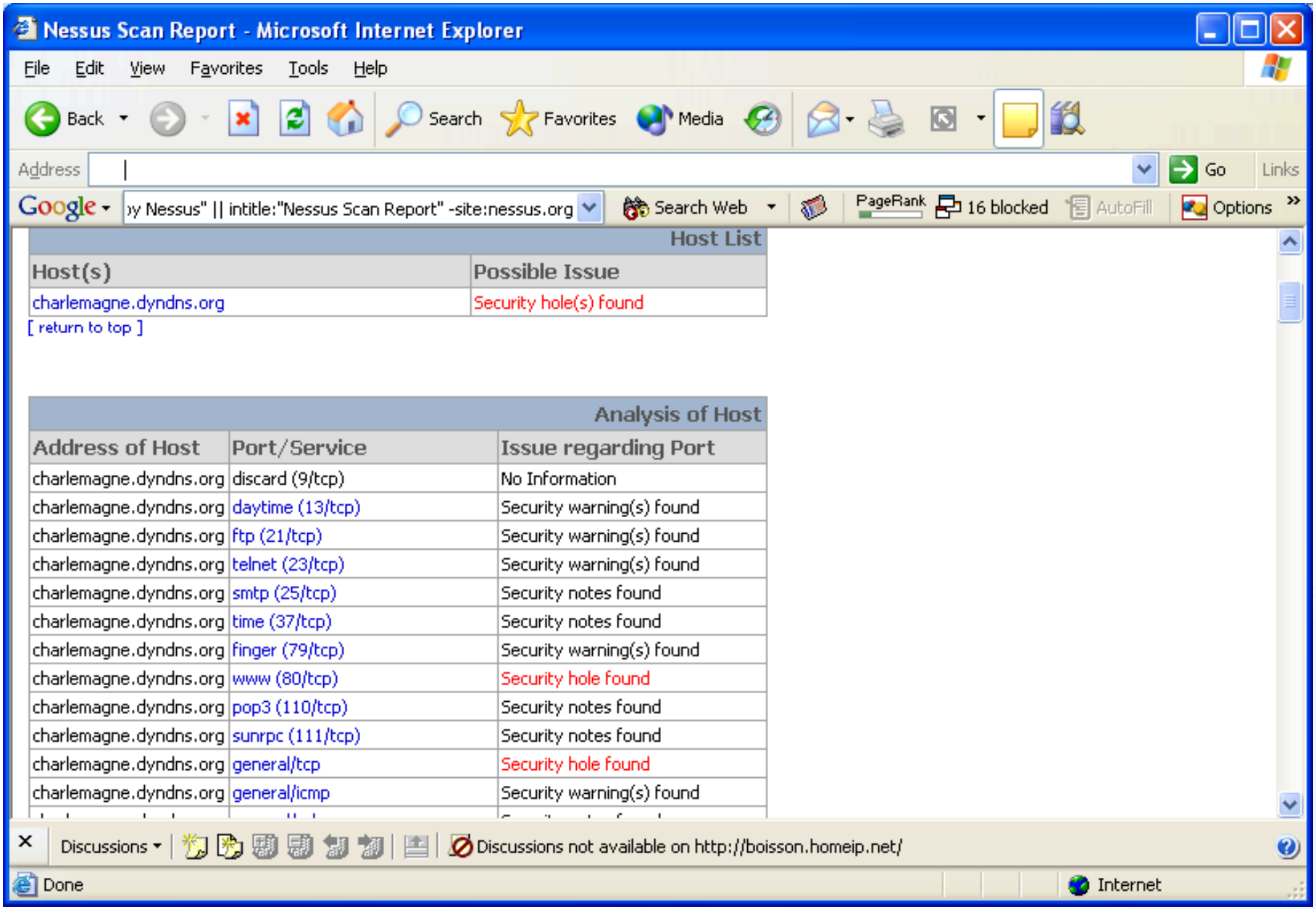
Google Hacking

- Network Security Report (ISS)
  - "Host Vulnerability Summary Report" (ISS report) (25)


Host Vulnerability Summary Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "Host Vulnerability Summary Report" Search Web PageRank 16 blocked AutoFill Options Host
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
Discussions
Discussions not available on http://216.239.39.104/
Done
Internet

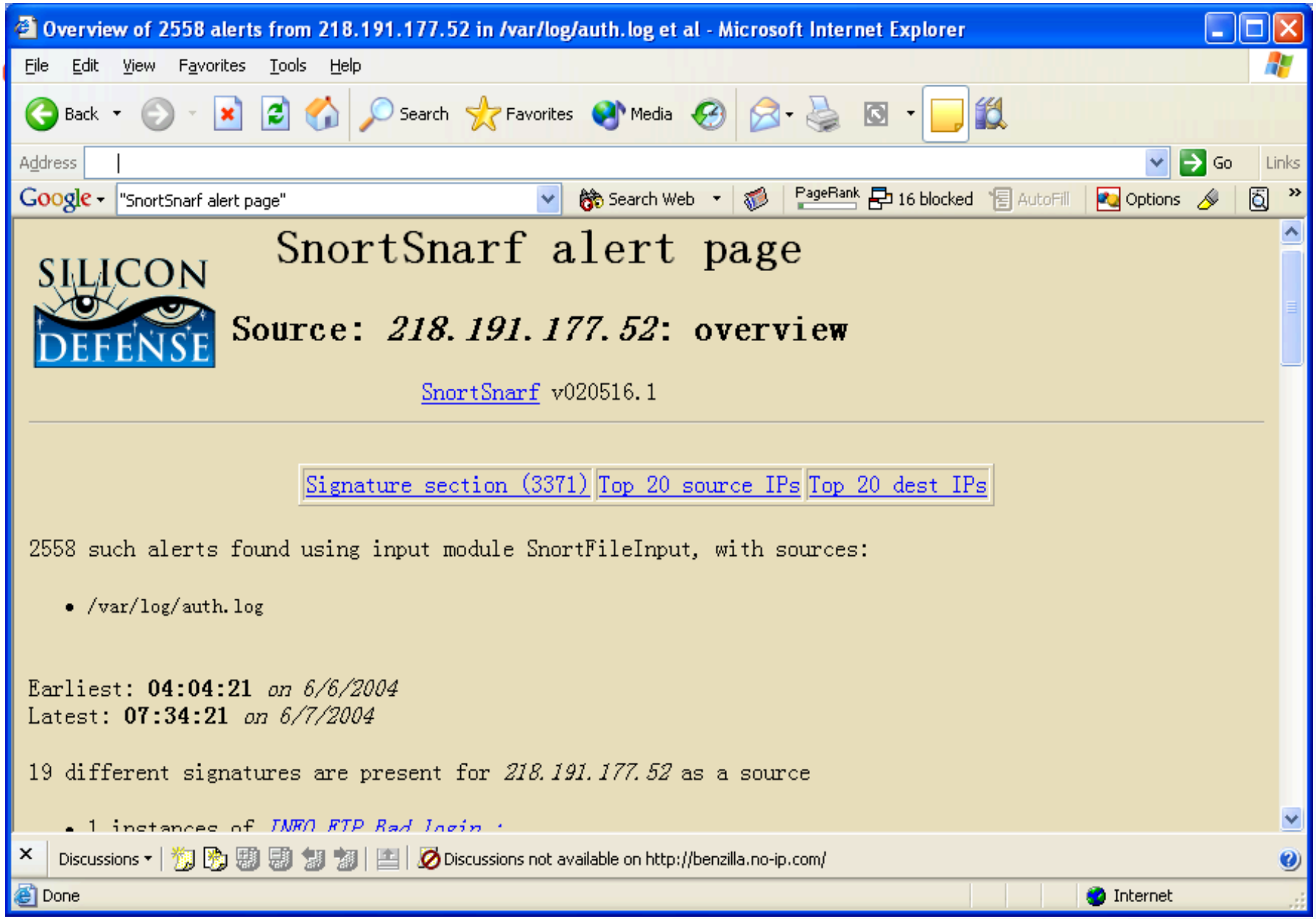
Google Hacking

- Network Security Report (nessus)
  - “This file was generated by Nessus” || intitle:”Nessus Scan Report” -site:nessus.org (185)


Nessus Scan Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google
y 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
Discussions
Discussions not available on http://boisson.homeip.net/
Done
Internet

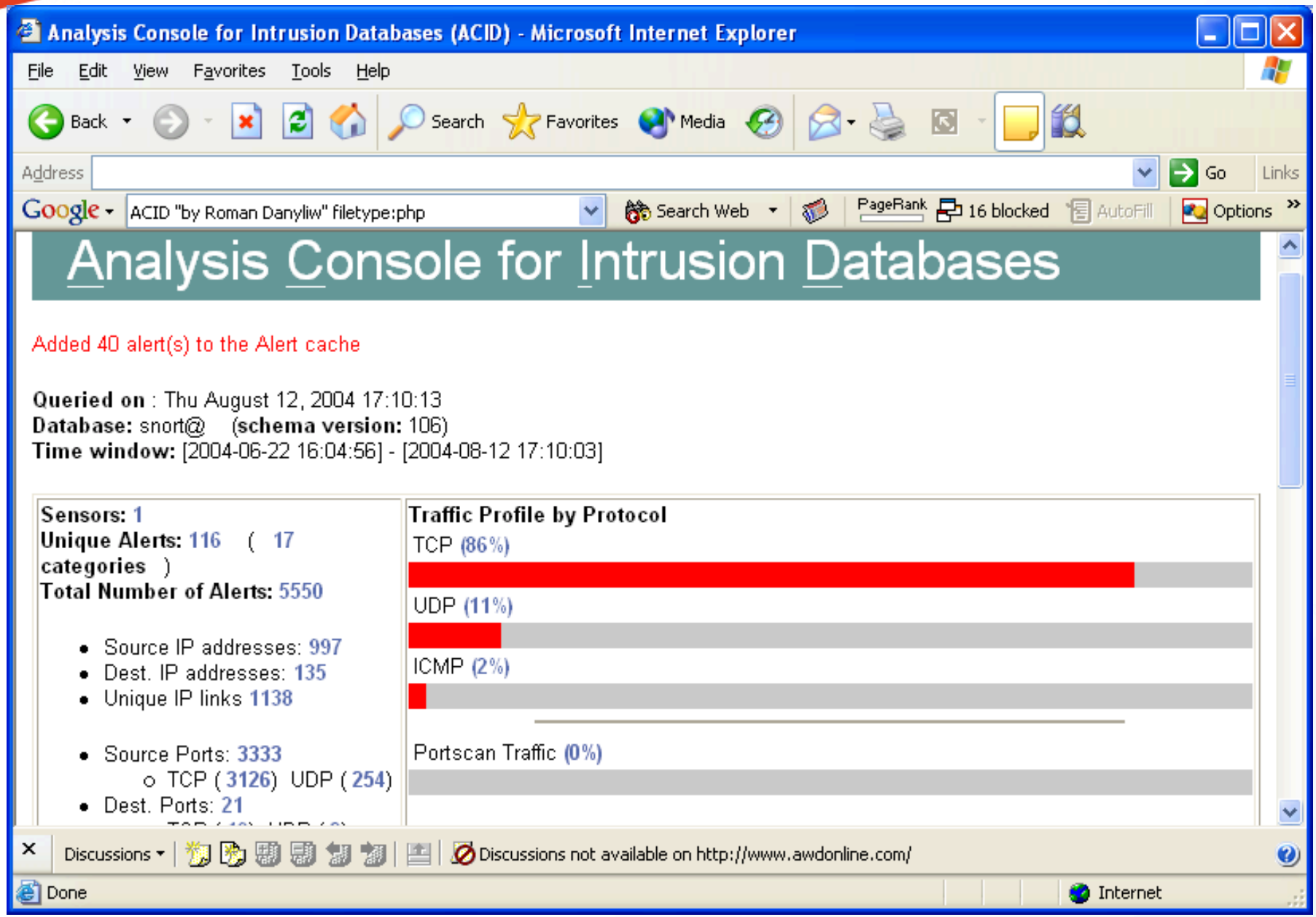
Google Hacking

- Network Scanner Report (Snort)
  - "SnortSnarf alert page" (15,500)


Overview of 2558 alerts from 218.191.177.52 in /var/log/auth.log et al - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "SnortSnarf alert page"
Search Web PageRank 16 blocked AutoFill Options
SnortSnarf alert page
SILICON DEFENSE
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
Discussions
Discussions not available on http://benzilla.no-ip.com/
Done
Internet

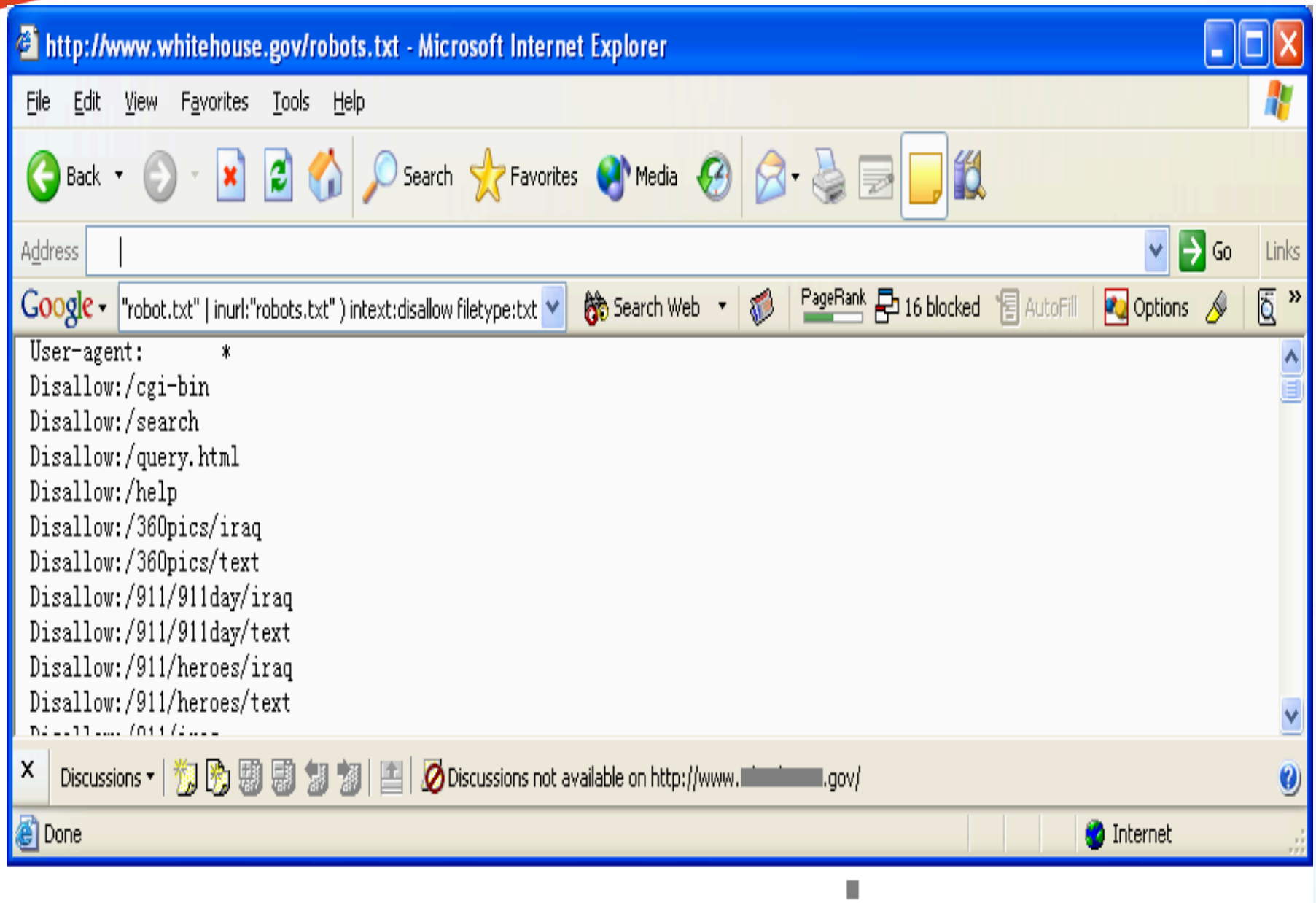
Google Hacking

- Network Security Report (Snort)
  - Intitle: “Analysis Console for Intrusion Databases” +intext:”by Roman Danyliw” inurl:acid/ acid_main.php (13 results, acid alert database)


Analysis Console for Intrusion Databases (ACID) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address Go Links
Google ACID "by Roman Danyliw" filetype:php Search Web PageRank 16 blocked AutoFill Options
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
TCP (86%)
UDP (11%)
ICMP (2%)
Portscan Traffic (0%)
Discussions
Discussions not available on http://www.awdonline.com/
Done
Internet

Google Hacking

- Configuration Files (robots.txt)
  - (inurl: “robot.txt” | inurl: “robots.txt”) intext:disallow filetype:txt
  - Robots.txt means to protect you privacy from crawlers
  - But allows you to determine the file system architecture

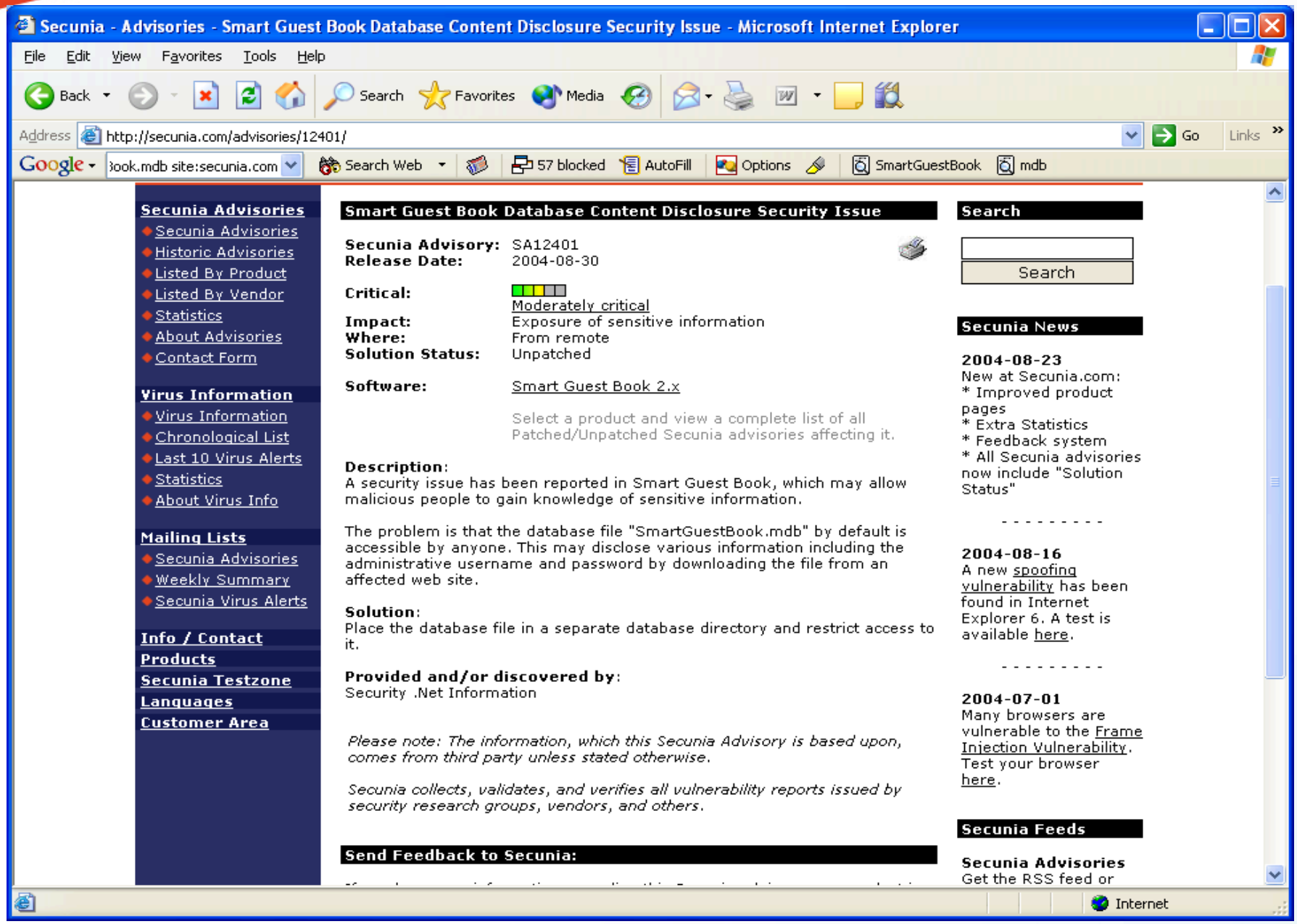

http://www.whitehouse.gov/robots.txt - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google "robot.txt" | inurl:"robots.txt") intext:disallow filetype:txt Search Web PageRank 16 blocked AutoFill Options
User-agent: *
Disallow:/cgi-bin
Disallow:/search
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.[redacted].gov/
Done
Internet

Google Hacking

- A vulnerable targets scanning example
  - Get the new vulnerabilities from advisory
  - Find the signature from vendor Website
  - Google search to find the targets
  - Perform further malicious actions

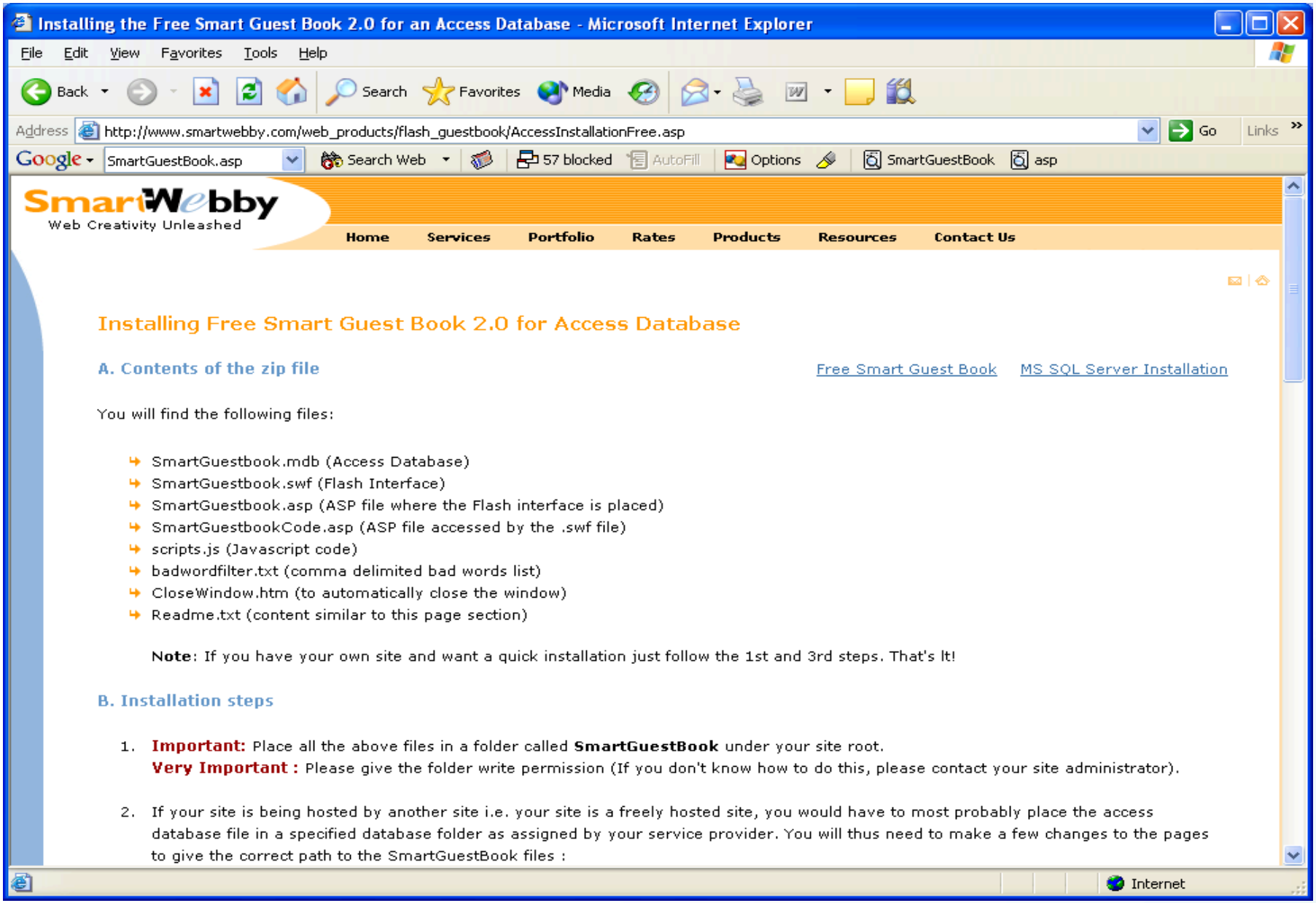
Google Hacking

- An advisory looks like……


Secunia - Advisories - Smart Guest Book Database Content Disclosure Security Issue - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://secunia.com/advisories/12401/
Go Links
Google book.mdb site:secunia.com Search Web 57 blocked AutoFill Options SmartGuestBook mdb
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
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
Internet

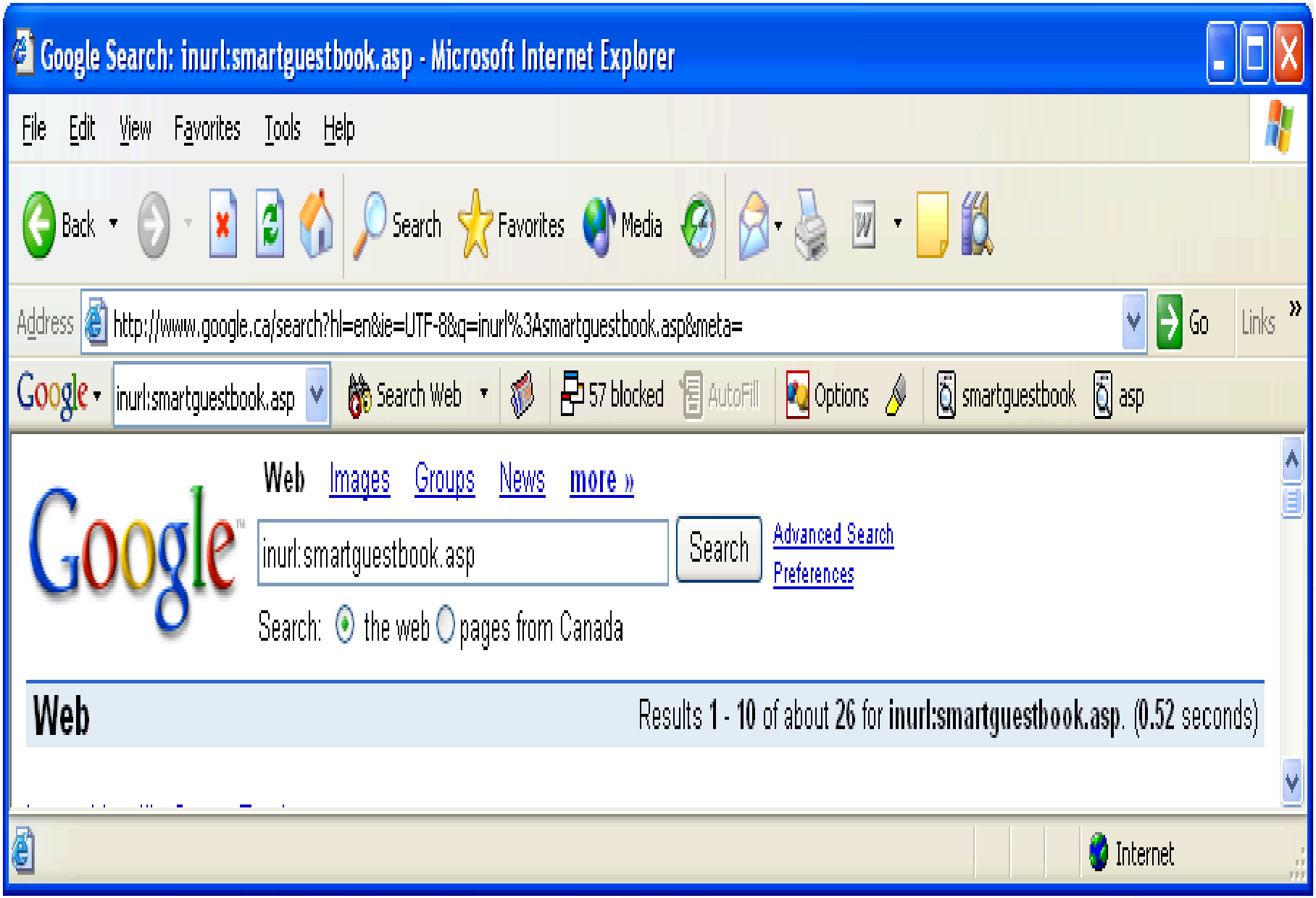
Google Hacking

- Vendor Website Information


Installing the Free Smart Guest Book 2.0 for an Access Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.smartwebby.com/web_products/flash_guestbook/AccessInstallationFree.asp
Go Links
Google SmartGuestBook.asp
Search Web 57 blocked AutoFill Options SmartGuestBook asp
SmartWebby
Web Creativity Unleashed
Home Services Portfolio Rates Products Resources Contact Us
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 :
Internet

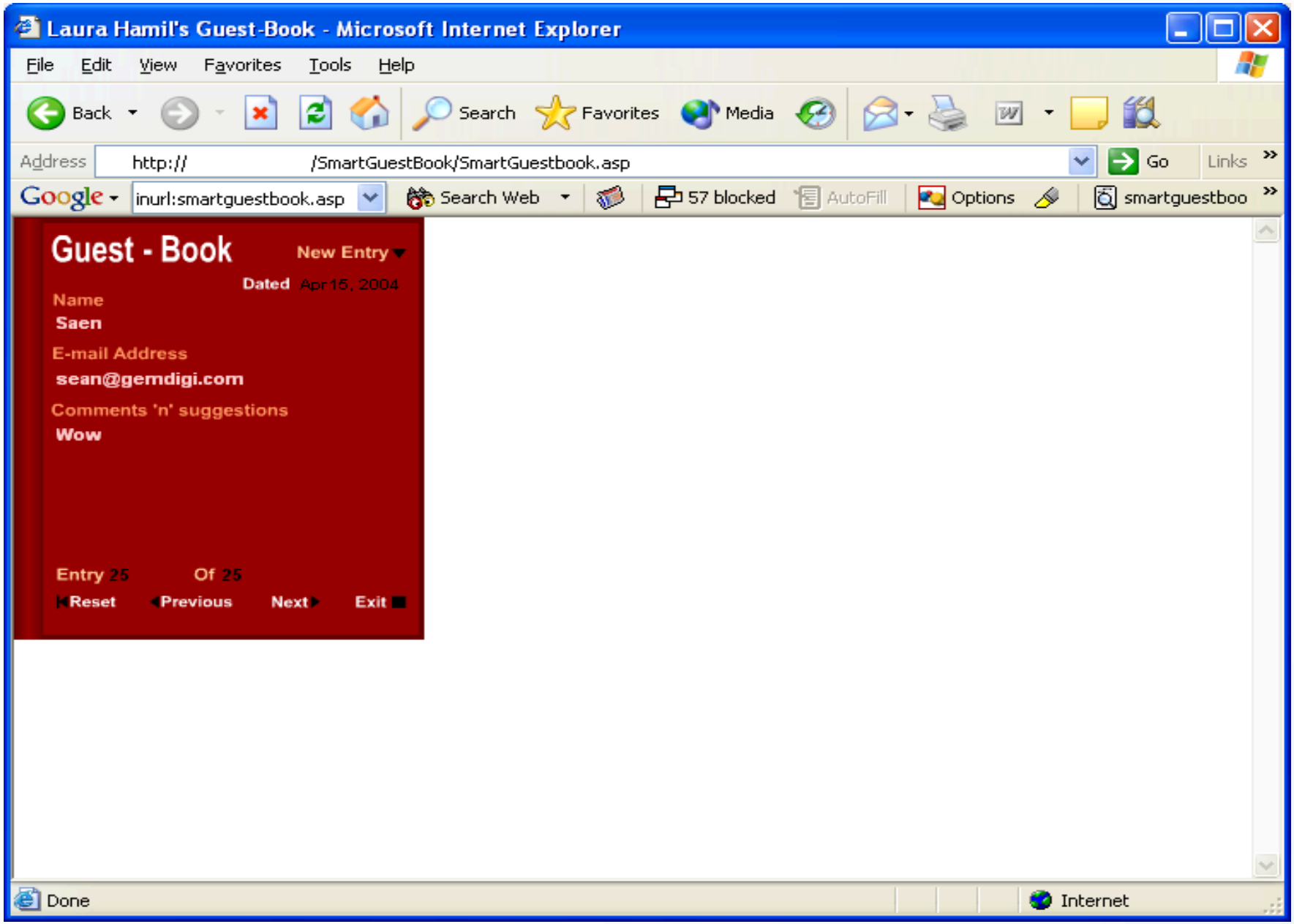
Google Hacking

- Google search……
  - Inurl: smartguestbook.asp


Google Search: inurl:smartguestbook.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?hl=en&ie=UTF-8&q=inurl%3Asmartguestbook.asp&meta=
Go Links
Google inurl:smartguestbook.asp Search Web 57 blocked AutoFill Options smartguestbook asp
Web Images Groups News more »
Google
inurl:smartguestbook.asp
Search
Advanced Search
Preferences
Search: the web pages from Canada
Web
Results 1 - 10 of about 26 for inurl:smartguestbook.asp. (0.52 seconds)
Internet

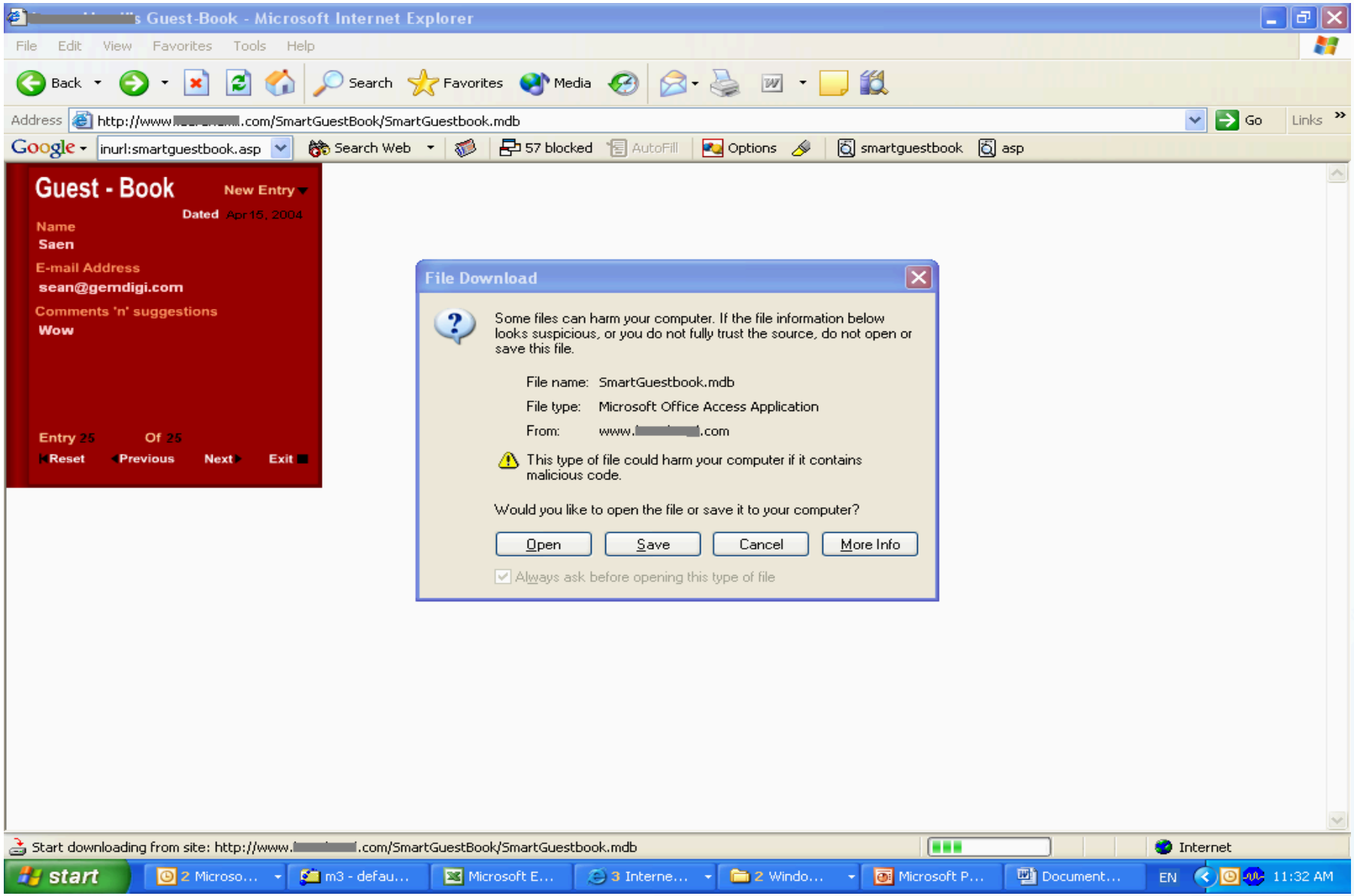
Google Hacking

- The victim's Website


Laura Hamil's Guest-Book - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:// /SmartGuestBook/SmartGuestbook.asp
Go Links
Google inurl:smartguestbook.asp
Search Web 57 blocked AutoFill Options smartguestboo
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
Done
Internet

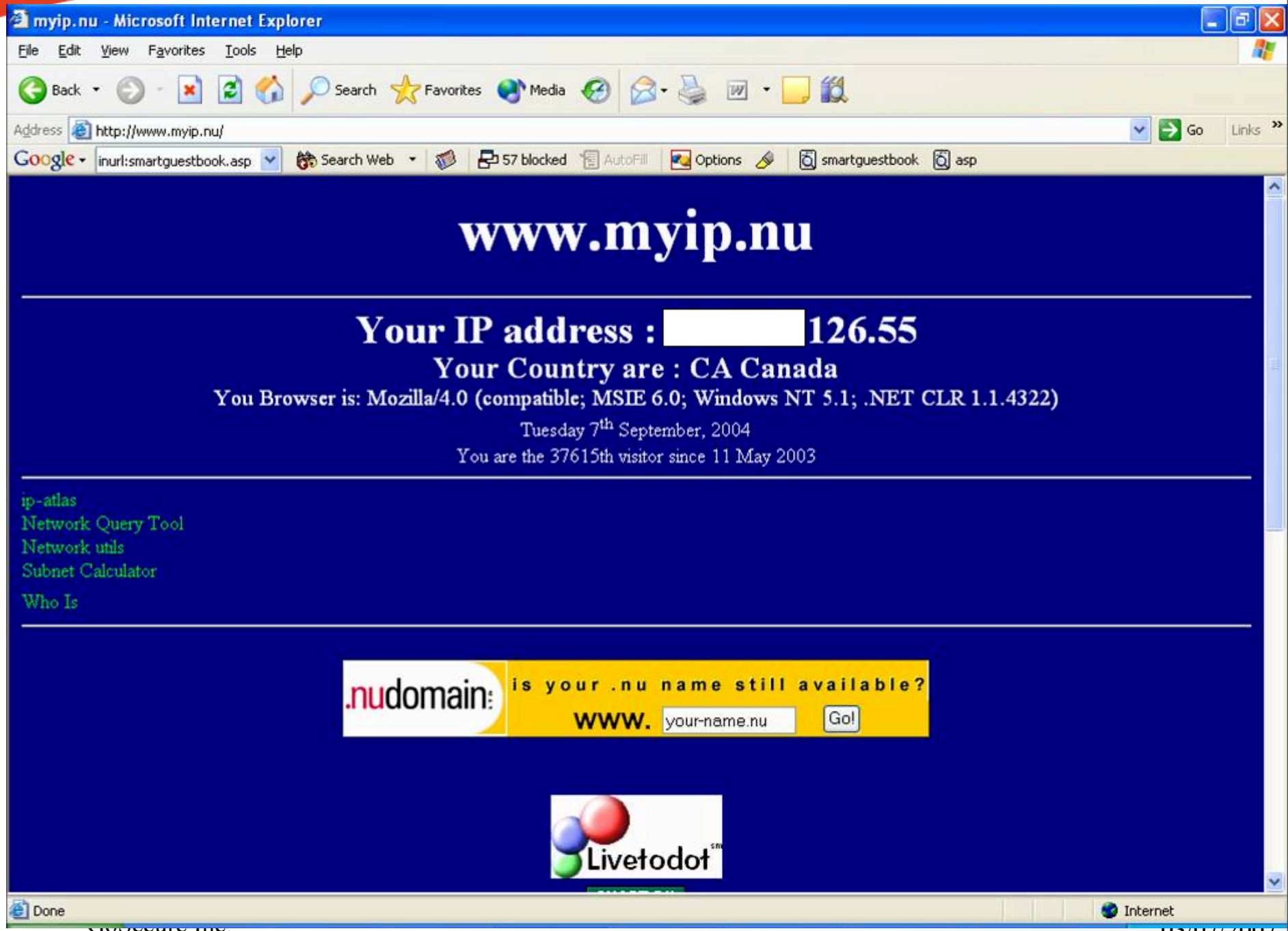
Google Hacking

- Download the database…… Game over


s Guest-Book - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.com/SmartGuestBook/SmartGuestbook.mdb
Go Links
Google inurl:smartguestbook.asp Search Web 57 blocked AutoFill Options smartguestbook asp
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
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.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?
Open Save Cancel More Info
Always ask before opening this type of file
Start downloading from site: http://www.com/SmartGuestBook/SmartGuestbook.mdb
Internet
start
2 Microso... m3 - defau... Microsoft E... 3 Interne... 2 Windo... Microsoft P... Document...
EN 11:32 AM

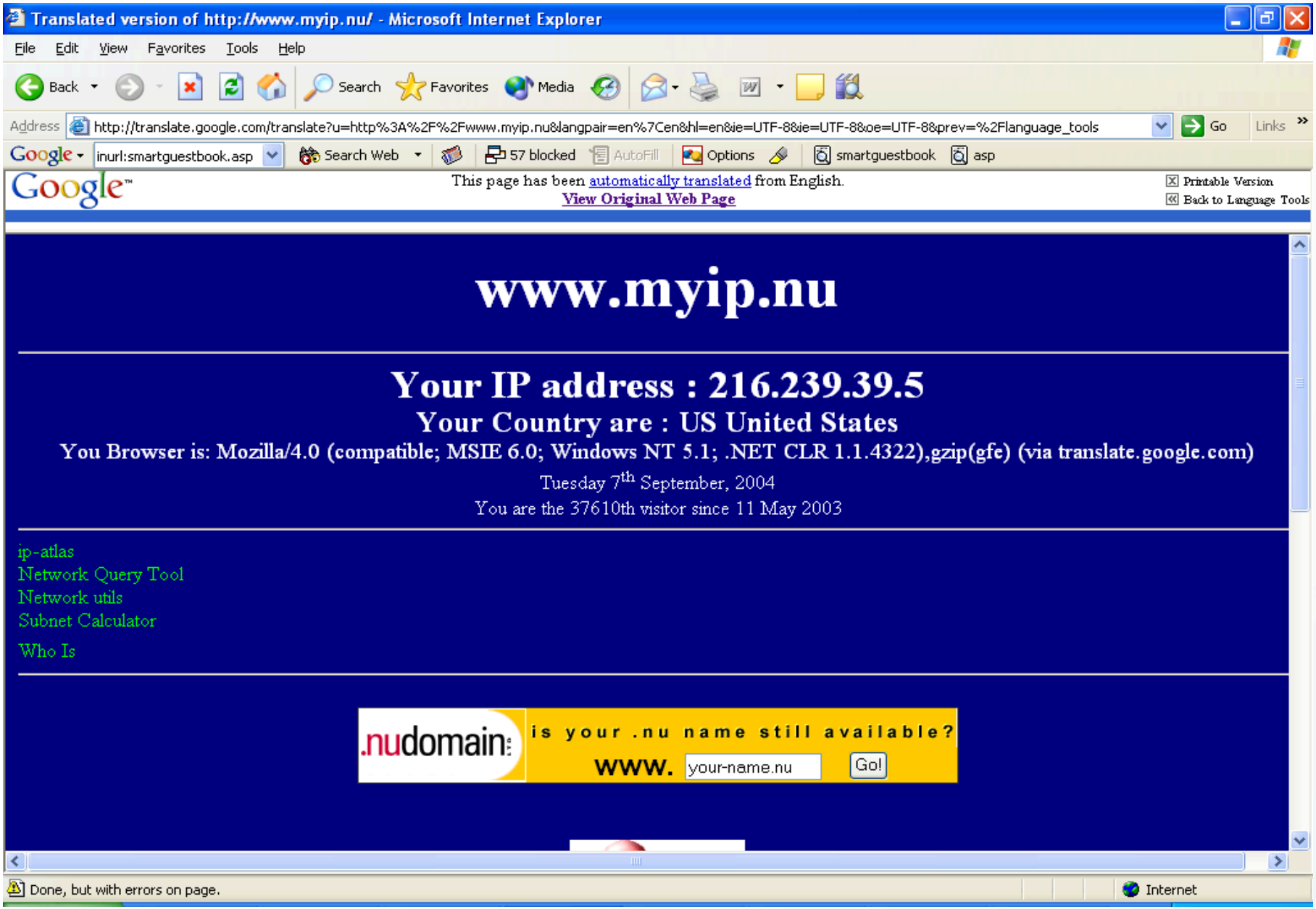
Google Hacking

- Transparent Proxy
  - Normal surfing on www.myip.nu


myip.nu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
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. your-name.nu Go!
Livetodot
Done
Internet

Google Hacking

- Transparent Proxy
  - When we use Google translation tool to surf www.myip.nu

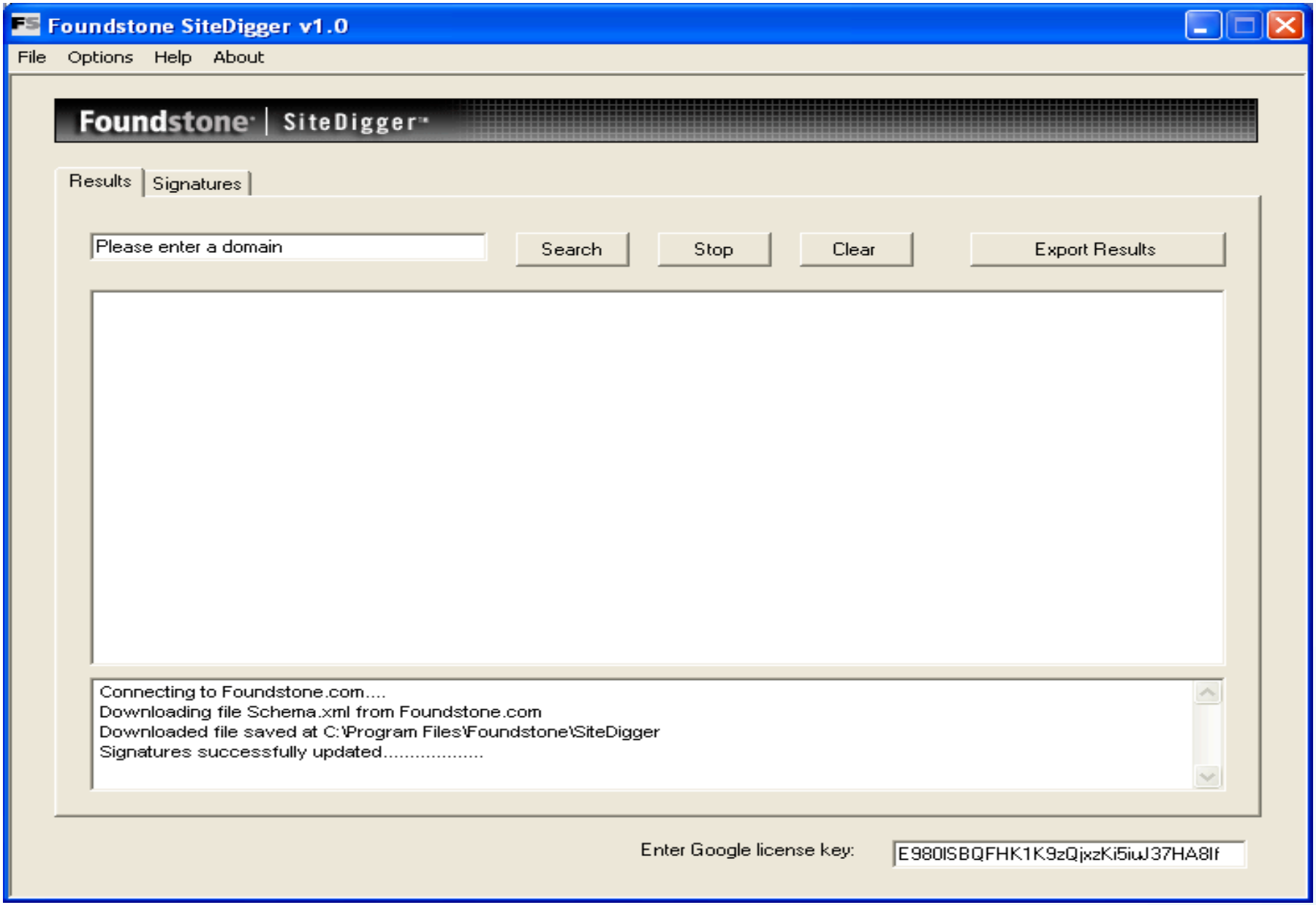

Translated version of http://www.myip.nu/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://translate.google.com/translate?u=http%3A%2F%2Fwww.myip.nu&langpair=en%7Cen&hl=en&ie=UTF-8&ie=UTF-8&oe=UTF-8&prev=%2Flanguage_tools
Go Links
Google inurl:smartguestbook.asp Search Web 57 blocked AutoFill Options smartguestbook asp
Google
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. your-name.nu Go!
Done, but with errors on page.
Internet

Google Hacking

- Google Automated Scanning
  - Google doesn't like the idea about automating Google scan. They issue a free licence limited to 1000 queries/ day to Google
  - Gooscan
  - Gooscan is a UNIX (Linux/BSD/Mac OS X) tool that automates queries against Google search appliances, which helps to do the external vulnerability assessment. For more information about this tool, including the ethical implications of its use. See: http://johnny.ihackstuff.com

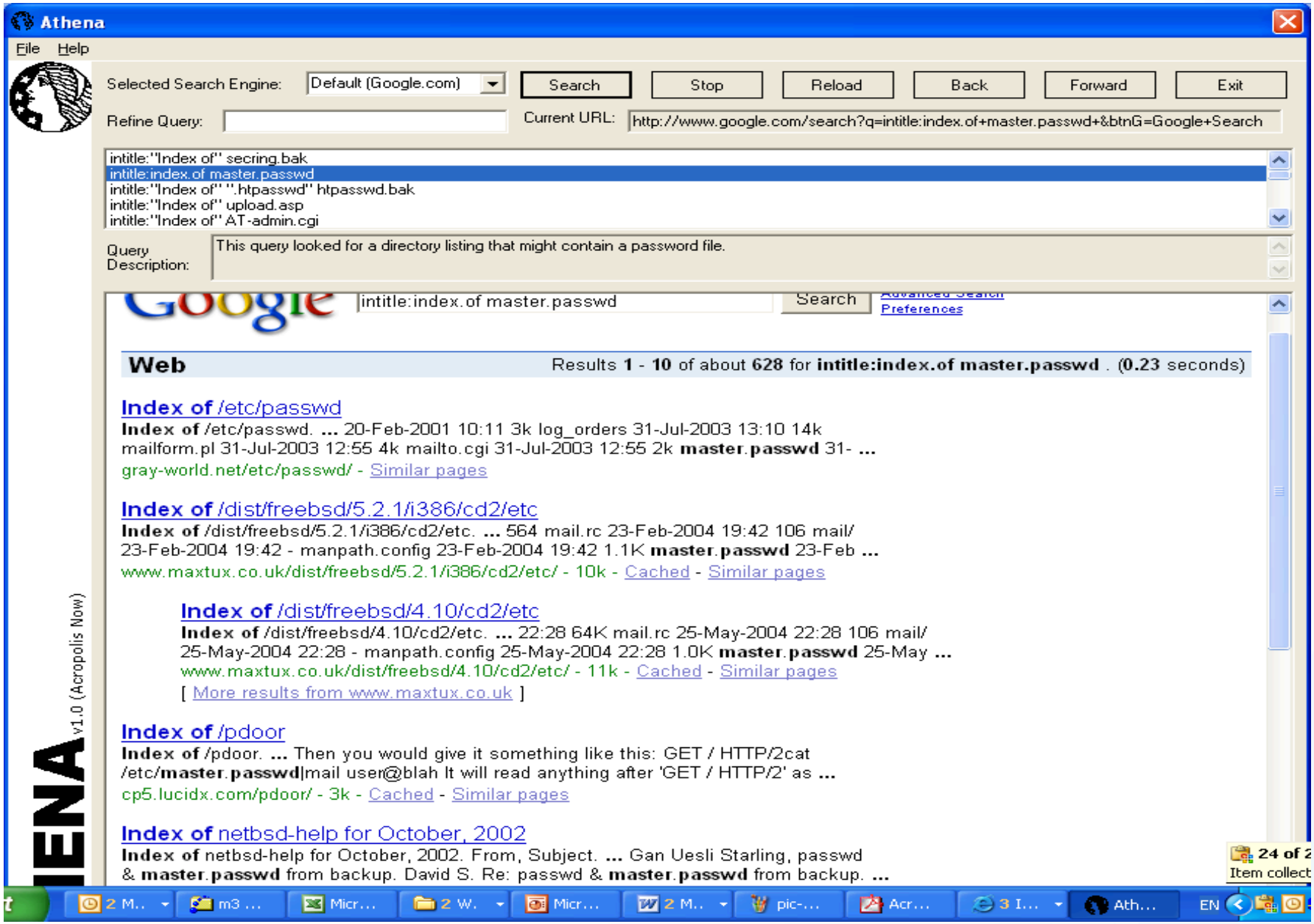
Google Hacking

- Google Automated Tools
  - SiteDigger
  - SiteDigger searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and interesting security nuggets on Web sites. See: 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:
E980ISBQFHK1K9zQjxzKi5iuJ37HA8If

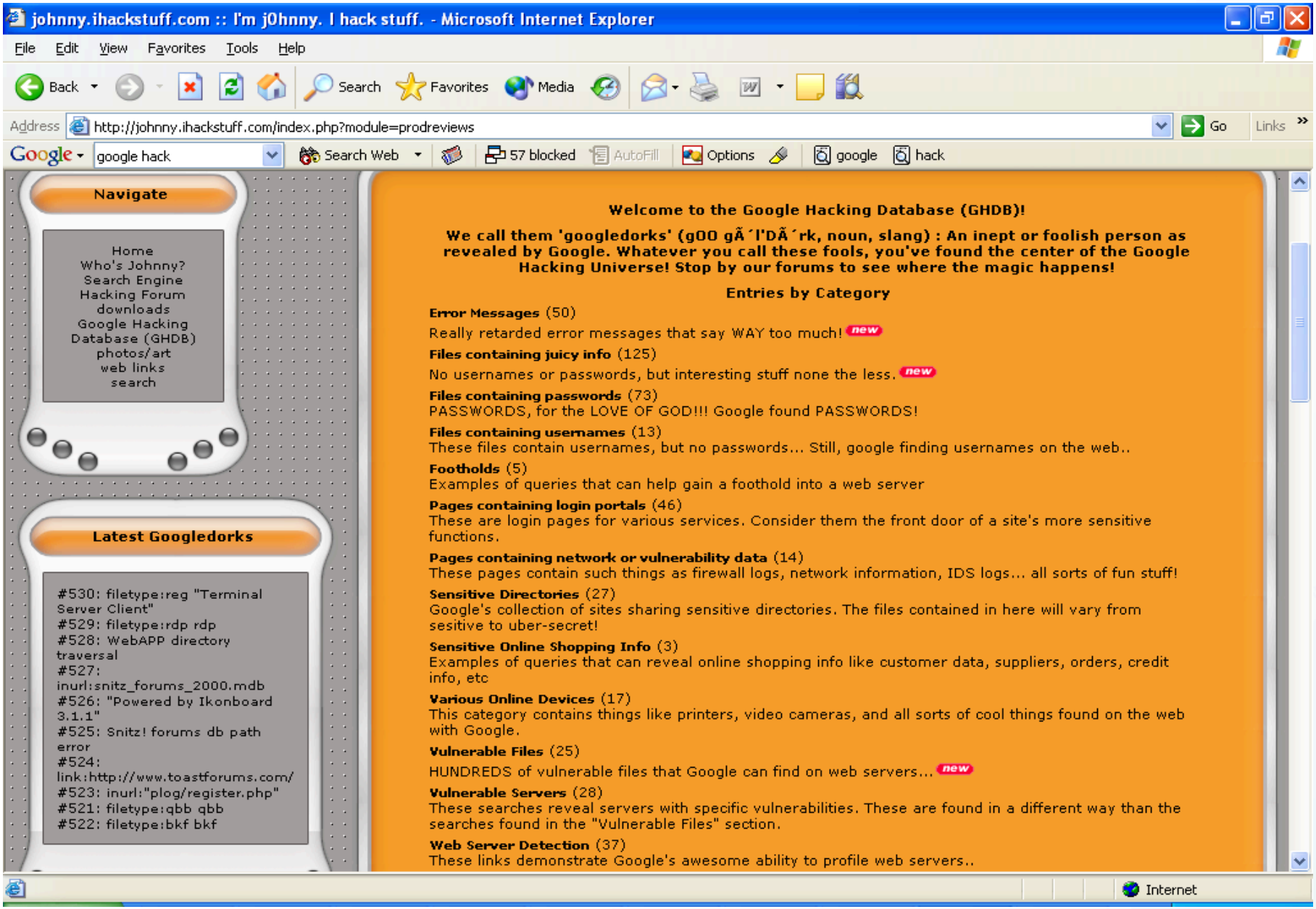
Google Hacking

- Google Automated Tools
  - Athena
  - Another Google query tool. It supports an open XML configuration format to support multiple search engines (not just Google)


Athena
File Help
Selected Search Engine: Default (Google.com)
Search
Stop
Reload
Back
Forward
Exit
Refine Query:
Current URL: http://www.google.com/search?q=intitle:index.of+master.passwd+&btnG=Google+Search
intitle:"Index of" secring.bak
intitle:index.of master.passwd
intitle:"Index of" ".htpasswd" htpasswd.bak
intitle:"Index of" upload.asp
intitle:"Index of" AT-admin.cgi
Query Description:
This query looked for a directory listing that might contain a password file.
Google
intitle:index.of master.passwd
Search
Advanced Search
Preferences
Web
Results 1 - 10 of about 628 for intitle:index.of master.passwd . (0.23 seconds)
Index of /etc/passwd
Index of /etc/passwd. ... 20-Feb-2001 10:11 3k log_orders 31-Jul-2003 13:10 14k
mailform.pl 31-Jul-2003 12:55 4k mailto.cgi 31-Jul-2003 12:55 2k master.passwd 31- ...
gray-world.net/etc/passwd/ - Similar pages
Index of /dist/freebsd/5.2.1/i386/cd2/etc
Index of /dist/freebsd/5.2.1/i386/cd2/etc. ... 564 mail.rc 23-Feb-2004 19:42 106 mail/
23-Feb-2004 19:42 - manpath.config 23-Feb-2004 19:42 1.1K master.passwd 23-Feb ...
www.maxtux.co.uk/dist/freebsd/5.2.1/i386/cd2/etc/ - 10k - Cached - Similar pages
Index of /dist/freebsd/4.10/cd2/etc
Index of /dist/freebsd/4.10/cd2/etc. ... 22:28 64K mail.rc 25-May-2004 22:28 106 mail/
25-May-2004 22:28 - manpath.config 25-May-2004 22:28 1.0K master.passwd 25-May ...
www.maxtux.co.uk/dist/freebsd/4.10/cd2/etc/ - 11k - Cached - Similar pages
[More results from www.maxtux.co.uk]
Index of /pdoor
Index of /pdoor. ... Then you would give it something like this: GET / HTTP/2cat
/etc/master.passwd|mail user@blah It will read anything after 'GET / HTTP/2' as ...
cp5.lucidx.com/pdoor/ - 3k - Cached - Similar pages
Index of netbsd-help for October, 2002
Index of netbsd-help for October, 2002. From, Subject. ... Gan Uesli Starling, passwd
& master.passwd from backup. David S. Re: passwd & master.passwd from backup. ...
HENA v1.0 (Acropolis Now)
24 of 2
Item collect
2 M...
m3 ...
Micr...
2 W...
Micr...
2 M...
pic-...
Acr...
3 I...
Ath...
EN

Google Hacking

- Google Materials
  - Googledorks
  - The famous Google Hack Website, it has many different examples of unbelievable things: http://johnny.ihackstuff.com.

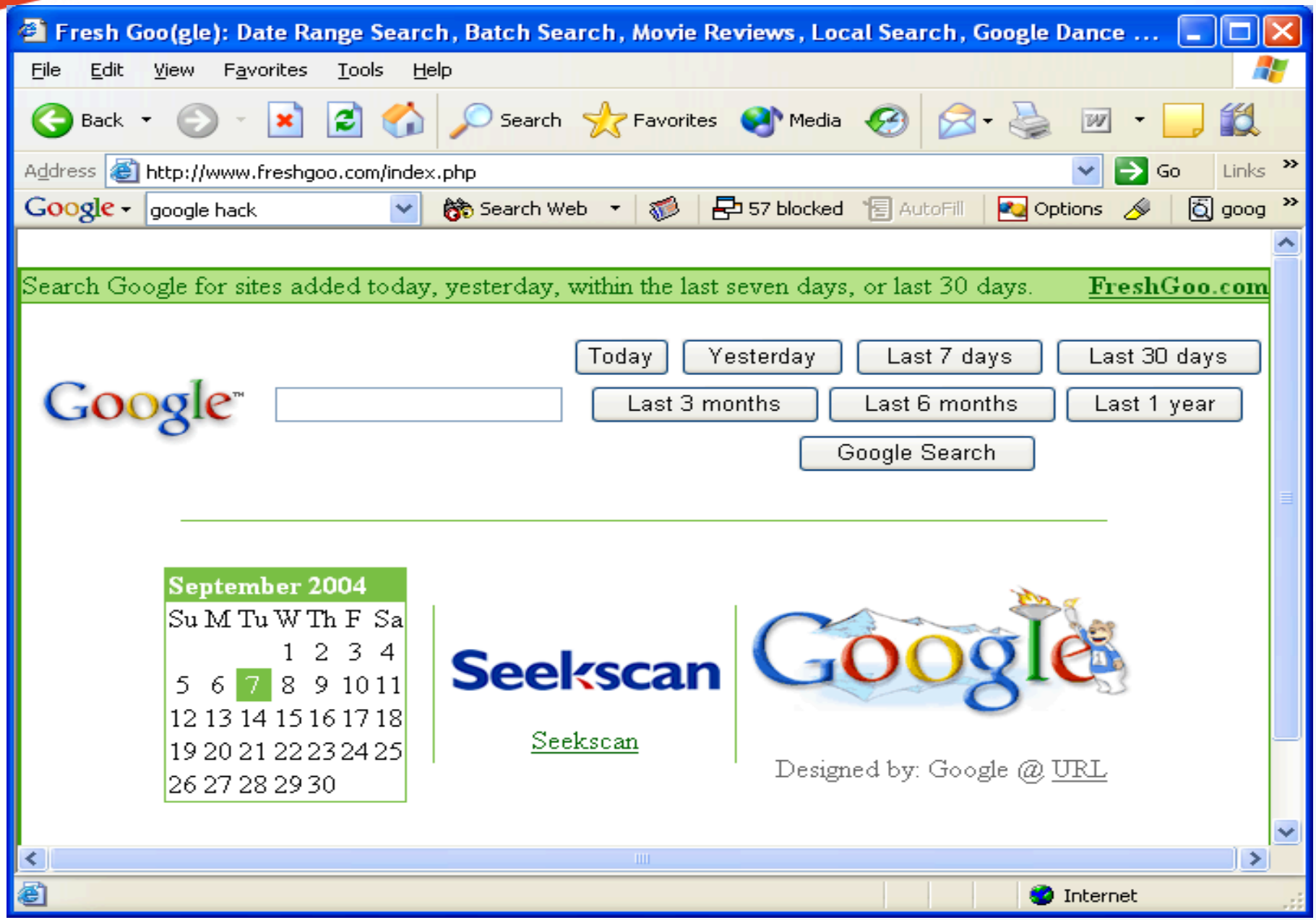

johnny.ihackstuff.com :: I'm j0hnny. I hack stuff. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://johnny.ihackstuff.com/index.php?module=prodreviews
Go Links
Google google hack
Search Web
57 blocked
AutoFill
Options
google
hack
Navigate
Home
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 sesitive 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..
Internet

Google Hacking

10 most popular entries	10 most recent entries
1) index.of.password	1) intitle:"Object not found!" intext:"Apache/2.0.* (Linux/SuSE)"
2) "access denied for user" "using password"	2) inurl:netw_tcp.shtml
3) auth_user_file.txt	3) intitle:"WebJeff - FileManager" intext:"login" intext:Pass|PAsse
4) The Master List	4) intitle:"EMUMAIL - Login" "Powered by EMU Webmail"
5) allinurl: admin mdb	5) intitle:"Open WebMail" "Open WebMail version (2.20|2.21|2.30) "
6) "A syntax error has occurred" filetype:ihtml	6) intitle:"error 404" "From RFC 2068 "
7) passlist.txt (a better way)	7) intitle:"Directory Listing, Index of /*/"
8) ORA-00921: unexpected end of SQL command	8) "Powered by Caudium Webserver" -caudium.net
9) Look in my backup directories! Please?	9) intitle:"IBM HTTP Server" "Use the Administration Server to configure"
10) config.php	10) intitle:"Lotus Domino Go Webserver:" "Tuning your webserver" -site:ibm.com

Google Hacking

- Google Materials
  - **Freshgoo**
  - Search Google for the page published on today, yesterday, within the last seven days or last 30 days: http://www.freshgoo.com/index.php


Fresh Goo(gle): Date Range Search, Batch Search, Movie Reviews, Local Search, Google Dance ...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.freshgoo.com/index.php
Go Links
Google google hack
Search Web 57 blocked AutoFill Options goog
Search Google for sites added today, yesterday, within the last seven days, or last 30 days.
FreshGoo.com
Today
Yesterday
Last 7 days
Last 30 days
Google
Last 3 months
Last 6 months
Last 1 year
Google Search
September 2004
Su M Tu W Th F Sa
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30
Seekscan
Seekscan
Google
Designed by: Google @ URL
Internet

Google Hacking

- Protect Your Data
  - Keep patching your systems and applications
  - Keep your sensitive data off the Web apply authentication
    - (RSA, Clienless VPN)
  - Disable directory browsing
  - Google hack your Website
  - Consider removing your site from Google's index: http://www.google.com/remove.html.
  - Use a robots.txt file to against Web crawlers: http://www.robotstxt.org.

Google Hacking References

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, Jonhnny 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

GoSecure

Contact Information:

Robert Masse
rmasse@gosecure.ca
www.GoSecure.ca

407 McGill, suite 900
Montréal, Québec, Canada
H2Y 2G2

514-287-7427