



LUGBE

GoogleTM HACKING

Marc Herren
21. Juni 2007



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



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



LugBE

Wie funktioniert Google?

Google
HACKING

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>



LugBE

Anonymität

Google HACKING

site:lugbe.ch - Google Search

http://www.google.com/search?client=safari&rls=en&q=site:lugbe.ch&ie=L 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](#)



LugBE

Anonymität

Google HACKING

site:lugbe.ch - Google Search

http://www.google.com/search?client=safari&rls=en&q=site:lugbe.ch&ie=L 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](#)



LugBE

Anonymität

Google HACKING

site:lugbe.ch - Google Search

http://www.google.com/search?client=safari&rls=en&q=site:lugbe.ch&ie=L 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](#)

Wo kommen diese Informationen her ?



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
```




LugBE

Anonymität

GoogleTM HACKING

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.



LugBE

Anonymität

Google HACKING

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 Google's cache of <http://www.lugbe.ch/> as retrieved on 9 Jun 2007 01:16:26 GMT.
Google's cache is the snapshot that we took of the page as we crawled the web.
The page may have changed since that time. Click here for the [current page](#) without highlighting.
This cached page may reference images which are no longer available. Click here for the [cached text](#) only.
To link to or bookmark this page, use the following url: <http://www.google.com/search?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 grundsätzlich jeden 1. Donnerstag im Monat.





LugBE

Anonymität

Google HACKING

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 Google's cache of <http://www.lugbe.ch/> as retrieved on 9 Jun 2007 01:16:26 GMT.
Google's cache is the snapshot that we took of the page as we crawled the web.
The page may have changed since that time. Click here for the [current page](#) without highlighting.
This cached page may reference images which are no longer available. Click here for the [cached text](#) only.
To link to or bookmark this page, use the following url: <http://www.google.com/search?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
```




LugBE

Anonymität

GoogleTM HACKING

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
```




LugBE

Anonymität

Google HACKING

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 standartmässig gebräuchliche Wörter (where, how, Zahlen, einzelne Buchstaben):

Beispiel: Star Wars Episode +I

- Ausschluss 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`



LugBE

• Wie sucht man gezielt mit Google ?

GoogleTM HACKING

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`



LugBE

• 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



LugBE

• Wie sucht man gezielt mit Google ?

Google HACKING

INURL:admin

INURL:orders

FILETYPE:php

osCommerce

om/catalog/admin/orders.php+filety



osCommerce

http://www. .com/catalog/admin/orders.php+filetype:php inurl:admin inurl:orders

This is Google's cache of <http://www. .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-7oI19sFkJ:www. .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

Orders

Customers

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

Order ID:
Status: AllOrders

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



SQL Passwörter

```
<?php
$host="127.0.0.1";
$user="cs3projo";
$password="tTnM76mx5";
$database="cs3projo"

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

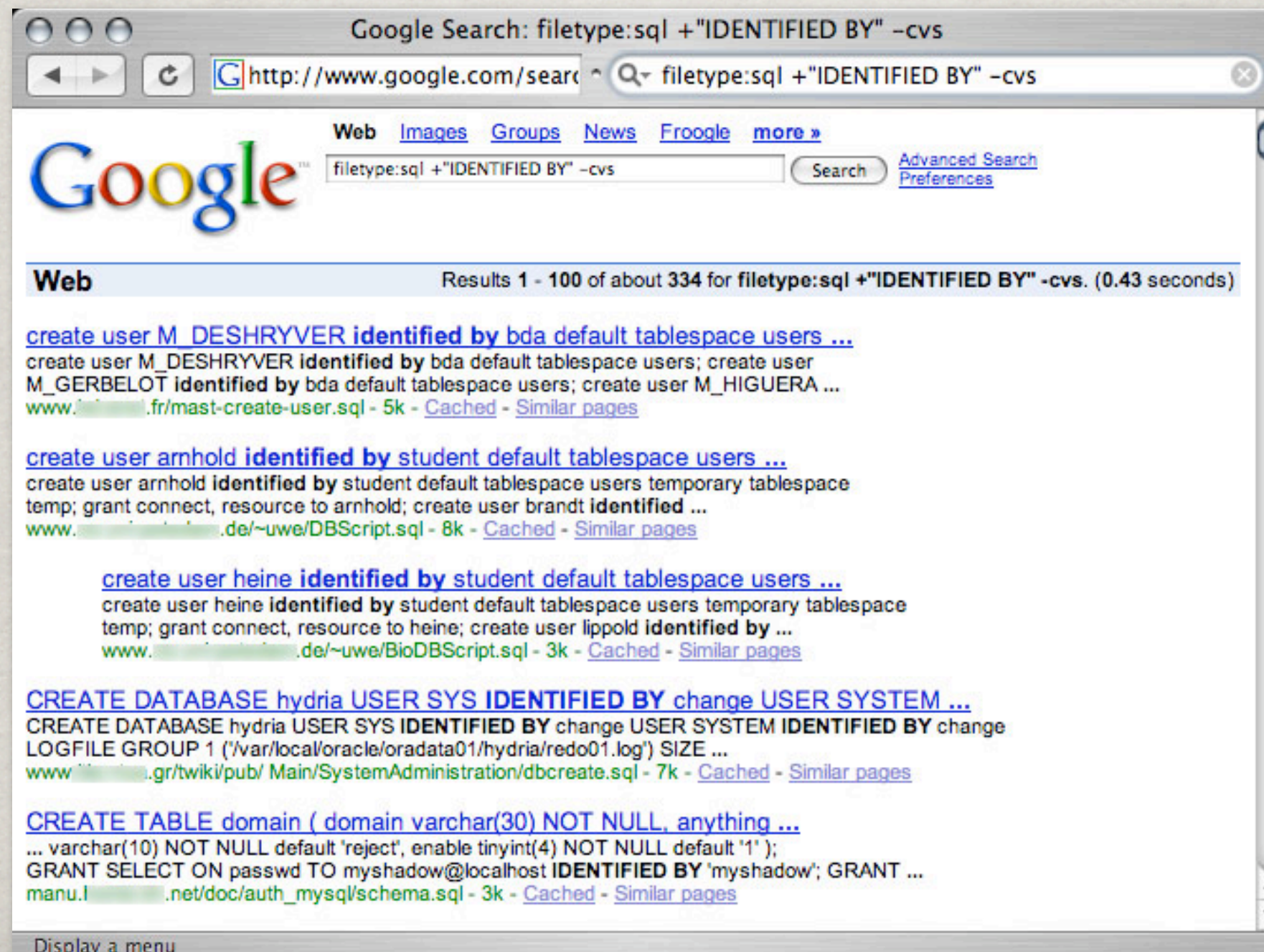
filetype:inc intext:mysql_connect

Include files with
cleartext
passwords...



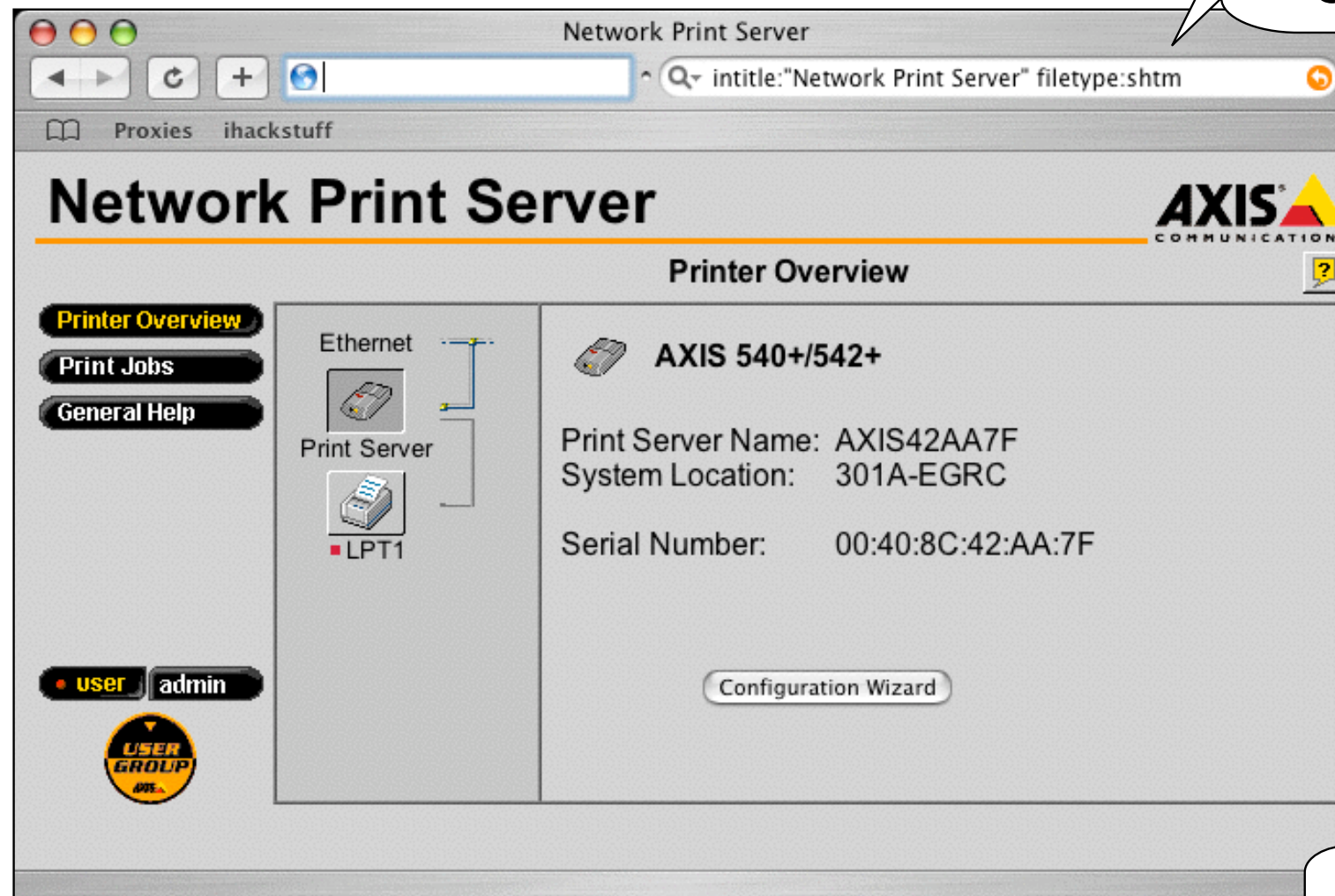
SQL Passwörter

filetype:sql +"IDENTIFIED BY" -cvs





Axis Print Servers

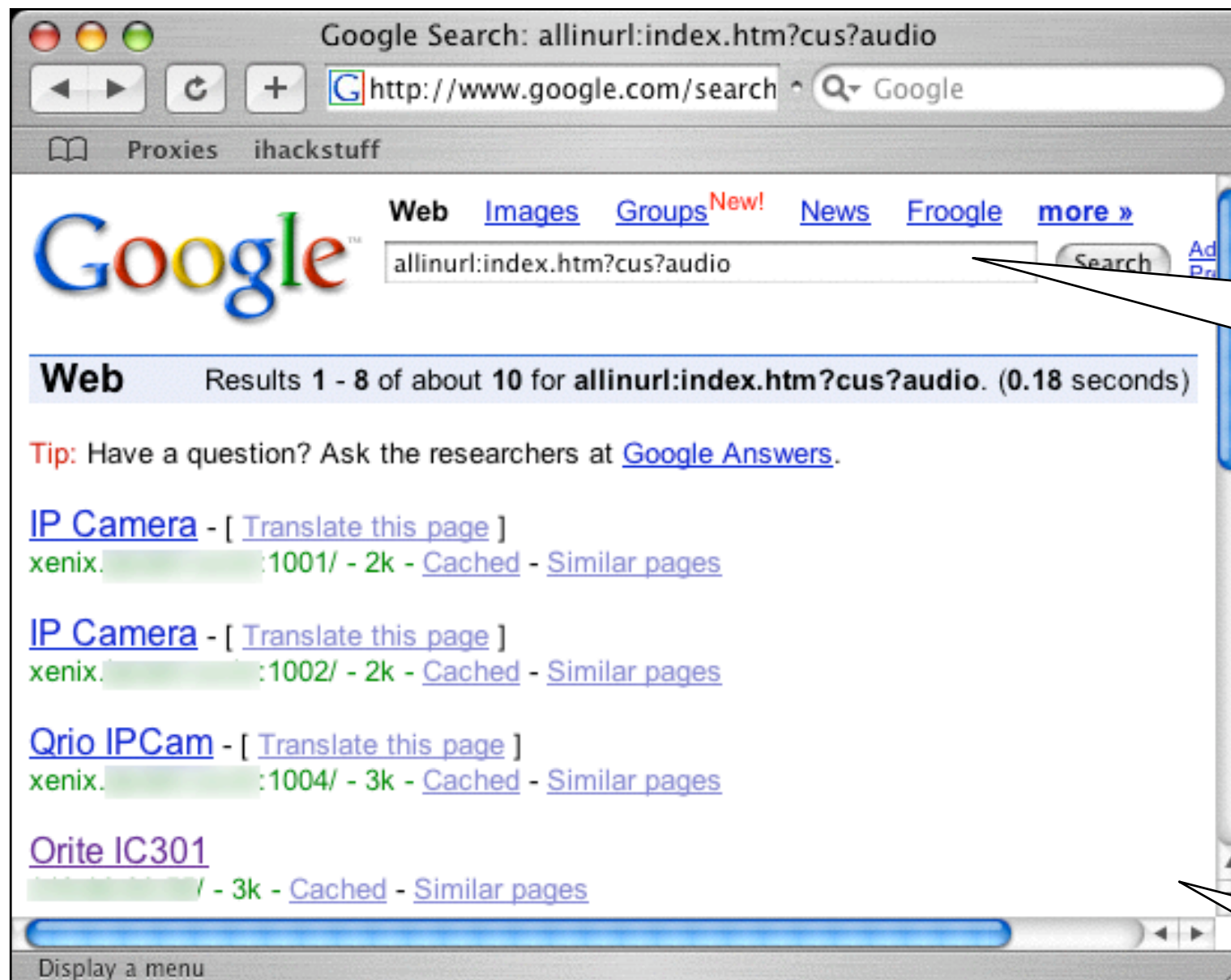


Print server
administration,
Google-style!

Thanks to
murfie for
this one!



Xenix, Sweex, Orite Web Cams



One query,
many
brands of
live cams!

Thanks to
server1 for
this one!

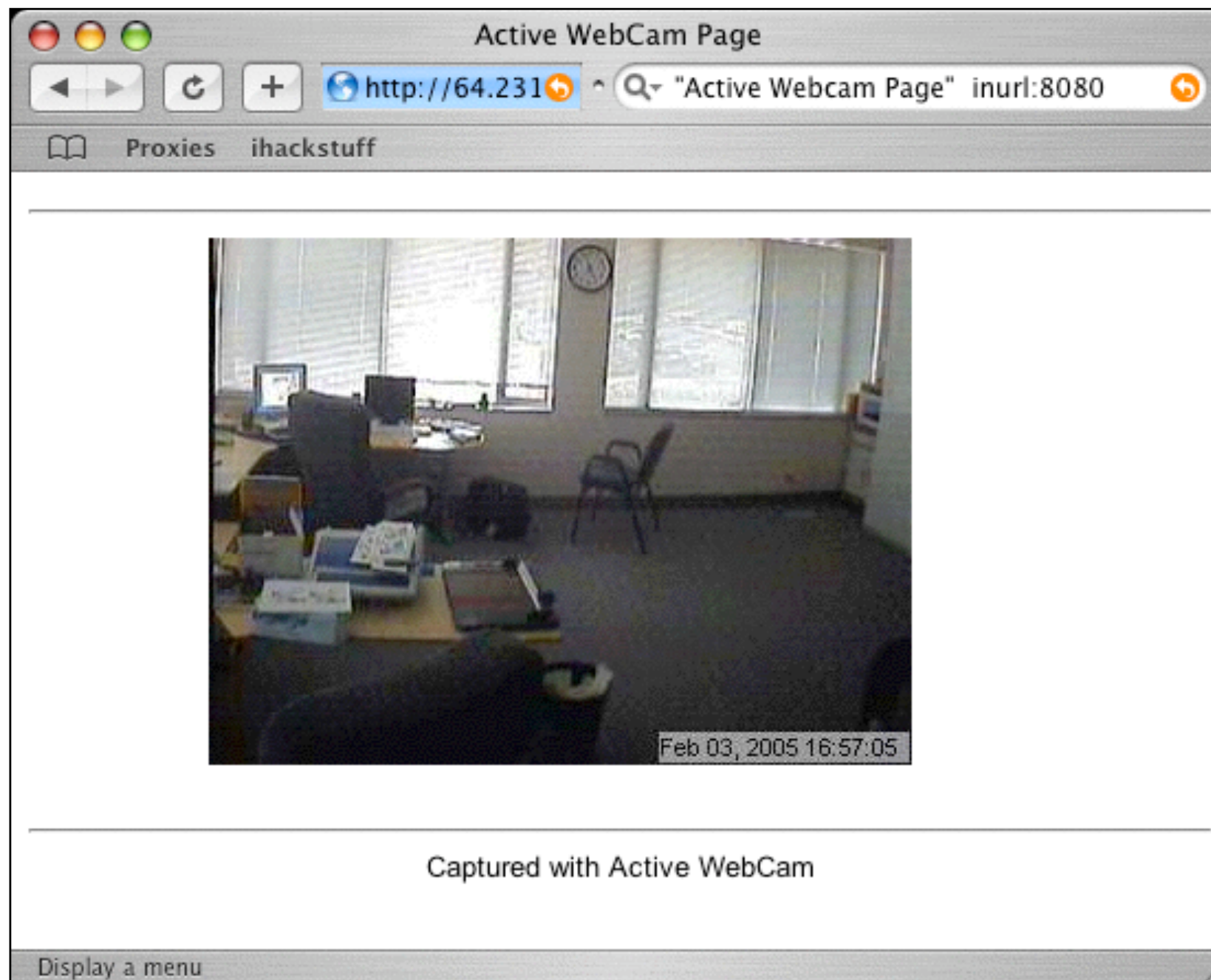


LugBE

Was kann man finden ;-)

Google HACKING

Active WebCam

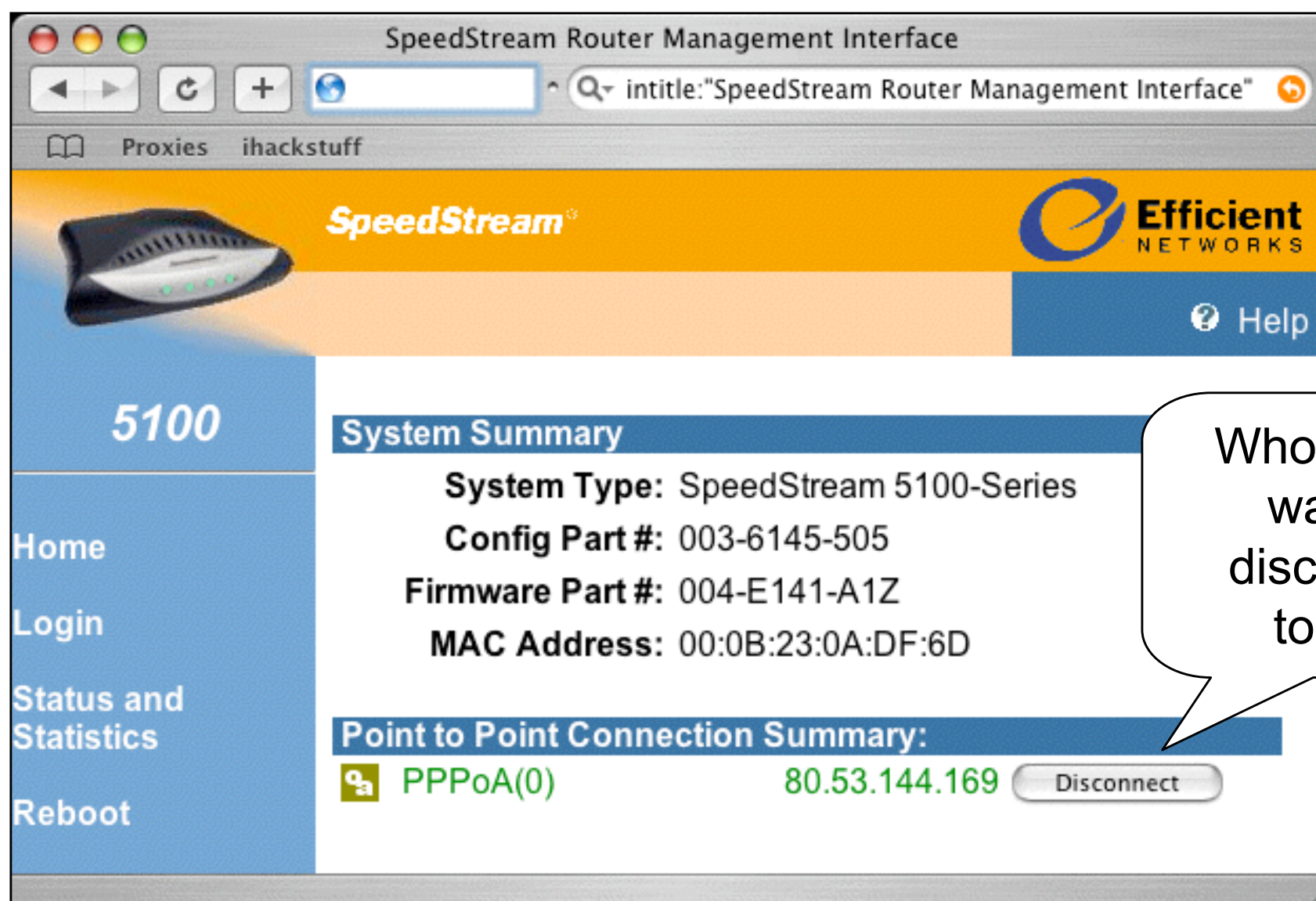


Thanks
klouw!



Speedstream DSL Routers

- Home broadband connectivity... Googled.



Found by
m00d!



LugBE

Was kann man finden ;-)

Google HACKING

Firewalls - Smoothwall

Main page - SmoothWall Express

https://212.226.171.43:441/cgi-bin intitle:"Smoothwall Express" inurl:cgi-bin "up * days"

Proxies ihackstuff

SmoothWall Express 2.0

connection status »

control about your smoothie services networking vpn logs tools maintenance

home | credits

shutdown | help

Welcome to **SmoothWall Express 2.0**
This is your gateway to configuring and administering your SmoothWall firewall. Please make sure you read the Administration Guide before reconfiguring your SmoothWall — the guide is available with our other documentation from **our website**.

Express Brand New!

Refresh

! Your update file is 13d 6h 50m 43s old. We recommend you update it on the "Updates" page.

1:16am up 41 days, 2:21, 0 users, load average: 0.04, 0.01, 0.00

Produced in association with
express 2.0 p5 ui-3.6.1
SmoothWall™ is a trademark of SmoothWall Limited.

© 2000 - 2003 The SmoothWall Team
Credits - Portions © original authors

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.

PHP-Nuke Powered Site

There are no Administrators Accounts yet, proceed to create the Super User:

Nickname:

HomePage:

Email:

Password:

Do you want to create a normal user with the same data? ☒ Yes ☐ No

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

Thanks to
arrested for
this beauty!

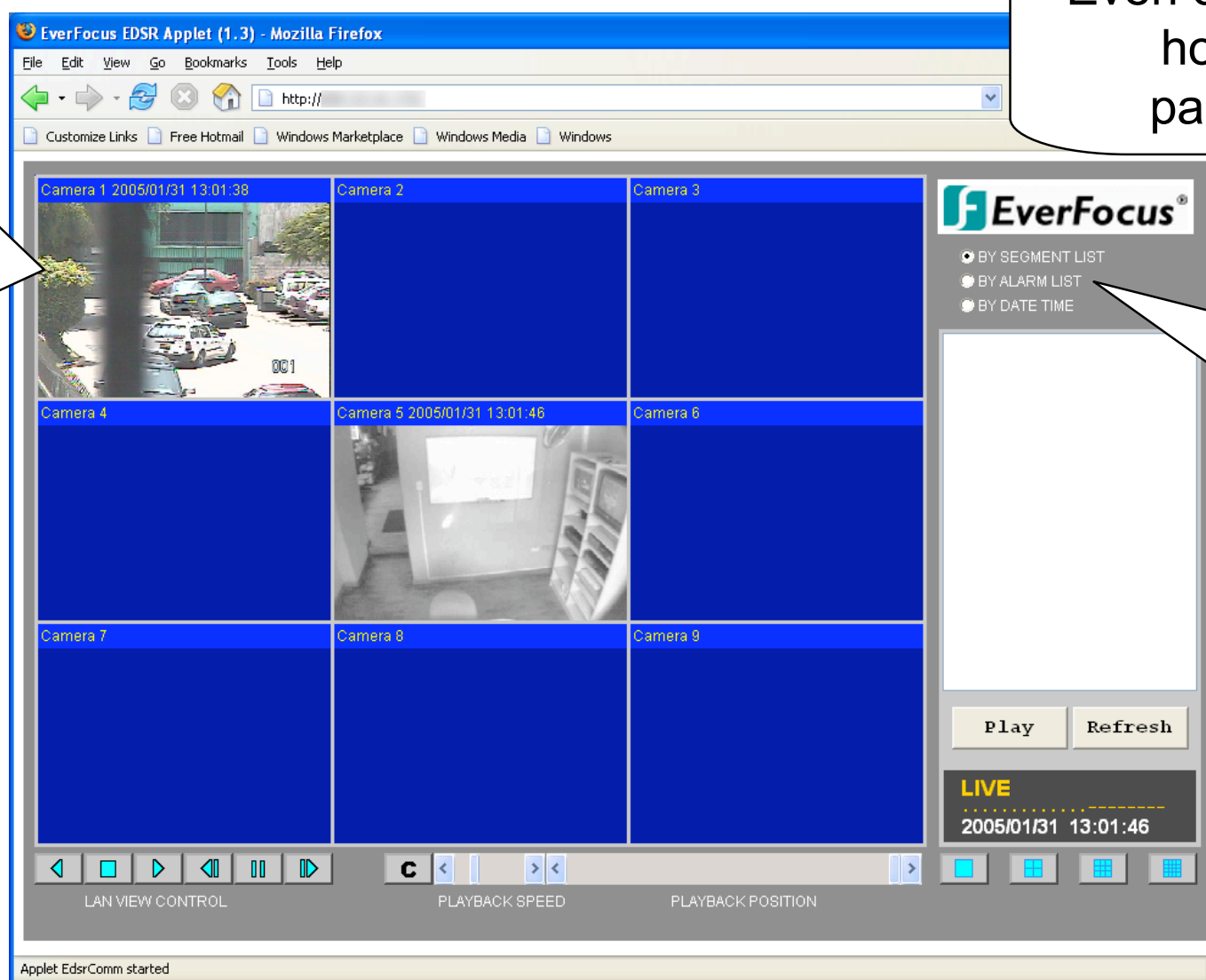


LugBE

Was kann man finden ;-)

Google HACKING

Time lapse video recorders



...multiple
live security
camera
views...

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

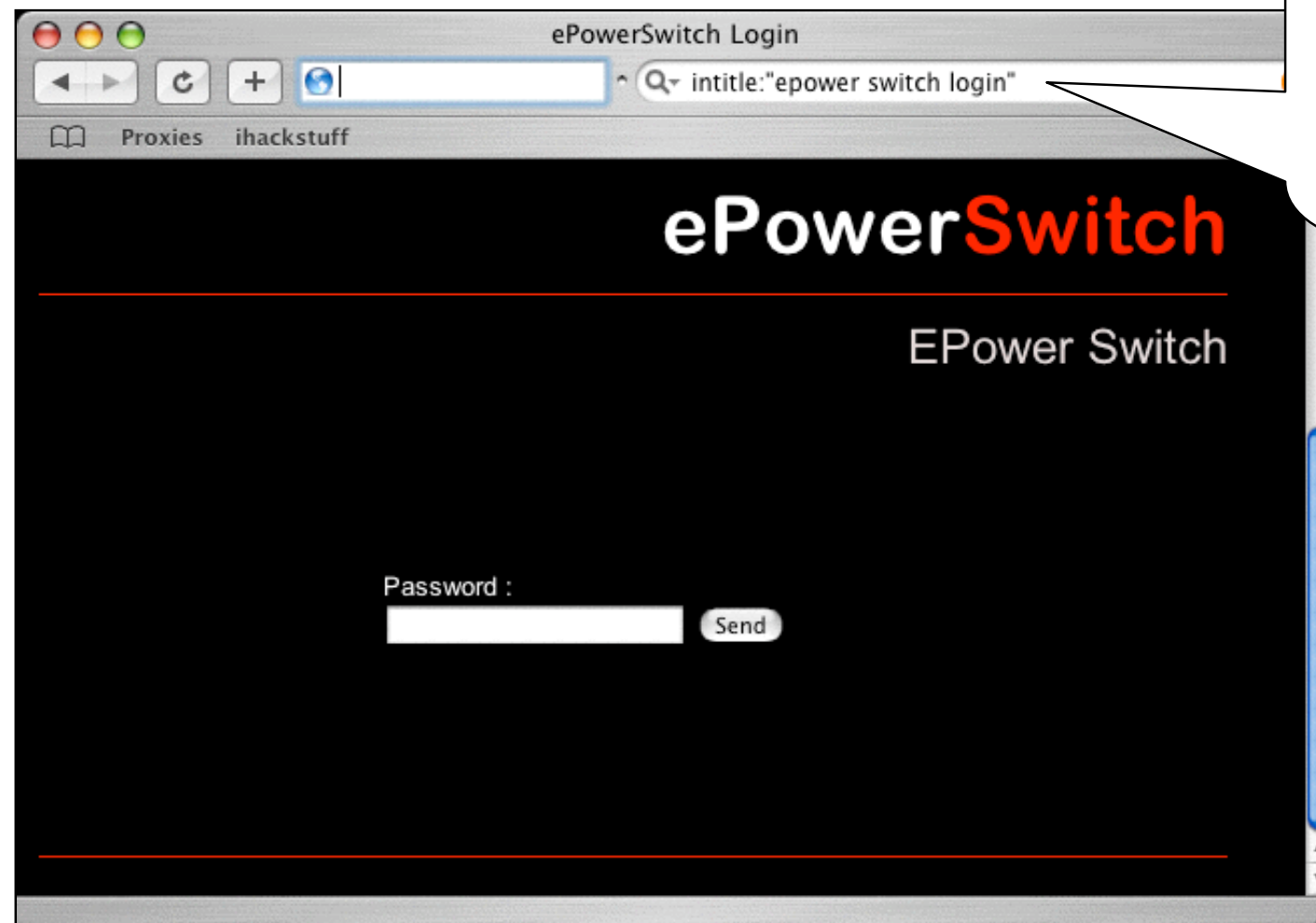
...and historical
records of
recorded video
feeds

Thanks to
stonersavant
for this beauty!



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?

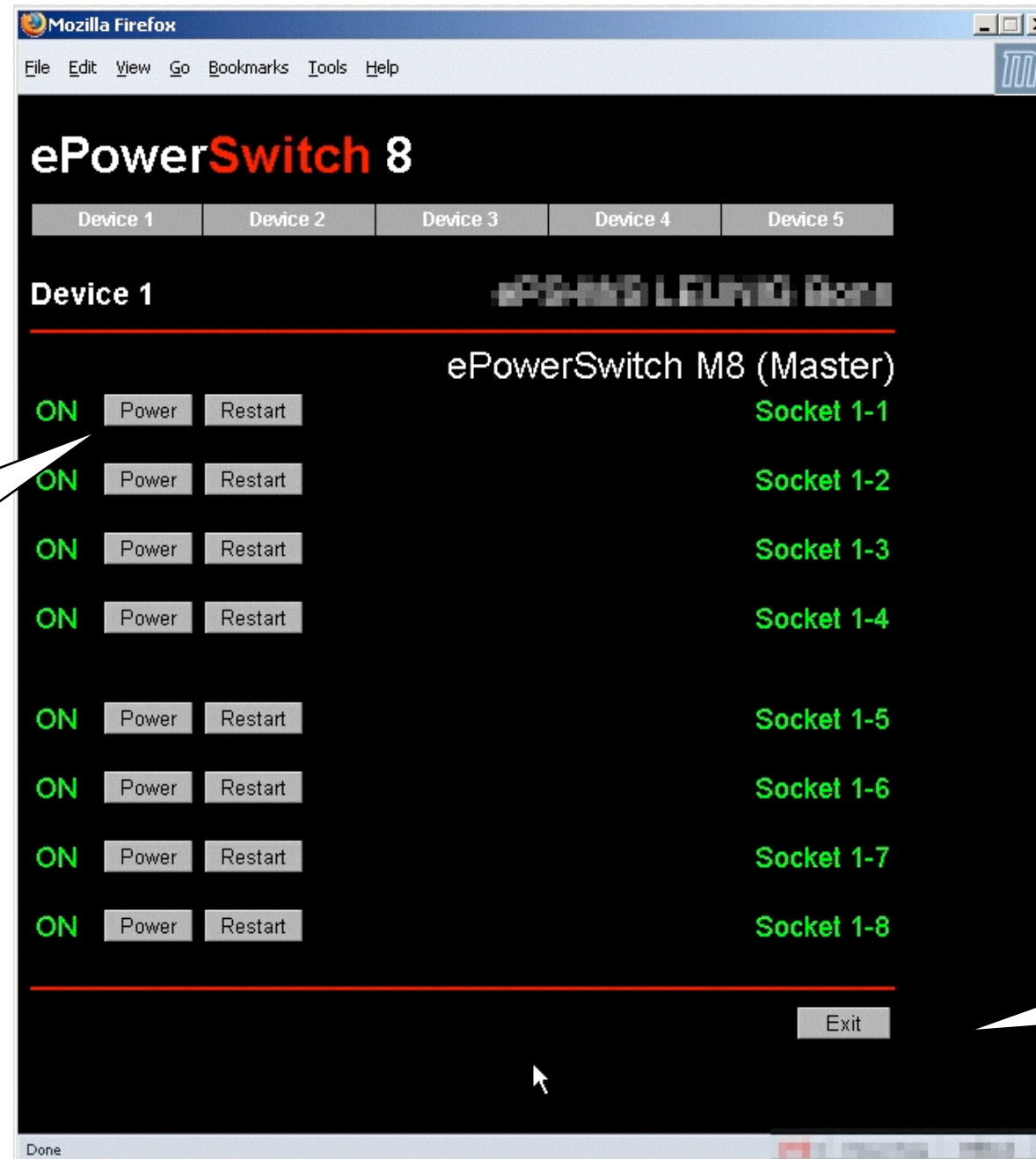


LugBE

Was kann man finden ;-)

Google HACKING

Hacking Power Systems!



Who do you
want to
power off
today?

Thanks to
JimmyNeutro
n for this
beauty!



Norton AntiVirus Corporate Passwords

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

http://www. Google

Proxies ihackstuff

Google 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!



`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.



LugBE

Automatisierung

GoogleTM
HACKING

Automatisierte Domänen Analyse mit lynx & sed/awk



LugBE

Automatisierung

GoogleTM
HACKING

Automatisierte Domänen Analyse mit lynx & sed/awk

Zuerst werden die Daten gesammelt:



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
```




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:



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}'
```




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



LugBE

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$
```




LugBE

Protect yourself!

Google HACKING

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>



LugBE

Links

GoogleTM
HACKING

<http://johnny.ihackstuff.com>

<http://www.sensepost.com/>

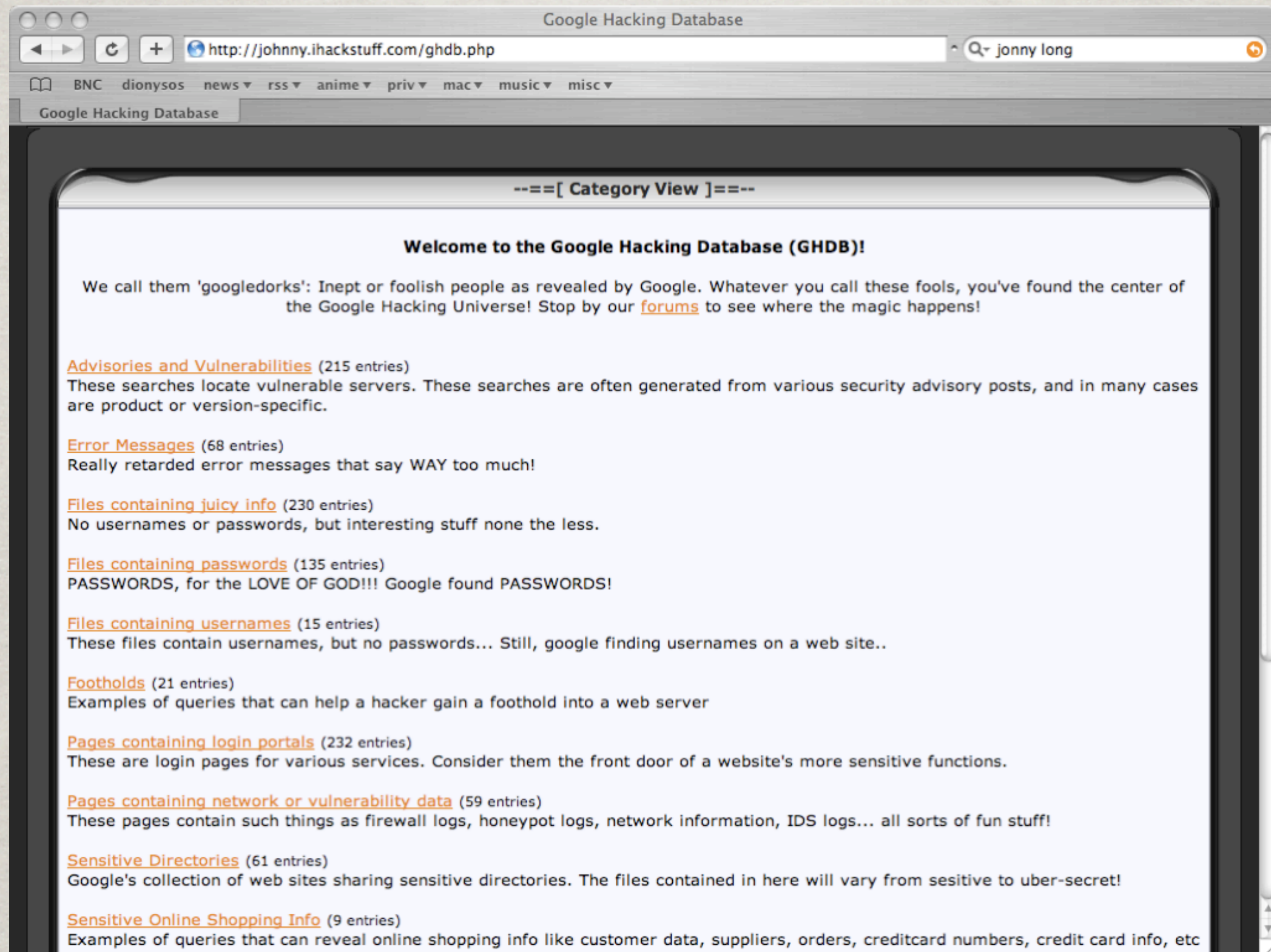
<http://www.gosecure.ca>



LugBE

GHDB

Google HACKING



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