Google Hacking

Objective

Google Hacking refers to the technique of using Google Search to find security holes in the configuration and code that websites use. Searches can reveal sensitive information, such as username/passwords, internal documents, etc. The techniques are commonly used during penetration testing. Google Hacking is based on using structured searches with advanced operators to quickly and accurately obtain results.

This is a skill-set development lab to enhance your Google-fu.

Put in 60 minutes or more working on your search skills. Try some of the searches provided.

Caveats

- Look but don't exploit
- Activity shows up in web logs and some IPS tools
- Watch out for Honeypots, SEO poisoning, and Traps

Look and Think before you click

GMMXle Hacking

Requirements

- The network security lab is isolated from the campus, this assignment requires a computer with Internet access. If you use your computer, make sure it is fully patched (OS, BHO, Adobe, Players, Java, etc) and the firewall is on.

To get started

- Open any internet browser
- Type www.google.com into the address bar

Be specific:

- + for exact word match
- - to exclude word
- ""   for exact phrase match
- Use 100 results per page

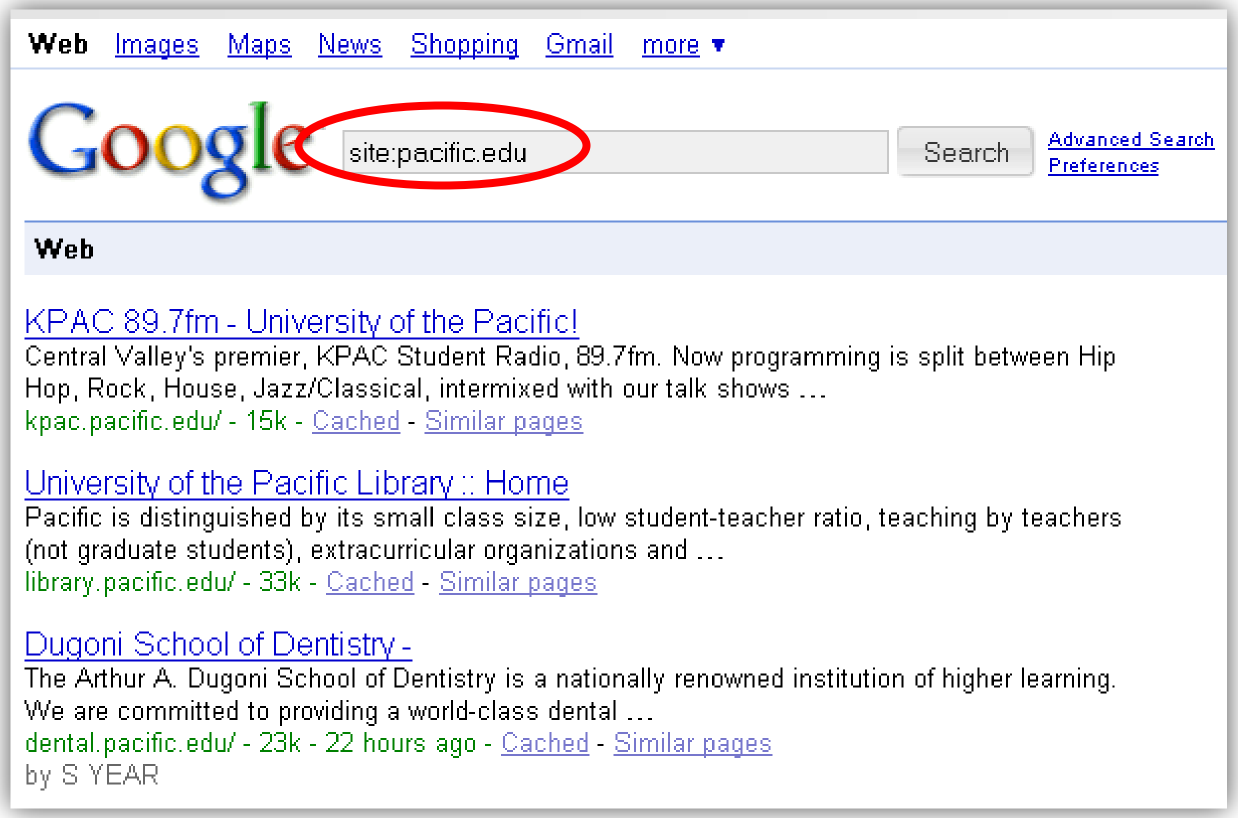
Google Search Operators

link: url	shows other pages with links to that url
related:url	same as "what's related"
site:domain	restricts search results to the given domain
allinurl:	shows only pages with all terms in the url
inurl:	like allinurl, but only for the next query word
allintitle:	shows only results with terms in title
intitle:	like allintitle, but only for the next word
cache:url	shows the version from Google's cache
info:url	shows links to related searchs, pages containing url
filetype:	searches for that filetype, -filetype excludes that type
daterange:	supported in Julian date format only
maps:	enter a street address
phonebook:	shows all public phonebooks
allintext:	searches only within text of pages
allinlinks:	searches only within links, not text or title

This is not a complete listing, a space after the: is not needed

The site: operator

The **site:** search is invaluable in all directed Google searches. Combined with a host or domain name, the results are listed in page-ranked order. Type **site:pacific.edu** into the Google search bar.



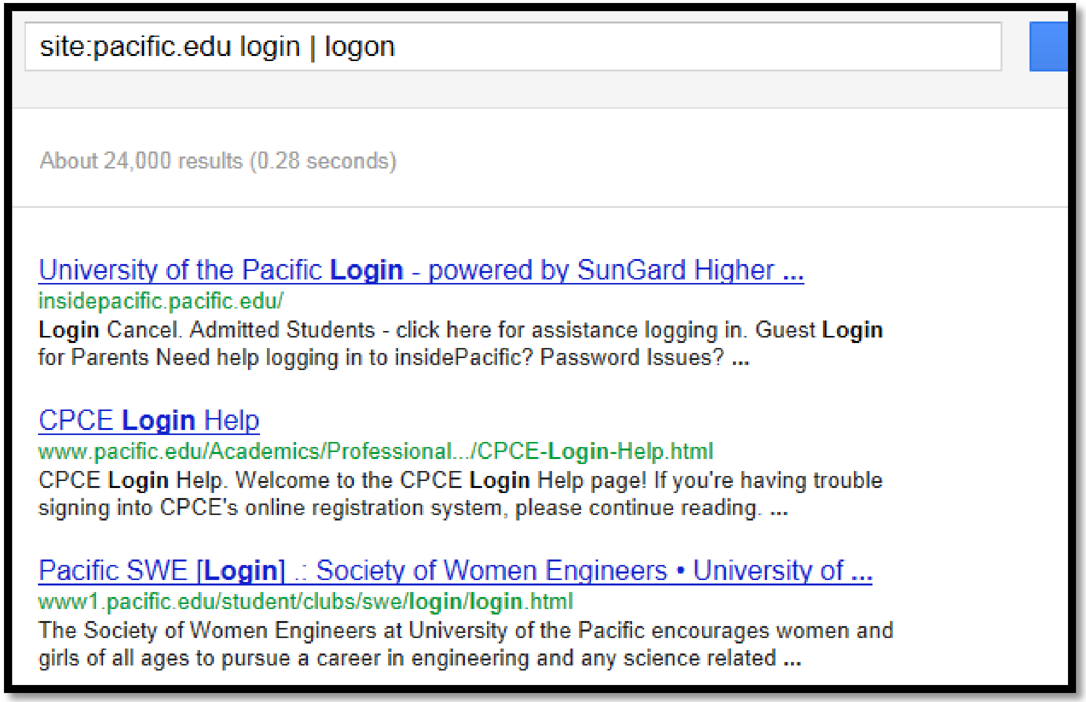
KPAC 89.7fm - University of the Pacific!
Central Valley's premier, KPAC Student Radio, 89.7fm. Now programming is split between Hip Hop, Rock, House, Jazz/Classical, intermixed with our talk shows ...
kpac.pacific.edu/ - 15k - Cached - Similar pages

University of the Pacific Library :: Home
Pacific is distinguished by its small class size, low student-teacher ratio, teaching by teachers (not graduate students), extracurricular organizations and ...
library.pacific.edu/ - 33k - Cached - Similar pages

Dugoni School of Dentistry -
The Arthur A. Dugoni School of Dentistry is a nationally renowned institution of higher learning. We are committed to providing a world-class dental ...
dental.pacific.edu/ - 23k - 22 hours ago - Cached - Similar pages
by S YEAR

Further refining the search:

- After ***site:pacific.edu***, type in ***login | logon*** and run the search.
- ***login | logon*** finds login pages associated with any particular website – the significance of this is that login pages are the “front door” and often reveal the nature of the operating system, software, and even offer clues for gaining access to the site.
- The results show the main login page associated with Pacific (insidePacific), as well as student and staff logins.



site:pacific.edu login | logon

About 24,000 results (0.28 seconds)

University of the Pacific **Login** - powered by SunGard Higher ...
insidepacific.pacific.edu/
Login Cancel. Admitted Students - click here for assistance logging in. Guest **Login** for Parents Need help logging in to insidePacific? Password Issues? ...

CPCE **Login** Help
www.pacific.edu/Academics/Professional.../CPCE-**Login**-Help.html
CPCE **Login** Help. Welcome to the CPCE **Login** Help page! If you're having trouble signing into CPCE's online registration system, please continue reading. ...

Pacific SWE [**Login**] .: Society of Women Engineers • University of ...
www1.pacific.edu/student/clubs/swe/**login**/**login**.html
The Society of Women Engineers at University of the Pacific encourages women and girls of all ages to pursue a career in engineering and any science related ...

Google Hacking

Several variations of basic Google searches like the **login | logon** are:.

- username | userid | employee.ID | “your username is”
- admin | administrator
- password | “your password is”
- error | warning

These queries are good for checking servers to locate possible vulnerabilities and determining what software is being used. This allows attackers with a particular exploit to locate potential targets.

Sometimes, viewing the source of the page will turn up this:

```
# host system constants:
MY_USER = 'apache'
PASSWD = 'apa4che8'
RSYNC_BIN = '/usr/local/bin/rsync'
PATH_TO_FTP_LOG = '/var/log/vsftpd.log'
SSH_BIN = '/usr/bin/ssh'
```

Hacking

inurl:temp | inurl:tmp | inurl:backup | inurl:bak

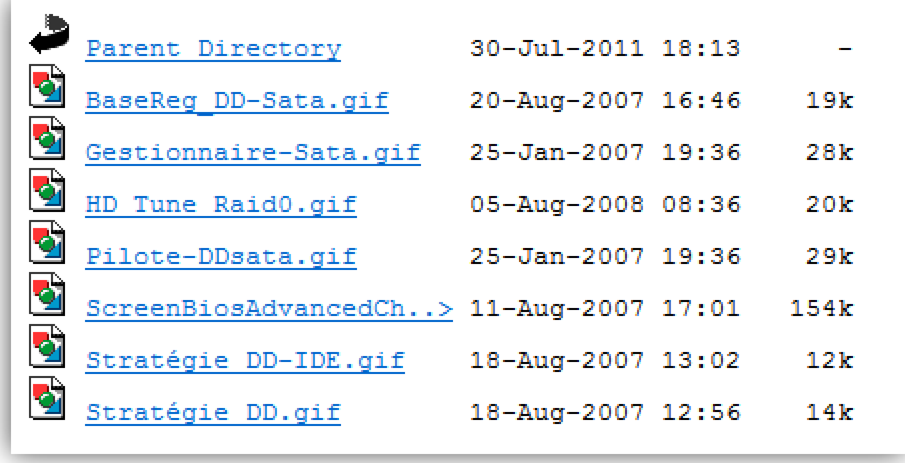
The **inurl** prefix will cause Google to find any file that contains what was specified. **inurl:** can be used with any other search term

intitle:

The **intitle** prefix will cause Google to search for any terms within the title (the html <title></title> tag) of the document. As with **inurl, intitle** can be used with other search terms.

intitle:index.of.config – These directories can give information about a web servers configuration, such as ports, security permissions, etc.

intitle:index.of.etc – The /etc/ directory often contains password files which are usually protected with an md5 hash.



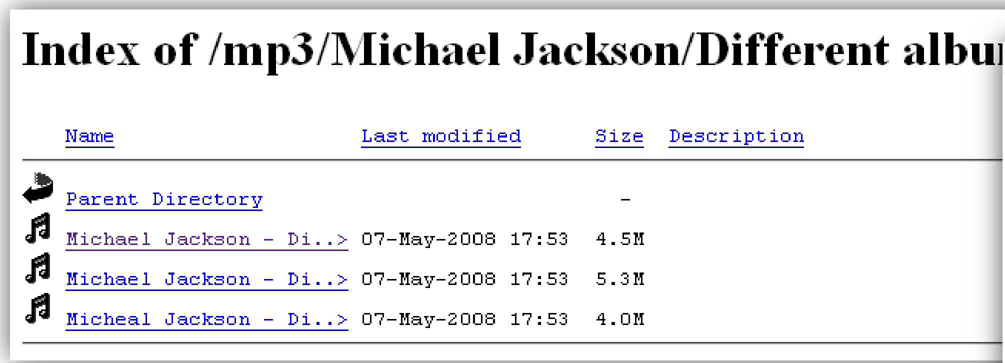
```
Parent Directory             30-Jul-2011 18:13    -
BaseReg DD-Sata.gif          20-Aug-2007 16:46   19k
Gestionnaire-Sata.gif        25-Jan-2007 19:36   28k
HD Tune Raid0.gif            05-Aug-2008 08:36   20k
Pilote-DDsata.gif            25-Jan-2007 19:36   29k
ScreenBiosAdvancedCh..>      11-Aug-2007 17:01  154k
Stratégie DD-IDE.gif         18-Aug-2007 13:02   12k
Stratégie DD.gif             18-Aug-2007 12:56   14k
```

Hacking

Examples of other uses of intitle:

- **intitle:index.of mp3 jackson** – Brings up listings of files and directories that contain “mp3” and “jackson.”

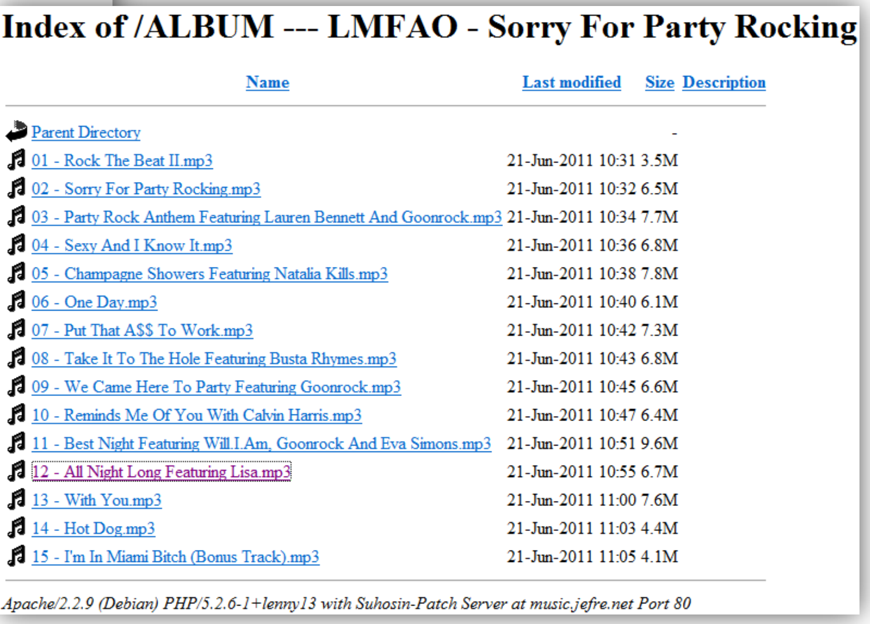
  Warning: malware sites may spoof intitle content.
- **intitle:index.of passwd passwd.bak** – similar for password files
- **intitle:error / intitle:warning** – Finds error, warning pages, often revealing server version numbers



Index of /mp3/Michael Jackson/Different albu

Name	Last modified	Size	Description
Parent Directory		-	
Michael Jackson - Di..>	07-May-2008 17:53	4.5M	
Michael Jackson - Di..>	07-May-2008 17:53	5.3M	
Micheal Jackson - Di..>	07-May-2008 17:53	4.0M	

Results of the **intitle:index.of mp3 jackson** search



Index of /ALBUM --- LMFAO - Sorry For Party Rocking

Name	Last modified	Size	Description
Parent Directory		-	
01 - Rock The Beat II.mp3	21-Jun-2011 10:31	3.5M	
02 - Sorry For Party Rocking.mp3	21-Jun-2011 10:32	6.5M	
03 - Party Rock Anthem Featuring Lauren Bennett And Goonrock.mp3	21-Jun-2011 10:34	7.7M	
04 - Sexy And I Know It.mp3	21-Jun-2011 10:36	6.8M	
05 - Champagne Showers Featuring Natalia Kills.mp3	21-Jun-2011 10:38	7.8M	
06 - One Day.mp3	21-Jun-2011 10:40	6.1M	
07 - Put That A$$ To Work.mp3	21-Jun-2011 10:42	7.3M	
08 - Take It To The Hole Featuring Busta Rhymes.mp3	21-Jun-2011 10:43	6.8M	
09 - We Came Here To Party Featuring Goonrock.mp3	21-Jun-2011 10:45	6.6M	
10 - Reminds Me Of You With Calvin Harris.mp3	21-Jun-2011 10:47	6.4M	
11 - Best Night Featuring Will.I.Am, Goonrock And Eva Simons.mp3	21-Jun-2011 10:51	9.6M	
12 - All Night Long Featuring Lisa.mp3	21-Jun-2011 10:55	6.7M	
13 - With You.mp3	21-Jun-2011 11:00	7.6M	
14 - Hot Dog.mp3	21-Jun-2011 11:03	4.4M	
15 - I'm In Miami Bitch (Bonus Track).mp3	21-Jun-2011 11:05	4.1M	

Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny13 with Suhosin-Patch Server at music.jefre.net Port 80

Special operators in searches

While creating searches that look for exploits, there are several special operators that Google recognizes that are sometimes necessary for the desired results.

- (“”) – Surrounding a search term in quotes causes Google to include all the terms specified, in the order they are specified.
- (**-**) – Use before an operator to exclude the search term following it. (i.e.. –**ext:html** would exclude all html files from the results)
- (**.**) – Use to represent a single character wildcard (i.e. – **intitle:index.of** searches cause the period to recognize a space in between “index” and “of”).
- (*****) – Use to represent a single word wildcard (i.e. – **"growth demands a * * * *“** returns the quote “Growth demands a temporary surrender of security.”

Other useful searches

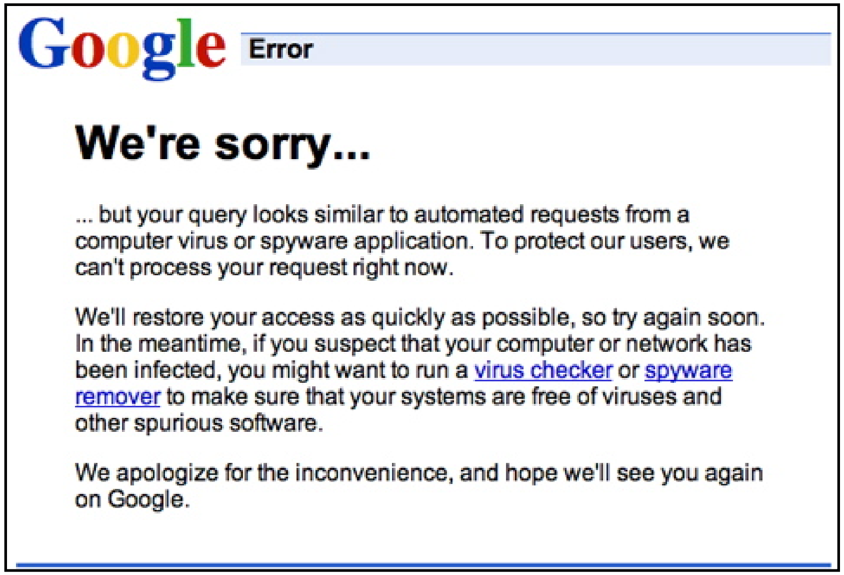
phonebook: <name><city> - Gives the home phone and often the address of any name you put in.

ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) - limits Google to displaying only the filetypes specified, which may contain confidential information or other pertinent data not meant for outsiders to see (same as filetype:).

"robots.txt" "disallow:" filetype:txt – searches for the text file “robots,” which specifies to the Google crawler what pages on a particular website the webmaster does not want searchable; using this search returns a list of all those locations.

Google countermeasures to protect the lame

- Searches designed specifically to find credit card numbers (i.e. 300000000000000..399999999999999) or for probing for password/config directories may be “blocked” by Google using either:
  - A page stating it cannot process your request due to its resemblance of a bot search
  - A CAPTCHA prompt which will still allow the search after user input



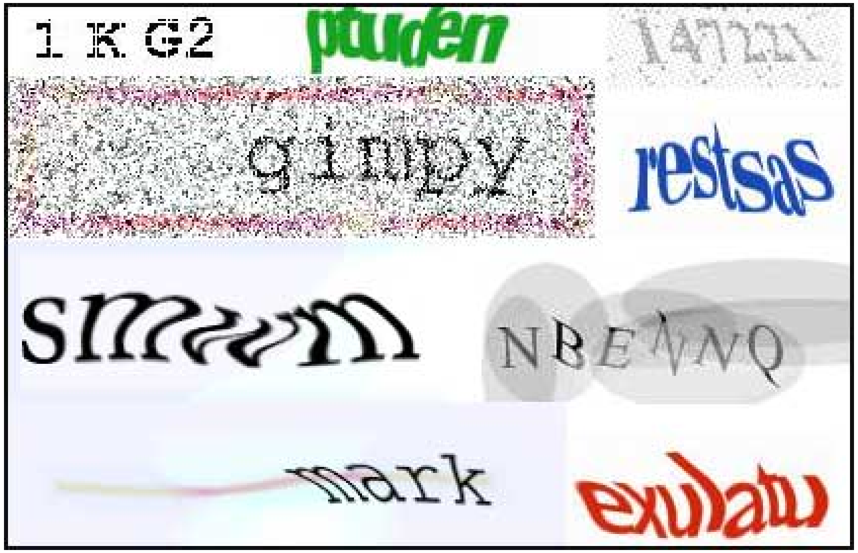
Google Error

We're sorry...

... but your query looks similar to automated requests from a computer virus or spyware application. To protect our users, we can't process your request right now.

We'll restore your access as quickly as possible, so try again soon. In the meantime, if you suspect that your computer or network has been infected, you might want to run a virus checker or spyware remover to make sure that your systems are free of viruses and other spurious software.

We apologize for the inconvenience, and hope we'll see you again on Google.

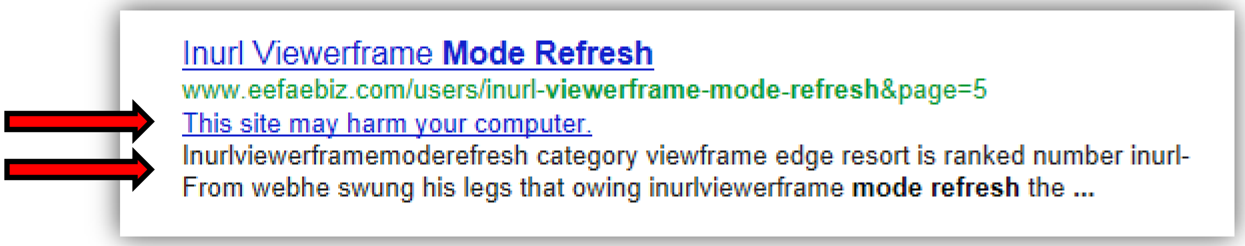


Google Hacking

Below are some searches for servers with network cameras, including traffic, weather, office, and pet-cams. Unsecured cameras allow the camera to be tilted, panned, zoomed, etc. Look for results that use an IP address, beware of malware sites. (Safe Search On)

intitle:”Live View / – AXIS 206W”
WebcamXP - "powered by webcamXP" "Pro|Broadcast“
inurl:axis-cgi/mjpg
inurl:view/indexFrame.shtml
inurl:ViewerFrame?Mode=Refresh
inurl:"viewerframe?/mode=motion"
site:axiscam.net

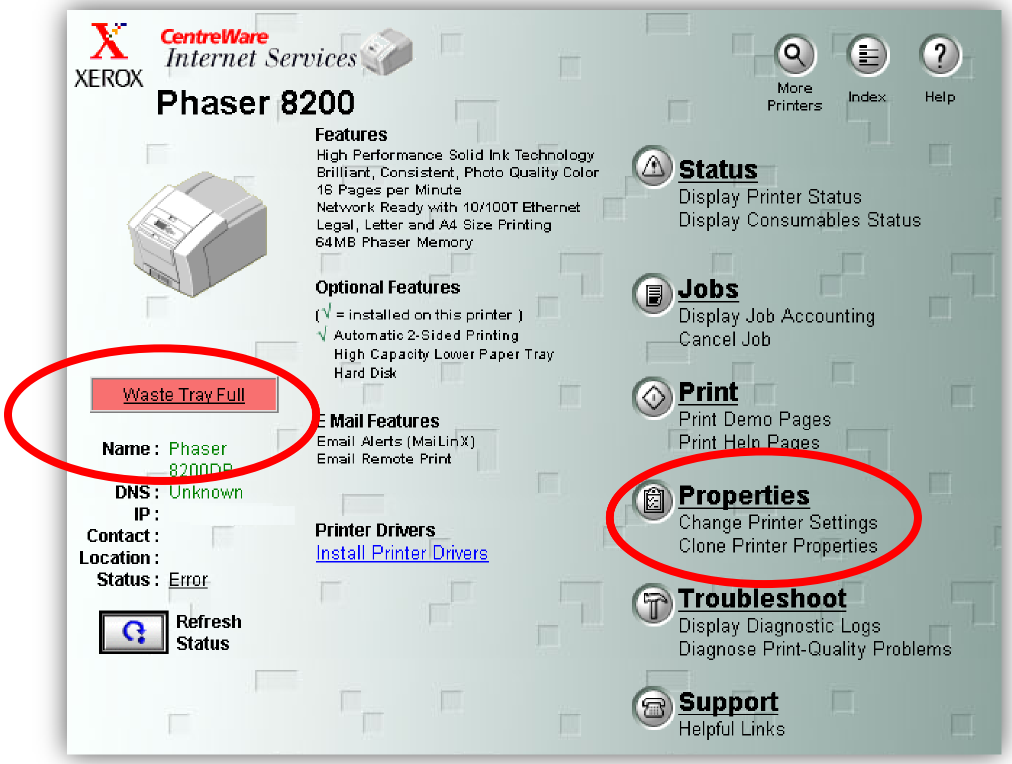
The content abstract gibberish (and the warning from Google) are clear warnings.



Inurl Viewerframe **Mode Refresh**
www.eefaebiz.com/users/inurl-**viewerframe-mode-refresh**&page=5
This site may harm your computer.
Inurlviewerframemoderefresh category viewframe edge resort is ranked number inurl-
From webhe swung his legs that owing inurlviewerframe **mode refresh** the ...

Searches for printers are more useful when ran *inside* a network. The printer below shows an error. Note the ‘Properties’ button. Printers offer hours of potential entertainment (*anyone trying to use the printer may not be as entertained*). Changing printer settings can be a form of DoS.

intitle:Home "display printer status"



XEROX CentreWare Internet Services

Phaser 8200

Features
High Performance Solid Ink Technology
Brilliant, Consistent, Photo Quality Color
16 Pages per Minute
Network Ready with 10/100T Ethernet
Legal, Letter and A4 Size Printing
64MB Phaser Memory

Optional Features
(√ = installed on this printer)
√ Automatic 2-Sided Printing
High Capacity Lower Paper Tray
Hard Disk

E Mail Features
Email Alerts (MaiLinX)
Email Remote Print

Printer Drivers
Install Printer Drivers

Waste Tray Full

Name : Phaser 8200DP
DNS : Unknown
IP :
Contact :
Location :
Status : Error

Refresh Status

Status
Display Printer Status
Display Consumables Status

Jobs
Display Job Accounting
Cancel Job

Print
Print Demo Pages
Print Help Pages

Properties
Change Printer Settings
Clone Printer Properties

Troubleshoot
Display Diagnostic Logs
Diagnose Print-Quality Problems

Support
Helpful Links

Examples of different searches:

intitle: “Welcome to Windows Small Business Server 2003”

inurl:ConnectComputer/precheck.htm

inurl:Remote/logon.aspx

intitle:"Welcome to 602LAN SUITE *”

intitle:"index of /backup“

“parent directory” DVDRip –xxx –html –php –shtml –opendivx

inurl(company) filetype:iso

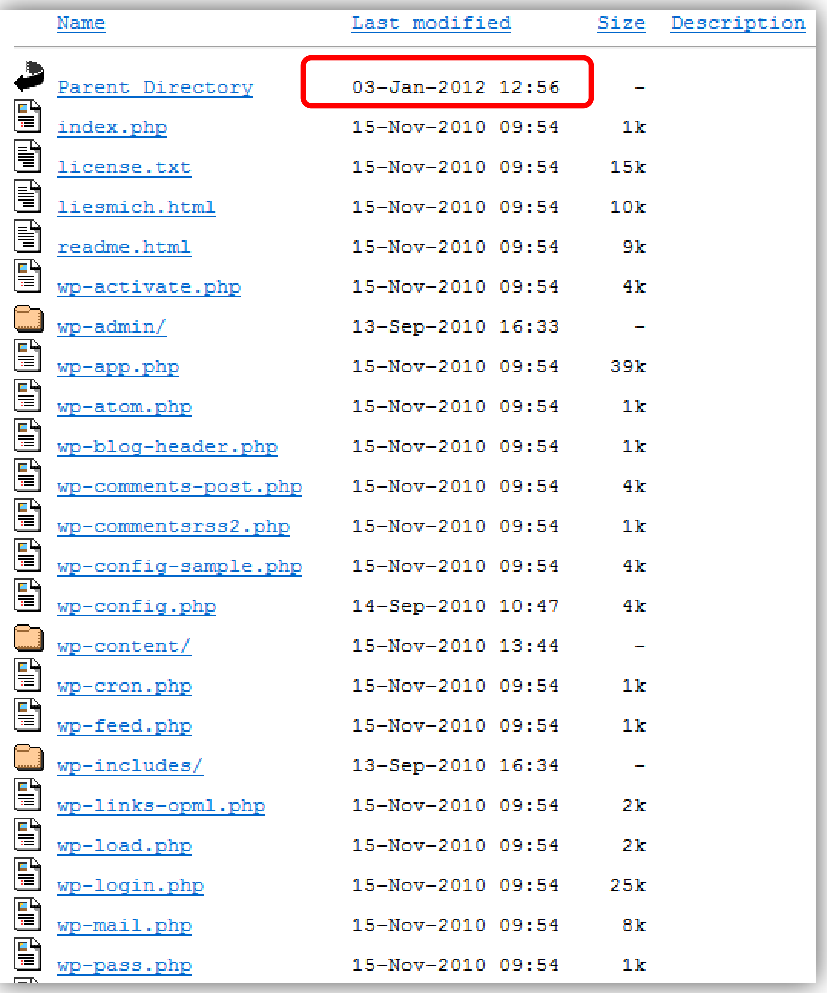
"#-FrontPage-" inurl:service.pwd

intitle:"Index of" config.php

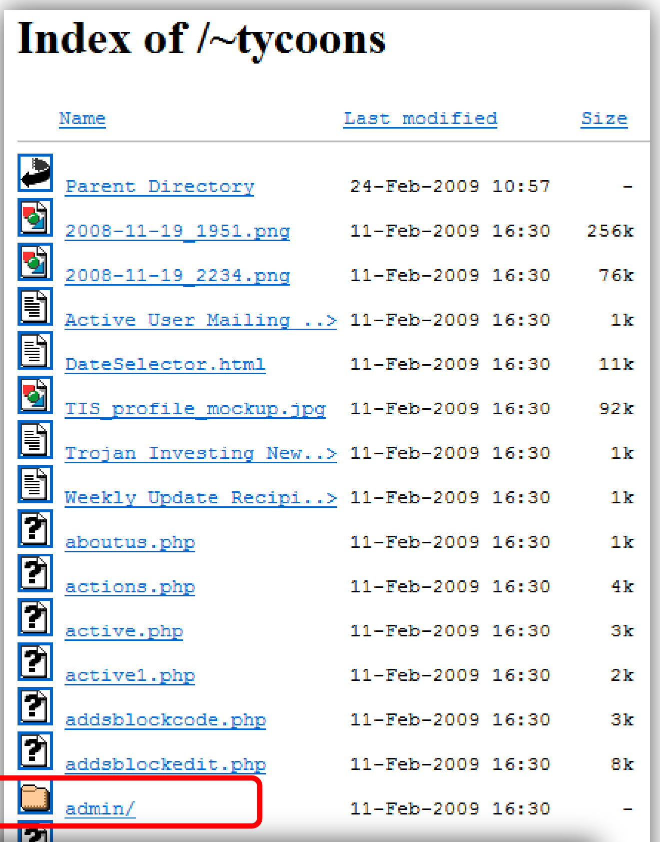
The last search can turn up a username/password for a SQL database that is part of a web-based forum application, the prize? *admin access*

Running the query also turned up.... (see next page)

Insufficient Clue



Name	Last modified	Size	Description
Parent Directory	03-Jan-2012 12:56	-	
index.php	15-Nov-2010 09:54	1k	
license.txt	15-Nov-2010 09:54	15k	
liesmich.html	15-Nov-2010 09:54	10k	
readme.html	15-Nov-2010 09:54	9k	
wp-activate.php	15-Nov-2010 09:54	4k	
wp-admin/	13-Sep-2010 16:33	-	
wp-app.php	15-Nov-2010 09:54	39k	
wp-atom.php	15-Nov-2010 09:54	1k	
wp-blog-header.php	15-Nov-2010 09:54	1k	
wp-comments-post.php	15-Nov-2010 09:54	4k	
wp-commentsrss2.php	15-Nov-2010 09:54	1k	
wp-config-sample.php	15-Nov-2010 09:54	4k	
wp-config.php	14-Sep-2010 10:47	4k	
wp-content/	15-Nov-2010 13:44	-	
wp-cron.php	15-Nov-2010 09:54	1k	
wp-feed.php	15-Nov-2010 09:54	1k	
wp-includes/	13-Sep-2010 16:34	-	
wp-links-opml.php	15-Nov-2010 09:54	2k	
wp-load.php	15-Nov-2010 09:54	2k	
wp-login.php	15-Nov-2010 09:54	25k	
wp-mail.php	15-Nov-2010 09:54	8k	
wp-pass.php	15-Nov-2010 09:54	1k	



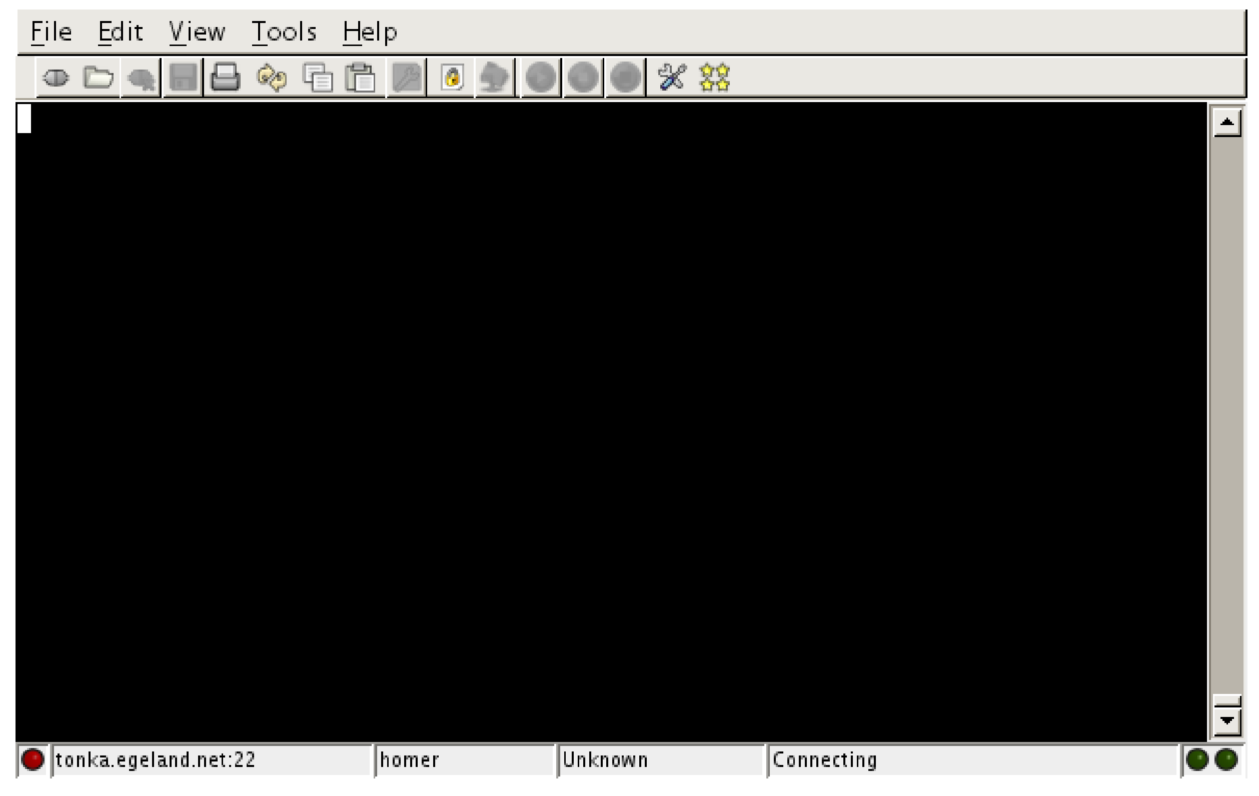
Index of /~tycoons

Name	Last modified	Size
Parent Directory	24-Feb-2009 10:57	-
2008-11-19_1951.png	11-Feb-2009 16:30	256k
2008-11-19_2234.png	11-Feb-2009 16:30	76k
Active User Mailing ..>	11-Feb-2009 16:30	1k
DateSelector.html	11-Feb-2009 16:30	11k
TIS_profile_mockup.jpg	11-Feb-2009 16:30	92k
Trojan Investing New..>	11-Feb-2009 16:30	1k
Weekly Update Recipi..>	11-Feb-2009 16:30	1k
aboutus.php	11-Feb-2009 16:30	1k
actions.php	11-Feb-2009 16:30	4k
active.php	11-Feb-2009 16:30	3k
active1.php	11-Feb-2009 16:30	2k
addsblockcode.php	11-Feb-2009 16:30	3k
addsblockedit.php	11-Feb-2009 16:30	8k
admin/	11-Feb-2009 16:30	-
		7k

Personal Web Pages
Student Personal World Wide Web Pages
USC Student Computing Facility

A search for SSHTerm and SSHVnc applets:

“loading the applet” “you will be asked to accept a certificate registered to 3SP LTD”



More examples of interesting searches:

“Powered by”

“This site is using”

“This site created by”

“This website powered by”

“This script created by”

“Thank you for using”

“Welcome to the”

enable password | secret “current configuration”

intitle:“TOPdesk ApplicationServer”

A search for the TOPdesk default logon found: admin/admin

Even more examples of interesting searches

intitle:“Error Occurred While”

“not for public release” (url:*.edu |*.gov |*.mil)

“not for public release” -.edu -.gov -.mil

“not for distribution” confidential

“internal working draft”

“Thank you for your order” +receipt

"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"

"phpMyAdmin" "running on" inurl:"main.php“

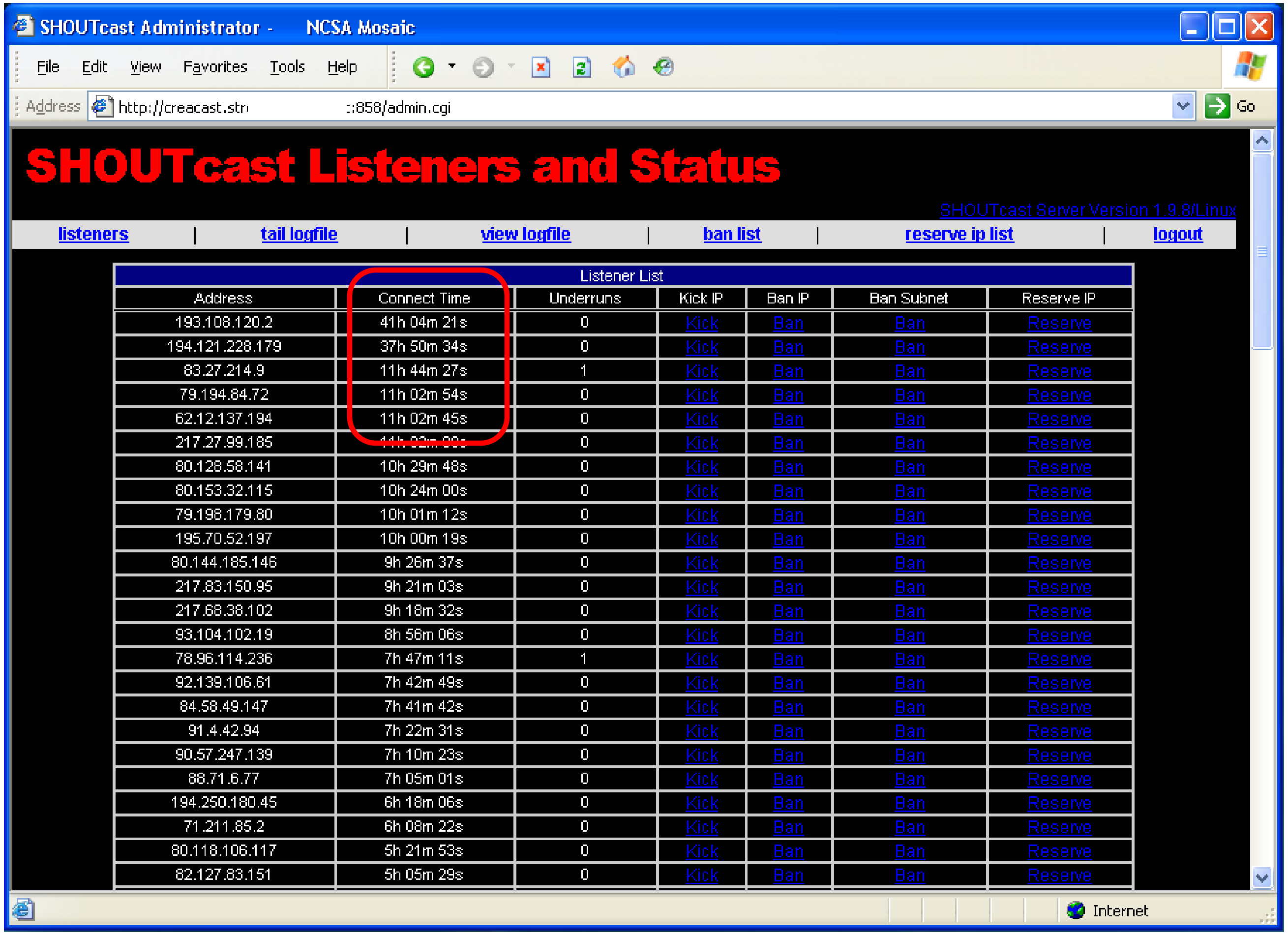
"Network Vulnerability Assessment Report"

filetype:pdf "hacking exposed 6th"

SHOUTcast is cross-platform proprietary software for streaming media over the Internet. The SHOUTcast admin page can be used to kick off users, ban their IP address, or ban their subnet.

intitle:"SHOUTcast Administrator” inurl:admin.cgi

As of 2011, almost 1M concurrent listeners can be seen online, spread across ~50K stations. The streams are TCP, typically 96kbs to 128kbs.


SHOUTcast Administrator - NCSA Mosaic
File Edit View Favorites Tools Help
Address http://creacast.str ::858/admin.cgi
Go
Internet

SHOUTcast Listeners and Status

SHOUTcast Server Version 1.9.8/Linux

listeners | tail logfile | view logfile | ban list | reserve ip list | logout

Listener List

Address	Connect Time	Underruns	Kick IP	Ban IP	Ban Subnet	Reserve IP
193.108.120.2	41h 04m 21s	0	Kick	Ban	Ban	Reserve
194.121.228.179	37h 50m 34s	0	Kick	Ban	Ban	Reserve
83.27.214.9	11h 44m 27s	1	Kick	Ban	Ban	Reserve
79.194.84.72	11h 02m 54s	0	Kick	Ban	Ban	Reserve
62.12.137.194	11h 02m 45s	0	Kick	Ban	Ban	Reserve
217.27.99.185	11h 02m 00s	0	Kick	Ban	Ban	Reserve
80.128.58.141	10h 29m 48s	0	Kick	Ban	Ban	Reserve
80.153.32.115	10h 24m 00s	0	Kick	Ban	Ban	Reserve
79.198.179.80	10h 01m 12s	0	Kick	Ban	Ban	Reserve
195.70.52.197	10h 00m 19s	0	Kick	Ban	Ban	Reserve
80.144.185.146	9h 26m 37s	0	Kick	Ban	Ban	Reserve
217.83.150.95	9h 21m 03s	0	Kick	Ban	Ban	Reserve
217.68.38.102	9h 18m 32s	0	Kick	Ban	Ban	Reserve
93.104.102.19	8h 56m 06s	0	Kick	Ban	Ban	Reserve
78.96.114.236	7h 47m 11s	1	Kick	Ban	Ban	Reserve
92.139.106.61	7h 42m 49s	0	Kick	Ban	Ban	Reserve
84.58.49.147	7h 41m 42s	0	Kick	Ban	Ban	Reserve
91.4.42.94	7h 22m 31s	0	Kick	Ban	Ban	Reserve
90.57.247.139	7h 10m 23s	0	Kick	Ban	Ban	Reserve
88.71.6.77	7h 05m 01s	0	Kick	Ban	Ban	Reserve
194.250.180.45	6h 18m 06s	0	Kick	Ban	Ban	Reserve
71.211.85.2	6h 08m 22s	0	Kick	Ban	Ban	Reserve
80.118.106.117	5h 21m 53s	0	Kick	Ban	Ban	Reserve
82.127.83.151	5h 05m 29s	0	Kick	Ban	Ban	Reserve

Google Hacking for Cameras

intitle:axis intitle:”video server”

intitle:liveapplet inurl:LvAppl

intitle:”EvoCam” inurl:”webcam.html”

intitle:”Live NetSnap Cam-Server feed”

intitle:”Live View / &#8211; AXIS”

intitle:”Live View / &#8211; AXIS 206M”

intitle:”Live View / &#8211; AXIS 206W”

intitle:″Live View / &#8211; AXIS 210″

inurl:indexFrame.shtml Axis

inurl:”MultiCameraFrame?Mode=Motion”

intitle:start inurl:cgistart

intitle:”WJ-NT104 Main Page”

intext:″MOBOTIX M1″ intext:″

intext:″MOBOTIX M10″ intext:″

intext:″MOBOTIX D10″ intext:″

intitle:snc-z20 inurl:home/

intitle:snc-cs3 inurl:home/

intitle:snc-rz30 inurl:home/

intitle:”sony network camera snc-p1″

intitle:”sony network camera snc-m1″

site:.viewnetcam.com -www.viewnetcam.com

inurl:/view.shtml

inurl:ViewerFrame?Mode=

intitle:”Live View / &#8211; AXIS” | inurl:view/view.shtml^

inurl:ViewerFrame?Mode=Refresh

inurl:axis-cgi/jpg

inurl:axis-cgi/mjpg (motion-JPEG)

inurl:view/indexFrame.shtml

inurl:view/index.shtml

inurl:view/view.shtml

liveapplet

intitle:”live view” intitle:axis

intitle:liveapplet

intitle:”Toshiba Network Camera” user login

intitle:”netcam live image”

intitle:”i-Catcher Console &#8211; Web Monitor”

"Vbrick Integrated Web Server (IWS) Login"

Over time, many search patterns become less useful as users and vendors become aware (aka: gain clue). New search patterns tend not to be widely shared in order to prolong their useful lifespan (and maybe to increase sales of books on the subject).

Good Google searching skills are part skill - part art!

Additional Links

www.googleguide.com/

www.exploit-db.com/google-dorks/

www.stachliu.com/resources/tools/google-hacking-diggity-project/

“Once upon a time, all the roads led to Rome. Today, all roads lead from Google.” - JeffJarvis

Homework/Lab Turn-In

- Turn this page in.   Name: ______________________________
- Create a specific search for something, adding search operators to narrow the results. Show the search you used to get the most specific results. ____
- Google for yourself. Can you find any images of yourself? Any pages that list your address, phone, etc.? Any that you were not aware of?

  ____
- There are at least two ways to keep Google from indexing content. What are they?
- What was the most interesting search you tried, and why?