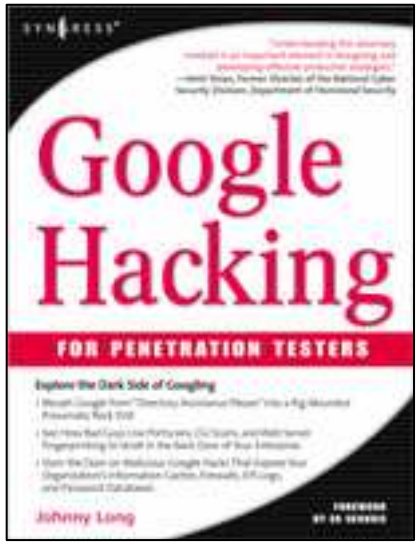
Google Hacking for Penetration Testers

Using Google as a Security Testing Tool

Johnny Long
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.

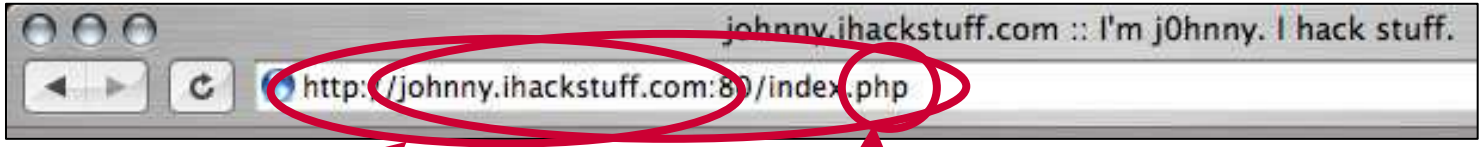
Some operators can only be used to search specific areas of Google, as these columns show.

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

In other cases, mixing should be avoided.

Crash course in advanced operators

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



SITE:

INURL:

FILETYPE:

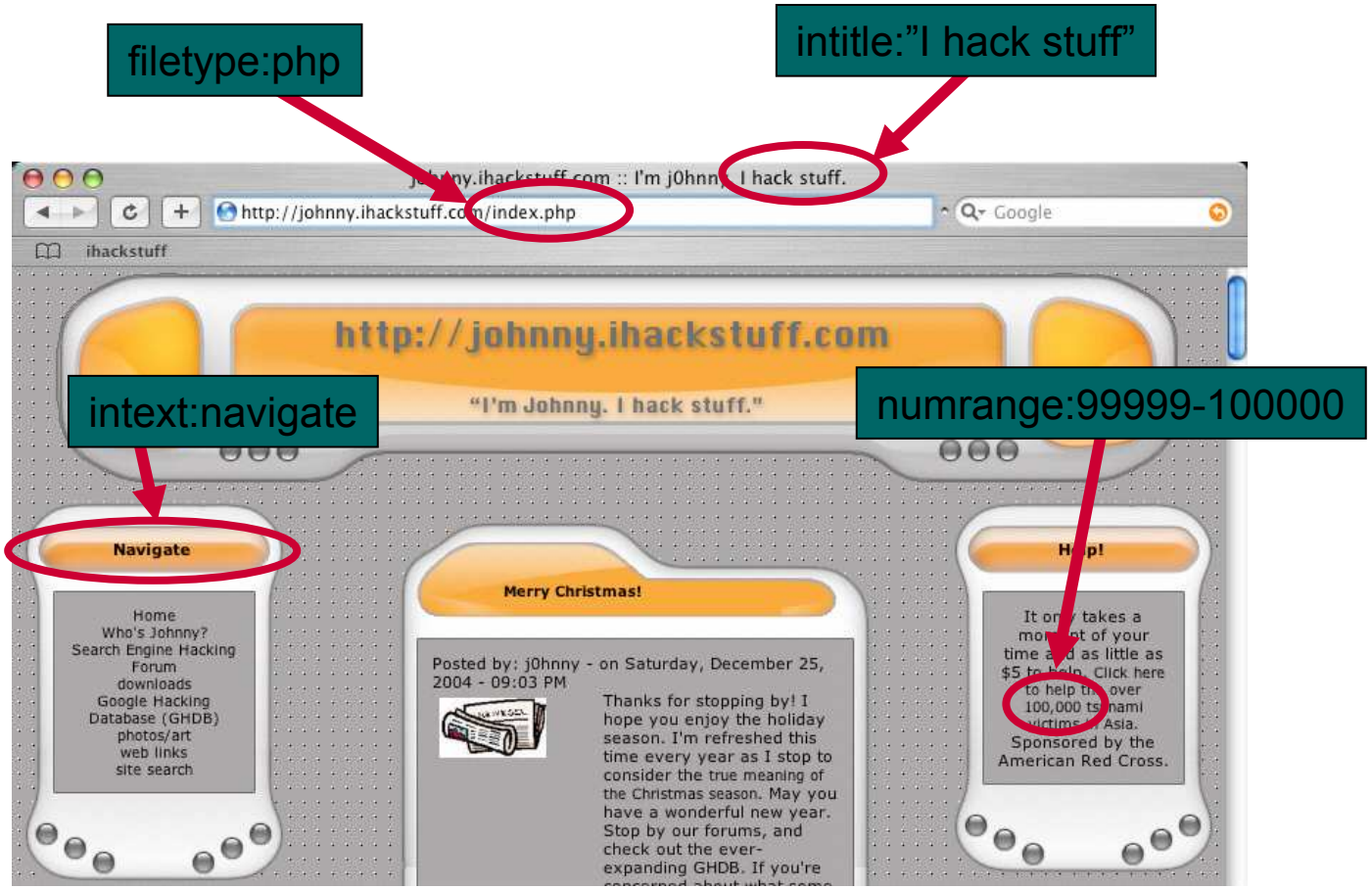
Site can not search port.

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

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

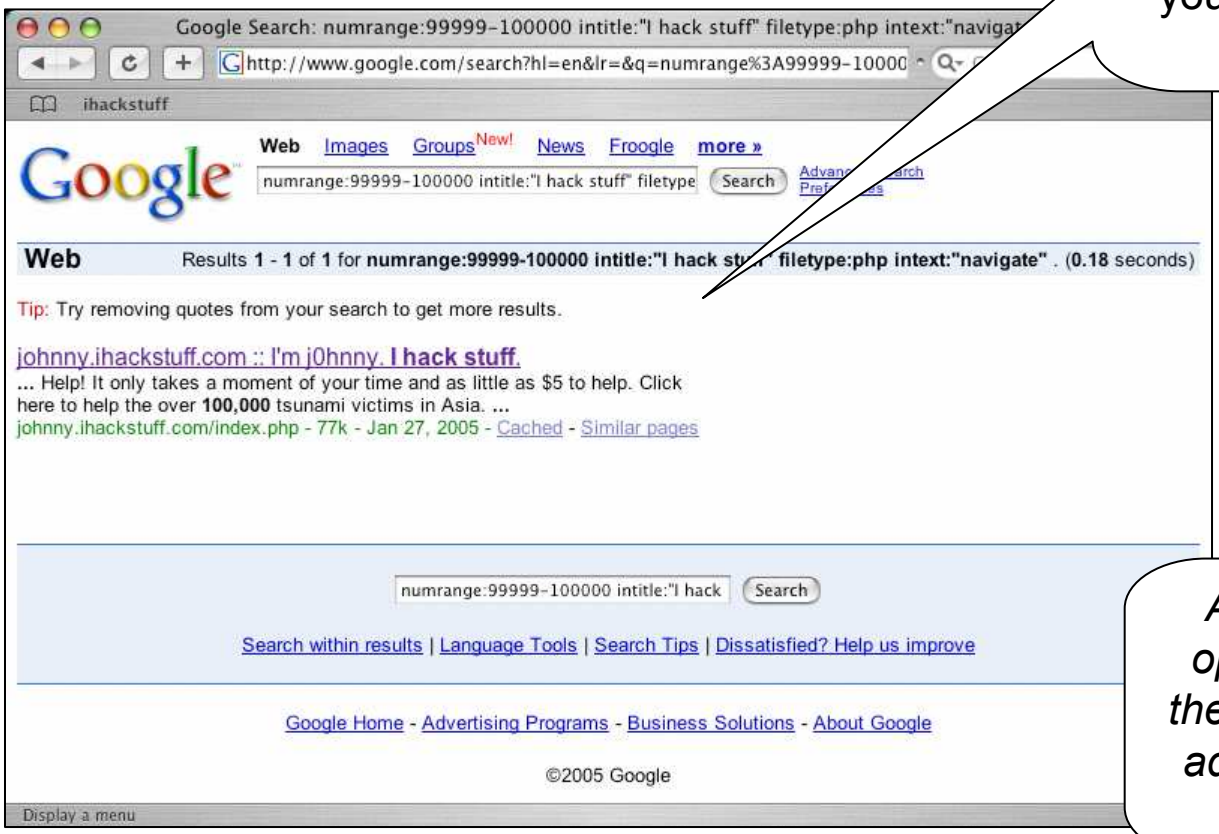
Advanced Google Searching

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



Advanced Google Searching

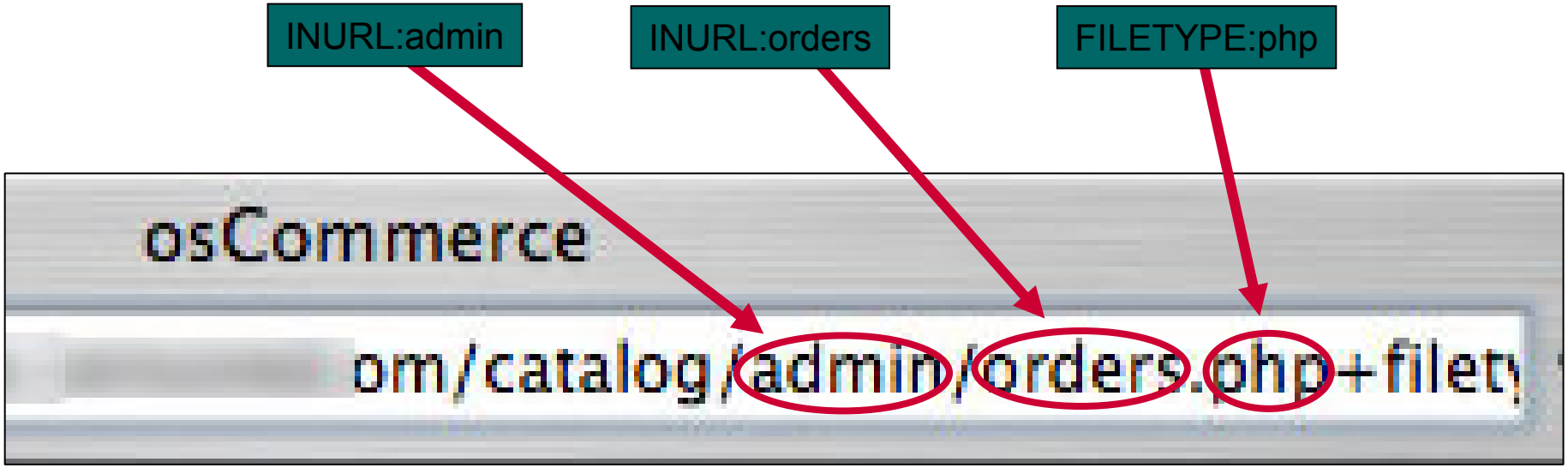
Put those individual queries together into one monster query and you only get that one specific result.



*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…



Google Hacking Basics

…can return *devastating* results!

osCommerce

http: [redacted] om/catalog/admin/orders.php+filet filetype:php inurl:admin inurl

This is Google's cache of http://www.[redacted].com/catalog/admin/orders.php.
Google's cache is the snapshot that we took of the page as we crawled the web.
The page may have changed since that time. Click here for the current page without highlighting.
This cached page may reference images which are no longer available. Click here for the cached text only.
To link to or bookmark this page, use the following url: http://www.google.com/search?q=cache:Vc-7oIl9sFkJ:www.[redacted].com/catalog/admin/orders.php+filetype:php+inurl:admin+inurl:orders&hl=en

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

These search terms have been highlighted: **orders**
These terms only appear in links pointing to this page: **admin**

Customer names

Order Amounts

Payment details!

Administration
Configuration
My Store
Minimum Values
Maximum Values
Images
Customer Details
Shipping/Packaging
Product Listing
Stock
Logging
Cache
E-Mail Options
Download

Support Site | Online Catalog | Administration

Order ID:
Status: AllOrders

Orders

Customers	Order Total	Date Purchased	Status	Action
[redacted]	$56.30	07/01/2004 20:19:33	Delivered	
[redacted]	$81.90	06/17/2004 11:22:22	Delivered	
[redacted] Hewitt	$69.50	06/16/2004 22:38:20	Pending	
[redacted]	$45.25	04/23/2004 02:08:24	Delivered	
[redacted]	$159.15	04/16/2004 22:37:00	Delivered	

[49] 07/01/2004 20:19:33

Date Created: 07/01/2004
Last Modified: 07/06/2004

Payment Method: Bank

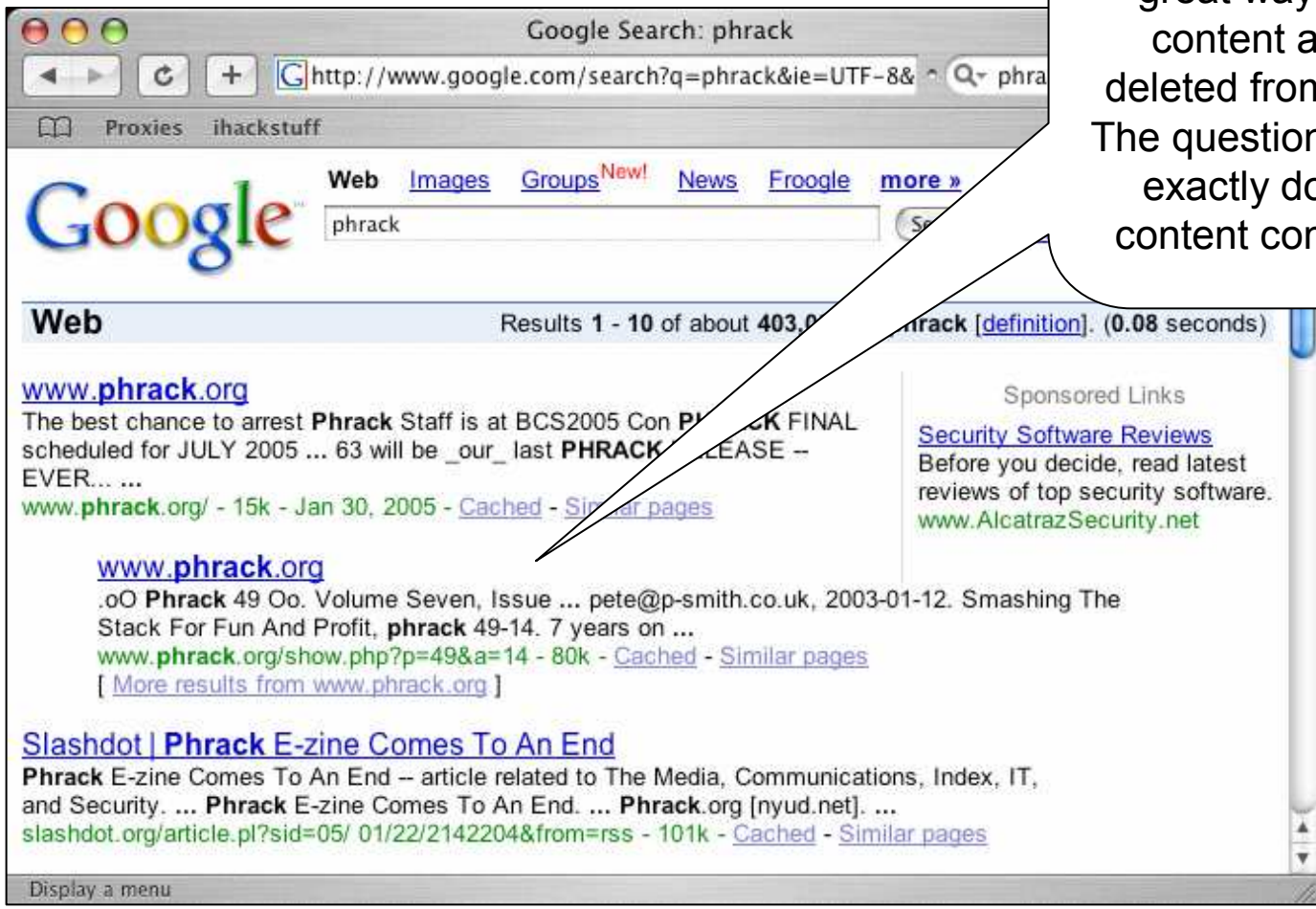
Display a menu

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.

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   .l..GET./grfx/81sm
0x0050   626c 7565 2e6a 7067 2048 5454 502f 312e   blue.jpg.HTTP/1.
0x0060   310d 0a48 6f73 743a 2077 7777 2e70 6872   1..Host:.www.phr
0x0070   6163 6b2e 6f72 670d 0a43 6f6e 6e65 6374   ack.org..Connect
0x0080   696f 6e3a 206b 6565 702d 616c 6976 650d   ion:.keep-alive.
0x0090   0a52 6566 6572 6572 3a20 6874 7470 3a2f   .Referer:.http:/
0x00a0   2f36 342e 3233 332e 3136 312e 3130 342f   /64.233.161.104/
0x00b0   7365 6172 6368 3f71 3d63 6163 6865 3a4c   search?q=cache:L
0x00c0   4251 5a49 7253 6b4d 6755 4a3a 7777 772e   BQZIrSkMgUJ:www.
0x00d0   7068 7261 636b 2e6f 7267 2f2b 2b73 6974   phrack.org/++sit
0x00e0   653a 7777 772e 7068 7261 636b 2e6f 7267   e:www.phrack.org
0x00f0   2b70 6872 6163 6b26 686c 3d65 6e0d 0a55   +phrack&hl=en..U
```

An image loaded!

Anonymous Googling

This line spells it out. Let's click this link and sniff the connection again….

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**

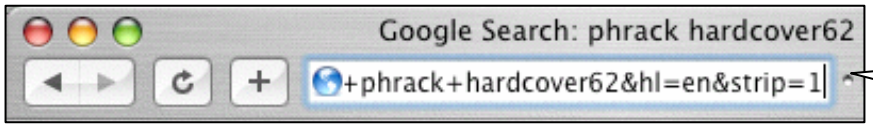
Adding **&strip=1** to the end of the cached URL only shows Google's text, not the target's.

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.



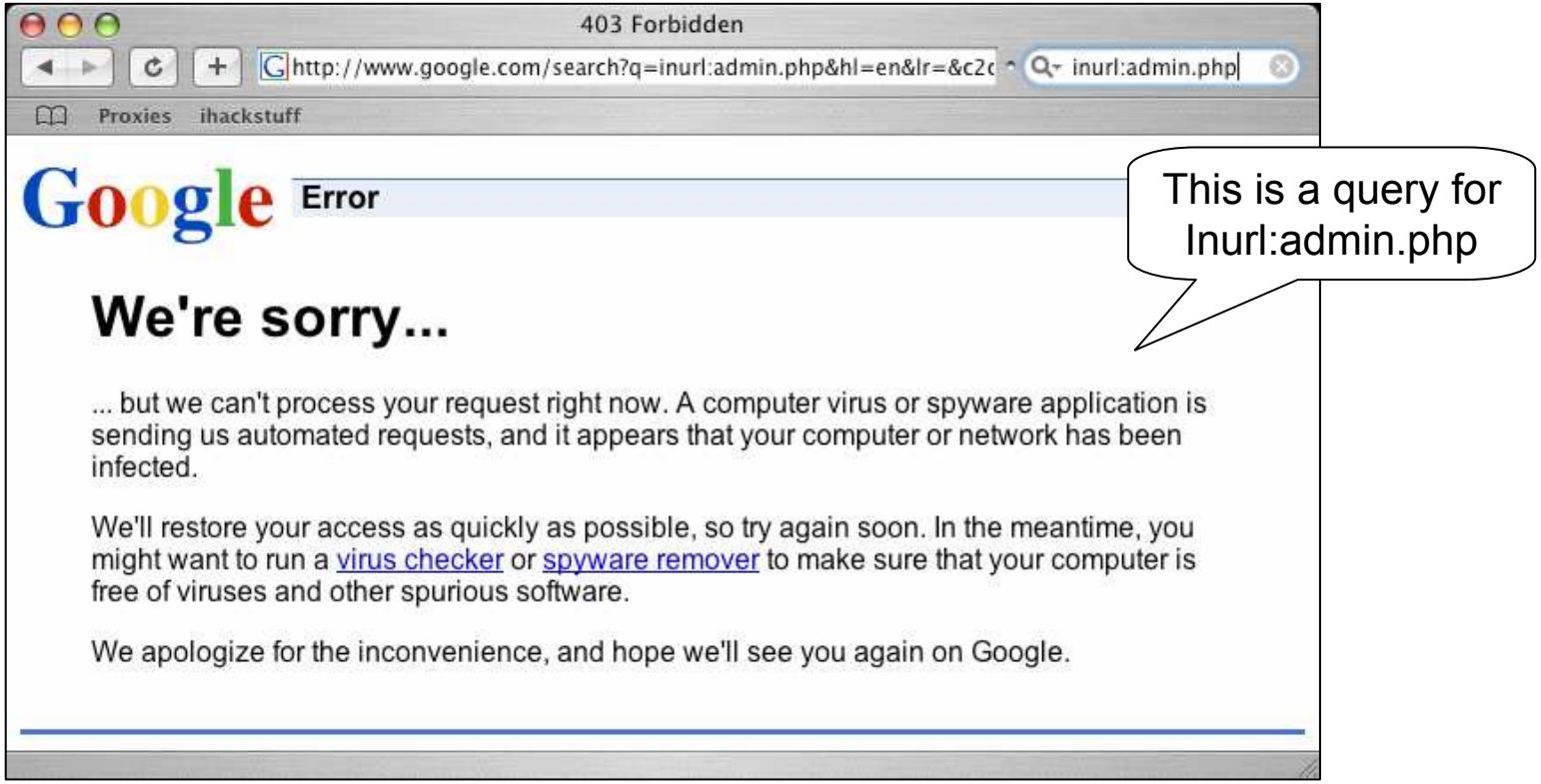
Paste the URL to the address bar, add **&strip=1**, hit return. You're only touching Google now…

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.'



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.

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:

```
Terminal — bash — 83x9
j0hnny-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
j0hnny-longs-Computer:~/Documents/workbench/Coding $
```

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

More Email Automation

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

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

More email address locations

Query	Description
"Internal Server Error" "server at"	Apache server error could reveal admin e-mail address
intitle:"Execution of this script not permitted"	Cgiwrap script can reveal *lots* of information, including e-mail addresses and even phone numbers
e-mail address filetype:csv csv	CSV files that could contain e-mail addresses
intitle:index.of dead.letter	dead.letter UNIX file contains the contents of unfinished e-mails that can contain sensitive information
inurl:fcgi-bin/echo	fastcgi echo script can reveal *lots* of information, including e-mail addresses and server information
filetype:pst pst -from -to -date	Finds Outlook PST files, which can contain e-mails, calendaring, and address information
intitle:index.of inbox	Generic "inbox" search can locate e-mail caches
intitle:"Index Of" -inurl:maillog maillog size	Maillog files can reveal usernames, e-mail addresses, user login/logout times, IP addresses, directories on the server, and more
inurl:email filetype:mdb	Microsoft Access databases that could contain e-mail information
filetype:xls inurl:"email.xls"	Microsoft Excel spreadsheets containing e-mail addresses
filetype:xls username password email	Microsoft Excel spreadsheets containing the words *username, password,* and *email*
intitle:index.of inbox dbx	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
filetype:eml eml +intext: "Subject" +intext:"From"	Outlook express e-mail files contain e-mails with full headers
intitle:index.of inbox dbx	Outlook Express e-mail folder
filetype:wab wab	Outlook Mail address books contain sensitive e-mail information
filetype:pst inurl:"outlook.pst"	Outlook PST files can contain e-mails, calendaring, and address information
filetype:mbx mbx intext:Subject	Outlook versions 1–4 or Eudora mailbox files contain sensitive e-mail information
inurl:cgi-bin/printenv	Printenv script can reveal *lots* of information, including e-mail addresses and server information
inurl:forward filetype:forward -cvs	UNIX user e-mail forward files can list e-mail addresses
(filetype:mail | filetype:eml | filetype:mbox | filetype:mbx) intext:password|subject	Various generic e-mail files
"Most Submitted Forms and Scripts" "this section"	WebTrends statistics pages reveal directory information, client access statistics, e-mail addresses, and more
filetype:reg reg +intext: "internet account manager"	Windows registry files can reveal information such as usernames, POP3 passwords, e-mail addresses, and more
"This summary was generated by wwwstat"	Wwwstat statistics information can reveal directory info, client access statistics, e-mail addresses, and more

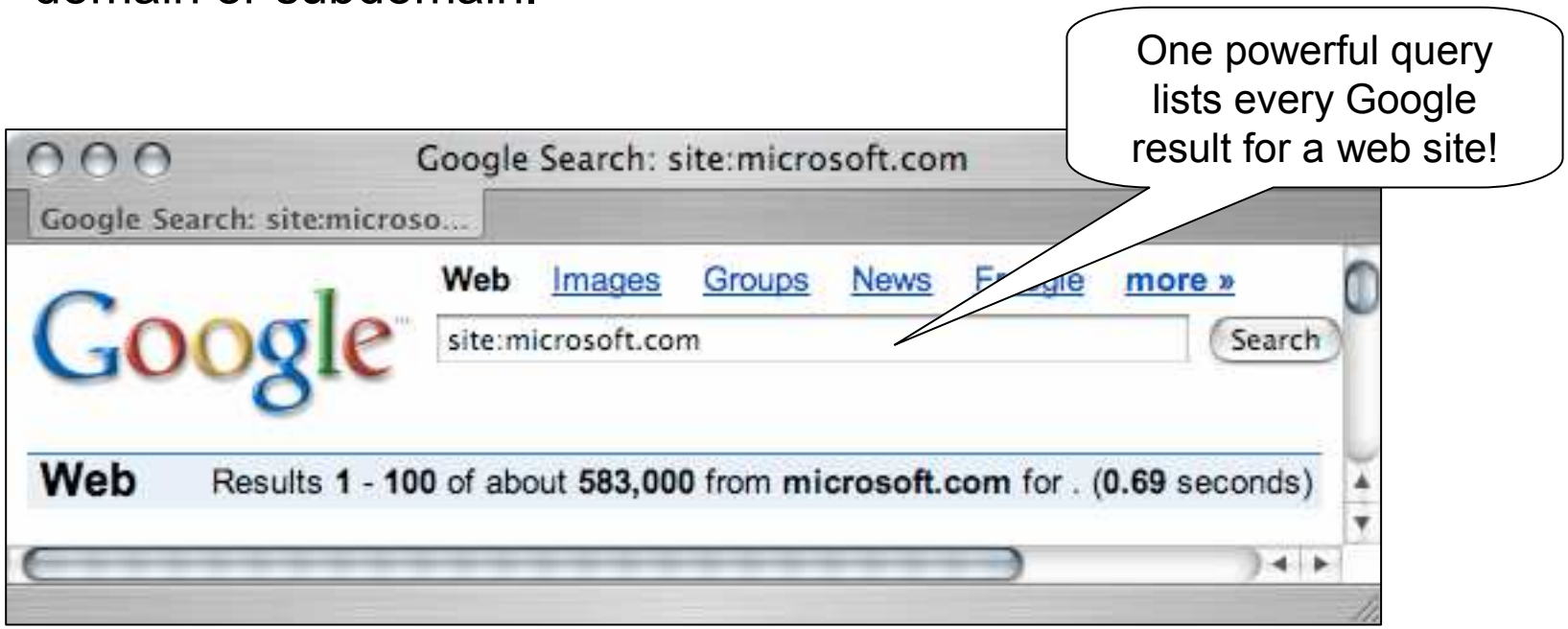
These queries locate email addresses in more "interesting" locations…

Network Mapping

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

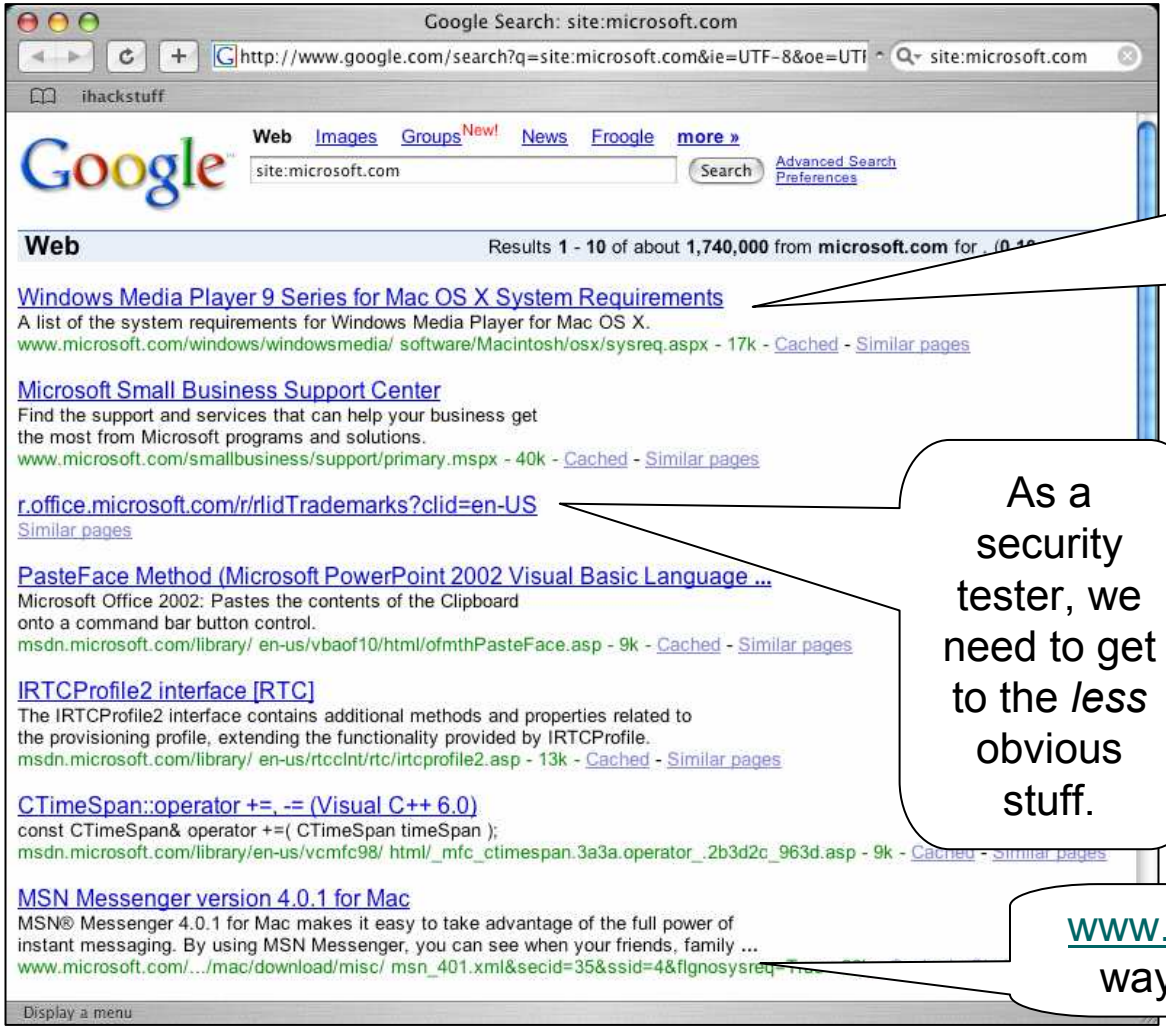
Basic Site Crawling

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



site: microsoft.com

Basic Site Crawling



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

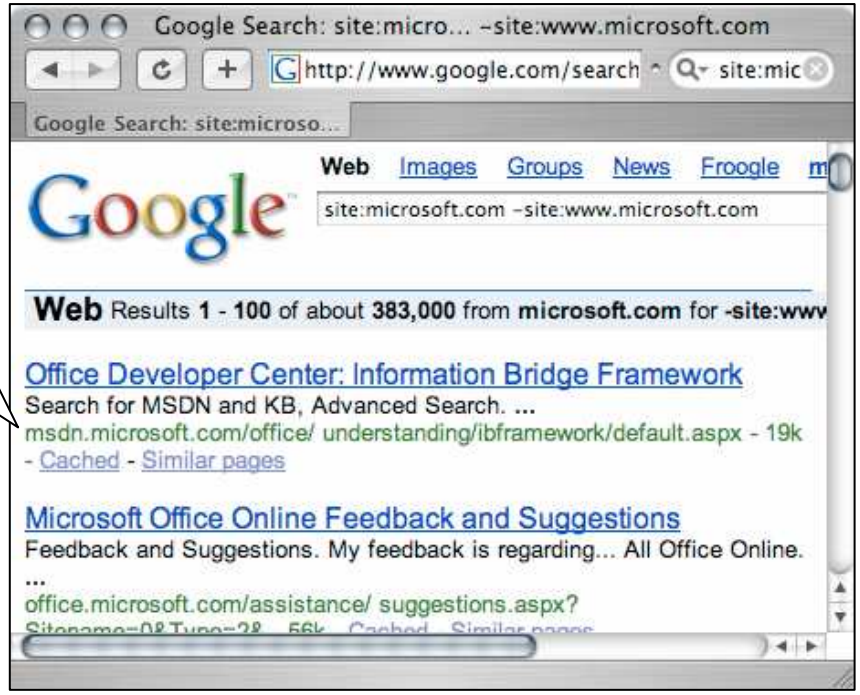
As a security tester, we need to get to the *less* obvious stuff.

www.microsoft.com 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

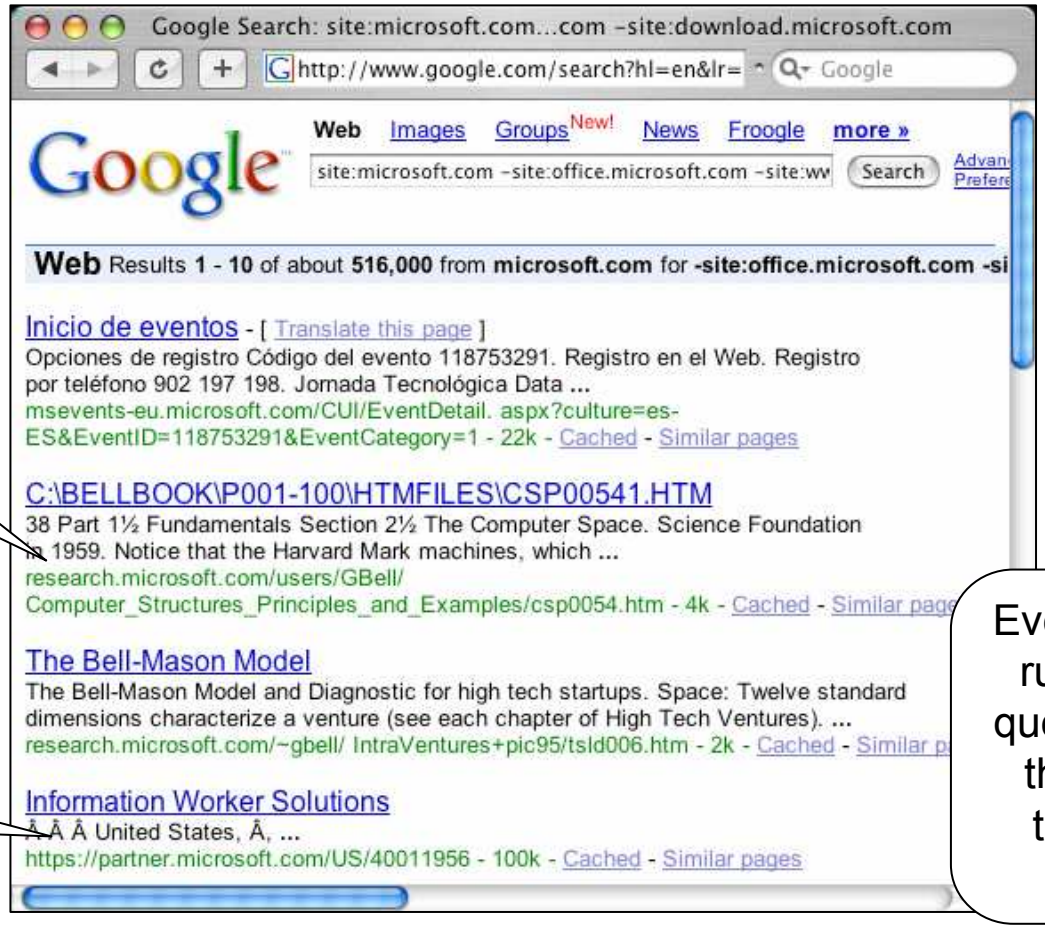
- Repeating this process of site reduction, tracking what floats to the top leads to nasty big queries like:

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.

..and sed and awk to process the HTML…

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:]]*:\/\/[[:alnum:]]*.microsoft.com\//& /p' te
st.html | awk '{print $2}' | sort -u
http://download.microsoft.com/
http://go.microsoft.com/
http://msdn.microsoft.com/
http://msevents.microsoft.com/
http://murl.microsoft.com/
http://office.microsoft.com/
http://protect.microsoft.com/
http://research.microsoft.com/
https://s.microsoft.com/
http://support.microsoft.com/
-bash-2.05b$
```

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

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

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$
```

Advanced Site Crawling

Terminal — ssh — 82x26

```
-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://terraserver.microsoft.com/
http://uddi.microsoft.com/
http://webevents.microsoft.com/
http://windowsbeta.microsoft.com/
-bash-2.05b$
```

Sifting through the ouput 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
terraserver.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…

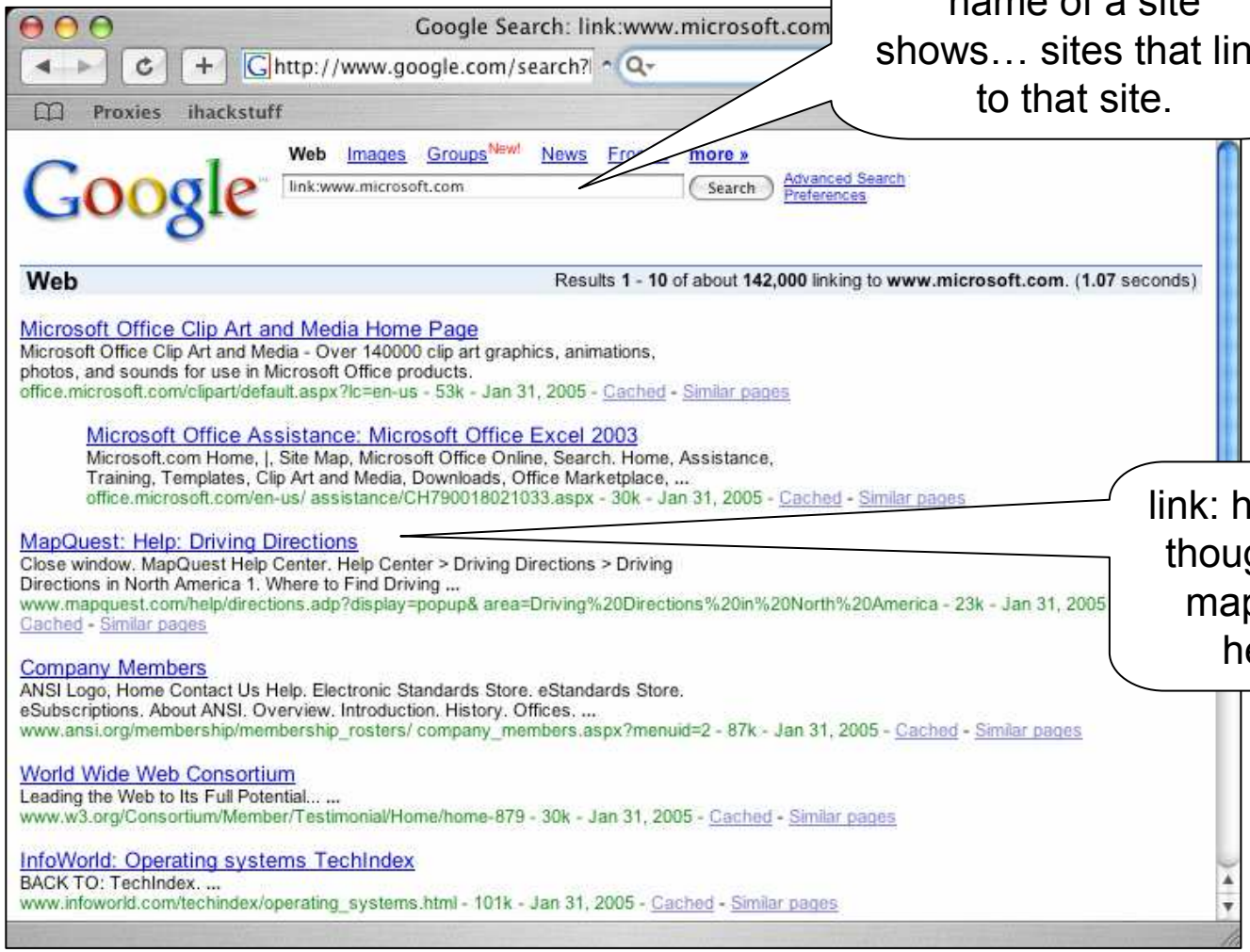
Too much noise, not enough signal…

- 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

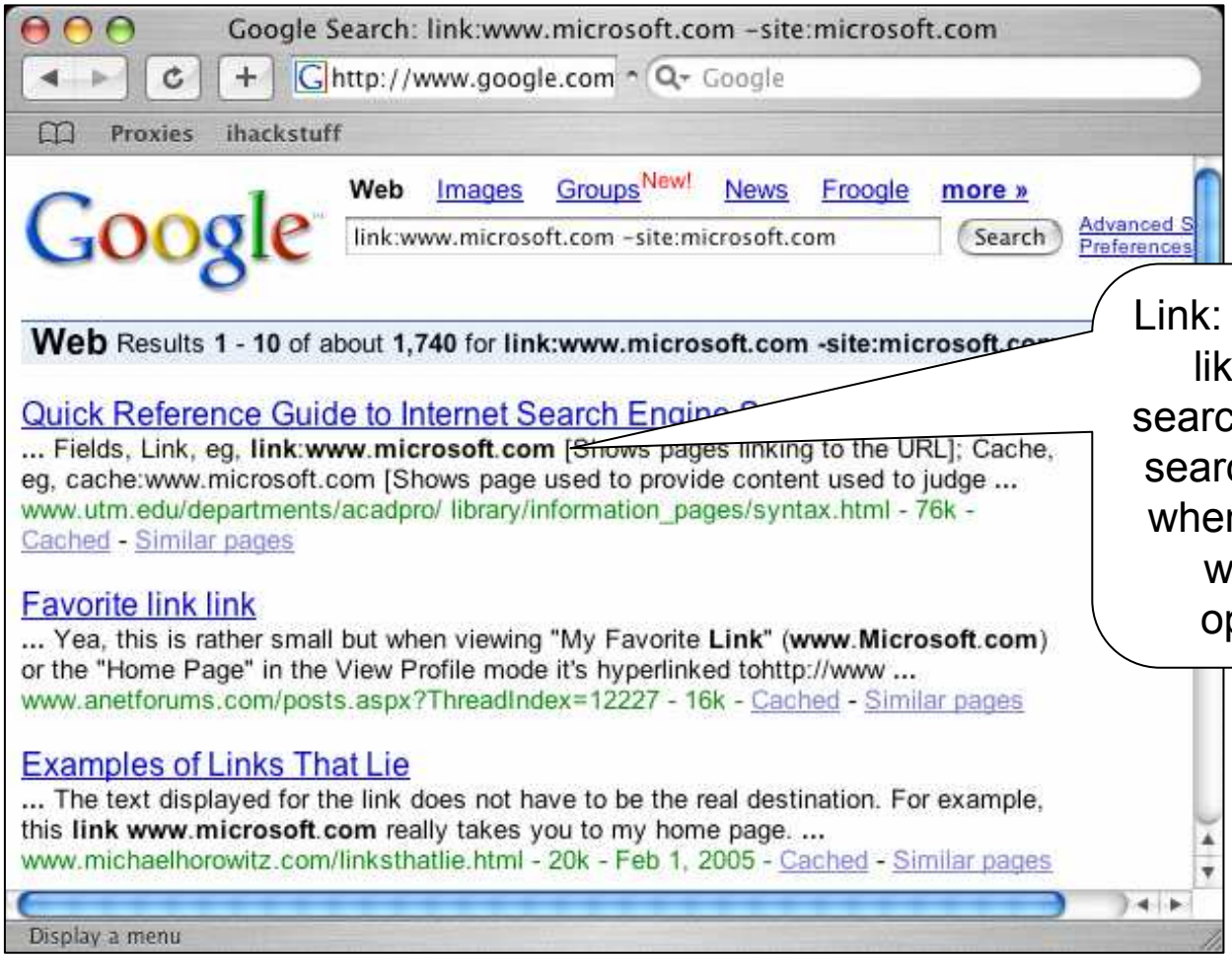


link: combined with the name of a site shows… sites that link to that site.

link: has limits though. See mapquest here?

Link has limits

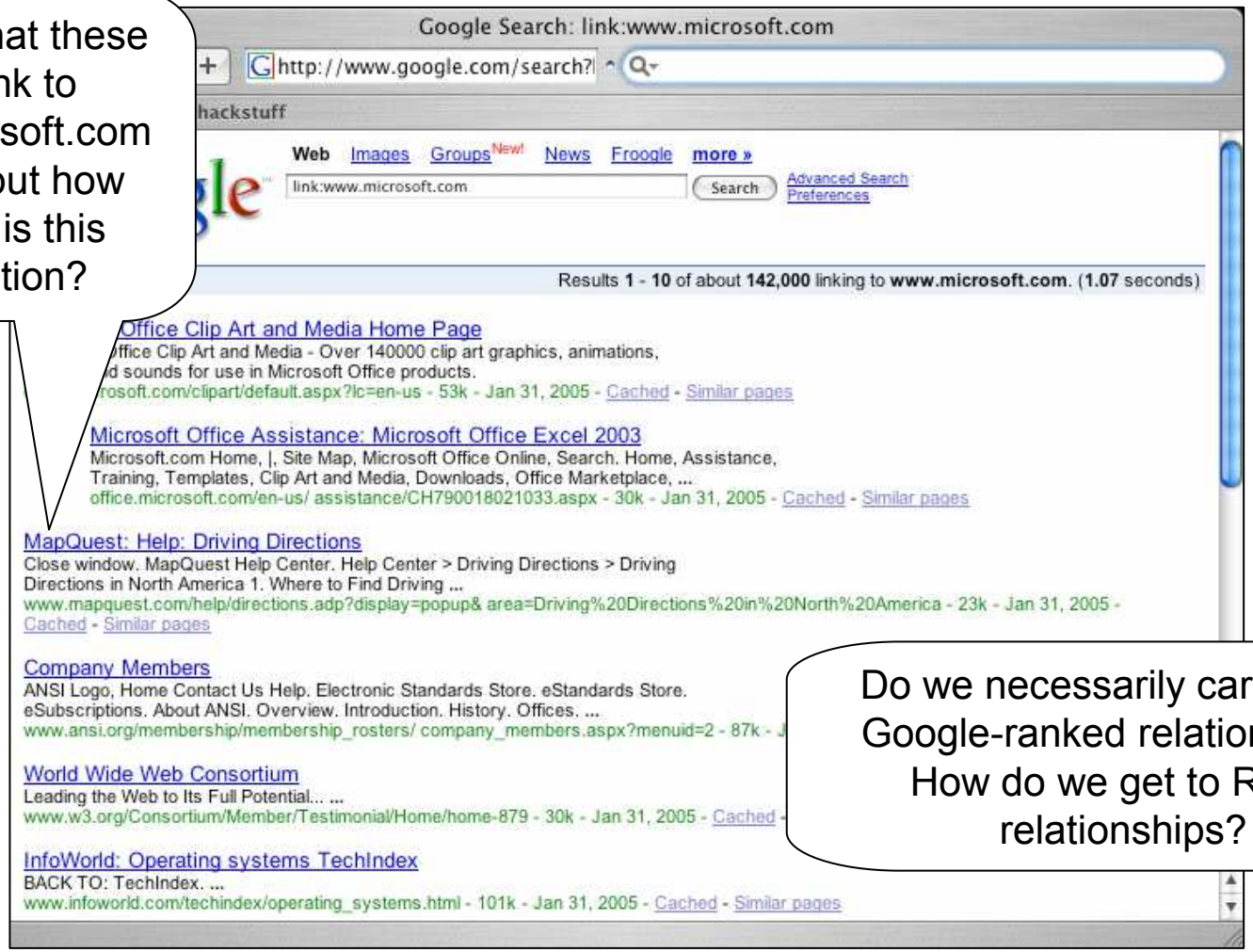
Link has limits



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 is great, but how relevant is this information?



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 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 that a link from a site with a small amount of links
  - This means specifically outbound links.
  - If a site has few outbound links, is 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 that 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?

Google Search: sensepost

http://www.google.com/search?q=sensepost&ie=UTF-

sensepost

Proxies ihackstuff

Web Images Groups News Froogle Local New! more »

Google

sensepost Search Advanced Search Preferences

Web Results **1** - **10** of about **6,490** for **sensepost**. (**0.24** secon

reroute
www.**sensepost**.com/ - 2k - Cached - Similar pages

SensePost
... for such threats. HackRack is a innovative, cutting edge automated scanner designed and maintained by **SensePost**. It encapsulates ...
www.**sensepost**.com/automatedscanning.html - 21k - Cached - Similar pages
[More results from www.sensepost.com]

SQL insertion
... During the time that we were preparing for BlackHat, Haroon Meer (haroon@**sensepost**.com) started extensive fiddling with SQL insertion. ... **SensePost** IT Security. ...
www.cgisecurity.com/lib/SQLinsertion.htm - 40k - Cached - Similar pages

SensePost
The Garage : : Downloads, Defcon/BlackHat 2003 Las Vegas
(Putting the Tea back into CyberTerrorism ...
168.210.134.6/garage.html - 21k - Cached - Similar pages

SensePost
The Garage : : News, Check out the New York Times Article on computer security mentioning **SensePost**. ... **SensePost** talks on Cyber-terrorism at BlackHat. ...
168.210.134.6/garage_news.html - 22k - Cached - Similar pages
[More results from 168.210.134.6]

Index of /nf0/convention_cdroms/defcon11/**SensePost**
Index of /nf0/convention_cdroms/defcon11/**SensePost**. Name Last modified Size Description Parent Directory 08-Dec-2004 15:36 - dc-11 ...
mediawhore.wi2600.org/nf0/ convention_cdroms/defcon11/SensePost/ - 2k - Cached - Similar pages

Display a menu

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 (via Google) and writing the results to a file called "out"…

Non-obvious site relationships

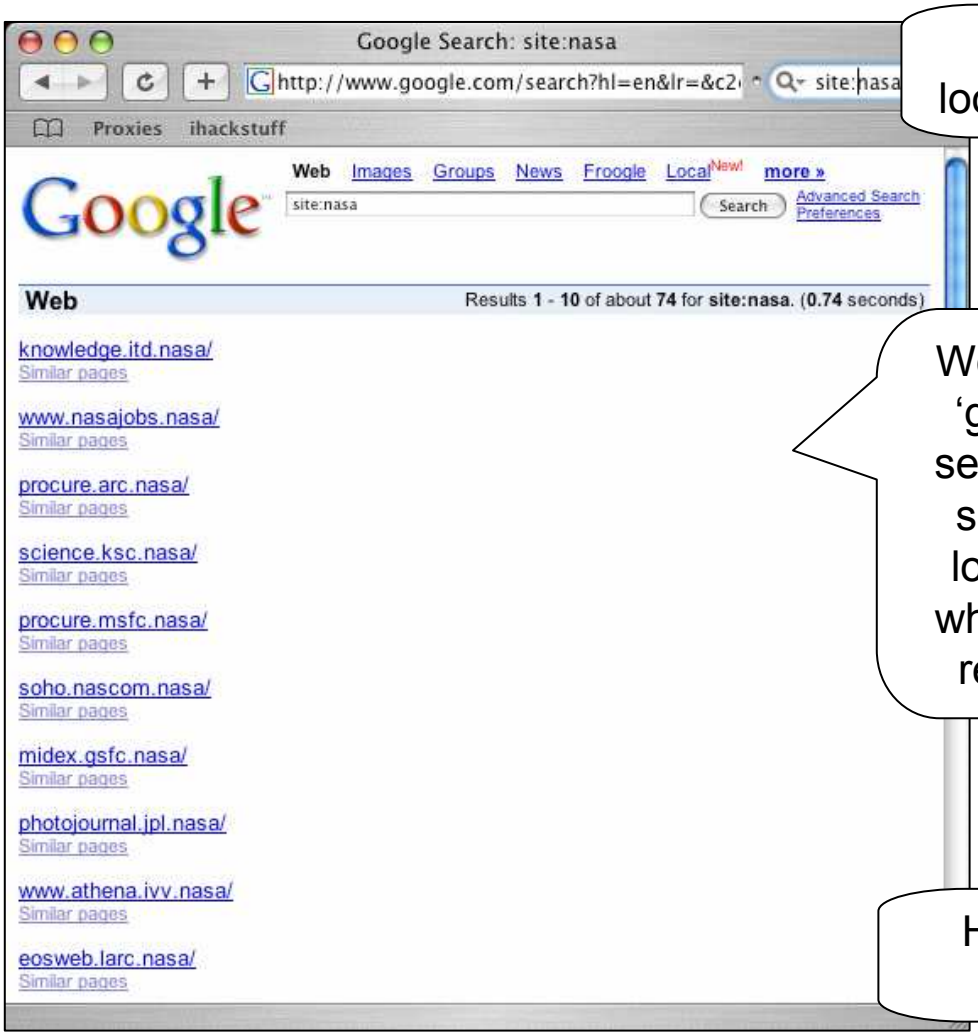
- This is the weigh phase. BiLE takes the output from the extraction phase…

```
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 verifiy 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
cossc.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.[illegible]5.75
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…

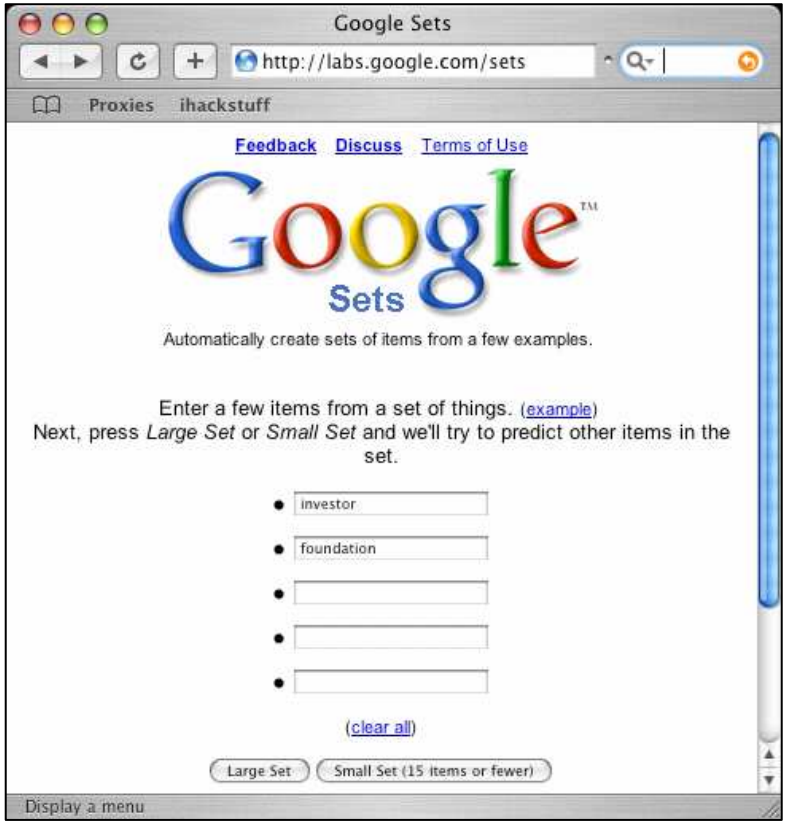
- Once armed with a list of sites and domains, we could expand out the list in several ways. DNS queries are helpful, but what else can we do to get more names to try?
- From whatever source, let's say we get two names from verizon, 'foundation' and investor'…

[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 - Similar pages

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

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/
Similar pages

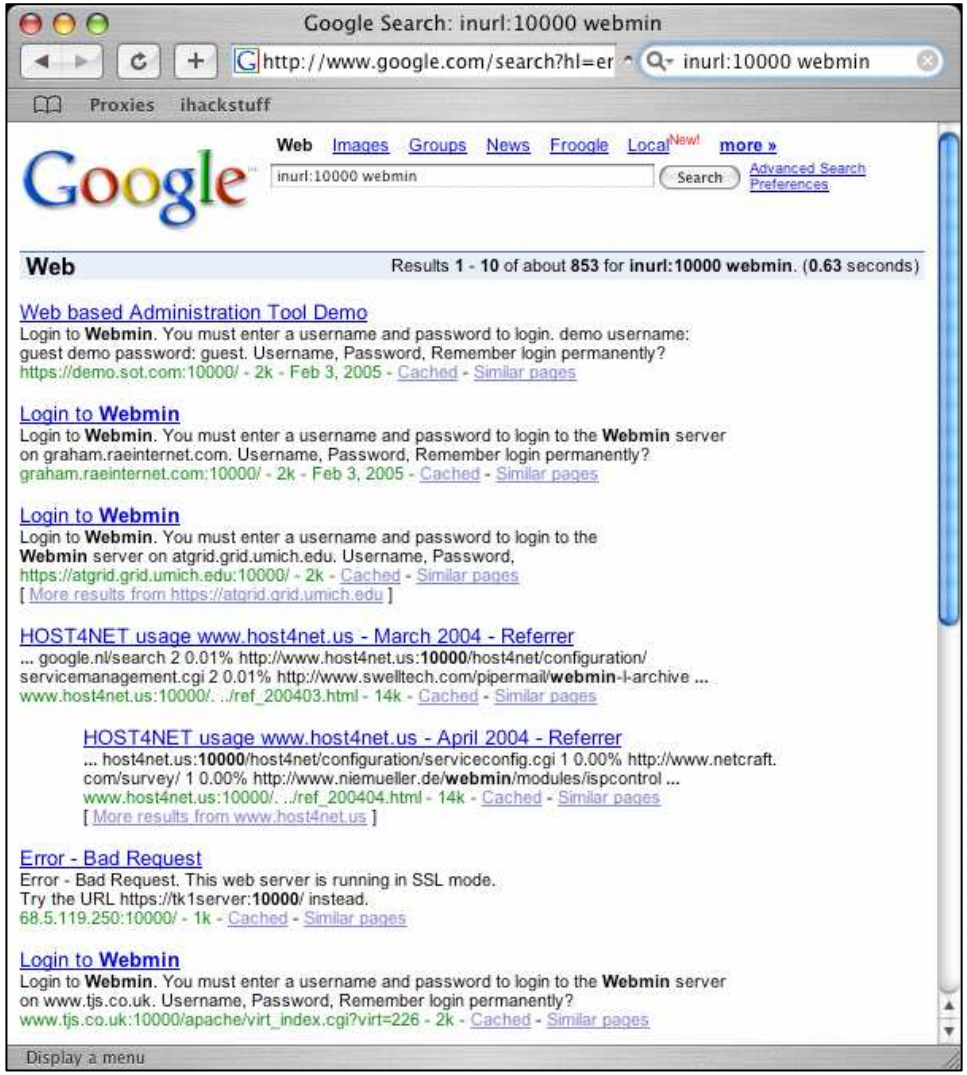
https://www33.verizon.com/wi-fi/login/locations/locations-remote.jsp
Similar pages

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

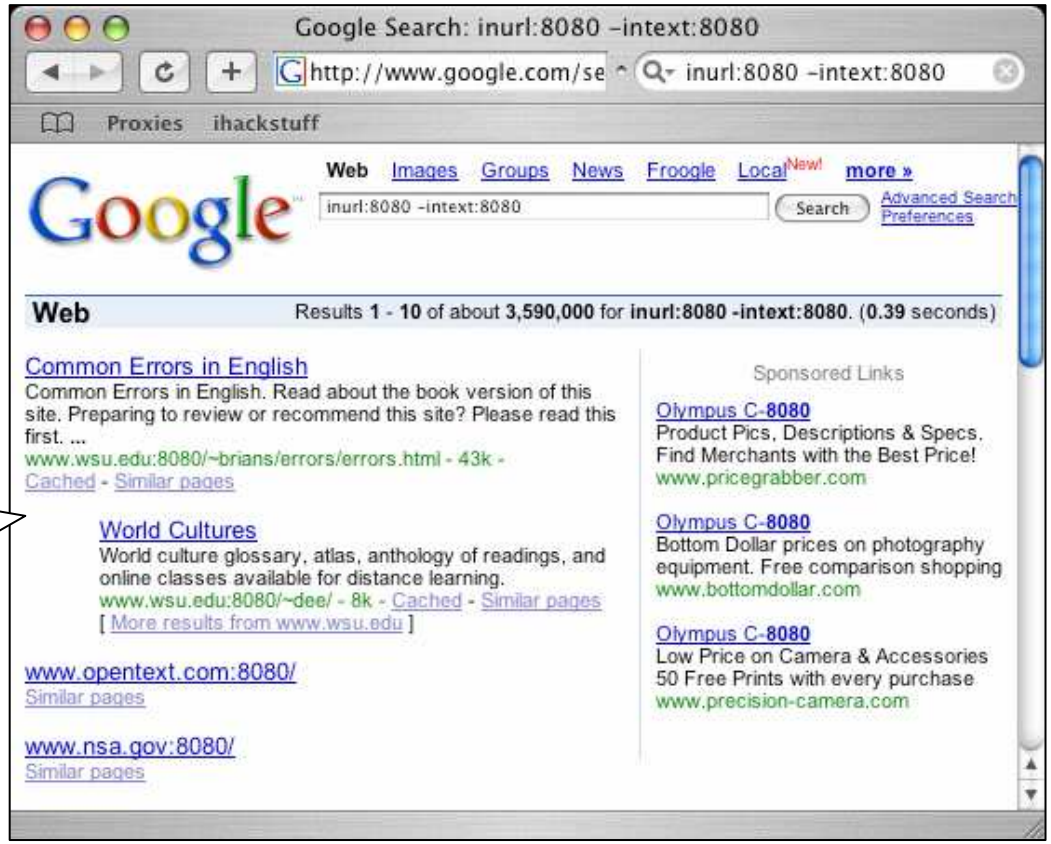
- Although crude, there are ways to do basic “portscanning” with Google.
- First, combine inurl searches for a port with the name of a service that commonly listens on that port… (optionally combined with the site operator)



Inurl -intext scanning

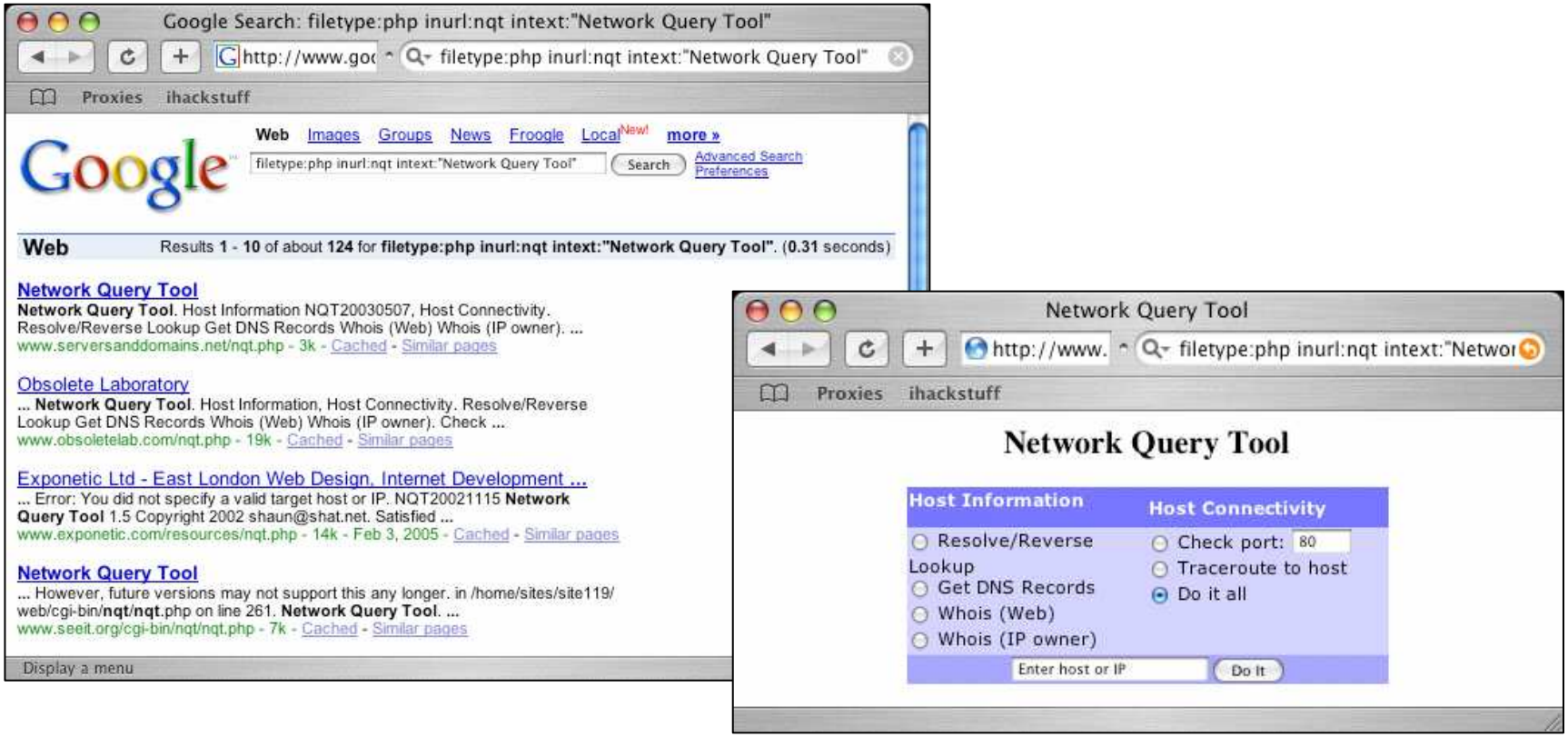
- Antoher way to go is to use a port number with inurl, combined with a negative intext search for that port number.

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”

 Warning: Access denied for u...t_o_index.php on line <

 Warning: A...

Forensic Science Service website | Contact us | Graphic version

Search:

Warning: Access denied for user: 'root@localhost' (**Using password**: NO) in **/var/www/html/paternity/t_o_index.php** on line **60**

Warning: MySQL Connection Failed: Access denied for user: 'root@localhost' (**Using password**: NO) in **/var/www/html/paternity/t_o_index.php** on line **60**

Warning: Supplied argument is not a valid MySQL-Link resource in **/var/www/html/paternity/t_o_index.php** on line **61**

Warning: Supplied argument is not a valid MySQL-Link resource in **/var/www/html/paternity/t_o_index.php** on line **63**

Warning: Access denied for user: 'root@localhost' (**Using password**: NO) in **/var/www/html/paternity/t_o_index.php** on line **130**

Warning: MySQL Connection Failed: Access denied for user: 'root@localhost' (**Using password**: NO) in **/var/www/html/paternity/t_o_index.php** on line **130**

Warning: Supplied argument is not a valid MySQL-Link resource in **/var/www/html/paternity/t_o_index.php** on line **131**

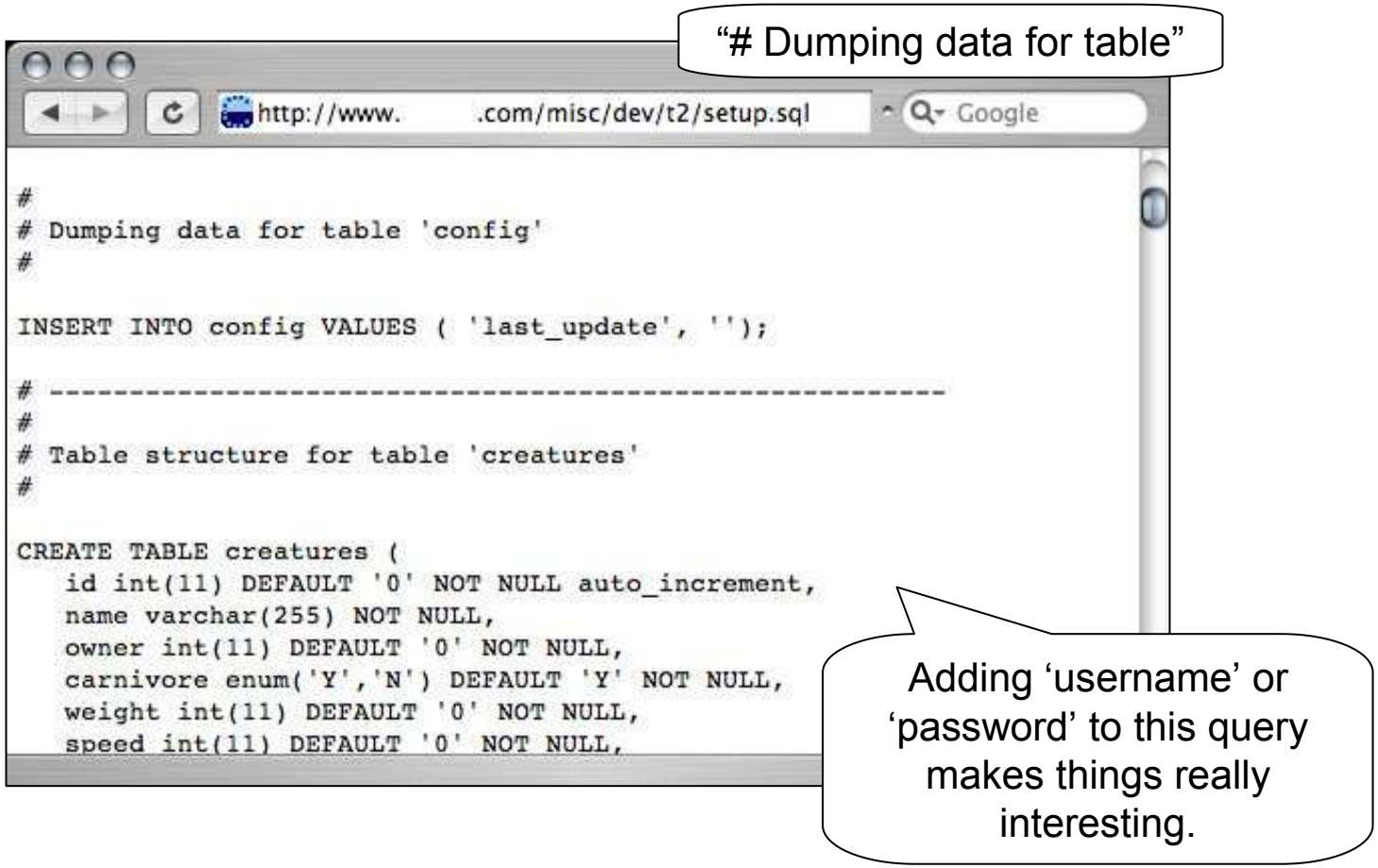
Warning: Supplied argument is not a valid MySQL-Link resource in **/var/www/html/paternity/t_o_index.php** on line **168**

Warning: Supplied argument is not a valid MySQL result resource in **/var/www/html/paternity/t_o_index.php** on line **170**

Warning: No MySQL-Link resource supplied in **/var/www/html/paternity/t_o_index.php** on line **220**

SQL Schemas

- Entire SQL Database dumps



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
```

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"

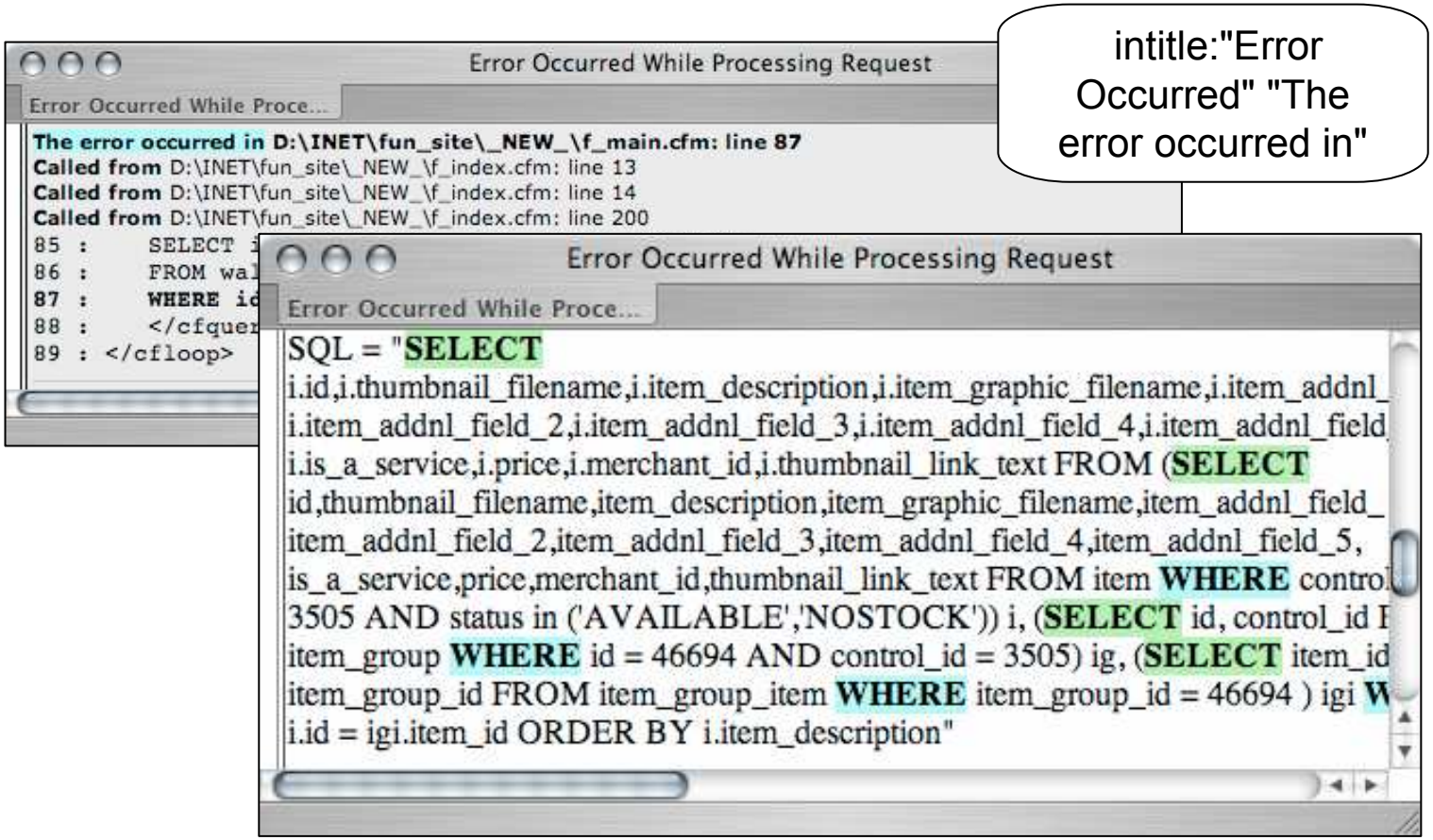
– Our Apologie

– 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.



intitle:"Error Occurred" "The error occurred in"

Going after SQL passwords

http://216.239.41.1...ysql_connect&hl=e

http://216.239.41.104/sear...

```
<?php
$host="[redacted]";
$user="cs3projo";
$password-="tTnM76mx5"
$database="cs3projo"

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

filetype:inc intext:mysql_connect

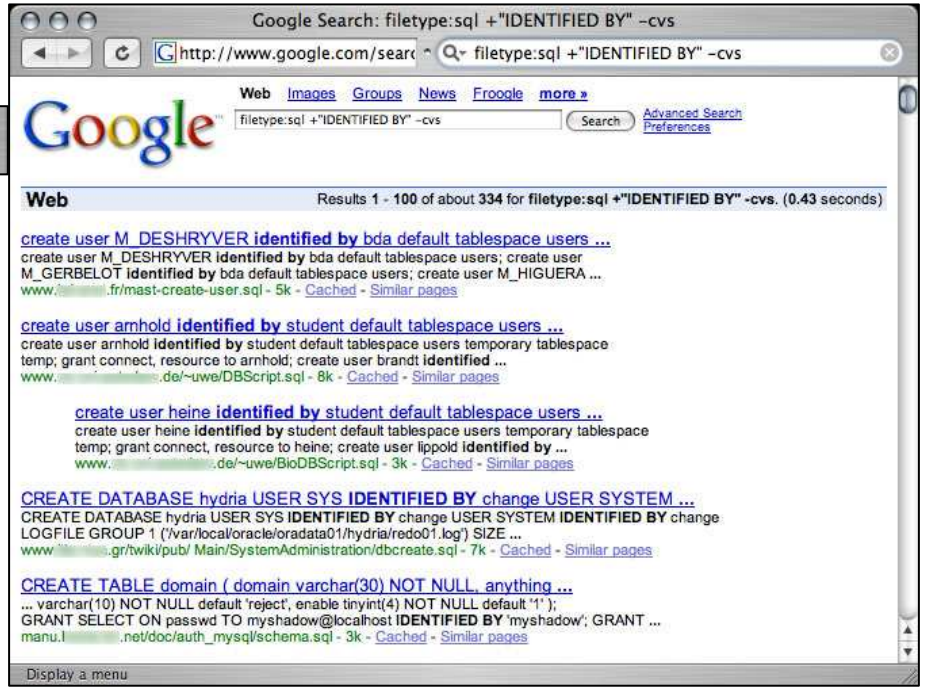
Include files with cleartext passwords…

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…

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.[redacted].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[redacted].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.[redacted].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.[redacted].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 ... pupbld.sql ### **Grant EXECUTE on dbms_pipe** on ...
www.[redacted]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

SQL dump detection

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

Database detection

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

Automation

Page Scraping in Perl
API querying in Perl

Page Scraping with Perl

- Thie 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 aparameter 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($)
{
my ($ourline) = @_;
$hits="";
$index = index($ourline, "of about");
$str = substr($ourline, $index, 30);
@buf=split(//,$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

This piece of code drives all the subroutines.

The socket is initialized…

…the query is sent…

…the total hits are determined…

```
socketInit();
$string = sendQuery($query);
$totalhits = getTotalHits($string);

#Printing to STDOUT the Total Hits Retrieved from Google
print ($totalhits);
```

…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.

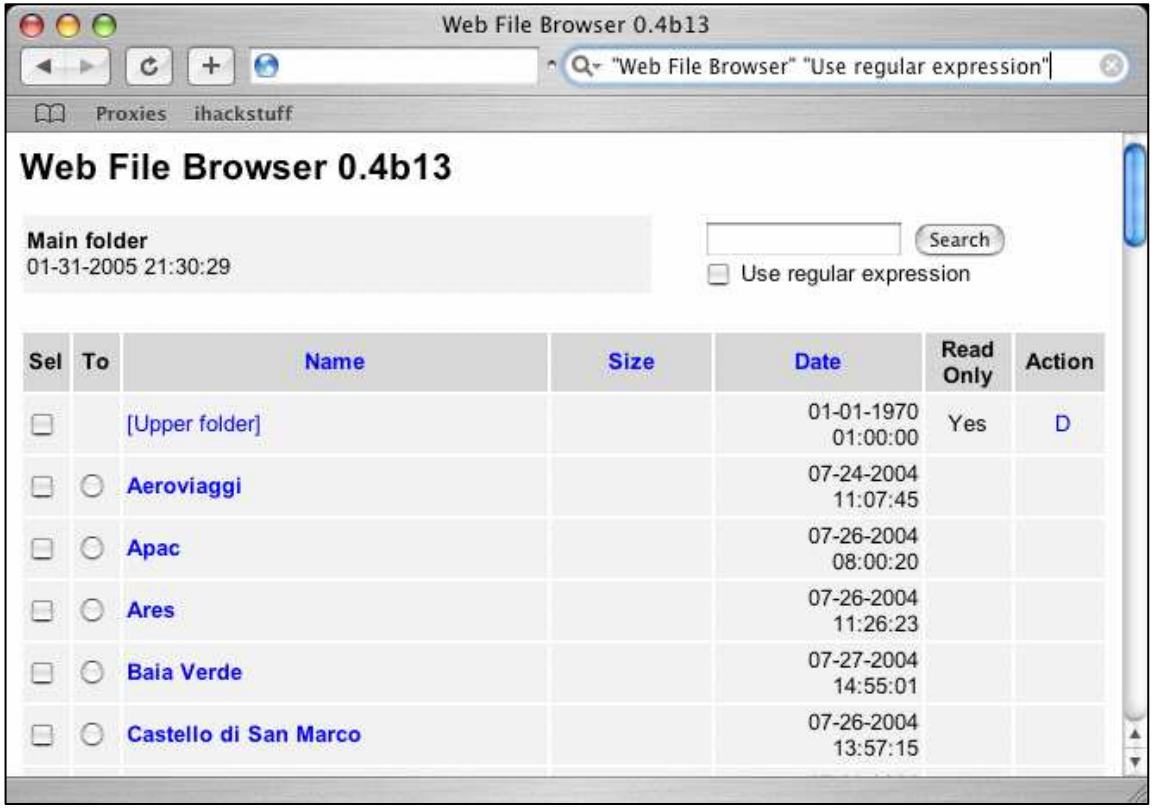
```
intitle:index.of /iisadmpwd/
intitle:index.of /iisadmpwd/achg.htr
intitle:index.of /iisadmpwd/aexp.htr
intitle:index.of /iisadmpwd/aexp2.htr
intitle:index.of /iisadmpwd/aexp2b.htr
```

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.

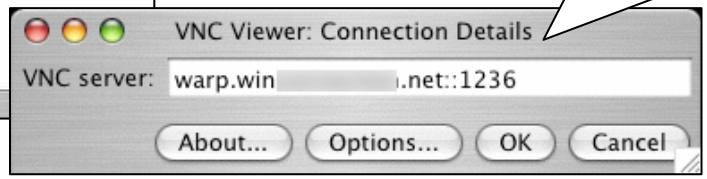


VNC Servers (with client)

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

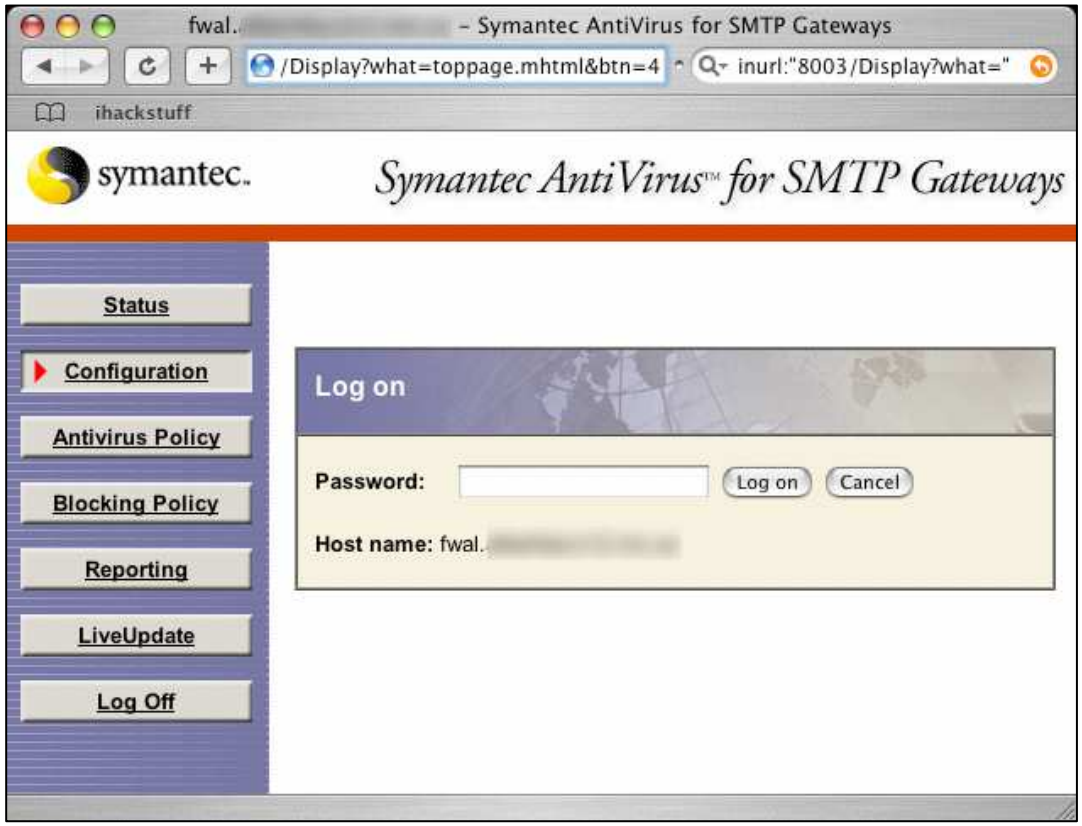
The search is very basic

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



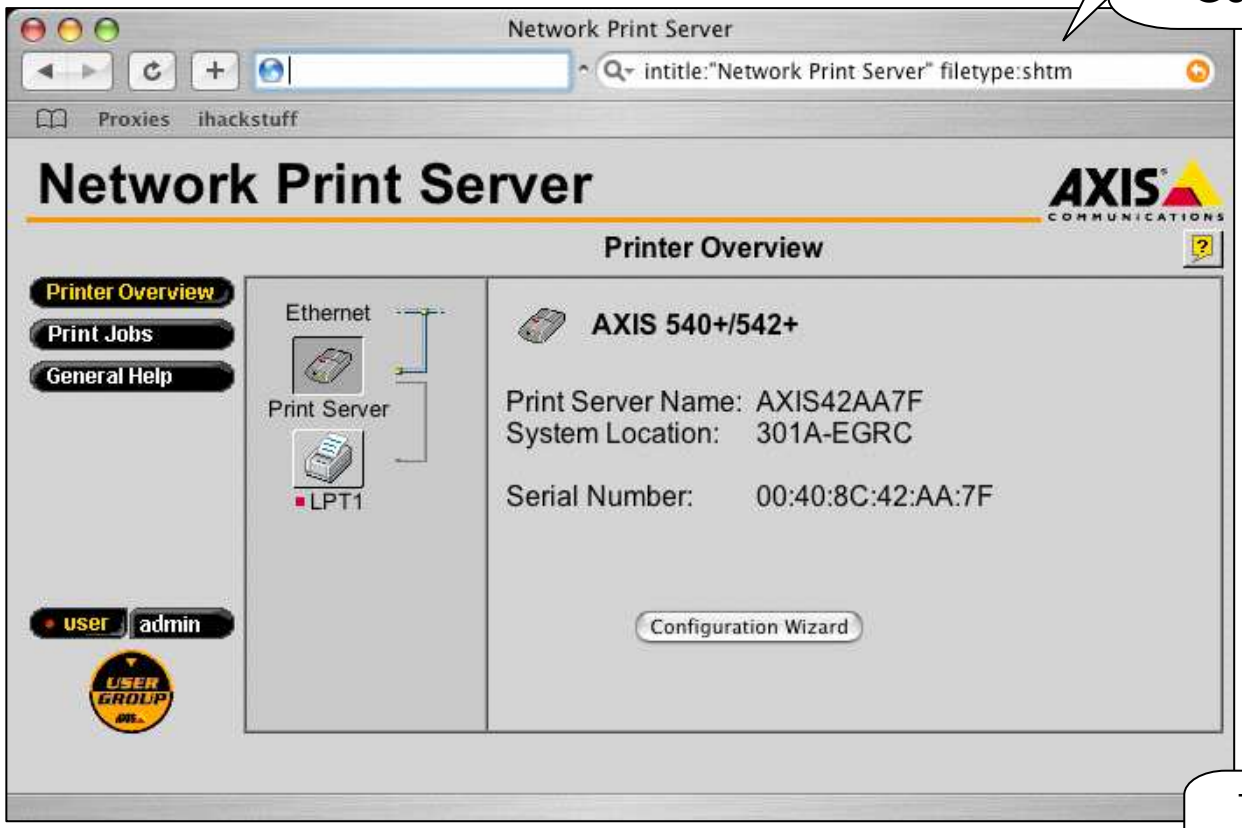
Thanks to lester for this one!

Symantec Anti-Virus SMTP Gateways



Axis Print Servers

Print server administration, Google-style!



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!

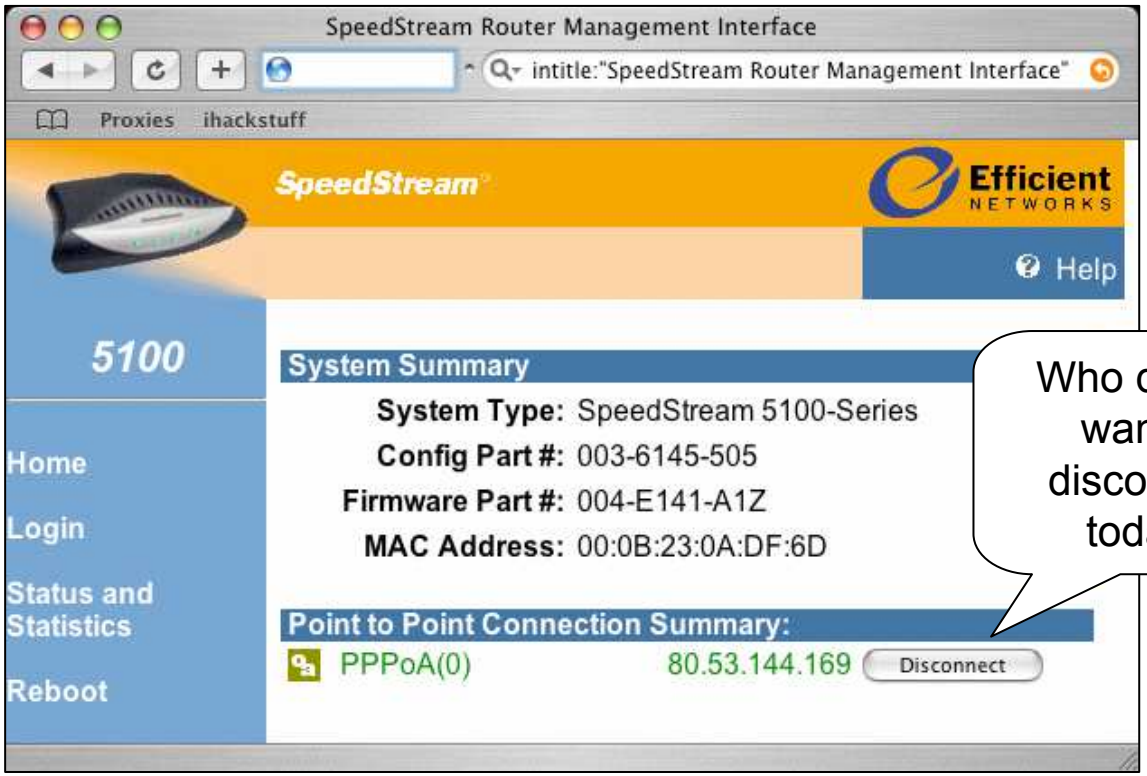
Toshiba Network Cameras

intitle:"toshiba network camera - User Login"

Found by WarriorClown!

Speedstream DSL Routers

- Home broadband connectivity… Googled.

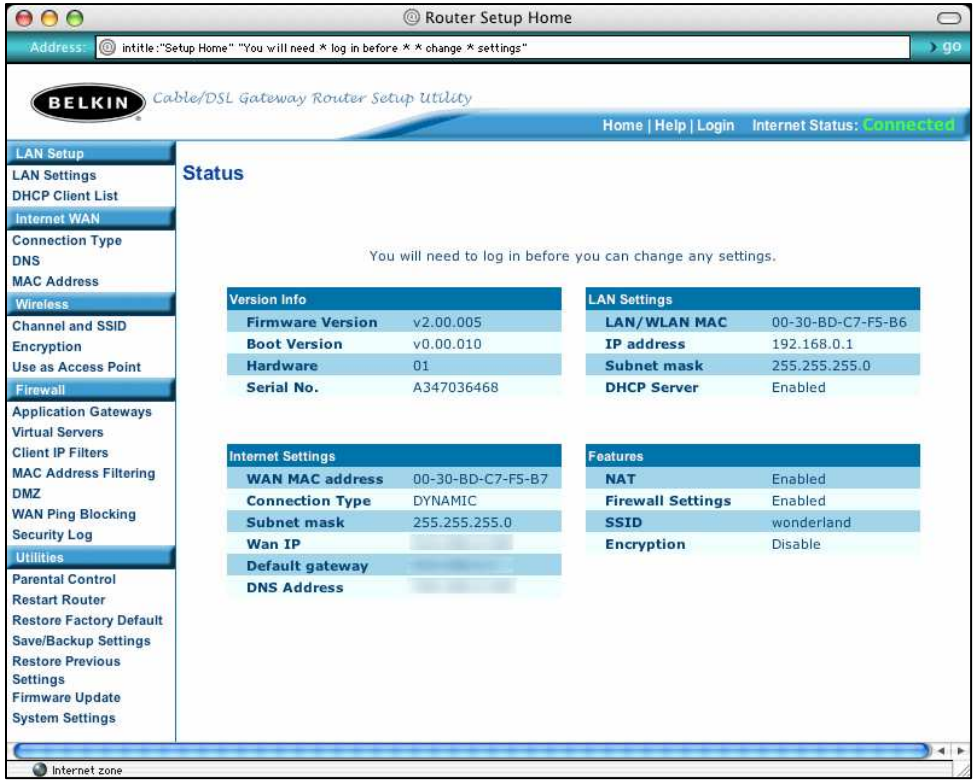


Who do you want to disconnect today?

Found by m00d!

Belkin Routers

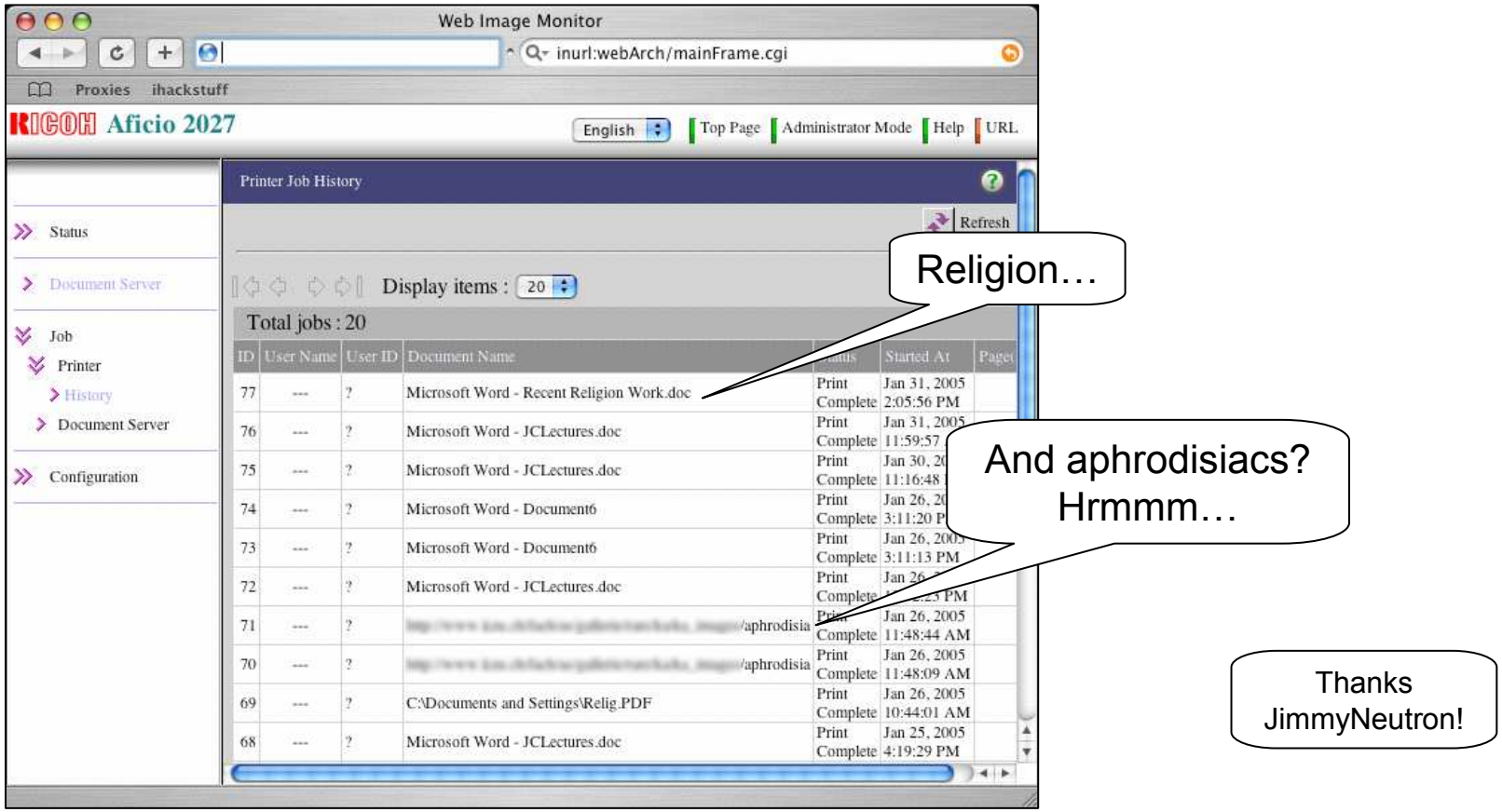
- Belkin routers have become a household name in connected households. The management interface shouldn't show up on Google… but it does.



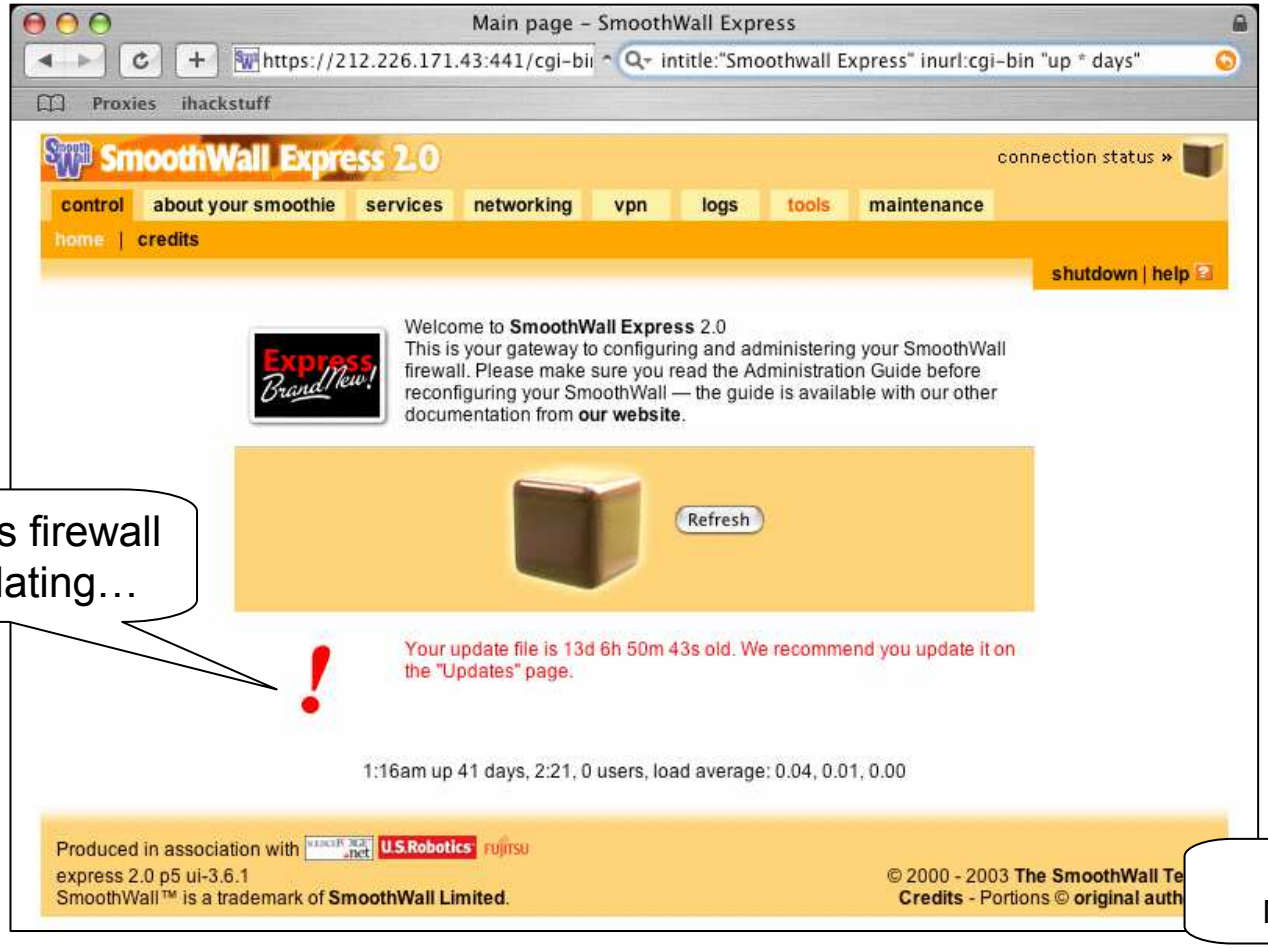
Thanks to darksun for this one!

Printers

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



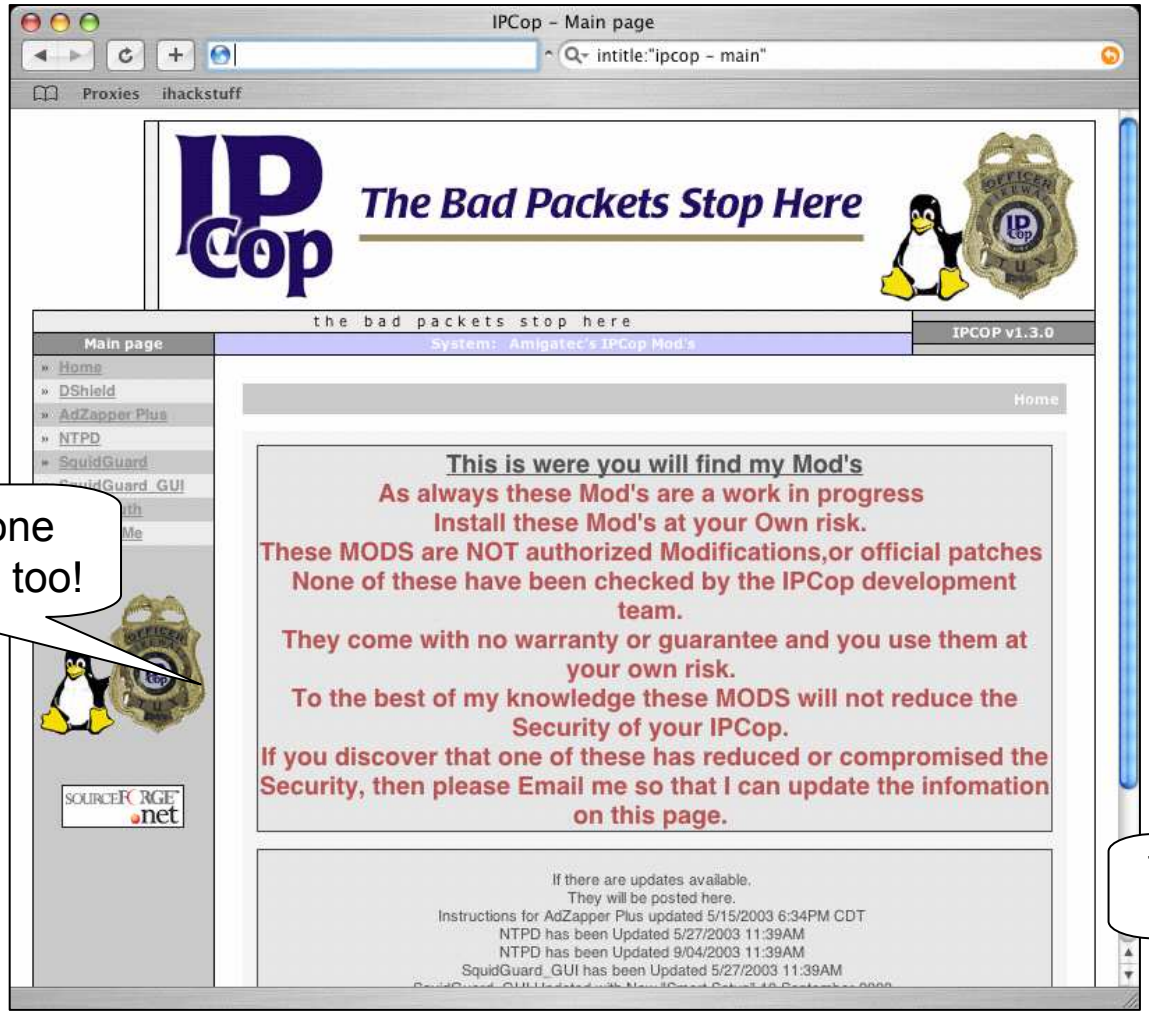
Firewalls - Smoothwall



Uh oh… this firewall needs updating…

Thanks Milkman!

Firewalls - IPCop

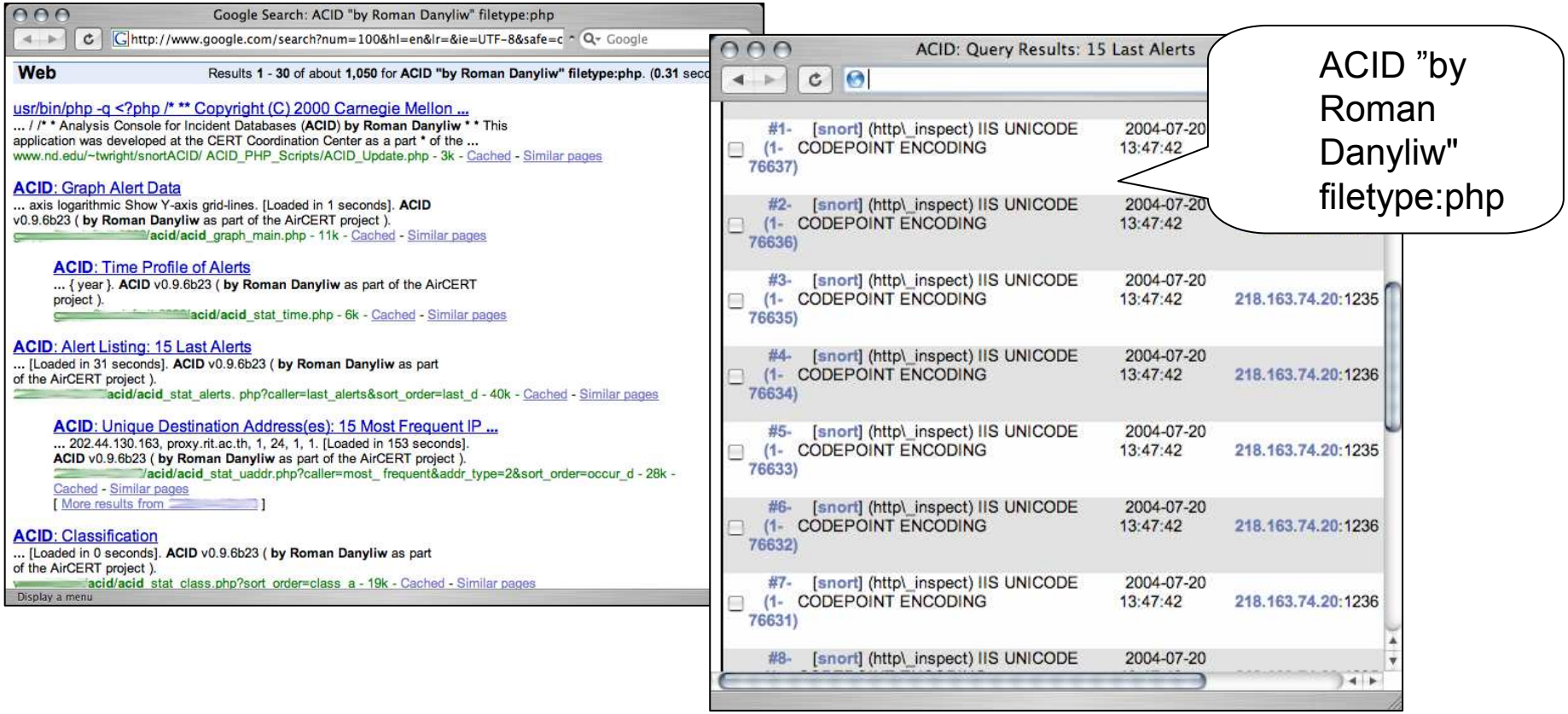


Uh oh… this one needs updating too!

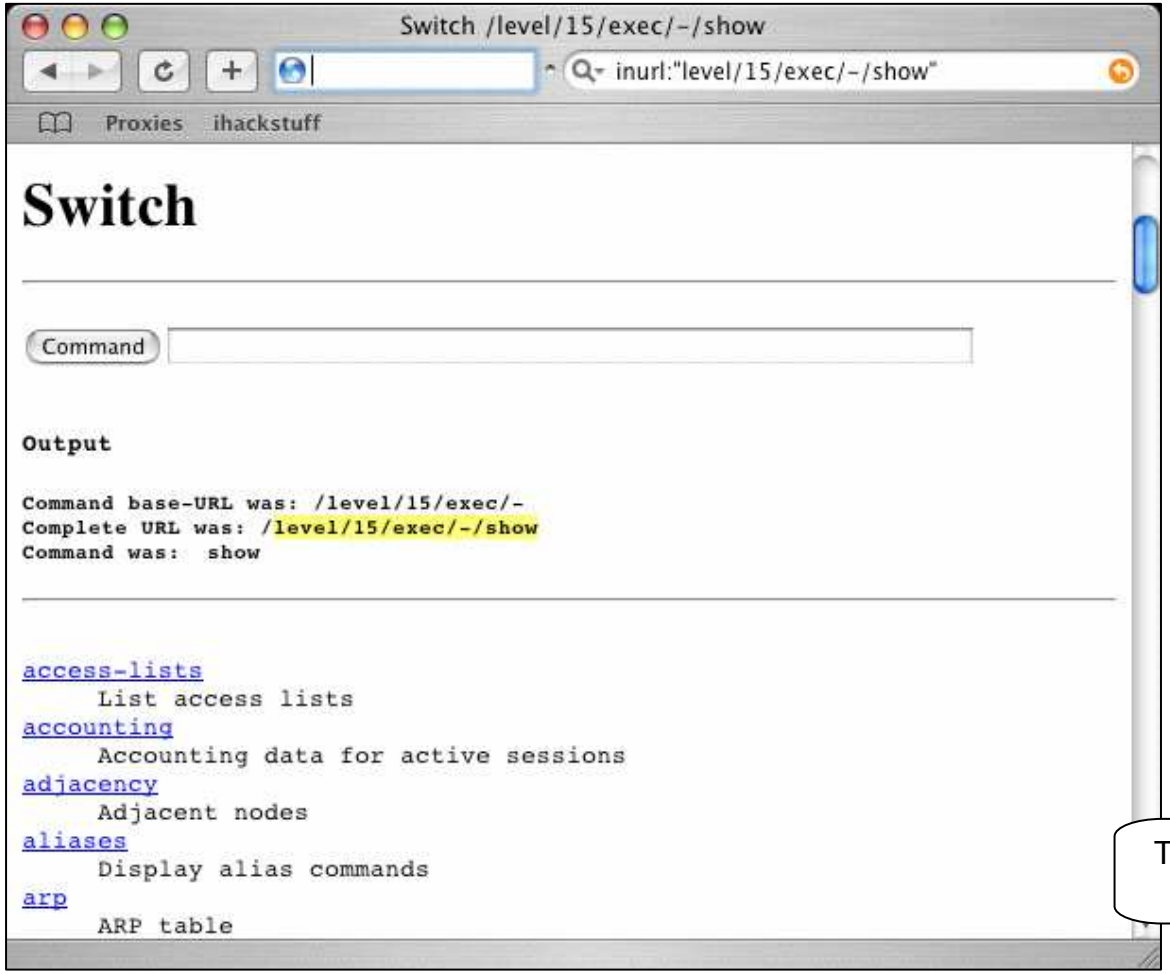
Thanks Jimmy Neutron!

IDS Data: ACID

- SNORT IDS data delivered graphically, served up fresh

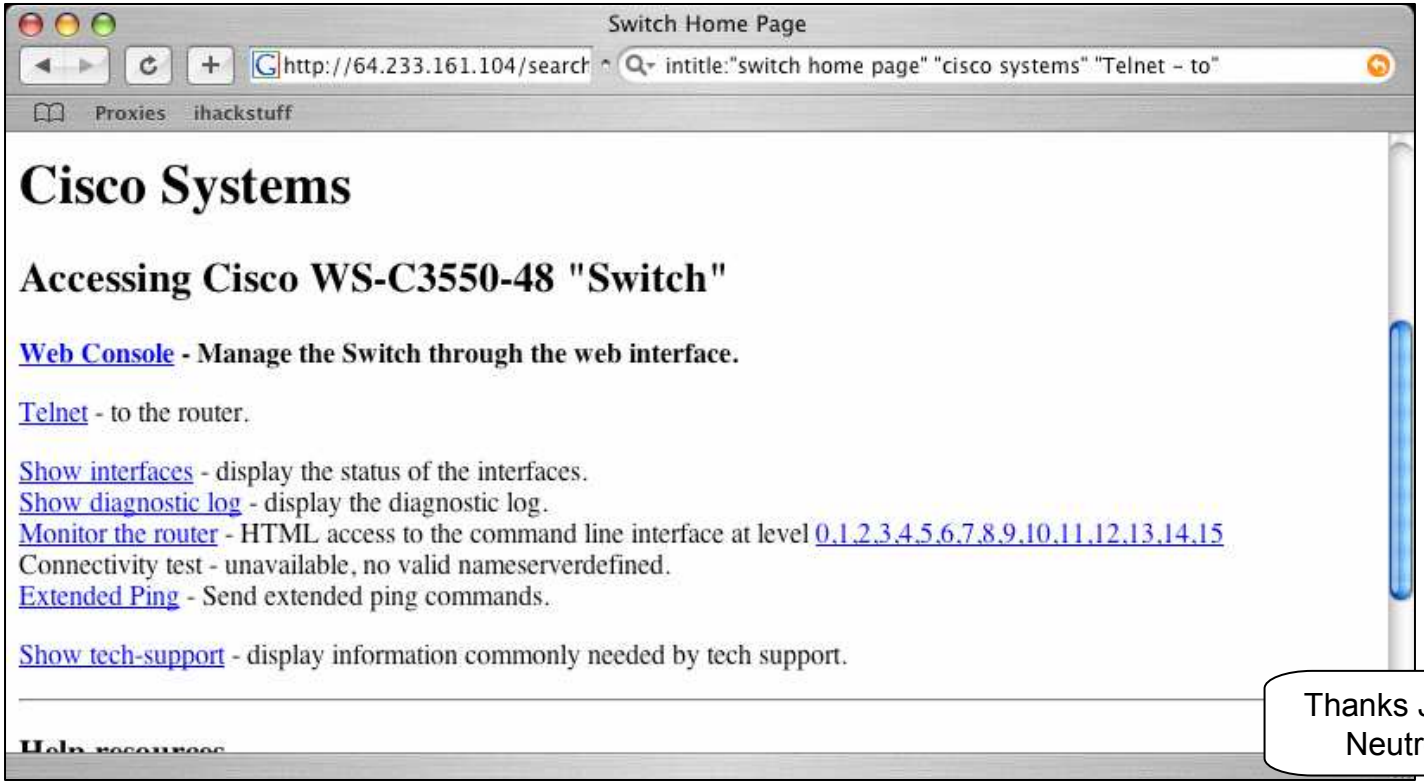


Open Cisco Devices



Thanks Jimmy Neutron!

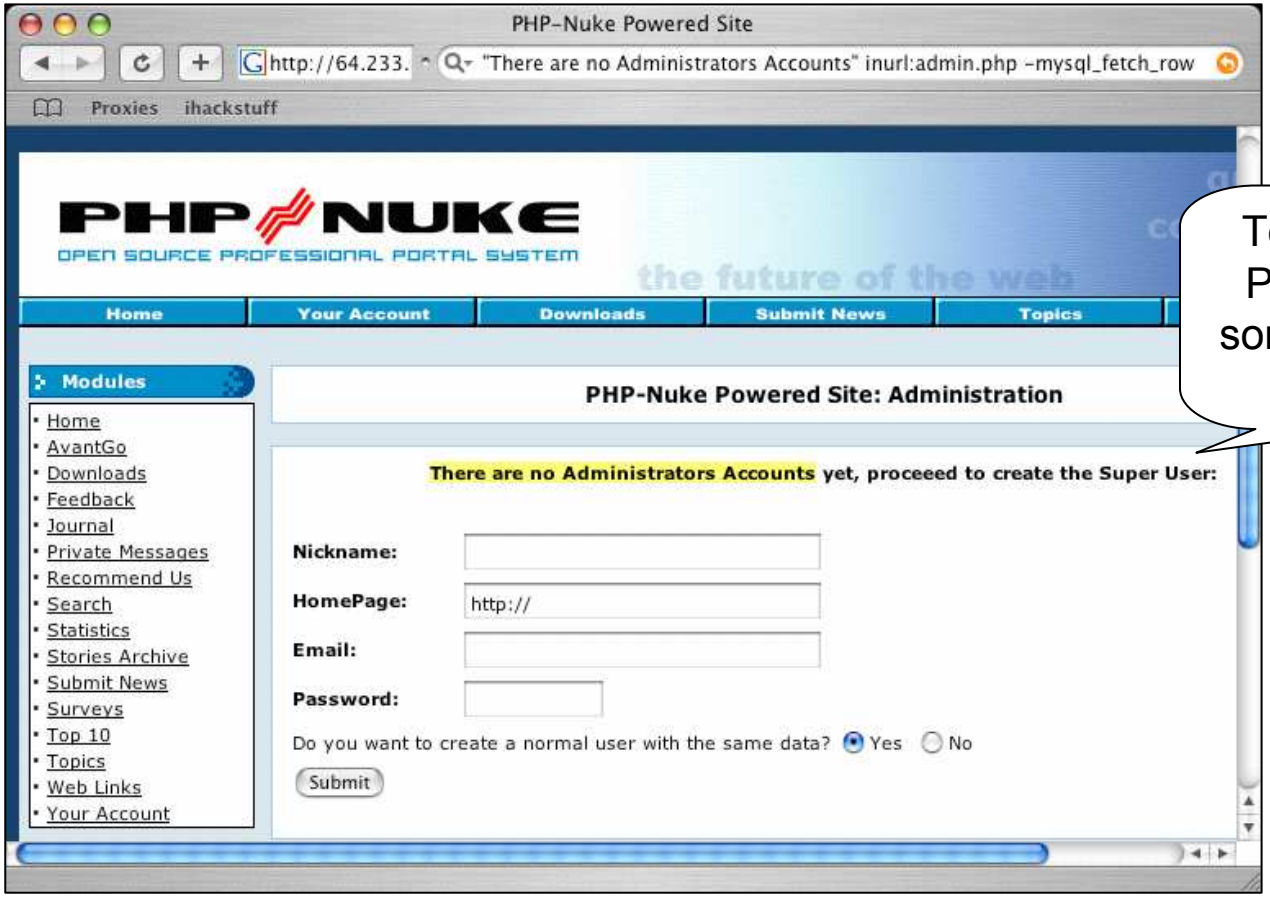
Cisco Switches



Thanks Jimmy Neutron!

Wide Open PHP Nuke Sites

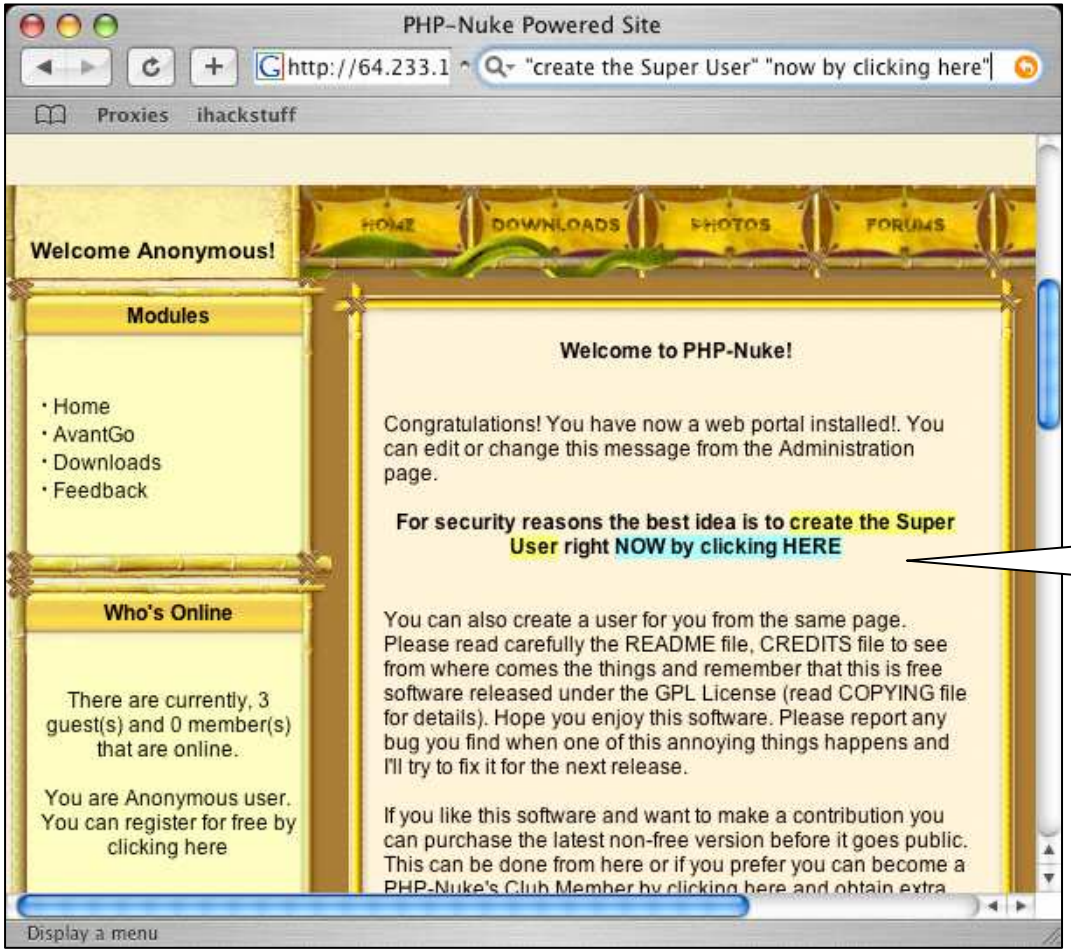
- PHP Nuke allows for the creation of a full-featured web site with little effort.



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

Thanks to arrested for this beauty!

Open PHP Nuke… another way…



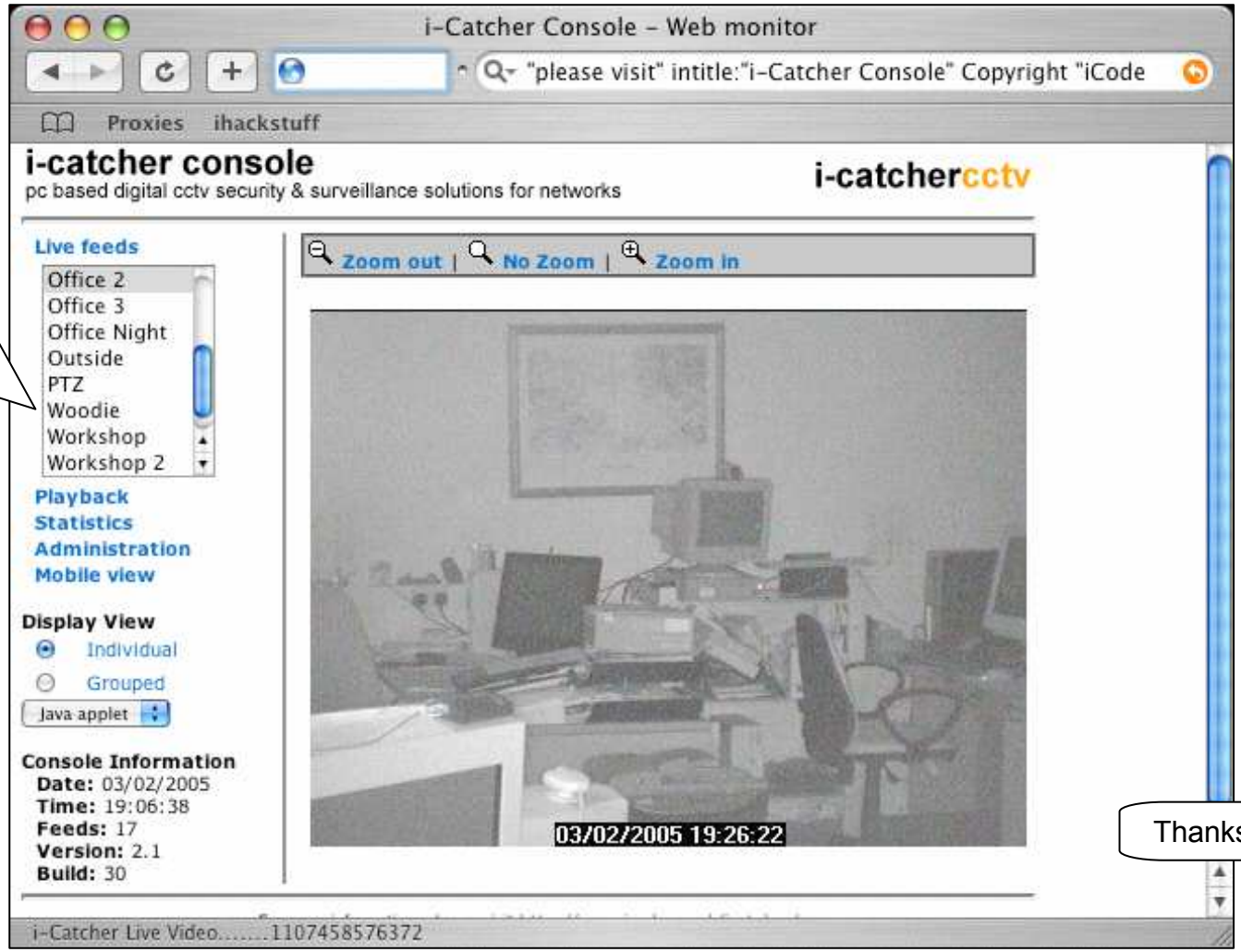
Click here, create superuser!

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!

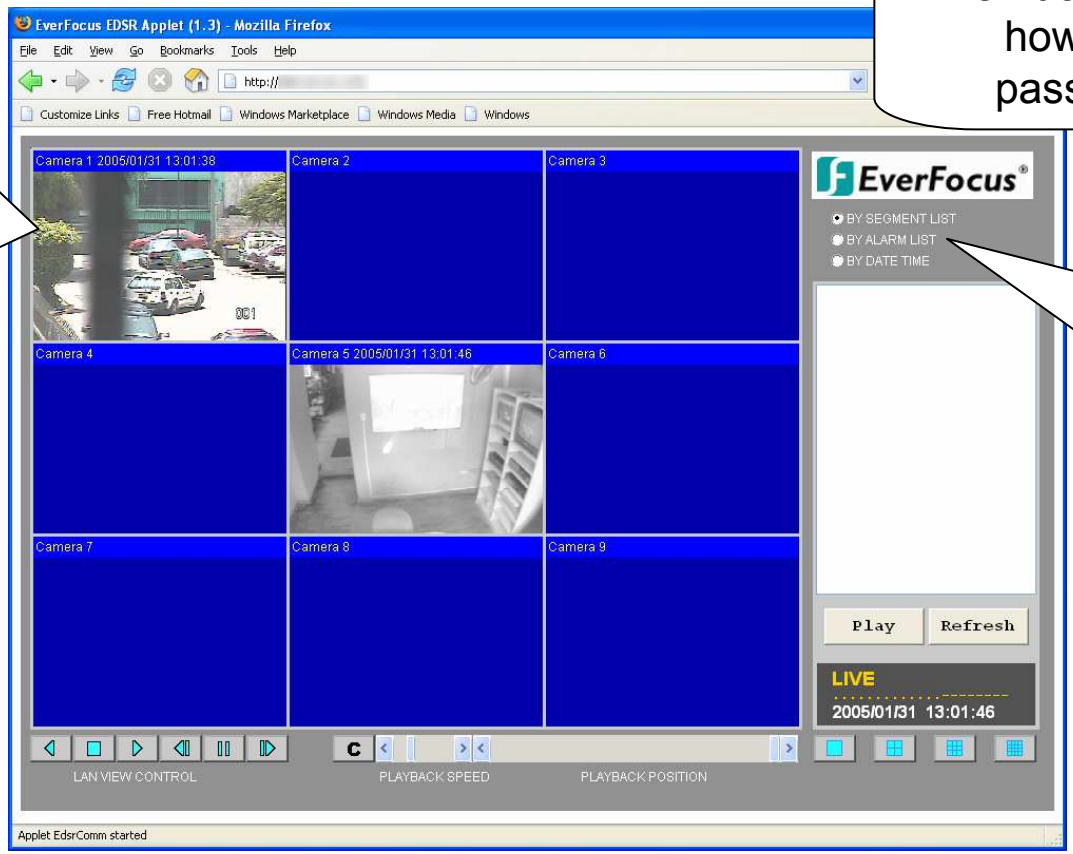
Time-lapse video recorders

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

Time lapse video recorders

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

…multiple live security camera views…

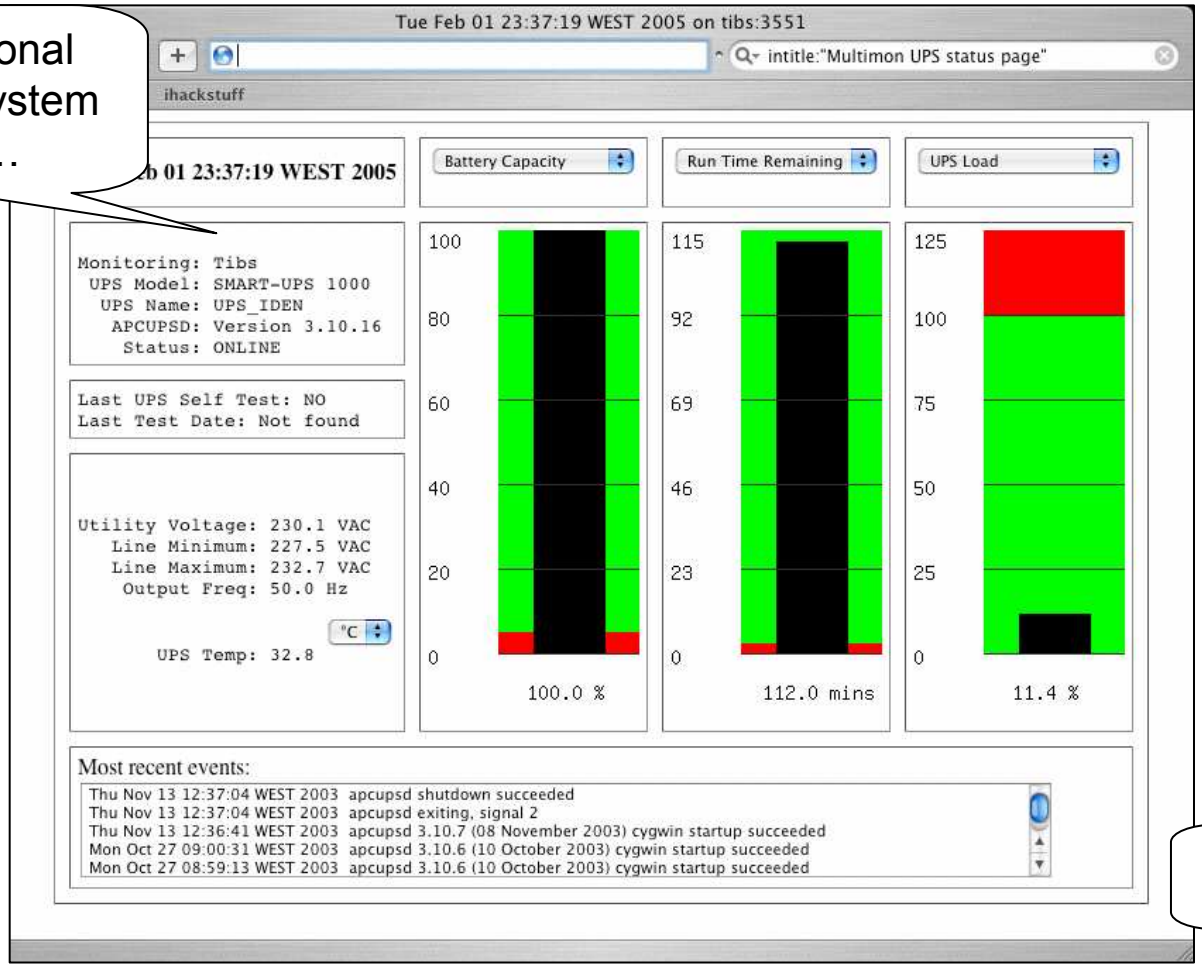


…and historical records of recorded video feeds

Thanks to stonersavant for this beauty!

UPS Monitors

Getting personal with Power System monitors…



Thanks yeseins!

UPS Monitors

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

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 New! 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 - 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=... - 29k - Cached - Similar pages

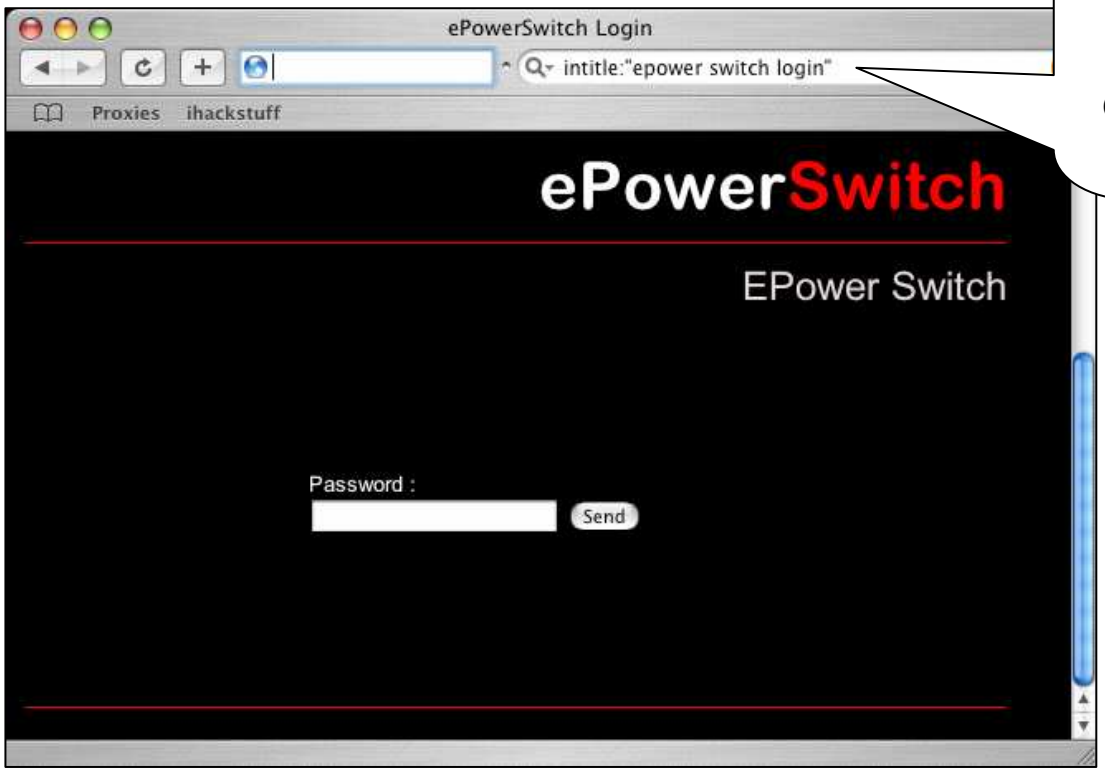
UPS Package Tracking
... Tracking Number. Status. Delivery Information. 1. **1Z** X77 386 03 5395 335 8. Delivered. Delivered on: Aug 4, 2004 3:39 PM. Delivered to: ODESSA, TX, US. ...
wwwapps.ups.com/etracking/tracking.cgi?& TypeOfInquiryNumber=T&HTMLVersion=4.0&InquiryNumber1=... - 29k - Cached - Similar 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=... - 28k - Cached - S

Thanks Digital Spirit!

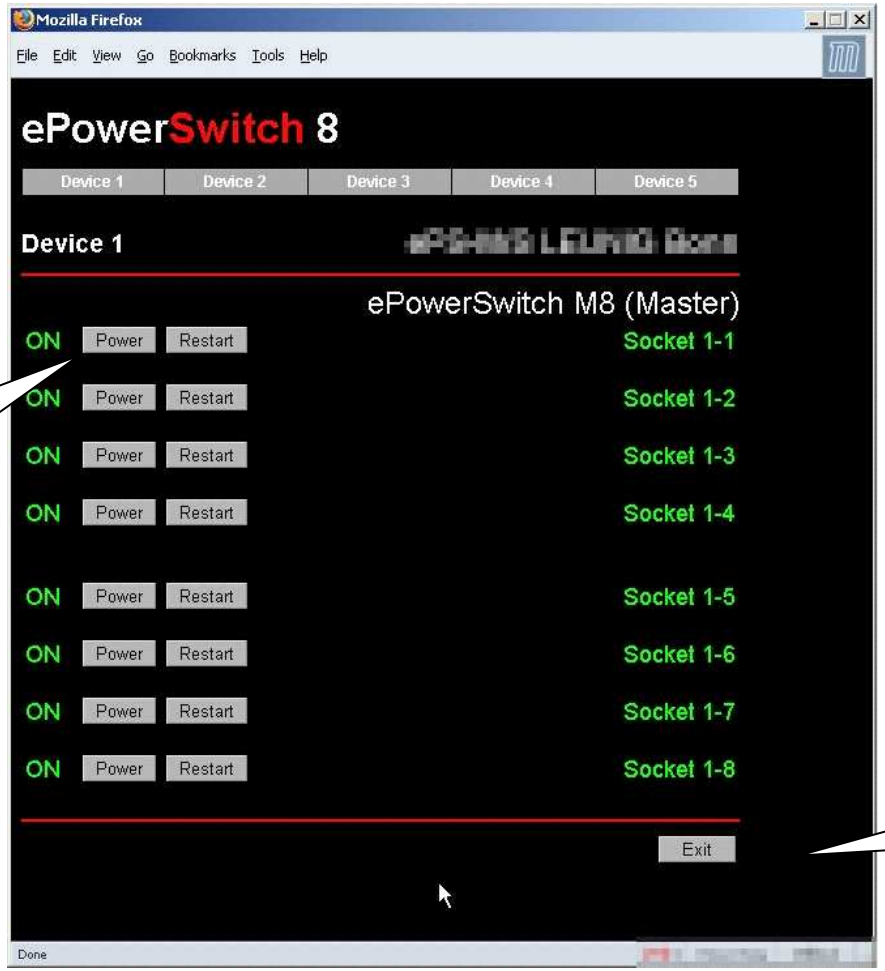
Hacking POWER Systems!

- 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!

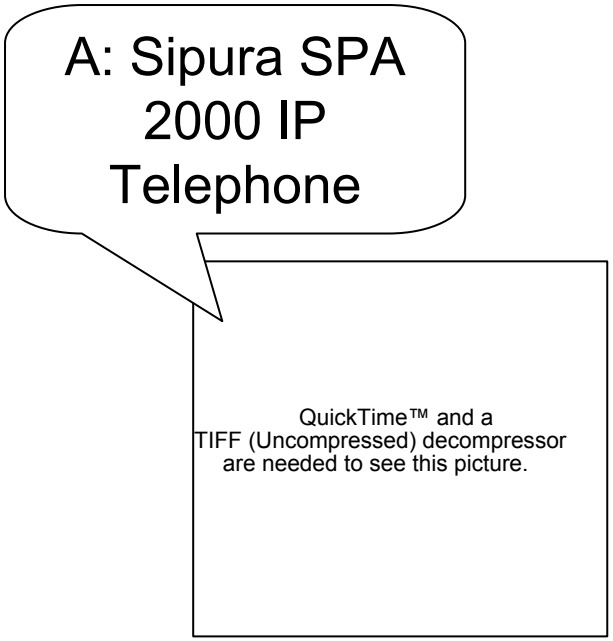


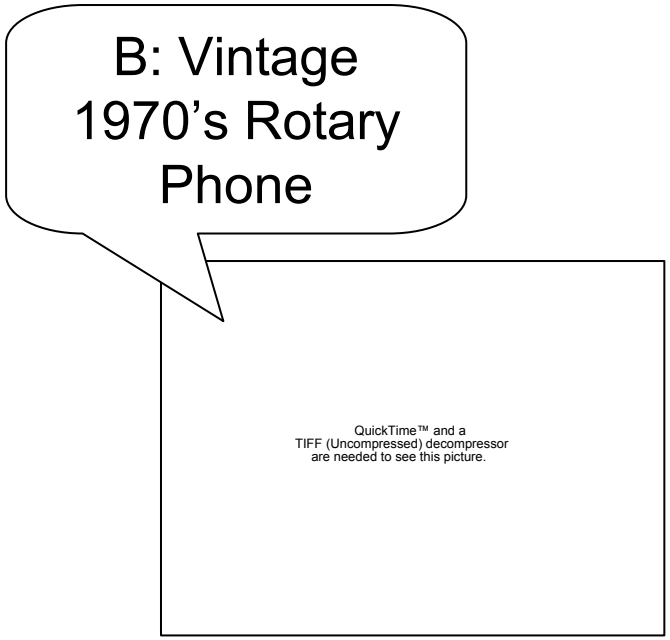
Who do you want to power off today?

Thanks to JimmyNeutron for this beauty!

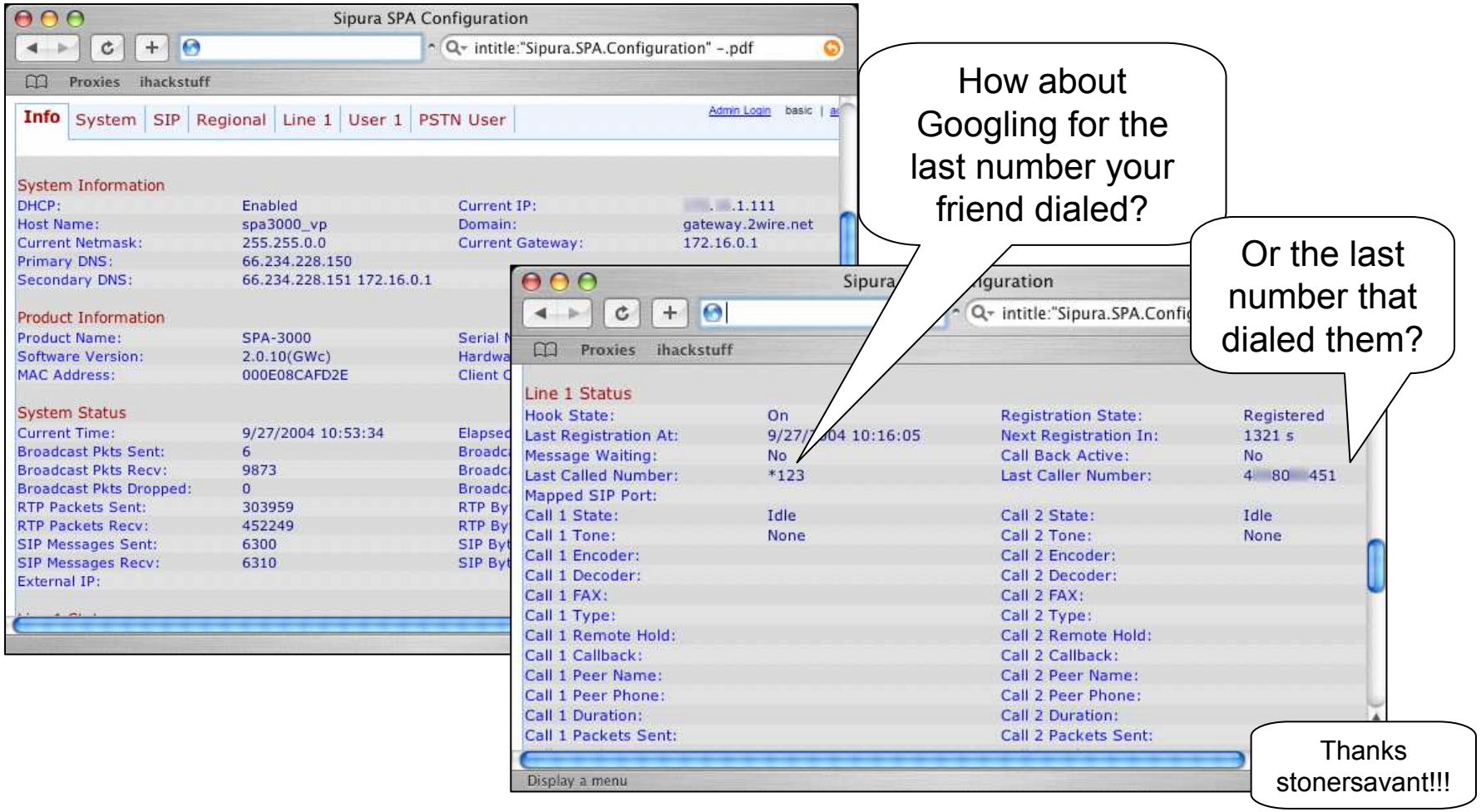
Google Phreaking

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



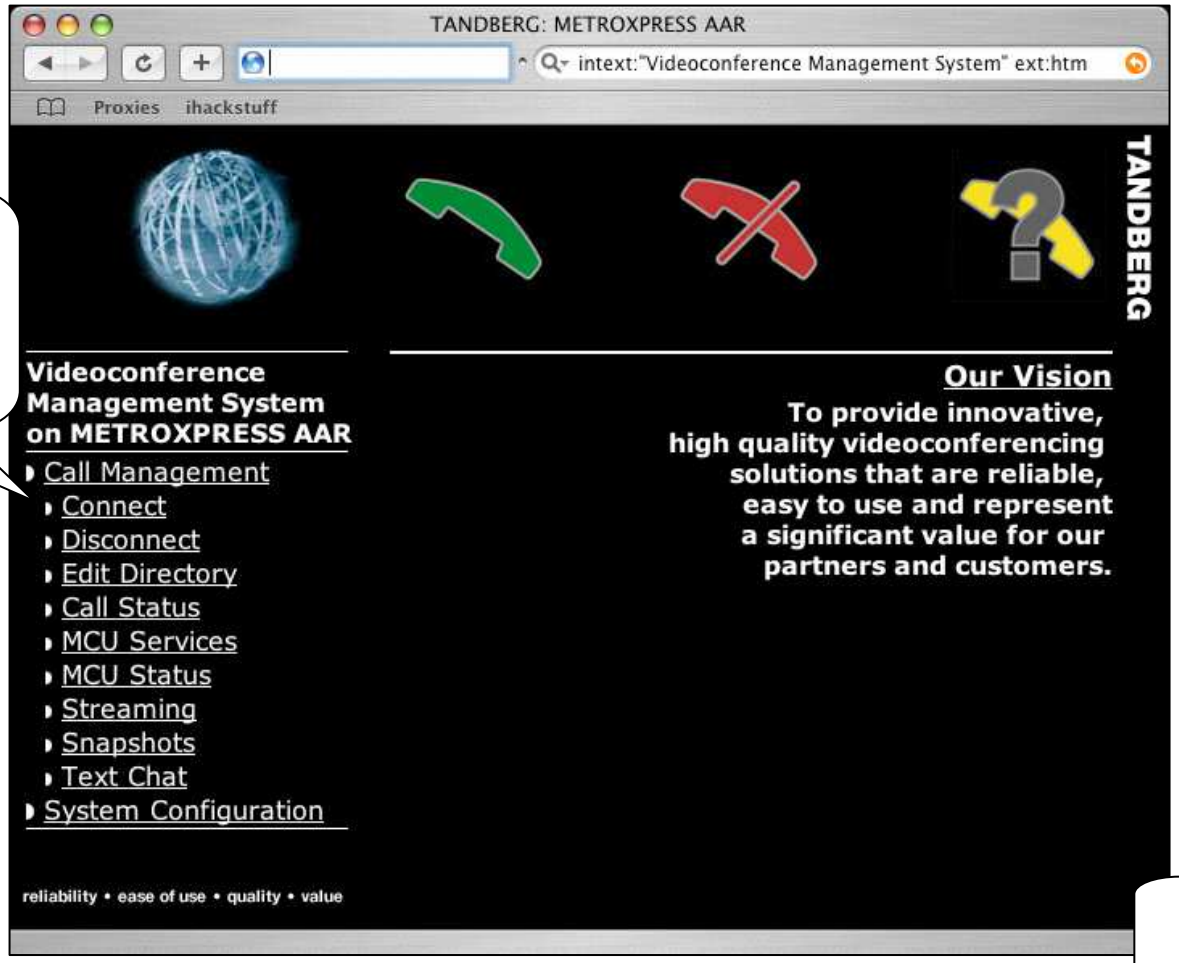


Sipura SPA IP Telephone



Videoconferencing

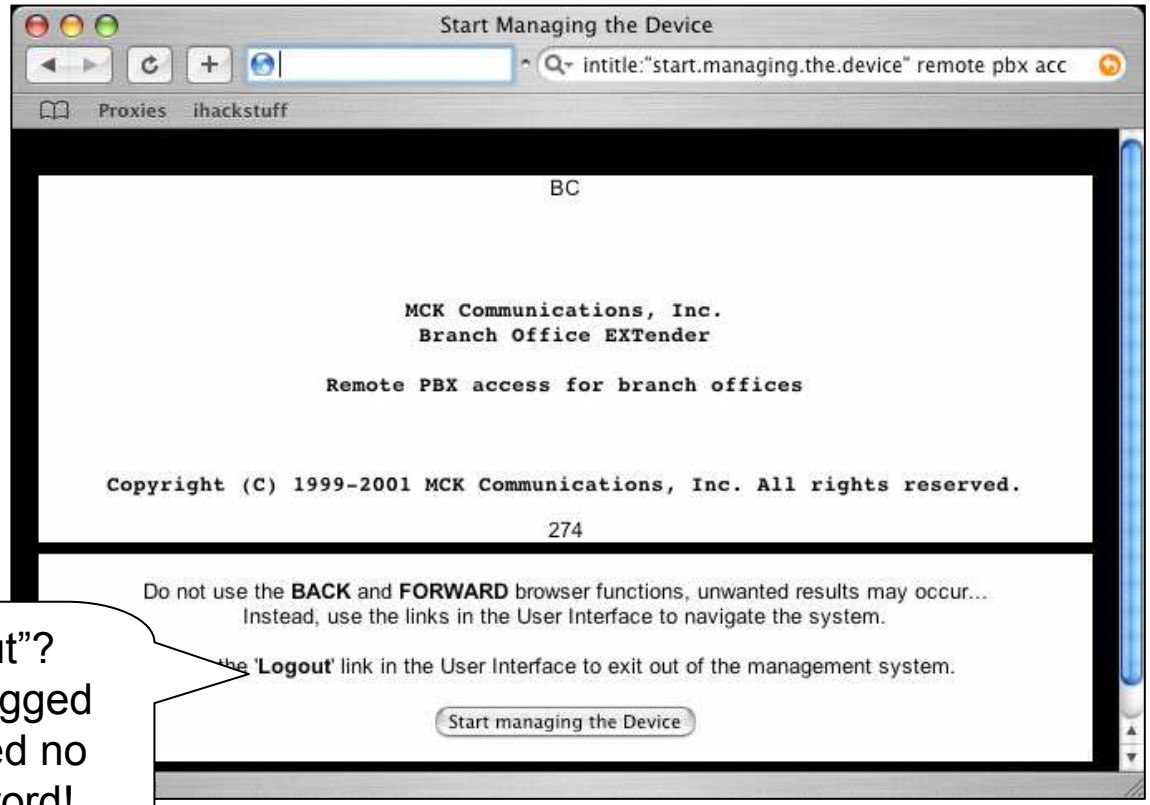
Who do you want to disconnect today?



Thanks yeseins!!!

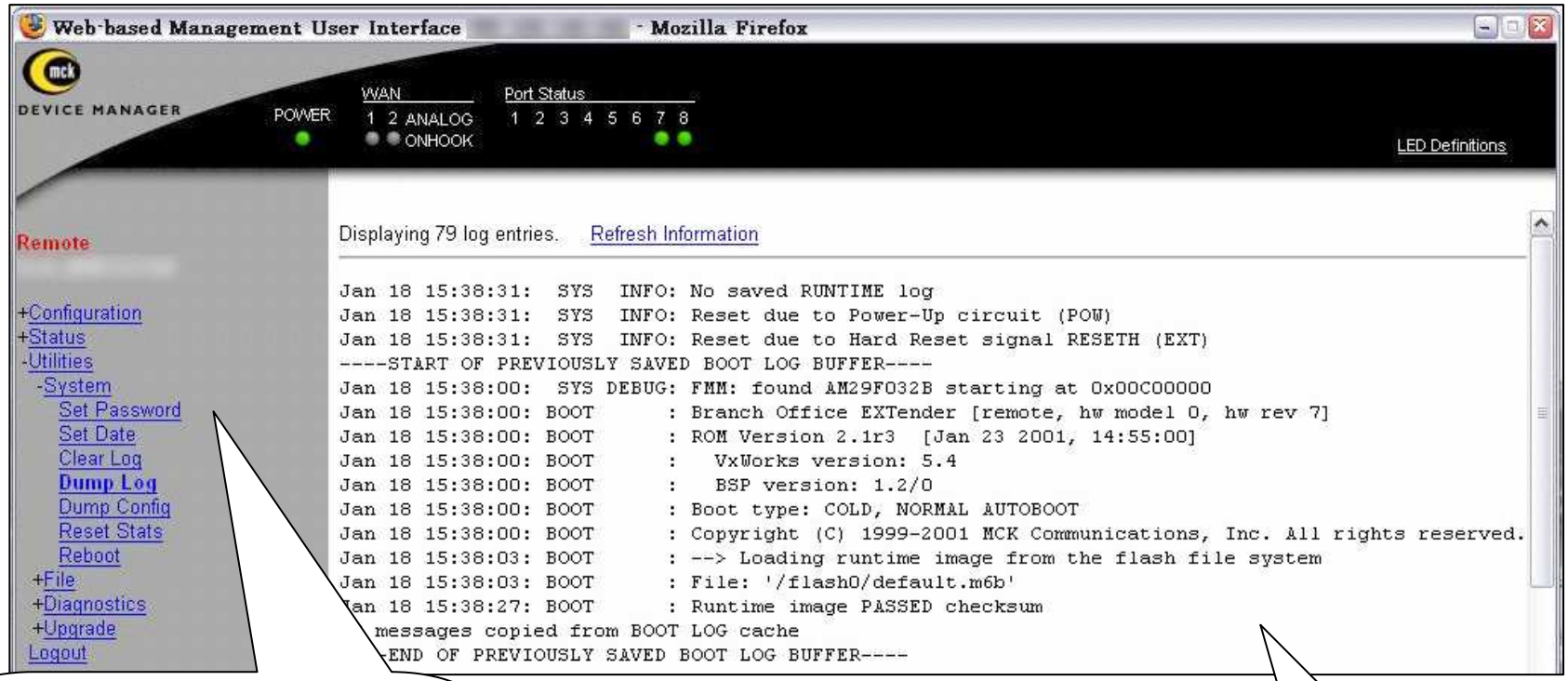
PBX Systems

- 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



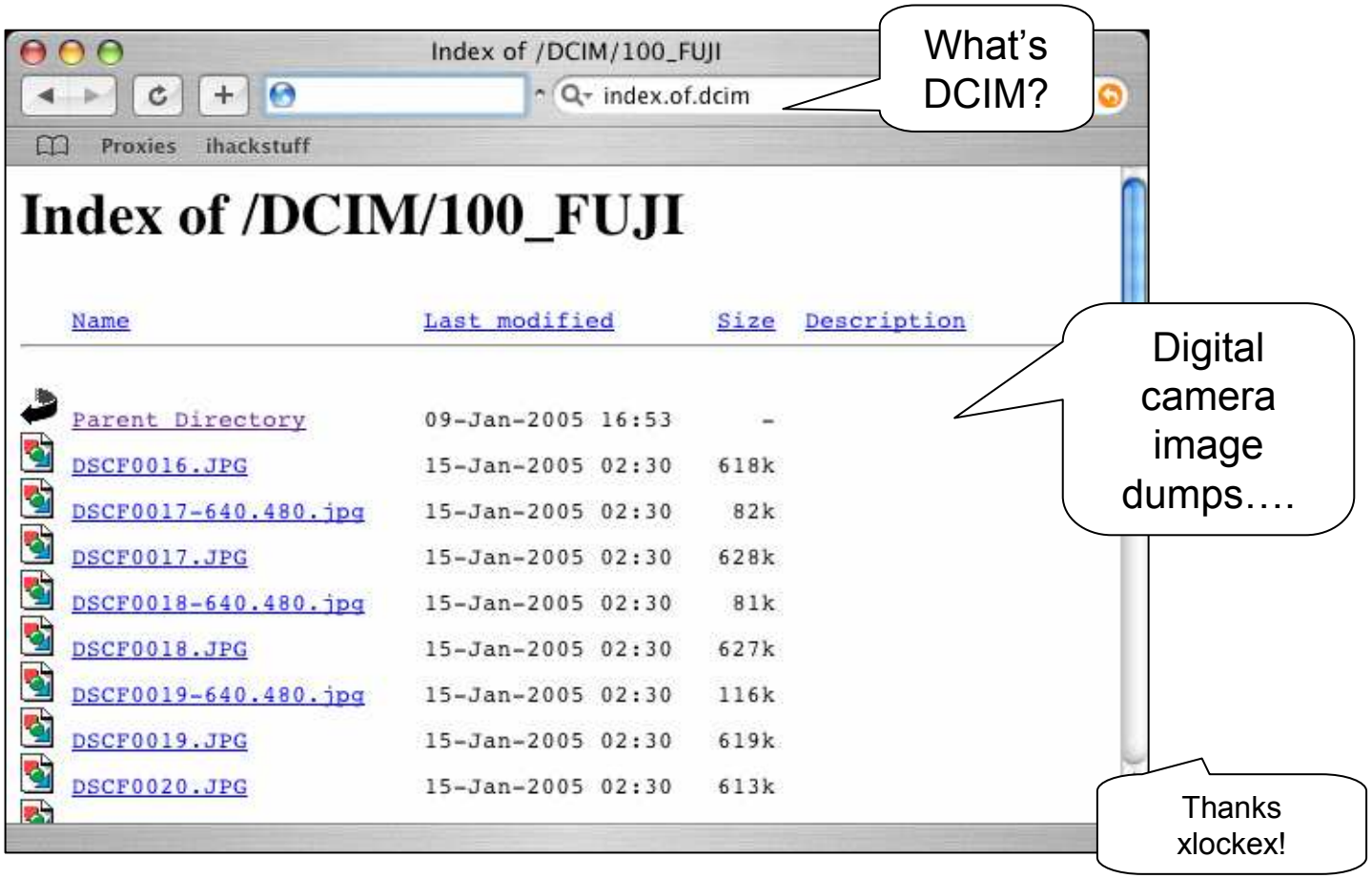
No password required. Even a novice web surfer can become a “PBX hacker”. =)

Thanks to stonersavant for this great find!

Usernames, 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
What's DCIM?
Index of /DCIM/100_FUJI
Name
Last modified
Size
Description
Parent Directory 09-Jan-2005 16:53 -
DSCF0016.JPG 15-Jan-2005 02:30 618k
DSCF0017-640.480.jpg 15-Jan-2005 02:30 82k
DSCF0017.JPG 15-Jan-2005 02:30 628k
DSCF0018-640.480.jpg 15-Jan-2005 02:30 81k
DSCF0018.JPG 15-Jan-2005 02:30 627k
DSCF0019-640.480.jpg 15-Jan-2005 02:30 116k
DSCF0019.JPG 15-Jan-2005 02:30 619k
DSCF0020.JPG 15-Jan-2005 02:30 613k
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 egirl252@hotmail.com</contact>
      <contact>bu be icker_7@hotmail.com</contact>
      <contact>jk co o@hotmail.com</contact>
      <contact>ks no @hotmail.com</contact>
      <contact>jo hu onuteaux@hotmail.com</contact>
      <contact>st ve rmala@hotmail.com</contact>
      <contact>bi ge bitch_4@hotmail.com</contact>
      <contact>rh vi @msn.com</contact>
      <contact>bo ko otmail.com</contact>
      <contact>kw nk man@hotmail.com</contact>
      <contact>pu ep 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 dr dyranch@hotmail.com</contact>
      <contact>to cb @olypen.com</contact>
      <contact>ty er _dog@hotmail.com</contact>
      <contact>re @o pen.com</contact>
      <contact>ga da 651@hotmail.com</contact>
      <contact>je nd 020@aol.com</contact>
      <contact>ab 6 @hotmail.com</contact>
```


Thanks to harry-aac!

Old School! Finger…

http://www.cs.wisc.edu/cgi-bin/finger?timc@tornado

inurl:/cgi-bin/finger? "In real life"

Proxies ihackstuff

```
[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

Google Search: inurl:"GRC.DAT" intext:"password"

http://www. Google

Proxies ihackstuff

Web Images Groups New! News Froogle more »

inurl:"GRC.DAT" intext:"password" Search Advanced Search Preferences

Web Results **1** - **5** of **5** for **inurl:"GRC.DAT" intext:"password"**. (**0.11** seconds)

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

[KEYS] !KEY!=$REGROOT$ LicenseNumber=S00141V-11CQ-1112 Connected ...
... D1 Description=Snav Location=S IPAddress=S10.1.2.110 Subnet=D0 SubnetMask=D0 Type=D2 Login=Scd **Password**=S105F3CD589B39EBDF8120110348 PasswordIsEncrypted=D1 ! ...
www. edu/updates/GRC.DAT - 10k - Cached - Similar pages

[KEYS] !KEY!=$REGROOT$ FullGRCUpdateCounter=D1 LicenseNumber ...
... D1 UpdateNow=D1 SourceCount=D1 Description=S Location=S IPAddress=S Subnet=D0 SubnetMask=D0 Type=D0 Login=S **Password**=S0004F627A3B PasswordIsEncrypted=D1 !KEY ...
Iss. edu/~sara/GRC.DAT - 8k - Cached - Similar pages

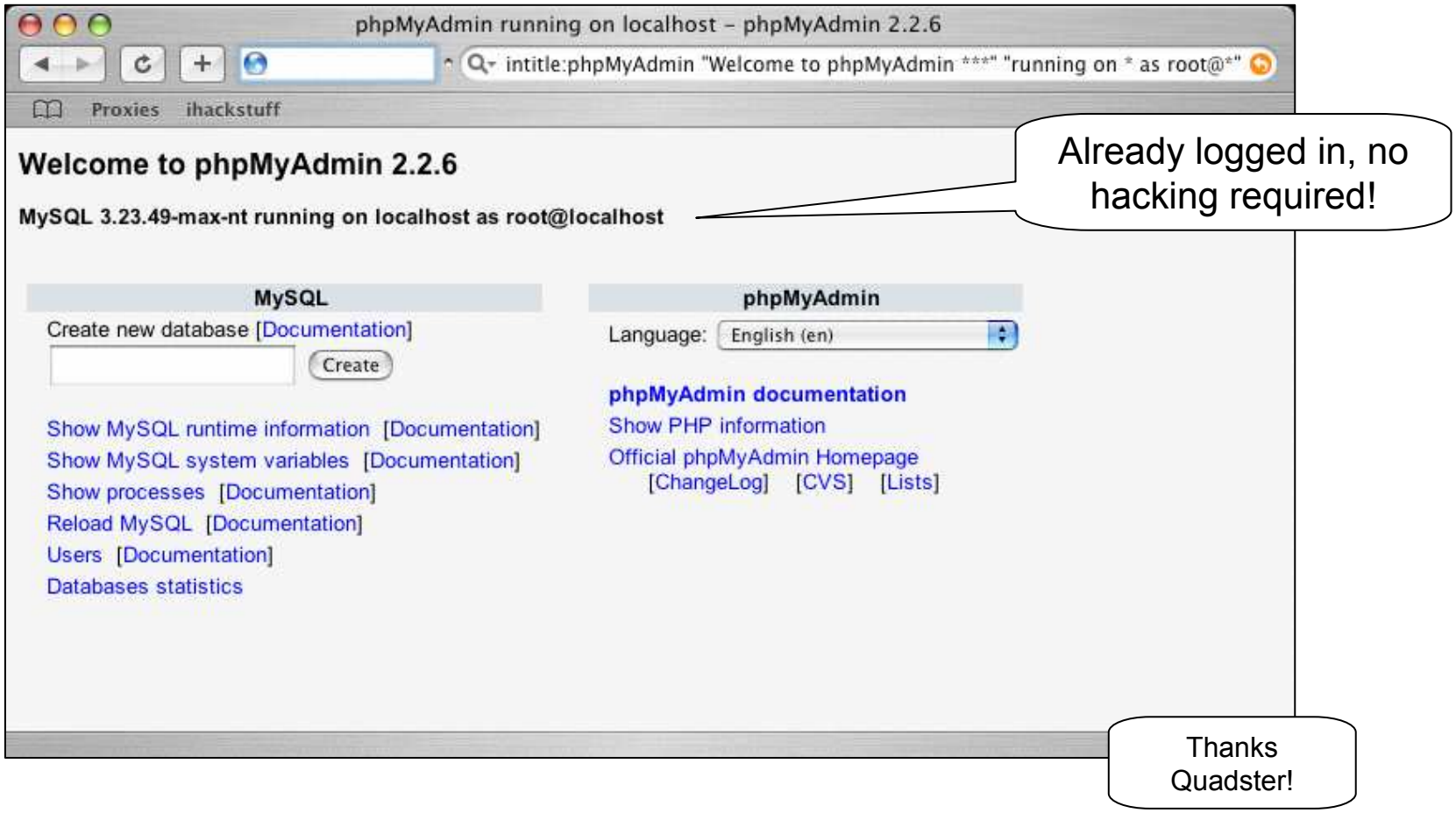
[KEYS] !KEY!=$REGROOT$ FullGRCUpdateCounter=D1 LicenseNumber ...
... 492000=D0 !KEY!=$REGROOT$\LiveUpdateSource Description=Ssoftzone Location=S IPAddress=S\\Softzone\Site-open\Navupdt\ **Password**=S0004F627A3B PasswordIsEncrypted ...
www. ch/services/ pcsupport/anleitungen/virus/GRC.DAT - 7k - Cached - Similar pages

[KEYS] !KEY!=$REGROOT$ FullGRCUpdateCounter=D1 LicenseNumber ...
... Description=S Location=S IPAddress=Spc002.w2.bo.infn.it **Password**= S3118D39BF29E8897D0E0A8A62A16DA73353C31CC83A219A04A456222464 PasswordIsEncrypted= ...
www. it/calcolo/helpdesk/antivirus/GRC.DAT - 5k - Cached - Similar pages

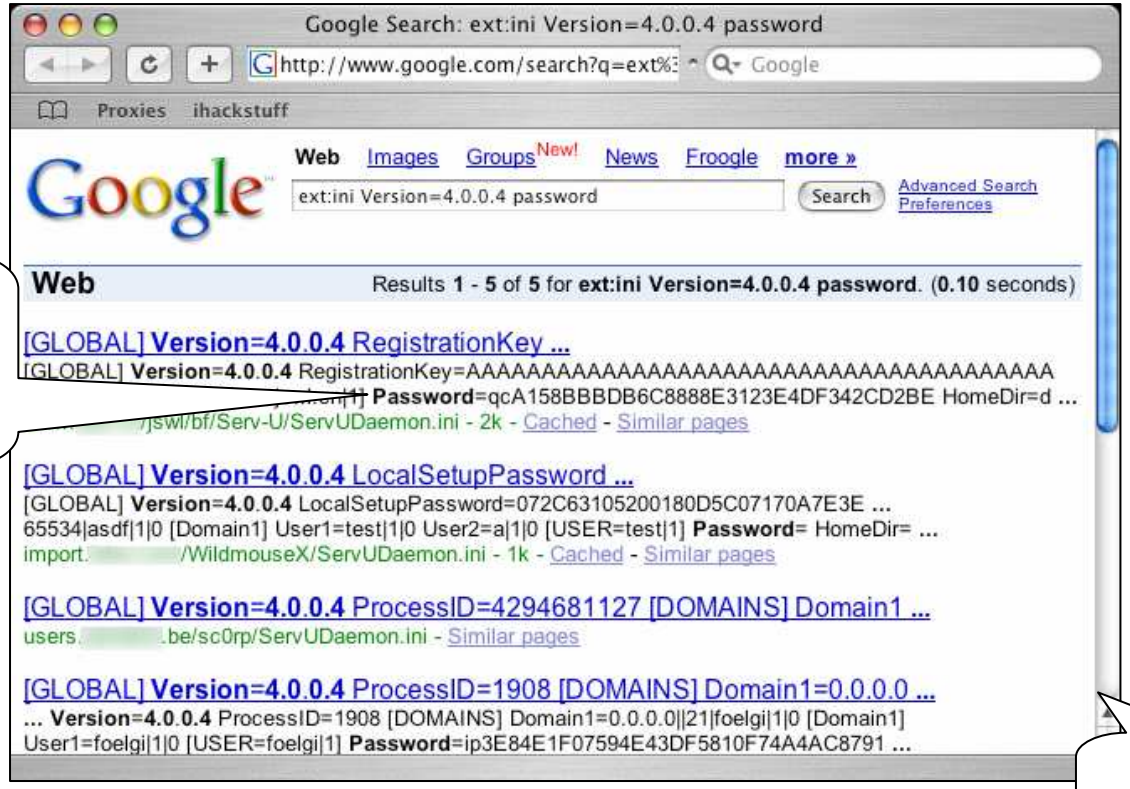
Encrypted, but yummy (and crackable)!

Thanks MILKMAN!

Open SQL servers



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/sea inurl:netscape.ini "Remember Password=yes"

Proxies ihackstuff

```
[Mail]
Check Time=0
POP Name=
Remember Password=yes
POP Password=O6iDK/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!

IPSec Final Encryption Keys

http://64.233.187.104/search?q=cach...tion+key%22+&hl=en&client=firefox-a

http://64.233.187.104/sea ext:log "Final encryption key"

Proxies ihackstuff

```
IP; Final encryption key[16] = 0x9d98d976 863415fe 5a7db2f6 7e768880
IP; IV hash .= g^xi[128] = 0xc22b1613 ee439b8f e1a1cbc8 0635e197 f2c9004e 4
IP; IV hash .= g^xr[128] = 0x977296f7 dffe428e 4da9351c 25a36bde 75f6cb09 0
IP; Output of IV hash[16] = 0x8dc0c413 0f7bed0c f1301102 bf03381e
IP; HASH_I hash .= g^xi[128] = 0xc22b1613 ee439b8f e1a1cbc8 0635e197 f2c900
IP; HASH_I hash .= g^xr[128] = 0x977296f7 dffe428e 4da9351c 25a36bde 75f6cb
IP; HASH_I hash .= CKY-I[8] = 0x1c2fa64d 8700001e
IP; HASH_I hash .= CKY-R[8] = 0xf7b61f69 a1ac09ea
IP; HASH_I hash .= SAi_b[1248] = 0x00000001 00000001 000004d8 00010824 1c2f
IP; Encoding ID = der_asn1_dn(any:0,[0..88]=C=DE, CN=Dipl. Ing. Reinhard Mo
IP; HASH_I hash .= IDii_b[93] = 0x09000000 3057310b 30090603 55040613 02444
IP; Output of HASH_I hash[20] = 0x366d1353 a2722990 0d71b2cd 70ac9eda 7d283
IP; Asyncronous public key operation started
IP; Restart packet
IP; Version = 1.0, Input packet fields = 0052 KE CR NONCE
IP; Encode pac version = 1.0, flags = 0x00000001
IP; Encod cket[93] = 0x09000000 3057310b 30090603 55040613 02444531
ding = 4, data[869] = 0x30820361 308202ca a0030201 020
] = 0x6f90b7d1 93a498fa e21422c0 0eceaa41 ec9ec230 b
proto = 1, type = 24578, spi[16] = 0x1c2fa64d
```

I only skimmed ‘Applied Cryptography’.. But this looks bad…

Thanks MILKMAN!

Explorer. EXPLORER!?!?!

http://64.233.187.104/search?q=cac..._Directory)&hl=en&client=firefox-a

inurl:explorer.cfm inurl:(dirpath|This_Directory)

Proxies ihackstuff

C:\WINNT\system32\

	Name	Size	Modified date	
[File]	$winnt$.inf	666	04/30/2000 08:47:11 PM	Delete
[Dir]	.	0	04/10/2004 04:48:34 AM	
[Dir]	..	0	04/10/2004 04:48:34 AM	
[File]	12520437.cpx	2151	03/29/2002 04:32:58 PM	Delete
[File]	12520850.cpx	2233	03/29/2002 04:32:58 PM	Delete
[File]	__MMtmp_	4096	04/20/2000 09:27:09 PM	Delete
[File]	aaaamon.dll	32016	12/07/1999 01:00:00 PM	Delete
[File]	abmsg.dll	8976	11/02/1997 12:18:32 PM	Delete
[File]	access.cpl	67344	12/07/1999 01:00:00 PM	Delete
[File]	accserv.mib	13753	12/07/1999 01:00:00 PM	Delete
[File]	acctres.dll	64512	08/17/2001 10:32:38 PM	Delete
[File]	accwiz.exe	150800	11/22/2002 04:58:56 PM	Delete
[File]	acelpdec.ax	61952	12/07/1999 01:00:00 PM	Delete
[File]	acledit.dll	131856	12/07/1999 01:00:00 PM	Delete
[File]	aclui.dll	78096	07/22/2002 08:05:04 PM	Delete
[File]	acs.mib	33298	12/07/1999 01:00:00 PM	Delete
[File]	acsetupc.dll	4368	12/07/1999 01:00:00 PM	Delete

Display a menu

What do you want to delete today???

Thanks JimmyNeutron!

More Explorers?!?!

Why hack when you can… click? =)

phpRemoteView: C:/Program Files/Ensim/Sitedata/hackersg/Inetpub/wwwroot/

intitle:"phpremoteview" filetype:php "Name, Size, Type, Modify"

Proxies ihackstuff

C:/Program Files/Ensim/Sitedata/hackersg/Inetpub/wwwroot/

<?phpRemoteView?>

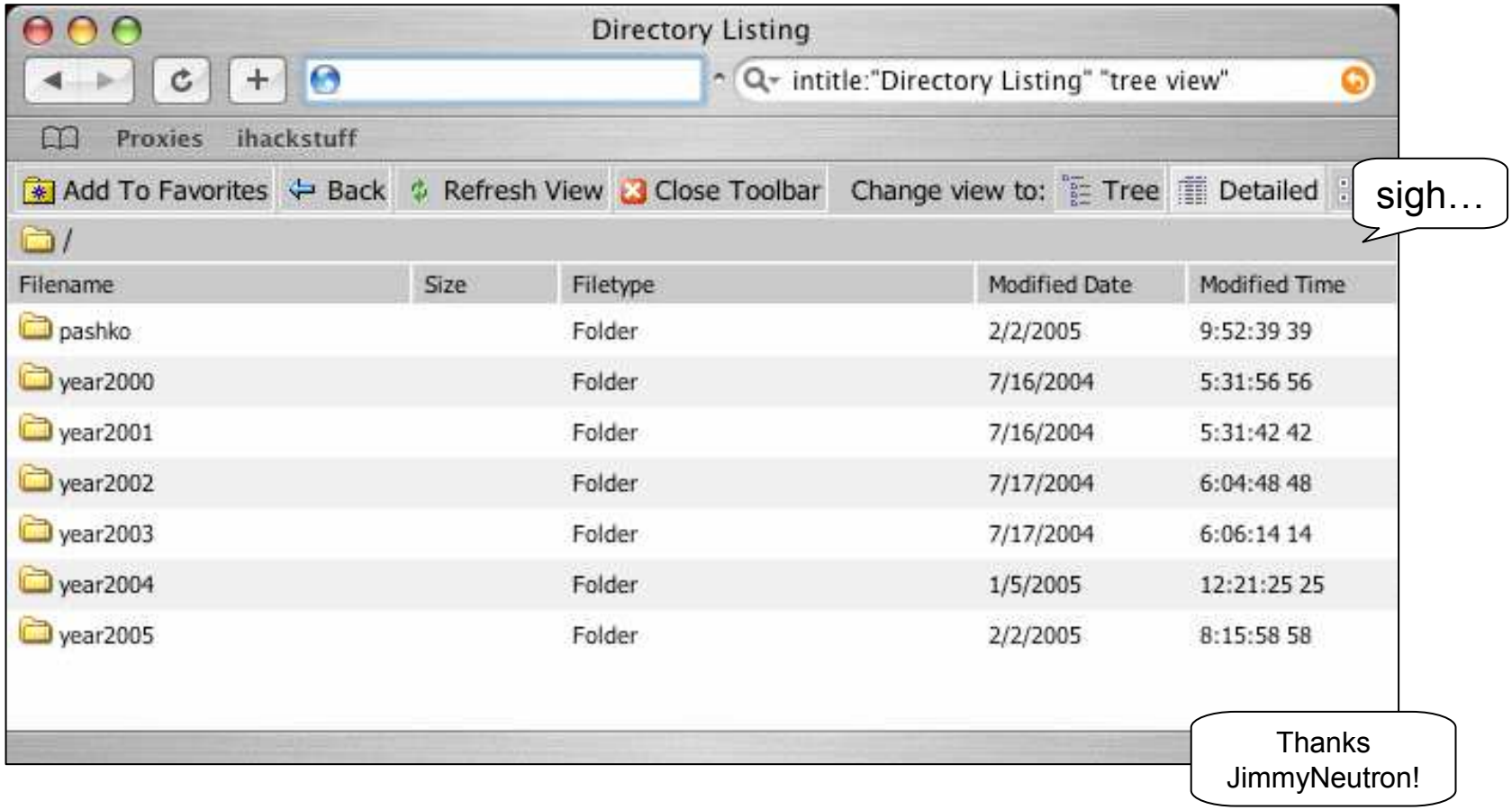
Name	Size	Type	Modify	Owner/Group	Perms
_vti_cnf		DIR	18/02/04 20:40	0/0	0
_vti_script		DIR	18/02/04 20:40	0/0	0
taam		DIR	29/09/04 03:42	0/0	0
tool		DIR	22/09/04 20:54	0/0	0
util		DIR	15/11/04 08:55	0/0	0
xxx		DIR	29/09/04 01:08	0/0	0
2p0p0PF4.zip	1 427 105		11/09/04 23:02	0/0	0
graphcount.php	3 854		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

Setup | PHP eval | phpinfo() | Shell | Char map | Language: English/Russian

phpRemoteView © Dmitry Borodin (version 2003-04-22)
Free download - http://php.spb.ru/remview/

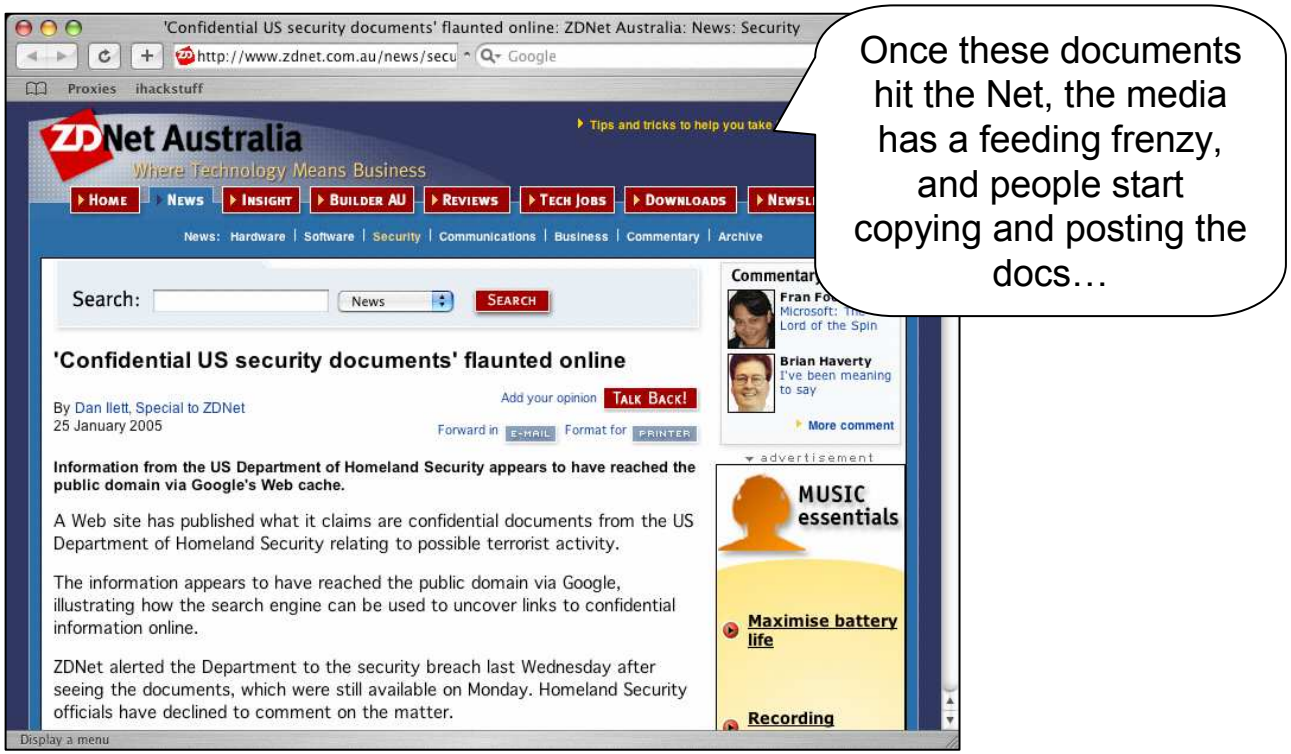
Thanks MacUK!

More Explorers?!?!



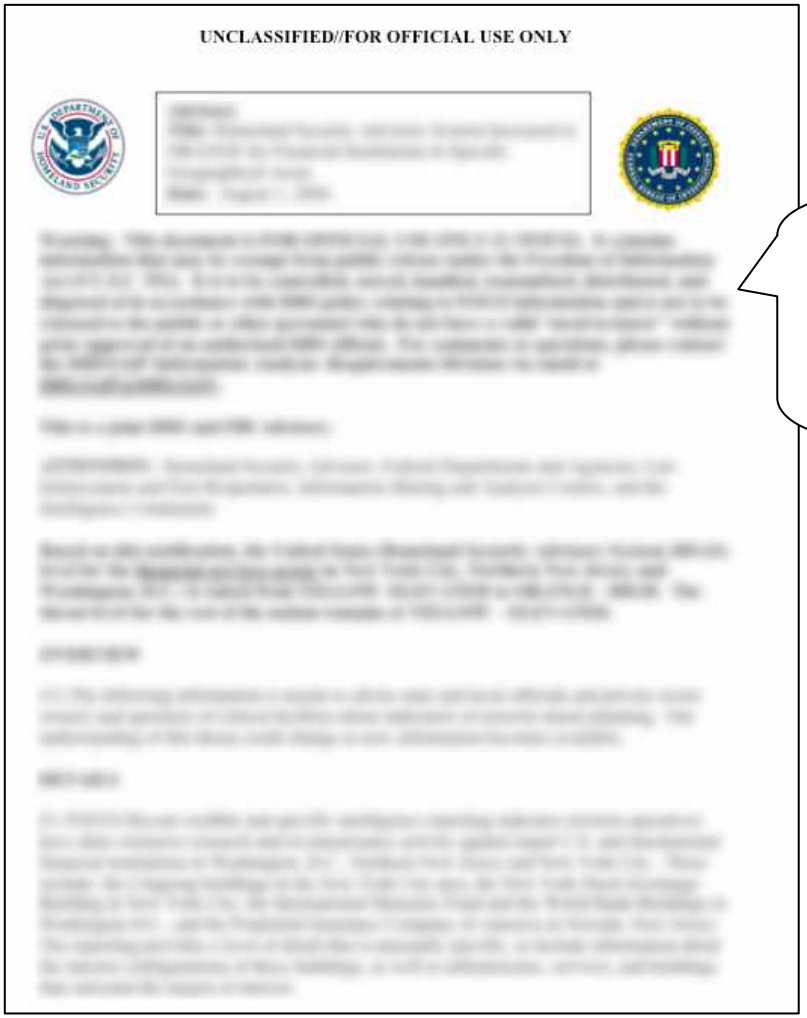
Sensitive Government Documents

- 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.

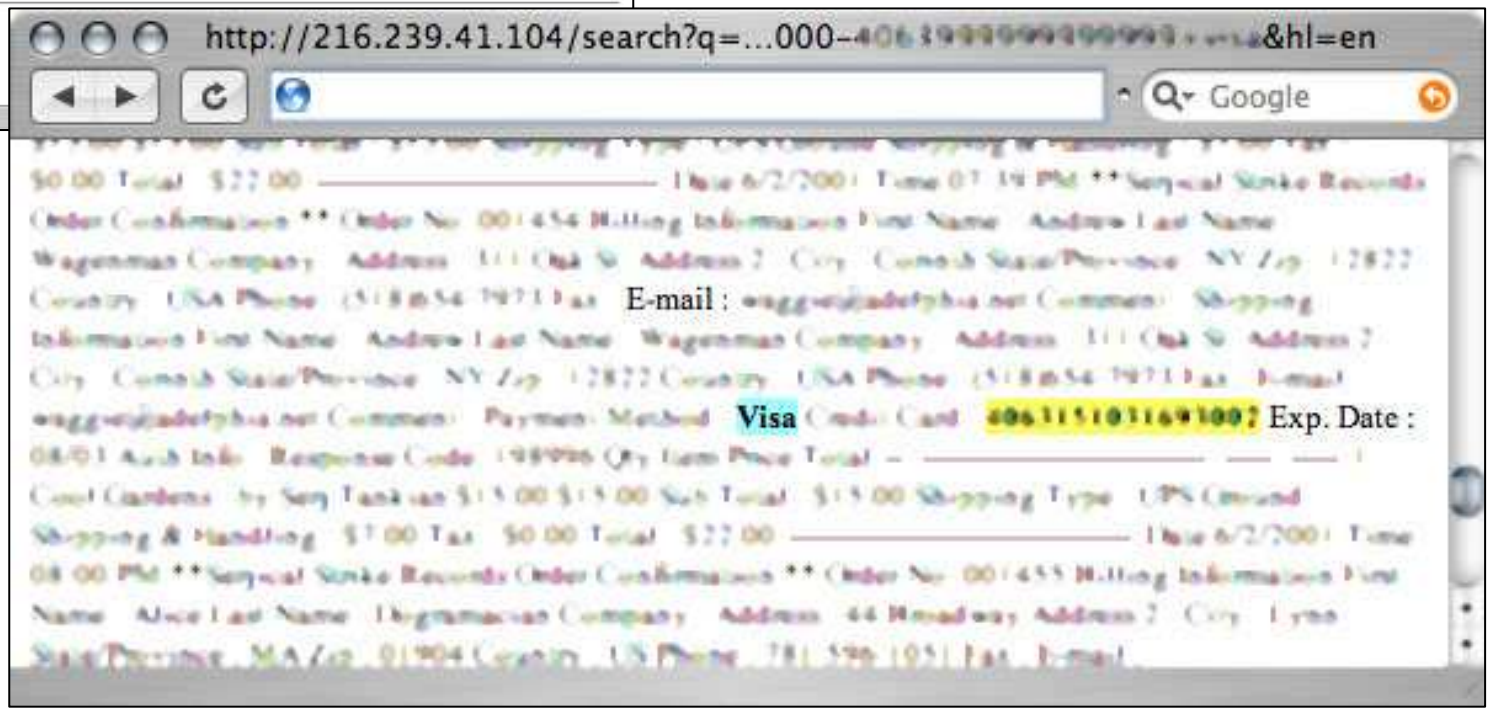
FOUO Documents

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

Locked out!

- Some sites lock down sensitive data..

- However, the Google cache image still remains.



Credit card info on the web?

- How can this happen? Let’s take a tour of some of the possibilities…

Court Documents

- Court cases sometimes give TONS of detail about cases, especially fraud.

UNITED STATES [illegible] COURT
[illegible]
[illegible] DIVISION

UNITED STATES OF AMERICA

v. CASE NO. [illegible]

[illegible]

Court Documents

Platinum
account number :

account #

account
#:

account #:

account
#:

statement account #

Bank #

Court Documents

- How much detail is too much detail? =)

		CREDIT CARD		ACCOUNT NUMBER	ACCOUNT NAME	AMOUNT
				138 23		$ .00
		Bank		059 13		$ .00
		Bank		040 97		$ .00
		t Bank		059 13		$ .00
		Bank		00 96		$ .00
		Bank		00 96		$ .00
		Bank		059 13		$ .00
		r Bank		00 64		$ .00
		Bank		710 17		$ .00
		Bank		100 64		$ .00
		Bank		081 019		$ .00

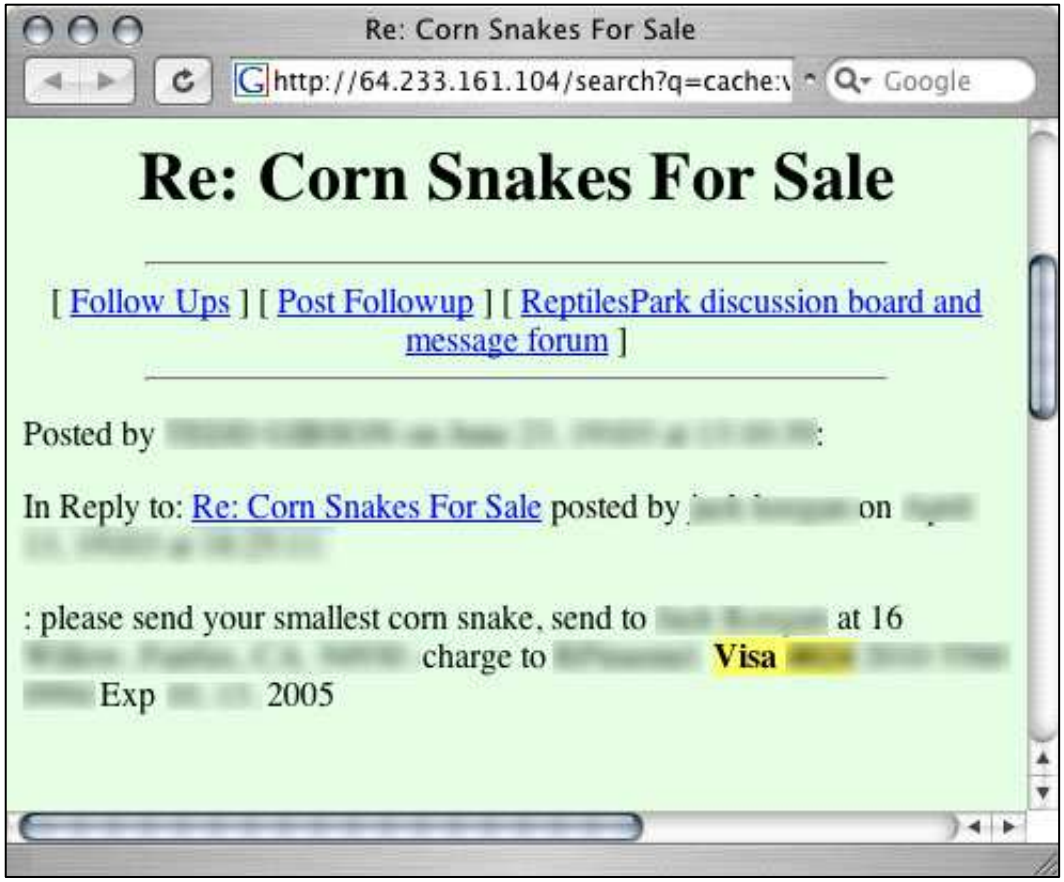
Court Documents

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

		BANK	ACCOUNT NUMBER	ACCOUNT NAME	AMOUNT
		t Bank	05 13		$1
			13 23		$3
		Bank	90 97		$7
		Bank	71 02		$2
		Bank	10 96		$3
		Bank	28 27		$11
		Bank	63 91		$2
			90 10		$3

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*: [illegible]
- *Subject*: applying for a shell acct
- *From*: [illegible]
- *Date*: [illegible]

```
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: [illegible]
password: [illegible]

Down here will be the details about me.
[illegible]
[illegible]
Fortuna,CA,95540

tel#: [illegible]
Billing Information:
Name on card: [illegible]
credit card #: [illegible]
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.

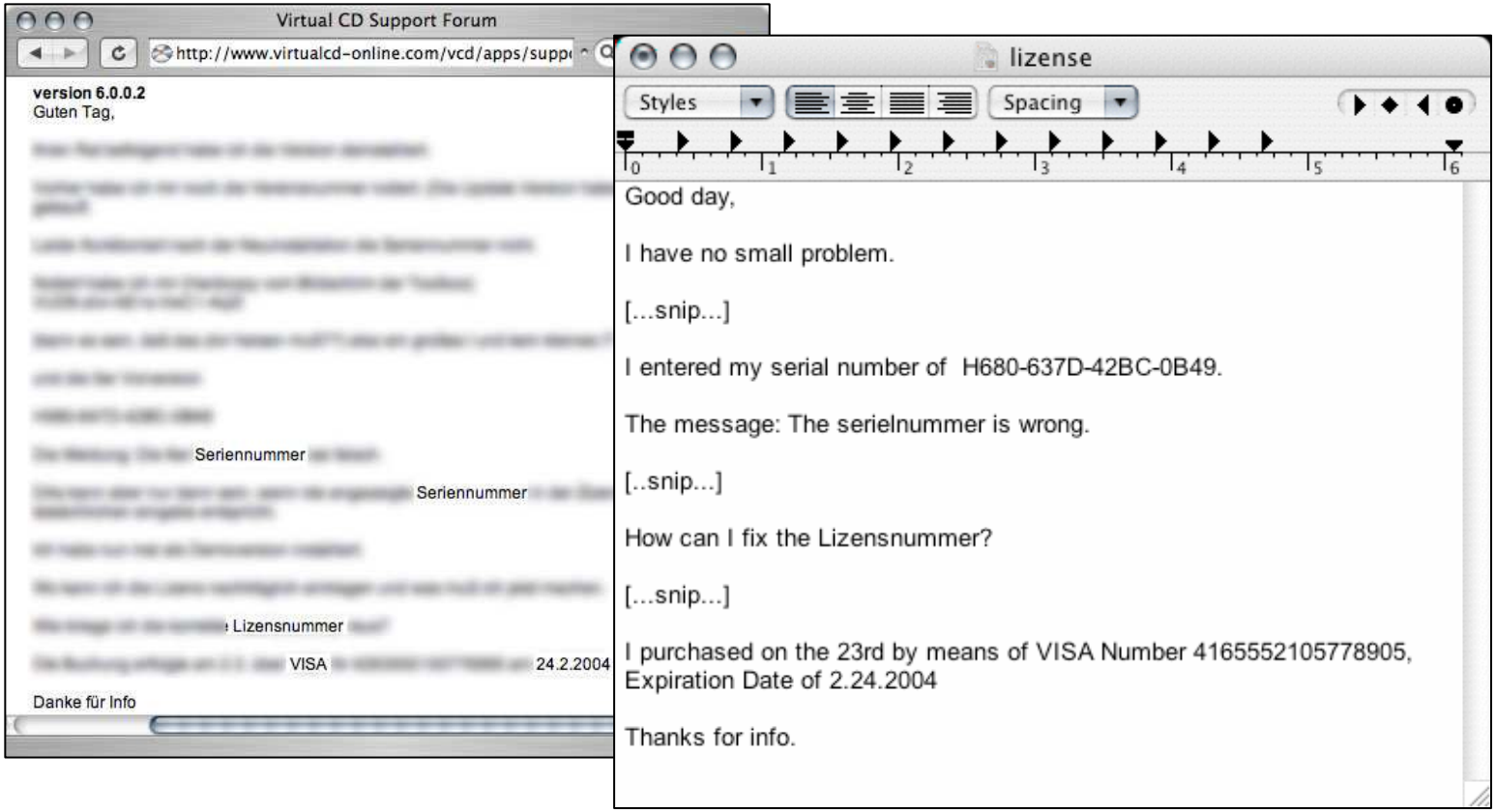
Questions & Offers between [redacted] and the Seller

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 cyy2 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…

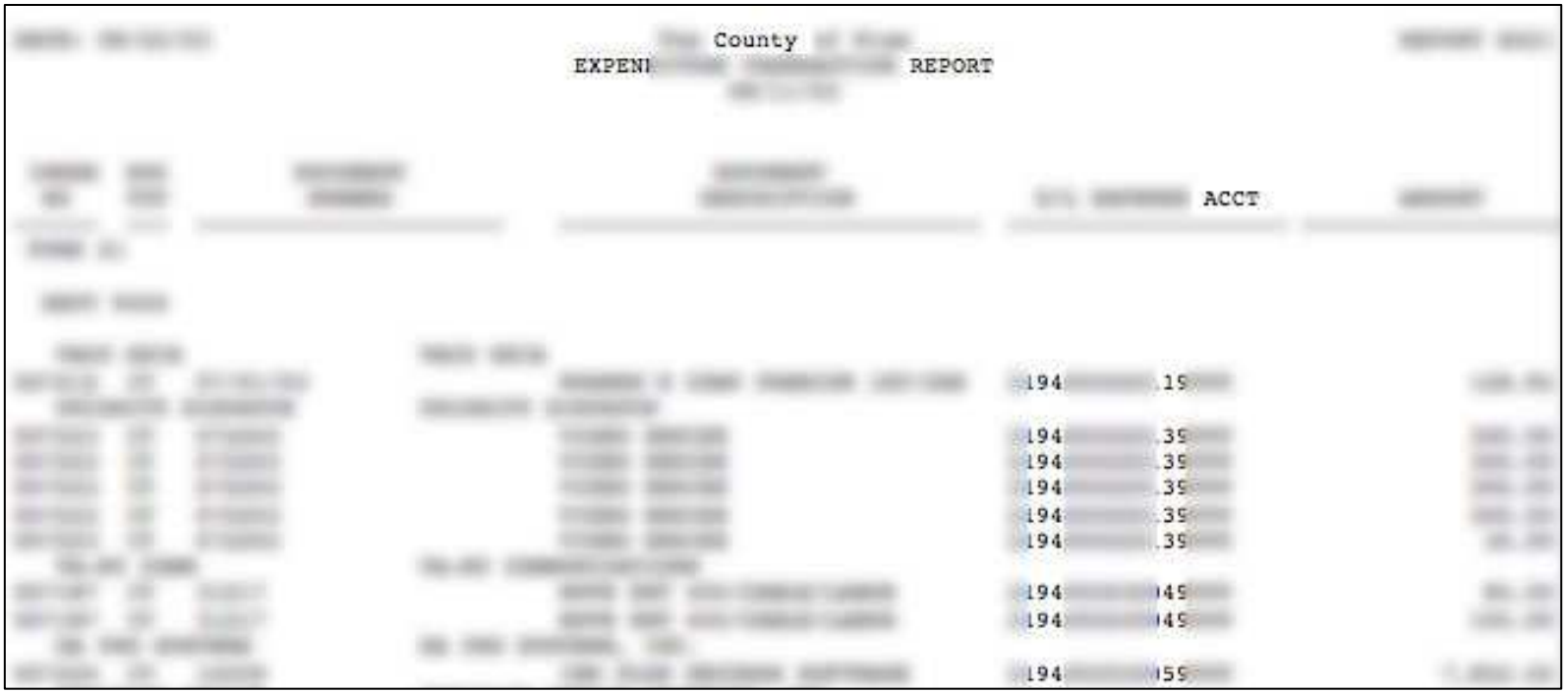
- I'm thinking there should be a process for filtering these reports.

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

Results **1** - **28** of **28**

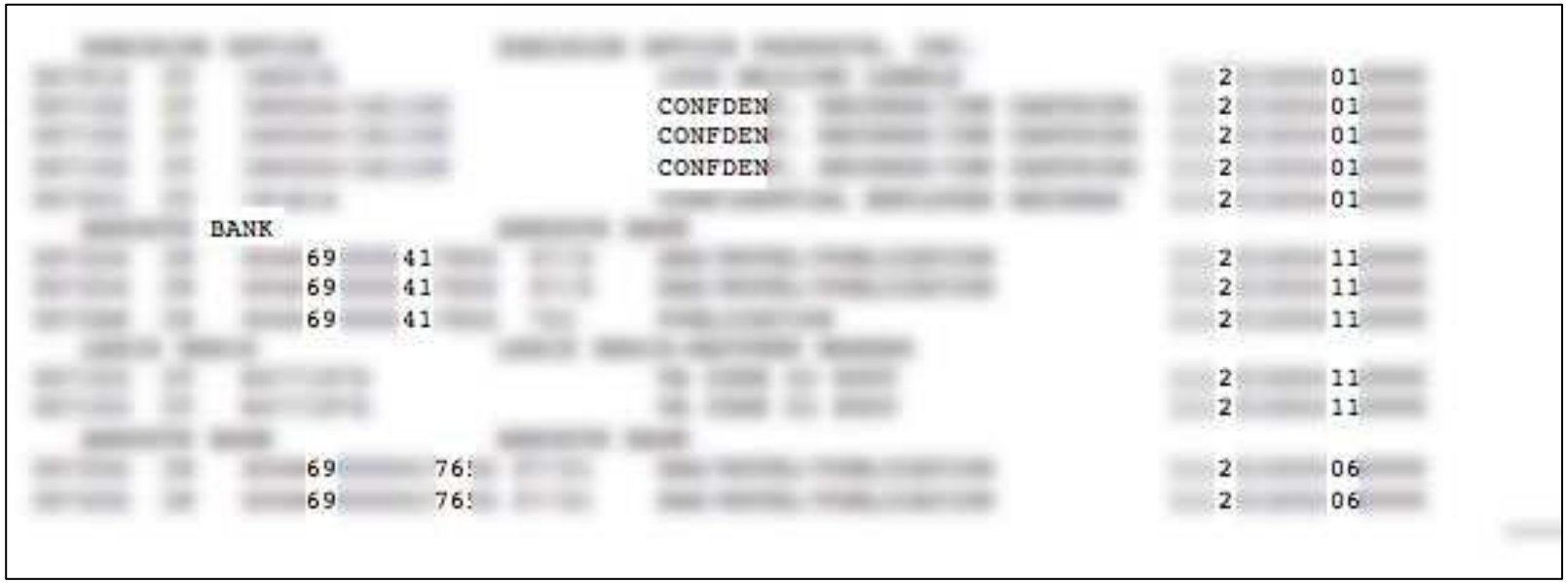
Expense Reports

- It’s not uncommon for expense reports to be generated. This one is for a county.



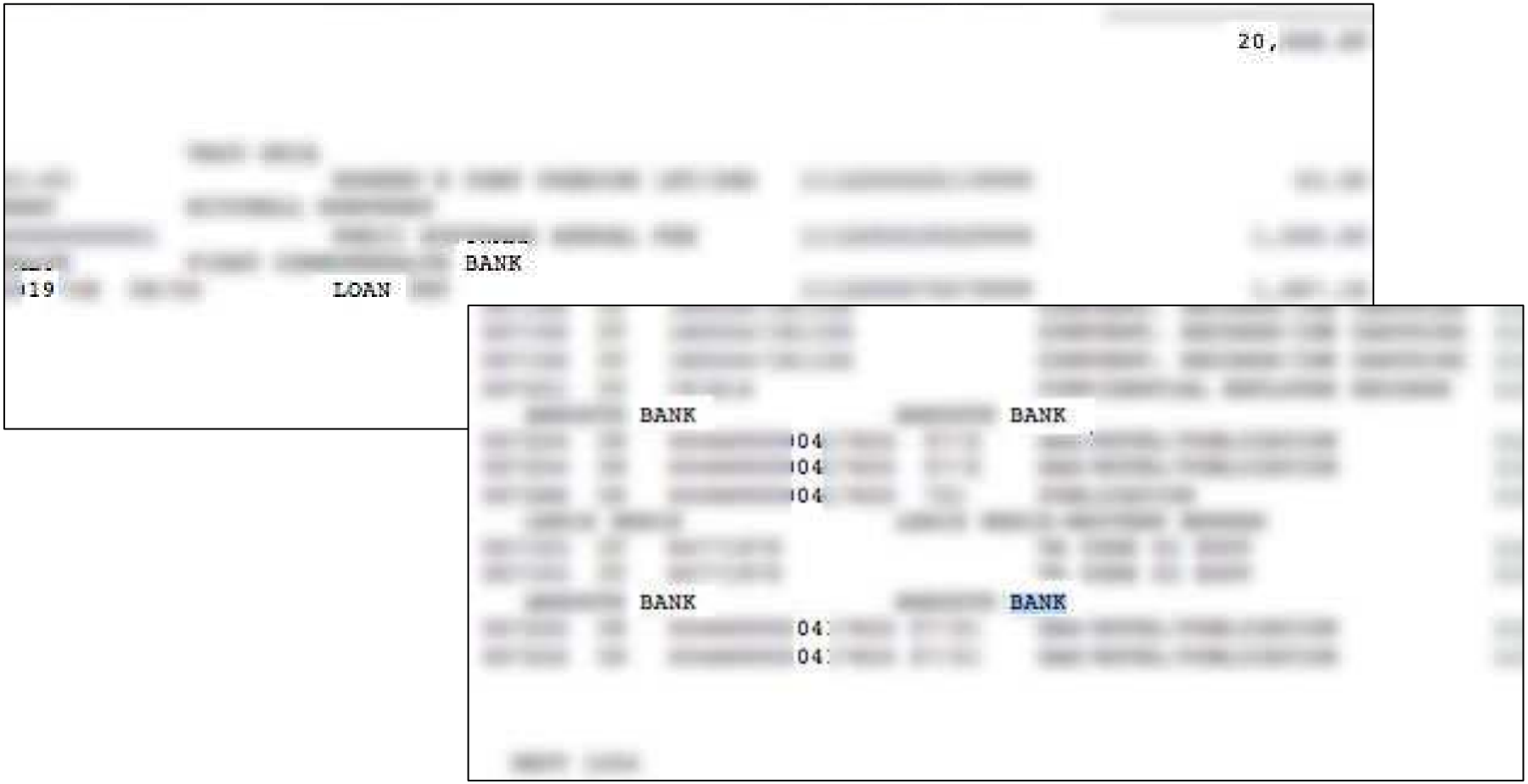
Expense Reports

- Bank account numbers….



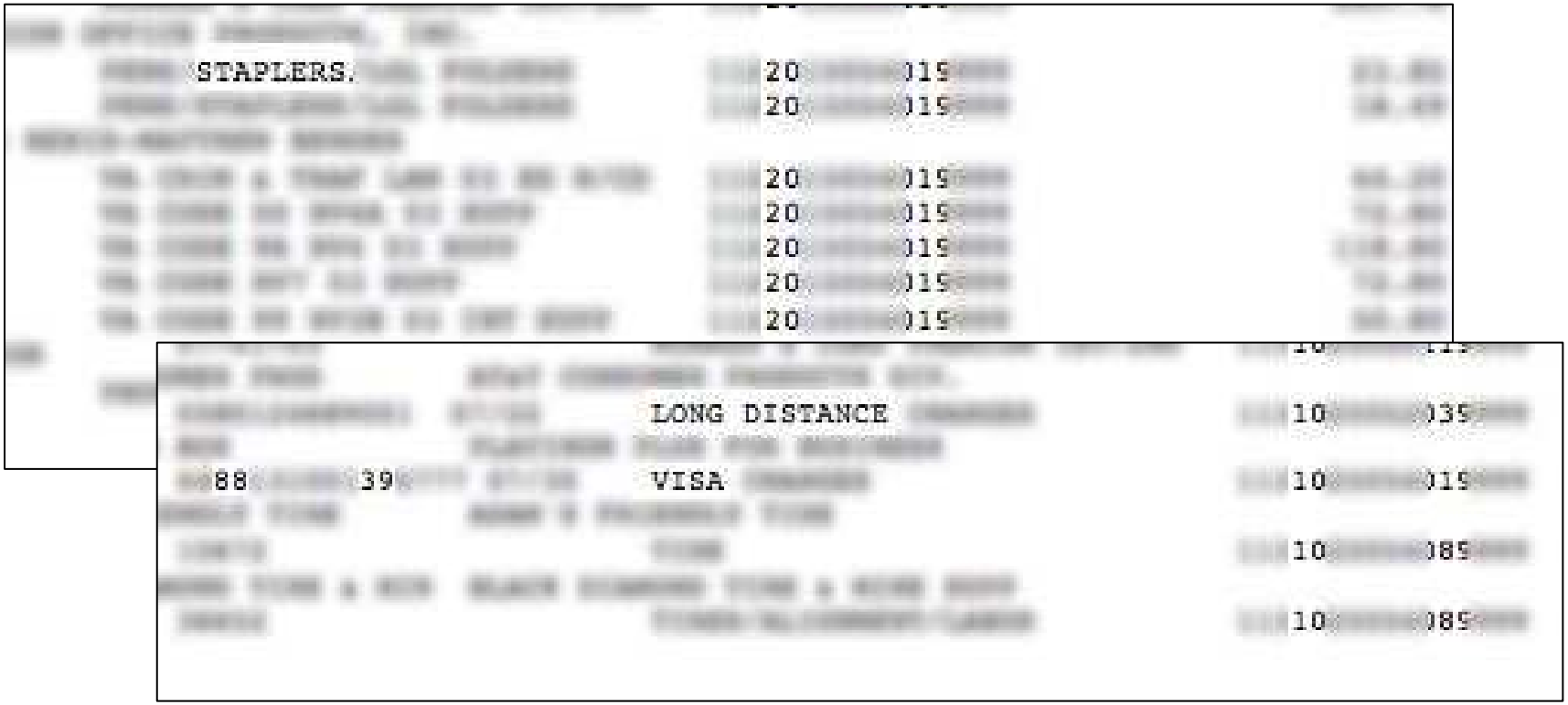
Expense Reports

- Bank loan information… $20,000 + transactions



Expense Reports

- Oh boy…



Expense Reports…

- Somebody has to pay for all this stuff….

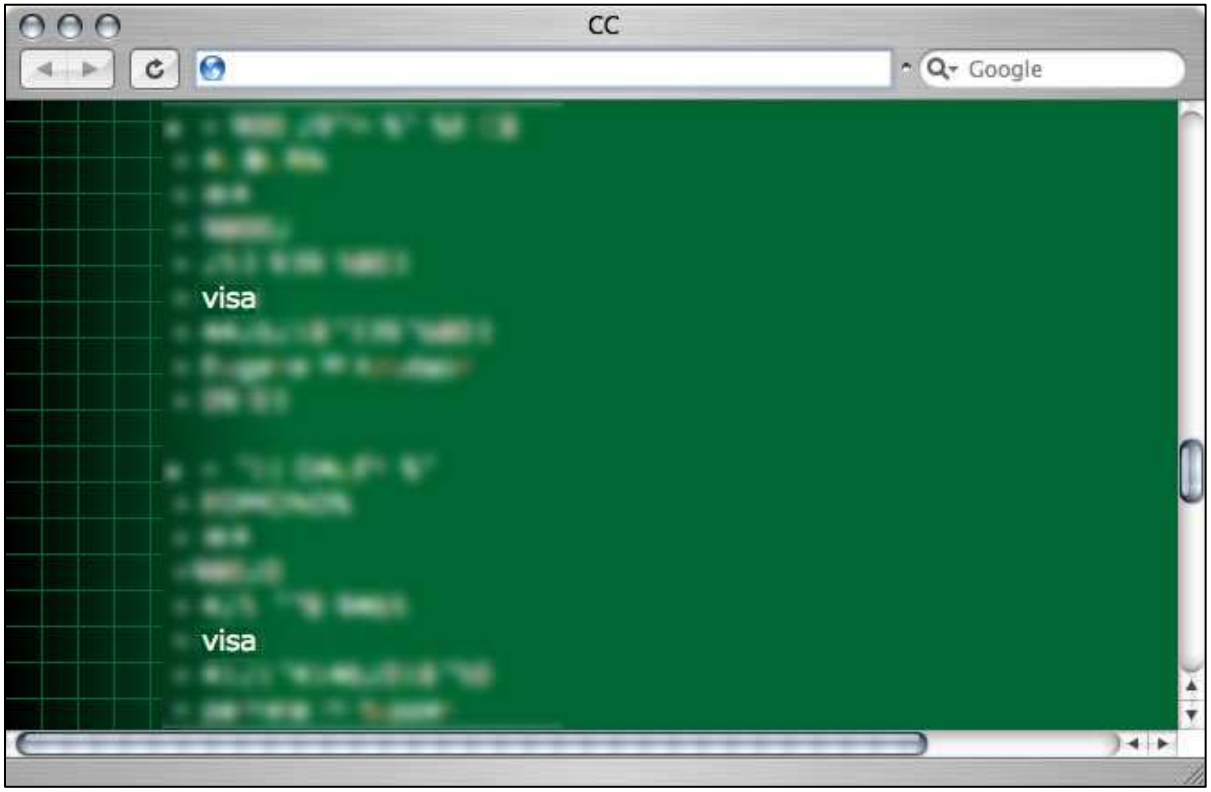
Expense Reports

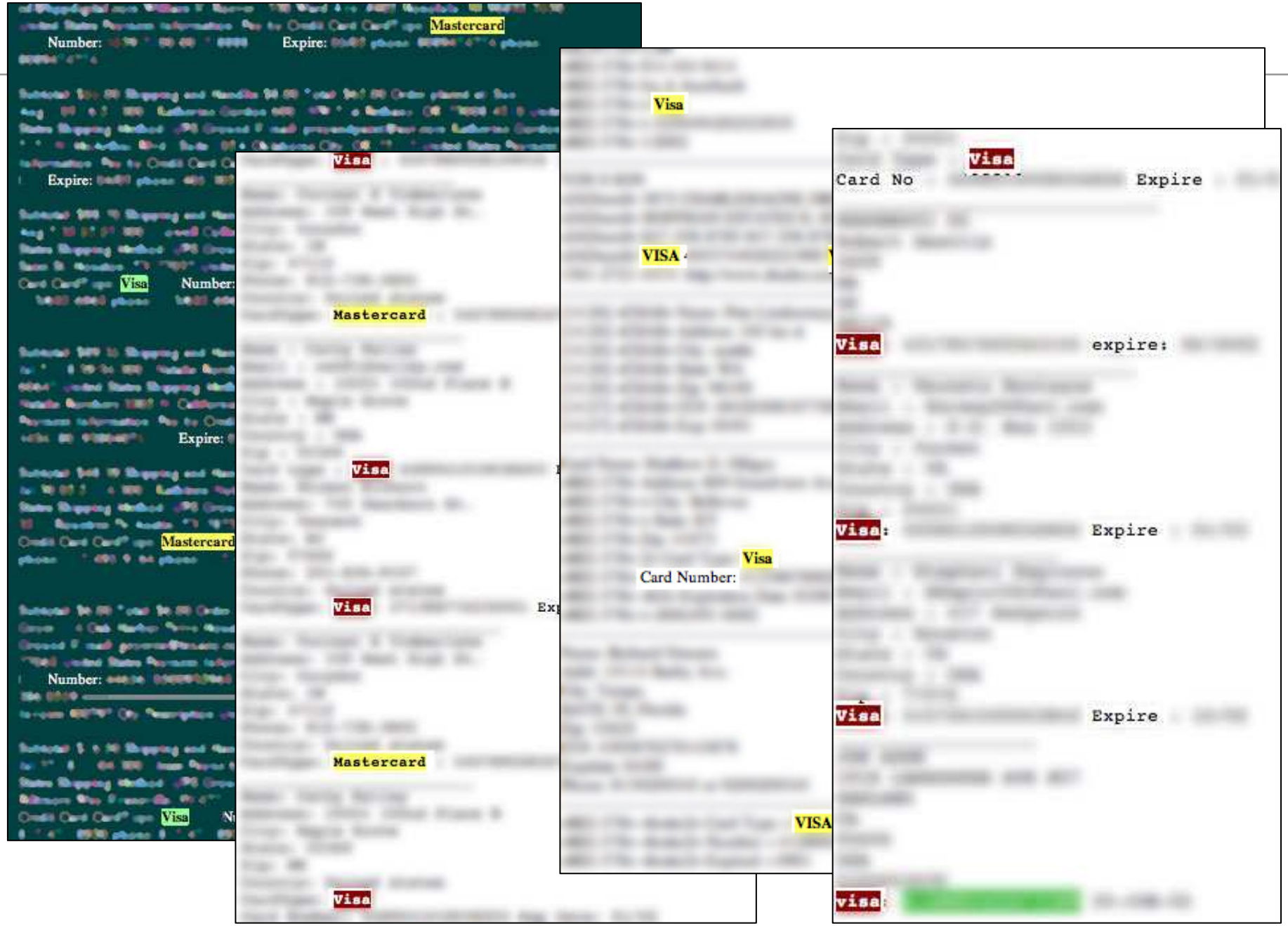
- That’s one heck of a video series…. $300+

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

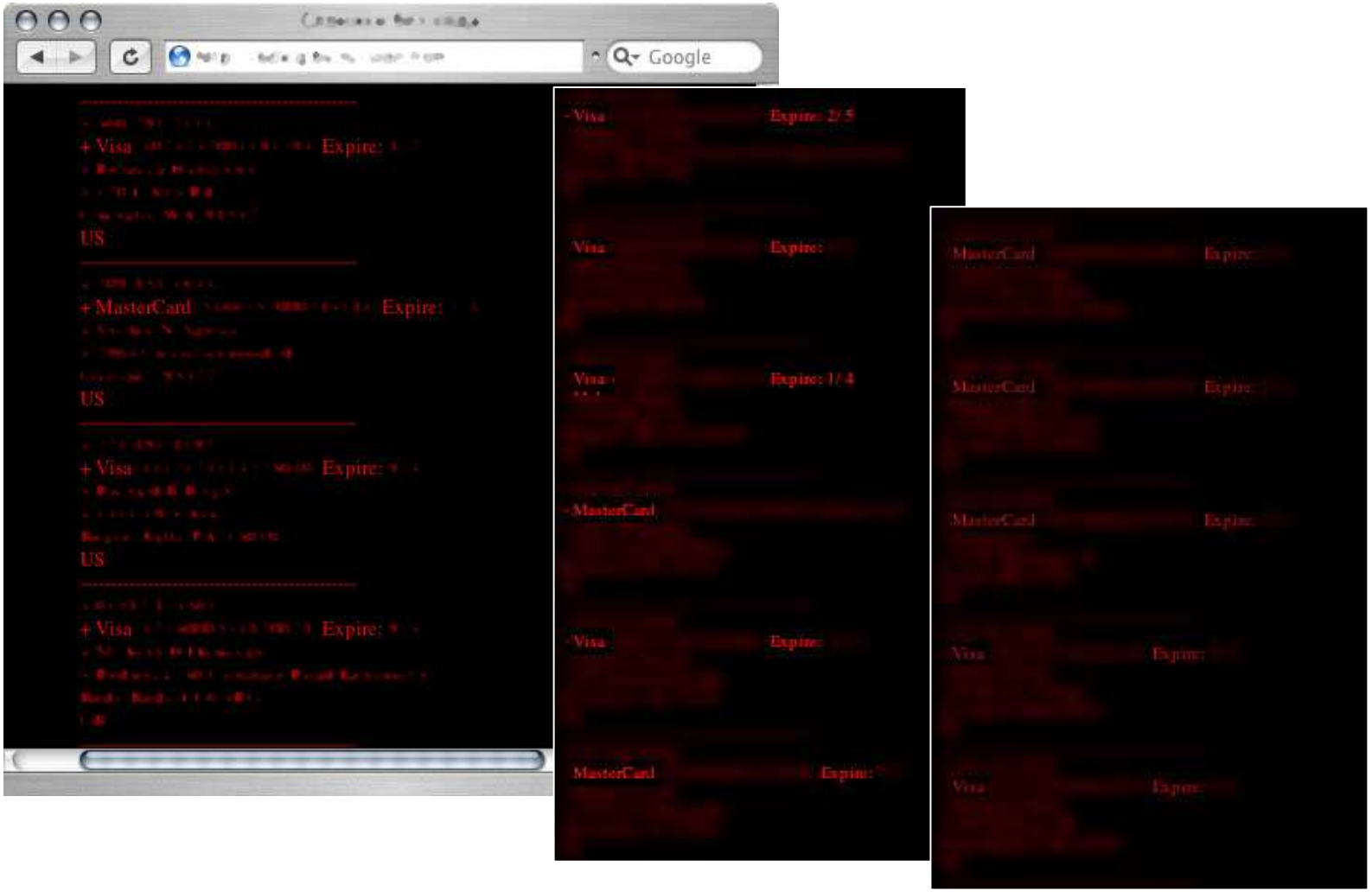
Credit cards… Google hacker's gold…

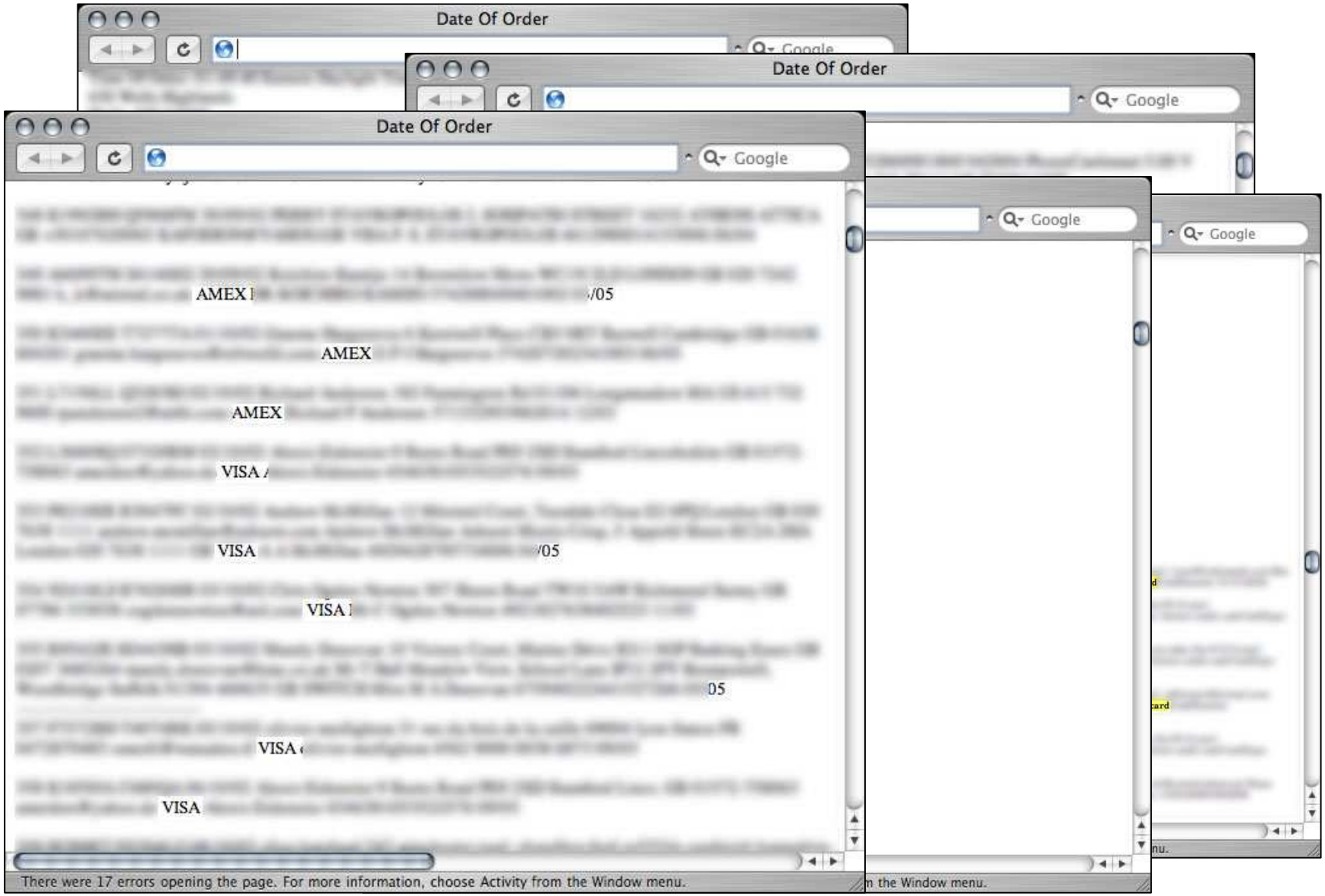
- The legend of finding credit cards online is true…
- I just get bored sifting through them all….

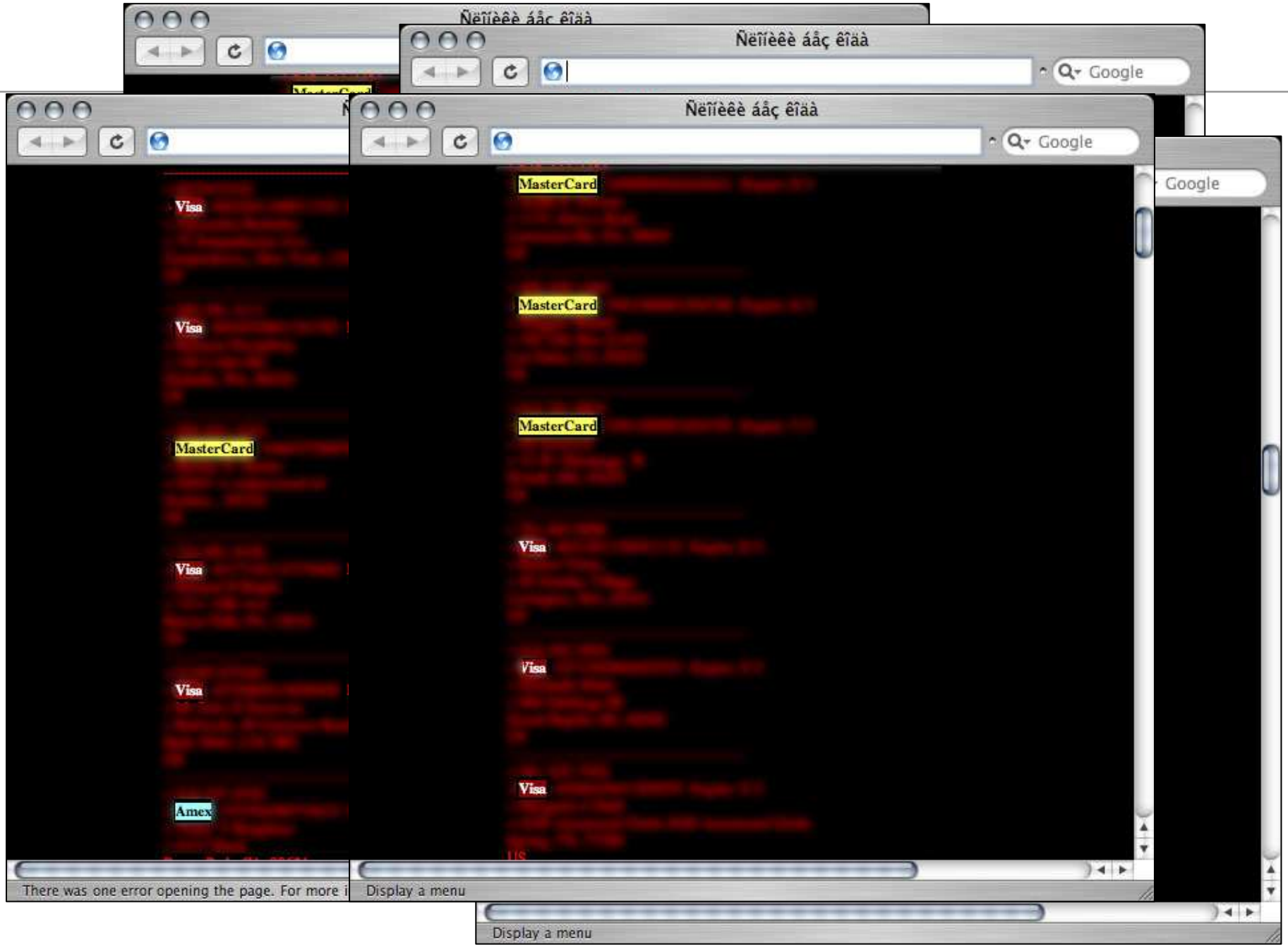


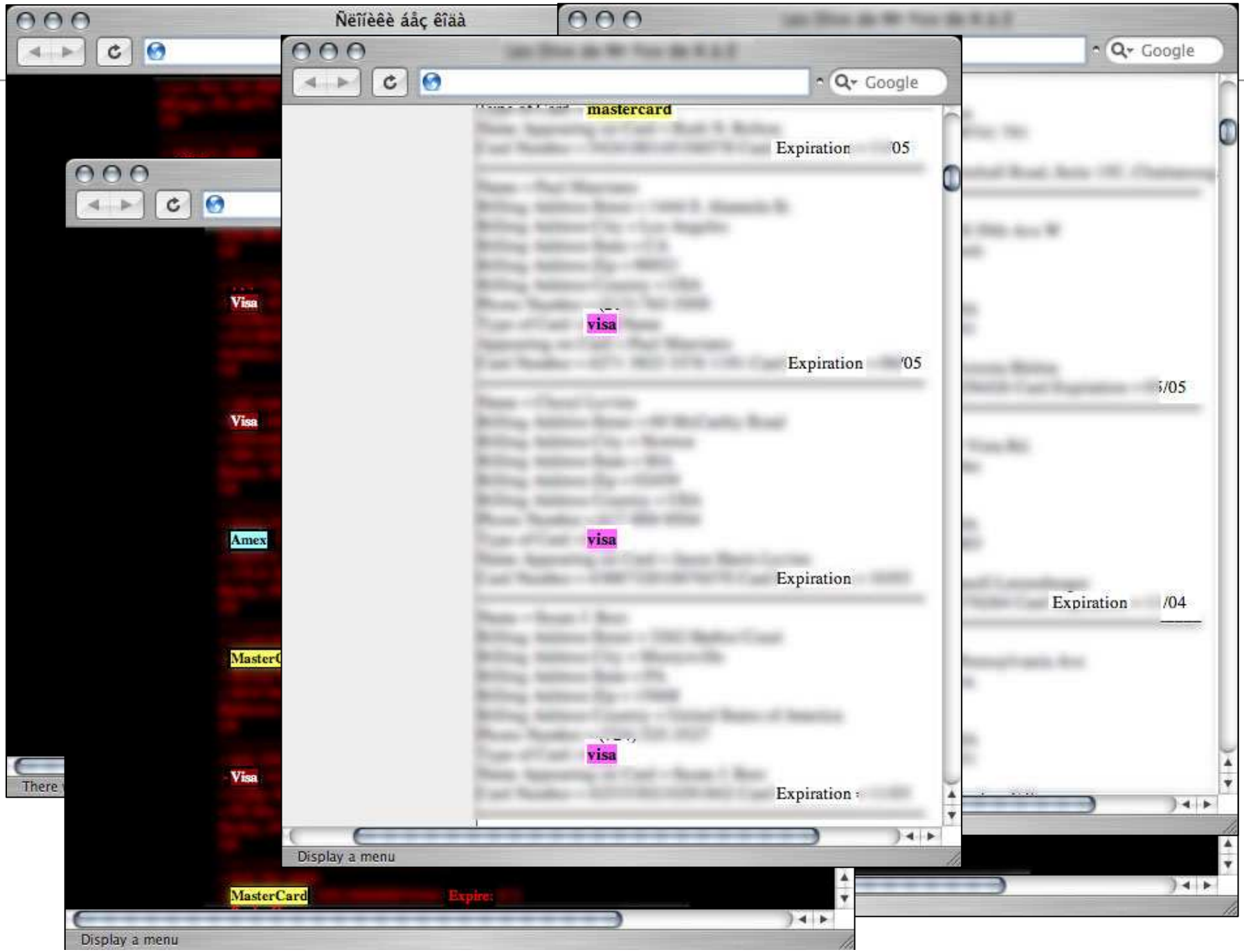

Mastercard
Number:
Expire:
Visa
Number:
Expire:
Mastercard
Visa
Mastercard
Number:
Visa
Visa
VISA
Visa
Card Number:
VISA
Card No
Expire
Visa
expire:
Visa:
Expire
Visa
Expire
visa:

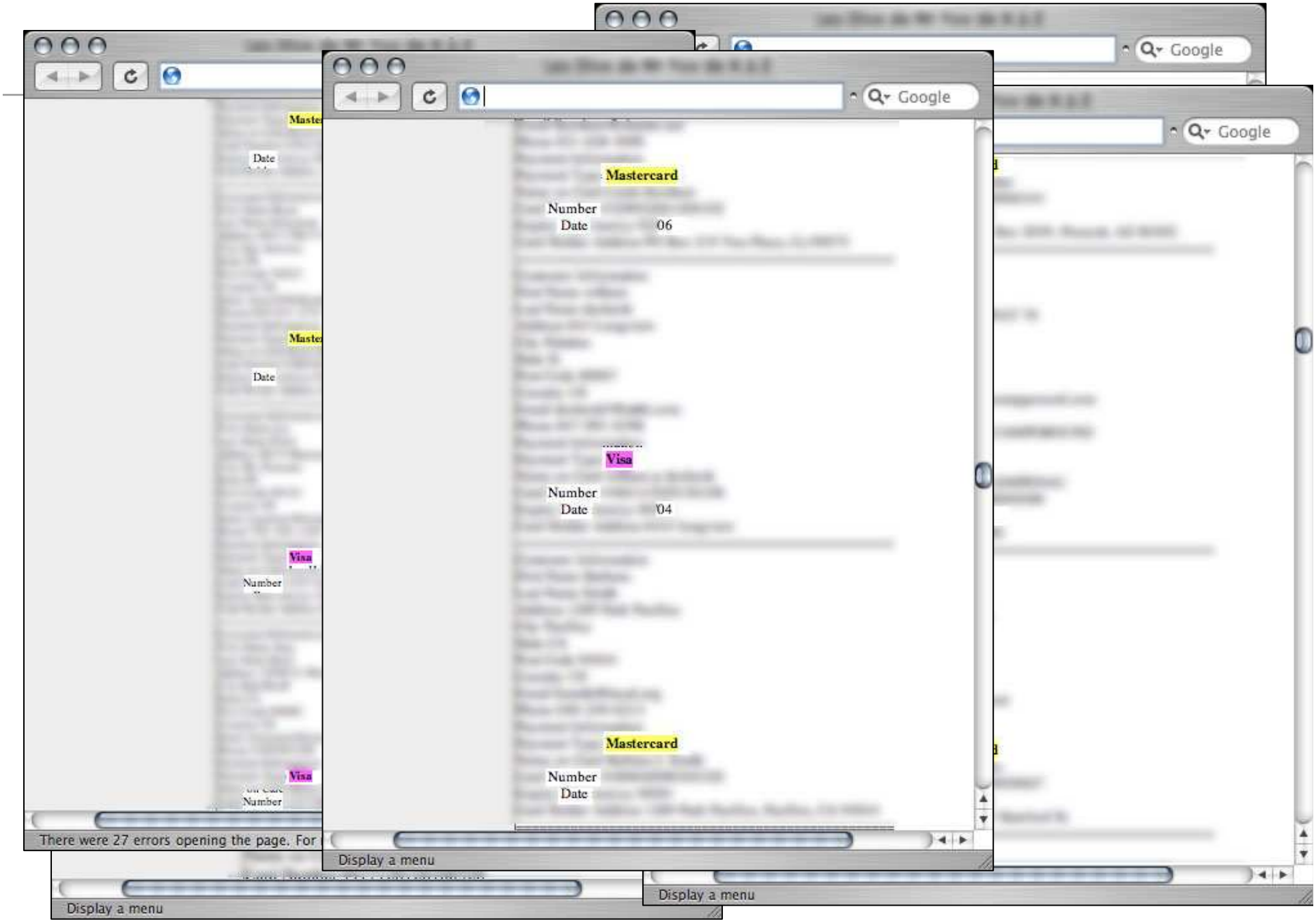
Credit Listings



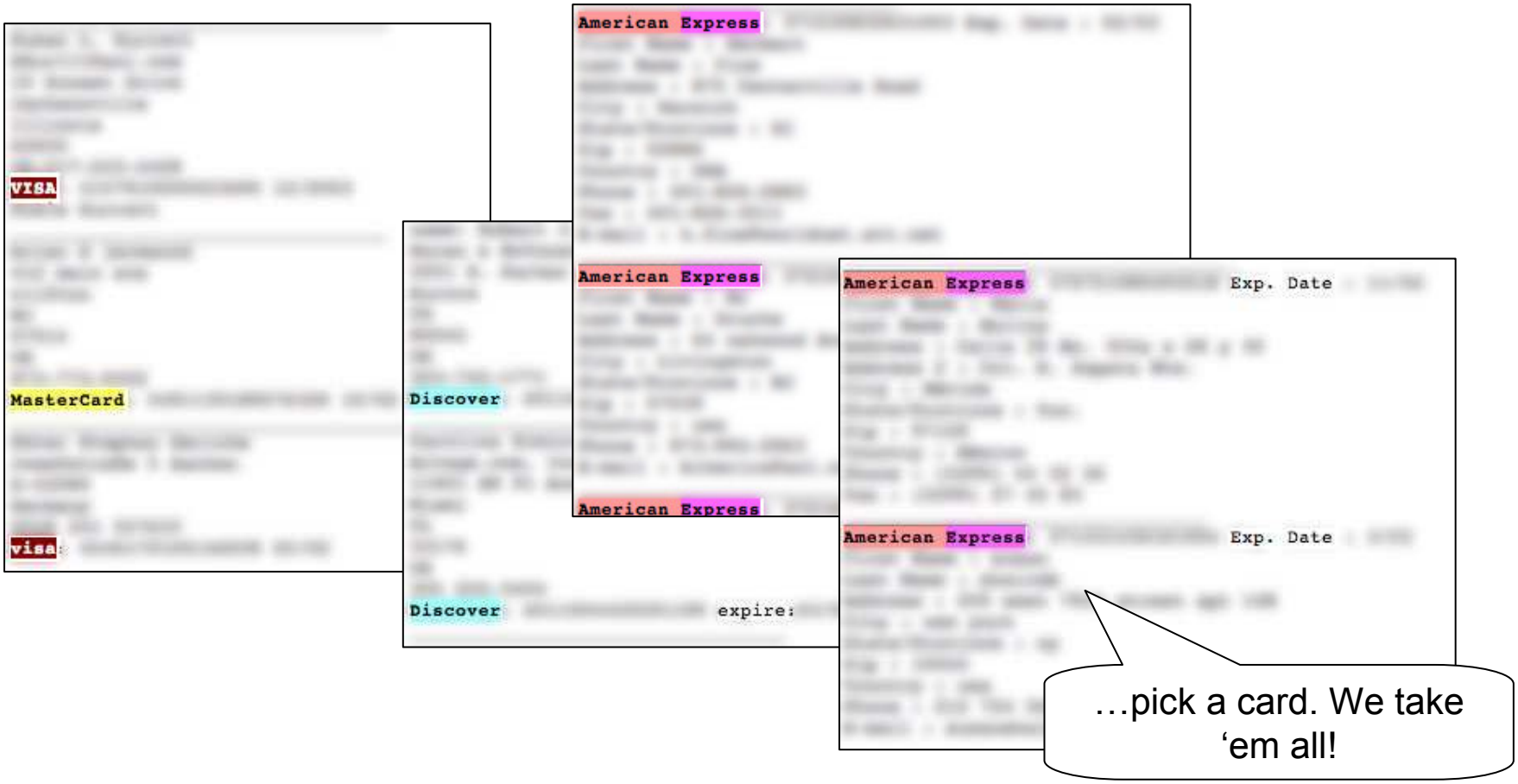

Date Of Order
Google
Date Of Order
Google
Date Of Order
Google
AMEX
/05
AMEX
AMEX
VISA
VISA
/05
VISA
05
VISA
VISA
There were 17 errors opening the page. For more information, choose Activity from the Window menu.


Ñëïíèêè áåç êîäà
Google
Visa
MasterCard
Amex
There was one error opening the page. For more i
Display a menu


Ñëïîèêè áåç êîäà
Google
mastercard
Expiration 05
visa
Expiration /05
visa
Expiration
visa
Expiration
Visa
Visa
Amex
MasterC
Visa
MasterCard
Expire:
Display a menu
Display a menu
Google
/05
Expiration /04
There


Google
Mastercard
Number
Date
06
Visa
Number
Date
04
Mastercard
Number
Date
Display a menu
There were 27 errors opening the page. For
Display a menu
Display a menu

Pick a card any card…

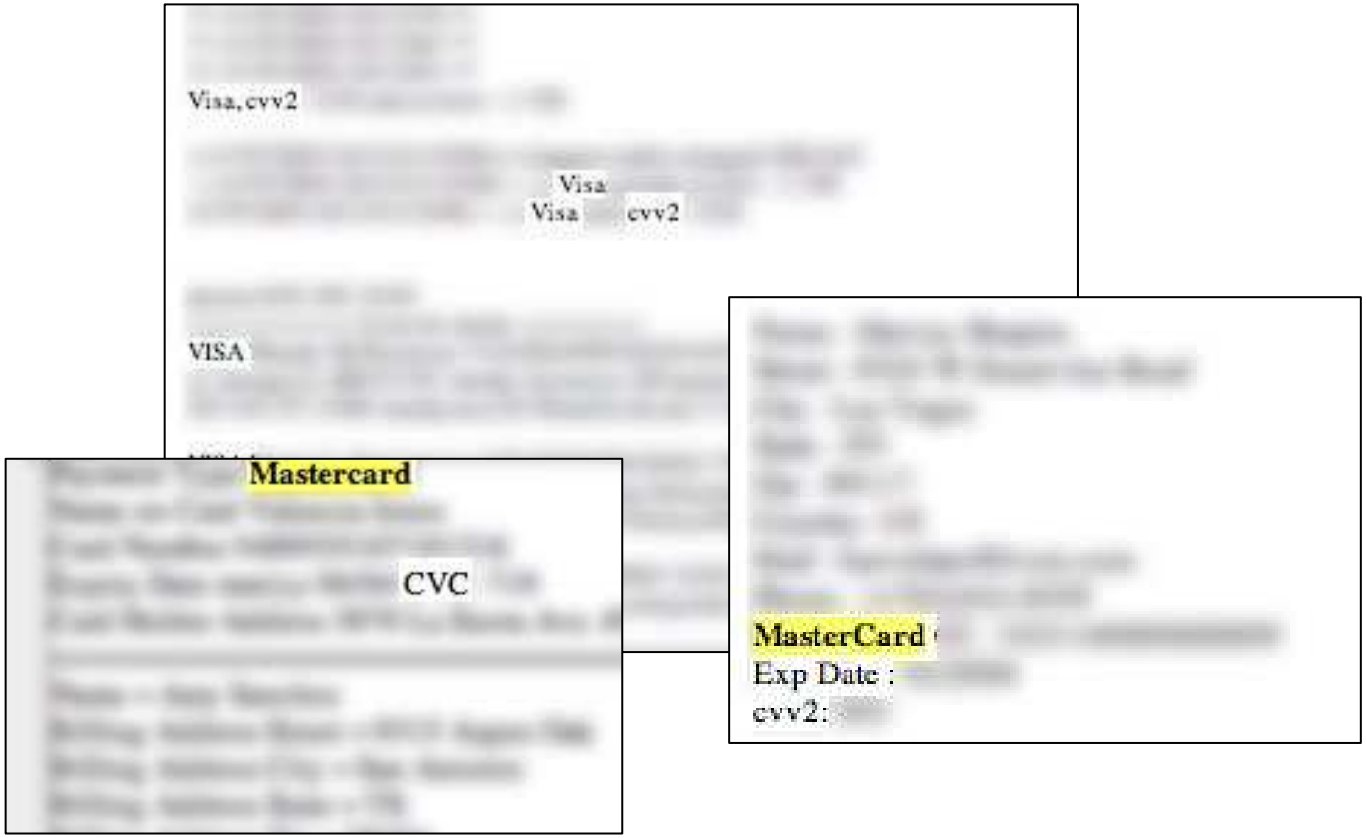


Credit Validation

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

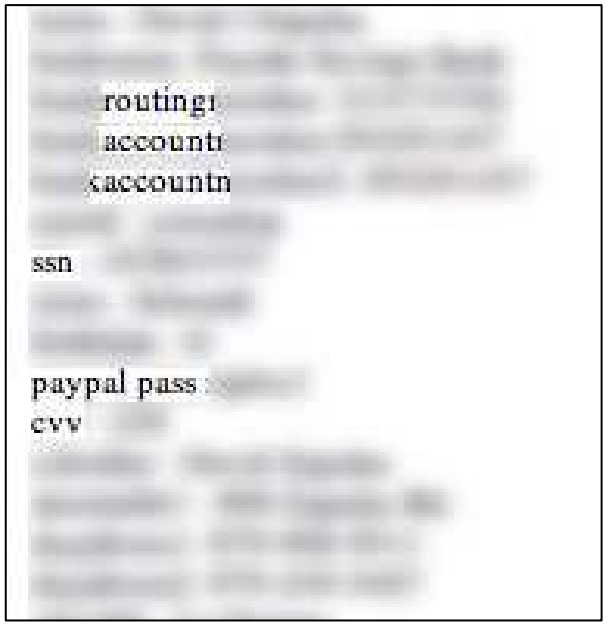
- Answer: That little code on the back of the card.
- Bonus question: What's that code called?
- Answer: A "CVV" code.

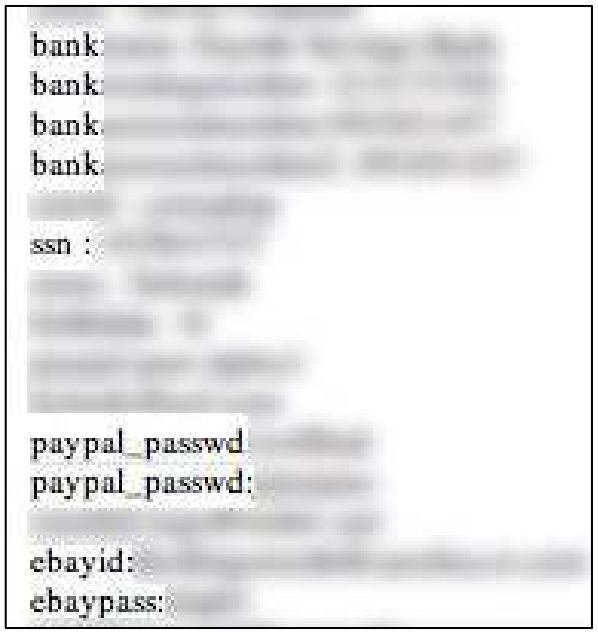
Credit Card Numbers, Expiration Date and CVV numbers, oh my!

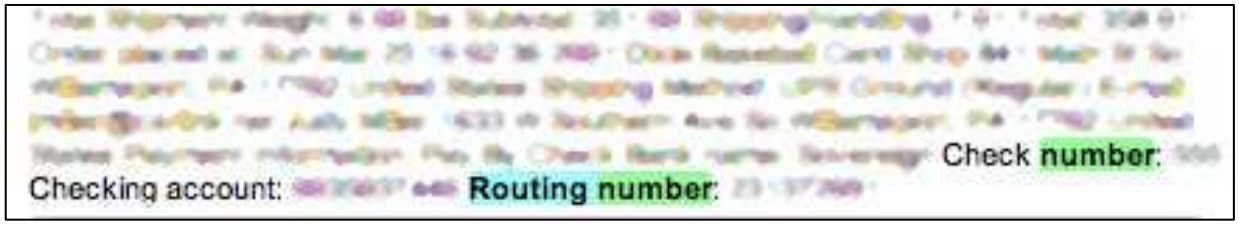


That’s not all….

- Credit cards are sooo 1990’s =)







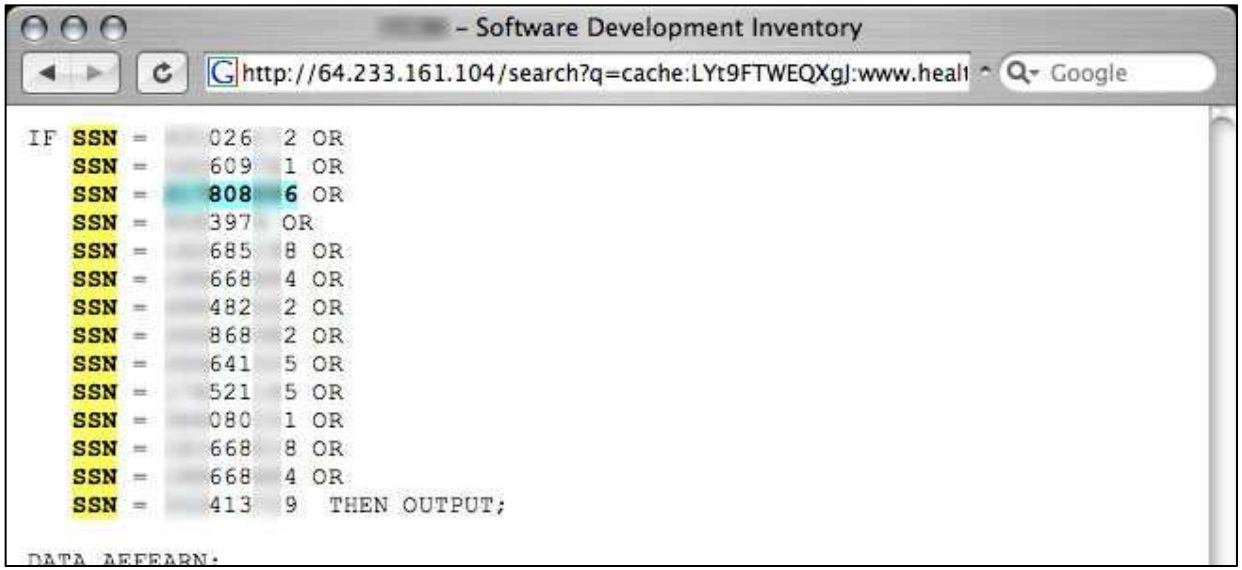
Getting more personal

- 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.

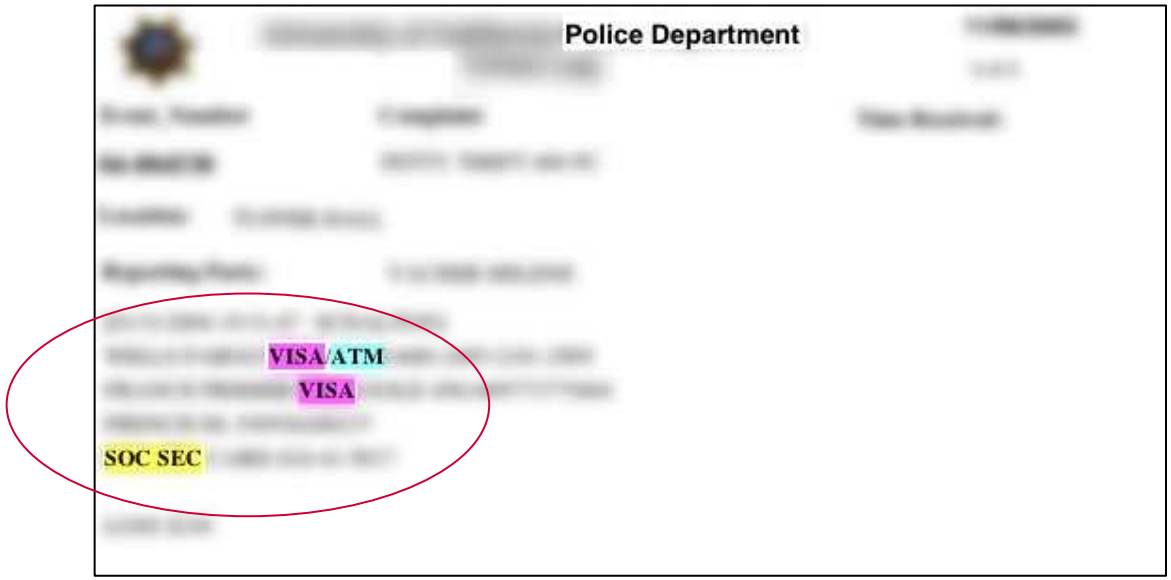
SSN's in source code

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

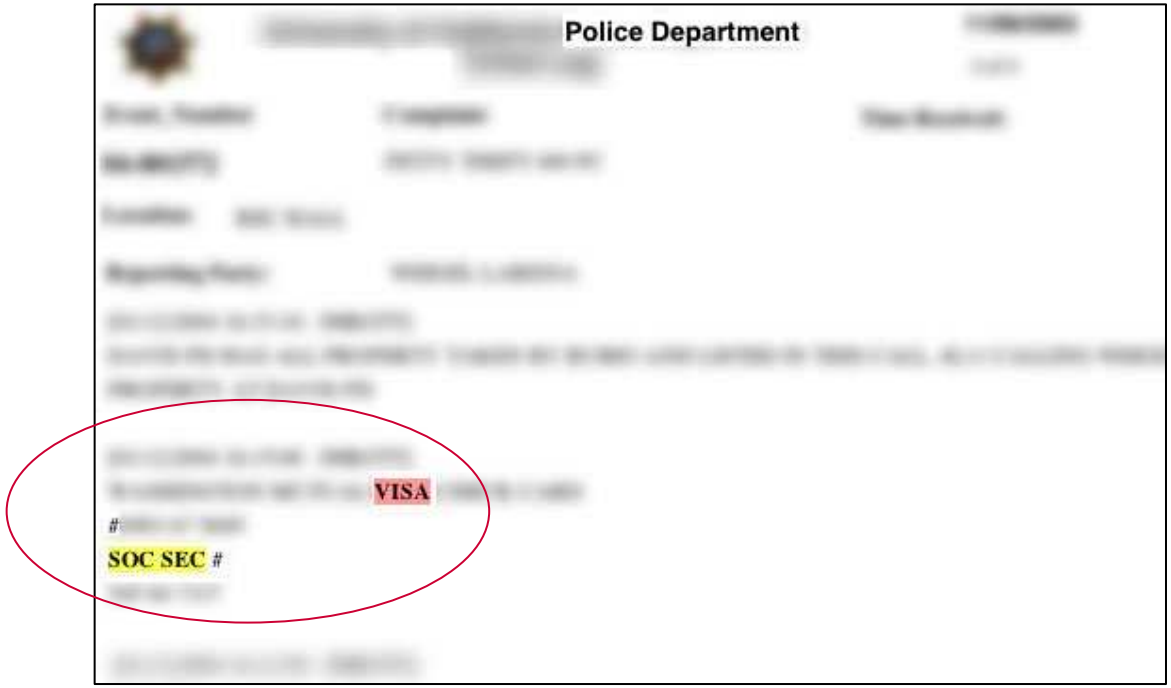


Crime shouldn't pay…

- 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


Police Department

VISA

#

SOC SEC #

SSN's

- Students have a right to know…


Police Department

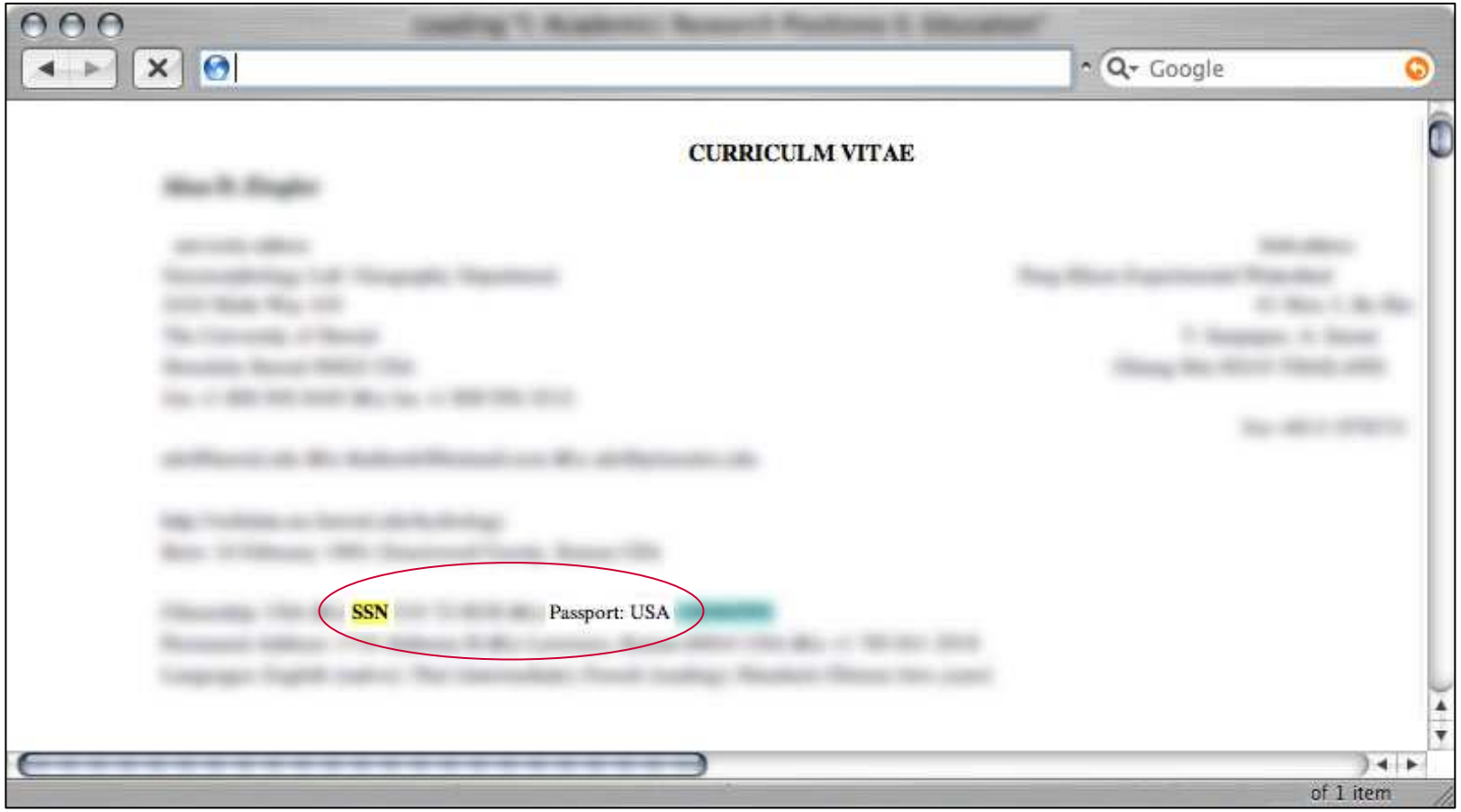
PETTY THEFT

DL MOTHER`S DL SS CARD #

Results **1** - **28** of **28**

Social Security Numbers

- Many privacy violations are self-inflicted…



Social Security Numbers

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

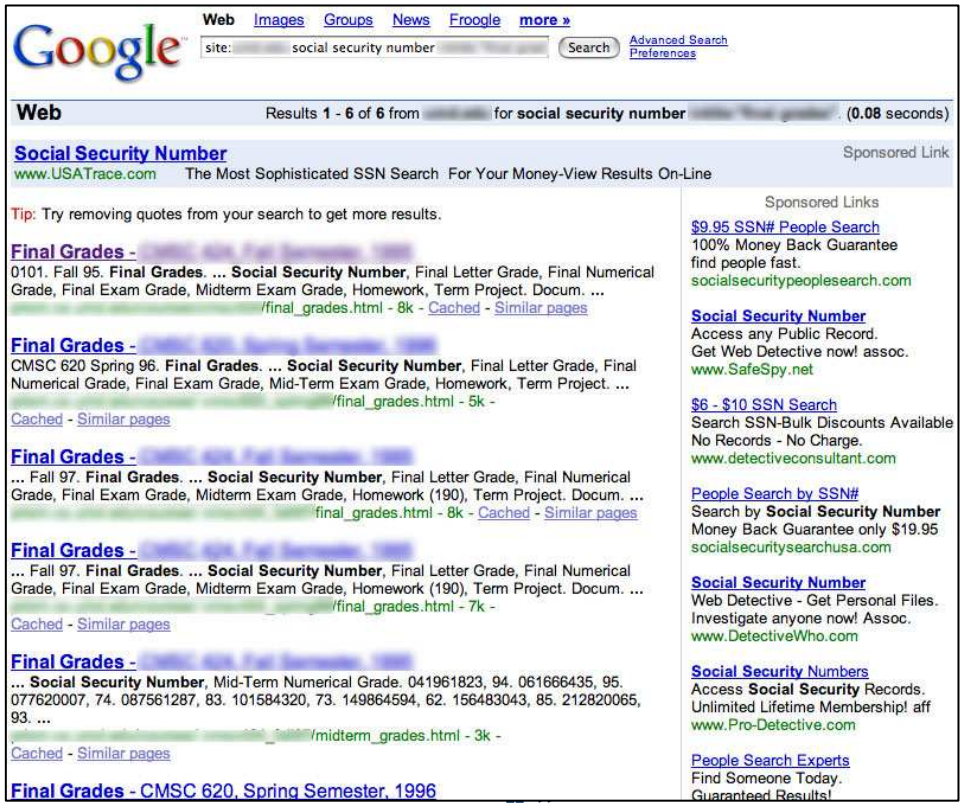
Final Grades –

http:// final_grades.html

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.



Social Security Numbers

Mid-Term Grades

Mid-Term Exam Average Grade = 73.22
Mid-Term Exam Median Grade = 83
Upper Quartile >= 93
2nd Quartile >= 83
3rd Quartile >= 68
Lower Quartile <= 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

Homework assignme

http:

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

http://www.

http://www edu site:um

SSN	Final Exam	Course Grade	
8 724	A	A	
72 590	A	B+	
78 552	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	
62 577	B	B	
78 544	C	C	
80 508	B	B	
70 561	C	C+	
70 057	F		D
74 146	C-		C
90 786	C-	D	
55 901	B	B	
74 573	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	
74 520	C	C+	
80 055	C	B	
62 503	F	C	
70 191	A	B	
84 185	B	B	
84 508	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
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**

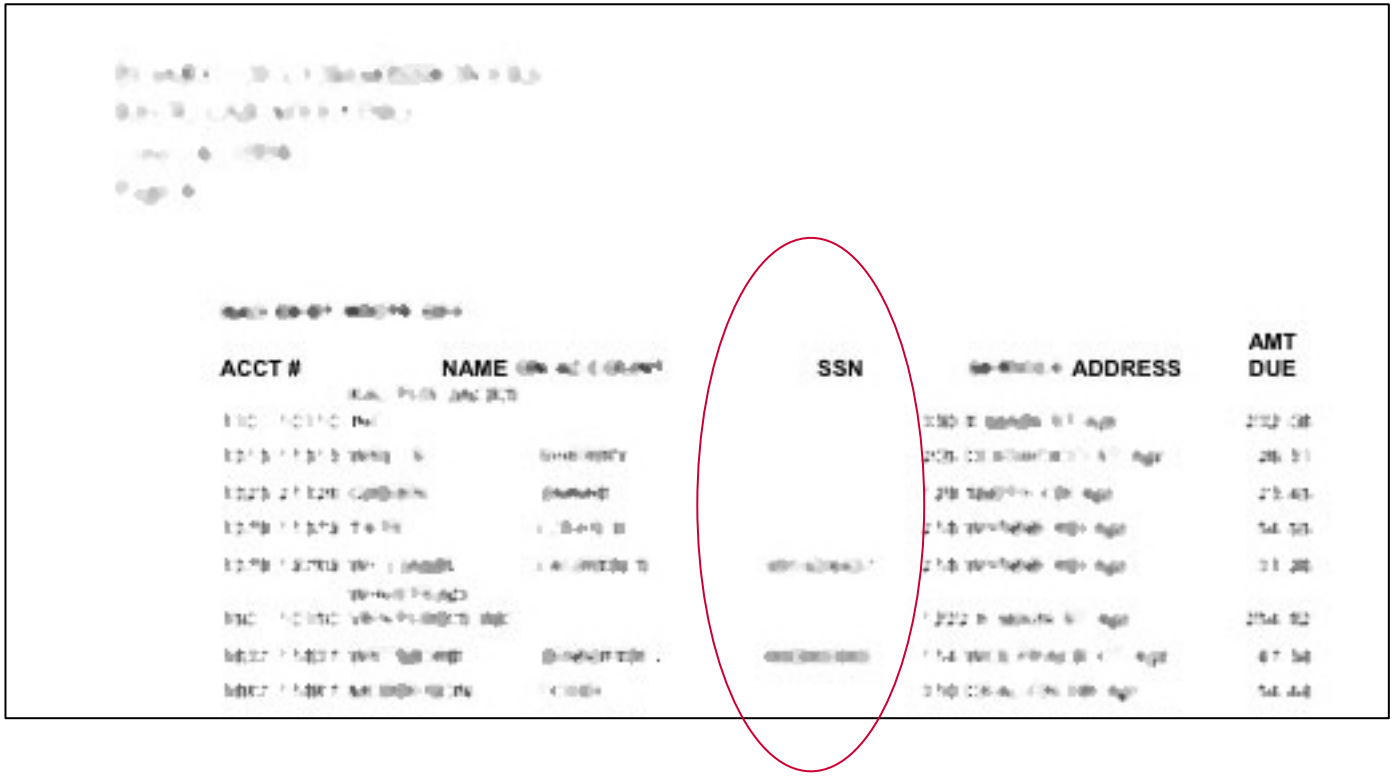
Page 1

	SSN	Student Name			
100	54 43				
100	64 69				
200 nds	64 15				
200 nds	70 09				
200 nds	80 90				
200 nds	60 22				
300 cot	62 23				
300 cot	62 23				
300 cot	80 60				
400 er	86 10				
400 er	70 24				
500 ticut	84 22				
500 ticut	76 33				
500	82 84				
500	76 71				
700 JCC	60 34				
200 uitas	93 08				
300 aga	66 60				

Google's cache says otherwise…

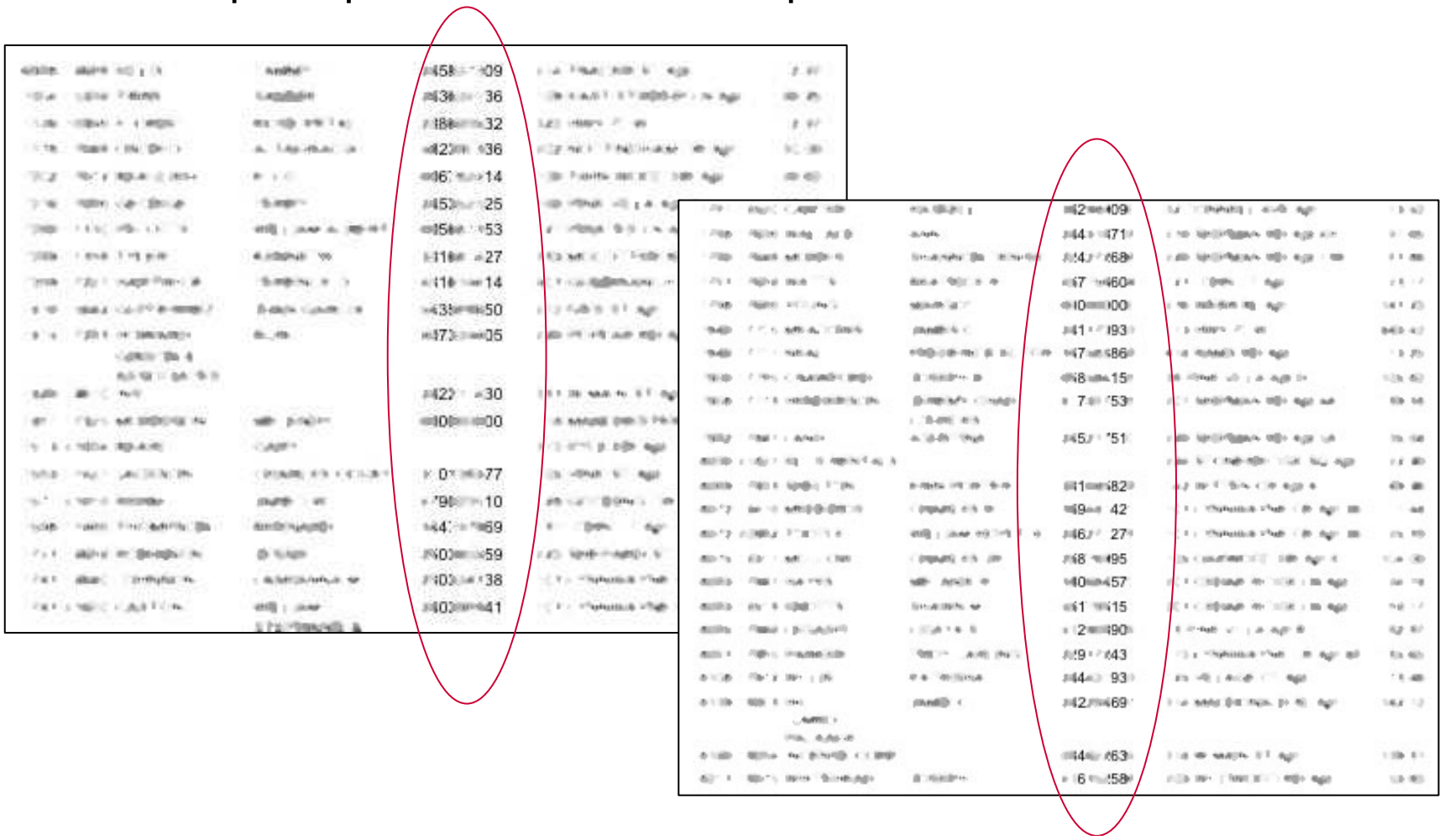
A tale of one city

- A city document outlining residents who are in debt to the city… A little report of names, addresses, amount owed and SSN numbers…



A tale of one city

- Or perhaps more than a little report…

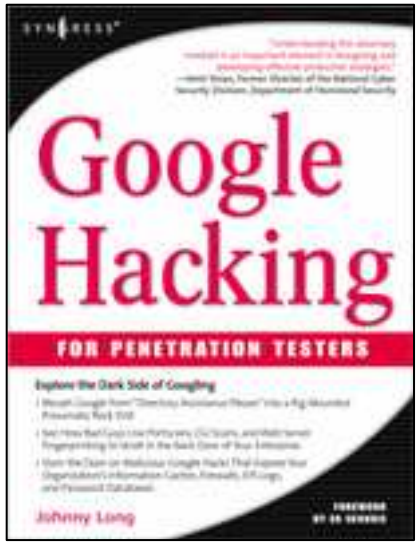


A tale of one city

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

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: Murfie, Jimmy Neutron, ThePsyko, Wasabi, l0om, Stonersavant
- Thanks to Roelof T for the great code, and to the current Google Masters: murfie, jimmyneutron, klouw, l0om, stonersavant, MILKMAN, ThePsyko, cybercide, yeseins, wolveso, Deadlink, crash_monkey, zoro25, digital.revolution, Renegade334, wasabi, urban, sfd, mlynch, Peefy, Vipsta, noAcces, brasileiro, john, Z!nCh