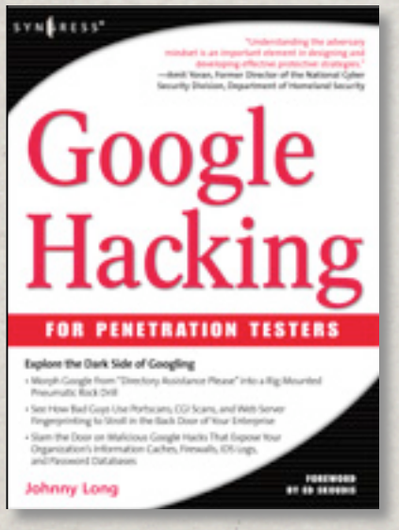
LUGBE

Google™ HACKING

Marc Herren

21. Juni 2007

Vorwort



In diesem Vortrag geht es darum die **Möglichkeiten** aufzuzeigen wie man mit Google auf bestimmte Informationen zugreifen kann.

Der Vortrag basiert auf Informationen und Beispielen aus dem Buch “Google Hacking” [1] von Johnny Long sowie seinem Vortrag von der Black Hat Europe Konferenz 2005.

Ebenfalls wurden Beispiel aus dem Vortrag von Robert Masse & Jian Hui Wang (GoSecure) “Hacking with Google for fun and profit!” [2] verwendet.

[1] http://johnny.ihackstuff.com/downloads/task,doc_details/gid,7/
[2] www.gosecure.ca/SecInfo/library/WebApplication/GOOGLE-HACKING-GS1004.ppt

Übersicht

- Wie funktioniert Google ?
- Anonymität
- Wie sucht man mit Google ?
- Wie sucht man gezielt mit Google ?
- Was kann man finden ;-)
- Automatisation
- Protect yourself!

Wie funktioniert Google?

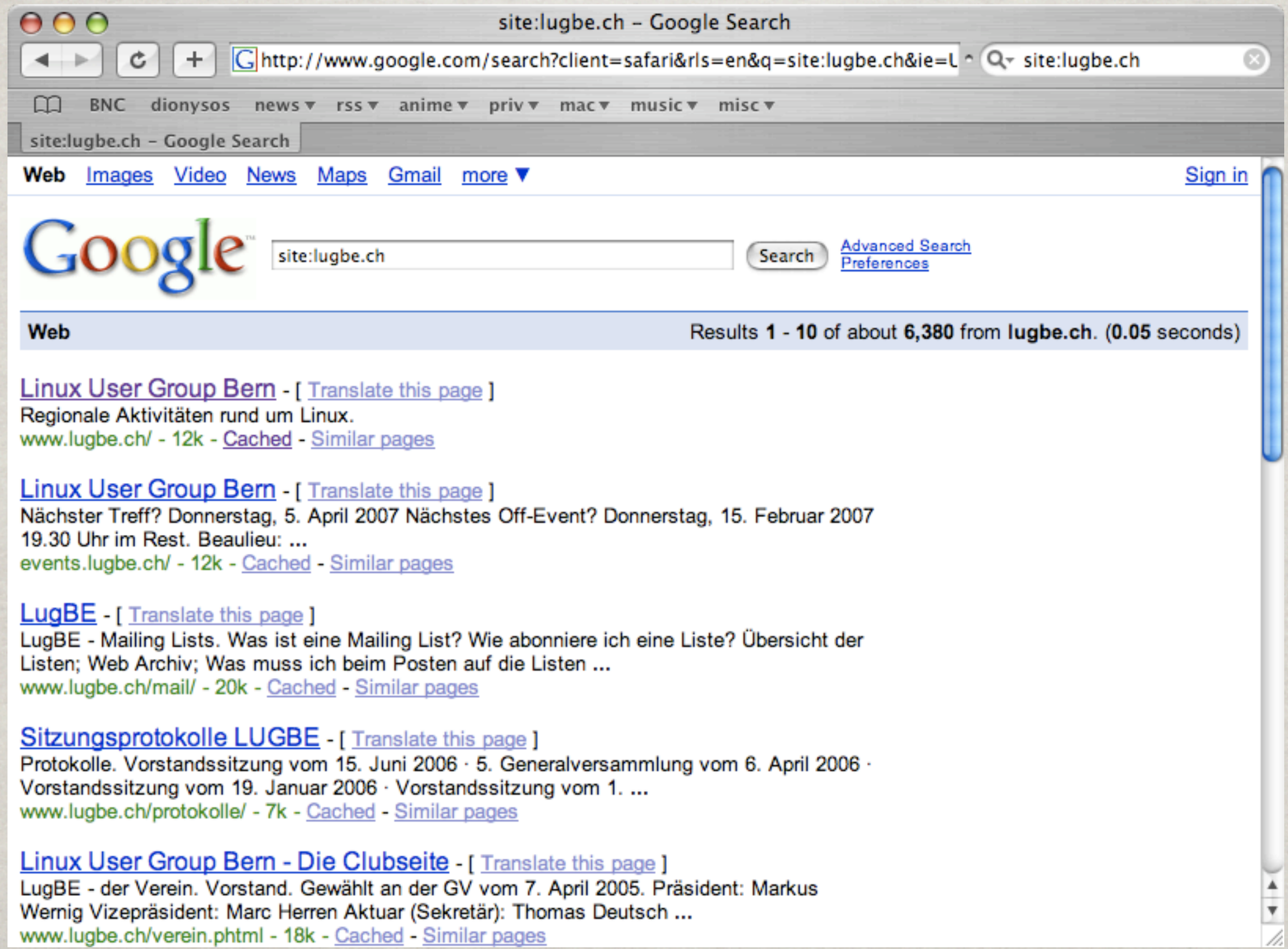
Google ist das einzige Unternehmen, das sich darauf konzentriert, die "perfekte Suchmaschine" zu entwickeln.

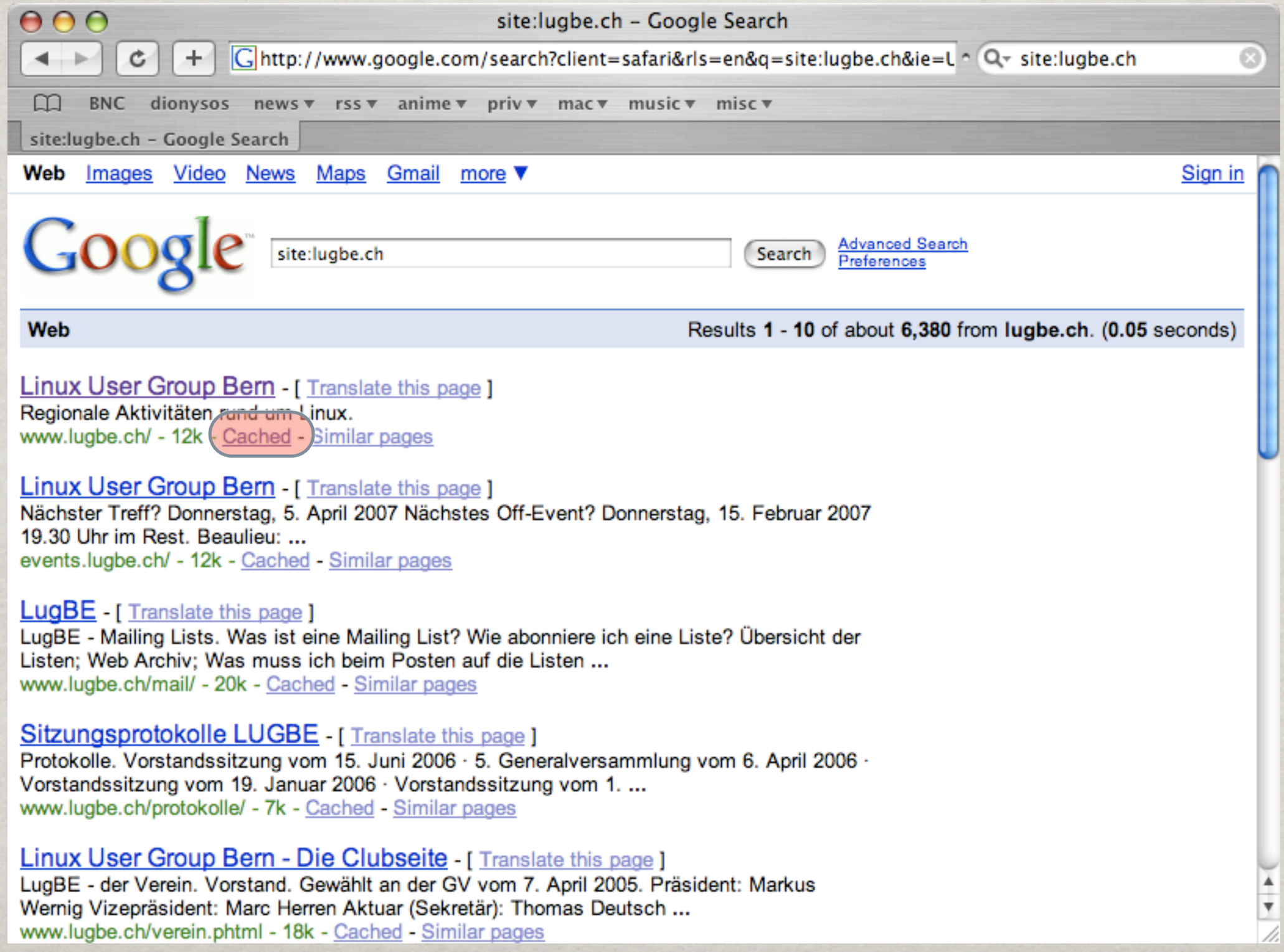
Der Mitbegründer von Google, Larry Page, sagt: "Die perfekte Suchmaschine würde genau erkennen, was der Nutzer meint, und genau die Ergebnisse ausgeben, die er sich wünscht"...

Die Suchmaschine von Google analysiert auch den Content einer Seite. Es werden jedoch der gesamte Content einer Seite und Faktoren wie Schriftarten, Unterteilungen und die genaue Position aller Begriffe auf der Seite analysiert, anstatt nur den seitenbasierten Text zu scannen (der über Metatags von Website-Publishern manipuliert werden kann).

http://www.google.de/corporate/tech.html

Anonymität


site:lugbe.ch – Google Search
http://www.google.com/search?client=safari&rls=en&q=site:lugbe.ch&ie=U
site:lugbe.ch
BNC dionysos news rss anime priv mac music misc
site:lugbe.ch – Google Search
Web Images Video News Maps Gmail more
Sign in
Google
site:lugbe.ch
Search
Advanced Search
Preferences
Web
Results 1 - 10 of about 6,380 from lugbe.ch. (0.05 seconds)
Linux User Group Bern - [Translate this page]
Regionale Aktivitäten rund um Linux.
www.lugbe.ch/ - 12k - Cached - Similar pages
Linux User Group Bern - [Translate this page]
Nächster Treff? Donnerstag, 5. April 2007 Nächstes Off-Event? Donnerstag, 15. Februar 2007 19.30 Uhr im Rest. Beaulieu: ...
events.lugbe.ch/ - 12k - Cached - Similar pages
LugBE - [Translate this page]
LugBE - Mailing Lists. Was ist eine Mailing List? Wie abonniere ich eine Liste? Übersicht der Listen; Web Archiv; Was muss ich beim Posten auf die Listen ...
www.lugbe.ch/mail/ - 20k - Cached - Similar pages
Sitzungsprotokolle LUGBE - [Translate this page]
Protokolle. Vorstandssitzung vom 15. Juni 2006 · 5. Generalversammlung vom 6. April 2006 · Vorstandssitzung vom 19. Januar 2006 · Vorstandssitzung vom 1. ...
www.lugbe.ch/protokolle/ - 7k - Cached - Similar pages
Linux User Group Bern - Die Clubseite - [Translate this page]
LugBE - der Verein. Vorstand. Gewählt an der GV vom 7. April 2005. Präsident: Markus Wernig Vizepräsident: Marc Herren Aktuar (Sekretär): Thomas Deutsch ...
www.lugbe.ch/verein.phtml - 18k - Cached - Similar pages


site:lugbe.ch - Google Search
http://www.google.com/search?client=safari&rls=en&q=site:lugbe.ch&ie=U
site:lugbe.ch
BNC dionysos news rss anime priv mac music misc
site:lugbe.ch - Google Search
Web Images Video News Maps Gmail more
Sign in
Google
site:lugbe.ch
Search
Advanced Search
Preferences
Web
Results 1 - 10 of about 6,380 from lugbe.ch. (0.05 seconds)
Linux User Group Bern - [Translate this page]
Regionale Aktivitäten rund um Linux.
www.lugbe.ch/ - 12k - Cached - Similar pages
Linux User Group Bern - [Translate this page]
Nächster Treff? Donnerstag, 5. April 2007 Nächstes Off-Event? Donnerstag, 15. Februar 2007 19.30 Uhr im Rest. Beaulieu: ...
events.lugbe.ch/ - 12k - Cached - Similar pages
LugBE - [Translate this page]
LugBE - Mailing Lists. Was ist eine Mailing List? Wie abonniere ich eine Liste? Übersicht der Listen; Web Archiv; Was muss ich beim Posten auf die Listen ...
www.lugbe.ch/mail/ - 20k - Cached - Similar pages
Sitzungsprotokolle LUGBE - [Translate this page]
Protokolle. Vorstandssitzung vom 15. Juni 2006 · 5. Generalversammlung vom 6. April 2006 · Vorstandssitzung vom 19. Januar 2006 · Vorstandssitzung vom 1. ...
www.lugbe.ch/protokolle/ - 7k - Cached - Similar pages
Linux User Group Bern - Die Clubseite - [Translate this page]
LugBE - der Verein. Vorstand. Gewählt an der GV vom 7. April 2005. Präsident: Markus Wernig Vizepräsident: Marc Herren Aktuar (Sekretär): Thomas Deutsch ...
www.lugbe.ch/verein.phtml - 18k - Cached - Similar pages

site:lugbe.ch - Google Search

http://www.google.com/search?client=safari&rls=en&q=site:lugbe.ch&ie=U

site:lugbe.ch

BNC dionysos news rss anime priv mac music misc

site:lugbe.ch - Google Search

Web Images Video News Maps Gmail more ▼ Sign in

Google site:lugbe.ch Search Advanced Search Preferences

Web Results **1** - **10** of about **6,380** from **lugbe.ch**. (**0.05** seconds)

Linux User Group Bern - [Translate this page]
Regionale Aktivitäten rund um Linux.
www.lugbe.ch/ - 12k - Cached - Similar pages

Wo kommen diese Informationen her ?

Linux User Group Bern - [Translate this page]
Nächster Treff? Donnerstag, 5. April 2007 Nächstes Off-Event? Donnerstag, 15. Februar 2007 19.30 Uhr im Rest. Beaulieu: ...
events.lugbe.ch/ - 12k - Cached - Similar pages

LugBE - [Translate this page]
LugBE - Mailing Lists. Was ist eine Mailing List? Wie abonniere ich eine Liste? Übersicht der Listen; Web Archiv; Was muss ich beim Posten auf die Listen ...
www.lugbe.ch/mail/ - 20k - Cached - Similar pages

Sitzungsprotokolle LUGBE - [Translate this page]
Protokolle. Vorstandssitzung vom 15. Juni 2006 · 5. Generalversammlung vom 6. April 2006 · Vorstandssitzung vom 19. Januar 2006 · Vorstandssitzung vom 1. ...
www.lugbe.ch/protokolle/ - 7k - Cached - Similar pages

Linux User Group Bern - Die Clubseite - [Translate this page]
LugBE - der Verein. Vorstand. Gewählt an der GV vom 7. April 2005. Präsident: Markus Wernig Vizepräsident: Marc Herren Aktuar (Sekretär): Thomas Deutsch ...
www.lugbe.ch/verein.phtml - 18k - Cached - Similar pages

Tcpdump des Interfaces

```
blackgate:~ marc$ sudo tcpdump -q -i en1 port 80
Password:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en1, link-type EN10MB (Ethernet), capture size 96 bytes
21:23:45.700610 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 0
21:23:45.743744 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 0
21:23:45.743791 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 0
21:23:45.744062 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 469
21:23:45.797389 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 0
21:23:45.885395 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 1408
21:23:45.888293 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 1408
21:23:45.888332 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 0
21:23:45.891231 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 1408
21:23:45.934401 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 1120
21:23:45.934435 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 0
21:23:46.108236 IP 192.168.100.162.55001 > kalinka.catatec.ch.http: tcp 0
21:23:46.121137 IP kalinka.catatec.ch.http > 192.168.100.162.55001: tcp 0
```

Tcpdump des Interfaces

```
blackgate:~ marc$ sudo tcpdump -q -i en1 port 80
Password:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en1, link-type EN10MB (Ethernet), capture size 96 bytes
21:23:45.700610 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 0
21:23:45.743744 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 0
21:23:45.743791 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 0
21:23:45.744062 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 469
21:23:45.797389 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 0
21:23:45.885395 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 1408
21:23:45.888293 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 1408
21:23:45.888332 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 0
21:23:45.891231 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 1408
21:23:45.934401 IP lm-in-f104.google.com.http > 192.168.100.162.55000: tcp 1120
21:23:45.934435 IP 192.168.100.162.55000 > lm-in-f104.google.com.http: tcp 0
21:23:46.108236 IP 192.168.100.162.55001 > kalinka.catatec.ch.http: tcp 0
21:23:46.121137 IP kalinka.catatec.ch.http > 192.168.100.162.55001: tcp 0
```

Tcpdump des Interfaces

```
blackgate:~ marc$ sudo tcpdump -A -i en1 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en1, link-type EN10MB (Ethernet), capture size 96 bytes

21:28:12.187153 IP 192.168.100.162.55019 > kalinka.catatec.ch.http:
P 373:754(381) ack 1795 win 65535 <nop,nop,timestamp 11433676 117860444>
E.....@.@..R..d..gBD...P.Q.KA........Y.....
..v...h\GET /images/lugbe_logo_med.jpg
```

Tcpdump des Interfaces

```
blackgate:~ marc$ sudo tcpdump -A -i en1 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en1, link-type EN10MB (Ethernet), capture size 96 bytes

21:28:12.187153 IP 192.168.100.162.55019 > kalinka.catatec.ch.http:
P 373:754(381) ack 1795 win 65535 <nop,nop,timestamp 11433676 117860444>
E.....@.@..R..d..gBD...P.Q.KA........Y.....
..v...h\GET /images/lugbe_logo_med.jpg
```

Wird ein Bild geladen so wird der wirkliche Server angefragt.

Linux User Group Bern

http://66.102.9.104/search?q=cache:DlruG3vLLDMJ:www.lugbe.ch/+site:lu

site:lugbe.ch

BNC dionysos news rss anime priv mac music misc

Linux User Group Bern

This is G o o g l e's cache of http://www.lugbe.ch/ as retrieved on 9 Jun 2007 01:16:26 GMT.
G o o g l e'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:DlruG3vLLDMJ:www.lugbe.ch/+site:lugbe.ch&hl=en&ct=clnk&cd=1&client=safari`

Google is neither affiliated with the authors of this page nor responsible for its content.

Über die LugBE | Mailing List | Treff & Events | Projekte | lost+found | Supp

Willkommen bei der LugBE

(Linux User Group Bern)

Die LugBE ist eine Gruppe von GNU/Linux- / Unix- / BSD-Interessierten (und
;-) im Raum Bern. Wir treffen uns einmal monatlich zum gemütlichen Fachsim
Projekteschmieden ..., und einmal monatlich gibt's ein "Off-Event": Vorträge,
Install- oder sonstige Parties. (siehe Treff & Events)
Unsere Treffs sind öffentlich - das "reguläre" Treffen ist grundsätzl
jeden 1. Donnerstag im Monat.

Linux User Group Bern

http://66.102.9.104/search?q=cache:DlruG3vLLDMJ:www.lugbe.ch/+site:lu

site:lugbe.ch

BNC dionysos news rss anime priv mac music misc

Linux User Group Bern

This is G o o g l e's cache of http://www.lugbe.ch/ as retrieved on 9 Jun 2007 01:16:26 GMT.
G o o g l e'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:DlruG3vLLDMJ:www.lugbe.ch/+site:lugbe.ch&hl=en&ct=clnk&cd=1&client=safari

Google is neither affiliated with the authors of this page nor responsible for its content.

Über die LugBE | Mailing List | Treff & Events | Projekte | lost+found | Supp

Willkommen bei der LugBE

(Linux User Group Bern)

Die LugBE ist eine Gruppe von GNU/Linux- / Unix- / BSD-Interessierten (und
;-) im Raum Bern. Wir treffen uns einmal monatlich zum gemütlichen Fachsim
Projekteschmieden ..., und einmal monatlich gibt's ein "Off-Event": Vorträge,
Install- oder sonstige Parties. (siehe Treff & Events)
Unsere Treffs sind öffentlich - das "reguläre" Treffen ist grundsätzl
jeden 1. Donnerstag im Monat.

Tcpdump des Interfaces

```
blackgate:~ marc$ sudo tcpdump -q -i en1 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on en1, link-type EN10MB (Ethernet), capture size 96 bytes
21:33:36.887585 IP 192.168.100.162.55034 > lm-in-f104.google.com.http: tcp 0
21:33:36.930301 IP lm-in-f104.google.com.http > 192.168.100.162.55034: tcp 0
21:33:36.930343 IP 192.168.100.162.55034 > lm-in-f104.google.com.http: tcp 0
21:33:36.930625 IP 192.168.100.162.55034 > lm-in-f104.google.com.http: tcp 439
21:33:36.979817 IP lm-in-f104.google.com.http > 192.168.100.162.55034: tcp 0
21:33:37.062363 IP lm-in-f104.google.com.http > 192.168.100.162.55034: tcp 1408
21:33:37.065264 IP lm-in-f104.google.com.http > 192.168.100.162.55034: tcp 1408
21:33:37.065307 IP 192.168.100.162.55034 > lm-in-f104.google.com.http: tcp 0
21:33:37.065380 IP lm-in-f104.google.com.http > 192.168.100.162.55034: tcp 20
21:33:37.065404 IP 192.168.100.162.55034 > lm-in-f104.google.com.http: tcp 0
21:33:37.110405 IP lm-in-f104.google.com.http > 192.168.100.162.55034: tcp 1408
21:33:37.112234 IP lm-in-f104.google.com.http > 192.168.100.162.55034: tcp 593
21:33:37.112264 IP 192.168.100.162.55034 > lm-in-f104.google.com.http: tcp 0
```

Vergleichen wir die URLS

```
http://66.102.9.104/search?q=cache:DlruG3vLLDMJ:www.lugbe.ch/
+site:lugbe.ch&hl=en&ct=clnk&cd=1&client=safari


http://66.102.9.104/search?q=cache:DlruG3vLLDMJ:www.lugbe.ch/
+site:lugbe.ch&hl=en&client=safari&strip=1
```

Vergleichen wir die URLS

```
http://66.102.9.104/search?q=cache:DlruG3vLLDMJ:www.lugbe.ch/
+site:lugbe.ch&hl=en&ct=clnk&cd=1&client=safari
```

```
http://66.102.9.104/search?q=cache:DlruG3vLLDMJ:www.lugbe.ch/
+site:lugbe.ch&hl=en&client=safari&strip=1
```

Vergleichen wir die URLS

```
http://66.102.9.104/search?q=cache:DlruG3vLLDMJ:www.lugbe.ch/
+site:lugbe.ch&hl=en&ct=clnk&cd=1&client=safari
```

```
http://66.102.9.104/search?q=cache:DlruG3vLLDMJ:www.lugbe.ch/
+site:lugbe.ch&hl=en&client=safari&strip=1
```

Damit können wir auch Webseiten ansurfen welcher ein Proxy sperrt ;)

Basis Operatoren

+ Bedingt den Einschluss eines Begriffes

Google ignoriert standtartmässig gebräuchliche Wörter (where, how, Zahlen, einzelne Buchstaben):

Beispiel: Star Wars Episode +I

- Auschluss eines Begriffes

Beispiel: apfel -rot

“ Mit Anführungszeichen kann man nach exakten Ausdrücken suchen:

Beispiel: “Marc Herren”

Marc Herren ohne “” liefert 1470000 Ergebnisse, “Marc Herren” hingegen nur 9150. Somit wurden 99.4% der irrelevanten Ergebnisse herausgefiltert.

Basis Operatoren

~ Suche nach Synonymen:

Beispiel: ~food

Die Ergebnisse beinhaltet alles über Essen sowie Rezepte, Ernährung usw.

. Ein single-character wildcard:

Example: m.trix

Ergibt als Ergebnisse alles über M@trix, matrix, metrix…….

***** jegliches Wort wildcard

Fortgeschrittene Operatoren

Google advanced operators helfen dabei die Suche zu verfeinern. Sie werden als Teil direkt in den Google Suchbegriff integriert.

Diese Operatoren verwenden folgenden Grundsyntax:

operator:search_term

Es gibt keine Leerzeichen zwischen dem Operator, dem Doppelpunkt und dem Suchbegriff!

Advanced Operators Site:

Findet Webseiten welche nur zu der spezifizierten Domäne assoziiert sind. Damit kann eine Struktur der Domäne ausfindig gemacht werden.

Beispiel:

- *site:ch*
- *site:lugbe.ch*
- *site:www.lugbe.ch*

Beispiel www.search.ch

http://www.google.com/search?q=site%3Asearch.ch+&btnG=Search

Beispiel www.search.ch

http://www.google.com/search?q=site%3Asearch.ch+&btnG=Search

meteo.search.ch

news.search.ch

tv.search.ch

werbearena.search.ch

date.search.ch

ferien.search.ch

...

Advanced Operators `Filetype:`

Findet Dokumente mit den spezifizierten Endungen.

Auswahl aus den möglichen Endungen:
- HyperText Markup Language (html)
- Microsoft PowerPoint (ppt)
- Adobe Portable Document Format (pdf)
- Microsoft Word (doc)
- Adobe PostScript (ps)
- Microsoft Works (wks, wps, wdb)
- Microsoft Excel (xls)
- Rich Text Format (rtf)
- Shockwave Flash (swf)
- Text (ans, txt)

...

Beispiel: *Budget filetype:xls*

Advanced Operators Intitel:

Intitel: Suchbegriff

Findet Webseiten mit den spezifizierten Suchbegriff im Titel.

Allintitle: Suchbegriff_1 Suchbegriff_2

Findet Webseiten mit all den spezifizierten Suchbegriffen im Titel.

Beispiel: Intitle: Index.of “parent directory”

Advanced Operators Inurl:

Inurl: Suchbegriff

Findet Webseiten mit den spezifizierten Suchbegriff in der URL.

Allinurl: Suchbegriff_1 Suchbegriff_2

Findet Webseiten mit all den spezifizierten Suchbegriffen in der URL.

Beispiel:

Inurl: cgi-bin

Allinurl: cgi-bin password

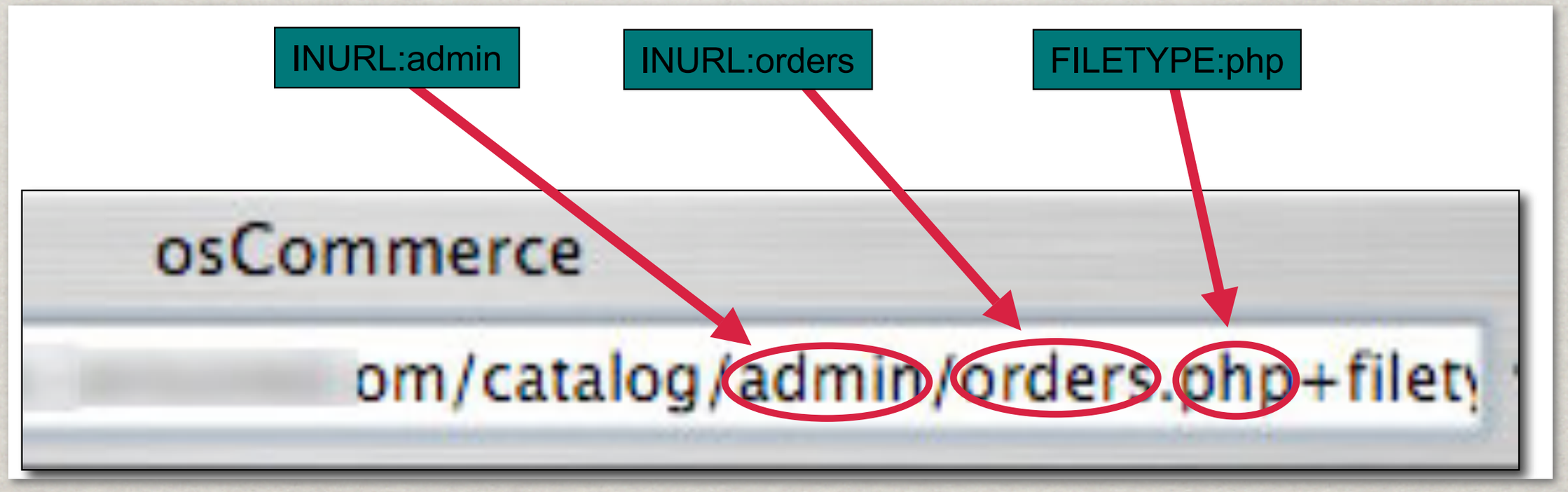
Google HACKING

- Wie sucht man gezielt mit Google ?

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

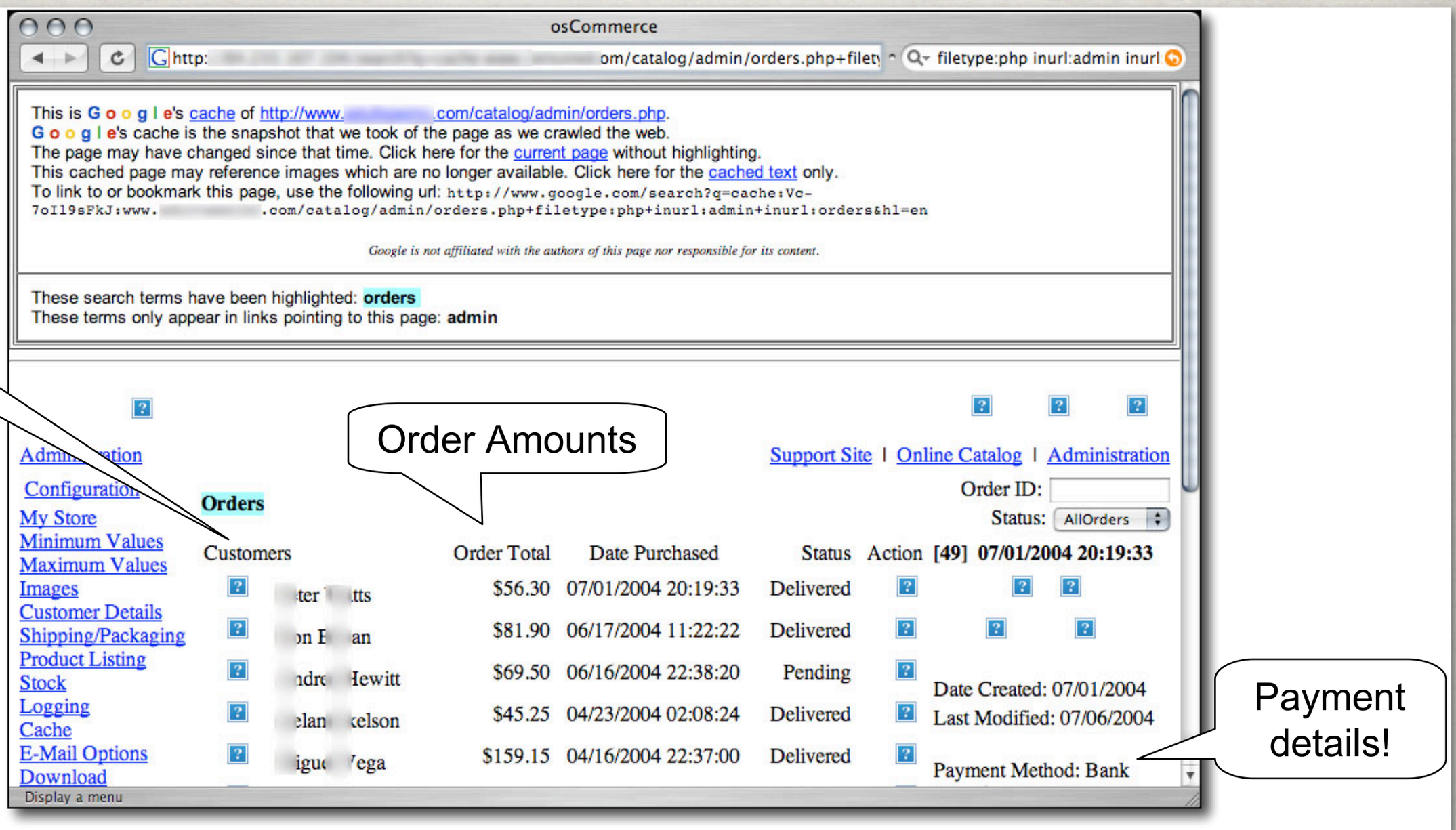
Google HACKING

- Wie sucht man gezielt mit Google ?

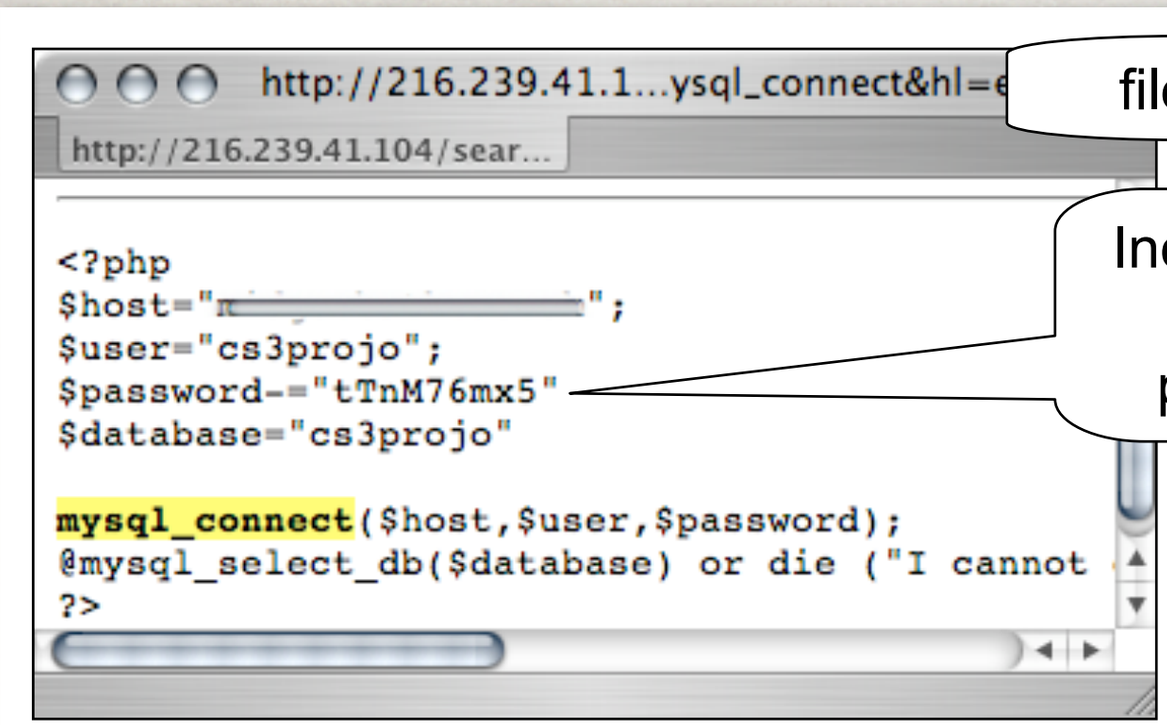


Google HACKING

• Wie sucht man gezielt mit Google ?

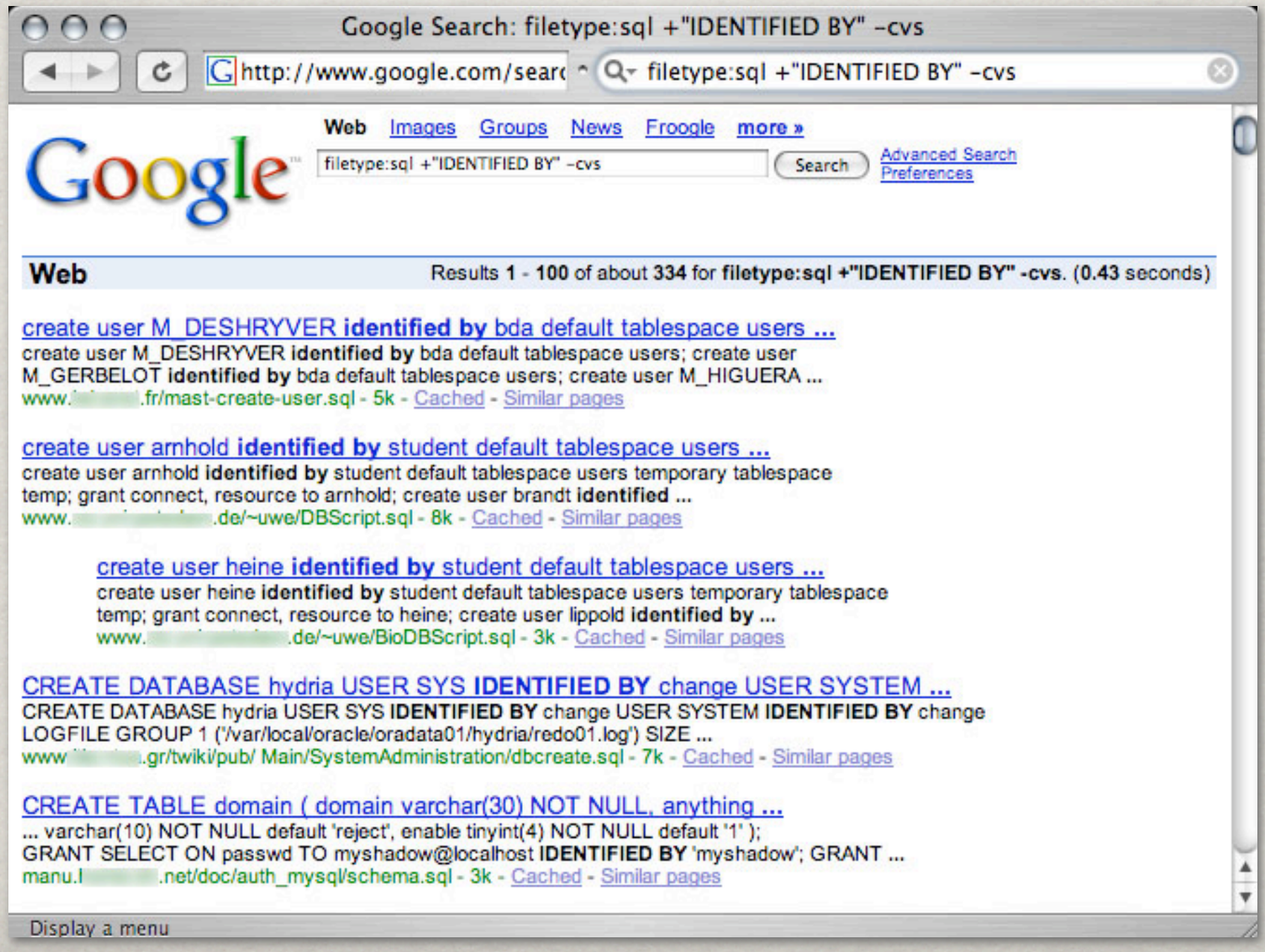


SQL Passwörter



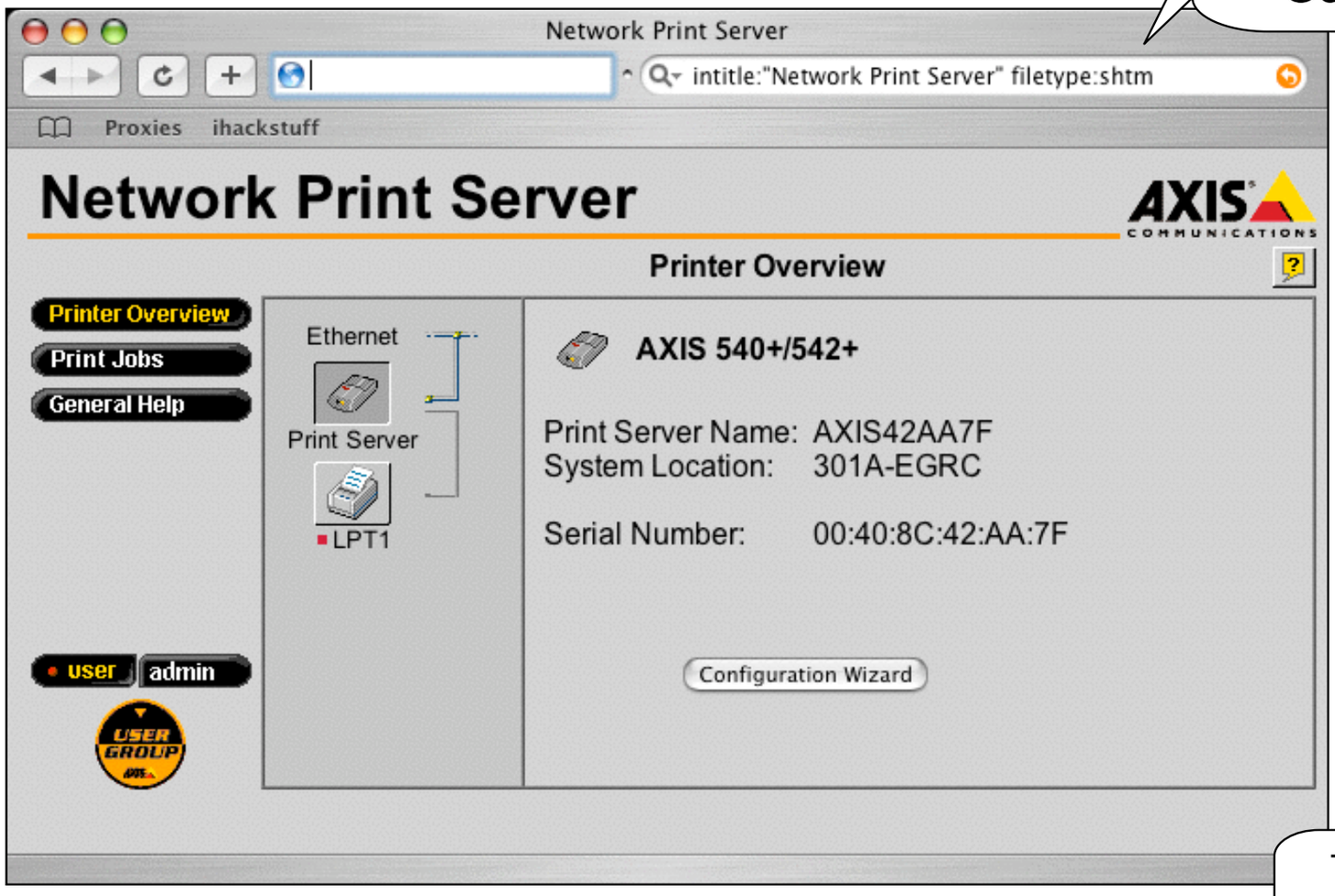
SQL Passwörter

filetype:sql +"IDENTIFIED BY" -cvs



Axis Print Servers

Print server administration, Google-style!



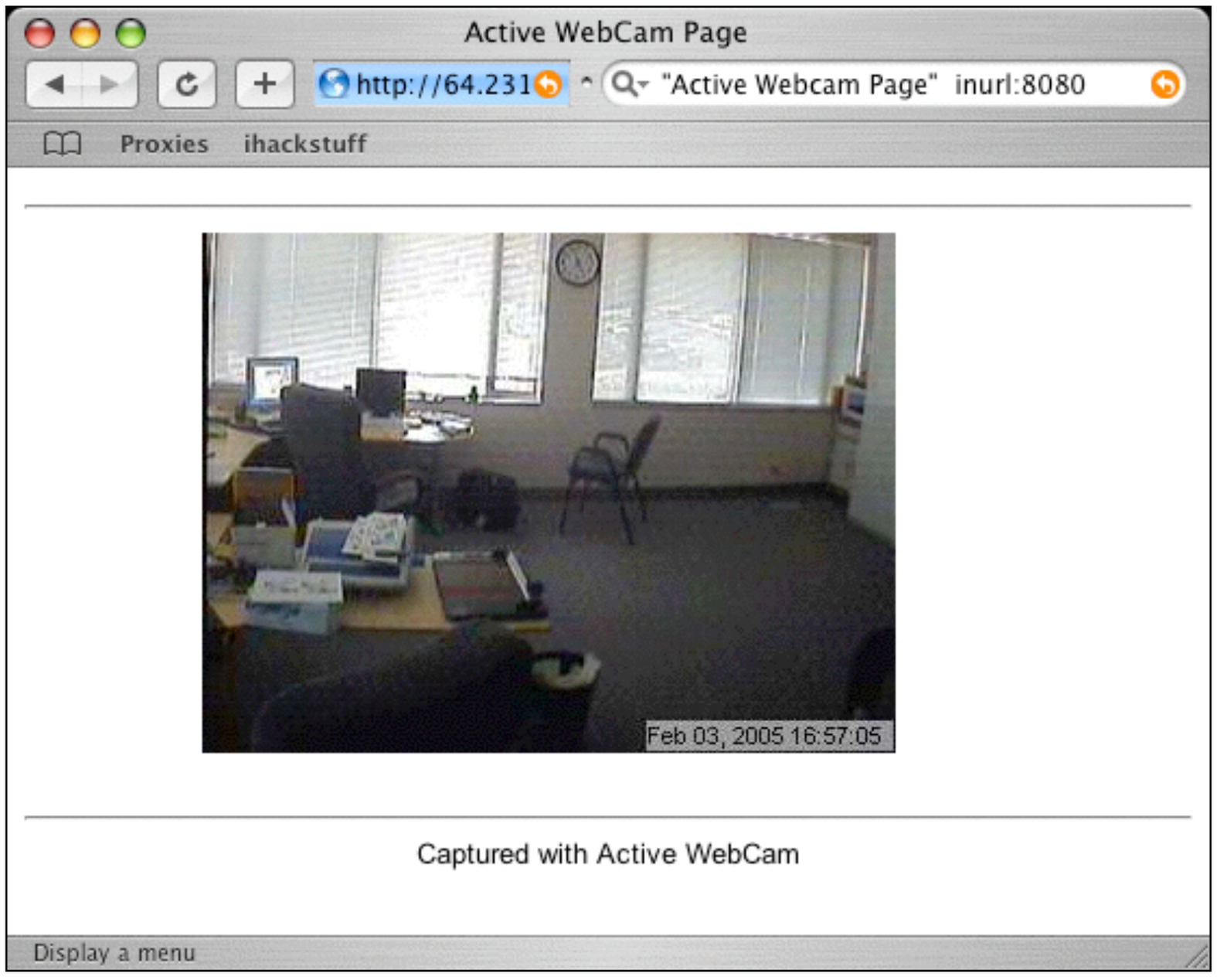
Thanks to murfie for this one!

Xenix, Sweex, Orite Web Cams

One query, many brands of live cams!

Thanks to server1 for this one!

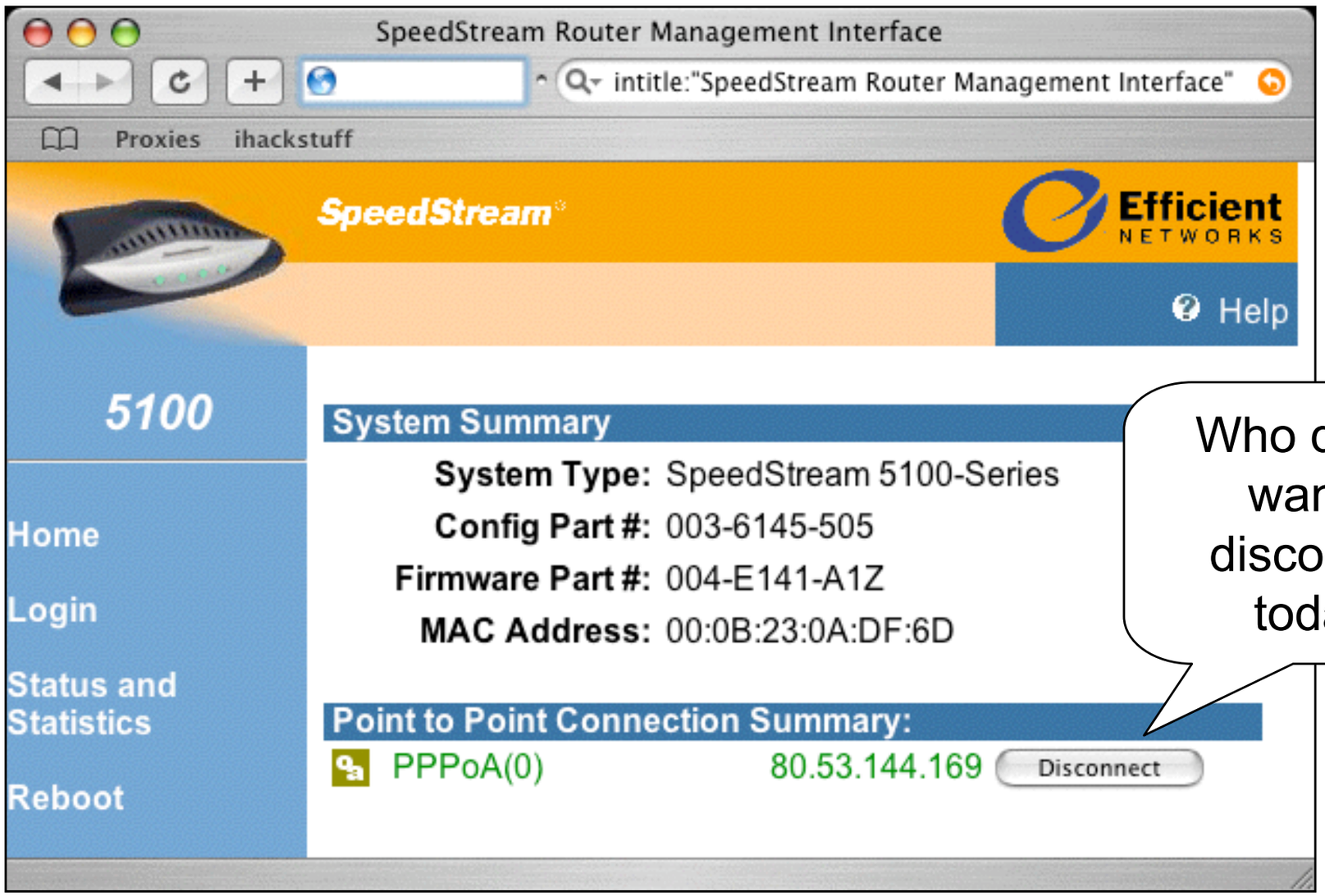
Active WebCam



Thanks klouw!

Speedstream DSL Routers

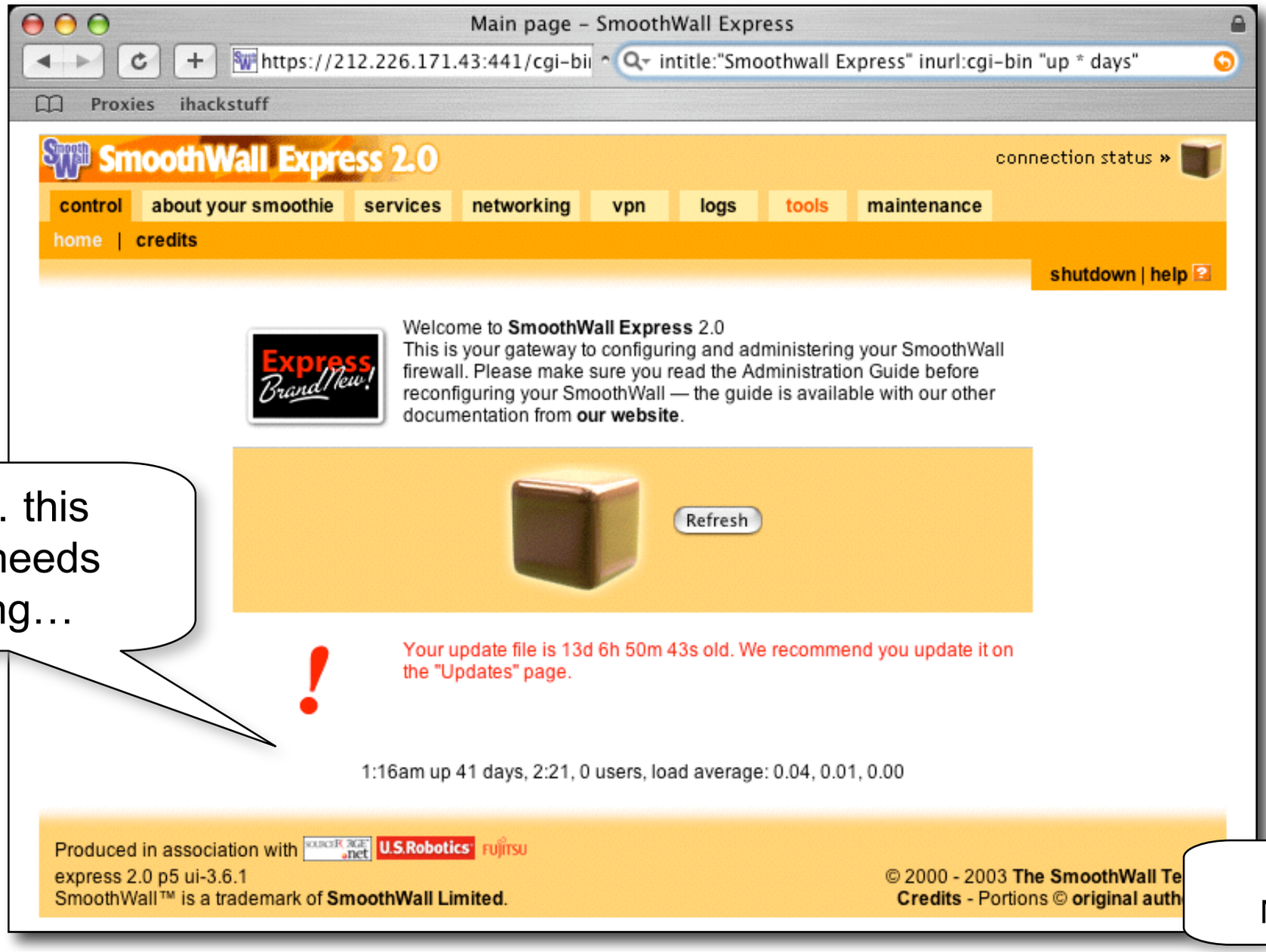
- Home broadband connectivity… Googled.



Who do you want to disconnect today?

Found by m00d!

Firewalls - Smoothwall

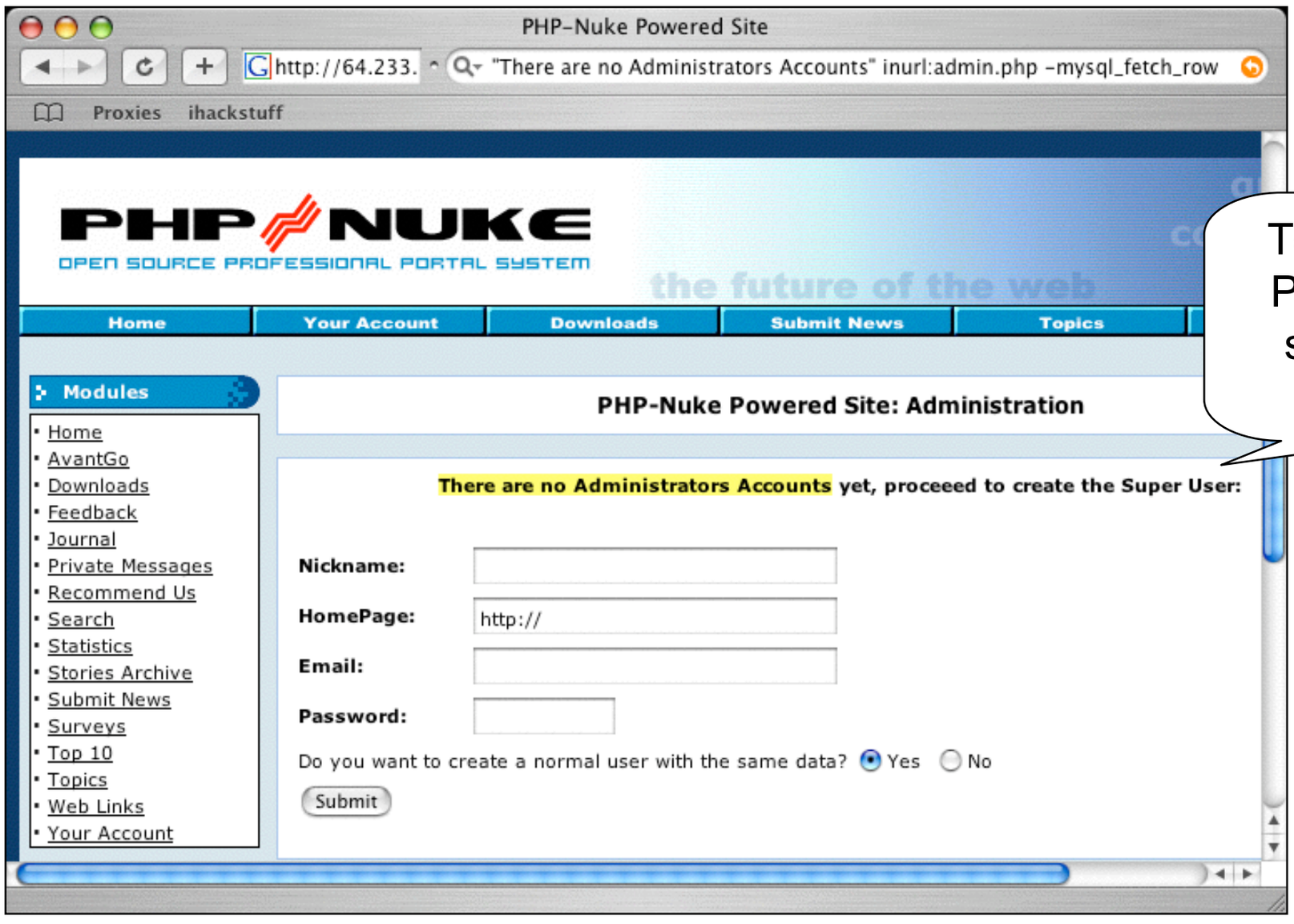


Uh oh… this firewall needs updating…

Thanks Milkman!

Wide Open PHP Nuke Sites

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



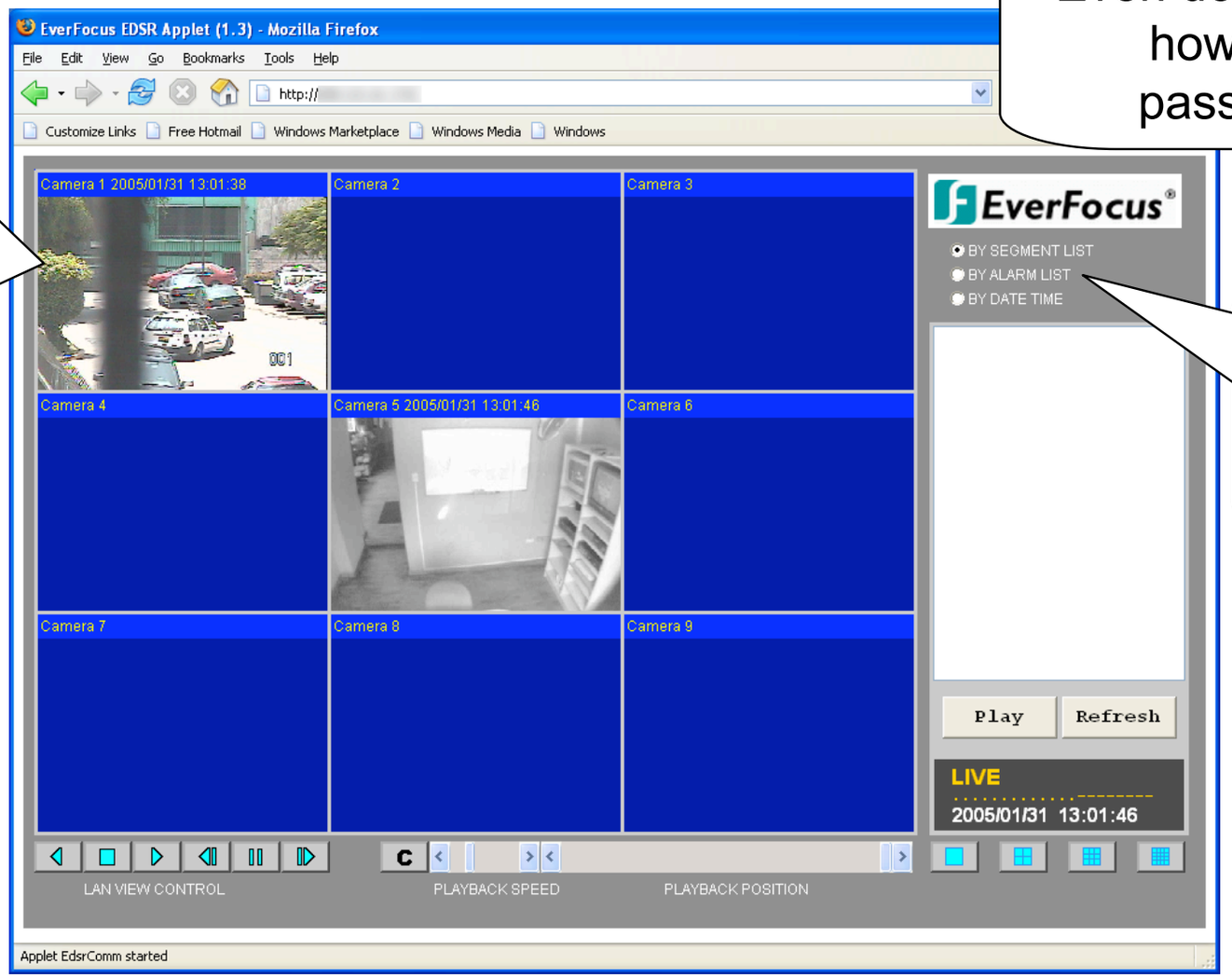
Too lazy to install PHP Nuke? Own someone else's site instead!

Thanks to arrested for this beauty!

Time lapse video recorders

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

…multiple live security camera views…

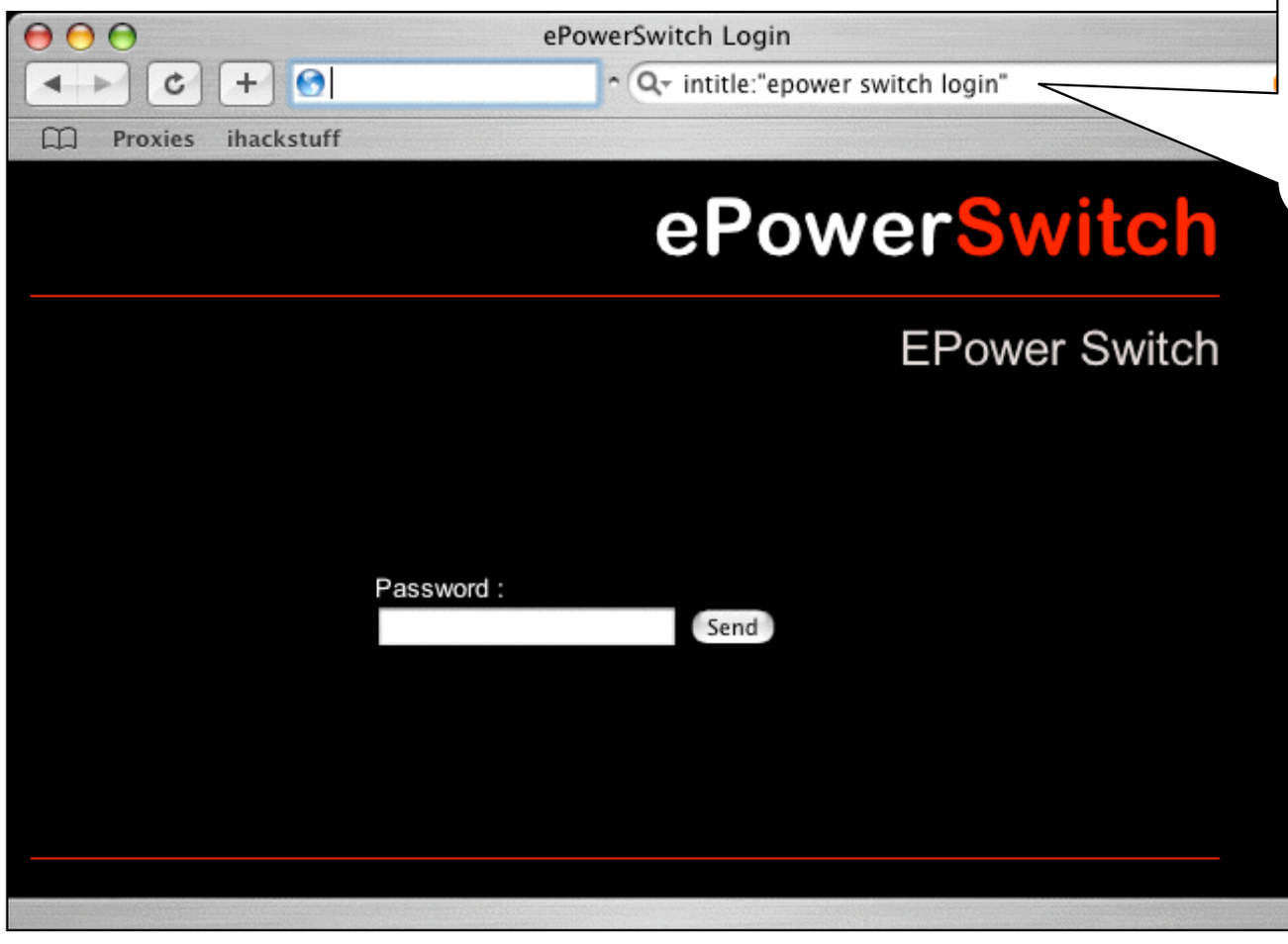


…and historical records of recorded video feeds

Thanks to stonersavant for this beauty!

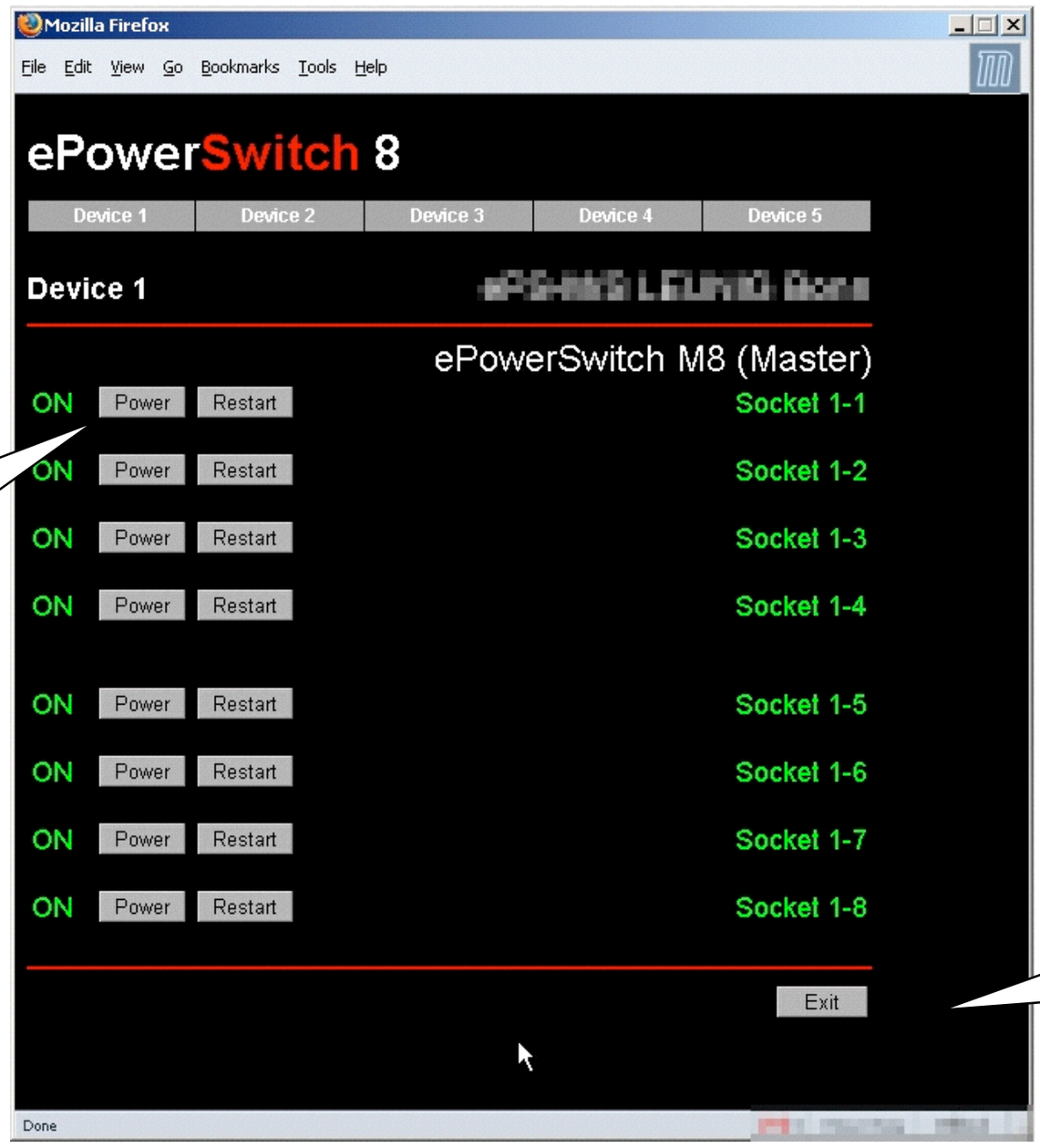
Hacking POWER Systems!

- 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!

Norton AntiVirus Corporate Passwords

Encrypted, but yummy (and crackable)!

Thanks MILKMAN!

Automatisierung

http://code.google.com/apis/

Es gab vor rein paar Jahren eine Google API mit welcher man automatisierte Suchabfragen durchführen konnte.

Doch auch ohne diese API kann man relativ einfach gewisse Abfragen automatisiert durchführen.

Automatisierung

Automatisierte Domänen Analyse mit lynx & sed/awk

Automatisierung

Automatisierte Domänen Analyse mit lynx & sed/awk

Zuerst werden die Daten gesammelt:

Automatisierung

Automatisierte Domänen Analyse mit lynx & sed/awk

Zuerst werden die Daten gesammelt:

```
lynx -dump "http://www.google.com/search?hl=en&q=site%
3Asearch.ch++-site%3Amap.search.ch&num=100" > test.html
```

Automatisierung

Automatisierte Domänen Analyse mit lynx & sed/awk

Zuerst werden die Daten gesammelt:

```
lynx -dump "http://www.google.com/search?hl=en&q=site%
3Asearch.ch++-site%3Amap.search.ch&num=100" > test.html
```

Danach ausgewertet:

Automatisierung

Automatisierte Domänen Analyse mit lynx & sed/awk

Zuerst werden die Daten gesammelt:

```
lynx -dump "http://www.google.com/search?hl=en&q=site%
3Asearch.ch++-site%3Amap.search.ch&num=100" > test.html
```

Danach ausgewertet:

```
sed -n 's/\. [[:alpha:]]*:\/\/[[:alnum:]]*.search.ch\//
& /p' test.html | awk '{print $2} '
```

Automatisierung

Automatisierte Domänen Analyse mit lynx & sed/awk

Zuerst werden die Daten gesammelt:

```
lynx -dump "http://www.google.com/search?hl=en&q=site%
3Asearch.ch++-site%3Amap.search.ch&num=100" > test.html
```

Danach ausgewertet:

```
sed -n 's/\. [[:alpha:]]*:\/\/[[:alnum:]]*.search.ch\//
& /p' test.html | awk '{print $2} '
```

Noch Besser!: Man nimmt das DNS Predict Perl Script von Jimmy Neutron von jonny.ihackstuff.com

Automatisierung

Default (156,34)

New Info Bookmarks Close

Default 1

```
blackgate:~ marc$ perl Documents/lugbe/vortraege/goggle\ hacking/dnspredict.pl --domain free.fr --item1 frodo --item2 aragorn
DNS Predictor by Jimmy Neutron 0.0.2

Warning: You aren't using a proxy. Remeber that this program is doing a direct g00gle scrapingAragorn   Resolving Aragorn.free.fr      -
Frodo   Resolving Frodo.free.fr -
Gandalf Resolving Gandalf.free.fr       -
Galadriel       Resolving Galadriel.free.fr     -
Legolas Resolving Legolas.free.fr       -
Gimli   Resolving Gimli.free.fr -
Boromir Resolving Boromir.free.fr       -
Arwen   Resolving Arwen.free.fr -
Gollum  Resolving Gollum.free.fr        212.27.63.150
Saruman Resolving Saruman.free.fr       -
Bilbo   Resolving Bilbo.free.fr 212.27.63.133
Merry   Resolving Merry.free.fr 212.27.63.125
Sam     Resolving Sam.free.fr   212.27.63.125
Pippin  Resolving Pippin.free.fr        -
Elrond  Resolving Elrond.free.fr        212.27.63.113
Eowyn   Resolving Eowyn.free.fr 212.27.63.139
Celeborn        Resolving Celeborn.free.fr      212.27.63.149
Faramir Resolving Faramir.free.fr       -
Eomer   Resolving Eomer.free.fr -
Sauron  Resolving Sauron.free.fr        212.27.63.146
Theoden Resolving Theoden.free.fr       -
Denethor        Resolving Denethor.free.fr      212.27.63.101
Radagast        Resolving Radagast.free.fr      -
Isildur Resolving Isildur.free.fr       212.27.63.125
Grima   Resolving Grima.free.fr 212.27.63.150
Orcs    Resolving Orcs.free.fr  212.27.63.125
Galva   Resolving Galva.free.fr -
Cirdan  Resolving Cirdan.free.fr        -
Beorn   Resolving Beorn.free.fr -
Celebrimbor     Resolving Celebrimbor.free.fr   -
blackgate:~ marc$
```

Protect yourself!

Apache (httpd.conf):

```
Options -Indexes FollowSymlinks MultiViews
```

Robots.txt (http://www.robotstxt.org):

```
#Away from my PDF files, Google!
User-Agent: Googlebot
Disallow: /*.PDF$
```

```
#Complete block
User-Agent: *
Disallow: /
```

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

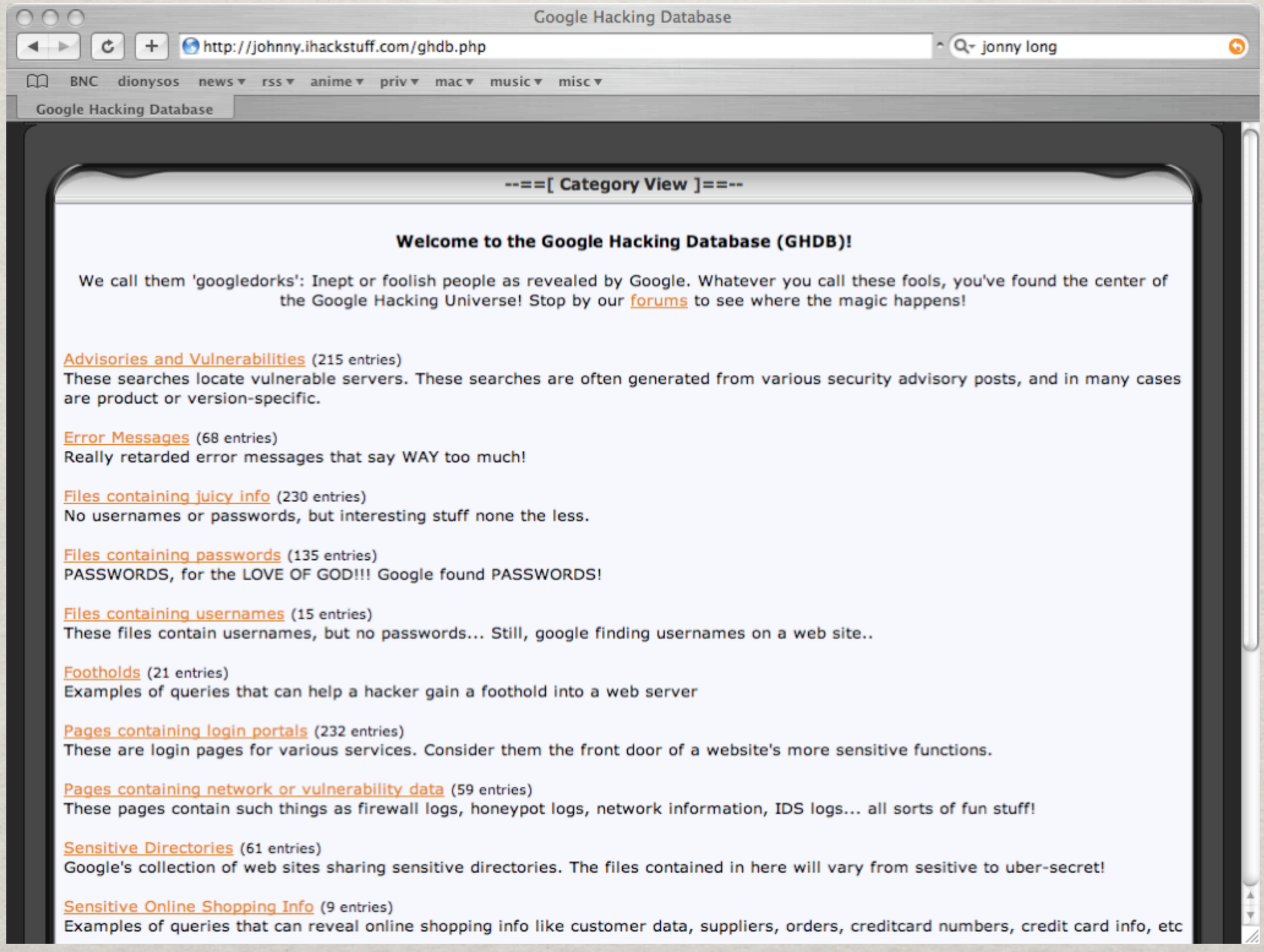
Links

http://johnny.ihackstuff.com

http://www.sensepost.com/

http://www.gosecure.ca

GHDB



http://johnny.ihackstuff.com/ghdb.php