

# Google Hacking for Penetration Testers

Using Google as a Security Testing Tool

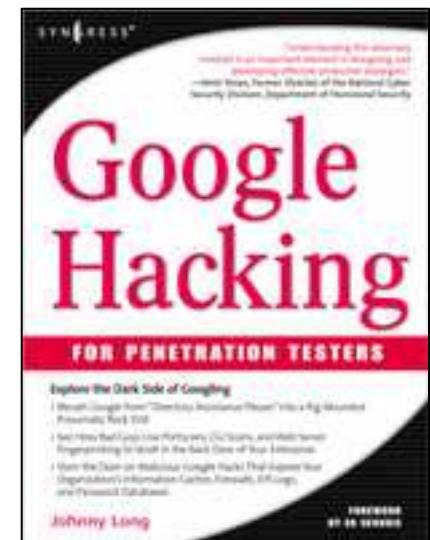
Johnny Long

[johnny@ihackstuff.com](mailto:johnny@ihackstuff.com)

---

## What we're doing

- I hate pimpin', but we're covering many techniques covered in the "Google Hacking" book.
- For much more detail, I encourage you to check out "Google Hacking for Penetration Testers" by Syngress Publishing.



# Advanced Operators

Before we can walk, we must run. In Google's terms this means understanding advanced operators.

---

## Advanced Operators

- Google advanced operators help refine searches.
- They are included as part of a standard Google query.
- Advanced operators use a syntax such as the following:

**operator:search\_term**

- There's no space between the operator, the colon, and the search term!

# Advanced Operators at a Glance

Advanced operators can be combined in some cases.

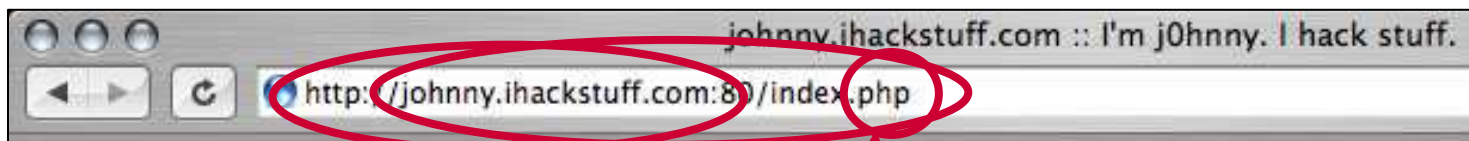
In other cases, mixing should be avoided.

Some operators can only be used to search specific areas of Google, as these columns show.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

## Crash course in advanced operators

Some operators search overlapping areas. Consider site, inurl and filetype.



**SITE:**

Site can not search port.

**INURL:**

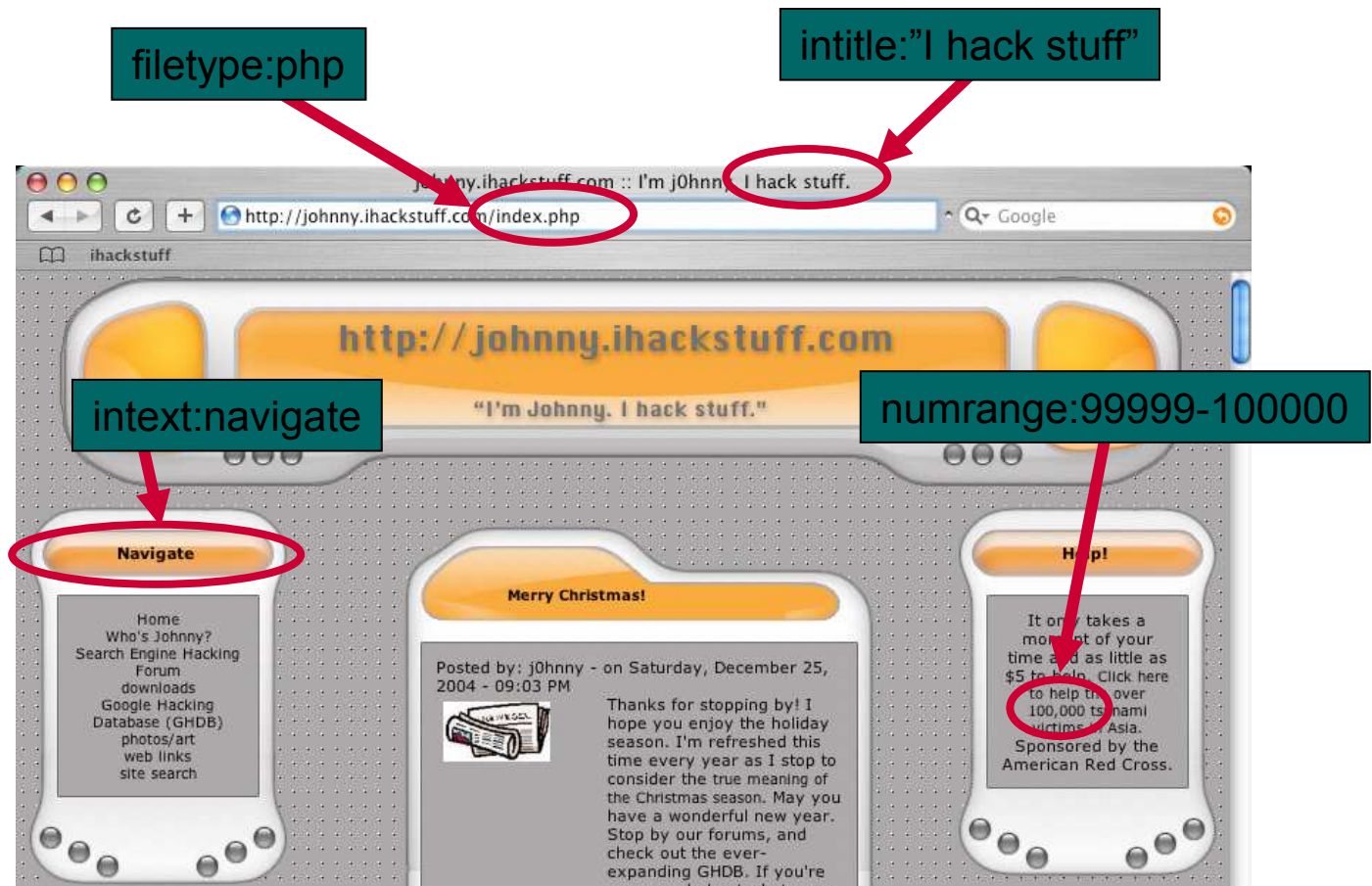
Inurl can search the whole URL, including port and filetype.

**FILETYPE:**

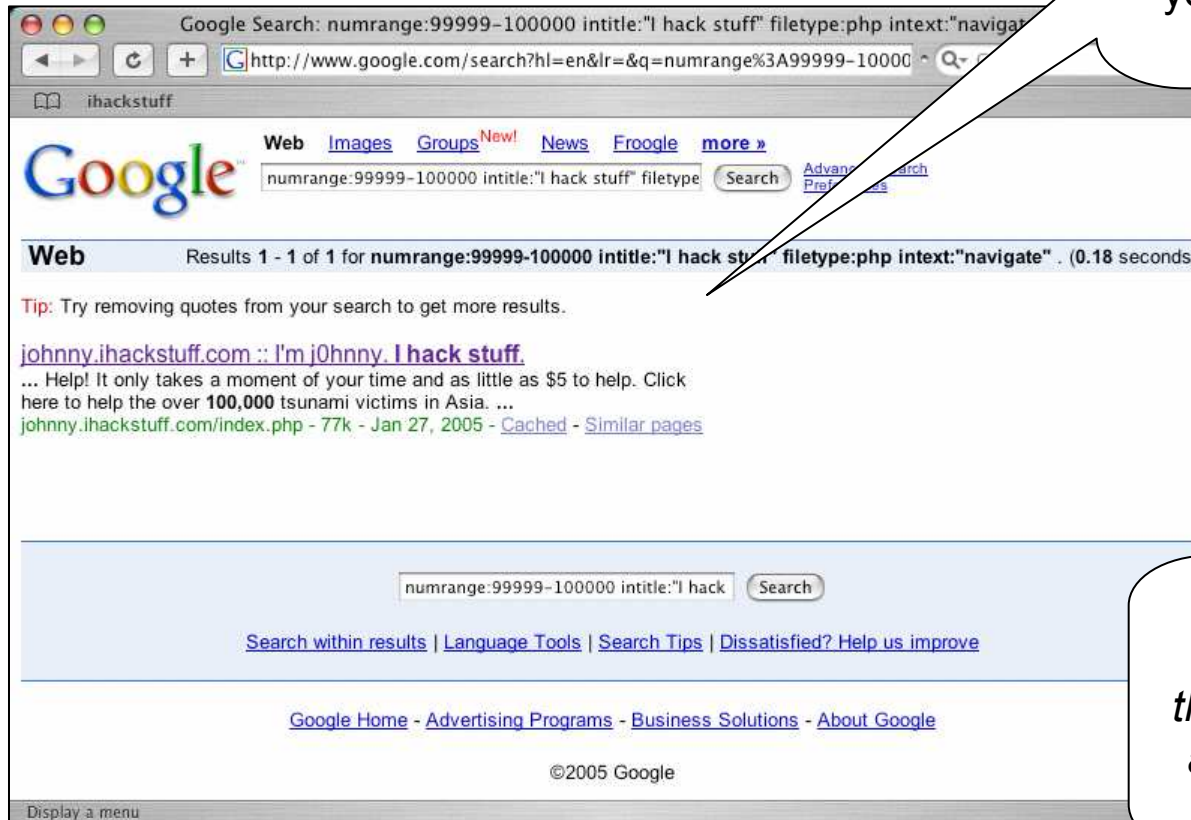
Filetype can only search file extension, which may be hard to distinguish in long URLs.

# Advanced Google Searching

There are many ways to find the same page. These individual queries could all help find the same page.



# Advanced Google Searching



Put those individual queries together into one monster query and you only get that one specific result.

*Adding advanced operators **reduces** the number of results adding **focus** to the search.*



---

## Google Hacking Basics

Putting operators together in intelligent ways can cause a seemingly innocuous query...

INURL:admin

INURL:orders

FILETYPE:php

osCommerce

om/catalog/admin/orders.php+filety

# Google Hacking Basics

...can return  
*devastating* results!

Customer  
names

Order Amounts

Payment  
details!

The screenshot shows a web browser window displaying a Google cache search result for the URL `http://www. ....com/catalog/admin/orders.php`. The search terms `orders` and `admin` are highlighted. Below the search results, there is a table of orders with columns for Customers, Order Total, Date Purchased, Status, and Action. The table contains four rows of order data. On the right side of the page, there are fields for Order ID and Status, and a date stamp `07/01/2004 20:19:33`. At the bottom right, there are fields for Date Created, Last Modified, and Payment Method.

Customers	Order Total	Date Purchased	Status	Action
ter tts	\$56.30	07/01/2004 20:19:33	Delivered	[?]
on E an	\$81.90	06/17/2004 11:22:22	Delivered	[?] [?]
ndre Hewitt	\$69.50	06/16/2004 22:38:20	Pending	[?]
elan kelson	\$45.25	04/23/2004 02:08:24	Delivered	[?] [?]
igu ega	\$159.15	04/16/2004 22:37:00	Delivered	[?] [?]

Order ID:   
Status:   
Date Created: 07/01/2004  
Last Modified: 07/06/2004  
Payment Method: Bank

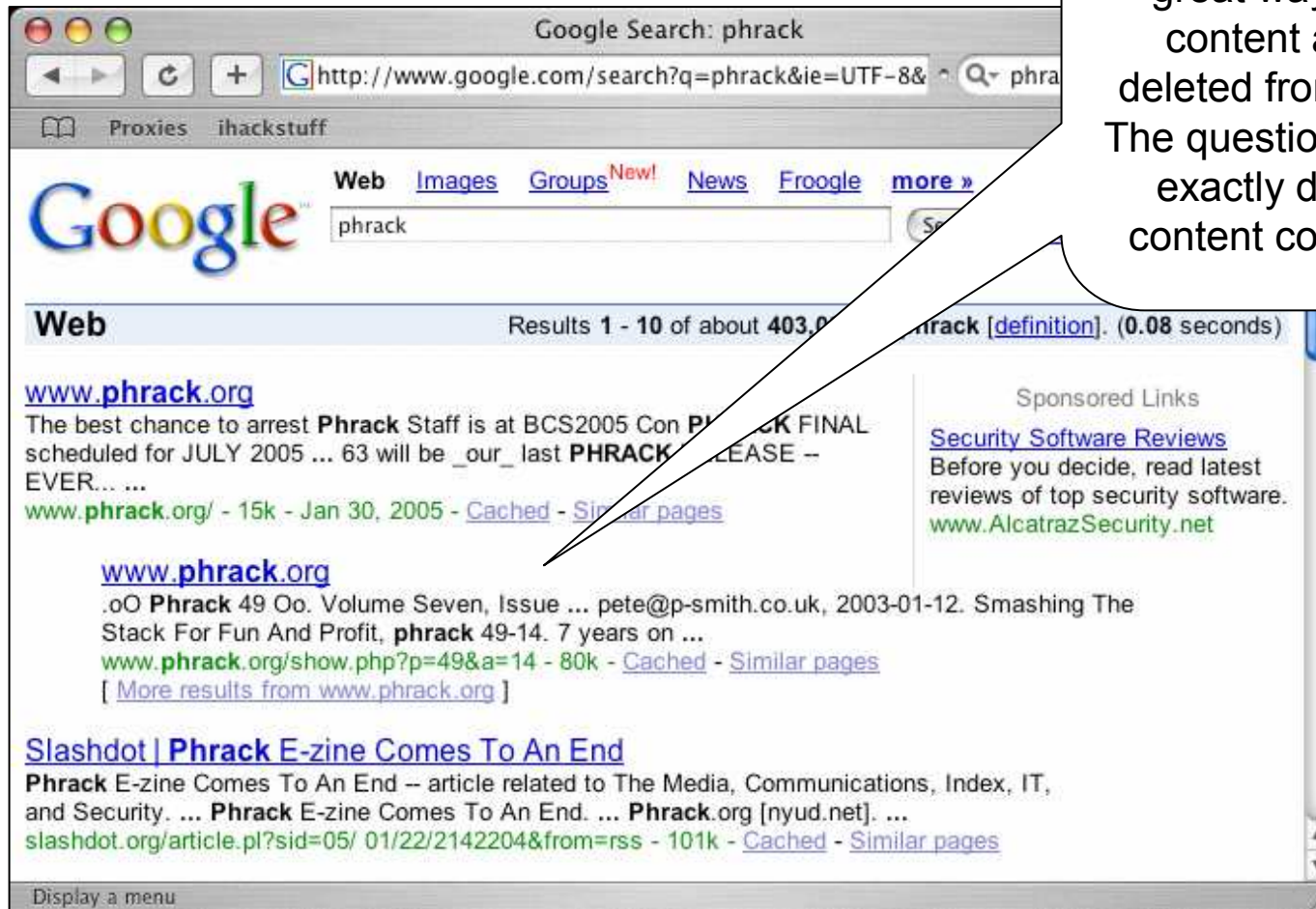
# Google Hacking Basics

Let's take a look at some basic techniques:

Anonymous Googling

Special Characters

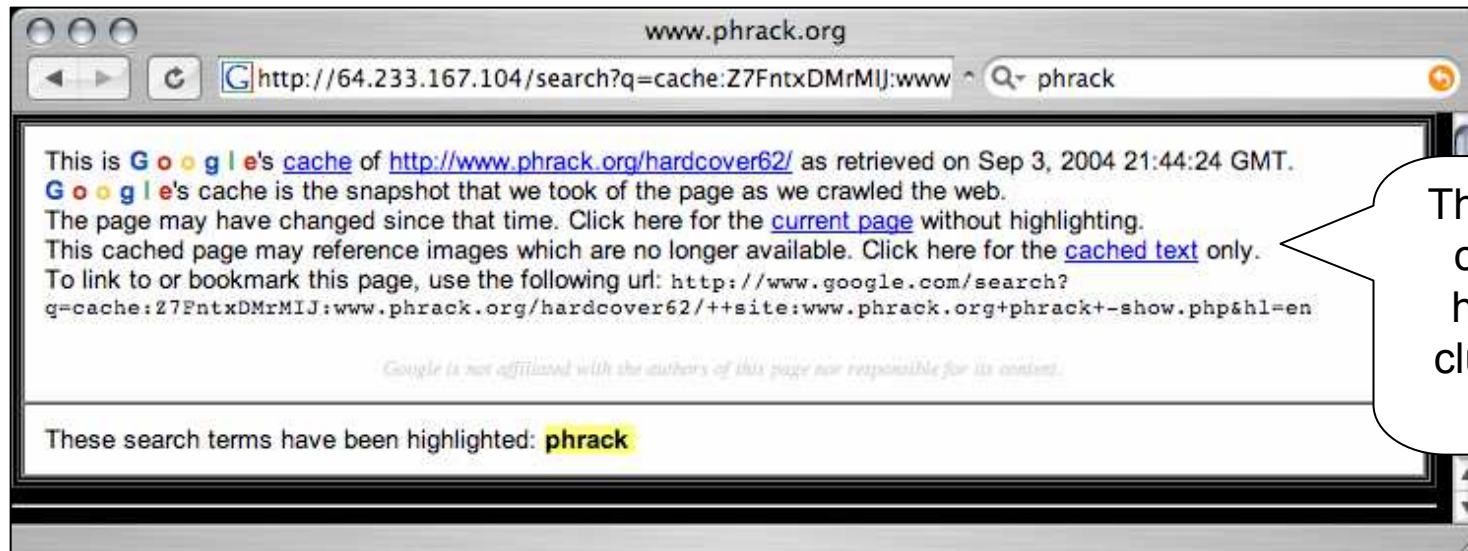
# Anonymous Googling



The cache link is a great way to grab content after it's deleted from the site. The question is, where exactly does that content come from?

## Anonymous Googling

- Some folks use the cache link as an anonymizer, thinking the content comes from Google. Let's take a closer look.



This line from the cached page's header gives a clue as to what's going on...

---

## Anonymous Googling

This tcpdump output shows our network traffic while loading that *cached* page.

```
21:39:24.648422 IP 192.168.2.32.51670 > 64.233.167.104.80
21:39:24.719067 IP 64.233.167.104.80 > 192.168.2.32.51670
21:39:24.720351 IP 64.233.167.104.80 > 192.168.2.32.51670
21:39:24.731503 IP 192.168.2.32.51670 > 64.233.167.104.80
21:39:24.897987 IP 192.168.2.32.51672 > 82.165.25.125.80
21:39:24.902401 IP 192.168.2.32.51671 > 82.165.25.125.80
21:39:24.922716 IP 192.168.2.32.51673 > 82.165.25.125.80
21:39:24.927402 IP 192.168.2.32.51674 > 82.165.25.125.80
21:39:25.017288 IP 82.165.25.125.80 > 192.168.2.32.51672
21:39:25.019111 IP 82.165.25.125.80 > 192.168.2.32.51672
21:39:25.019228 IP 192.168.2.32.51672 > 82.165.25.125.80
21:39:25.023371 IP 82.165.25.125.80 > 192.168.2.32.51671
21:39:25.025388 IP 82.165.25.125.80 > 192.168.2.32.51671
21:39:25.025736 IP 192.168.2.32.51671 > 82.165.25.125.80
21:39:25.043418 IP 82.165.25.125.80 > 192.168.2.32.51673
21:39:25.045573 IP 82.165.25.125.80 > 192.168.2.32.51673
21:39:25.045707 IP 192.168.2.32.51673 > 82.165.25.125.80
21:39:25.052853 IP 82.165.25.125.80 > 192.168.2.32.51674
```

This is Google.

This is Phrack.

We touched Phrack's web server. We're not anonymous.


---

## Anonymous Googling

- Obviously we touched the site, but why?
- Here's more detailed tcpdump output:

```
0x0040 0d6c 4745 5420 2f67 7266 782f 3831 736d
0x0050 626c 7565 2e6a 7067 2048 5454 502f 312e
0x0060 310d 0a48 6f73 743a 2077 7777 2e70 6872
0x0070 6163 6b2e 6f72 670d 0a43 6f6e 6e65 6374
0x0080 696f 6e3a 206b 6565 702d 616c 6976 650d
0x0090 0a52 6566 6572 6572 3a20 6874 7470 3a2f
0x00a0 2f36 342e 3233 332e 3136 312e 3130 342f
0x00b0 7365 6172 6368 3f71 3d63 6163 6865 3a4c
0x00c0 4251 5a49 7253 6b4d 6755 4a3a 7777 772e
0x00d0 7068 7261 636b 2e6f 7267 2f2b 2b73 6974
0x00e0 653a 7777 772e 7068 7261 636b 2e6f 7267
0x00f0 2b70 6872 6163 6b26 686c 3d65 6e0d 0a55
```

...Host: www.phrack.org..Connection: keep-alive.  
.Referer: http://64.233.161.104/search?q=cache:L BQZIrSkMgUJ:www.phrack.org/++site:www.phrack.org+phrack&hl=en..U



An image loaded!

## Anonymous Googling





---

## Anonymous Googling

This time, the entire conversation was between us (192.168.2.32) and Google (64.233.167.104)

23:46:53.996067 IP 192.168.2.32.52912 > 64.233.167.104.80  
23:46:54.025277 IP 64.233.167.104.80 > 192.168.2.32.52912  
23:46:54.025345 IP 192.168.2.32.52912 > 64.233.167.104.80  
23:46:54.025465 IP 192.168.2.32.52912 > 64.233.167.104.80  
23:46:54.094007 IP 64.233.167.104.80 > 192.168.2.32.52912  
23:46:54.124930 IP 64.233.167.104.80 > 192.168.2.32.52912  
23:46:54.127202 IP 64.233.167.104.80 > 192.168.2.32.52912  
23:46:54.128762 IP 64.233.167.104.80 > 192.168.2.32.52912  
23:46:54.128836 IP 192.168.2.32.52912 > 64.233.167.104.80  
23:47:54.130200 IP 192.168.2.32.52912 > 64.233.167.104.80  
23:47:54.154500 IP 64.233.167.104.80 > 192.168.2.32.52912  
23:47:54.154596 IP 192.168.2.32.52912 > 64.233.167.104.80

---

## Anonymous Googling

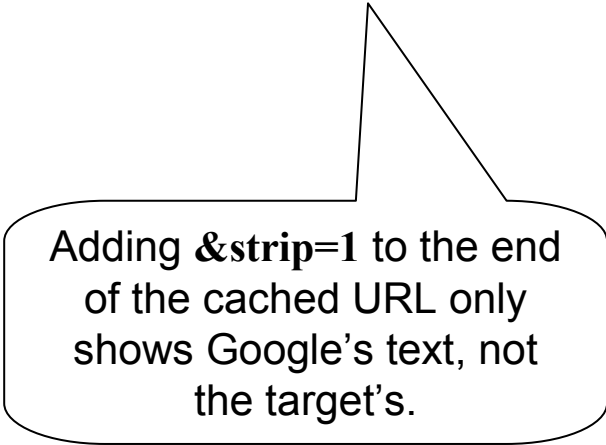
- What made the difference? Let's compare the two URLs:

- Original:

`http://64.233.187.104/search?q=cache:Z7FntxDMrMIJ:www.phrack.org/hardcover62/+phrack+hardcover62&hl=en`

- Cached Text Only:

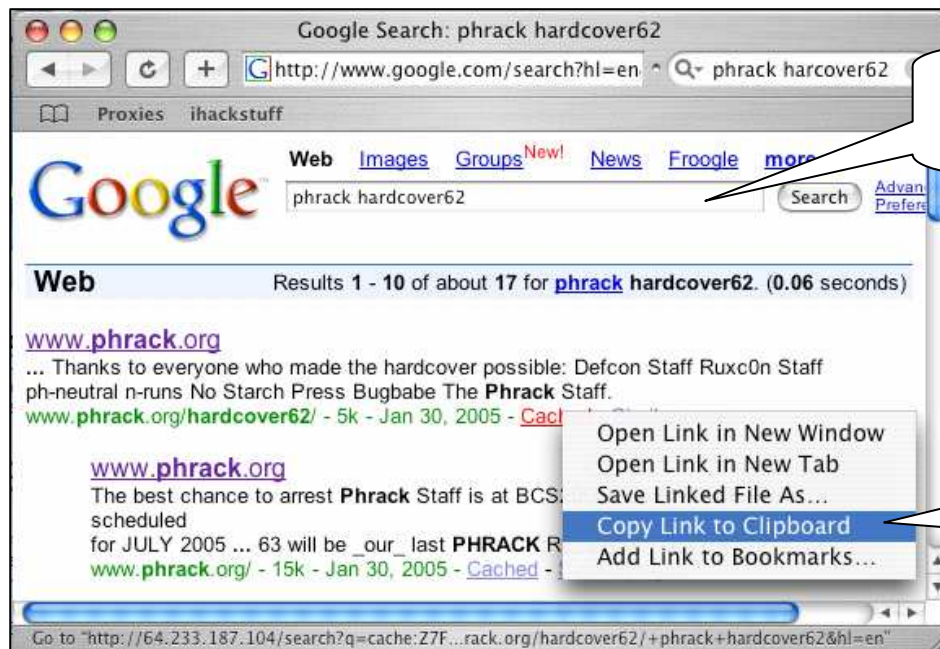
`http://64.233.187.104/search?q=cache:Z7FntxDMrMIJ:www.phrack.org/hardcover62/+phrack+hardcover62&hl=en&lr=&strip=1`



Adding **&strip=1** to the end of the cached URL only shows Google's text, not the target's.

## Anonymous Googling

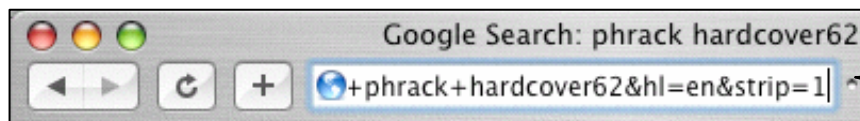
- Anonymous Googling can be helpful, especially if combined with a proxy. Here's a summary.



Perform a Google search.

Right-click the cached link and copy the link to the clipboard.

Paste the URL to the address bar, add `&strip=1`, hit return. You're only touching Google now...



---

## Special Search Characters

- We'll use some special characters in our examples. These characters have special meaning to Google.
- Always use these characters without surrounding spaces!
  - ( + ) force inclusion of something common
  - ( - ) exclude a search term
  - ( " ) use quotes around search phrases
  - ( . ) a single-character wildcard
  - ( \* ) any word
  - ( | ) boolean 'OR'
  - Parenthesis group queries ("master card" | mastercard)

## Google's PHP Blocker: "We're Sorry.."

- Google has started blocking queries, most likely as a result of worms that slam Google with 'evil queries.'



This is a query for  
Inurl:admin.php

---

## Google Hacker's workaround

- Our original query looks like this:

`http://www.google.com/search?q=inurl:admin.php&hl=en&lr=&c2coff=1&start=10&sa=N`

- Stripped down, the query looks like this:

`http://www.google.com/search?q=inurl:admin.php&start=10`

- We can modify our query (`inurl:something.php` is bad) by changing the case of the file extension, like so:

`http://www.google.com/search?q=inurl:admin.PHP&start=10`

`http://www.google.com/search?q=inurl:admin.pHp&start=10`

`http://www.google.com/search?q=inurl:admin.PhP&start=10`

This works in the web interface as well.

# Pre-Assessment

There are many things to consider before testing a target, many of which Google can help with. One shining example is the collection of email addresses and usernames.

## Trolling for Email Addresses

- A seemingly simple search uses the @ sign followed by the primary domain name.



The screenshot shows a web browser window with the address bar displaying "http://www.google.com/search?hl=en&lr=&c2cc...". The search bar contains the query "@gmail.com". The search results are displayed under the heading "Web" and show "Results 1 - 100 of about 2,900,000 for '@gmail.com'. (0.20 seconds)". The first result is "Welcome to Gmail" with a snippet: "Welcome to Gmail, A Google approach to email. Gmail is an experiment in a new kind of webmail, built on the idea that you should ...". The second result is "gmail swap" with a snippet: "... the gates. Why settle for g\_r\_a\_m\_o\_p\_43fp@gmail.com when you could sneak in early and nab gramophone@gmail.com? Everyone's talking ...". A "Sponsored Links" section is also visible, featuring "Gmail - New From Google" with the text "Introducing a Free Webmail Service: 1000 MB of Storage & Google Search" and the URL "gmail.google.com". Two callout boxes are present: one pointing to the search bar with the text "The '@' sign doesn't translate well..." and another at the bottom right with the text "But we can still use the results..."

Google Search: "@gmail.com"

http://www.google.com/search?hl=en&lr=&c2cc... | Q- |

Proxies ihackstuff

Google

Web Images Groups **New!** News Froogle more

"@gmail.com" Search Advanced Search Preferences

**Web** Results 1 - 100 of about 2,900,000 for "@gmail.com". (0.20 seconds)

[Welcome to Gmail](#)  
Welcome to Gmail, A Google approach to email. Gmail is an experiment in a new kind of webmail, built on the idea that you should ...  
gmail.google.com/ - 12k - Jan 30, 2005 - [Cached](#) - [Similar pages](#)

[gmail swap](#)  
... the gates. Why settle for g\_r\_a\_m\_o\_p\_43fp@gmail.com when you could sneak in early and nab gramophone@gmail.com? Everyone's talking ...  
www.gmailswap.com/ - 10k - [Cached](#) - [Similar pages](#)

Sponsored Links

[Gmail - New From Google](#)  
Introducing a Free Webmail Service:  
1000 MB of Storage & Google Search  
gmail.google.com

The "@" sign doesn't translate well...

But we can still use the results...



---

## Automated Trolling for Email Addresses

- We could use a lynx to automate the download of the search results:

```
lynx -dump http://www.google.com/search?q=@gmail.com > test.html
```

- We could then use regular expressions (like this puppy by Don Ranta) to troll through the results:

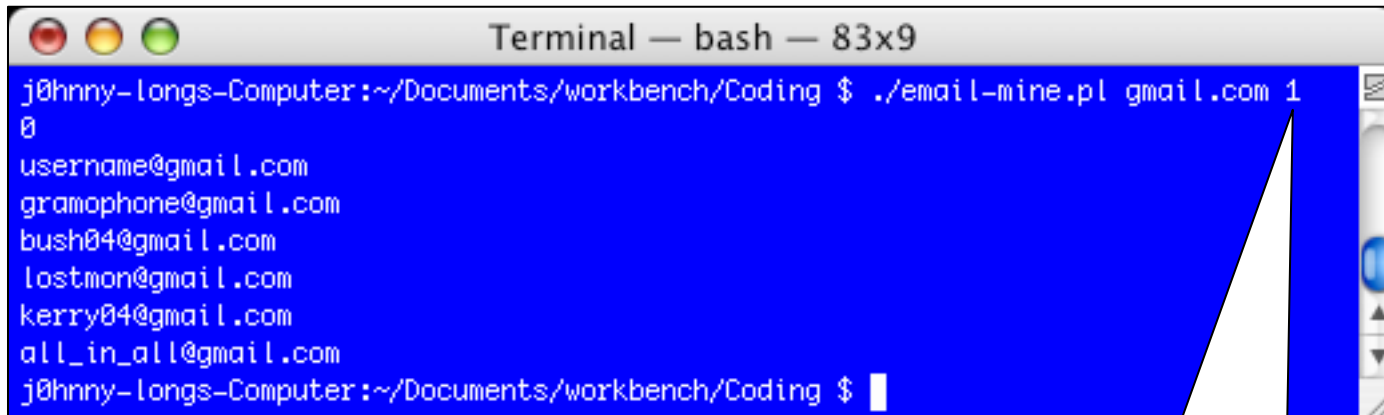
```
[a-zA-Z0-9._-]+@(((a-zA-Z0-9_-){2,99}\.)+[a-zA-Z]{2,4})(((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[1-9])\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[1-9])\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[1-9])\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[1-9]))
```

- Run through grep, this regexp would effectively find email addresses (including addresses containing IP numbers)

---

## More Email Automation

- The 'email miner' PERL script by Roelof Temmingh at sensepost will effectively do the same thing, but via the Google API:

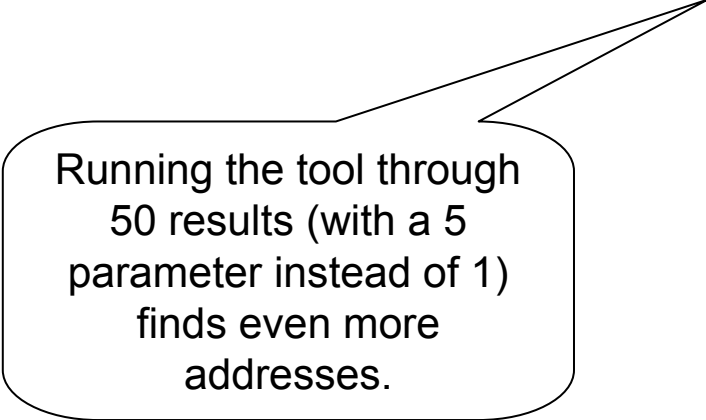
A terminal window titled "Terminal — bash — 83x9" with a blue background. The prompt is "j0hnnny-longs-Computer:~/Documents/workbench/Coding \$". The command entered is "./email-mine.pl gmail.com 1". The output is a list of email addresses: "username@gmail.com", "gramophone@gmail.com", "bush04@gmail.com", "lostmon@gmail.com", "kerry04@gmail.com", and "all\_in\_all@gmail.com". The prompt returns to "j0hnnny-longs-Computer:~/Documents/workbench/Coding \$".

```
Terminal — bash — 83x9
j0hnnny-longs-Computer:~/Documents/workbench/Coding $ ./email-mine.pl gmail.com 1
0
username@gmail.com
gramophone@gmail.com
bush04@gmail.com
lostmon@gmail.com
kerry04@gmail.com
all_in_all@gmail.com
j0hnnny-longs-Computer:~/Documents/workbench/Coding $
```

This searches the first ten Google results... with only one hit against your API key.

---

## More Email Automation



Running the tool through  
50 results (with a 5  
parameter instead of 1)  
finds even more  
addresses.

movabletype@gmail.com  
fakubabe@gmail.com  
lostmon@gmail.com  
label@gmail.com  
charlescapps@gmail.com  
billgates@gmail.com  
ymtang@gmail.com  
tonyedgecombe@gmail.com  
ryawillifor@gmail.com  
jruderman@gmail.com  
itchy@gmail.com  
gramophone@gmail.com  
poojara@gmail.com  
london2012@gmail.com  
bush04@gmail.com  
fengfs@gmail.com  
username@gmail.com  
madrid2012@gmail.com  
somelabel@gmail.com  
bartjcannon@gmail.com  
fillmybox@gmail.com  
silverwolfwsc@gmail.com  
all\_in\_all@gmail.com  
mentzer@gmail.com  
kerry04@gmail.com  
presidentbush@gmail.com  
prabhav78@gmail.com

---

## More email address locations

Query	Description
<i>"Internal Server Error" "server at"</i>	Apache server error could reveal admin e-mail address
<i>intitle:"Execution of this script not permitted"</i>	Cgiwrap script can reveal <i>lots</i> of information, including e-mail addresses and even phone numbers
<i>e-mail address filetype:csv csv</i>	CSV files that could contain e-mail addresses
<i>intitle:index.of dead.letter</i>	dead.letter UNIX file contains the contents of unfinished e-mails that can contain sensitive information
<i>inurl:fcgi-bin/echo</i>	fastcgi echo script can reveal <i>lots</i> of information, including e-mail addresses and server information
<i>filetype:pst pst -from -to -date</i>	Finds Outlook PST files, which can contain e-mails, calendaring, and address information
<i>intitle:index.of inbox</i>	Generic "inbox" search can locate e-mail caches
<i>intitle:"Index Of" -inurl:maillog maillog size</i>	Maillog files can reveal usernames, e-mail addresses, user login/logout times, IP addresses, directories on the server, and more
<i>inurl:email filetype:mdb</i>	Microsoft Access databases that could contain e-mail information
<i>filetype:xls inurl:"email.xls"</i>	Microsoft Excel spreadsheets containing e-mail addresses
<i>filetype:xls username password email</i>	Microsoft Excel spreadsheets containing the words <i>username</i> , <i>password</i> , and <i>email</i>
<i>intitle:index.of inbox dbx</i>	Outlook Express cleanup.log file can contain locations of e-mail information

These queries locate email addresses in more "interesting" locations...

## More email address locations

Query	Description
<i>filetype:eml eml +intext:"Subject" +intext:"From"</i>	Outlook express e-mail files contain e-mails with full headers
<i>intitle:index.of inbox dbx</i>	Outlook Express e-mail folder
<i>filetype:wab wab</i>	Outlook Mail address books contain sensitive e-mail information
<i>filetype:pst inurl:"outlook.pst"</i>	Outlook PST files can contain e-mails, calendaring, and address information
<i>filetype:mbx mbx intext:Subject</i>	Outlook versions 1-4 or Eudora mailbox files contain sensitive e-mail information
<i>inurl:cgi-bin/printenv</i>	Printenv script can reveal lots of information, including e-mail addresses and server information
<i>inurl:forward filetype:forward -cvs</i>	UNIX user e-mail forward files can list e-mail addresses
<i>( filetype:mail   filetype:eml   filetype:mbox   filetype:mbx ) intext:password subject</i>	Various generic e-mail files
<i>"Most Submitted Forms and Scripts" "this section"</i>	WebTrends statistics pages reveal directory information, client access statistics, e-mail addresses, and more
<i>filetype:reg reg +intext:"internet account manager"</i>	Windows registry files can reveal information such as usernames, POP3 passwords, e-mail addresses, and more
<i>"This summary was generated by wwwstat"</i>	Wwwstat statistics information can reveal directory info, client access statistics, e-mail addresses, and more

These queries locate email addresses in more "interesting" locations...

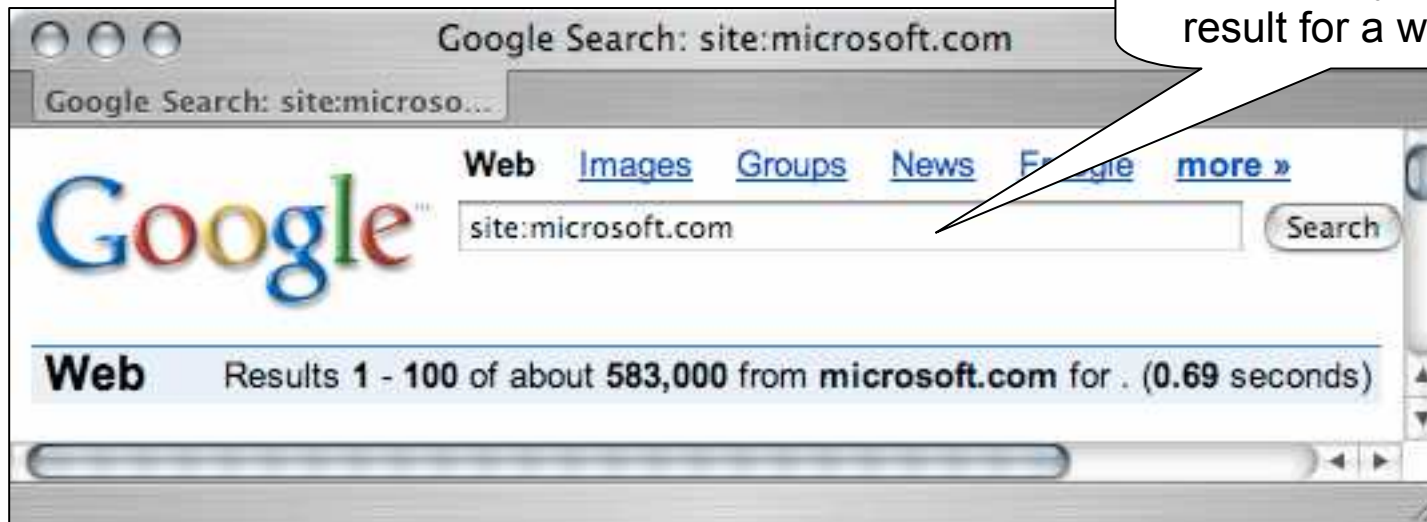
# Network Mapping

Google is an indispensable tool for mapping out an Internet-connected network.

---

## Basic Site Crawling

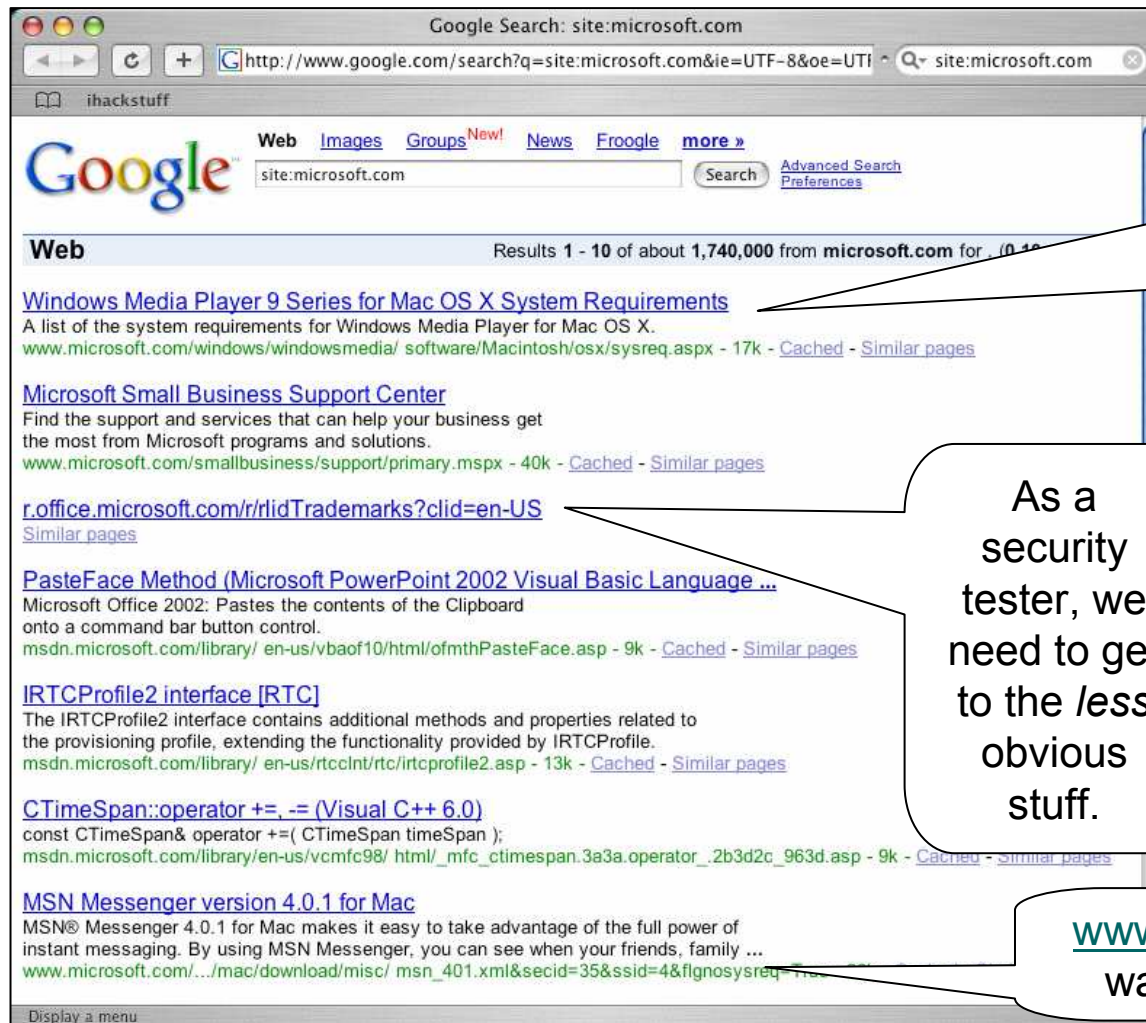
- the site: operator narrows a search to a particular site, domain or subdomain.



One powerful query lists every Google result for a web site!

**site: microsoft.com**

# Basic Site Crawling



Most often, a site search makes the *obvious* stuff float to the top.

As a security tester, we need to get to the *less obvious* stuff.

[www.microsoft.com](http://www.microsoft.com) is way too obvious...

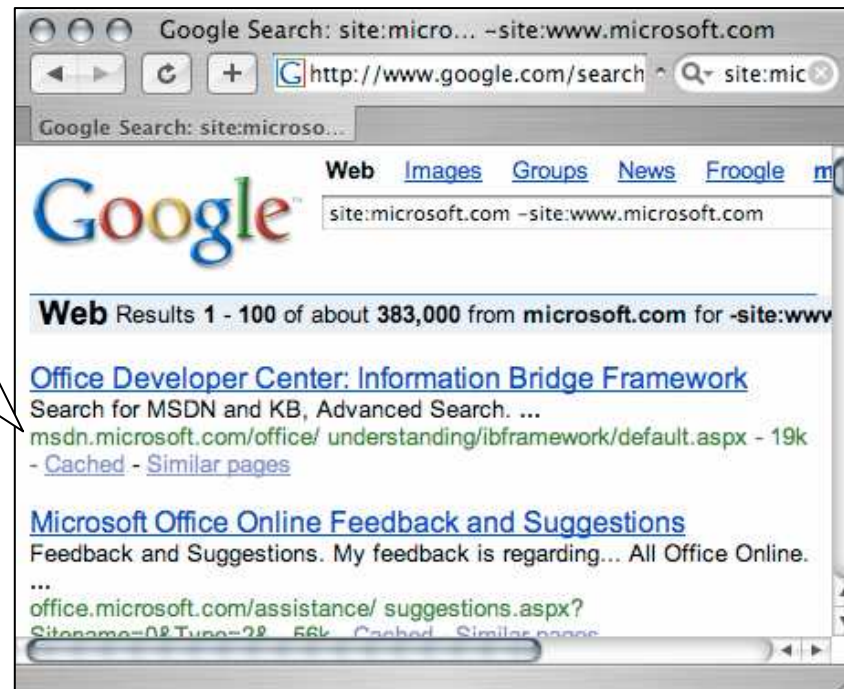


---

## Basic Site Crawling

- To get rid of the more obvious crap, do a negative search.

Notice that the obvious “www” is missing, replaced by more interesting domains.



**site: microsoft.com**  
**-site:www.microsoft.com**

---

## Basic Site Crawling

- Repeating this process of site reduction, tracking what floats to the top leads to nasty big queries like:

site:microsoft.com

-site:www.microsoft.com

-site:msdn.microsoft.com

-site:support.microsoft.com

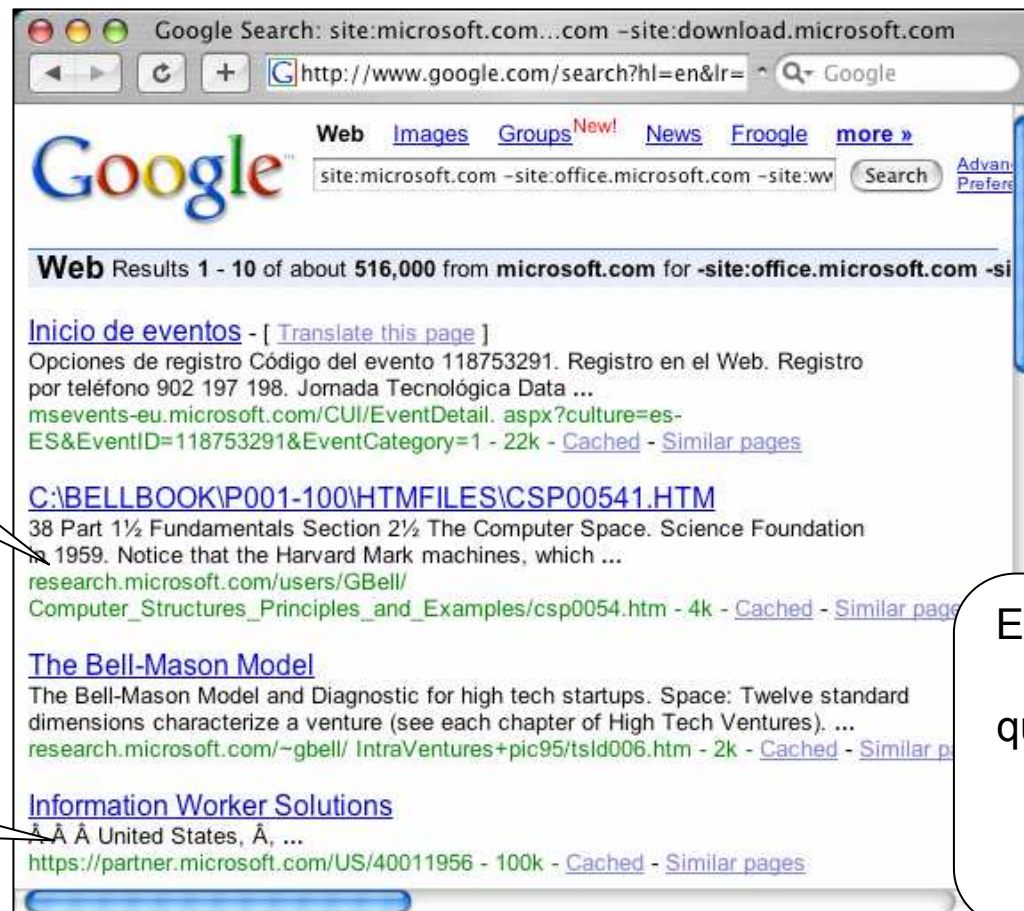
-site:download.microsoft.com

-site:office.microsoft.com

...

## Basic Site Crawling

- The results of such a big query reveal more interesting results...



Research page...

HTTPS page...

Eventually we'll run into a 32 query limit, and this process tends to be tedious.

## Intermediate Site Crawling

Using lynx to capture the Google results page...

..returns the same results.

```
Terminal — ssh — 80x24
-bash-2.05b$ lynx -dump "http://www.google.com/search?q=site:microsoft.com+www.microsoft.com&num=100" > test.html
-bash-2.05b$ sed -n 's/\.[[:alpha:]]*:\V\V[[:alnum:]]*.microsoft.com\//& /p' test.html | awk '{print $2}' | sort -u
http://download.microsoft.com/
http://go.microsoft.com/
http://msdn.microsoft.com/
http://msevents.microsoft.com/
http://murl.microsoft.com/
http://office.microsoft.com/
http://protect.microsoft.com/
http://research.microsoft.com/
https://s.microsoft.com/
http://support.microsoft.com/
-bash-2.05b$
```

..and sed and awk to process the HTML...

---

## So what?

- Well, honestly, host and domain enumeration isn't new, but we're doing this without sending any packets to the target we're analyzing.
- This has several benefits:
  - Low profile. The target can't see your activity.
  - Results are “ranked” by Google. This means that the most public stuff floats to the top. Some more “interesting stuff” trolls near the bottom.
  - “Hints” for follow-up recon. You aren't just getting hosts and domain names, you get application information just by looking at the snippet returned from Google. One results page can be processed for many types of info.. Email addresses, names, etc.. More on this later on...
  - Since we're getting data from several sources, we can focus on non obvious relationships. This is huge!
- Some down sides:
  - In some cases it may be faster and easier as a good guy to use traditional techniques and tools that connect to the target, but remember- the bad guys can still *find and target you* via Google!

---

## Advanced Site Crawling

- Google frowns on automation, unless you use tools written with their API. Know what you're running unless you don't care about their terms of service.
- We could easily modify our lynx retrieval command to pull more results, but in many cases, more results won't equal more unique hosts.
- So, we could also use another technique to locate hosts... plain old fashion common word queries.

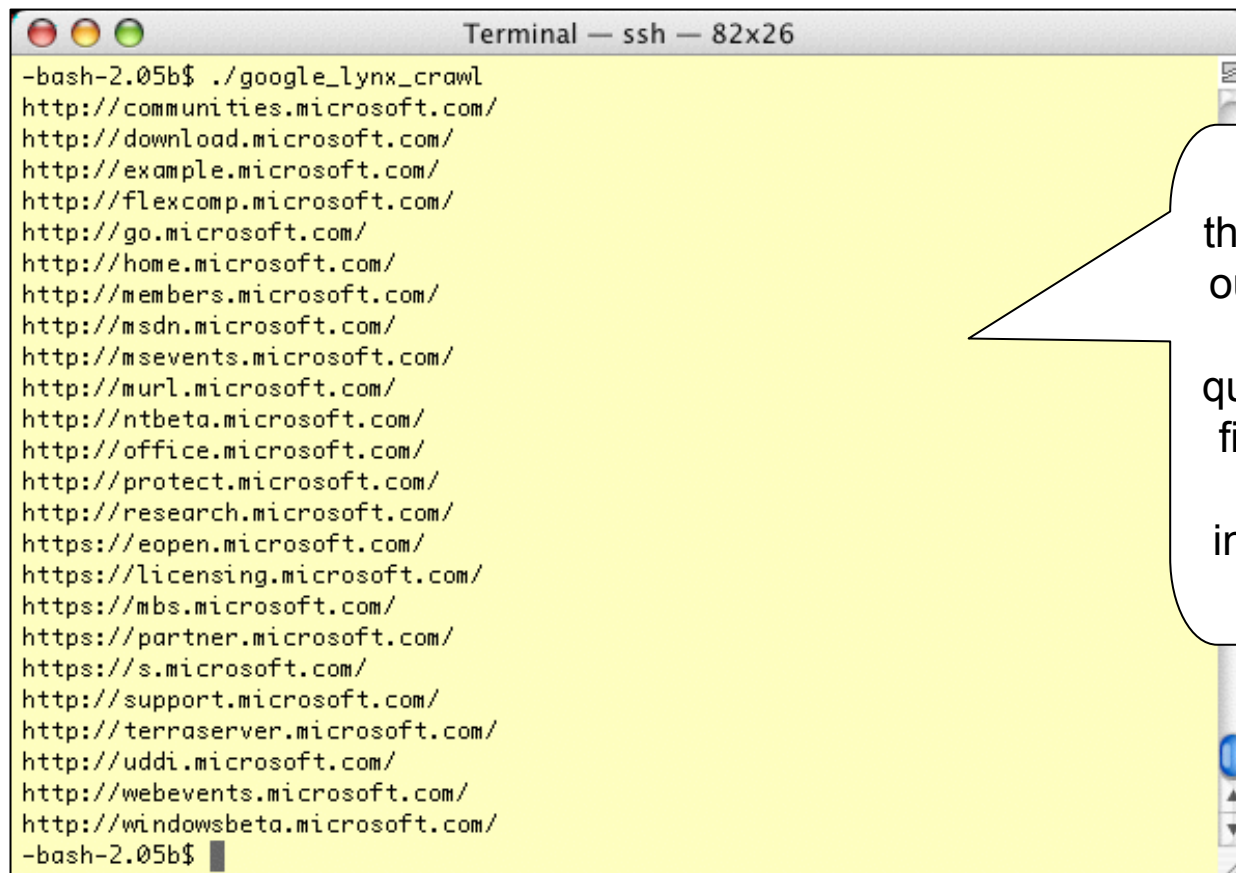
## Advanced Site Crawling

```
Terminal — ssh — 80x13
-bash-2.05b$ lynx -dump "http://www.google.com/search?q=site:microsoft.com+www.microsoft.com&num=100" > test.html
-bash-2.05b$ lynx -dump "http://www.google.com/search?q=site:microsoft.com+www.microsoft.com+web&num=100" >> test.html
-bash-2.05b$ lynx -dump "http://www.google.com/search?q=site:microsoft.com+www.microsoft.com+site&num=100" >> test.html
-bash-2.05b$ lynx -dump "http://www.google.com/search?q=site:microsoft.com+www.microsoft.com+email&num=100" >> test.html
-bash-2.05b$ lynx -dump "http://www.google.com/search?q=site:microsoft.com+www.microsoft.com+about&num=100" >> test.html
-bash-2.05b$
-bash-2.05b$
```

Searching for multiple common words like “web”, “site”, “email”, and “about” along with site... appended to a file...

---

## Advanced Site Crawling

A terminal window titled "Terminal — ssh — 82x26" with a yellow background. The prompt is "-bash-2.05b\$". The command executed is "./google\_lynx\_crawl". The output is a list of 20 URLs from Microsoft, including communities, download, example, flexcomp, go, home, members, msdn, msevents, murl, ntbeta, office, protect, research, eopen, licensing, mbs, partner, s, support, terraserver, uddi, webevents, and windowsbeta. The prompt "-bash-2.05b\$" is visible at the bottom.

```
-bash-2.05b$ ./google_lynx_crawl
http://communities.microsoft.com/
http://download.microsoft.com/
http://example.microsoft.com/
http://flexcomp.microsoft.com/
http://go.microsoft.com/
http://home.microsoft.com/
http://members.microsoft.com/
http://msdn.microsoft.com/
http://msevents.microsoft.com/
http://murl.microsoft.com/
http://ntbeta.microsoft.com/
http://office.microsoft.com/
http://protect.microsoft.com/
http://research.microsoft.com/
https://eopen.microsoft.com/
https://licensing.microsoft.com/
https://mbs.microsoft.com/
https://partner.microsoft.com/
https://s.microsoft.com/
http://support.microsoft.com/
http://teraserver.microsoft.com/
http://uddi.microsoft.com/
http://webevents.microsoft.com/
http://windowsbeta.microsoft.com/
-bash-2.05b$
```

Sifting through the output from those queries, we find many more interesting hits.



## Advanced Site Crawling

```
Terminal — bash — 88x30
-----
DNS names:
-----
v5.windowsupdate.microsoft.com
dgl.microsoft.com
www.beta.microsoft.com
g.microsoft.com
msevents.microsoft.com
www.microsoft.com
windowsbeta.microsoft.com
office.microsoft.com
netscan.research.microsoft.com
go.microsoft.com
webevents.microsoft.com
msdn.microsoft.com
partnering.one.microsoft.com
beta.microsoft.com
officebeta.microsoft.com
activex.microsoft.com
oca.microsoft.com
eopen.microsoft.com
lab.msdn.microsoft.com
download.microsoft.com
teraserver.microsoft.com
murl.microsoft.com
ntbeta.microsoft.com
v4.windowsupdate.microsoft.com
home.microsoft.com
support.microsoft.com
research.microsoft.com
```

Roelof Temmingh from sensepost.com coded this technique into a PERL (API-based) script called dns-mine.pl to achieve much more efficient results.

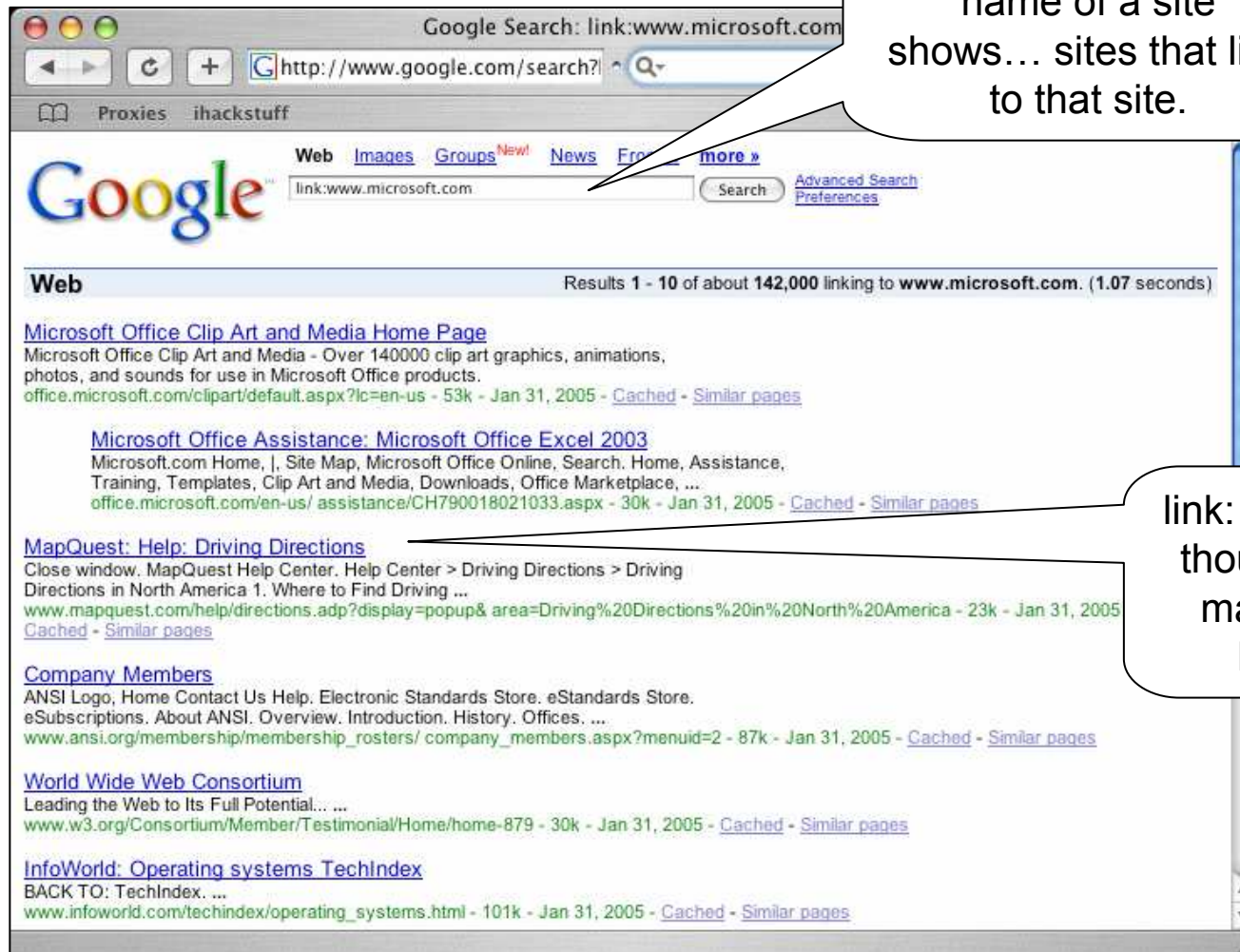
We'll look more at coding later...

---

## Too much noise, not enough signal...

- Getting lists of hosts and (sub)domains is great. It gives you more targets, but there's another angle.
- Most systems are only as secure as their weakest link.
- If a poorly-secured company has a trust relationship with your target, that's your way in.
  
- Question: How can we determine site relationships with Google?
  
- One Answer: the "link" operator.


# Raw Link Usage



link: combined with the name of a site shows... sites that link to that site.

link: has limits though. See mapquest here?

## Link has limits



The screenshot shows a web browser window with the Google search interface. The search bar contains the query "link:www.microsoft.com site:mapquest.com". The search results section displays the message: "Your search - link:www.microsoft.com site:mapquest.com - did not match any documents." Below this, there are suggestions for improving the search, such as checking spelling and using different keywords. A speech bubble points to the search bar with the text: "...combining link: with site: doesn't seem to work...".

Google Search: link:www.microsoft.com site:mapquest.com

http://www.google.com/ Google

Proxies ihackstuff

Web Images Groups <sup>New!</sup> News Froogle more »

Google link:www.microsoft.com site:mapquest.com Search Advanced Search Preferences

**Web**

Tip: Try [Google Answers](#) for help from expert researchers

Your search - **link:www.microsoft.com site:mapquest.com** - did not match any documents.

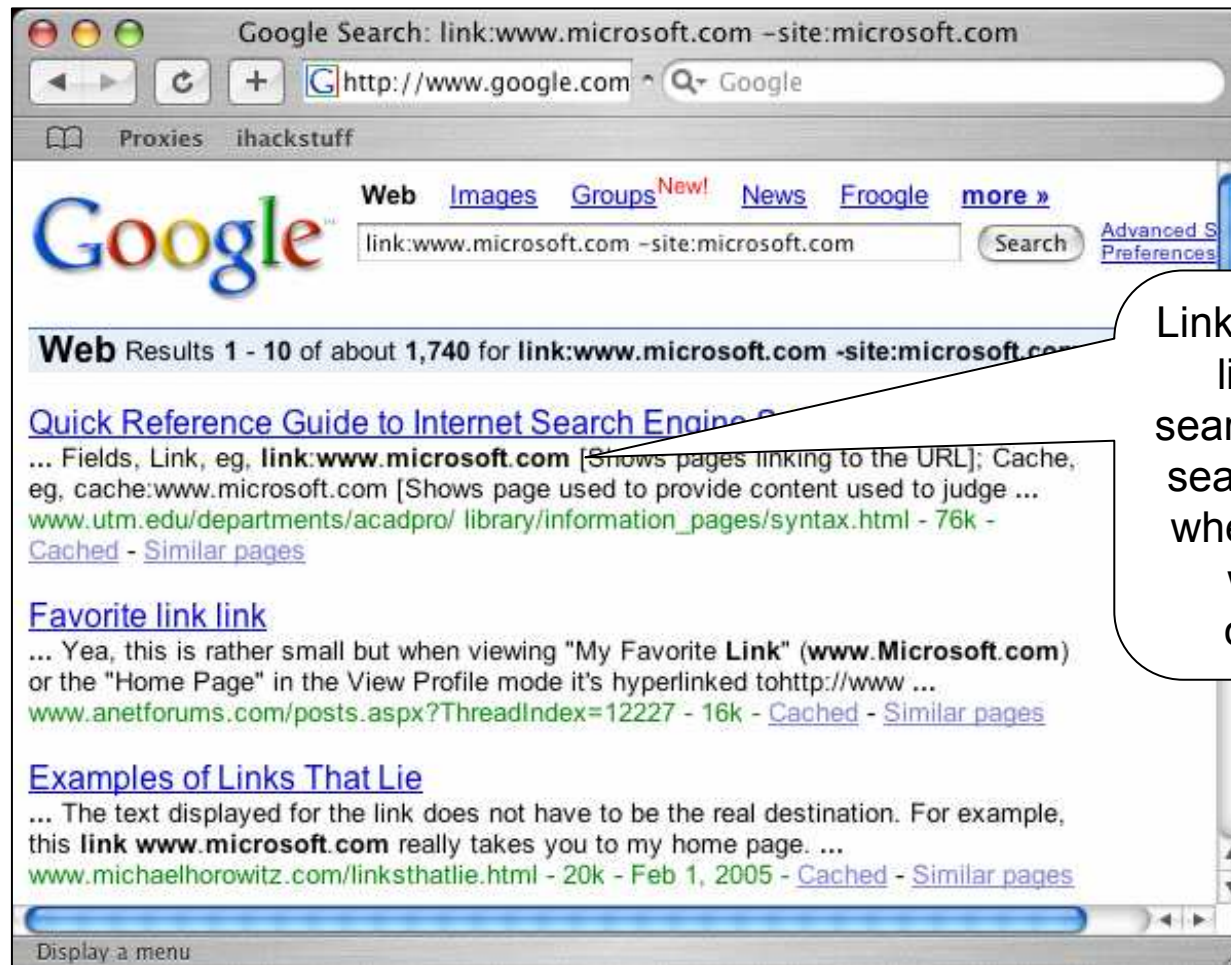
Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Also, you can try [Google Answers](#) for expert help with your search.

Display a menu

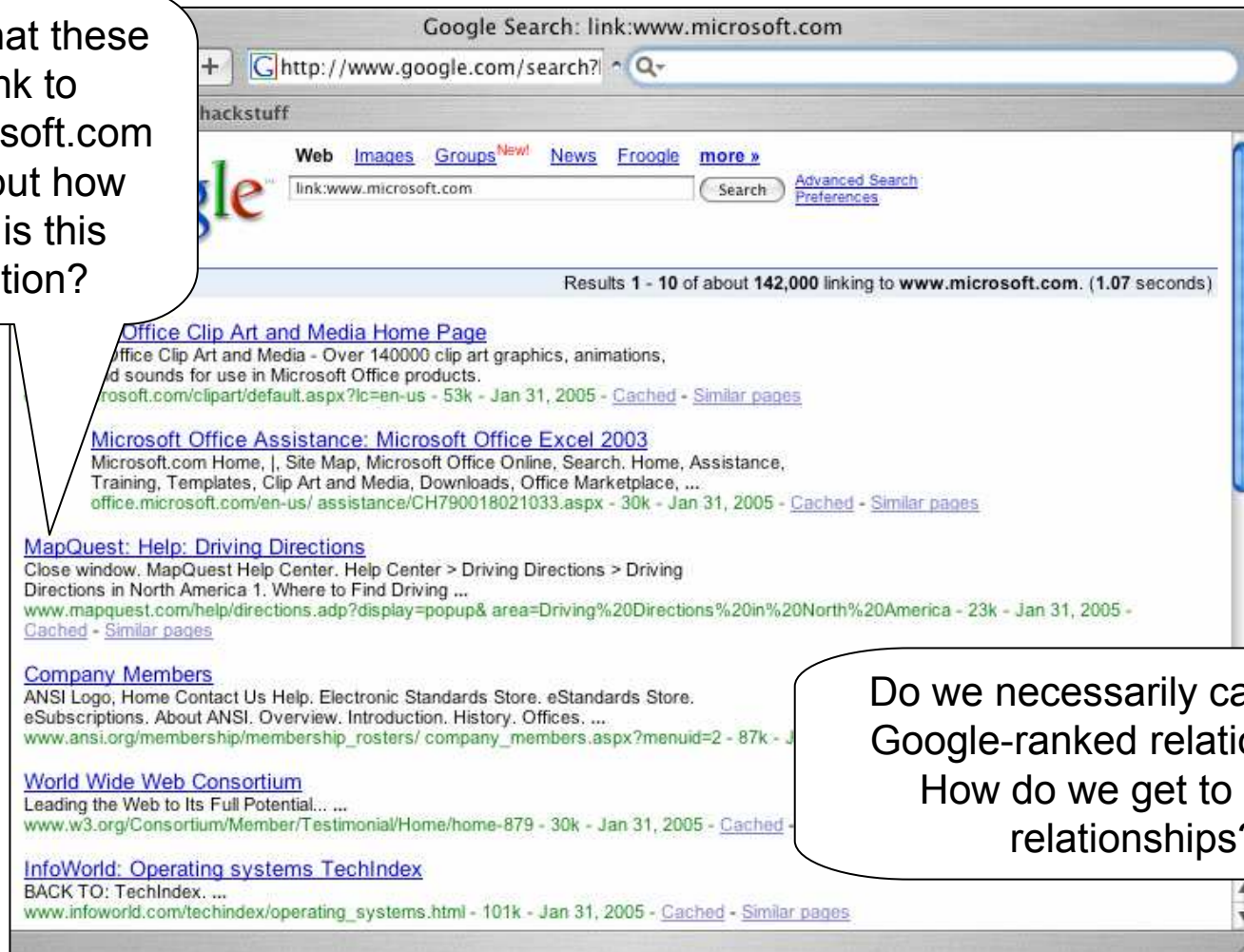
## Link has limits



Link: gets treated like normal search text (not a search modifier) when combined with other operators.

## Link has other limits

Knowing that these sites link to [www.microsoft.com](http://www.microsoft.com) is great, but how relevant is this information?



The screenshot shows a Google search interface with the following elements:

- Search bar: <http://www.google.com/search?>
- Search results: "Results 1 - 10 of about 142,000 linking to [www.microsoft.com](http://www.microsoft.com). (1.07 seconds)"
- Search filters: Web, Images, Groups, News, Froogle, more »
- Search input: [link:www.microsoft.com](http://www.microsoft.com)
- Search buttons: Search, Advanced Search, Preferences
- Search results list:
  - Office Clip Art and Media Home Page**  
Office Clip Art and Media - Over 140000 clip art graphics, animations, and sounds for use in Microsoft Office products.  
[www.microsoft.com/clipart/default.aspx?lc=en-us](http://www.microsoft.com/clipart/default.aspx?lc=en-us) - 53k - Jan 31, 2005 - [Cached](#) - [Similar pages](#)
  - Microsoft Office Assistance: Microsoft Office Excel 2003**  
Microsoft.com Home, |, Site Map, Microsoft Office Online, Search, Home, Assistance, Training, Templates, Clip Art and Media, Downloads, Office Marketplace, ...  
[office.microsoft.com/en-us/assistance/CH790018021033.aspx](http://office.microsoft.com/en-us/assistance/CH790018021033.aspx) - 30k - Jan 31, 2005 - [Cached](#) - [Similar pages](#)
  - MapQuest: Help: Driving Directions**  
Close window. MapQuest Help Center. Help Center > Driving Directions > Driving Directions in North America 1. Where to Find Driving ...  
[www.mapquest.com/help/directions.adp?display=popup&area=Driving%20Directions%20in%20North%20America](http://www.mapquest.com/help/directions.adp?display=popup&area=Driving%20Directions%20in%20North%20America) - 23k - Jan 31, 2005 - [Cached](#) - [Similar pages](#)
  - Company Members**  
ANSI Logo, Home Contact Us Help. Electronic Standards Store. eStandards Store. eSubscriptions. About ANSI. Overview. Introduction. History. Offices. ...  
[www.ansi.org/membership/membership\\_rosters/company\\_members.aspx?menuid=2](http://www.ansi.org/membership/membership_rosters/company_members.aspx?menuid=2) - 87k - Jan 31, 2005 - [Cached](#) - [Similar pages](#)
  - World Wide Web Consortium**  
Leading the Web to Its Full Potential... ...  
[www.w3.org/Consortium/Member/Testimonial/Home/home-879](http://www.w3.org/Consortium/Member/Testimonial/Home/home-879) - 30k - Jan 31, 2005 - [Cached](#) - [Similar pages](#)
  - InfoWorld: Operating systems TechIndex**  
BACK TO: TechIndex. ...  
[www.infoworld.com/techindex/operating\\_systems.html](http://www.infoworld.com/techindex/operating_systems.html) - 101k - Jan 31, 2005 - [Cached](#) - [Similar pages](#)

Do we necessarily care about Google-ranked relationships? How do we get to REAL relationships?

---

## Non-obvious site relationships

- Sensepost to the rescue again! =)
- BiLE (the Bi-directional Link Extractor), available from [http://www.sensepost.com/garage\\_portal.html](http://www.sensepost.com/garage_portal.html) helps us gather together links from Google and piece together these relationships.
- There's much more detail on this process in their whitepaper, but let's cover the basics...

---

## Non-obvious site relationships

- A link from a site weighs more than a link to a site
  - Anyone can link to a site if they own web space (which is free to all)
- A link from a site with a lot of links weighs less than a link from a site with a small amount of links
  - This means specifically outbound links.
  - If a site has few outbound links, it is probably lighter.
  - There are obvious exceptions like link farms.

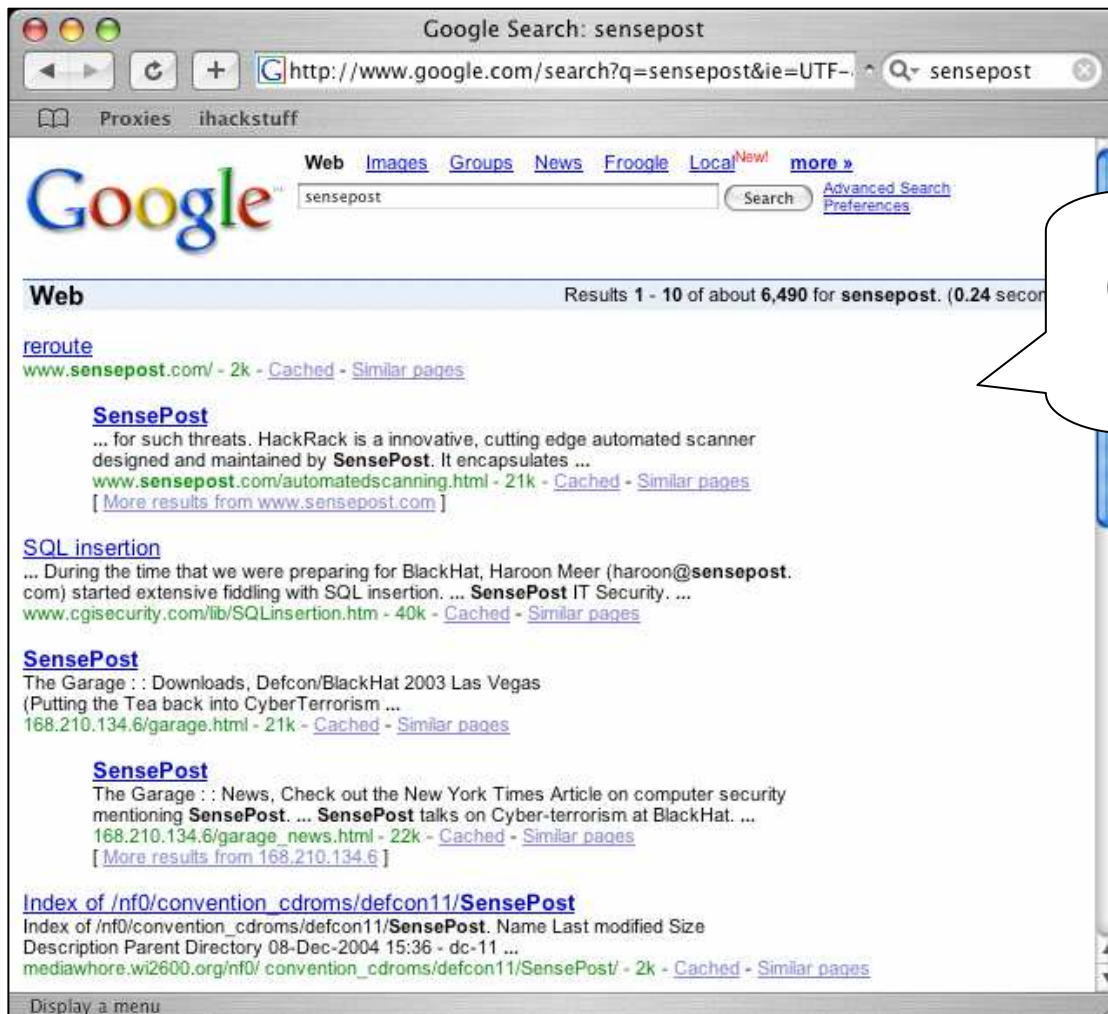


---

## Non-obvious site relationships

- A link to a site with a lot of links to the site weighs less than a link to a site with a small amount of links to the site.
  - If external sources link to a site, it must be important (or more specifically popular)
  - This is basically how Google weighs a site.
- The site that was given as input parameter need not end up with the highest weight – a good indication that the provided site is not the central site of the organization.”
  - If after much research, the site you are investigating doesn't weight the most, you've probably missed the target's main site.

# Who is Sensepost?



Relying on Google's 6400+ results can be daunting... and misleading.

## Non-obvious site relationships

- It seems dizzying to pull all this together, but BiLE does wonders. Let's point it at sensepost.com:

```
root@localhost
root@attack:~/workbench/google# ./bile-public-ext.pl www.sensepost.com out

##Link to www.sensepost.com
burger.za.org:www.sensepost.com
lists.jammed.com:www.sensepost.com
search.linuxsecurity.com:www.sensepost.com
www.blackhat.com:www.sensepost.com
www.antiserver.it:www.sensepost.com
list.cineca.it:www.sensepost.com
www.mail-archive.com:www.sensepost.com
packetstormsecurity.org:www.sensepost.com
packetstormsecurity.nl:www.sensepost.com
archives.neohapsis.com:www.sensepost.com
www.derkeiler.com:www.sensepost.com
packetstorm.trustica.cz:www.sensepost.com
www.supernature-forum.de:www.sensepost.com
www.defcon.org:www.sensepost.com
biatchux.dmzs.com:www.sensepost.com
cert.uni-stuttgart.de:www.sensepost.com
www.baboo.com.br:www.sensepost.com
listserv.ntsecurity.net:www.sensepost.com
opensores.thebunker.net:www.sensepost.com
seclists.org:www.sensepost.com
www.packetstormsecurity.org:www.sensepost.com
```

This is the extraction phase. BiLE is looking for links to [www.sensepost.com](http://www.sensepost.com) (via Google) and writing the results to a file called "out"...

## Non-obvious site relationships

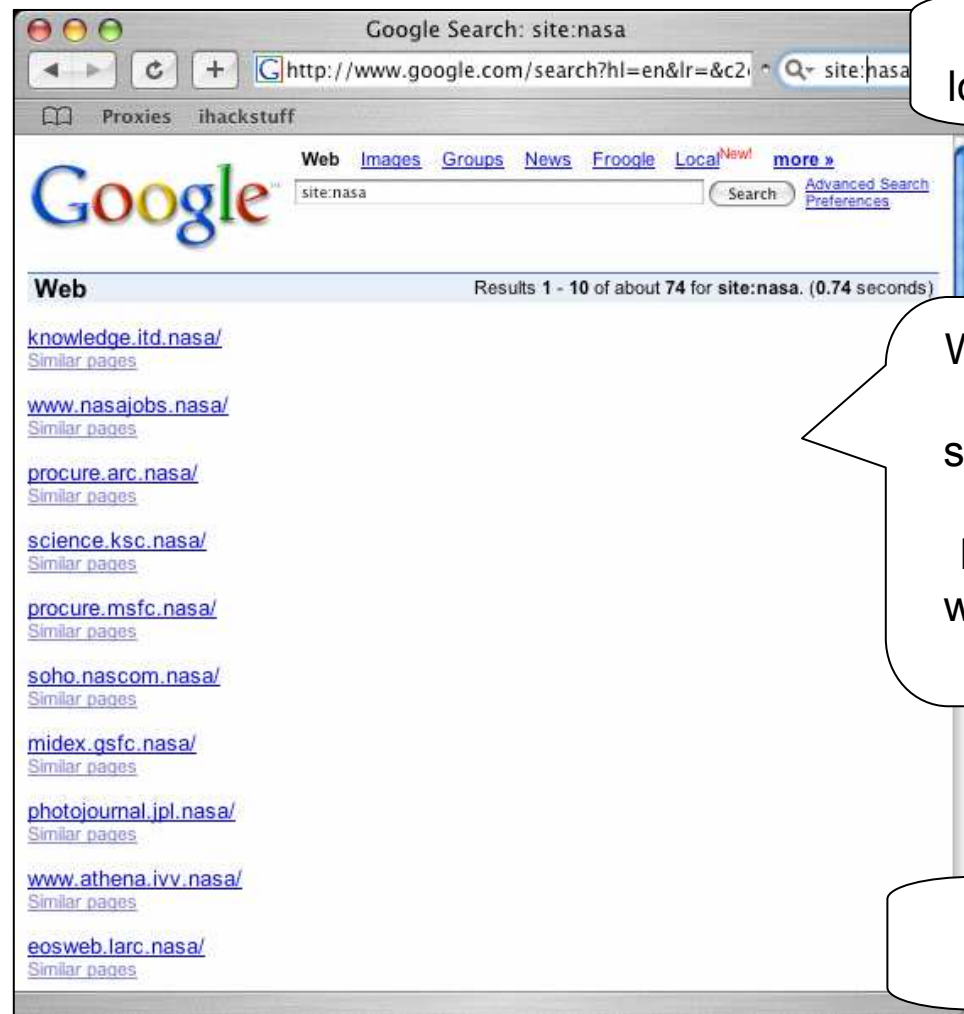
- This is the weigh phase. BiLE takes the output from the extraction phase...

```
root@localhost:~/file/final — ssh — 3
root@attack:~/workbench/google# ./bile-public-weigh.pl www.sensepost.com out new
root@attack:~/workbench/google# more new
www.sensepost.com:144.600
www.blackhat.com:18.000
biatchux.dmzs.com:18.000
packetstormsecurity.org:11.400
packetstormsecurity.nl:11.400
securitylab.ru:10.800
www.packetstormsecurity.org:9.346
dewil.ru:7.817
lists.virus.org:7.726
search.linuxsecurity.com:7.344
lists.jammed.com:7.344
list.cineca.it:7.344
www.securityfocus.com:7.298
www.mail-archive.com:7.298
archives.neohapsis.com:7.298
www.supernature-forum.de:7.200
www.derkeiler.com:7.200
www.defcon.org:7.200
www.baboo.com.br:7.200
www.antiserver.it:7.200
seclists.org:7.200
packetstorm.trustica.cz:7.200
--More--(9%)
```

And weighs the results using the four main criteria of weighing discussed above... aided primarily by Google searches.

This shows the strongest relationships to our target site first, which during an assessment equate to secondary targets, especially for information gathering.

## The next step...



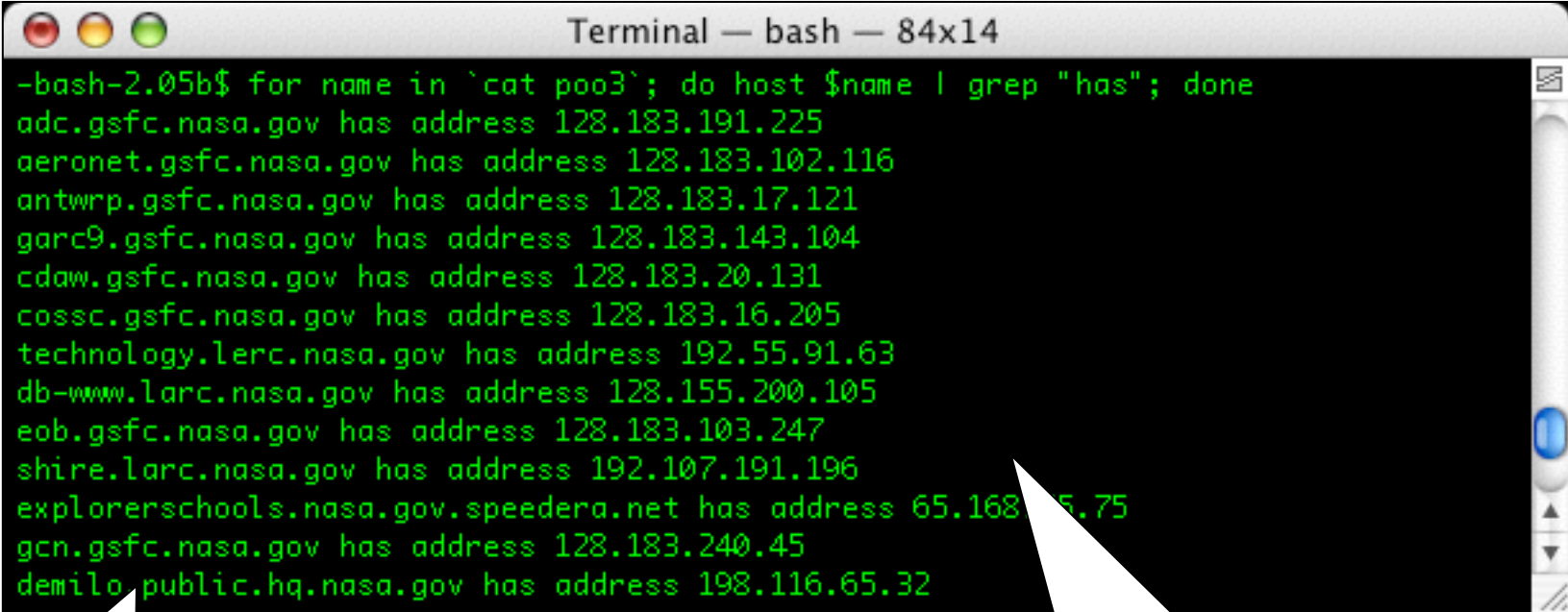
Let's say we're looking at NASA....

We could use 'googleturd' searches, like site:nasa to locate typos which may be real sites...

How can we verify these???

## Host verification...

- Cleaning the names and running DNS lookups is one way...



```
Terminal — bash — 84x14
-bash-2.05b$ for name in `cat poo3`; do host $name | grep "has"; done
adc.gsfc.nasa.gov has address 128.183.191.225
aeronet.gsfc.nasa.gov has address 128.183.102.116
antwrp.gsfc.nasa.gov has address 128.183.17.121
garc9.gsfc.nasa.gov has address 128.183.143.104
cdaw.gsfc.nasa.gov has address 128.183.20.131
cosscc.gsfc.nasa.gov has address 128.183.16.205
technology.lerc.nasa.gov has address 192.55.91.63
db-www.larc.nasa.gov has address 128.155.200.105
eob.gsfc.nasa.gov has address 128.183.103.247
shire.larc.nasa.gov has address 192.107.191.196
explorerschools.nasa.gov.speedera.net has address 65.168.15.75
gcn.gsfc.nasa.gov has address 128.183.240.45
demilo-public.hq.nasa.gov has address 198.116.65.32
```

Pay dirt! Now what???

We could further expand on these IP ranges via DNS queries as well...

---

## Expanding out...

- Once armed with a list of sites and domains, we could expand out the list in several ways. DNS queries are helpful, but what else can we do to get more names to try?
- From whatever source, let's say we get two names from verizon, 'foundation' and investor'...

[\[PDF\] Verizon's 2003 Annual Report - Investor Information](#)

File Format: PDF/Adobe Acrobat

Page 1. Registered Shareowner Services Questions or requests for assistance regarding changes to or transfers of your registered ...

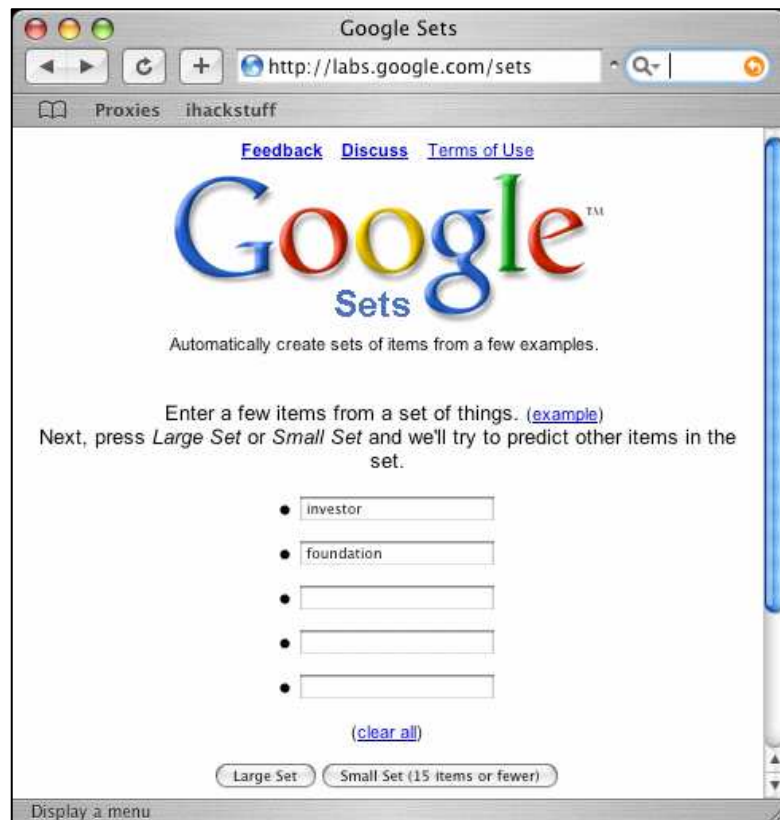
[investor.verizon.com/2003annual/download/vz\\_investor\\_info.pdf](http://investor.verizon.com/2003annual/download/vz_investor_info.pdf) - [Similar pages](#)

[foundation.verizon.com/cybergrants/plsql/incomm.info?x\\_type\\_flag=DELETE](http://foundation.verizon.com/cybergrants/plsql/incomm.info?x_type_flag=DELETE)

[Similar pages](#)

# Google Sets

- Although this is a simple example, we can throw these two words into Google Sets....

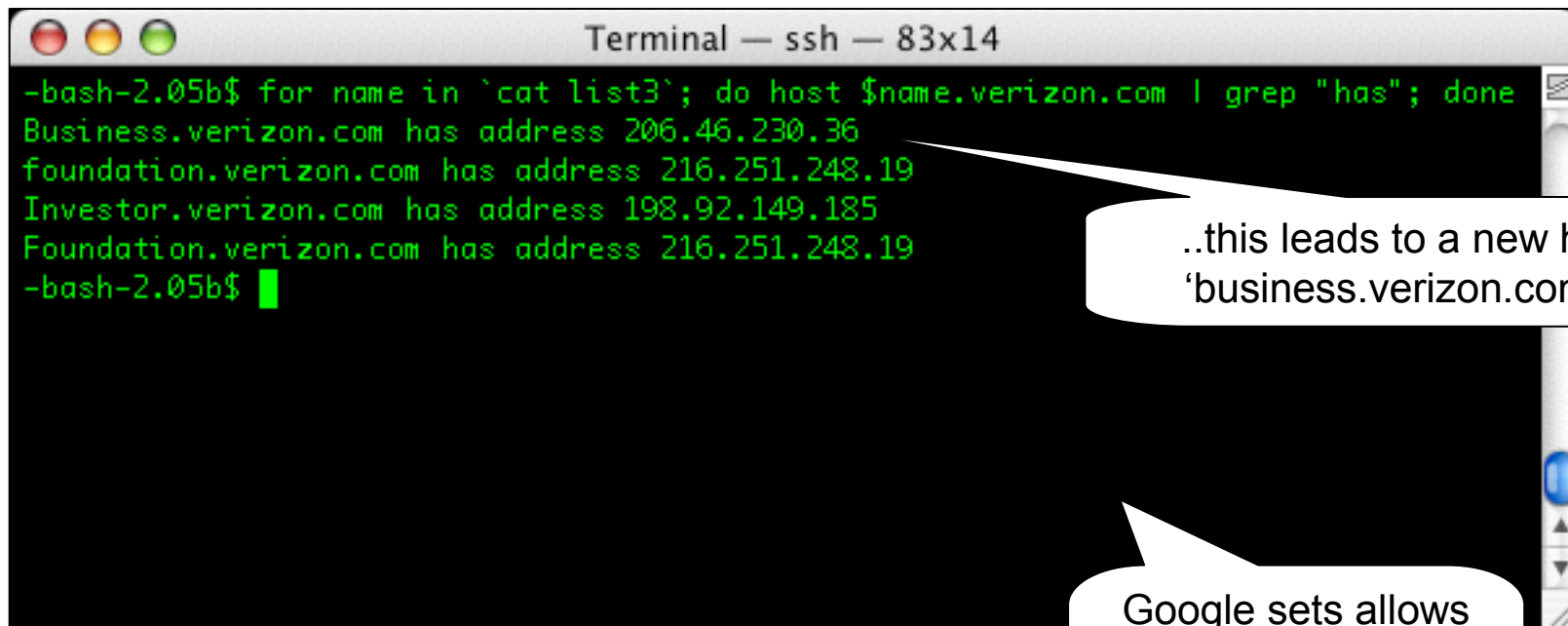


Predicted Items
<a href="#">Investor</a>
<a href="#">foundation</a>
<a href="#">Second Foundation</a>
<a href="#">Intermediate</a>
<a href="#">Entrepreneur</a>
<a href="#">Self Employed</a>
<a href="#">Advanced</a>
<a href="#">Roof</a>
<a href="#">framing</a>
<a href="#">Alliances</a>
<a href="#">Careers</a>
<a href="#">Community</a>
<a href="#">columns</a>
<a href="#">Completion</a>
<a href="#">Lender</a>
<a href="#">Excavation</a>
<a href="#">BOARD MEMBERS</a>
<a href="#">walls</a>
<a href="#">Application</a>
<a href="#">Earnings Reports</a>
<a href="#">IPOs</a>
<a href="#">Financial</a>
<a href="#">Certificate</a>
<a href="#">professional</a>
<a href="#">Blusher</a>
<a href="#">Research</a>
<a href="#">groundwork</a>
<a href="#">fundament</a>
<a href="#">roof structure</a>
<a href="#">Business Directory</a>
<a href="#">floors</a>
<a href="#">P.F</a>
<a href="#">Contact Us</a>
<a href="#">Metal Roof</a>
<a href="#">FOGA FOPA</a>
<a href="#">Owner Occupied</a>
<a href="#">STEM Methodology</a>
<a href="#">TEACHERS</a>
<a href="#">DISTRIBUTION</a>



## Expanding

- Then, we can take all these words and perform DNS host lookups against each of these combinations:



```
Terminal — ssh — 83x14
-bash-2.05b$ for name in `cat list3`; do host $name.verizon.com | grep "has"; done
Business.verizon.com has address 206.46.230.36
foundation.verizon.com has address 216.251.248.19
Investor.verizon.com has address 198.92.149.185
Foundation.verizon.com has address 216.251.248.19
-bash-2.05b$ █
```

..this leads to a new hit, 'business.verizon.com'.

Google sets allows you to expand on a list once you run out of options.

---

## Fuzzing

- Given hosts with numbers and “predictable” names, we could fuzz the numbers, performing DNS lookups on those names...
- I’ll let Roelof at sensepost discuss this topic, however... =)

[bhst03.verizon.com/](http://bhst03.verizon.com/)

[Similar pages](#)

<https://www33.verizon.com/wi-fi/login/locations/locations-remote.jsp>

[Similar pages](#)

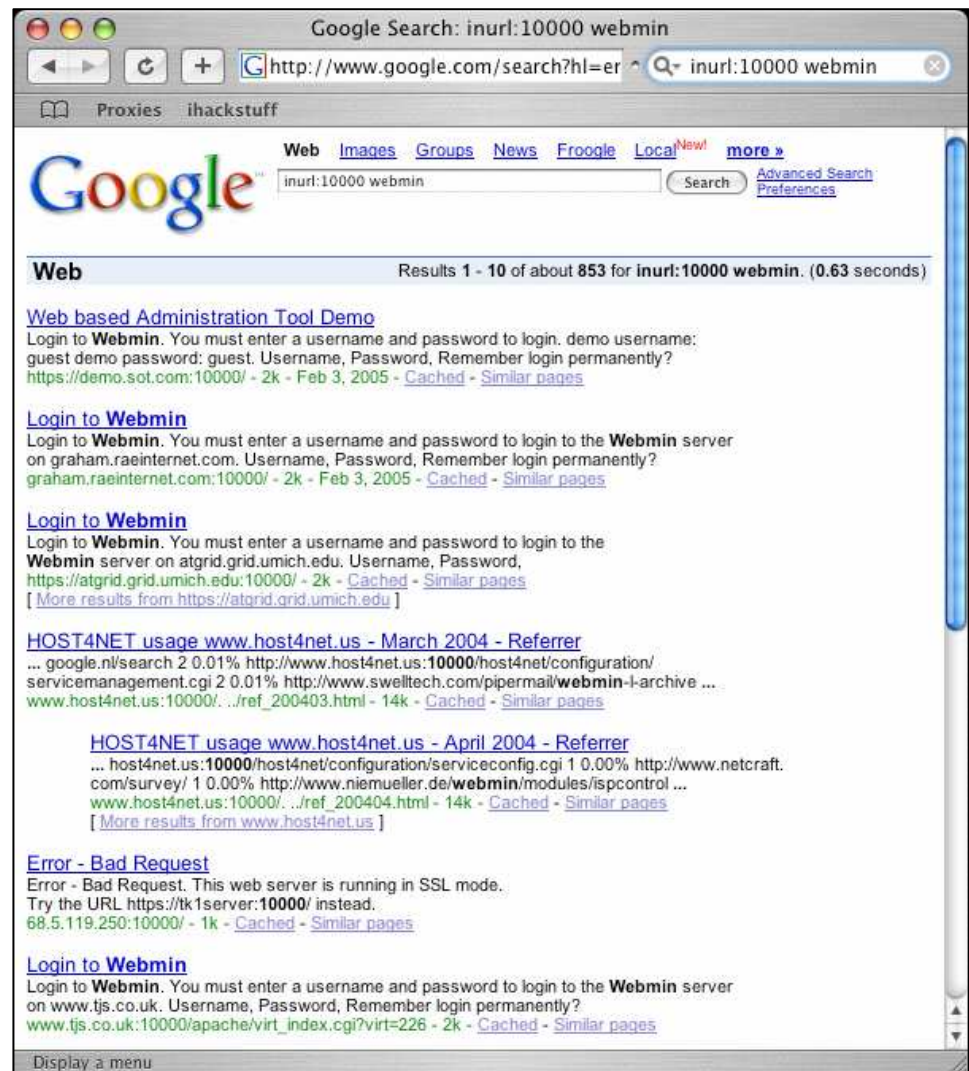
---

## **Limitless mapping possibilities...**

- Once you get rolling with Google mapping, especially automated recursive mapping, you'll be **AMAZED** at how deep you can dig into the layout of a target.

## Port scanning

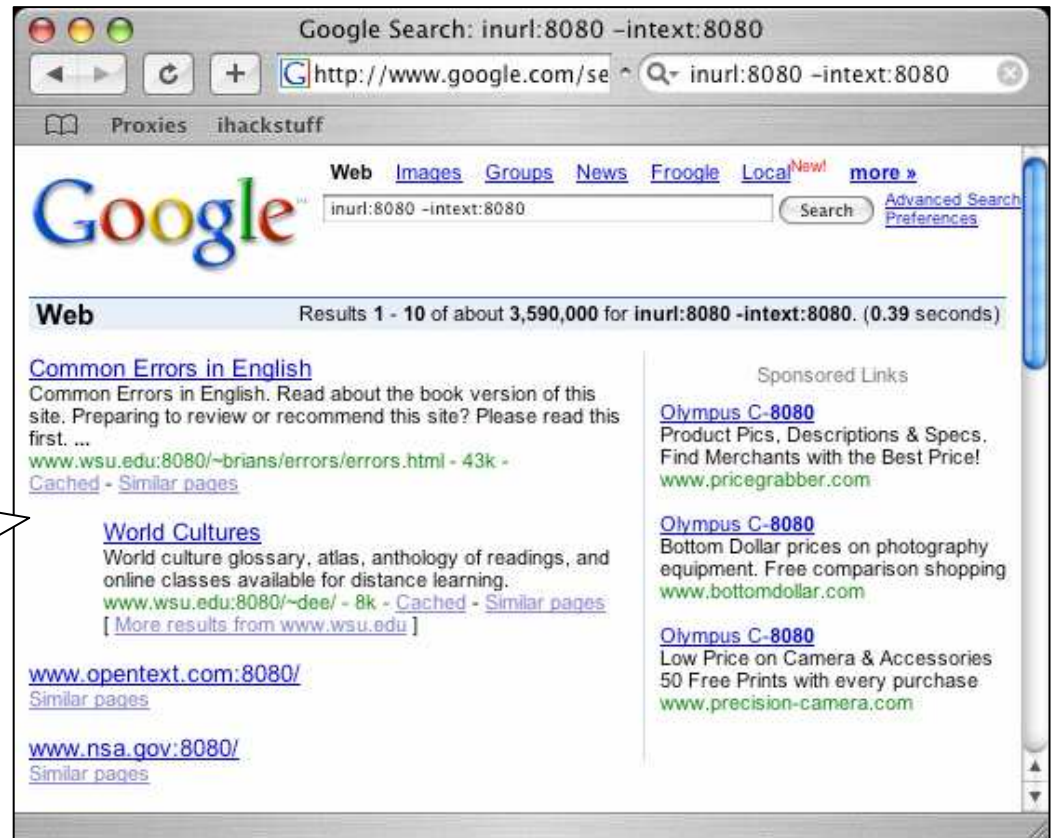
- Although crude, there are ways to do basic “portscanning” with Google.
- First, combine inurl searches for a port with the name of a service that commonly listens on that port... (optionally combined with the site operator)



## Inurl -intext scanning

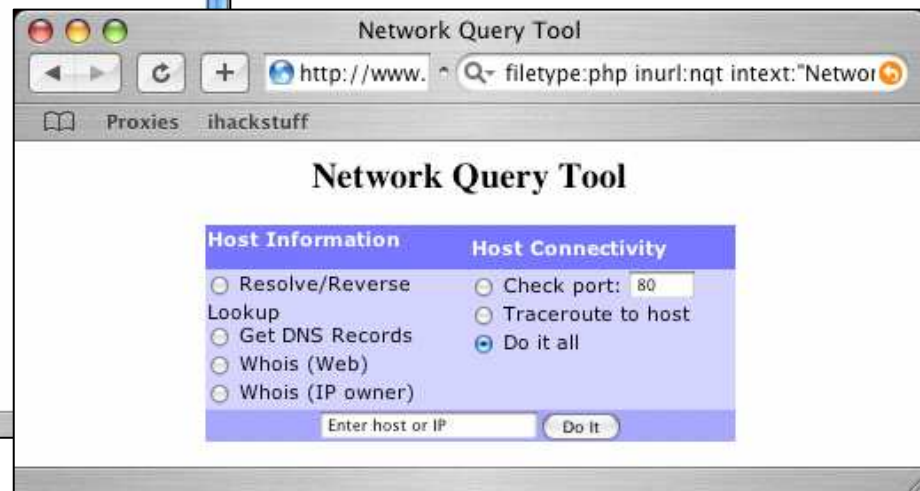
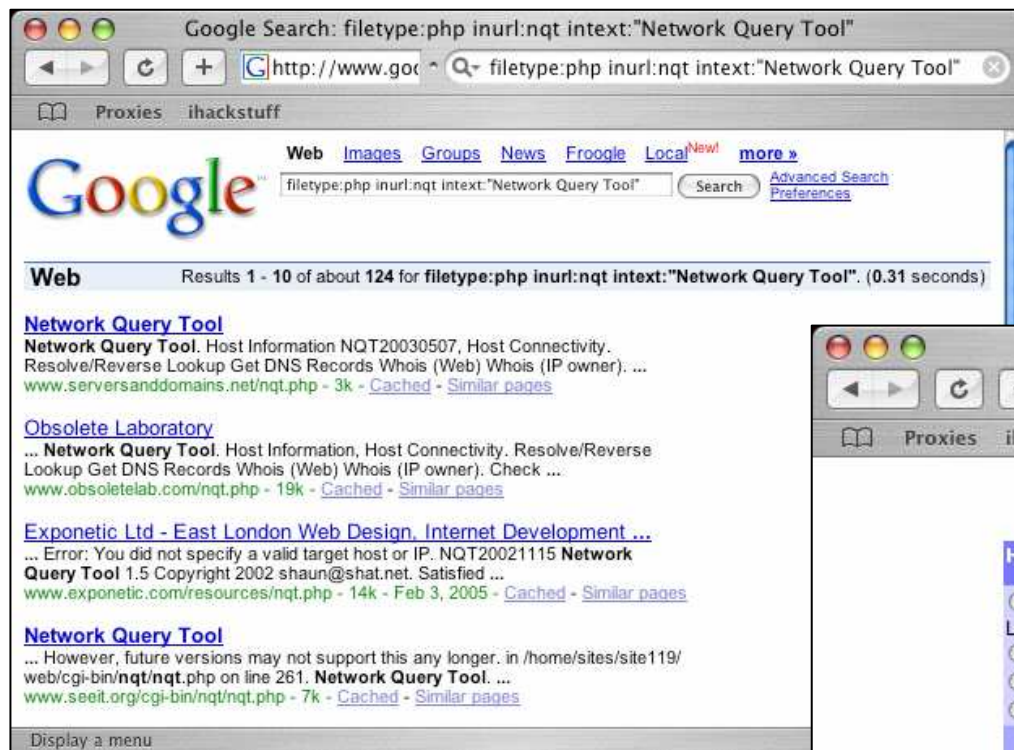
- Another way to go is to use a port number with inurl, combined with a negative intext search for that port number.

This search locates servers listening on port 8080.



## Third party scanners

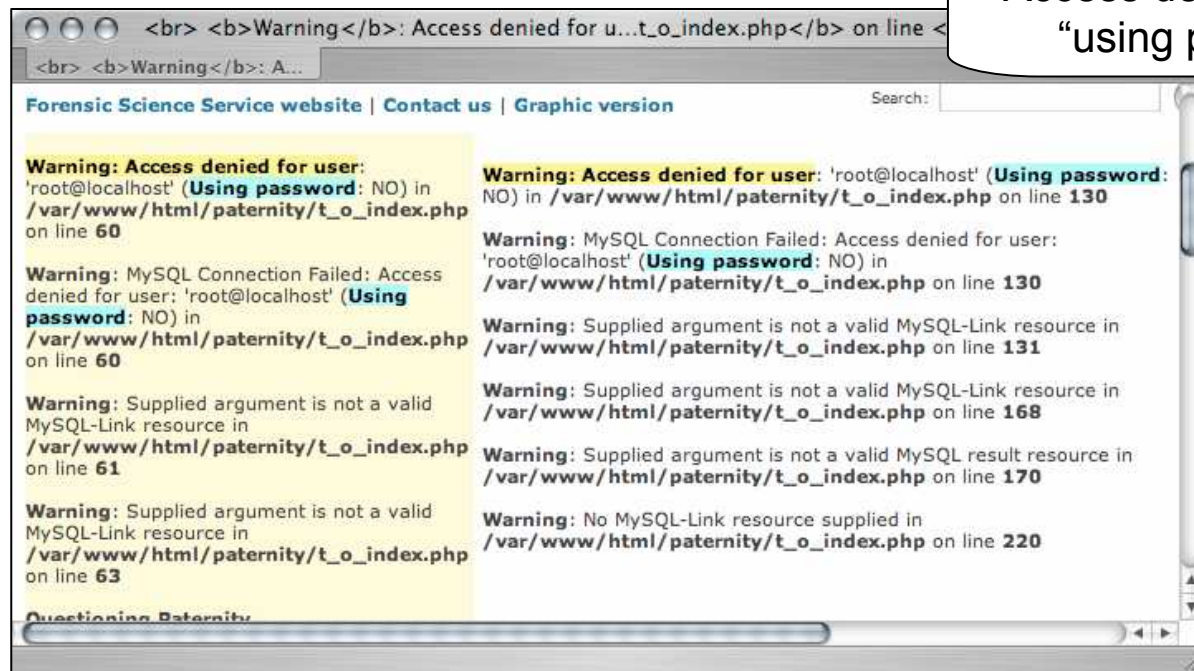
- When all else fails, Google for servers that can do your portscan for you!



# Document Grinding and Database Digging

Documents and databases contain a wealth of information.  
Let's look at ways to foster abuse of SQL databases with Google.

# SQL Usernames

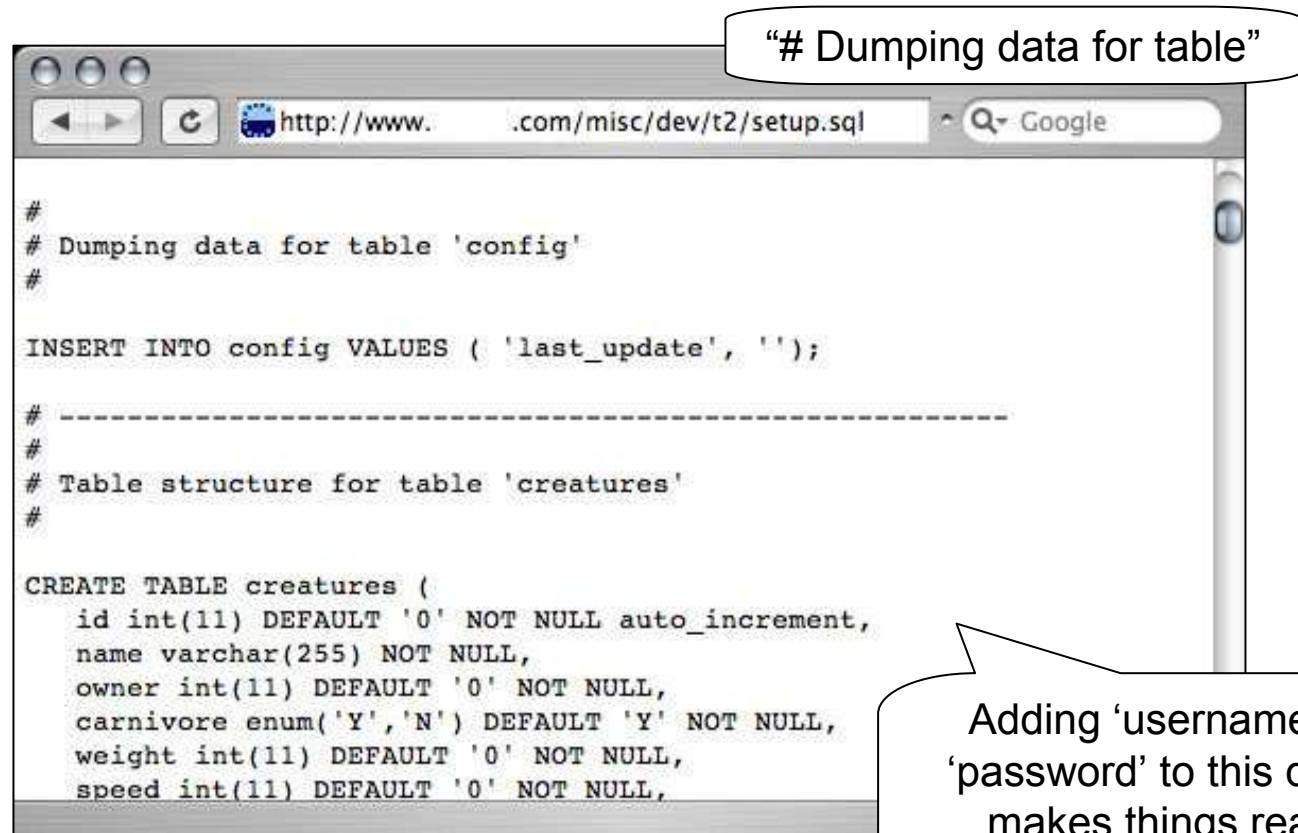


“Access denied for user”  
“using password”



## SQL Schemas

- Entire SQL Database dumps



The screenshot shows a web browser window with the address bar containing `http://www. .com/misc/dev/t2/setup.sql`. The main content area displays SQL code. A callout bubble points to the first line of code, and another callout bubble points to the table creation code.

```
#  
# Dumping data for table 'config'  
#  
INSERT INTO config VALUES ( 'last_update', '' );  
  
# -----  
#  
# Table structure for table 'creatures'  
#  
CREATE TABLE creatures (  
  id int(11) DEFAULT '0' NOT NULL auto_increment,  
  name varchar(255) NOT NULL,  
  owner int(11) DEFAULT '0' NOT NULL,  
  carnivore enum('Y','N') DEFAULT 'Y' NOT NULL,  
  weight int(11) DEFAULT '0' NOT NULL,  
  speed int(11) DEFAULT '0' NOT NULL,
```

"# Dumping data for table"

Adding 'username' or 'password' to this query makes things really interesting.

Improper command termination can be abused quite easily by an attacker.

## SQL injection hints

"ORA-00933: SQL command not properly ended"

```
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1
```

Error Occurred While Processing Request

Error Occurred While Proce...

[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string '>Mrs. Prisbrey"s Second Grade Class v'.

SQL = "SELECT LinkBuilder\_Enabled, FK\_...  
INNER JOIN TB\_Teacher ON TB\_ClassPage...  
WHERE PK\_ClassPageID = 30365 AND Lin...  
Class v"

"Unclosed quotation mark before the character string"

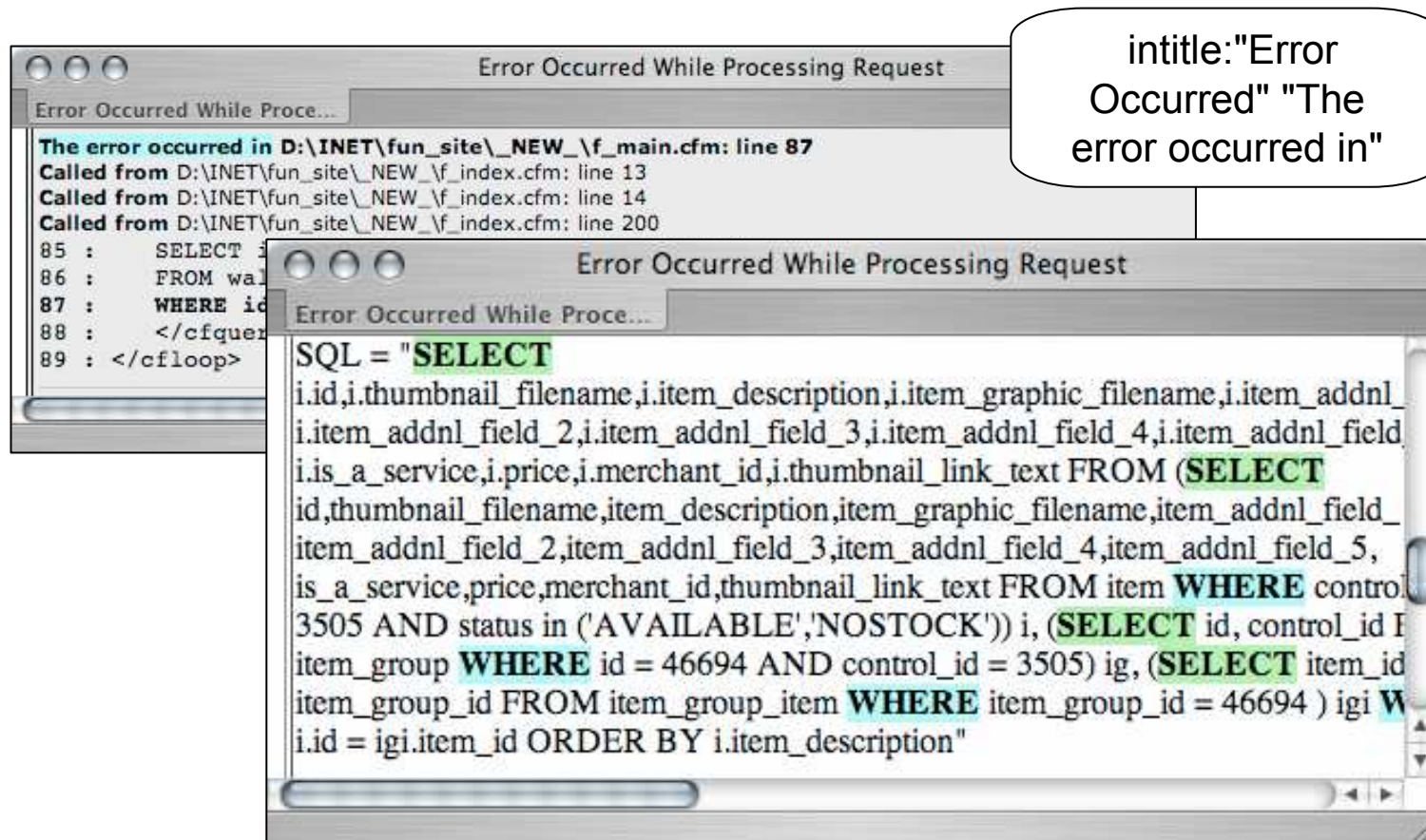
Our Apologies

Our Apologies

Error Detail: [MERANT][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string 'Discover Platinum Card'

## SQL source

- Getting lines of SQL source can aid an attacker.



## Going after SQL passwords

The screenshot shows a web browser window with the address bar containing `http://216.239.41.104/...`. The page content is a PHP script:

```
<?php
$host="";
$user="cs3projo";
$password="tTnM76mx5";
$database="cs3projo"

mysql_connect($host,$user,$password);
@mysql_select_db($database) or die ("I cannot
?>
```

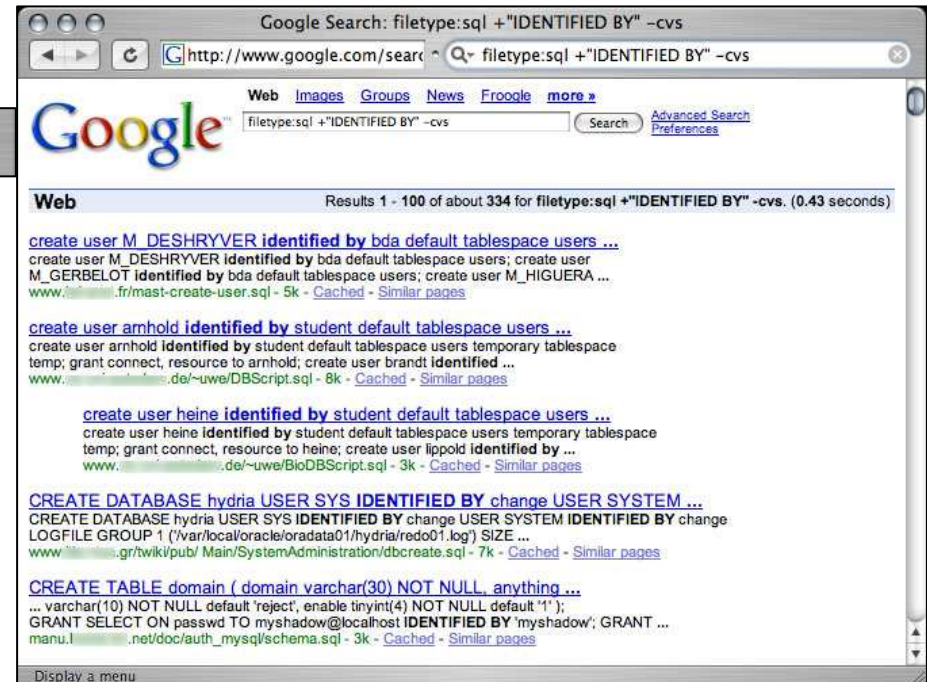
Two callouts are present:

- A callout pointing to the `mysql_connect` function call in the code, containing the text: `filetype:inc intext:mysql_connect`
- A callout pointing to the `$password="tTnM76mx5"` line in the code, containing the text: `Include files with cleartext passwords...`

## More SQL Passwords

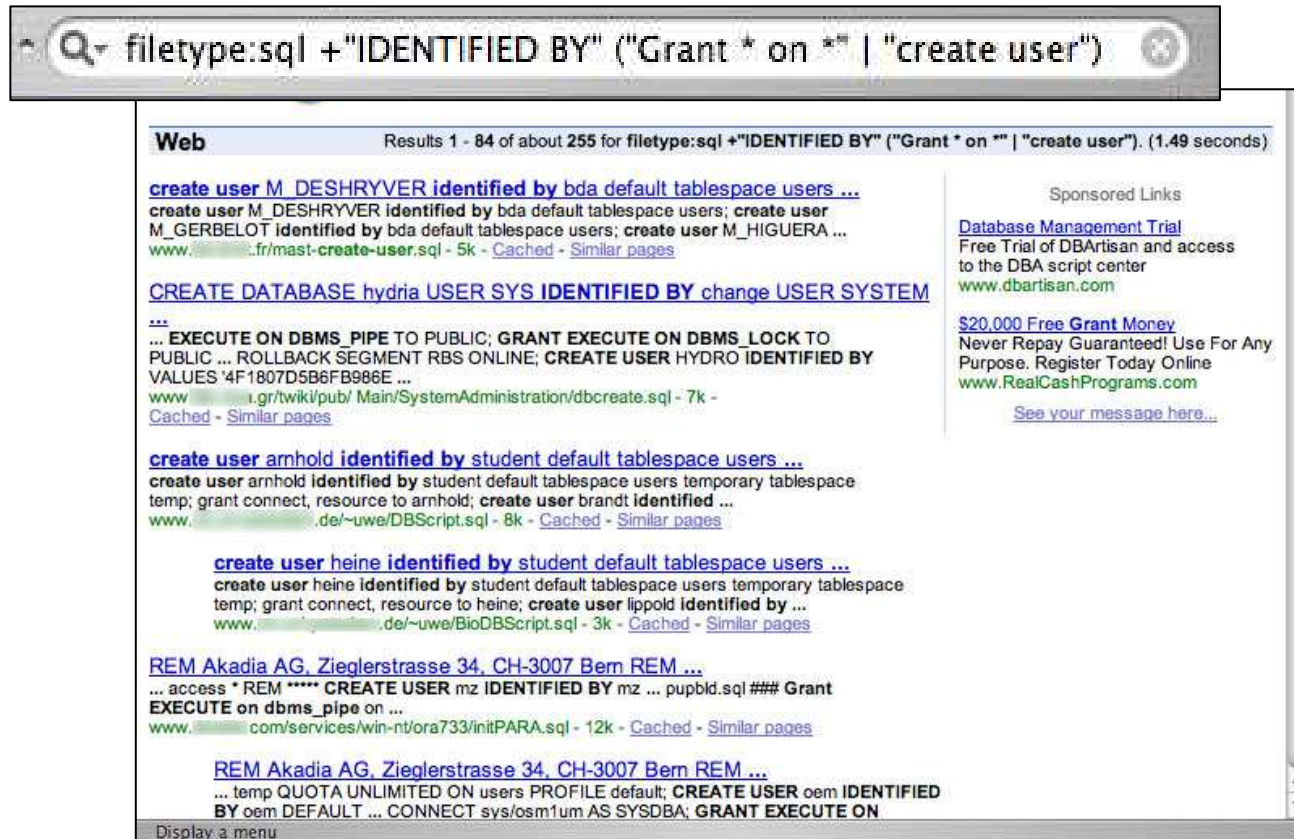
- Question: What's the SQL syntax that can be used to set a passwords?
- (TWO WORDS)
- One Answer: "Identified by"

filetype:sql +"IDENTIFIED BY" -cvs



## More SQL Passwords

- The slightly more hardcore version...



Q- filetype:sql +"IDENTIFIED BY" ("Grant \* on \*" | "create user")

**Web** Results 1 - 84 of about 255 for filetype:sql +"IDENTIFIED BY" ("Grant \* on \*" | "create user"). (1.49 seconds)

[create user M\\_DESHRYVER identified by bda default tablespace users ...](#)  
create user M\_DESHRYVER identified by bda default tablespace users; create user M\_GERBELOT identified by bda default tablespace users; create user M\_HIGUERA ...  
www. ....fr/mast-create-user.sql - 5k - [Cached](#) - [Similar pages](#)

[CREATE DATABASE hydria USER SYS IDENTIFIED BY change USER SYSTEM](#)  
...  
... EXECUTE ON DBMS\_PIPE TO PUBLIC; GRANT EXECUTE ON DBMS\_LOCK TO PUBLIC ... ROLLBACK SEGMENT RBS ONLINE; CREATE USER HYDRO IDENTIFIED BY VALUES '4F1807D5B6FB986E ...  
www. ....gr/twiki/pub/ Main/SystemAdministration/dbcreate.sql - 7k - [Cached](#) - [Similar pages](#)

[create user arnhold identified by student default tablespace users ...](#)  
create user arnhold identified by student default tablespace users temporary tablespace temp; grant connect, resource to arnhold; create user brandt identified ...  
www. ....de/~uwe/DBScript.sql - 8k - [Cached](#) - [Similar pages](#)

[create user heine identified by student default tablespace users ...](#)  
create user heine identified by student default tablespace users temporary tablespace temp; grant connect, resource to heine; create user lippold identified by ...  
www. ....de/~uwe/BioDBScript.sql - 3k - [Cached](#) - [Similar pages](#)

[REM Akadia AG, Zieglerstrasse 34, CH-3007 Bern REM ...](#)  
... access \* REM \*\*\*\*\* CREATE USER mz IDENTIFIED BY mz ... pupbid.sql### Grant EXECUTE on dbms\_pipe on ...  
www. ....com/services/win-nt/ora733/initPARA.sql - 12k - [Cached](#) - [Similar pages](#)

[REM Akadia AG, Zieglerstrasse 34, CH-3007 Bern REM ...](#)  
... temp QUOTA UNLIMITED ON users PROFILE default; CREATE USER oem IDENTIFIED BY oem DEFAULT ... CONNECT sys/osm1um AS SYSDBA; GRANT EXECUTE ON

Sponsored Links  
[Database Management Trial](#)  
Free Trial of DBArtisan and access to the DBA script center  
[www.dbartisan.com](#)

[\\$20,000 Free Grant Money](#)  
Never Repay Guaranteed! Use For Any Purpose. Register Today Online  
[www.RealCashPrograms.com](#)

[See your message here...](#)

Display a menu

## Various database detection queries

Query	Description
<i>inurl:nuke filetype:sql</i>	php-nuke or postnuke CMS dumps
<i>filetype:sql password</i>	SQL database dumps or batched SQL commands
<i>filetype:sql "IDENTIFIED BY" -cvs</i>	SQL database dumps or batched SQL commands, focus on "IDENTIFIED BY", which can locate passwords
<i>"# Dumping data for table (username user users password)"</i>	SQL database dumps or batched SQL commands, focus on interesting terms
<i>"#mysql dump" filetype:sql</i>	SQL database dumps
<i>"# Dumping data for table"</i>	SQL database dumps
<i>"# phpMyAdmin MySQL-Dump" filetype:txt</i>	SQL database dumps created by phpMyAdmin
<i>"# phpMyAdmin MySQL-Dump" "INSERT INTO" -"the"</i>	SQL database dumps created by phpMyAdmin (variation)

SQL dump detection

Database detection

Query	Description
<i>filetype:cfm "cfapplication name" password</i>	ColdFusion source code
<i>filetype:mdb inurl:users.mdb</i>	Microsoft Access user database
<i>inurl:email filetype:mdb</i>	Microsoft Access e-mail database
<i>inurl:backup filetype:mdb</i>	Microsoft Access backup databases
<i>inurl:forum filetype:mdb</i>	Microsoft Access forum databases
<i>inurl:/db/main.mdb</i>	ASP-Nuke databases
<i>inurl:profiles filetype:mdb</i>	Microsoft Access user profile databases
<i>filetype:asp DBQ=" * Server.MapPath("*.mdb")</i>	Microsoft Access database connection string search
<i>allinurl: admin mdb</i>	Microsoft Access administration databases

# Automation

Page Scraping in Perl  
API querying in Perl



---

## Page Scraping with Perl

- This Perl code, by James Foster, provides a good framework for “page scraping” Google results.
- This method relies on manually querying Google, and searching the resultant HTML for the “interesting stuff.”

```
#!/usr/bin/perl -w  
use IO::Socket;
```

```
#Section 2
```

```
$query = '/search?hl=en&q=dog';
```

```
$server = 'www.google.com';
```

```
$port = 80;
```

We will be making socket calls. We need IO::Socket.

We hardcode our query (which we can make a parameter later), our Google server and our port number.

---

## Page Scraping with Perl

```
sub socketInit()
{
    $socket = IO::Socket::INET->new(
        Proto => 'tcp',
        PeerAddr => $server,
        PeerPort => $port,
        Timeout => 10,
    );

    unless($socket)
    {
        die("Could not connect to $server:$port");
    }

    $socket->autoflush(1);
}
```

Next we have a very generic socket initialization subroutine.

## Page Scraping with Perl

```
sub sendQuery($)  
{  
  my ($myquery) = @_;  
  print $socket ("GET $myquery HTTP/1.0\n\n");  
  while ($line = <$socket>)  
  {  
    if ($line =~ /Results.*of\sabout/)  
    {  
      return $line;  
    }  
  }  
}
```

This subroutine sends the Google query (hardcoded above) and accepts one parameter, the Google query.

Google returned HTML is processed, and the line containing "of about" (our result line) is returned from this routine.

Results 1 - 10 of about **46,600** for "[james foster](#)". (0.49 seconds)

## Page Scraping with Perl

```
sub getTotalHits($)  
{  
  my ($sourline) = @_;  
  $hits="";  
  $index = index($sourline, "of about");  
  $str = substr($sourline, $index, 30);  
  @buf=split(//,$str);  
  for ($i = 0; $i < 30; $i++)  
  {  
    if ($buf[$i] =~ /[0-9]/)  
    {  
      $hits=$hits.$buf[$i];  
    }  
  }  
  return $hits;  
}
```

This subroutine takes one parameter (the results line from the Sendquery)

"of about is located" ...

...the next 30 characters are grabbed...

... all the digits are removed....

...stored in \$hits...

...and returned.

Results 1 - 10 of about **46,600** for "[james foster](#)". (0.49 seconds)

---

## Page Scraping with Perl

```
socketInit();  
$string = sendQuery($query);  
$totalhits = getTotalHits($string);  
  
#Printing to STDOUT the Total Hits Retrieved from Google  
print ($totalhits);
```

The socket is  
initialized...

...the query is  
sent...

This piece of code  
drives all the  
subroutines.

...the total hits are  
determined...

...and printed out.

---

## CGI Scanning

/iisadmpwd/  
/iisadmpwd/achg.htr  
/iisadmpwd/aexp.htr  
/iisadmpwd/aexp2.htr  
/iisadmpwd/aexp2b.htr

Another automation example  
might involve chopping up a  
CGI scanner's vulnerability  
file...

inurl:/iisadmpwd/  
inurl:/iisadmpwd/achg.htr  
inurl:/iisadmpwd/aexp.htr  
inurl:/iisadmpwd/aexp2.htr  
inurl:/iisadmpwd/aexp2b.htr

... converting the checks into  
Google queries, sending these  
queries to a Google scanner.

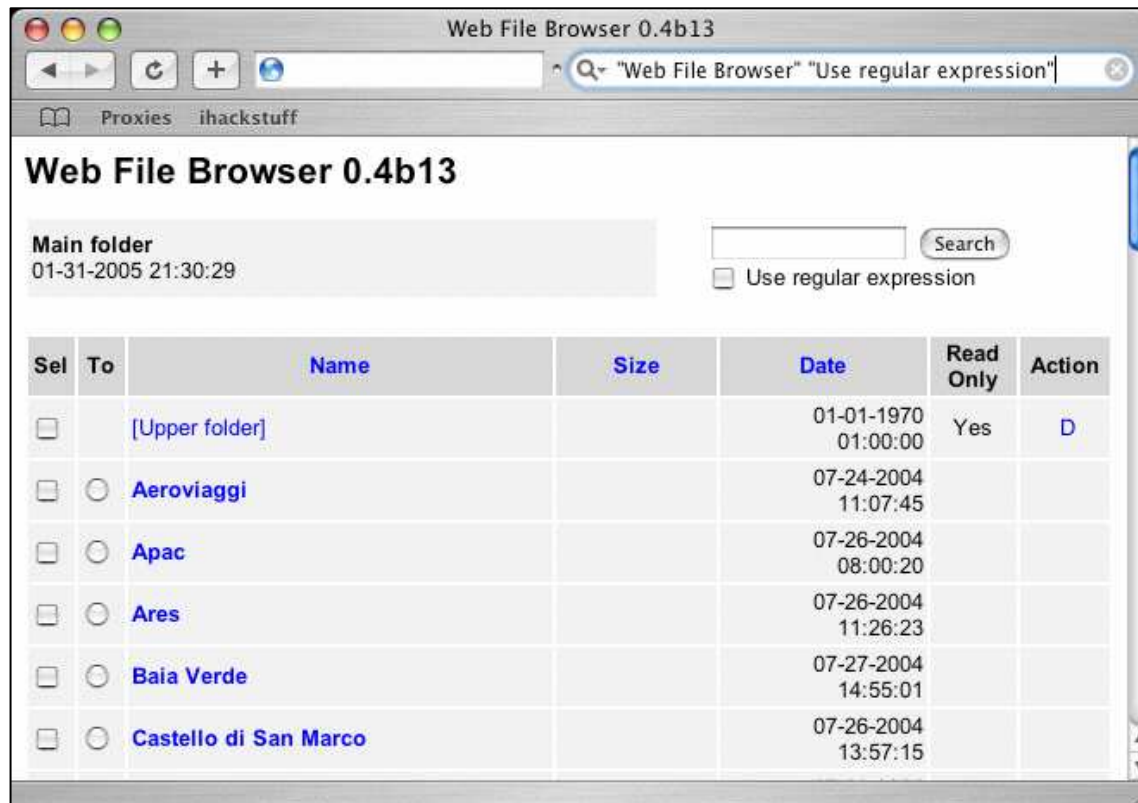
intitle:index.of /iisadmpwd/  
intitle:index.of /iisadmpwd/achg.htr  
intitle:index.of /iisadmpwd/aexp.htr  
intitle:index.of /iisadmpwd/aexp2.htr  
intitle:index.of /iisadmpwd/aexp2b.htr

# Web Servers, Login Portals, Network Hardware

Network devices can be soooo much fun to Google for...

# Web File Browser

- This program allows directory walking, file uploading, and more.





## VNC Servers (with client)

- VNC (Virtual Network Computing) allows you to control a workstation remotely.

The image shows a browser window titled "VNC viewer for Java" with a search bar containing "intitle:'VNC viewer for Java'". The browser displays the RealVNC logo and version information. A dialog box titled "VNC Viewer: Connection Details" is open, showing the VNC server address as "warp.win .net::1236".

The search is very basic

These sites launch a VNC Java client so you can connect! Even if password protected, the client reveals the server name and port.

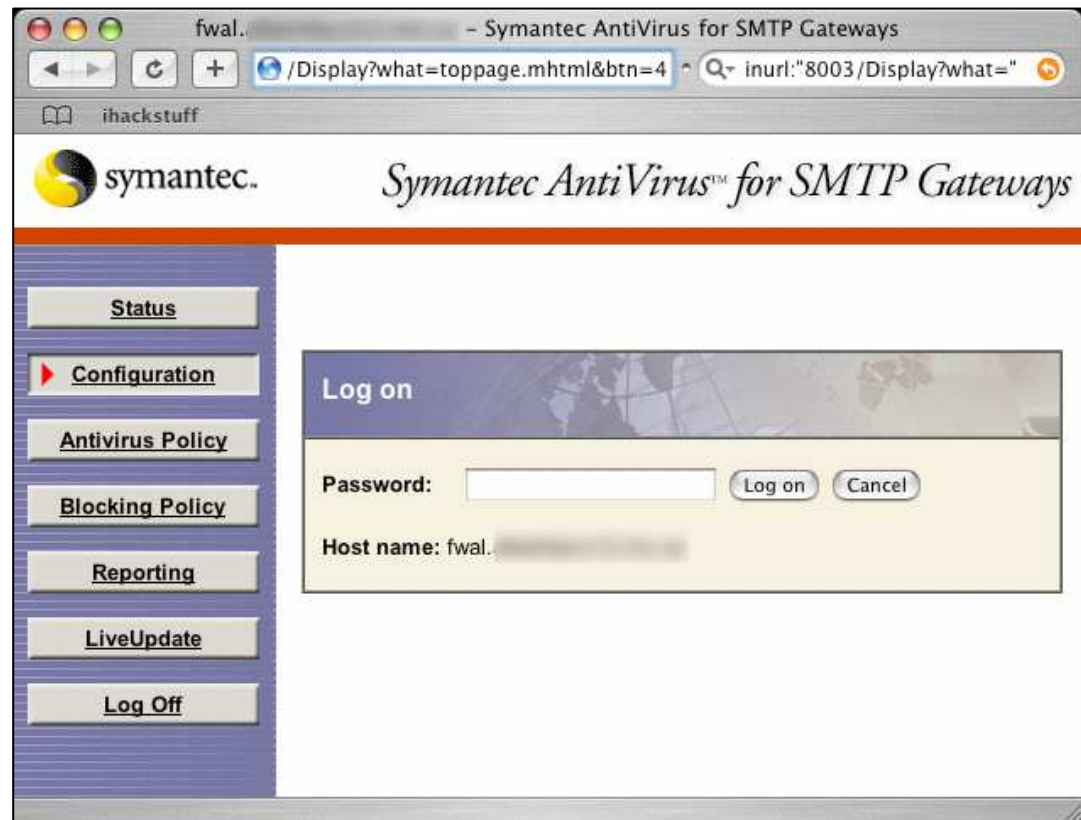
VNC viewer for Java version 4.0  
Copyright (C) 2002-2004 RealVNC Ltd.  
See <http://www.realvnc.com> for information on VNC.

VNC server: warp.win .net::1236

Buttons: About... Options... OK Cancel

Thanks to lester for this one!

# Symantec Anti-Virus SMTP Gateways



# Axis Print Servers

Print server administration, Google-style!

The screenshot shows a web browser window titled "Network Print Server". The address bar contains the search query "intitle: 'Network Print Server' filetype: shtml". The browser's proxy settings are set to "ihackstuff". The main content area features the "Network Print Server" title and the "AXIS COMMUNICATIONS" logo. Below this is a "Printer Overview" section. On the left, there are navigation buttons for "Printer Overview", "Print Jobs", and "General Help". A sidebar shows "user" and "admin" buttons, along with a "USER GROUP" icon. The main content area displays a diagram of the printer's connections (Ethernet, Print Server, LPT1) and the following information:

- Model: **AXIS 540+/542+**
- Print Server Name: **AXIS42AA7F**
- System Location: **301A-EGRC**
- Serial Number: **00:40:8C:42:AA:7F**

A "Configuration Wizard" button is located at the bottom of the overview section.

Thanks to murfie for this one!

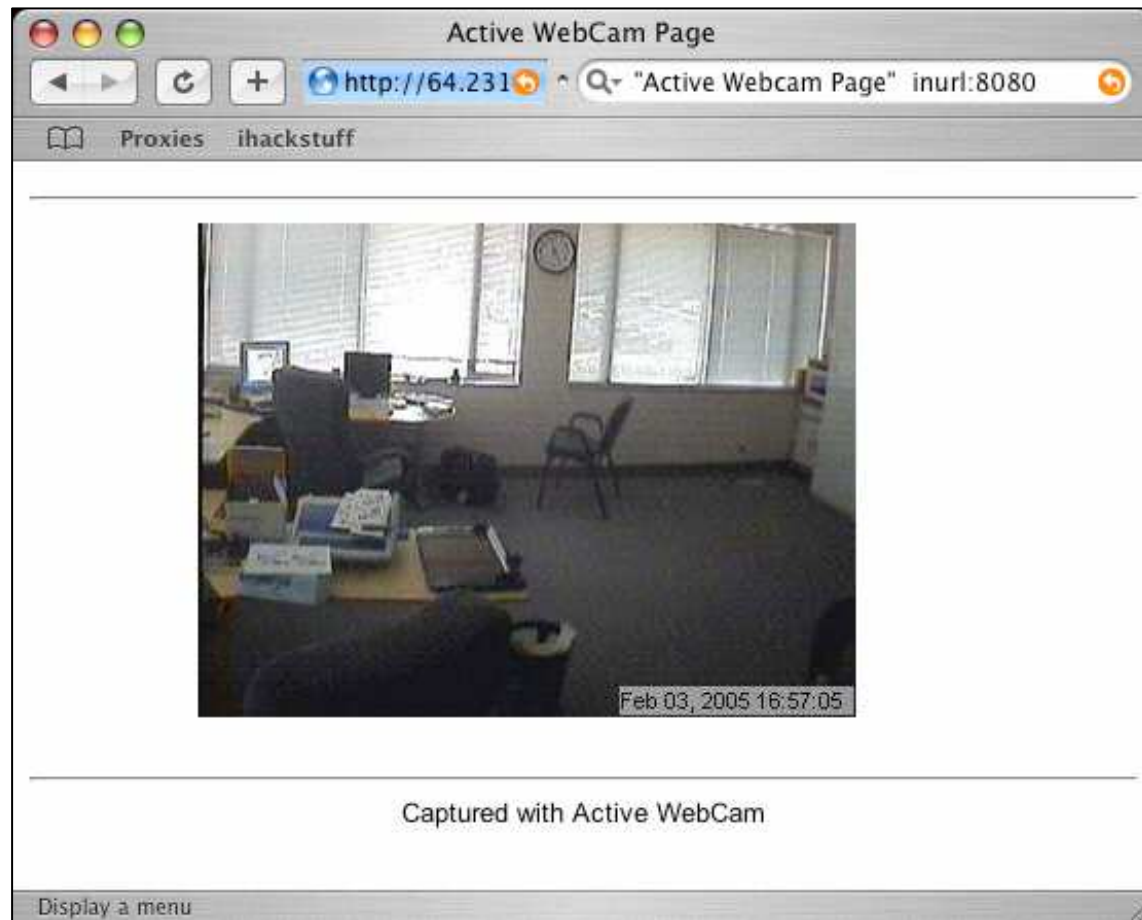
# Xenix, Sweex, Orite Web Cams



One query,  
many  
brands of  
live cams!

Thanks to  
server1 for  
this one!

# Active WebCam



Thanks  
klouw!

# Toshiba Network Cameras

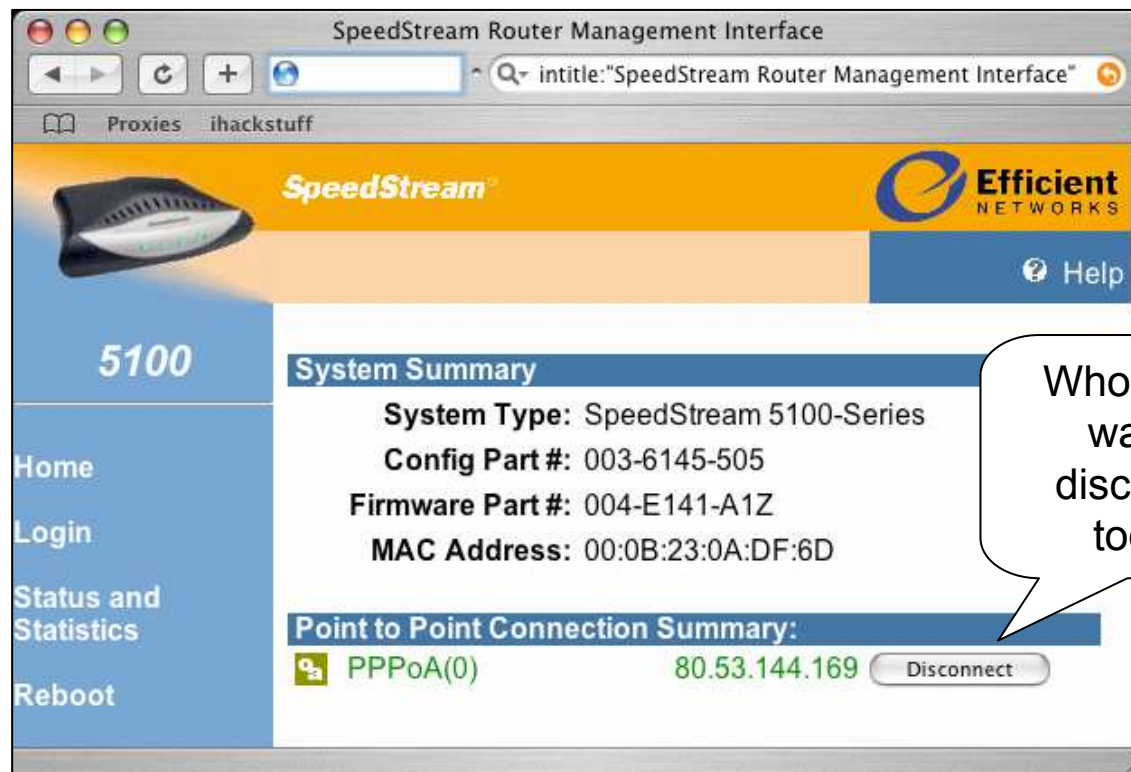


intitle:"toshiba  
network camera -  
User Login"

Found by  
WarriorClown!

# Speedstream DSL Routers

- Home broadband connectivity... Googled.

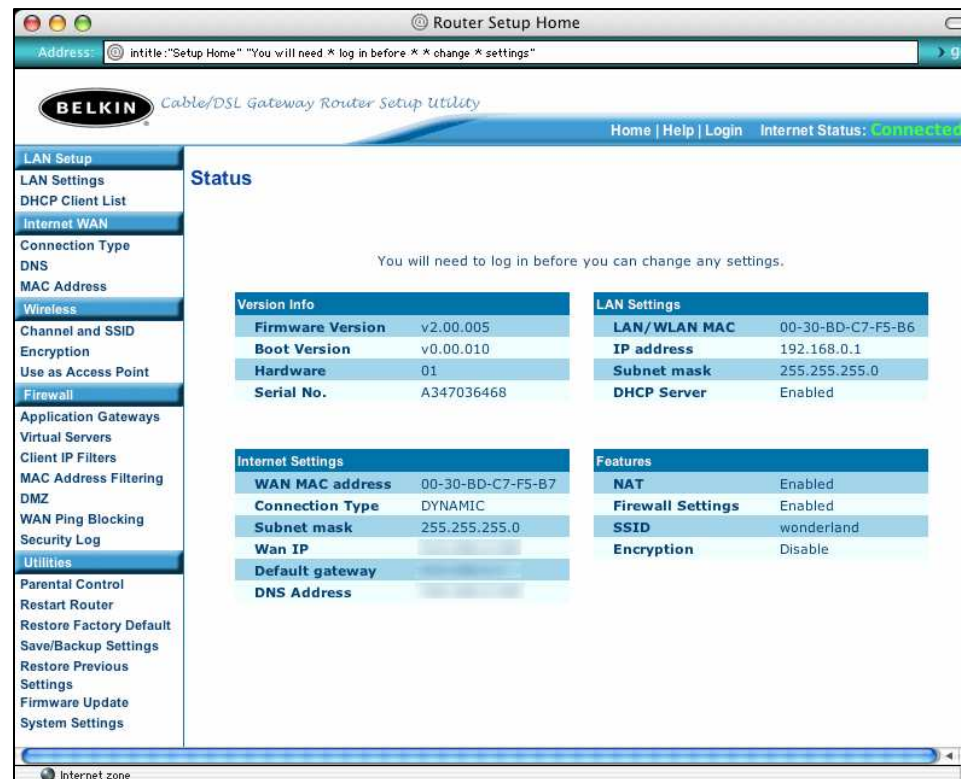


Who do you want to disconnect today?

Found by m00d!

## Belkin Routers

- Belkin routers have become a household name in connected households. The management interface shouldn't show up on Google... but it does.



Router Setup Home

Address: intitle:"Setup Home" "You will need \* log in before \*\* change \* settings"

**BELKIN** Cable/DSL Gateway Router Setup Utility

Home | Help | Login | Internet Status: **Connected**

**LAN Setup**

- LAN Settings
- DHCP Client List

**Internet WAN**

- Connection Type
- DNS
- MAC Address

**Wireless**

- Channel and SSID
- Encryption
- Use as Access Point

**Firewall**

- Application Gateways
- Virtual Servers
- Client IP Filters
- MAC Address Filtering
- DMZ
- WAN Ping Blocking
- Security Log

**Utilities**

- Parental Control
- Restart Router
- Restore Factory Default
- Save/Backup Settings
- Restore Previous Settings
- Firmware Update
- System Settings

**Status**

You will need to log in before you can change any settings.

Version Info	
Firmware Version	v2.00.005
Boot Version	v0.00.010
Hardware	01
Serial No.	A347036468

LAN Settings	
LAN/WLAN MAC	00-30-BD-C7-F5-B6
IP address	192.168.0.1
Subnet mask	255.255.255.0
DHCP Server	Enabled

Internet Settings	
WAN MAC address	00-30-BD-C7-F5-B7
Connection Type	DYNAMIC
Subnet mask	255.255.255.0
Wan IP	
Default gateway	
DNS Address	

Features	
NAT	Enabled
Firewall Settings	Enabled
SSID	wonderland
Encryption	Disable

Thanks to  
darksun for  
this one!





# Printers

- Trolling printers through Google can be fun, especially when you can see and download what others are printing...

The screenshot shows a web browser window titled 'Web Image Monitor' with the URL 'inurl:webArch/mainFrame.cgi'. The page is for a 'RICOH Aficio 2027' printer. The main content area is titled 'Printer Job History' and shows a table of print jobs. A speech bubble points to the job with ID 77, 'Microsoft Word - Recent Religion Work.doc'.

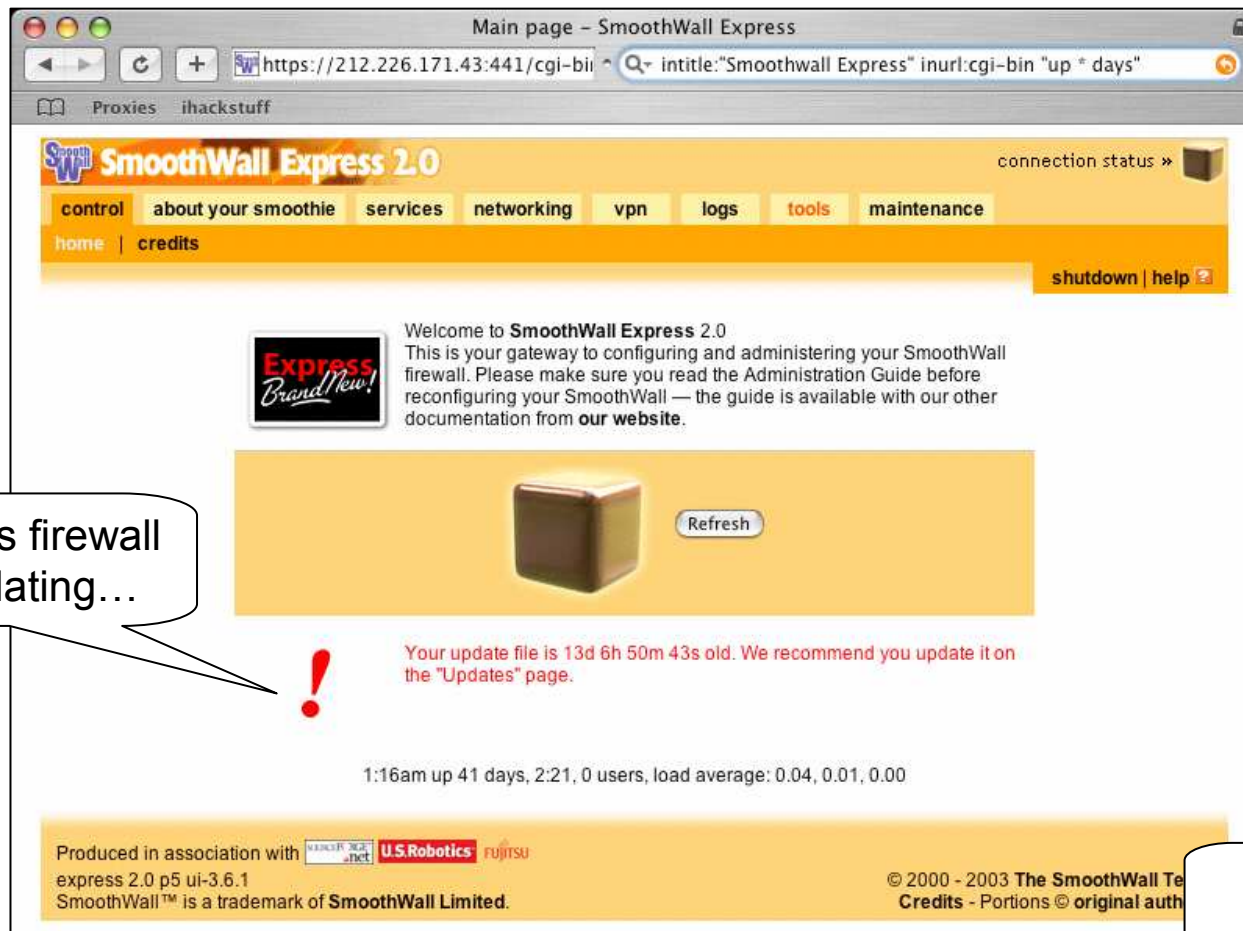
ID	User Name	User ID	Document Name	Status	Started At	Pages
77	---	?	Microsoft Word - Recent Religion Work.doc	Print Complete	Jan 31, 2005 2:05:56 PM	
76	---	?	Microsoft Word - JCLectures.doc	Print Complete	Jan 31, 2005 11:59:57 PM	
75	---	?	Microsoft Word - JCLectures.doc	Print Complete	Jan 30, 2005 11:16:48 AM	
74	---	?	Microsoft Word - Document6	Print Complete	Jan 26, 2005 3:11:20 PM	
73	---	?	Microsoft Word - Document6	Print Complete	Jan 26, 2005 3:11:13 PM	
72	---	?	Microsoft Word - JCLectures.doc	Print Complete	Jan 26, 2005 11:48:25 PM	
71	---	?	http://www.kim.dhhs.gov/pulcherrima/aphrodisia	Print Complete	Jan 26, 2005 11:48:44 AM	
70	---	?	http://www.kim.dhhs.gov/pulcherrima/aphrodisia	Print Complete	Jan 26, 2005 11:48:09 AM	
69	---	?	C:\Documents and Settings\Relig.PDF	Print Complete	Jan 26, 2005 10:44:01 AM	
68	---	?	Microsoft Word - JCLectures.doc	Print Complete	Jan 25, 2005 4:19:29 PM	

Religion...

And aphrodisiacs?  
Hrrmmm...

Thanks  
JimmyNeutron!

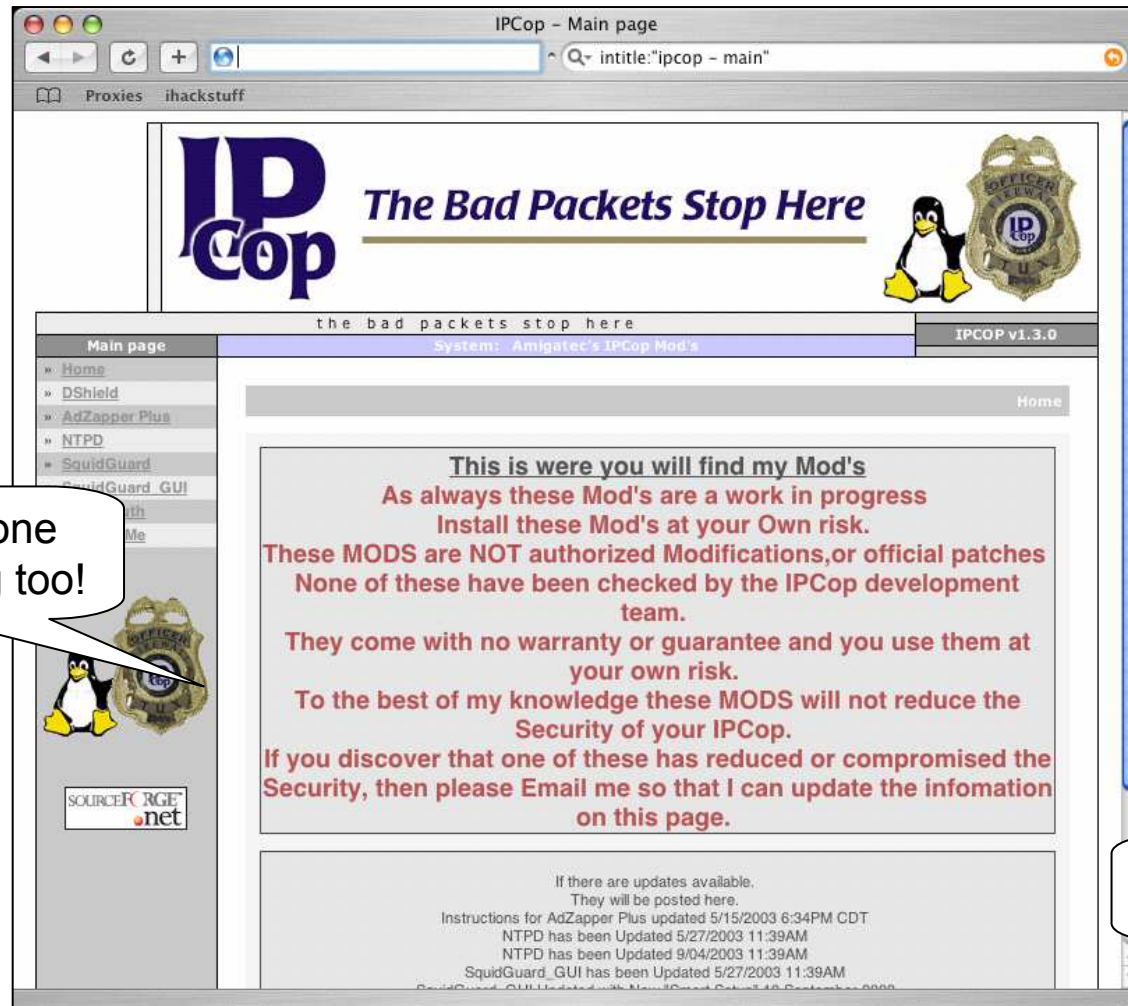
# Firewalls - Smoothwall



Uh oh... this firewall needs updating...

Thanks Milkman!

# Firewalls - IPCop



Uh oh... this one needs updating too!

Thanks Jimmy Neutron!

# IDS Data: ACID

- SNORT IDS data delivered graphically, served up fresh

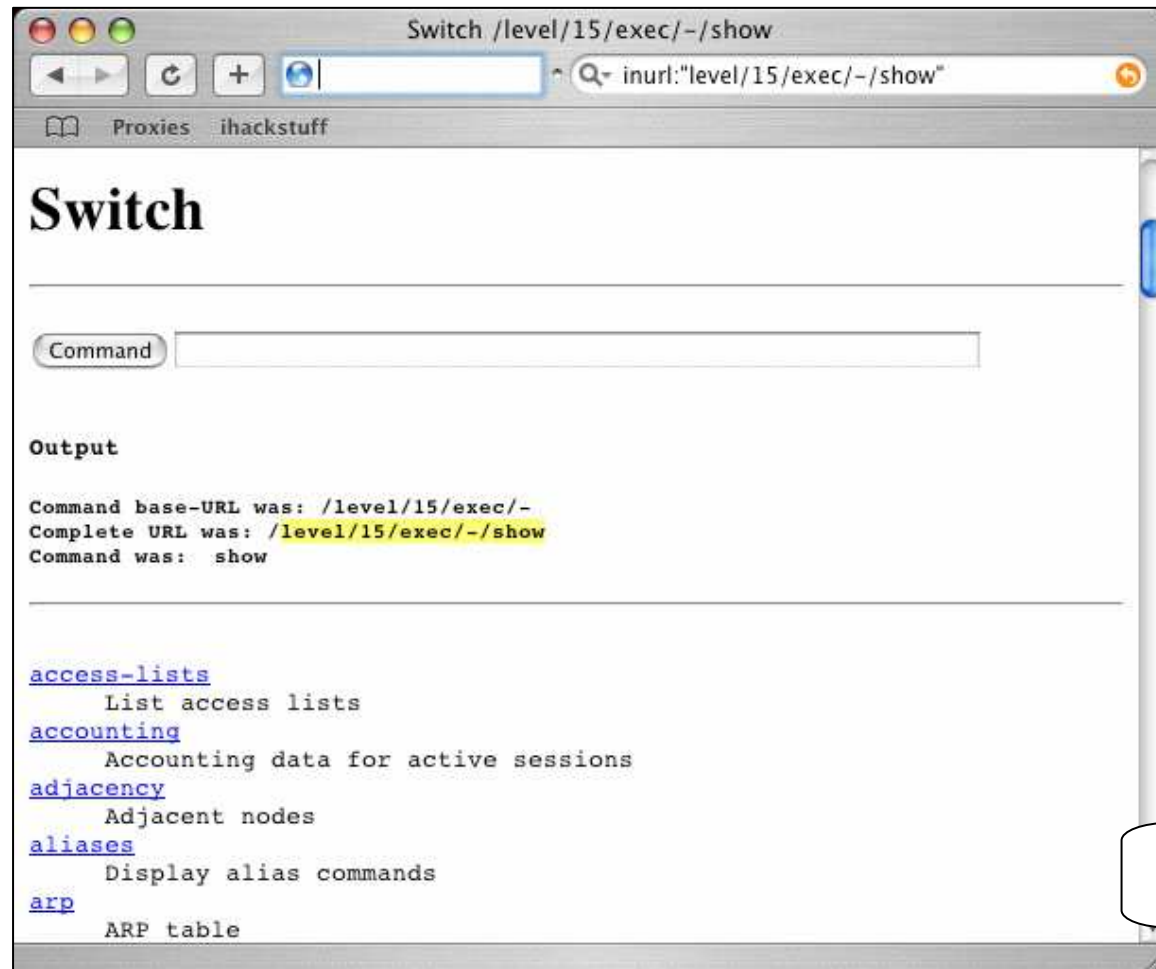
The image shows two browser windows. The left window is a Google search for "ACID 'by Roman Danyliw' filetype:php". The right window shows the "ACID: Query Results: 15 Last Alerts" page, which is a table of alerts.

**ACID: Query Results: 15 Last Alerts**

Alert ID	Rule	Source	Destination	Time
#1- 76637	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20 13:47:42		
#2- 76636	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20 13:47:42		
#3- 76635	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20 13:47:42	218.163.74.20:1235	
#4- 76634	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20 13:47:42	218.163.74.20:1236	
#5- 76633	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20 13:47:42	218.163.74.20:1235	
#6- 76632	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20 13:47:42	218.163.74.20:1236	
#7- 76631	[snort] (http_inspect) IIS UNICODE (1- CODEPOINT ENCODING)	2004-07-20 13:47:42	218.163.74.20:1236	
#8-	[snort] (http_inspect) IIS UNICODE	2004-07-20		

ACID "by Roman Danyliw" filetype:php

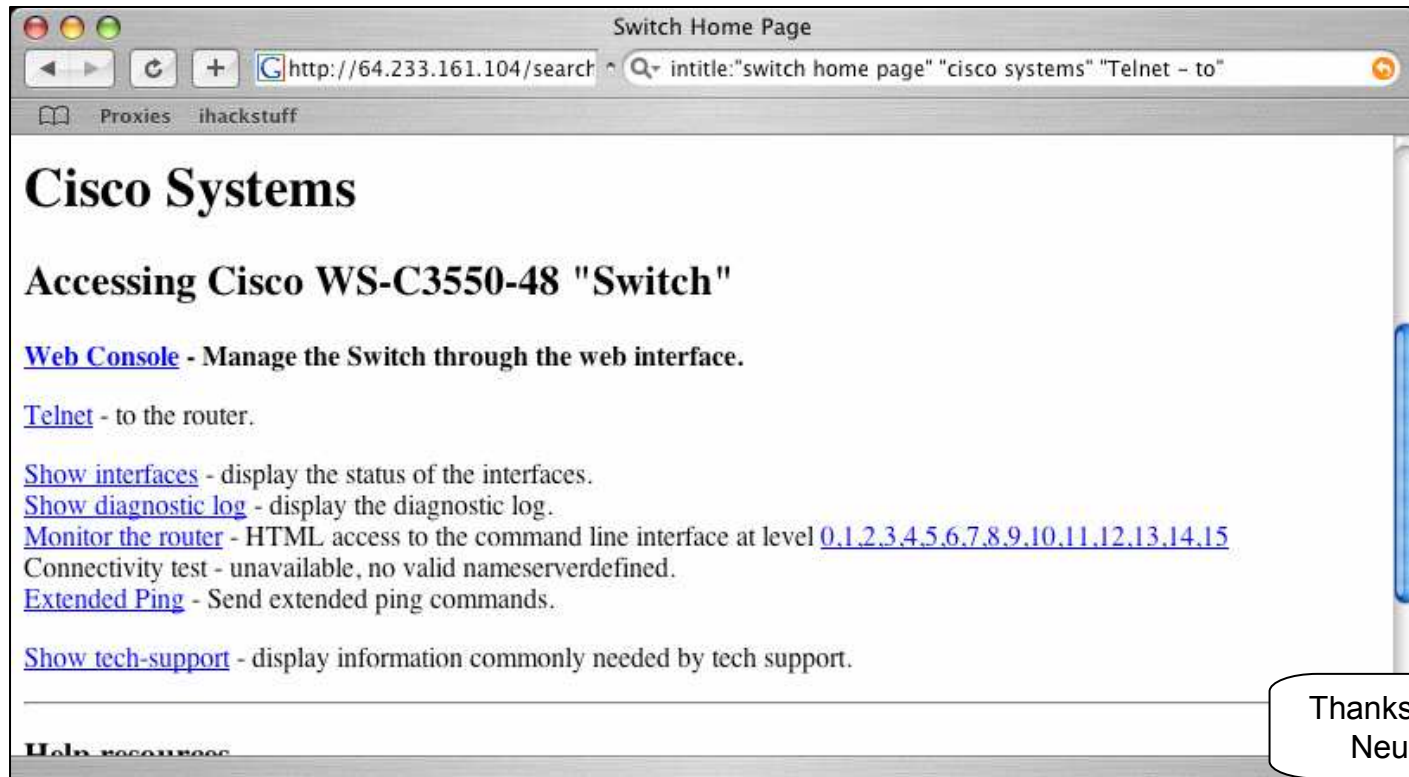
# Open Cisco Devices



Thanks Jimmy  
Neutron!

---

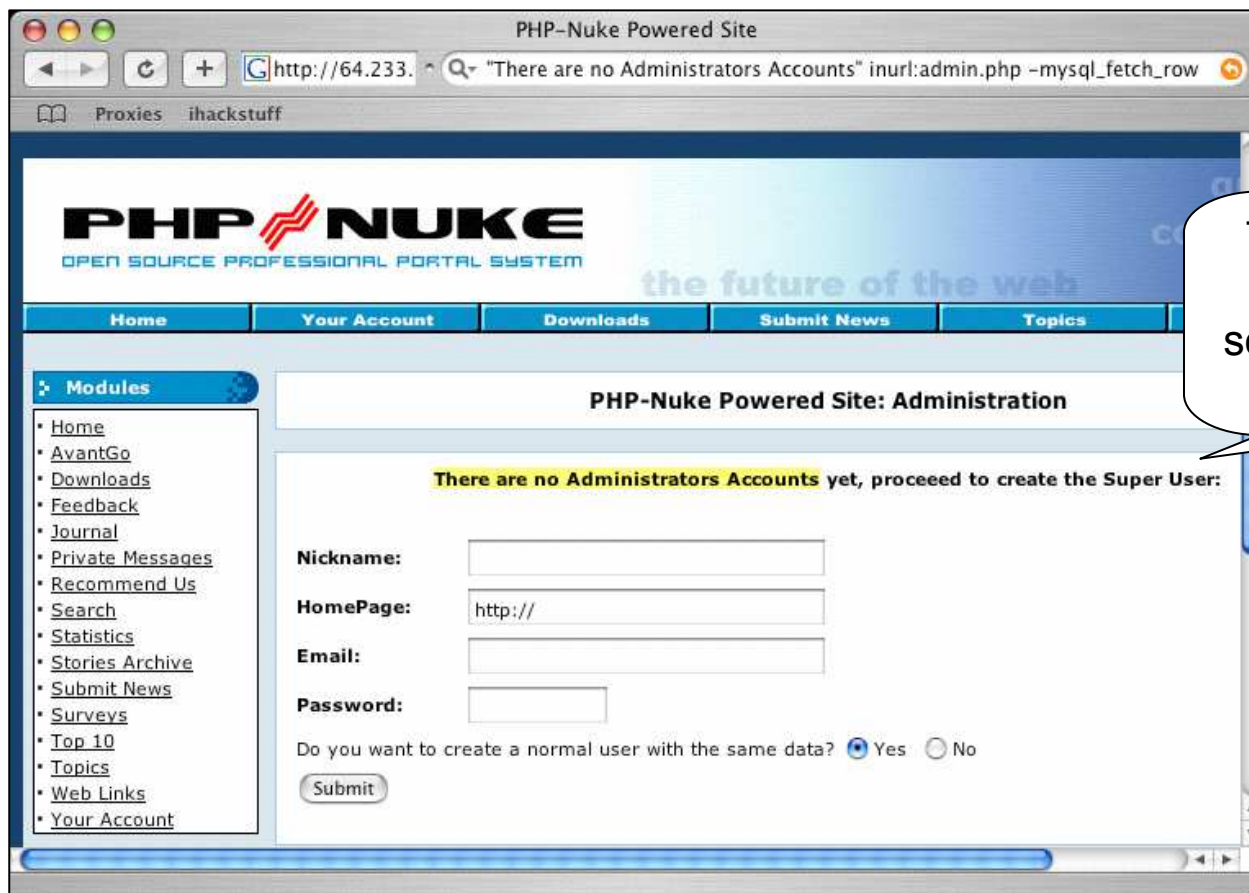
# Cisco Switches



Thanks Jimmy Neutron!

## Wide Open PHP Nuke Sites

- PHP Nuke allows for the creation of a full-featured web site with little effort.

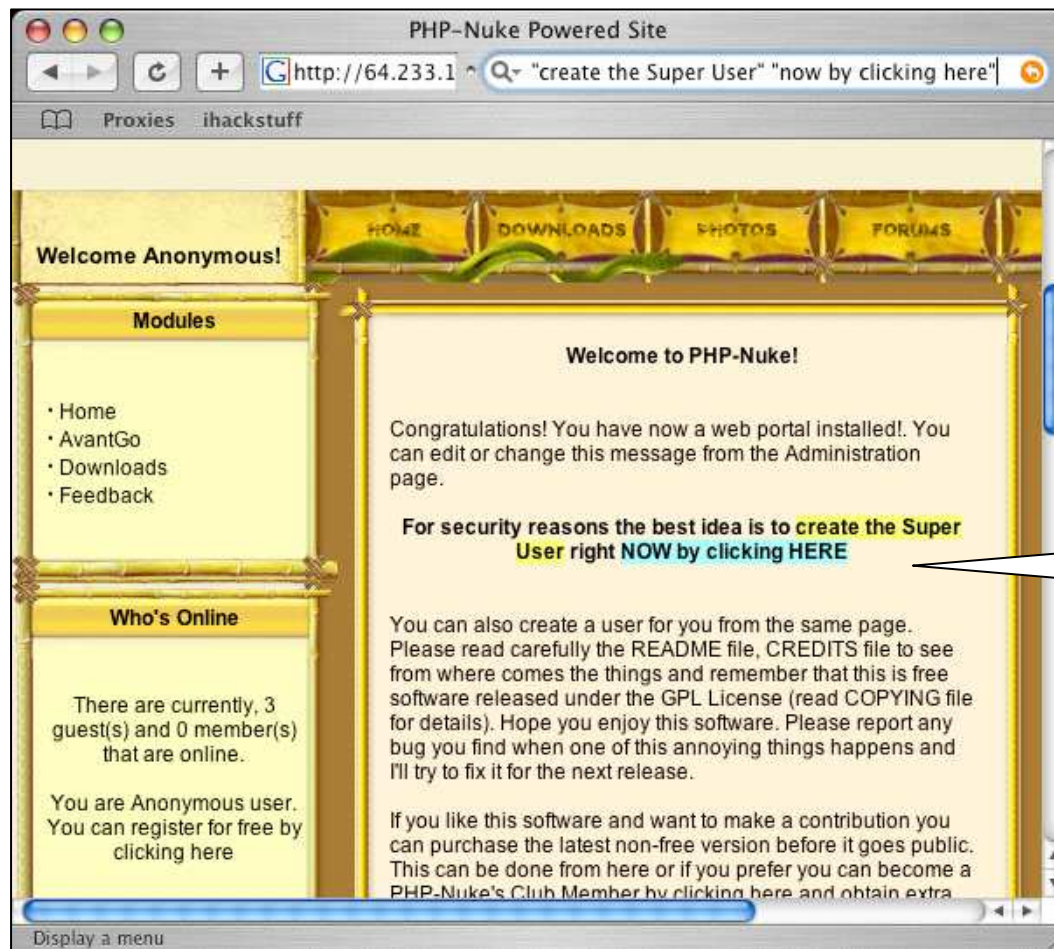


Too lazy to install  
PHP Nuke? Own  
someone else's site  
instead!

Thanks to  
arrested for  
this beauty!



## Open PHP Nuke... another way...



## Security Cameras

- Although many cameras are multi-purpose, certain brands tend to be used more for security work.



Thanks  
stonersavant!

# Security Cameras

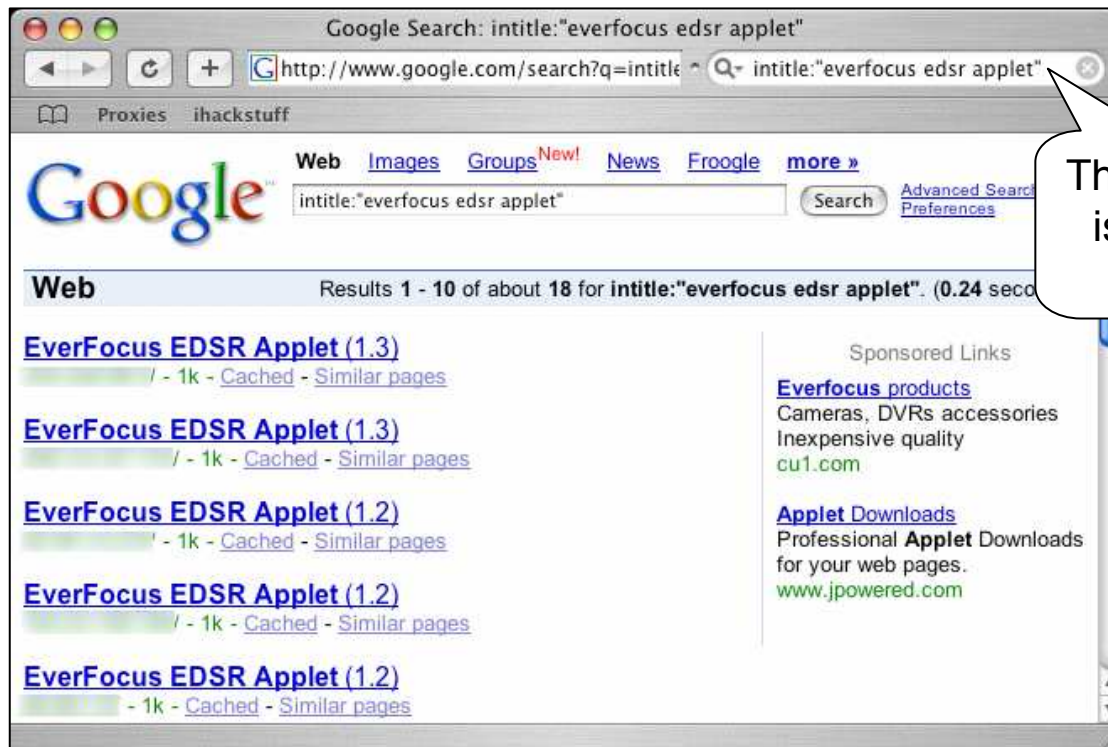


Not sure what "Woodie" is, but I'm not clicking it....

Thanks murfie!

## Time-lapse video recorders

- A staple of any decent security system, these camera control units have gotten high-tech.. And Googlable...



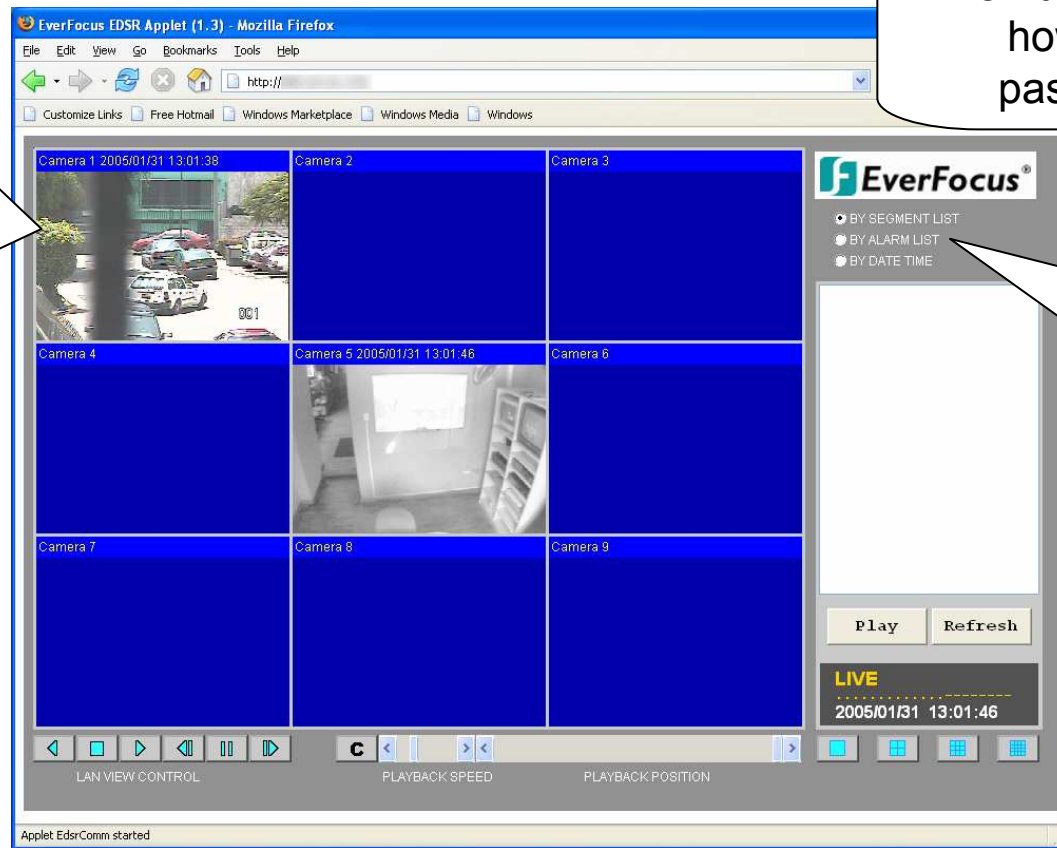
The search is no big deal...

Then there's the pesky login box...

A screenshot of a login box with a grey background. It features the title "Login" at the top. Below the title, there are two input fields: "User" and "Password". A "Submit" button is positioned below the password field. At the bottom of the box, the text "Best View Quality: IE5, 1024x768" is displayed.

# Time lapse video recorders

...multiple live security camera views...



Even doofus hackers know how to use default passwords to get...

...and historical records of recorded video feeds

Thanks to stonersavant for this beauty!

# UPS Monitors

Getting personal with Power System monitors...

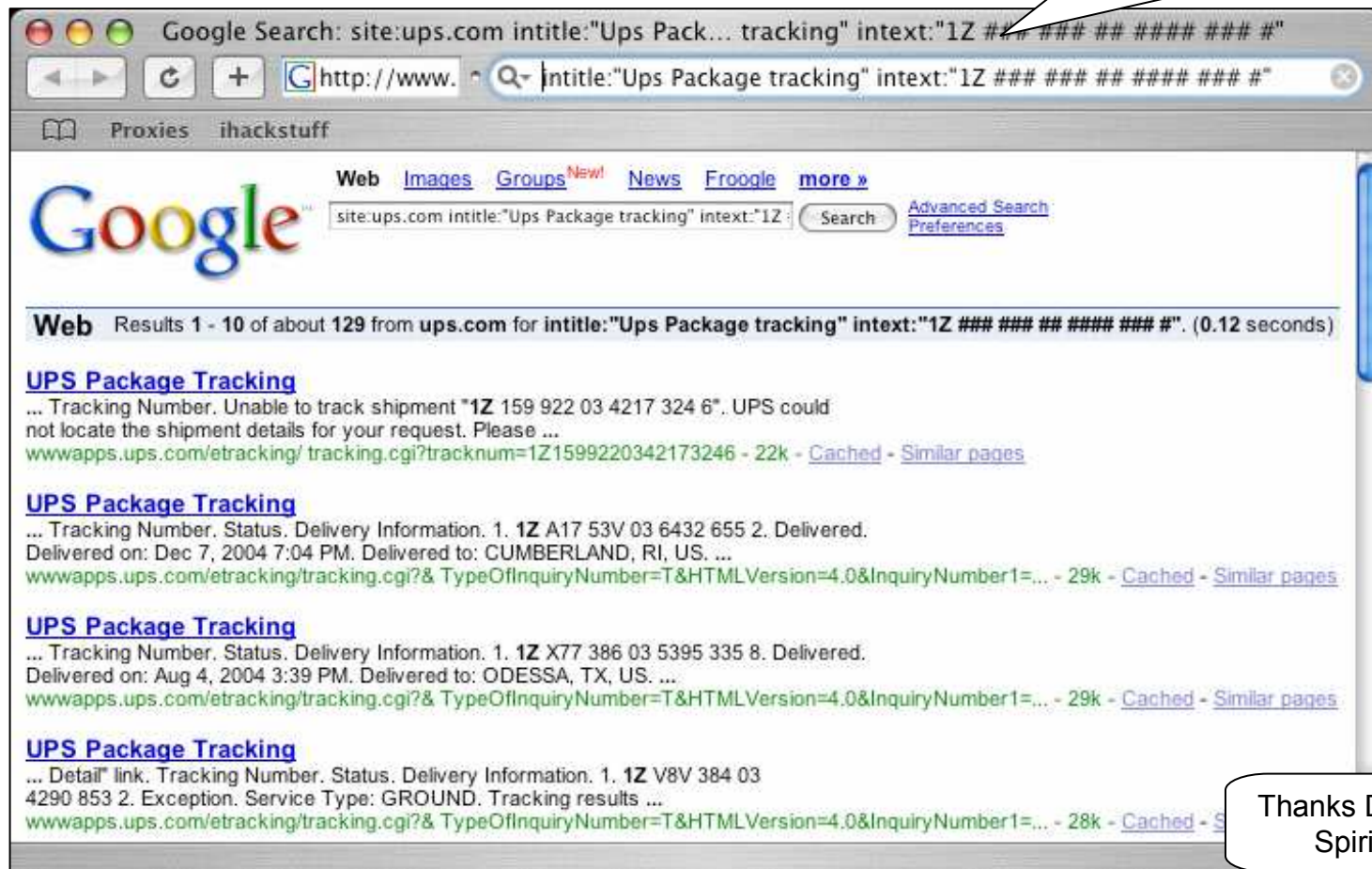
The screenshot shows a web browser window with the following content:

- Browser title: Tue Feb 01 23:37:19 WEST 2005 on tibs:3551
- Search bar: intitle:"Multimon UPS status page"
- Page title: ihackstuff
- Page content: Tue Feb 01 23:37:19 WEST 2005
- Monitoring: Tibs  
UPS Model: SMART-UPS 1000  
UPS Name: UPS\_IDEN  
APCUPSD: Version 3.10.16  
Status: ONLINE
- Last UPS Self Test: NO  
Last Test Date: Not found
- Utility Voltage: 230.1 VAC  
Line Minimum: 227.5 VAC  
Line Maximum: 232.7 VAC  
Output Freq: 50.0 Hz
- UPS Temp: 32.8 °C
- Battery Capacity: 100.0 % (Bar chart: 100% green)
- Run Time Remaining: 112.0 mins (Bar chart: 112% green)
- UPS Load: 11.4 % (Bar chart: 11.4% green, 88.6% red)
- Most recent events:
  - Thu Nov 13 12:37:04 WEST 2003 apcupsd shutdown succeeded
  - Thu Nov 13 12:37:04 WEST 2003 apcupsd exiting, signal 2
  - Thu Nov 13 12:36:41 WEST 2003 apcupsd 3.10.7 (08 November 2003) cygwin startup succeeded
  - Mon Oct 27 09:00:31 WEST 2003 apcupsd 3.10.6 (10 October 2003) cygwin startup succeeded
  - Mon Oct 27 08:59:13 WEST 2003 apcupsd 3.10.6 (10 October 2003) cygwin startup succeeded

Thanks yeseins!

# UPS Monitors

Oh wait.. Wrong kind of UPS...this is package tracking hacking... =P



The screenshot shows a web browser window with a Google search for "intitle: 'Ups Package tracking' intext: '1Z ### ### ## #### ## #'". The search results are from ups.com and show several entries for "UPS Package Tracking" with tracking numbers and delivery information. A speech bubble points to the search query, and another bubble at the bottom right says "Thanks Digital Spirit!".

Google Search: site:ups.com intitle:"Ups Pack... tracking" intext:"1Z ### ### ## #### ## #'"

http://www. intitle:"Ups Package tracking" intext:"1Z ### ### ## #### ## #'"

Proxies ihackstuff

Google Web Images Groups <sup>New!</sup> News Froogle more »

site:ups.com intitle:"Ups Package tracking" intext:"1Z : Search Advanced Search Preferences

Web Results 1 - 10 of about 129 from ups.com for intitle:"Ups Package tracking" intext:"1Z ### ### ## #### ## #'". (0.12 seconds)

**UPS Package Tracking**  
... Tracking Number. Unable to track shipment "1Z 159 922 03 4217 324 6". UPS could not locate the shipment details for your request. Please ...  
[wwwapps.ups.com/etracking/tracking.cgi?tracknum=1Z1599220342173246](http://wwwapps.ups.com/etracking/tracking.cgi?tracknum=1Z1599220342173246) - 22k - [Cached](#) - [Similar pages](#)

**UPS Package Tracking**  
... Tracking Number. Status. Delivery Information. 1. 1Z A17 53V 03 6432 655 2. Delivered. Delivered on: Dec 7, 2004 7:04 PM. Delivered to: CUMBERLAND, RI, US. ...  
[wwwapps.ups.com/etracking/tracking.cgi?& TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...](http://wwwapps.ups.com/etracking/tracking.cgi?& TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...) - 29k - [Cached](#) - [Similar pages](#)

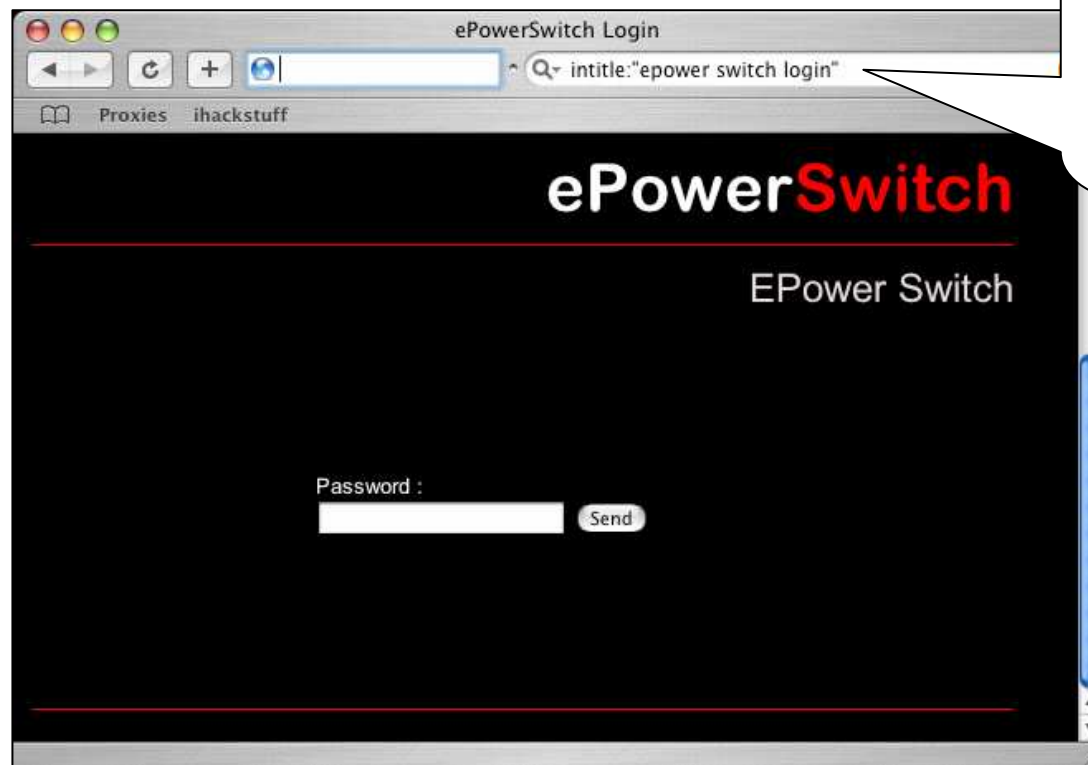
**UPS Package Tracking**  
... Tracking Number. Status. Delivery Information. 1. 1Z X77 386 03 5395 335 8. Delivered. Delivered on: Aug 4, 2004 3:39 PM. Delivered to: ODESSA, TX, US. ...  
[wwwapps.ups.com/etracking/tracking.cgi?& TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...](http://wwwapps.ups.com/etracking/tracking.cgi?& TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...) - 29k - [Cached](#) - [Similar pages](#)

**UPS Package Tracking**  
... Detail link. Tracking Number. Status. Delivery Information. 1. 1Z V8V 384 03 4290 853 2. Exception. Service Type: GROUND. Tracking results ...  
[wwwapps.ups.com/etracking/tracking.cgi?& TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...](http://wwwapps.ups.com/etracking/tracking.cgi?& TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=...) - 28k - [Cached](#) - [S](#)

Thanks Digital Spirit!

## Hacking POWER Systems!

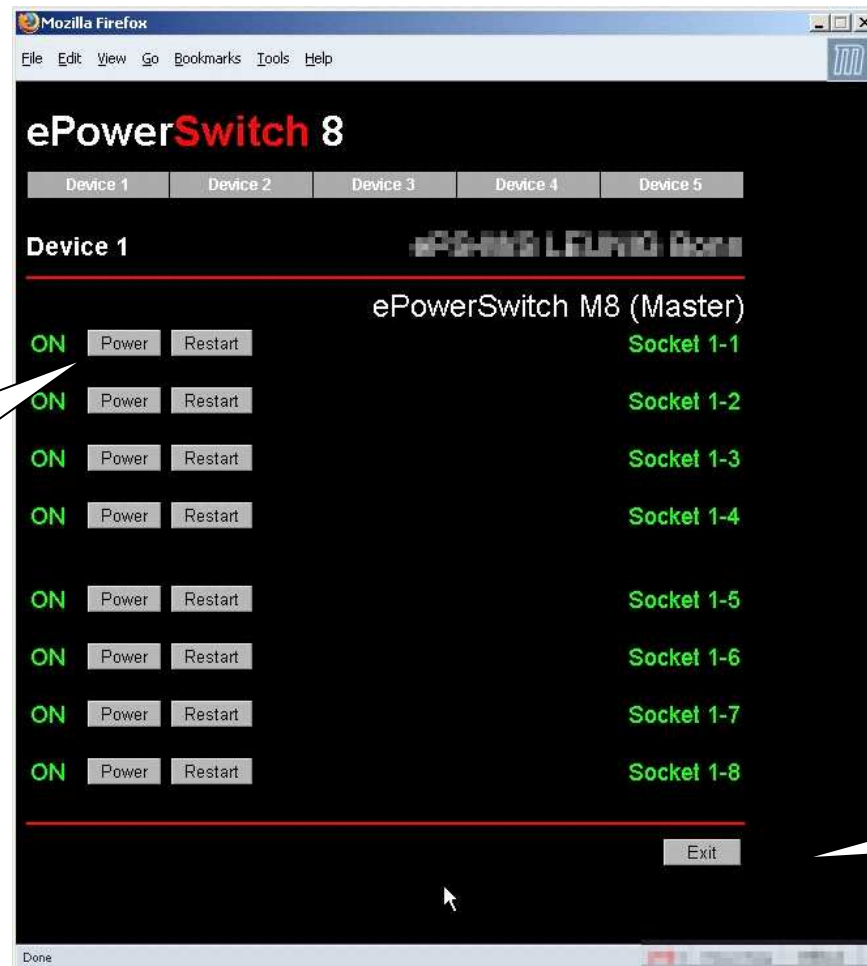
- Ain't technology grand? This product allows web management of power outlets!



Google search locates login page.  
What does any decent hacker do to a login page?



# Hacking Power Systems!



Who do you want to power off today?

Thanks to JimmyNeutron for this beauty!

---

## Google Phreaking

- Question... Which is easier to hack with a web browser?

A: Sipura SPA  
2000 IP  
Telephone

QuickTime™ and a  
TIFF (Uncompressed) decompressor  
are needed to see this picture.

B: Vintage  
1970's Rotary  
Phone

QuickTime™ and a  
TIFF (Uncompressed) decompressor  
are needed to see this picture.

# Sipura SPA IP Telephone

**Sipura SPA Configuration**

Info System SIP Regional Line 1 User 1 PSTN User Admin Login basic |

**System Information**

DHCP:	Enabled	Current IP:	172.16.0.111
Host Name:	spa3000_vp	Domain:	gateway.2wire.net
Current Netmask:	255.255.0.0	Current Gateway:	172.16.0.1
Primary DNS:	66.234.228.150		
Secondary DNS:	66.234.228.151 172.16.0.1		

**Product Information**

Product Name:	SPA-3000	Serial Number:	
Software Version:	2.0.10(GWc)	Hardware Version:	
MAC Address:	000E08CAFD2E	Client Address:	

**System Status**

Current Time:	9/27/2004 10:53:34	Elapsed Time:	
Broadcast Pkts Sent:	6	Broadcast Pkts Recv:	
Broadcast Pkts Recv:	9873	Broadcast Pkts Dropped:	
Broadcast Pkts Dropped:	0	RTP Packets Sent:	303959
RTP Packets Sent:	303959	RTP Packets Recv:	452249
RTP Packets Recv:	452249	SIP Messages Sent:	6300
SIP Messages Sent:	6300	SIP Messages Recv:	6310
SIP Messages Recv:	6310	External IP:	

How about  
Googling for the  
last number your  
friend dialed?

Or the last  
number that  
dialed them?

**Sipura SPA Configuration**

Proxies ihackstuff

**Line 1 Status**

Hook State:	On	Registration State:	Registered
Last Registration At:	9/27/2004 10:16:05	Next Registration In:	1321 s
Message Waiting:	No	Call Back Active:	No
Last Called Number:	*123	Last Caller Number:	4 80 451
Mapped SIP Port:		Call 2 State:	Idle
Call 1 State:	Idle	Call 2 Tone:	None
Call 1 Tone:	None	Call 2 Encoder:	
Call 1 Encoder:		Call 2 Decoder:	
Call 1 Decoder:		Call 2 FAX:	
Call 1 FAX:		Call 2 Type:	
Call 1 Type:		Call 2 Remote Hold:	
Call 1 Remote Hold:		Call 2 Callback:	
Call 1 Callback:		Call 2 Peer Name:	
Call 1 Peer Name:		Call 2 Peer Phone:	
Call 1 Peer Phone:		Call 2 Duration:	
Call 1 Duration:		Call 2 Packets Sent:	
Call 1 Packets Sent:			

Display a menu

Thanks  
stonersavant!!!

# Videoconferencing

TANDBERG: METROXPRESS AAR

intext:"Videoconference Management System" ext:htm

Proxies ihackstuff

**Who do you want to disconnect today?**

**Videoconference Management System on METROXPRESS AAR**

- ▶ [Call Management](#)
  - ▶ [Connect](#)
  - ▶ [Disconnect](#)
  - ▶ [Edit Directory](#)
  - ▶ [Call Status](#)
  - ▶ [MCU Services](#)
  - ▶ [MCU Status](#)
  - ▶ [Streaming](#)
  - ▶ [Snapshots](#)
  - ▶ [Text Chat](#)
- ▶ [System Configuration](#)

**Our Vision**

To provide innovative, high quality videoconferencing solutions that are reliable, easy to use and represent a significant value for our partners and customers.

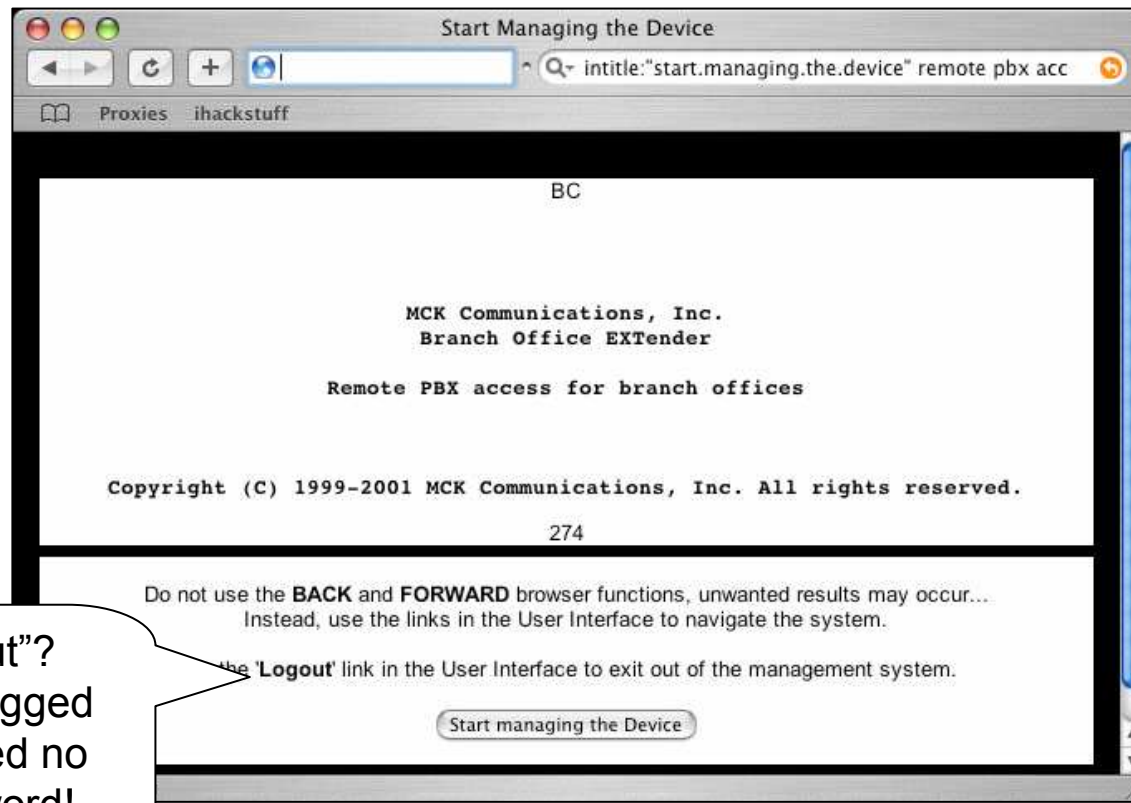
TANDBERG

reliability • ease of use • quality • value

Thanks  
yeseins!!!

## PBX Systems

- Web-based management interfaces open the door for a creative Google Hacker.



See the "logout"?  
We're already logged  
in! We don't need no  
steenkin password!

# PBX Systems

The screenshot shows a web browser window titled "Web-based Management User Interface" in Mozilla Firefox. The interface includes a navigation menu on the left with options like Configuration, Status, Utilities, System, File, Diagnostics, Upgrade, and Logout. The main content area displays a log of 79 entries, including system information, boot messages, and a copyright notice for MCK Communications, Inc. The log entries are as follows:

```
Jan 18 15:38:31: SYS INFO: No saved RUNTIME log
Jan 18 15:38:31: SYS INFO: Reset due to Power-Up circuit (POW)
Jan 18 15:38:31: SYS INFO: Reset due to Hard Reset signal RESETH (EXT)
----START OF PREVIOUSLY SAVED BOOT LOG BUFFER----
Jan 18 15:38:00: SYS DEBUG: FMM: found AM29F032B starting at 0x00C00000
Jan 18 15:38:00: BOOT      : Branch Office EXTender [remote, hw model 0, hw rev 7]
Jan 18 15:38:00: BOOT      : ROM Version 2.1r3 [Jan 23 2001, 14:55:00]
Jan 18 15:38:00: BOOT      : VxWorks version: 5.4
Jan 18 15:38:00: BOOT      : BSP version: 1.2/0
Jan 18 15:38:00: BOOT      : Boot type: COLD, NORMAL AUTOBOOT
Jan 18 15:38:00: BOOT      : Copyright (C) 1999-2001 MCK Communications, Inc. All rights reserved.
Jan 18 15:38:03: BOOT      : --> Loading runtime image from the flash file system
Jan 18 15:38:03: BOOT      : File: '/flash0/default.m6b'
Jan 18 15:38:27: BOOT      : Runtime image PASSED checksum
messages copied from BOOT LOG cache
--END OF PREVIOUSLY SAVED BOOT LOG BUFFER----
```

No password required.  
Even a novice web surfer  
can become a "PBX  
hacker". =)

Thanks to  
stonersavant for this  
great find!

# Username, Passwords and Secret Stuff, oh my!

There's all sorts of stuff out there that people probably didn't mean to make public. Let's take a look at some examples...

# DCIM

Index of /DCIM/100\_FUJI

index.of.dcim

Proxies ihackstuff

## Index of /DCIM/100\_FUJI

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>	09-Jan-2005 16:53	-	
<a href="#">DSCF0016.JPG</a>	15-Jan-2005 02:30	618k	
<a href="#">DSCF0017-640.480.jpg</a>	15-Jan-2005 02:30	82k	
<a href="#">DSCF0017.JPG</a>	15-Jan-2005 02:30	628k	
<a href="#">DSCF0018-640.480.jpg</a>	15-Jan-2005 02:30	81k	
<a href="#">DSCF0018.JPG</a>	15-Jan-2005 02:30	627k	
<a href="#">DSCF0019-640.480.jpg</a>	15-Jan-2005 02:30	116k	
<a href="#">DSCF0019.JPG</a>	15-Jan-2005 02:30	619k	
<a href="#">DSCF0020.JPG</a>	15-Jan-2005 02:30	613k	

What's DCIM?

Digital camera image dumps....

Thanks xlockex!



# MSN Contact Lists

MSN contact lists allow an attacker to get 'personal'

```
http://64.233.187.104/search?q...t+filetype:ctt+%22msn%22&hl=en
filetype:ctt "msn"
Proxies ihackstuff
<?xml version="1.0"?>
<messenger>
  <service name=".NET Messenger Service">
    <contactlist>
      <contact>ca ly ^ofson@hotmail.com</contact>
      <contact>vi ey ^d@cnw.com</contact>
      <contact>su sh ^egirl1252@hotmail.com</contact>
      <contact>bu be ^icker_7@hotmail.com</contact>
      <contact>jk ^o ^@hotmail.com</contact>
      <contact>ks ^no ^@hotmail.com</contact>
      <contact>jo ^u ^onuteaux@hotmail.com</contact>
      <contact>st ^ve ^rmala@hotmail.com</contact>
      <contact>bi ^je ^bitch_4@hotmail.com</contact>
      <contact>rh ^vi ^@msn.com</contact>
      <contact>bo ^ko ^otmail.com</contact>
      <contact>kw ^k ^nan@hotmail.com</contact>
      <contact>pu ^p ^yaz4u@hotmail.com</contact>
      <contact>ks ^no ^@hotmail.com</contact>
      <contact>rm ^lm ^27@hotmail.com</contact>
      <contact>aw ^it ^gsecond@hotmail.com</contact>
      <contact>rs ^n9 ^hotmail.com</contact>
      <contact>me ^od ^121@hotmail.com</contact>
      <contact>ol ^vi ^@hotmail.com</contact>
      <contact>wi ^ir ^dyranch@hotmail.com</contact>
      <contact>to ^b ^@olypen.com</contact>
      <contact>ty ^er ^_dog@hotmail.com</contact>
      <contact>re ^o ^pen.com</contact>
      <contact>ga ^da ^551@hotmail.com</contact>
      <contact>je ^nd ^020@aol.com</contact>
      <contact>ab ^16 ^@hotmail.com</contact>
```

Thanks to harry-aac!

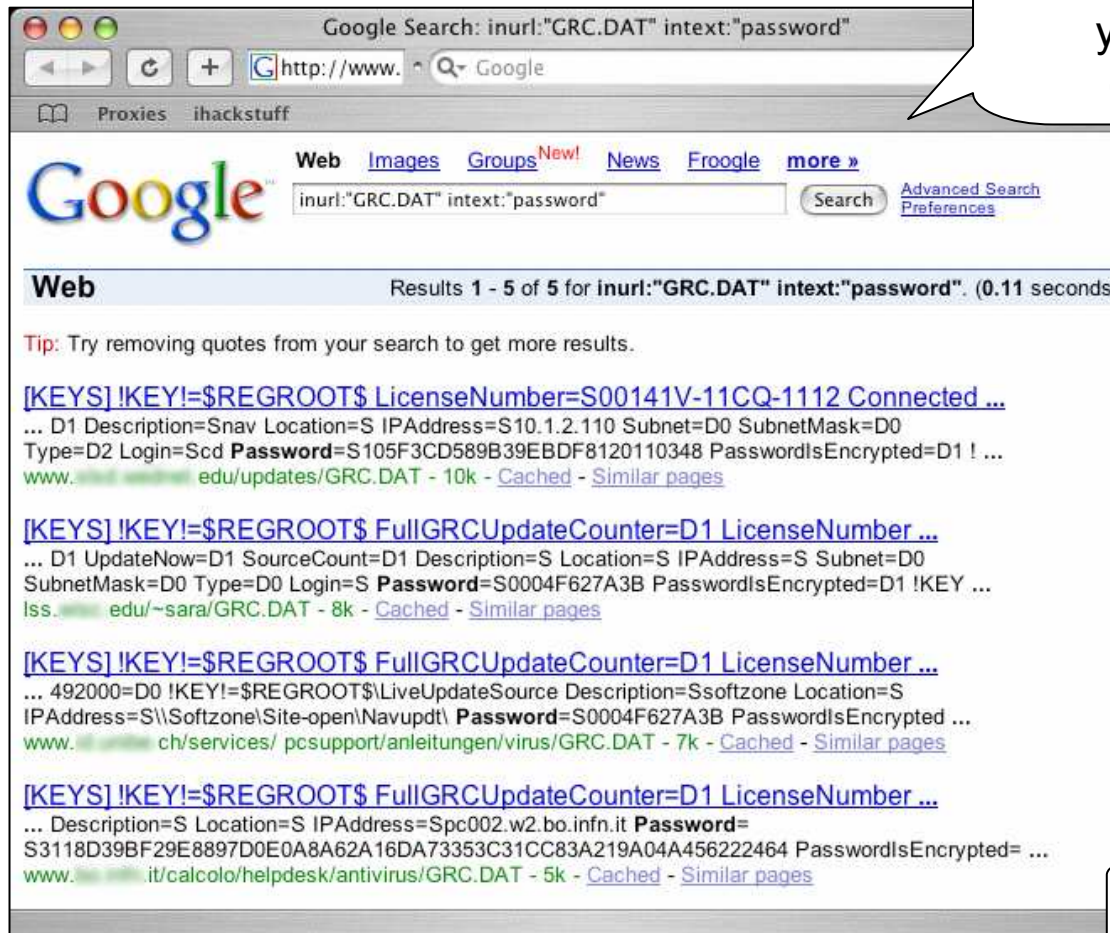
## Old School! Finger...

```
[timc@tornado.cs.wisc.edu]
Login name: timc      (messages off)   In real life: Tim Czerwonka
Directory: /u/t/i/timc      Shell: /bin/ksh
On since Jan 31 08:27:33 on :0
On since Jan 31 08:34:31 on pts/1 from cookie.cs.wisc.edu
    3 days 4 hours Idle Time
On since Jan 31 15:26:09 on pts/3 from :0.0
    1 hour 22 minutes Idle Time
On since Jan 31 15:28:16 on pts/4 from :0.0
    5 hours 8 minutes Idle Time
On since Jan 31 15:30:00 on pts/5 from :0.0
    1 day 0 hours Idle Time
On since Jan 31 15:43:54 on pts/7 from :0.0
    3 hours 6 minutes Idle Time
On since Jan 31 15:57:18 on pts/8 from :0.0
    1 day 5 hours Idle Time
On since Feb  2 13:58:15 on pts/10 from orange.cs.wisc.edu
    1 day 0 hours Idle Time
On since Feb  2 13:58:15 on pts/9 from orange.cs.wisc.edu
    22 hours Idle Time
On since Feb  2 13:58:15 on pts/2 from orange.cs.wisc.edu
    37 minutes Idle Time
On since Feb  2 16:04:51 on pts/11 from orange.cs.wisc.edu
    38 minutes Idle Time
On since Jan 31 15:26:09 on X0
    ?? Idle Time
Project: <A HREF="http://www.cs.wisc.edu/~timc">
Plan:
```

Google  
Hacking circa  
1980!!?!?

Thanks to  
Jimmy Neutron!

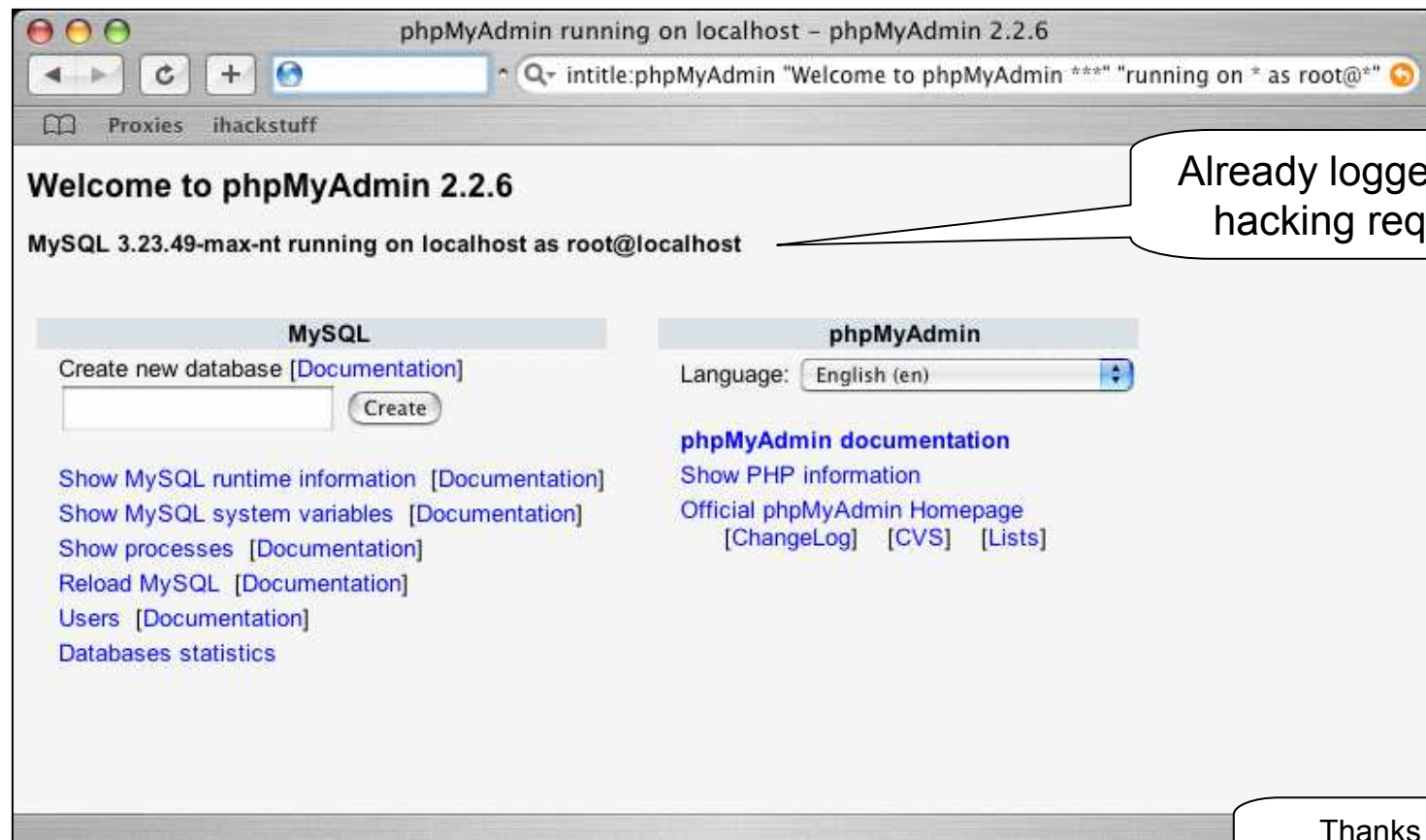
# Norton AntiVirus Corporate Passwords



Encrypted, but yummy (and crackable)!

Thanks MILKMAN!

# Open SQL servers



Already logged in, no hacking required!

Thanks Quadster!

# ServU FTP Passwords

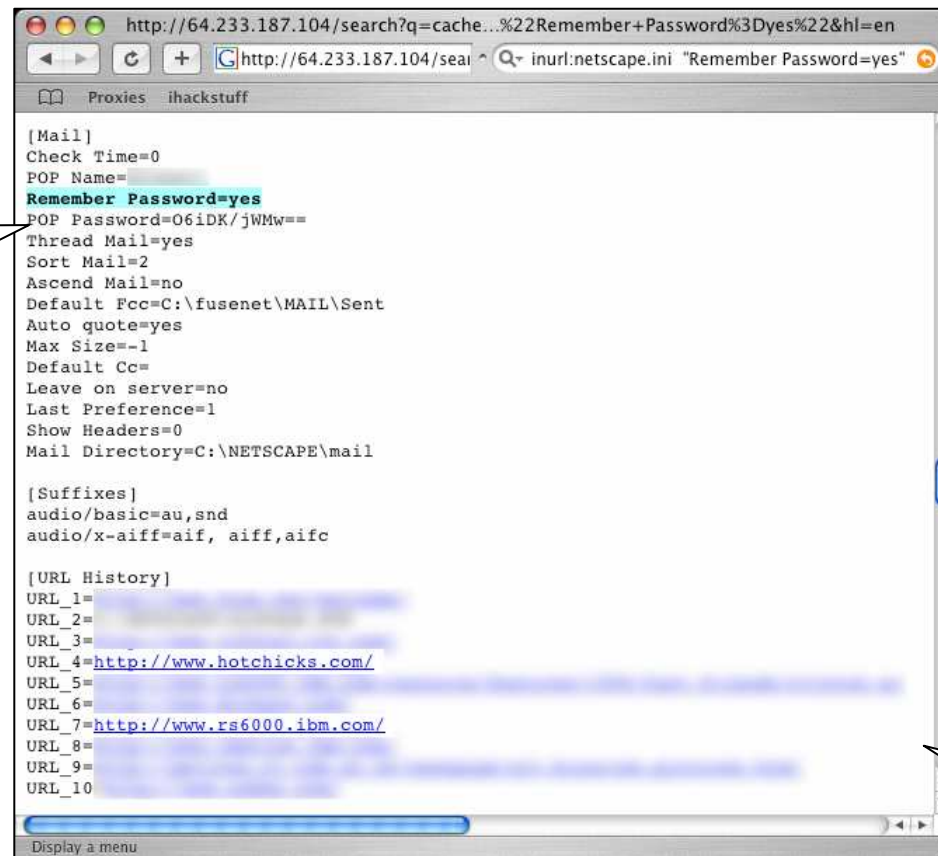
ServU FTP Daemon passwords, super encrypto! =P



Thanks to vs1400 for this one!

# Netscape History Files

Oops.. POP  
email  
passwords!



```
http://64.233.187.104/search?q=cache...%22Remember+Password%3Dyes%22&hl=en
http://64.233.187.104/seal inurl:netscape.ini "Remember Password=yes"
Proxies ihackstuff

[Mail]
Check Time=0
POP Name=
Remember Password=yes
POP Password=06iDK/jWMw==
Thread Mail=yes
Sort Mail=2
Ascend Mail=no
Default Fcc=C:\fusenet\MAIL\Sent
Auto quote=yes
Max Size=-1
Default Cc=
Leave on server=no
Last Preference=1
Show Headers=0
Mail Directory=C:\NETSCAPE\mail

[Suffixes]
audio/basic=au,snd
audio/x-aiff=aif, aiff,aifc

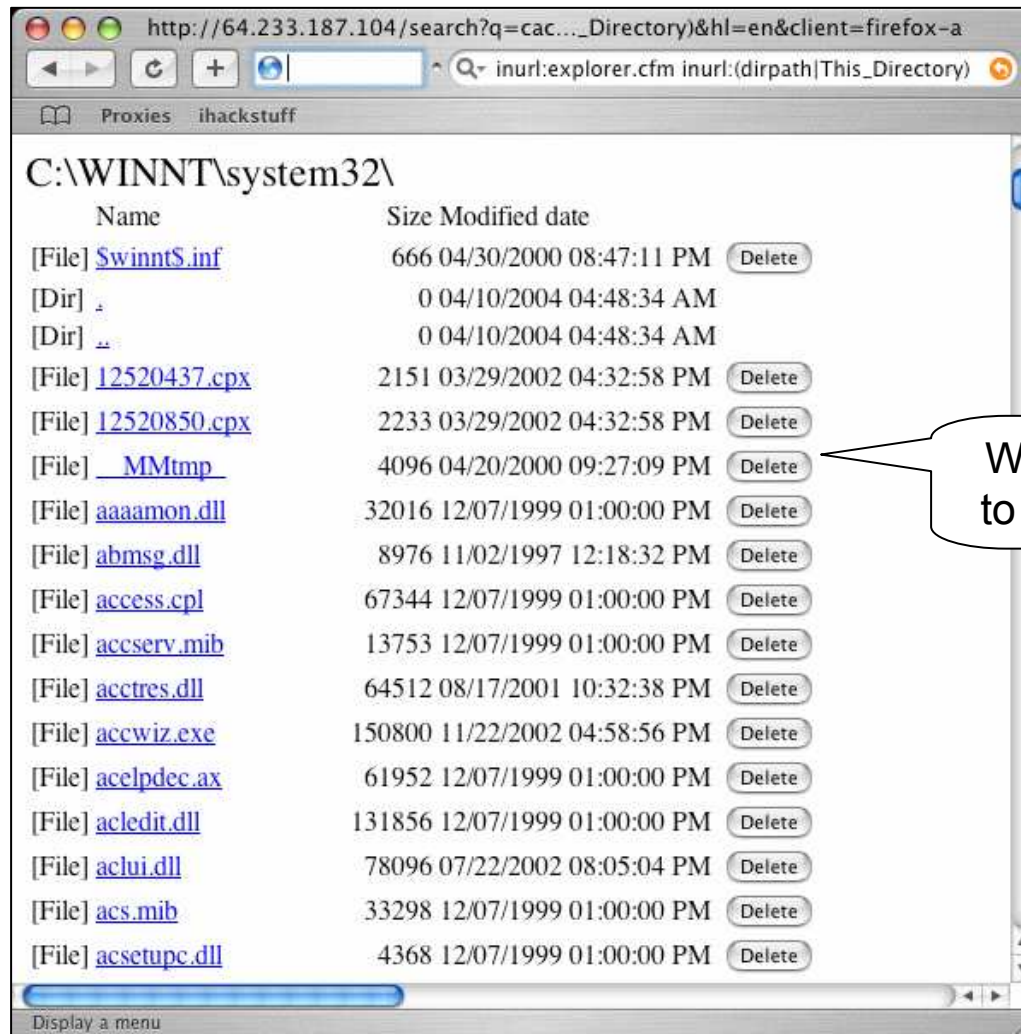
[URL History]
URL_1=
URL_2=
URL_3=
URL_4=http://www.hotchicks.com/
URL_5=
URL_6=
URL_7=http://www.rs6000.ibm.com/
URL_8=
URL_9=
URL_10=

Display a menu
```

Thanks to  
digital.revolution  
for this one!



# Explorer. EXPLORER!?!?!



What do you want to delete today???

Thanks JimmyNeutron!



# More Explorers?!?!

The screenshot shows a web browser window displaying the phpRemoteView interface. The address bar shows the URL: `C:/Program Files/Ensim/Sitedata/hackersg/Inetpub/wwwroot/`. The search bar contains the query: `intitle:"phpremoteview" filetype:php "Name, Size, Type, Modify"`. The main content area displays a file explorer view of the directory `C:/Program Files/Ensim/Sitedata/hackersg/Inetpub/wwwroot/`. The file list is as follows:

Name	Size	Type	Modify	Owner/Group	Perms
vti_cnf		DIR	18/02/04 20:40	0/0	0
vti_script		DIR	18/02/04 20:40	0/0	0
taam		DIR	29/09/04 03:42	0/0	0
tool		DIR	22/09/04 20:54	0/0	0
util		DIR	15/11/04 08:55	0/0	0
xxx		DIR	29/09/04 01:08	0/0	0
2p0p0PF4.zip	1 427 105		11/09/04 23:02	0/0	0
graphcount.php	3 854		29/09/04 02:58	0/0	0
test.php	90 895		28/09/04 22:06	0/0	0
Z_nakeR2.zip	91 425		11/09/04 23:02	0/0	0

At the bottom of the interface, there are navigation links: `Setup | PHP eval | phpinfo() | Shell | Char map | Language: English/Russian`. Below these links is the copyright information: `phpRemoteView © Dmitry Borodin (version 2003-04-22)` and a link to the free download: `http://php.spb.ru/remview/`.

Why hack when you can... click? =)

Thanks MacUK!

## More Explorers?!?!

Directory Listing

intitle:"Directory Listing" "tree view"

Proxies ihackstuff

Add To Favorites Back Refresh View Close Toolbar Change view to: Tree Detailed

sigh...

Filename	Size	Filetype	Modified Date	Modified Time
folder pashko		Folder	2/2/2005	9:52:39 39
folder year2000		Folder	7/16/2004	5:31:56 56
folder year2001		Folder	7/16/2004	5:31:42 42
folder year2002		Folder	7/17/2004	6:04:48 48
folder year2003		Folder	7/17/2004	6:06:14 14
folder year2004		Folder	1/5/2005	12:21:25 25
folder year2005		Folder	2/2/2005	8:15:58 58

Thanks JimmyNeutron!

## Sensitive Government Documents

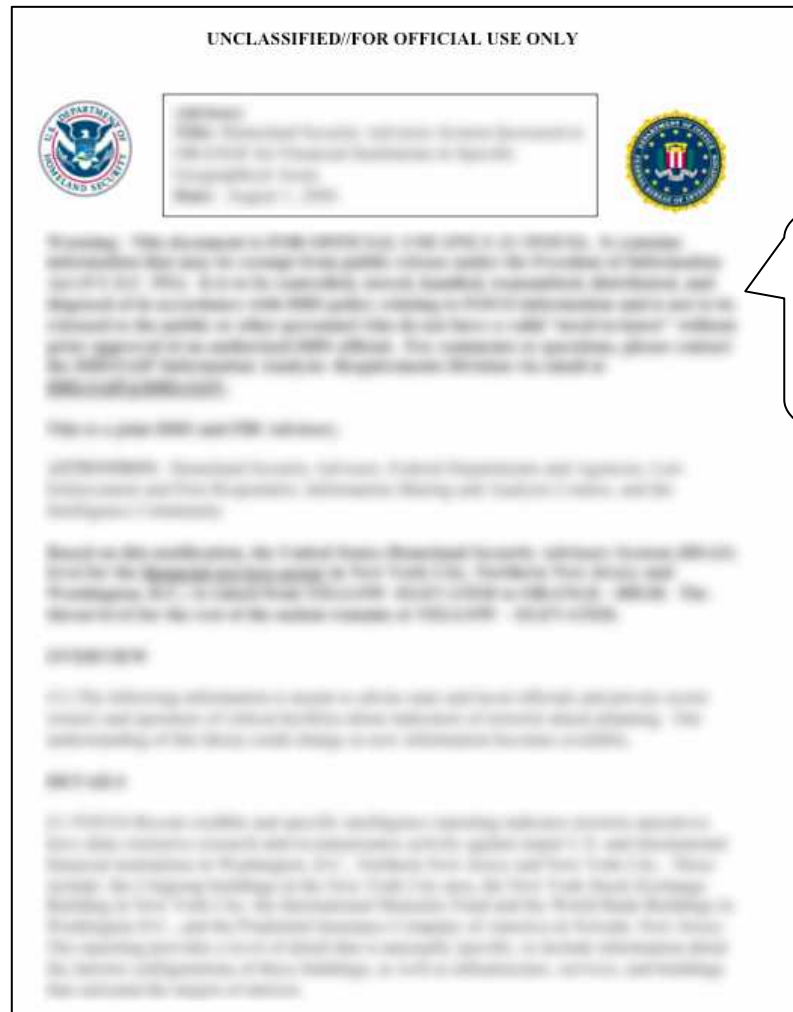
- Question: Are sensitive, non-public Government documents on the web?
- Answer: Yes.



Once these documents hit the Net, the media has a feeding frenzy, and people start copying and posting the docs...

---

# FOUO Documents



Although unclassified, this document was obviously not meant to be posted online.

# FOUO Documents



FOUO "Prevention Guides", like this 19 page beauty, can give bad guys horrible ideas.



---

## **Credit card info on the web?**

- How can this happen? Let's take a tour of some of the possibilities...





---

# Court Documents

Platinum The bank address is New York regarding  
account number :  
account #:  
account  
#:   
account #:  
account  
#:   
statement account #   
Bank #

## Court Documents

- How much detail is too much detail? =)

DATE	TIME	CREDIT CARD	ACCOUNT NUMBER	ACCOUNT NAME	AMOUNT
11/11/2011	10:00	Bank of America	1382 23	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0590 13	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0040 97	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0590 13	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0000 96	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0000 96	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0590 13	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0000 64	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0100 17	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0000 64	Bank of America	\$ 100.00
11/11/2011	10:00	Bank of America	0810 19	Bank of America	\$ 100.00

## Court Documents

- Of course, fraud accounts are closed pretty quickly, no?

ACCOUNT NUMBER	ACCOUNT NAME	AMOUNT
0513	Bank	\$1
13123	Bank	\$3
9097	Bank	\$7
7102	Bank	\$2
10096	Bank	\$3
2827	Bank	\$11
6391	Bank	\$2
9010	Bank	\$2

---

## A tale of a corn snake

- Is this for real? Either way it's pretty sad...



---

## Getting shell.. the easy way

- Now I've heard the term 'using your credit card online' but this is ridiculous!

### applying for a shell acct

- *To:* `hrlng_sak@hrlng.org`
- *Subject:* `applying for a shell acct`
- *From:* `'power passionat' <power1111@b.tnmail.com>`
- *Date:* `Sat, 09 Oct 1999 14:19:17 GMT`

hi there i am interested to buy a shell acct for my son.  
i m 2 busy because of some reasons. This is my only way to communicate  
with my son... so i want 2 buy a shell acct using my creditcard

the login name and password will be:  
login name: `mysonpac10`  
password: `q10q10`

Down here will be the details about me.

`name: Lorraine Biden`  
`1861 Woodlake View Road`  
Fortuna, CA, 95540

tel#: 755231  
Billing Information:  
Name on card: `Lorraine Biden`  
credit card #: `4178881160798162`  
expiration date: 01/00  
type of card: **visa**

Thank you and I hope to hear from you soon.

# Some people just don't get it....

## Questions & Offers Board

Our Questions & Offers board is the place to view questions and offers between other buyers and the seller. Please review this board before you [make an offer](#) or [ask the seller a question](#).

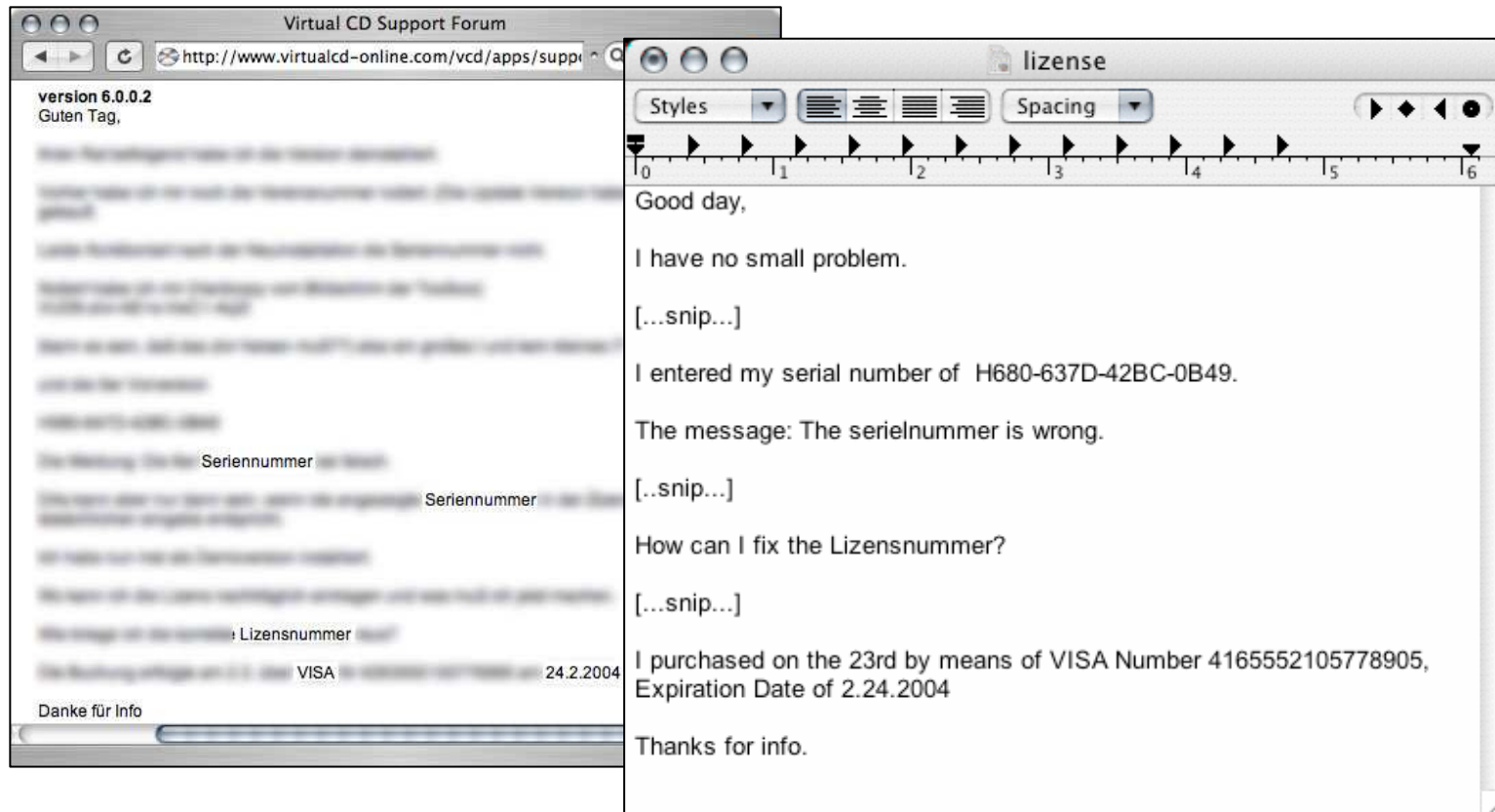
### Questions & Offers between [redacted] and the Seller

**Buyer** **Question:** hi there here is my credit card details below : name on card : [redacted] card number : [redacted] expire date : 10/05 CVV2 number : [redacted] card type : **Visa** name on card : [redacted] card number : [redacted] expire date : 02/05 cvv2 number : [redacted] card type : **Visa** please let me know if you finished charge my credit card. thanks Mar 23 14:10PDT

**Seller** **Answer:** Ok, I will attempt to charge your card first thing tomorrow when I am back at the office. Also, what address do you want this shipped to? Thanks Mar 23 16:27PDT

## Getting serialz... wha-hay!! and MORE!

- This is a very generous person. He's willing to give his software serial numbers and his credit card info to the whole world. Generosity like this could change the world.



---

## **Police Crime reports**

- Two questions:
- Are police reports public record?
- YES.
- Are they on the web?
- YES.
- Many states have begun placing campus police crime reports on the web. Students have a right to know what crimes take place on campus.



---

## Crime shouldn't pay...

- I'm thinking there should be a process for filtering these reports.



- A few might fall through the cracks....

Results 1 - 28 of 28









---

## Expense Reports...

- Somebody has to pay for all this stuff....

The image shows a blurry screenshot of what appears to be an expense report or a ledger. The text is mostly illegible due to low resolution, but some words and numbers are visible. At the top, there are some numbers: "381" and "577". Below that, the word "VISA" is visible. In the middle, there are several columns of numbers, possibly representing amounts. At the bottom, the words "DOG FOOD" and "VISA" are visible, along with the numbers "88" and "95".

Account	Amount	Description
381	577	VISA
88	95	VISA
		DOG FOOD

---

## Expense Reports

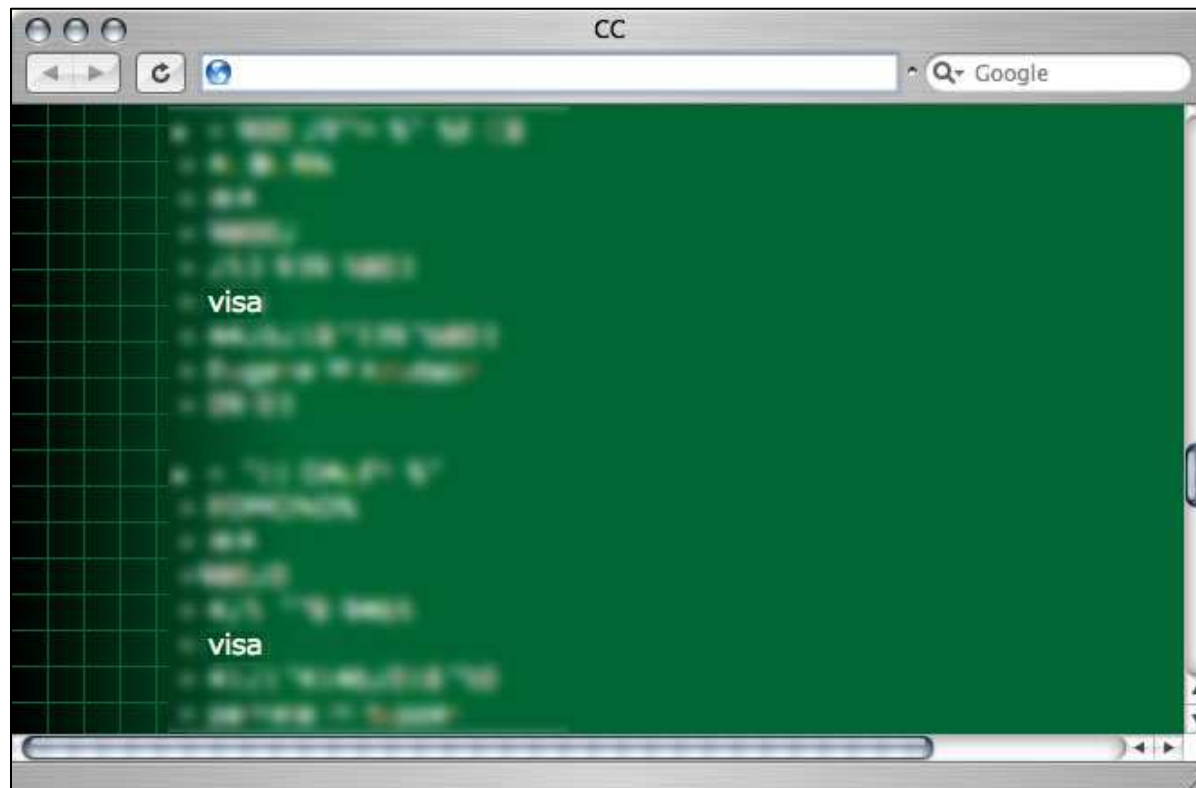
- That's one heck of a video series.... \$300+

VIDEO SERIES	9400!	39	3
VIDEO SERIES	9400!	39	3
VIDEO SERIES	9400!	39	3
VIDEO SERIES	9400!	39	3
VIDEO SERIES	9400!	39	3
		49	
		49	

---

## Credit cards... Google hacker's gold...

- The legend of finding credit cards online is true...
- I just get bored sifting through them all....





United States Payment Information. Pay by Credit Card? **Mastercard**  
Number: 0000 0000 0000 0000 Expire: 00/00 phone: 0000 0000 0000 0000

Subtotal \$0.00 Shipping and Handle \$0.00 \*total \$0.00 Order placed at Sun  
Aug 10 11:00 Eastern Standard Time \* a Release Of \*2000 All 3 United  
States Shipping Method: UPS Ground \* read general@release.com Eastern Standard  
\* \* \* \* \* Release Date: 08 \* \* \* \* \* Release City: 08 \* \* \* \* \* United States Payment  
Information. Pay by Credit Card?  
Expire: 00/00 phone: 000 000

Subtotal \$0.00 Shipping and Handle \$0.00 \*total \$0.00 Order placed at Sun  
Aug 10 11:00 Eastern Standard Time \* a Release Of \*2000 All 3 United  
States Shipping Method: UPS Ground \* read general@release.com Eastern Standard  
\* \* \* \* \* Release Date: 08 \* \* \* \* \* Release City: 08 \* \* \* \* \* United States Payment  
Information. Pay by Credit Card? **Visa** Number:  
0000 0000 phone: 0000 000

Subtotal \$0.00 Shipping and Handle \$0.00 \*total \$0.00 Order placed at Sun  
Aug 10 11:00 Eastern Standard Time \* a Release Of \*2000 All 3 United  
States Shipping Method: UPS Ground \* read general@release.com Eastern Standard  
\* \* \* \* \* Release Date: 08 \* \* \* \* \* Release City: 08 \* \* \* \* \* United States Payment  
Information. Pay by Credit  
Expire: 00/00 phone: 000 000

Subtotal \$0.00 Shipping and Handle \$0.00 \*total \$0.00 Order placed at Sun  
Aug 10 11:00 Eastern Standard Time \* a Release Of \*2000 All 3 United  
States Shipping Method: UPS Ground \* read general@release.com Eastern Standard  
\* \* \* \* \* Release Date: 08 \* \* \* \* \* Release City: 08 \* \* \* \* \* United States Payment  
Information. Pay by Credit Card? **Mastercard**  
Number: 0000 0000 phone: 0000 000

Subtotal \$0.00 Shipping and Handle \$0.00 \*total \$0.00 Order placed at Sun  
Aug 10 11:00 Eastern Standard Time \* a Release Of \*2000 All 3 United  
States Shipping Method: UPS Ground \* read general@release.com Eastern Standard  
\* \* \* \* \* Release Date: 08 \* \* \* \* \* Release City: 08 \* \* \* \* \* United States Payment  
Information. Pay by Credit Card? **Visa** Number:  
0000 0000 phone: 0000 000

Subtotal \$0.00 Shipping and Handle \$0.00 \*total \$0.00 Order placed at Sun  
Aug 10 11:00 Eastern Standard Time \* a Release Of \*2000 All 3 United  
States Shipping Method: UPS Ground \* read general@release.com Eastern Standard  
\* \* \* \* \* Release Date: 08 \* \* \* \* \* Release City: 08 \* \* \* \* \* United States Payment  
Information. Pay by Credit Card? **Visa** Number:  
0000 0000 phone: 0000 000

Subtotal \$0.00 Shipping and Handle \$0.00 \*total \$0.00 Order placed at Sun  
Aug 10 11:00 Eastern Standard Time \* a Release Of \*2000 All 3 United  
States Shipping Method: UPS Ground \* read general@release.com Eastern Standard  
\* \* \* \* \* Release Date: 08 \* \* \* \* \* Release City: 08 \* \* \* \* \* United States Payment  
Information. Pay by Credit Card? **Mastercard**  
Number: 0000 0000 phone: 0000 000

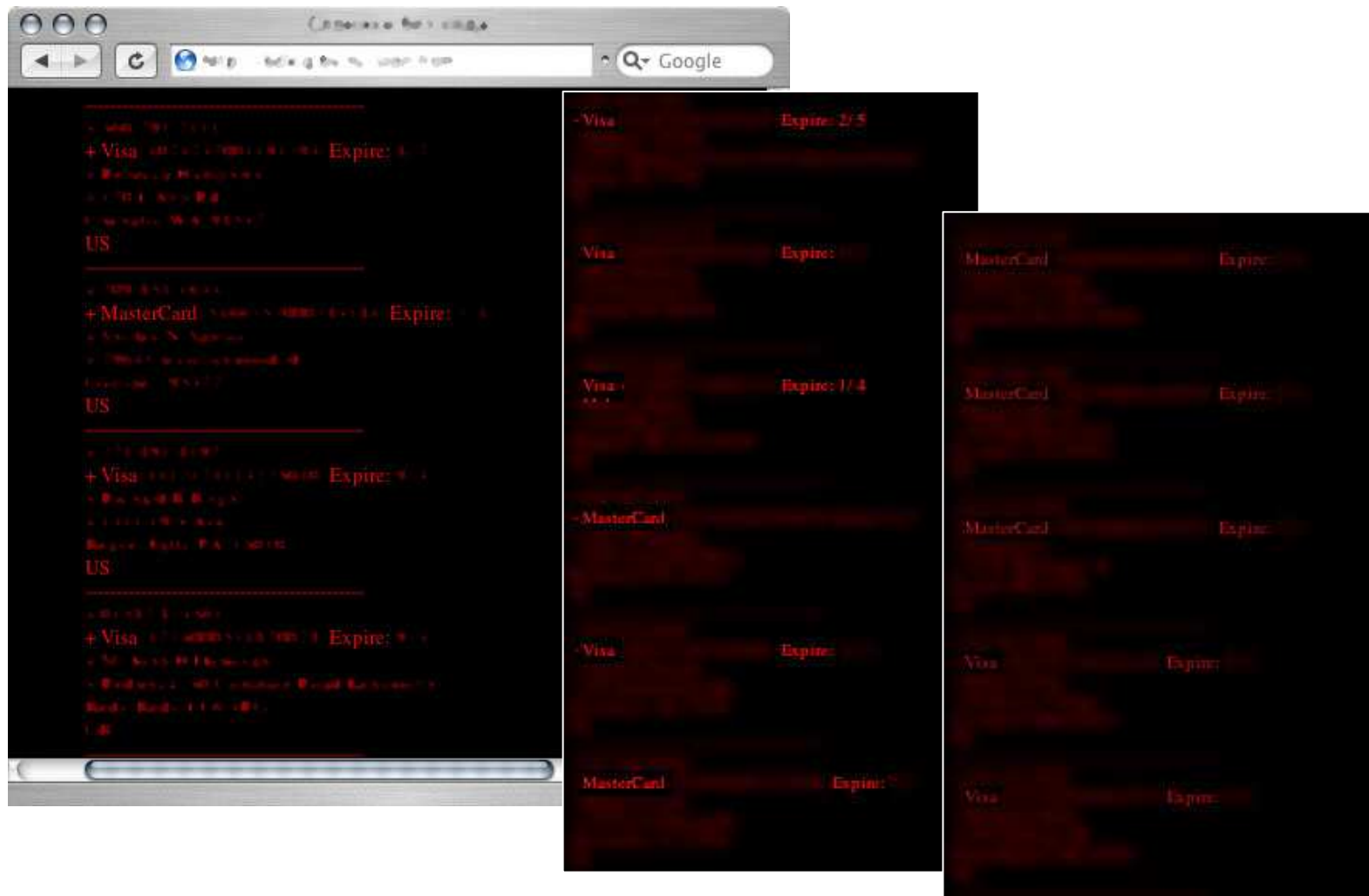
Subtotal \$0.00 Shipping and Handle \$0.00 \*total \$0.00 Order placed at Sun  
Aug 10 11:00 Eastern Standard Time \* a Release Of \*2000 All 3 United  
States Shipping Method: UPS Ground \* read general@release.com Eastern Standard  
\* \* \* \* \* Release Date: 08 \* \* \* \* \* Release City: 08 \* \* \* \* \* United States Payment  
Information. Pay by Credit Card? **Visa** Number:  
0000 0000 phone: 0000 000

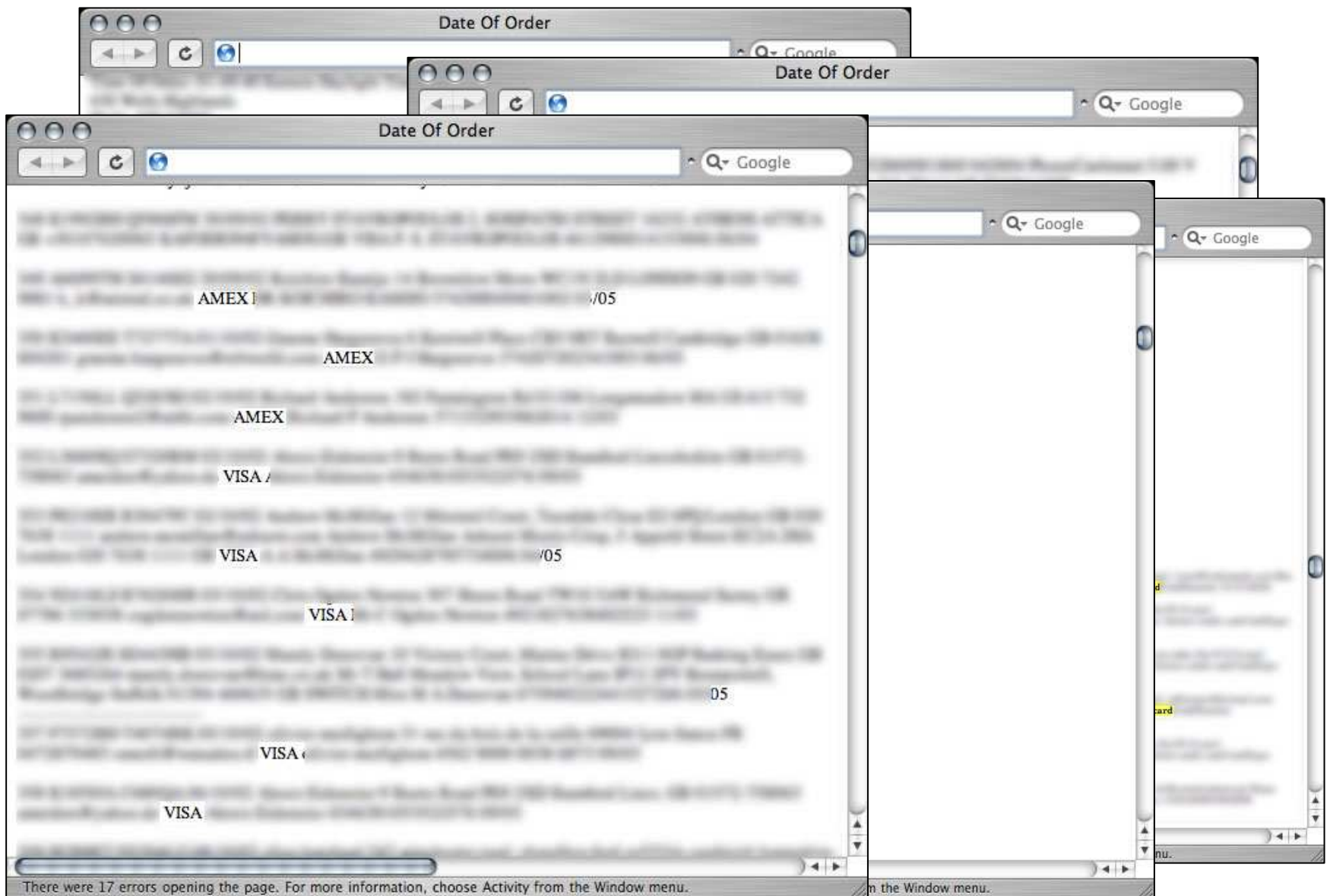
**Visa**  
**Visa**  
**Mastercard**  
**Visa**  
**Visa**  
**Visa**  
**Mastercard**  
**Visa**

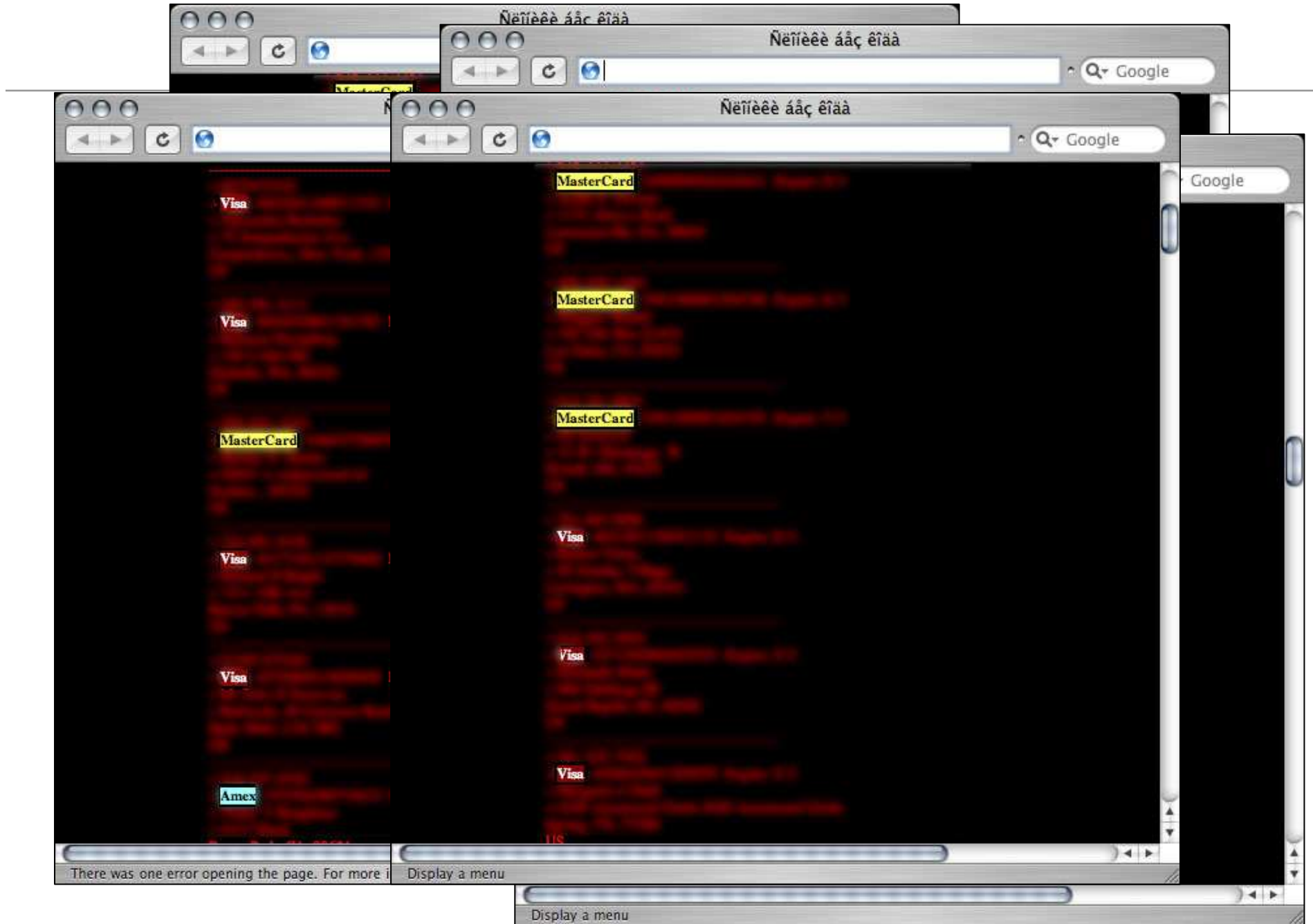
**Visa**  
**VISA**  
**Visa**  
Card Number: **Visa**  
**VISA**

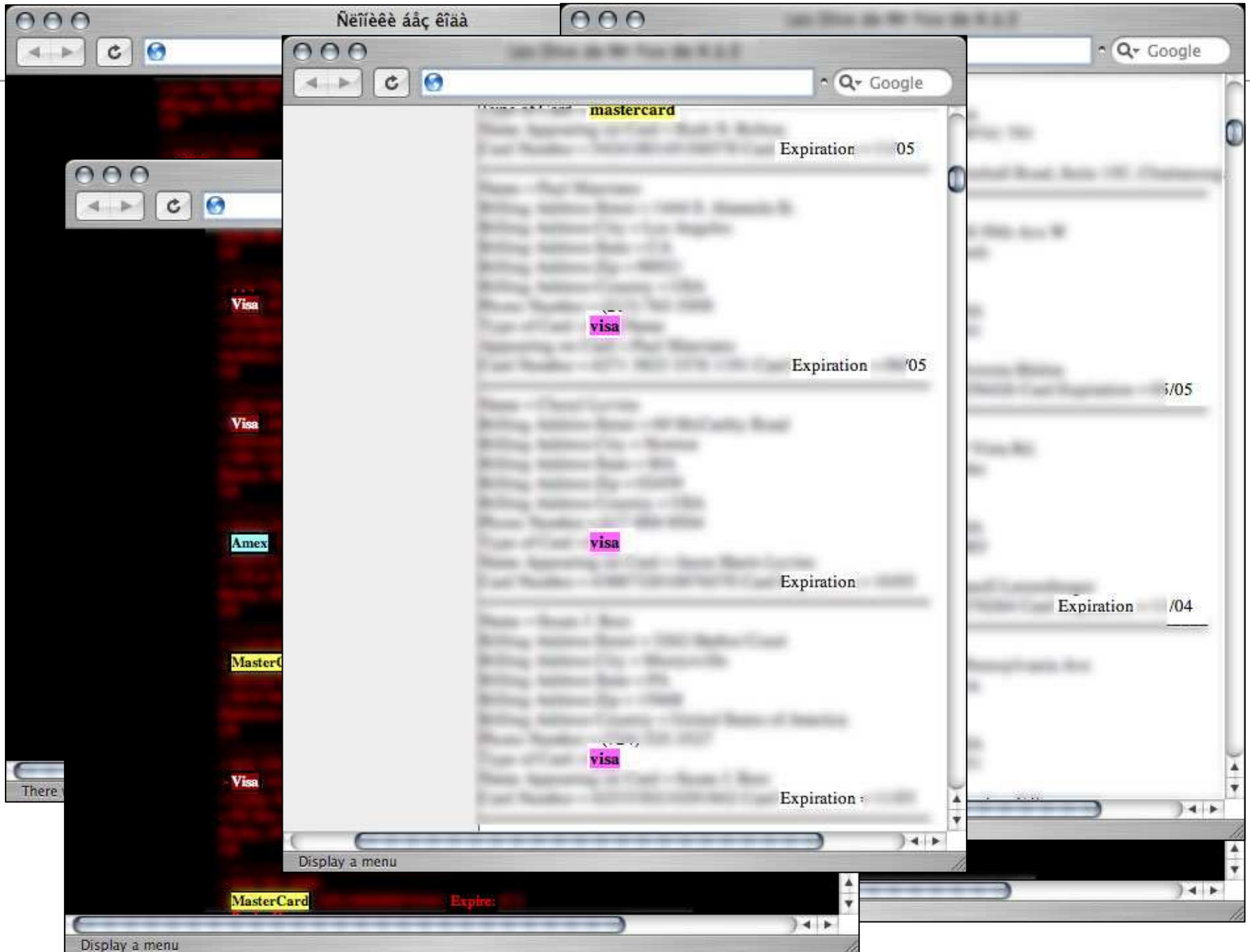
Card No	Visa	Expire
	<b>Visa</b>	expire: 00/00
	<b>Visa:</b>	Expire : 00/00
	<b>Visa:</b>	Expire : 00/00
	<b>Visa</b>	Expire : 00/00
	<b>visa:</b>	00/00

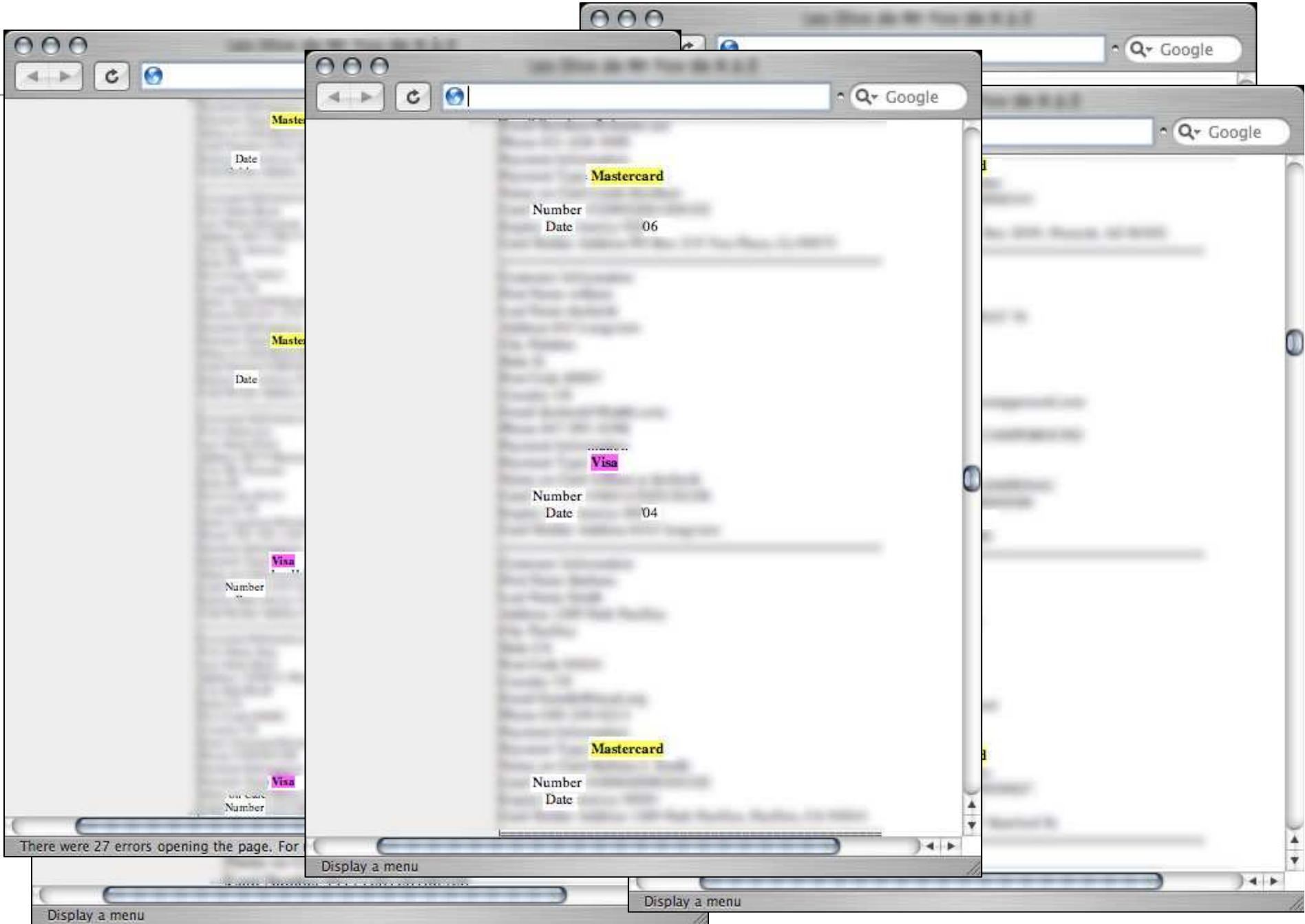
# Credit Listings











---

## Pick a card any card...

The image displays several overlapping rectangular boxes, each representing a different credit card brand. The boxes are arranged in a staggered, overlapping fashion from left to right and top to bottom. The brands visible are:

- VISA**: Located in the top-left box.
- MasterCard**: Located in the middle-left box.
- Discover**: Located in the middle-center box.
- American Express**: Located in the top-right, middle-center, and bottom-right boxes.

A speech bubble at the bottom right of the image contains the text: "...pick a card. We take 'em all!".

---

## Credit Validation

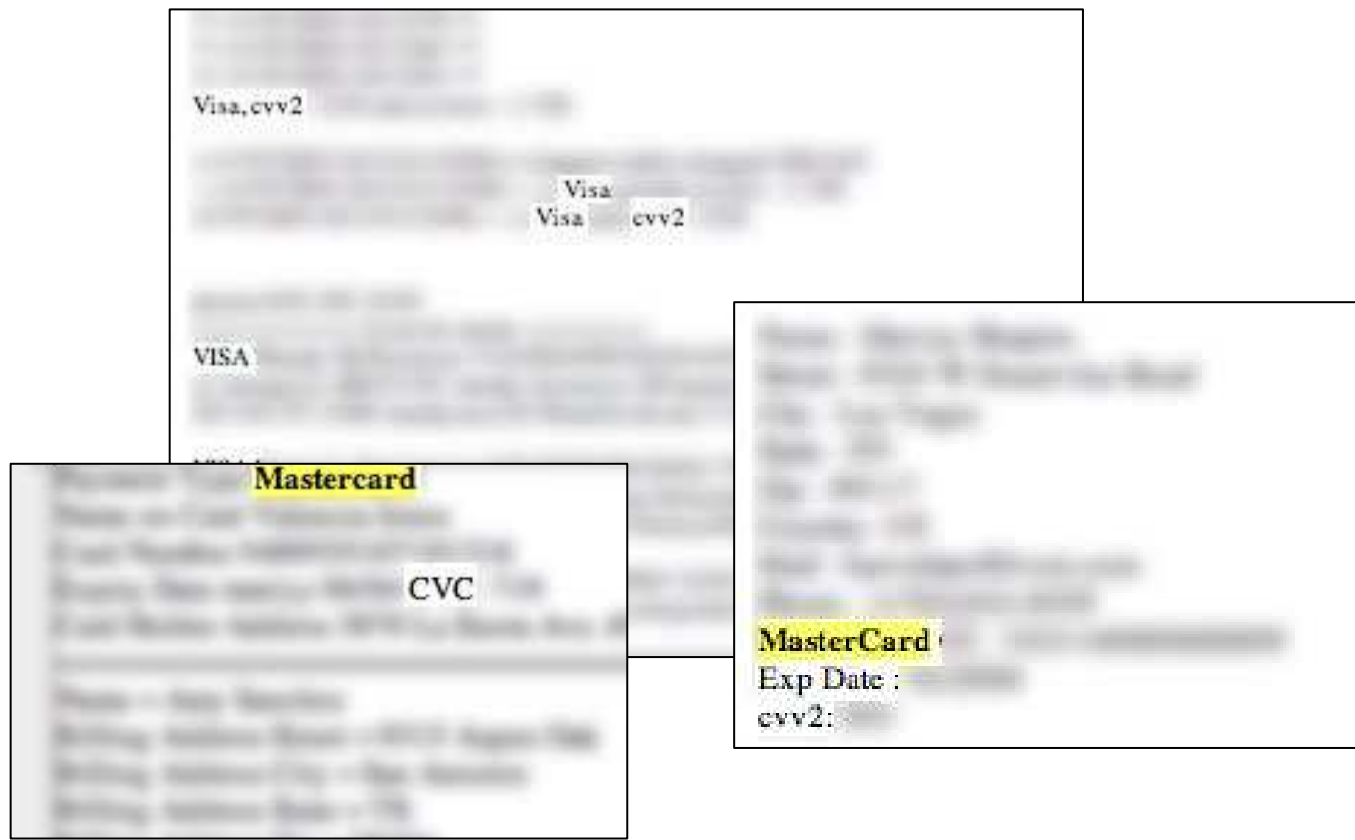
Question: What keeps someone from using a pilfered credit card number and expiration date to make an online purchase?

- Answer: That little code on the back of the card.
- Bonus question: What's that code called?
- Answer: A "CVV" code.



---

## Credit Card Numbers, Expiration Date and CVV numbers, oh my!



## That's not all....

- Credit cards are sooo 1990's =)

```
routing:
account:
accountn
ssn
paypal pass:
cvv
```

```
bank:
bank:
bank:
bank:
ssn :
paypal_passwd
paypal_passwd:
ebayid:
ebaypass:
```

```
* Total Shipping Weight: 6.00 lbs Subtotal: 25.00 Shipping/Handling: 7.00 Total: 32.00
Order placed at Sun Mar 25 14:42:36 2007 - Order Received Card Shop 84 - 1000 W 1st
St - Harrisburg, PA - 17102 United States Shipping Method: UPS Ground (Regular) - 6.00
lbs/36.00oz net July 2007 - 1523 W Southern Ave - Harrisburg, PA - 17102 United
States Payment Information Pay By: Check Bank name: Sovereign Check number: 000
Checking account: 0030607 *** Routing number: 23-17269 *
```

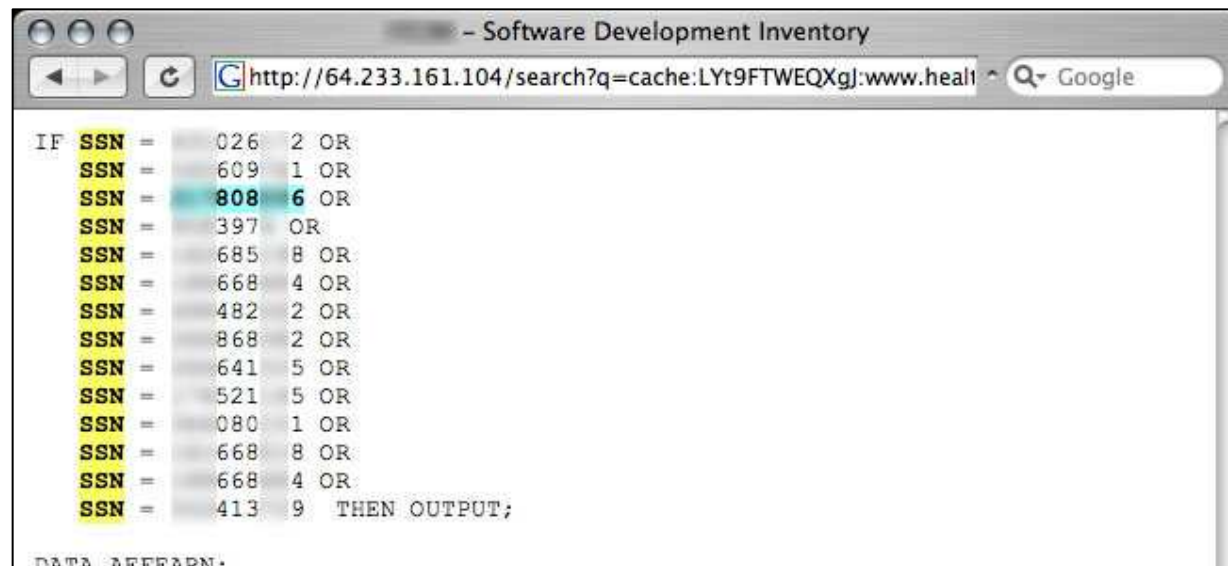
---

## Getting more personal

- Question: What's the one 9 digit number you shouldn't give to ANYONE?
  - Answer: SSN
  - Bonus question: What can you do with someone's SSN?
  - Answer: Steal their identity.
- 
- How do SSN's get on the web? Let's take a look at some possibilities.

## SSN's in source code

- Well, they could be hardcoded into a healthcare system... and uhmmm... put on the web...



The screenshot shows a web browser window titled "Software Development Inventory". The address bar contains the URL `http://64.233.161.104/search?q=cache:LYt9FTWEQXgj:www.health`. The page content displays a list of Social Security Numbers (SSNs) in a structured format. The text is as follows:

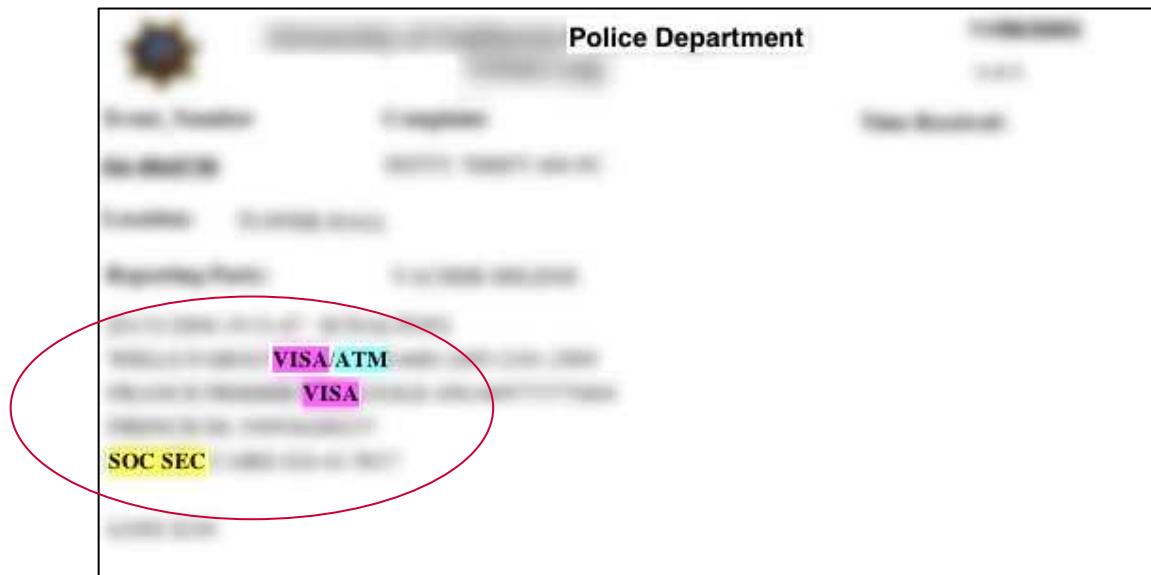
```
IF SSN = 026 2 OR
   SSN = 609 1 OR
   SSN = 808 6 OR
   SSN = 397 OR
   SSN = 685 8 OR
   SSN = 668 4 OR
   SSN = 482 2 OR
   SSN = 868 2 OR
   SSN = 641 5 OR
   SSN = 521 5 OR
   SSN = 080 1 OR
   SSN = 668 8 OR
   SSN = 668 4 OR
   SSN = 413 9 THEN OUTPUT;
```

At the bottom of the page, the text "DATA AFFEARN:" is visible.

---

## Crime shouldn't pay...

- Remember the police reports? Since the credit card accounts in them are no good, maybe we should troll them some more....



---

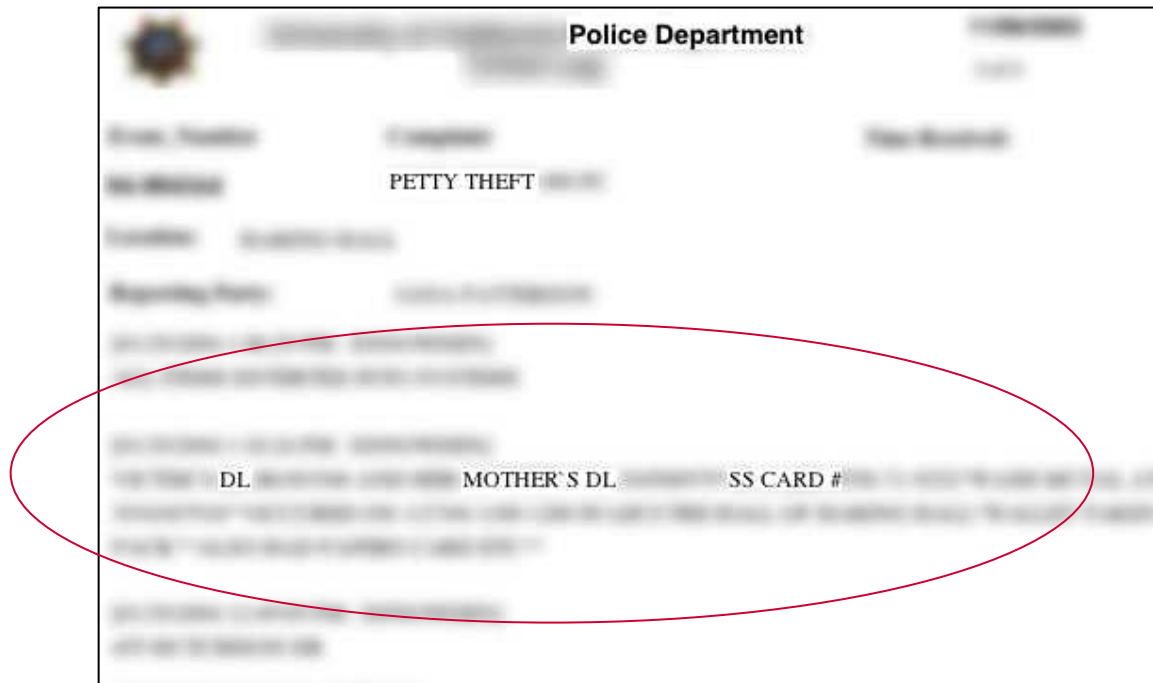
## SSN's - Police Reports

The image shows a blurred police report form. At the top, the text "Police Department" is visible. Below this, there are several lines of text, including "Officer Name", "Case Number", and "Date". A red circle highlights a section of the form containing the text "SOC SEC #". To the right of this section, the word "VISA" is printed in red. The rest of the form is mostly illegible due to blurring.

---

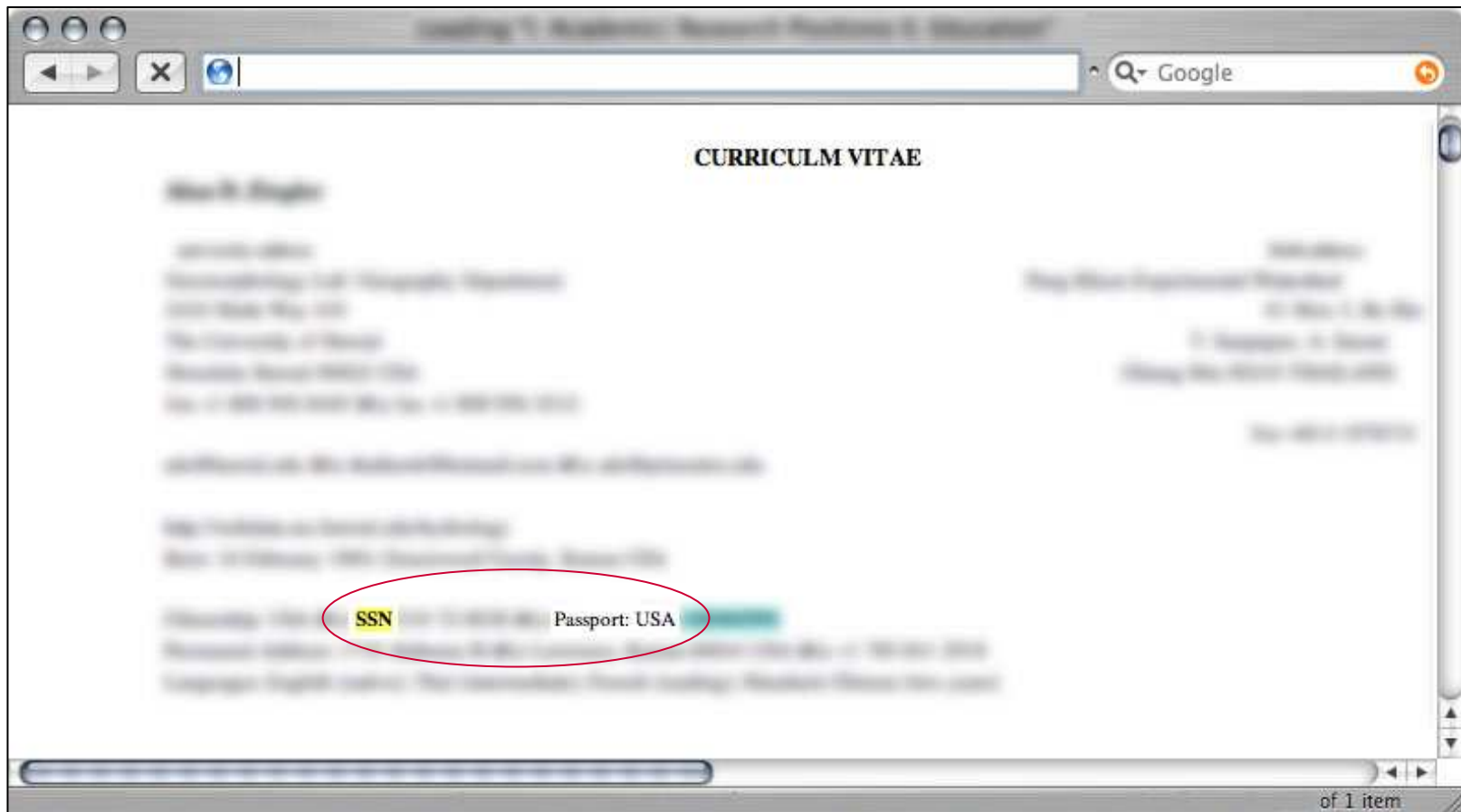
## SSN's

- Students have a right to know...



## Social Security Numbers

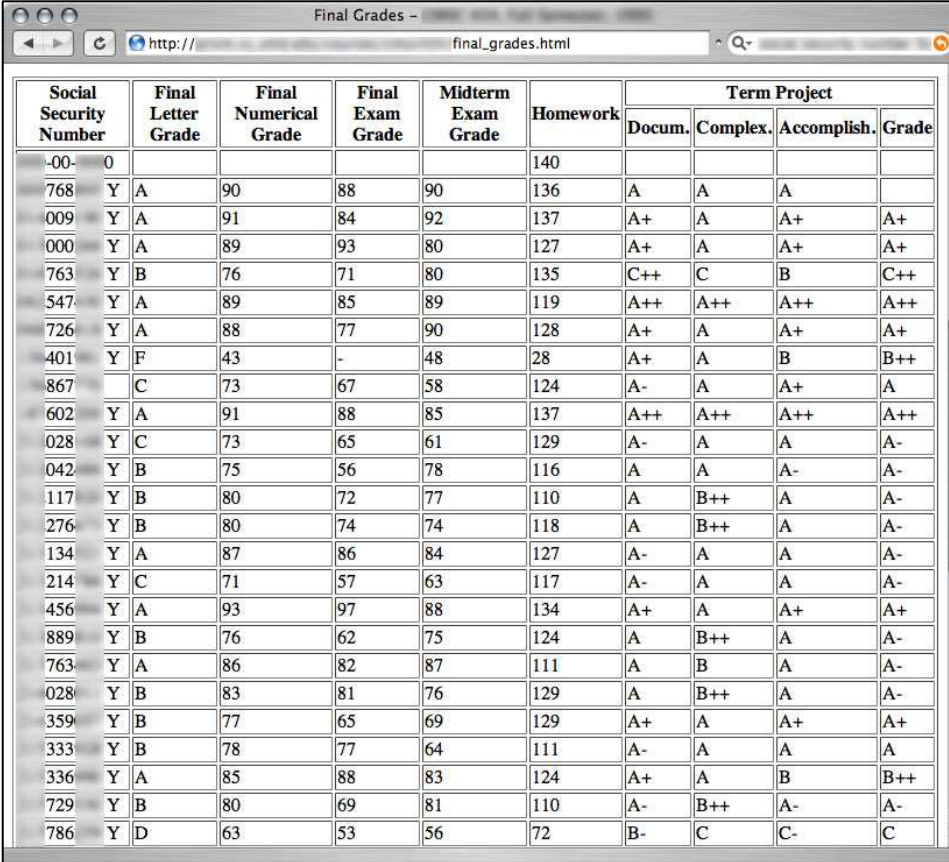
- Many privacy violations are self-inflicted...





## Social Security Numbers

- Schools are notorious... Grades posted w/ student's SSN's



The image shows a screenshot of a web browser window titled "Final Grades -". The address bar shows the URL "http://.../final\_grades.html". The browser displays a table with the following columns: Social Security Number, Final Letter Grade, Final Numerical Grade, Final Exam Grade, Midterm Exam Grade, Homework, and Term Project (subdivided into Docum., Complex., Accomplish., and Grade). The table contains 30 rows of student data.

Social Security Number	Final Letter Grade	Final Numerical Grade	Final Exam Grade	Midterm Exam Grade	Homework	Term Project				
						Docum.	Complex.	Accomplish.	Grade	
-00-	0				140					
768	Y A	90	88	90	136	A	A	A		
009	Y A	91	84	92	137	A+	A	A+	A+	
000	Y A	89	93	80	127	A+	A	A+	A+	
763	Y B	76	71	80	135	C++	C	B	C++	
547	Y A	89	85	89	119	A++	A++	A++	A++	
726	Y A	88	77	90	128	A+	A	A+	A+	
401	Y F	43	-	48	28	A+	A	B	B++	
867		C	73	67	58	124	A-	A	A+	A
602	Y A	91	88	85	137	A++	A++	A++	A++	
028	Y C	73	65	61	129	A-	A	A	A-	
042	Y B	75	56	78	116	A	A	A-	A-	
117	Y B	80	72	77	110	A	B++	A	A-	
276	Y B	80	74	74	118	A	B++	A	A-	
134	Y A	87	86	84	127	A-	A	A	A-	
214	Y C	71	57	63	117	A-	A	A	A-	
456	Y A	93	97	88	134	A+	A	A+	A+	
889	Y B	76	62	75	124	A	B++	A	A-	
763	Y A	86	82	87	111	A	B	A	A-	
028	Y B	83	81	76	129	A	B++	A	A-	
359	Y B	77	65	69	129	A+	A	A+	A+	
333	Y B	78	77	64	111	A-	A	A	A	
336	Y A	85	88	83	124	A+	A	B	B++	
729	Y B	80	69	81	110	A-	B++	A-	A-	
786	Y D	63	53	56	72	B-	C	C-	C	

# Social Security Numbers

- Once you get a lock on a grade list, the results fan out as you explore the site.

The screenshot shows a Google search interface with the search term "social security number". The search results are displayed in a list format, with each result including a title, a snippet of text, and a link to the source page. The results are categorized under "Web" and "Sponsored Links".

**Web** Results 1 - 6 of 6 from [redacted] for **social security number** (0.08 seconds)

**Social Security Number** Sponsored Link  
[www.USATrace.com](http://www.USATrace.com) The Most Sophisticated SSN Search For Your Money-View Results On-Line

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

**Final Grades - [redacted]**  
0101. Fall 95. **Final Grades. ... Social Security Number**, Final Letter Grade, Final Numerical Grade, Final Exam Grade, Midterm Exam Grade, Homework, Term Project. Docum. ...  
/final\_grades.html - 8k - [Cached](#) - [Similar pages](#)

**Final Grades - [redacted]**  
CMSC 620 Spring 96. **Final Grades. ... Social Security Number**, Final Letter Grade, Final Numerical Grade, Final Exam Grade, Mid-Term Exam Grade, Homework, Term Project. ...  
/final\_grades.html - 5k - [Cached](#) - [Similar pages](#)

**Final Grades - [redacted]**  
... Fall 97. **Final Grades. ... Social Security Number**, Final Letter Grade, Final Numerical Grade, Final Exam Grade, Midterm Exam Grade, Homework (190), Term Project. Docum. ...  
final\_grades.html - 8k - [Cached](#) - [Similar pages](#)

**Final Grades - [redacted]**  
... Fall 97. **Final Grades. ... Social Security Number**, Final Letter Grade, Final Numerical Grade, Final Exam Grade, Midterm Exam Grade, Homework (190), Term Project. Docum. ...  
/final\_grades.html - 7k - [Cached](#) - [Similar pages](#)

**Final Grades - [redacted]**  
... **Social Security Number**, Mid-Term Numerical Grade. 041961823, 94. 061666435, 95. 077620007, 74. 087561287, 83. 101584320, 73. 149864594, 62. 156483043, 85. 212820065, 93. ...  
/midterm\_grades.html - 3k - [Cached](#) - [Similar pages](#)

**Final Grades - CMSC 620, Spring Semester, 1996**

**Sponsored Links**

**\$9.95 SSN# People Search**  
100% Money Back Guarantee  
find people fast.  
[socialsecuritypeoplesearch.com](http://socialsecuritypeoplesearch.com)

**Social Security Number**  
Access any Public Record.  
Get Web Detective now! assoc.  
[www.SafeSpy.net](http://www.SafeSpy.net)

**\$6 - \$10 SSN Search**  
Search SSN-Bulk Discounts Available  
No Records - No Charge.  
[www.detectiveconsultant.com](http://www.detectiveconsultant.com)

**People Search by SSN#**  
Search by **Social Security Number**  
Money Back Guarantee only \$19.95  
[socialsecuritysearchusa.com](http://socialsecuritysearchusa.com)

**Social Security Number**  
Web Detective - Get Personal Files.  
Investigate anyone now! Assoc.  
[www.DetectiveWho.com](http://www.DetectiveWho.com)

**Social Security Numbers**  
Access **Social Security** Records.  
Unlimited Lifetime Membership! aff  
[www.Pro-Detective.com](http://www.Pro-Detective.com)

**People Search Experts**  
Find Someone Today.  
Guaranteed Results!

# Social Security Numbers

## Mid-Term Grades

Mid-Term Exam Average Grade = 73.22  
 Mid-Term Exam Median Grade = 83  
 Upper Quartile  $\geq$  93  
 2nd Quartile  $\geq$  83  
 3rd Quartile  $\geq$  68  
 Lower Quartile  $\leq$  65  
 High Grade = 97  
 Low Grade = 27

Social Security Number	Mid-Term Num
43	68
90	61
15	71
39	86
11	93
98	71
04	79
35	95
64	43
61	97
45	91
17	86
04	69
02	65

SSN	Demo (80)	Self-evaluation (20)
84	64	11
82	64	18
80	79	19
78	69	18
37	69	18
82	75	19
00	62	18
82	62	16
68	77	19
64	62	19
66	77	19
91	69	18
74	62	19
70	79	19
56	45	18
00	79	20
74	66	18
88	75	19
78	45	18
60	59	16
00	79	20
80	45	18
80	79	19
68	64	16
76	62	17
16	77	18
68	48	17
78	69	16
76	50	18
74	48	17
90	59	18
92	69	18
64	69	18
68	43	19
74	50	18
62	59	16
76	79	19
74	62	18
82	68	19
70	48	17
98	43	19
66	68	19
04	60	18
00	60	18

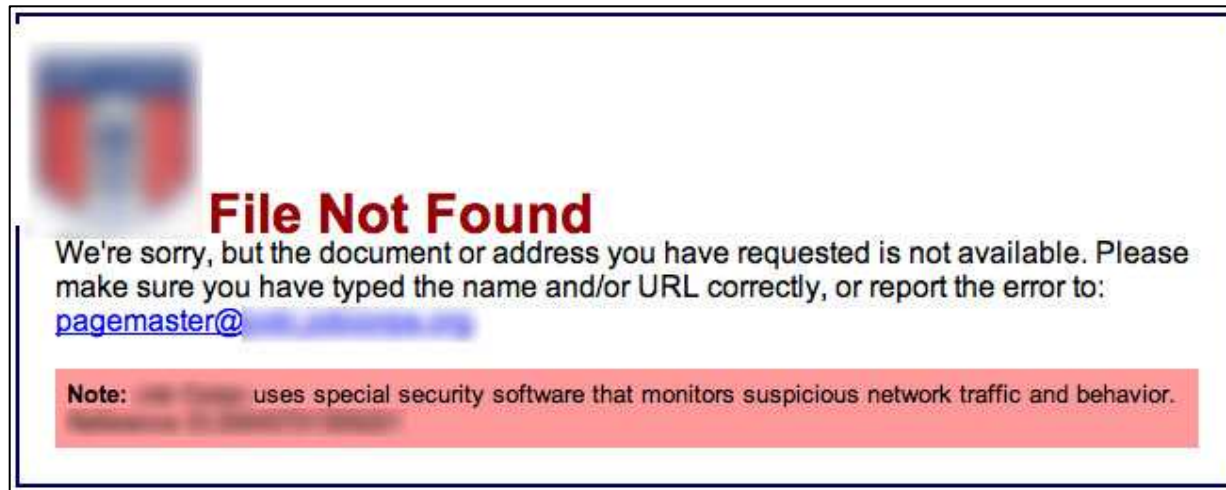
SSN	Final Exam	Course Grade
88 724	A	A
72 690	A	B+
78 652	C	B
68 902	B	B
80 067	C	B
80 354	B+	B
84 959	C	C+
72 932	B	B
62 340	C-	C
72 701	A	A
82 193	F	F
62 677	B	B
78 644	C	C
80 608	B	B
70 661	C	C+
70 057	F	D
74 146	C-	C
90 786	C-	D
55 901	B	B
74 673	B	B
84 791	B	B
78 085	C+	B
78 323	D	C
72 380	B	C
72 104		TF
66 158	C+	C
74 620	C	C+
80 055	C	B
62 603	F	C
70 191	A	B
84 185	B	B
84 608	A	A
27 152	C	B
66 114	C+	C
72 051	C	C+
76 981	C	C+
72 253	B+	A
62 380	B	A
72 062	C	C
76 930	D	C
76 240	B	B
76 651	C-	C
74 780	D	D

There's no shortage of examples...

---

## Social Security Numbers

- In order to steal someone's identity, you need names. SSN's with names are usually blocked... aren't they?



# Social Security Numbers

ion of the file [\[redacted\]](#)  
cally generates html versions of documents as we crawl the web.  
rk this page, use the following url: <http://www.google.com/search?>

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

have been highlighted: **ssn** [\[redacted\]](#)

**Page 1**

	<b>SSN</b>	Student Name		
100	54 43	[redacted]		
100	64 69	[redacted]		
200	64 15	[redacted]		
200	70 09	[redacted]		
200	80 90	[redacted]		
200	60 22	[redacted]		
300	62 23	[redacted]		
300	62 23	[redacted]		
300	80 60	[redacted]		
400	86 10	[redacted]		
400	70 24	[redacted]		
500	84 22	[redacted]		
500	76 33	[redacted]		
500	82 84	[redacted]		
500	76 71	[redacted]		
700	60 34	[redacted]		
200	93 08	[redacted]		
300	66 60	[redacted]		

Google's  
cache says  
otherwise...





# A tale of one city

- Hundreds of city residents' personal information posted to the web... 90% including SSN and address.

The image displays five overlapping screenshots of a web browser showing a list of personal information. Each screenshot has a red oval highlighting a specific row of data. The data includes names, addresses, phone numbers, and Social Security Numbers (SSNs). The screenshots are arranged in a way that shows the same list of information from different angles, emphasizing the volume and accessibility of the data.

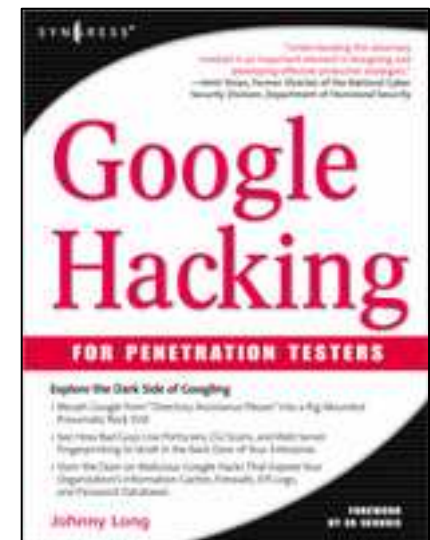
Name	Address	Phone Number	SSN
JOHN J. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JANE D. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JOHN J. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JANE D. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JOHN J. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JANE D. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JOHN J. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JANE D. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JOHN J. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789
JANE D. SMITH	1234 MAIN ST, NEW YORK, NY 10001	(212) 555-1234	123-45-6789



---

## What we've done...

- We've skimmed "Google Hacking for Penetration Testers" by Syngress Publishing, which doesn't seem to suck.
- We've looked at some great tools by Roelof Temmingh. Check out Sensepost.com.
- We've invaded the privacy of millions.
- We're all still awake. Right?



---

## Thanks!

- Thanks to God for the gift of life.
- Thanks to my family for the gift of love.
- Thanks to my friends for filling in the blanks.
- Thanks to the moderators of [ihackstuff.com](http://ihackstuff.com): Murfie, Jimmy Neutron, ThePsyko, Wasabi, I0om, Stonersavant
- Thanks to Roelof T for the great code, and to the current Google Masters: murfie, jimmyneutron, klouw, I0om, stonersavant, MILKMAN, ThePsyko, cybercide, yeseins, wolveso, Deadlink, crash\_monkey, zoro25, digital.revolution, Renegade334, wasabi, urban, sfd, mlynch, Peefy, Vipsta, noAcces, brasileiro, john, Z!nCh