



Google Hacking

Search Engine Black-Ops

Joshua Brashars



Obligatory C.Y.A. Disclaimer:

I am in NO way, shape, or form affiliated with the almighty Google. Google is a registered trademark, owned by people that are almost completely, but not at all like me. Void where prohibited, actual colors may vary, see your dealer for details, batteries not included. So please, Google, don't sue me or pull the plug on me. I can't imagine a life without Google, and trying to makes me cry, just like at the end of Old Yeller. What a great movie.

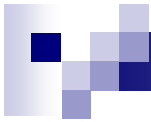


Now that that's out of the way...



Who the heck is this guy?

- Based out of San Diego
- A moderator of <http://johnny.ihackstuff.com/>
- IT Support and Network Security
- A heck of a dancer
- Not as funny as he thinks he is...



Google Hacking?!

- What it is *not*:

- ☐ NOT hacking into Google itself!
- ☐ NOT something that requires “leet skillz”
- ☐ NOT limited to security!
- ☐ NOT related to the O'Reilly Book about SEO



Ok, so what *is* it then?

Simply put, mining data the Google search engine has already indexed.

- YES! It is easy...
- YES! Anyone can do it...
- YES! It can be very dangerous...
- YES! It is a great book written by Johnny Long...
- YES! That was a shameless plug...



Advanced Operators

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



Advanced Operators

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

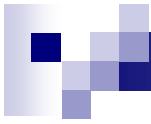
Operator:search_term

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



Advanced Operators at a glance

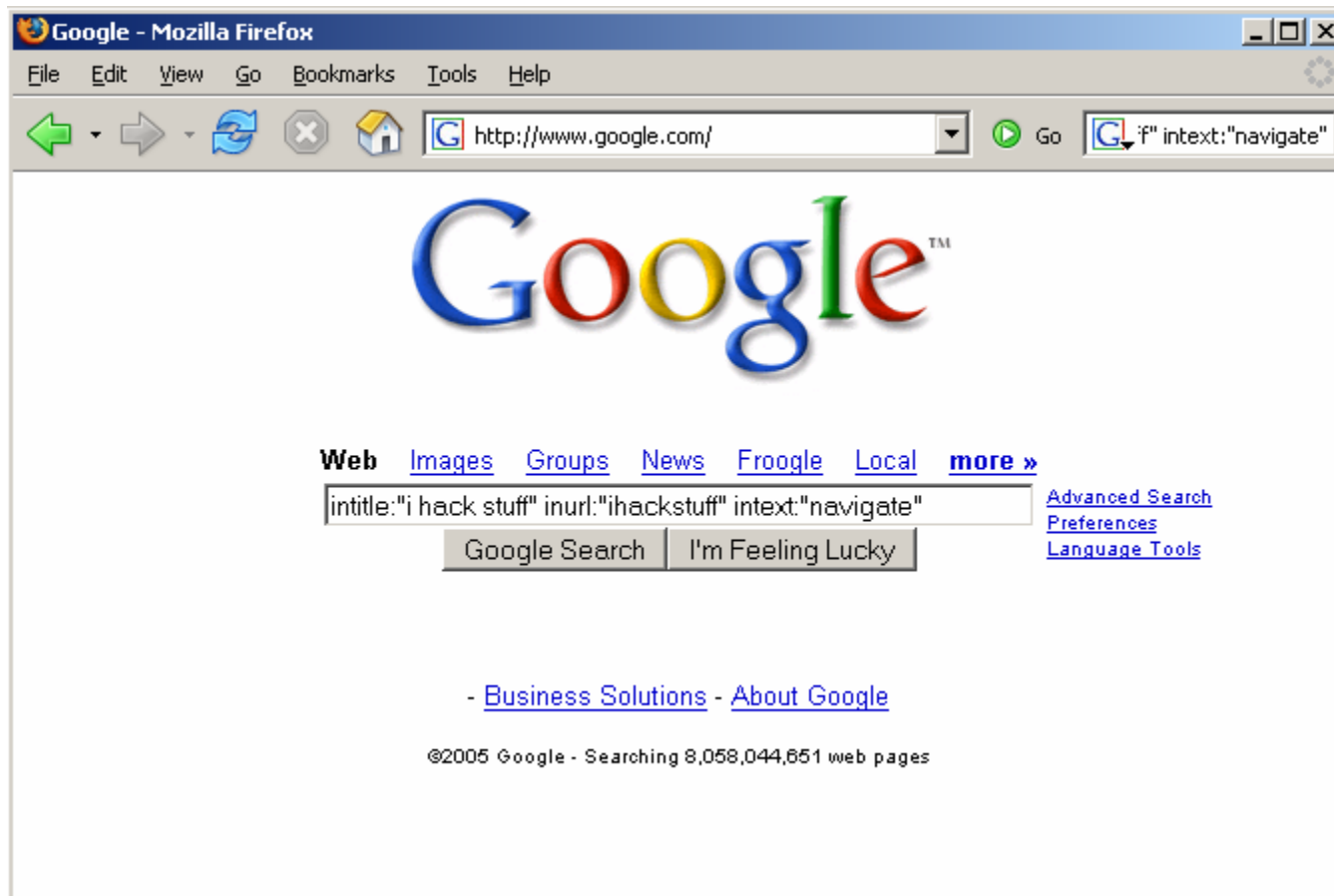
- intitle: - Search page title
- inurl: - Search URL
- site: - limit results to a specific site
- link: - other sites that link to our subject
- inanchor: - search within hyperlinks
- filetype: - Starting to see a pattern yet?



A note on numrange...

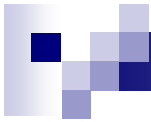
- Received a lot of press in the past
- Used for credit card and social security number searches.
- Sorry, that type of stuff is beyond the scope of this talk.

A crash course in Advanced Googling



Advanced Google Searching





Google Hacking Basics

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



Google Hacking Basics

...can have *devastating* results!



Administration Support Site | Online Catalog | Administration

Configuration

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

Orders

Order ID:

Status:

Customers	Order Total	Date Purchased	Status	Action
mike moon	\$37.35	10/06/2004 02:26:44	Pending	
Keith Berman	\$25.35	08/23/2004 04:25:18	Pending	
mike moon	\$17.60	04/27/2004 08:03:23	Pending	

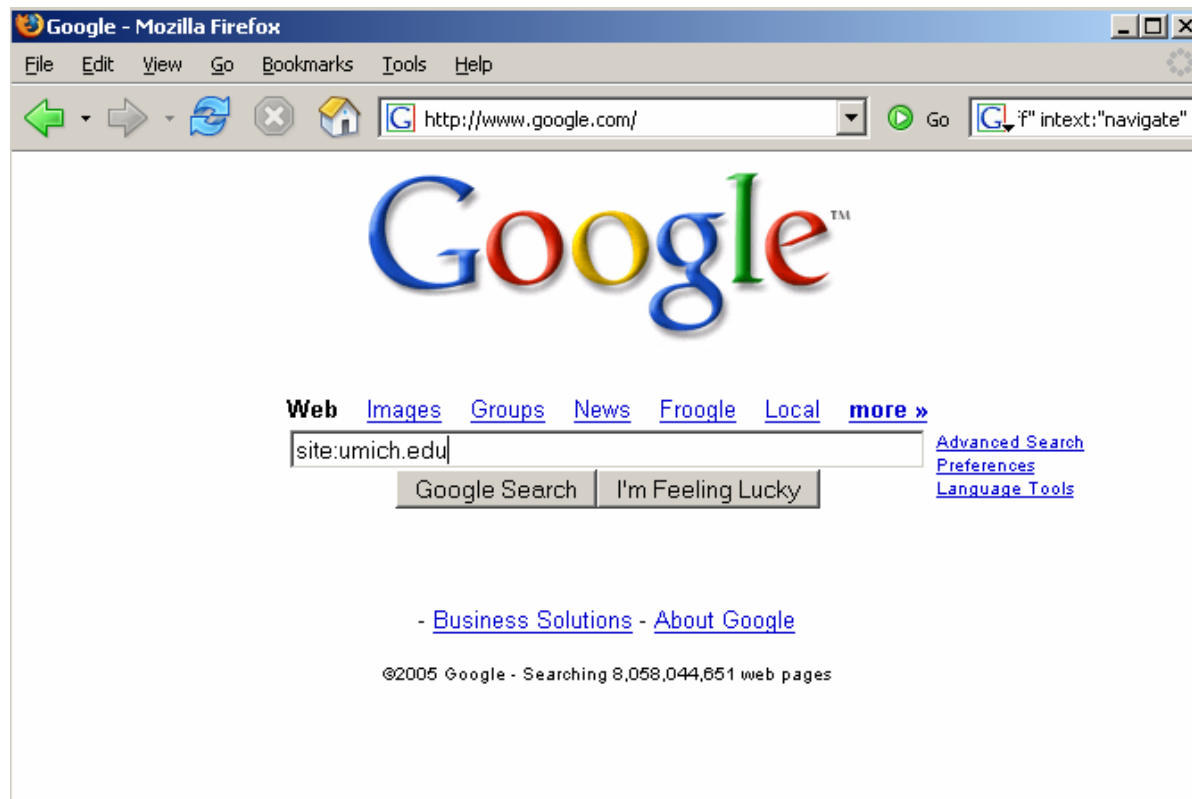
Displaying 1 to 3 (of 3 orders)

Page 1 of 1 Date Created: 10/06/2004

Payment Method: Credit Card

Basic Domain Crawling

- The site: operator narrows a search to a particular site, domain, or sub domain.
- Consider, site:umich.edu...



site:umich.edu - Google Search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.google.com/search?q=site%3Aumich.edu&sourceid=mozilla-search&start=0&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-US:official Go site:umich.edu

Google Web Images Groups News Froogle Local more »

site:umich.edu Search Advanced Search Preferences

Web Results 1 - 10 of about 8,100,000 from umich.edu for . (0.66 seconds)

[How to Apply](#)
UM Chemical Biology. How to Apply. IT IS RECOMMENDED THAT APPLICANTS APPLY ONLINE.
This will ensure the fastest response to your application. ...
www.chembio.umich.edu/apply/ - 9k - [Cached](#) - [Similar pages](#)

[UM SOE: Administration](#)
Quick Links. Dean's Office · Student Travel Reimbursement · Educational and Soc.
Justice Committee · Prospective Students · Who we are ...
www.soe.umich.edu/administration/ - 14k - [Cached](#) - [Similar pages](#)

[UM Office of the Provost: Arthur F. Thurnau Professorship](#)
Arthur F. Thurnau Professorship. General Information. The Thurnau Professorships
are named after Arthur F. Thurnau, a student at the University of Michigan ...
www.provost.umich.edu/programs/thurnau/ - 14k - [Cached](#) - [Similar pages](#)

[The University Record](#)
The University of Michigan · News Services · The University Record Online. search.
front · accolades · briefs · view events · submit events · UM employment ...
www.umich.edu/~urecord/events_submission.shtml - 18k - [Cached](#) - [Similar pages](#)

[Welcome UM Comprehensive Cancer Center](#)
Institutional information about this Ann Arbor, Michigan facility, including
access to the Patient Education Resource Center.
www.cancer.med.umich.edu/ - 12k - Jul 31, 2005 - [Cached](#) - [Similar pages](#)

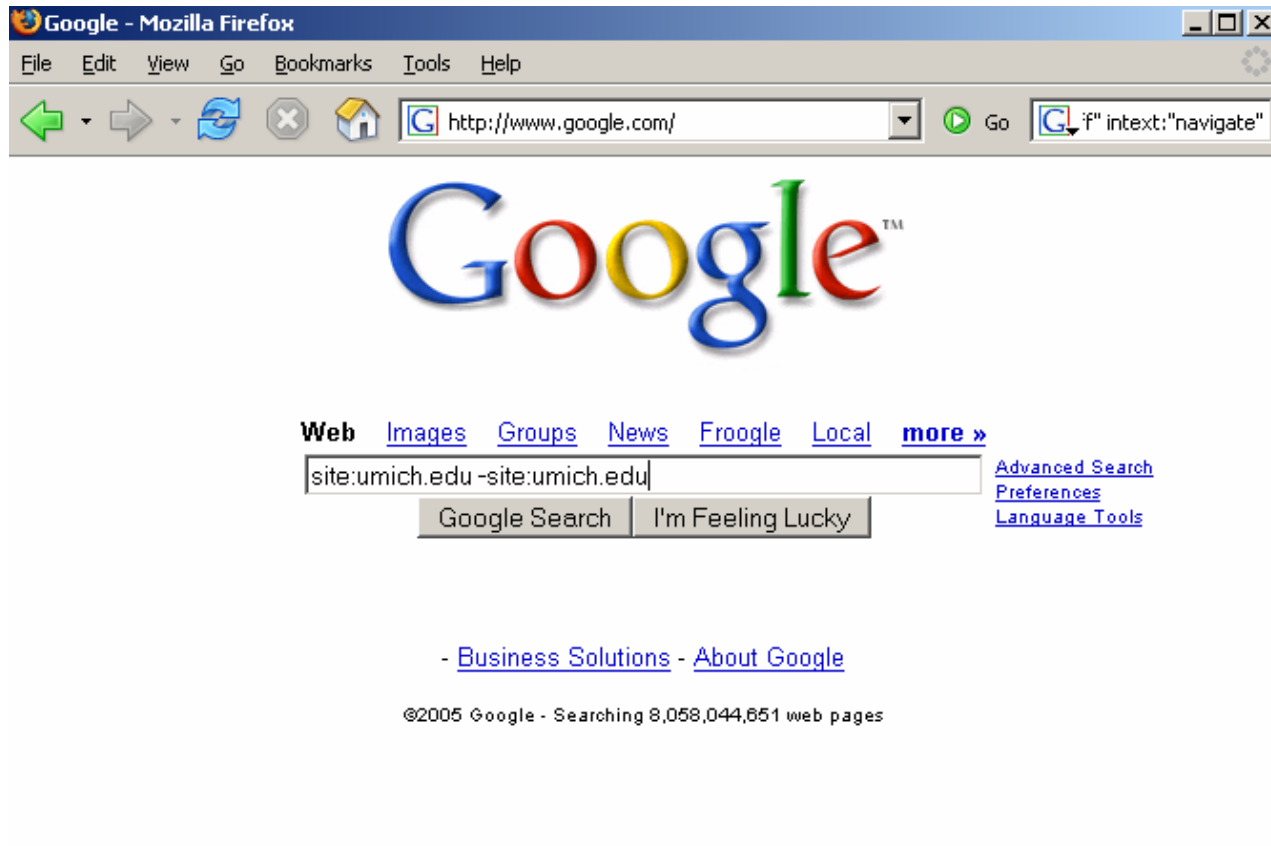


Basic Domain Crawling

- Most obvious stuff floats to the top
- As a security tester (or an attacker) we need to get to the less obvious stuff
- www.umich.edu is *way* too obvious.

Basic Domain Filter

- To get rid of the most obvious junk, do a negative search!
 - `site:umich.edu -site:www.umich.edu`





[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [Local](#) [more »](#)

site:umich.edu -site:www.umich.edu

Search

[Advanced Search](#)
[Preferences](#)

[Get the Google Toolbar](#)

Web

Results **1 - 10** of about **5,340,000** from **umich.edu** for **-site:www.umich.edu**. (0.31 seconds)

[UM-SSW: Information Request](#)

Admissions and Financial Aid Links About the Area. About the Area. Admissions.

MSW Program · Doctoral Program · Non-degree Enrollment. Fees & Expenses ...

www.ssw.umich.edu/admissions-doctoral/infoform.html - 20k - [Cached](#) - [Similar pages](#)

[UM School of Music - Prospective Students](#)

Welcome to the University of Michigan School of Music! We look forward to working

with you during your time at the UM. You probably have many questions that ...

www.music.umich.edu/prospective_students/admitted.htm - 54k - Jul 31, 2005 - [Cached](#) - [Similar pages](#)

[JOBS at the University of Michigan](#)

University of Michigan Archived Posting (For Information Only. Do NOT Apply.)

Printable Version (opens new window). Posting No: T-045873-DW ...

websvcs.itcs.umich.edu/jobnet/job_posting.php?postingnumber=045873 - 8k - [Cached](#) - [Similar pages](#)

[UM | Museum of Art \(UMMA\)](#)

search · e-news · become a member · UMMA Logo · Exhibitions · Collections Galleries ·

Coming Soon · Past Exhibitions · For Students ...

www.umma.umich.edu/view/past.html - 10k - [Cached](#) - [Similar pages](#)

[How to Apply](#)

UM Chemical Biology. How to Apply. IT IS RECOMMENDED THAT APPLICANTS APPLY ONLINE.

This will ensure the fastest response to your application. ...

www.chembio.umich.edu/apply/ - 9k - [Cached](#) - [Similar pages](#)



Basic Domain Filter

- This has several benefits:
 - Low profile. The target can't see the activity.
 - Results are “ranked” by Google. This means that the most public stuff floats to the top. Some more interesting stuff trolls to the bottom.
 - Leads for follow up recon. You aren't just getting hosts and domain names, you get application data just by looking at the results snippet. One page of results can contain *tons* of info, such as e-mail addresses, names, etc...
 - We can explore non-obvious relationships. This is HUGE!



You're ranting, Josh...

- There are downsides, though.
 - In many cases it would 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 through Google*.

Google Translation as a proxy

- Use Google to do your work
- English to English translation
 - Still get the content, still readable, not your IP!
 - <http://www.google.com/translate?u=http%3A%2F%2Fwww.umich.edu&langpair=en%7Cen&hl=en&ie=UTF8>





Google translation as a proxy

■ The Caveat – Images

- Not truly anonymous
- Images requested from the site will still be processed with our IP address
- Still, it's a creative use of Google
- Always test your proxies!
 - www.whatismyip.com



Server Identification

- Intitle:"index.of" "server at"
- There are two ways this is useful
 - If an attacker knows what version a server is, he may be able to locate an exploit for it
 - If an attacker has an exploit for a certain type of server, Google can ferret out some vulnerable hosts

Server Identification

Index of /staffhp/tupac - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://72.14.207.104/search?q=cache:YadhFUTrRrAJ:www.uprod. Index of "server at"

Index of /staffhp/tupac

Name	Last modified	Size	Description
Parent Directory	16-Mar-2005 17:10	-	
UserSelections.txt	15-Mar-2005 15:24	1k	
images/	15-Mar-2005 15:30	-	
index.htm	15-Mar-2005 15:23	8k	
index 2.htm	15-Mar-2005 15:23	8k	
index 3.htm	15-Mar-2005 15:24	8k	
index 4.htm	15-Mar-2005 15:24	8k	
index 5.htm	15-Mar-2005 15:24	2k	
kmtupac.jpg	07-May-1999 17:52	109k	
pages/	15-Mar-2005 15:23	-	
psp0214.JPG	11-Mar-2005 14:06	2.9M	
thumbnails/	15-Mar-2005 15:30	-	

Apache/1.3.33 **Server** at www.uprod.music.umich.edu Port 16080

Done



More server identification queries

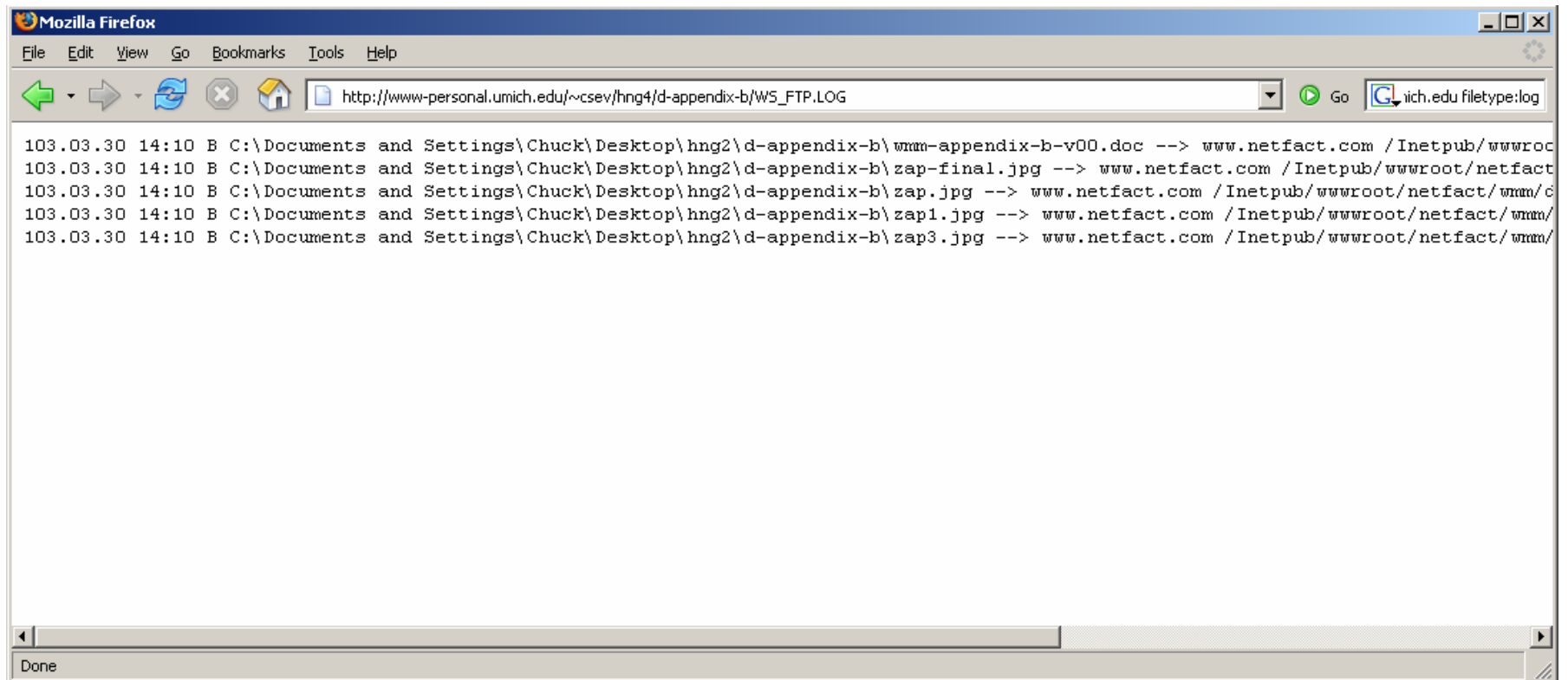
- “Apache/” “server at” intitle:”index.of”
- “Microsoft-IIS/* server at” intitle:”index.of”
- “Oracle HTTP Server Powered by Apache”
intitle:”index.of”
- “Red Hat Secure/3.0 server at”
intitle:”index.of”
- “Apache Tomcat/” intitle:”index.of”
- “AnWeb/1.42h” intitle:”index.of”



Finding specific files


- The filetype: operator allows us to find specific types of files.
- Consider log files, such as ws_ftp.log
 - Log files often contain juicy info such as IP addresses, directory structures, and more...
 - Site:umich.edu filetype:log

site:umich.edu filetype:log



Directory Transversal

■ This...



Deploying BIRT - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.eclipse.org/birt/index.php?page=deploy/viewer-php.html

eclipse BIRT

Eclipse home
BIRT home
integration
viewer setup
viewer usage
using PHP
design engine API
report engine API

Integrating BIRT

Integrating BIRT with PHP

Contents

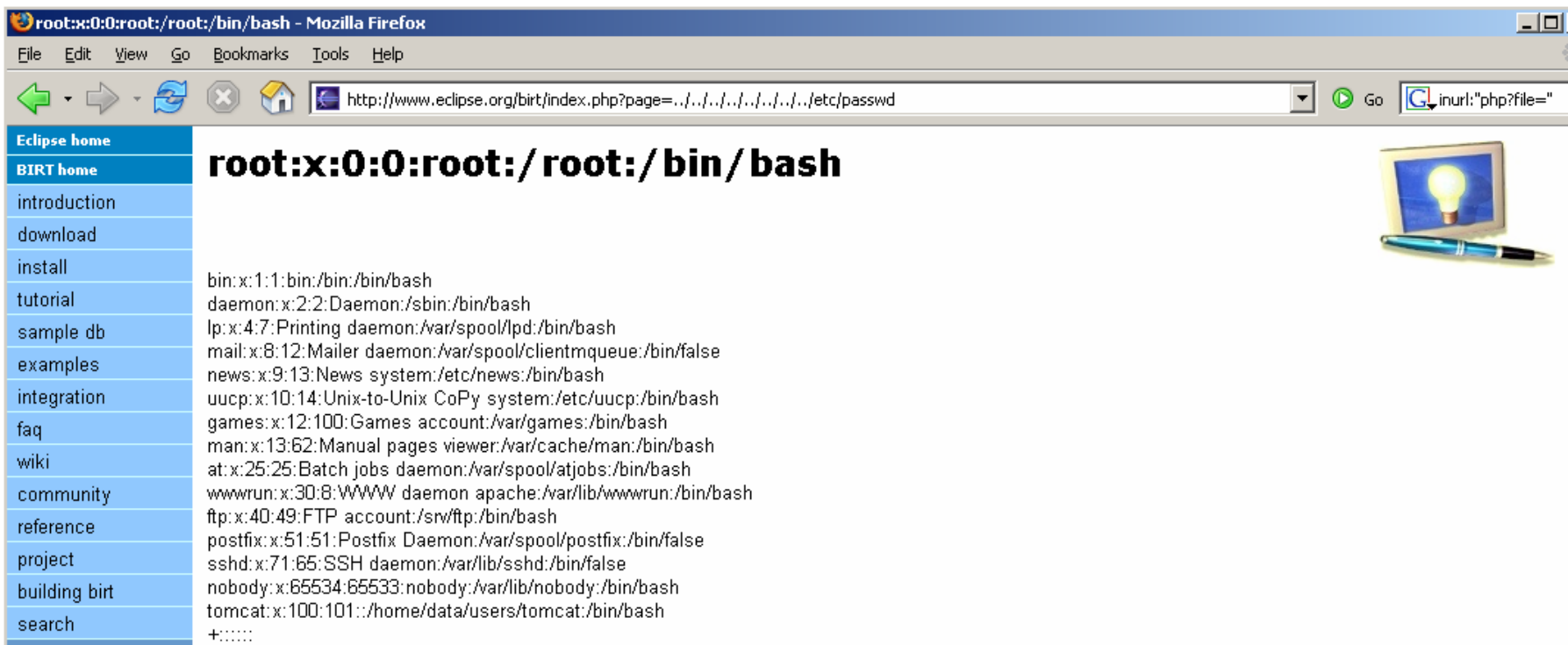
- Motivation
- Setup
- Running a Report
- Passing Parameters
- Parameter Form
- Generating Reports Dynamically

Motivation

BIRT is designed to be integrated into a J2EE web application. But, what if your chosen development environment is something else, such as PHP? Can you still use BIRT? Yes, you can. This page discusses how to use BIRT from PHP, but the techniques apply to any server-side scripting environment.

Directory Transversal

■ ...becomes this!



root:x:0:0:root:/root:/bin/bash - Mozilla Firefox


File Edit View Go Bookmarks Tools Help

http://www.eclipse.org/birt/index.php?page=../../../../../../../../etc/passwd

Eclipse home
BIRT home
introduction
download
install
tutorial
sample db
examples
integration
faq
wiki
community
reference
project
building birt
search

root:x:0:0:root:/root:/bin/bash

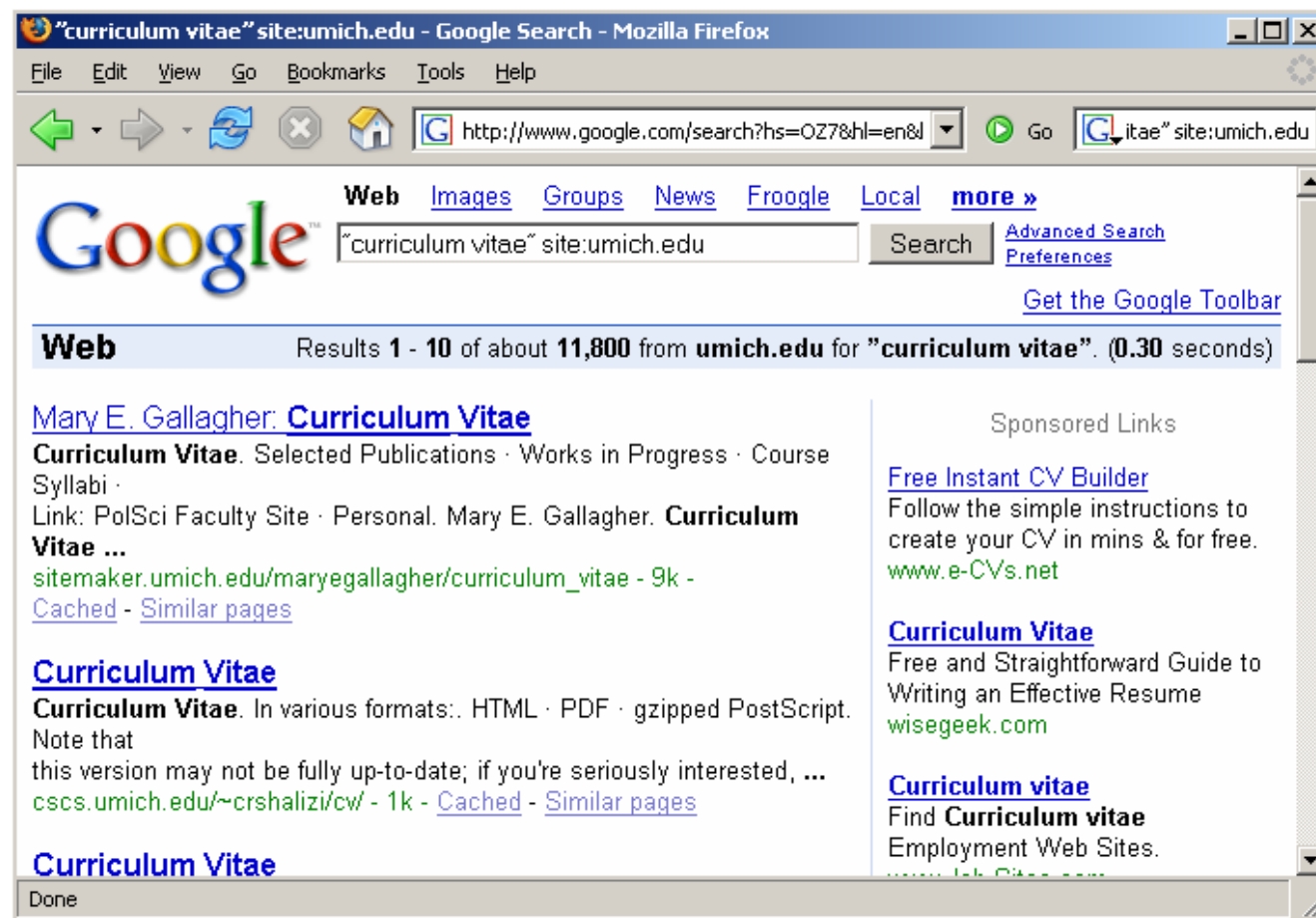
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
sshd:x:71:65:SSH daemon:/var/lib/ssh:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
tomcat:x:100:101:/home/data/users/tomcat:/bin/bash
+.....



Social Engineering

Resumes can be valuable!

- "curriculum vitae" site:umich.edu



robots.txt

- Robots.txt can provide a roadmap for unknown, and potentially sensitive, directories and files.
- Robots.txt should not be spidered by the web server... but is that always the case?



Web

Results **1 - 5** of **5** from **umich.edu** for **inurl:robots.txt**. (0.19 seconds)



- User-agent: *
- Disallow: /htbin/
- Disallow: /shtbin/
- Disallow: /stats/dynamic/
- Disallow: /stats/static/
- Disallow: /search/
- Disallow: /caen/EITC2004/
- Disallow: /ipe/studyabroad/funding/scholarships/
- Disallow: /caen/news/Volume_18/
- Disallow: /caen/news/Volume_19/
- Disallow: /caen/news/Volume_20/
- Disallow: /admin/dean/
- Disallow: /caen/systems/
- Disallow: /caen/staff/
- Disallow: /lost/
- Disallow: /class/eecs381/
- Disallow: /class/eecs493/



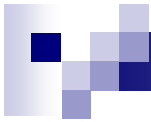
Zero-Packet Port Scanning

Why get your hands dirty when someone else will do it for you?



Whatchoo talkin' bout, Willis?

- Ok, before you throw things at me, allow me to clear up a few things about the phrase “zero packet” in this context:
 - Passive techniques are truly zero-packet. That's not what I'm talking about.
 - I'm talking about zero packets directly from source to target. Think proxy. It's about staying out of the targets logs.
 - Um... plus this is a talk about Google Hacking, sheesh!
 - Oh, come on, it's silly but it's still fun!



Zero-packet verification

- So, *it takes a few packets* from us to the target to verify and fingerprint hosts.
- Now, DNS resolution is no big deal, but *port scanning* is. This flags IDS systems.
- Is there an interesting way to do traditional recon without sending any packets directly from us to the target?

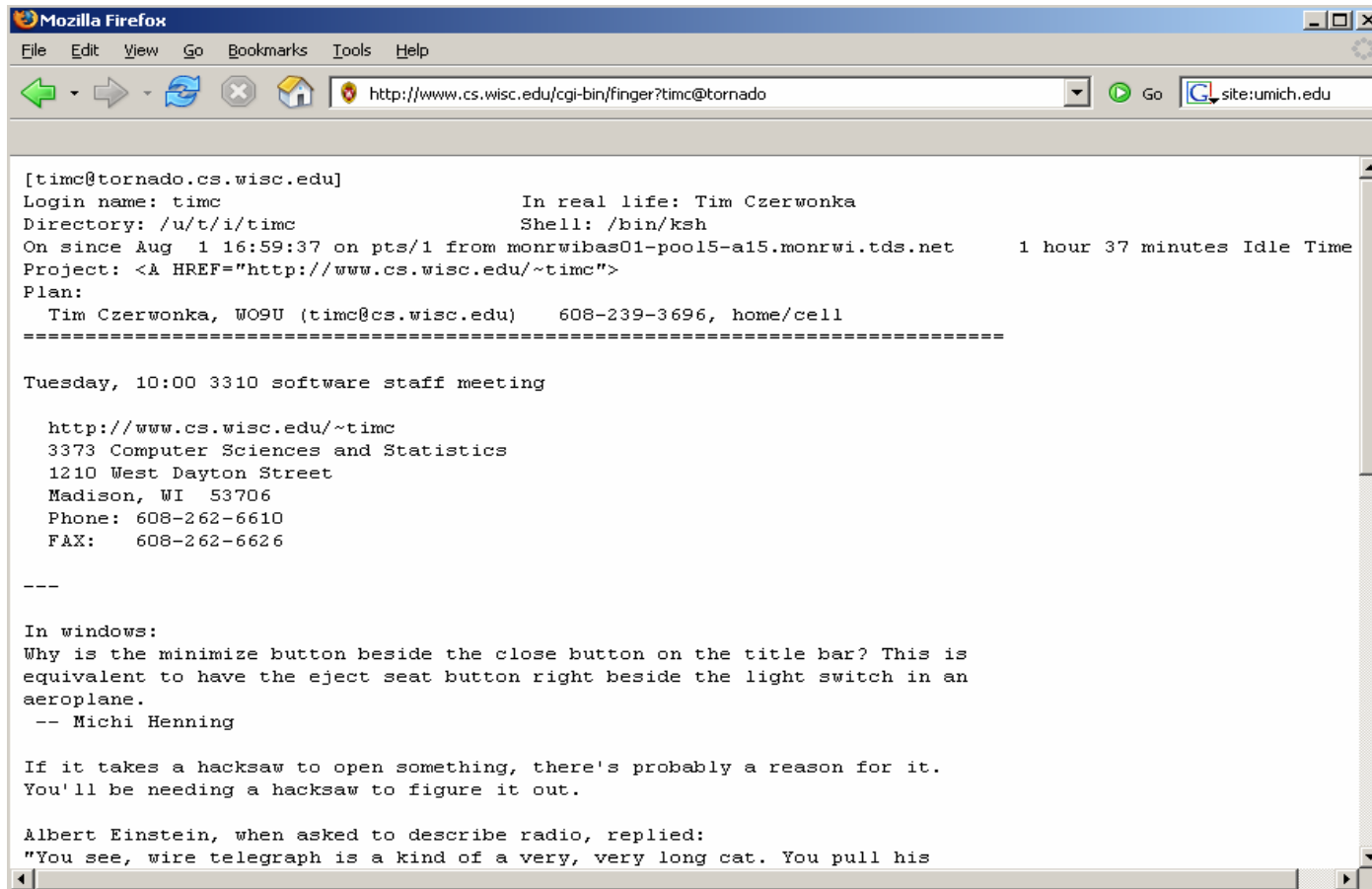


Everyone, say it with me...

(yes, even you in the front. Say it with me...)

Old School! Finger...

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



The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://www.cs.wisc.edu/cgi-bin/finger?timc@tornado`. The main content area displays the output of a finger command for the user `timc` on the `tornado.cs.wisc.edu` host. The output includes login details, real name (Tim Czerwonka), directory, shell, and a plan section. The plan section mentions a software staff meeting and provides contact information for Tim Czerwonka. It also includes a humorous anecdote about a hacksaw and a quote from Albert Einstein.

```
[timc@tornado.cs.wisc.edu]
Login name: timc                      In real life: Tim Czerwonka
Directory: /u/t/i/timc                Shell: /bin/ksh
On since Aug  1 16:59:37 on pts/1 from monrwibas01-pool5-a15.monrwi.tds.net  1 hour 37 minutes Idle Time
Project: <A HREF="http://www.cs.wisc.edu/~timc">
Plan:
  Tim Czerwonka, W09U (timc@cs.wisc.edu)  608-239-3696, home/cell
=====

Tuesday, 10:00 3310 software staff meeting

  http://www.cs.wisc.edu/~timc
  3373 Computer Sciences and Statistics
  1210 West Dayton Street
  Madison, WI  53706
  Phone: 608-262-6610
  FAX:   608-262-6626

---

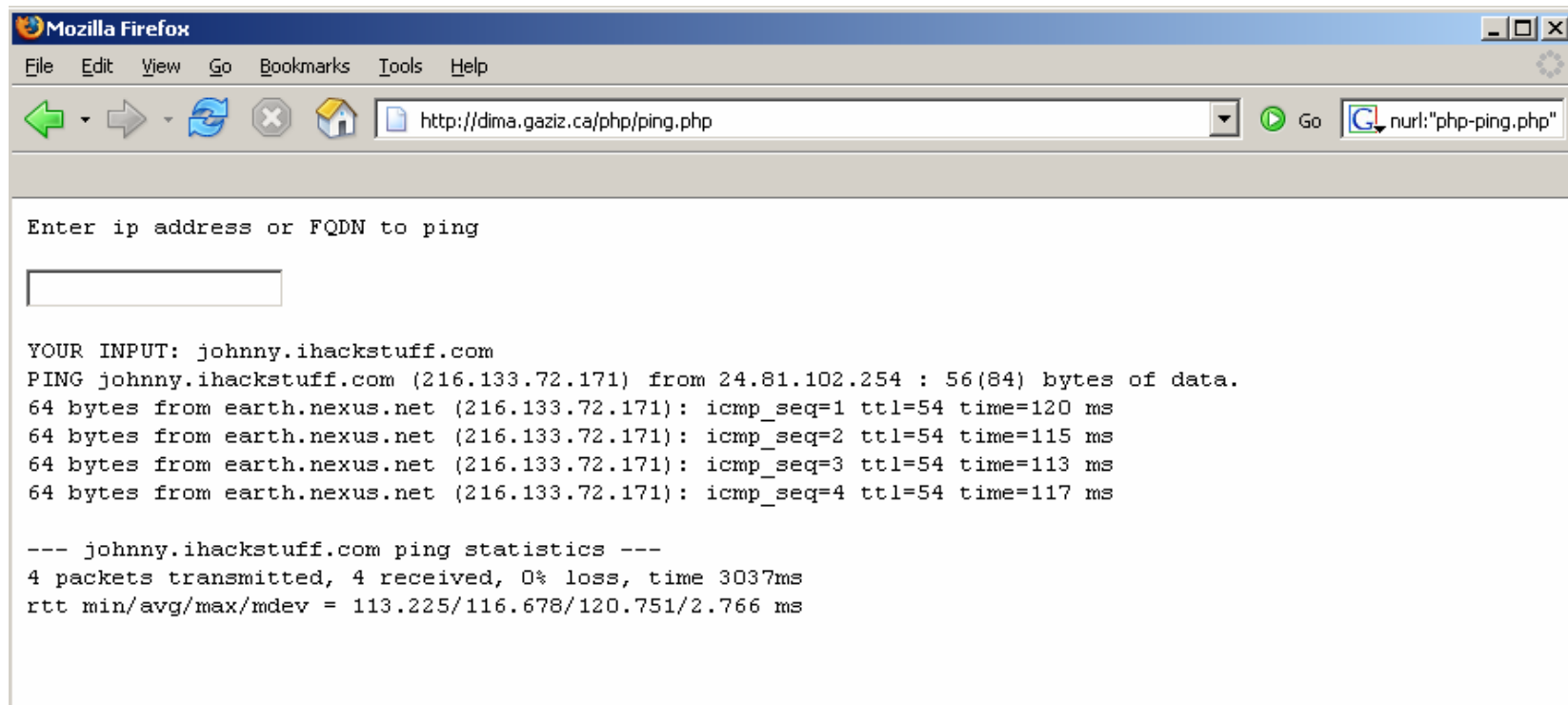
In windows:
Why is the minimize button beside the close button on the title bar? This is
equivalent to have the eject seat button right beside the light switch in an
aeroplane.
-- Michi Henning

If it takes a hacksaw to open something, there's probably a reason for it.
You'll be needing a hacksaw to figure it out.

Albert Einstein, when asked to describe radio, replied:
"You see, wire telegraph is a kind of a very, very long cat. You pull his
```

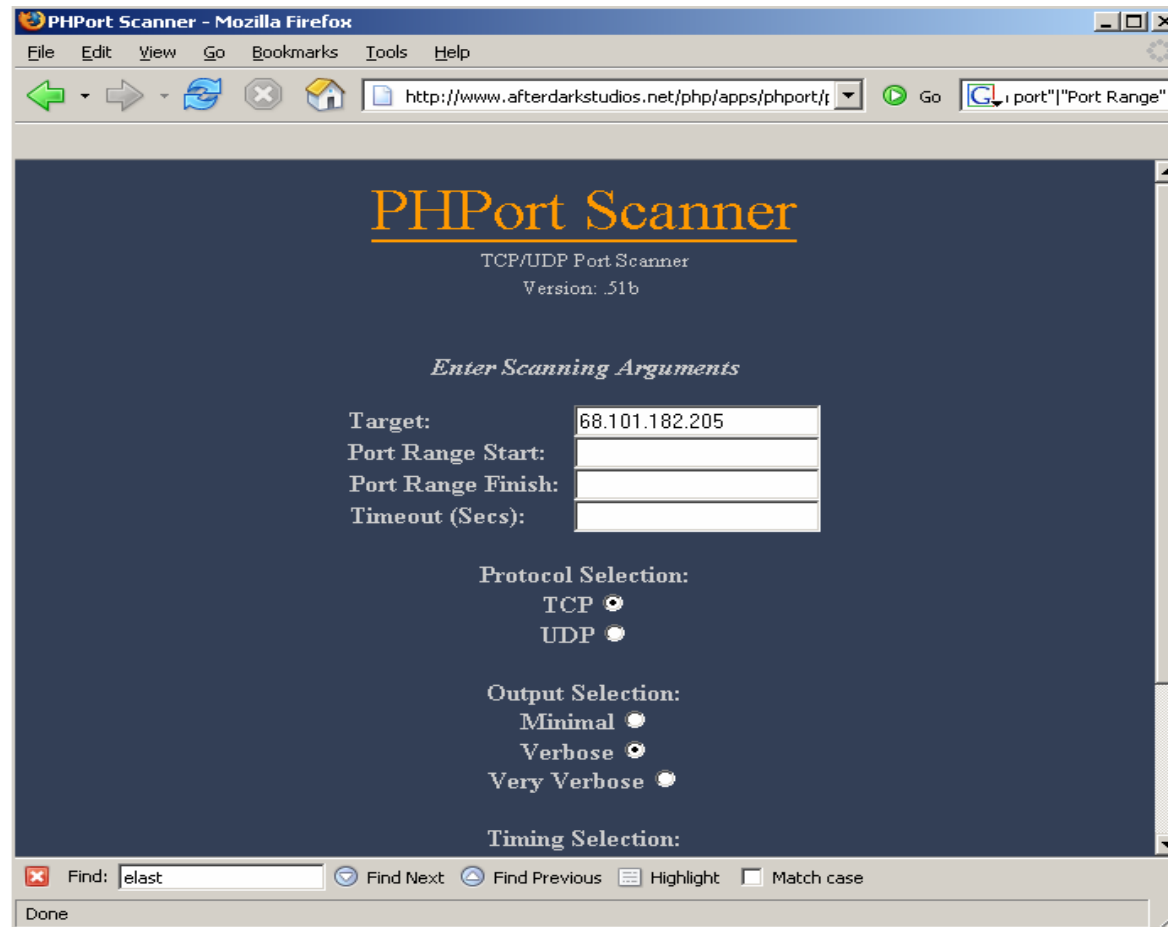
PHP Ping

- "Enter ip" inurl:"php-ping.php"



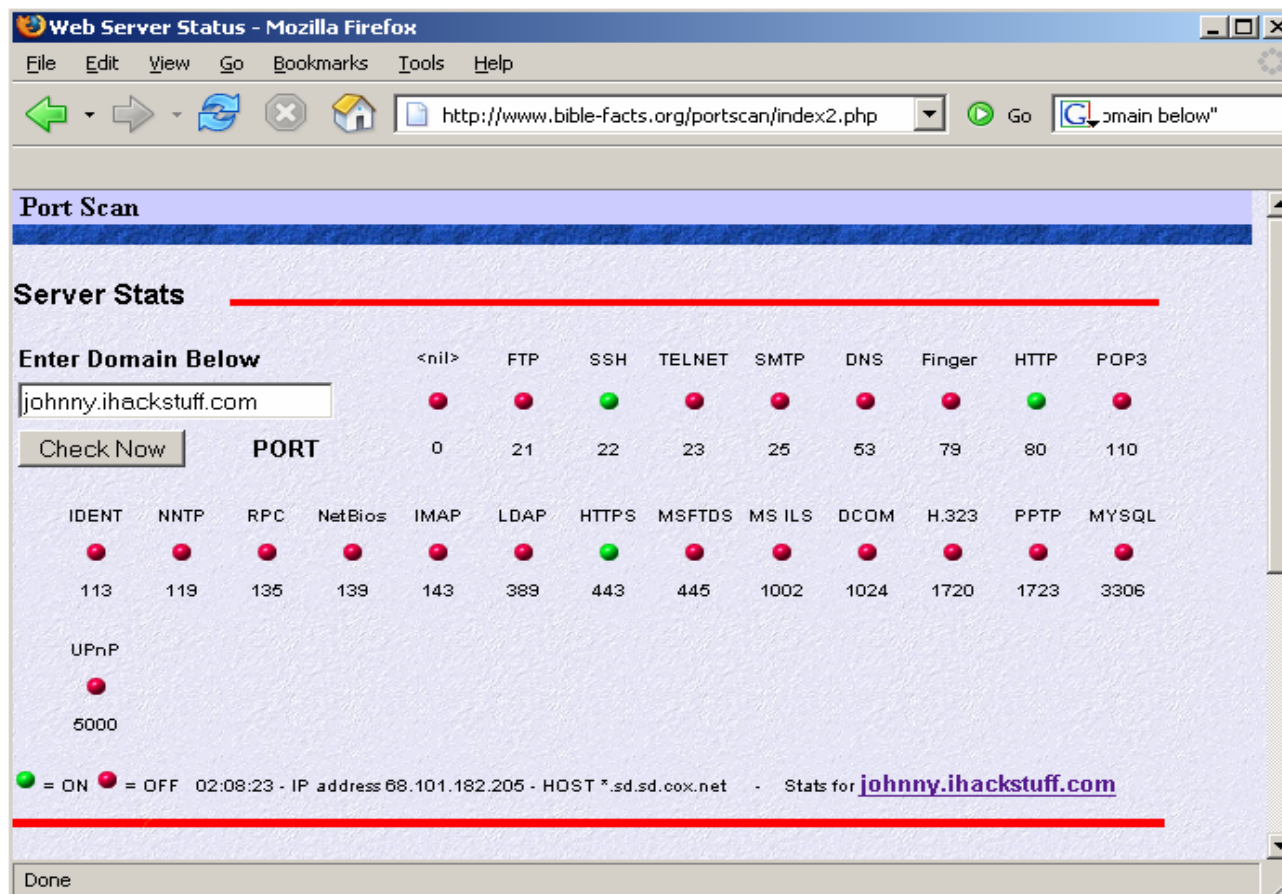
PHP Port Scanner

- inurl:portscan.php "from port"|"Port Range"



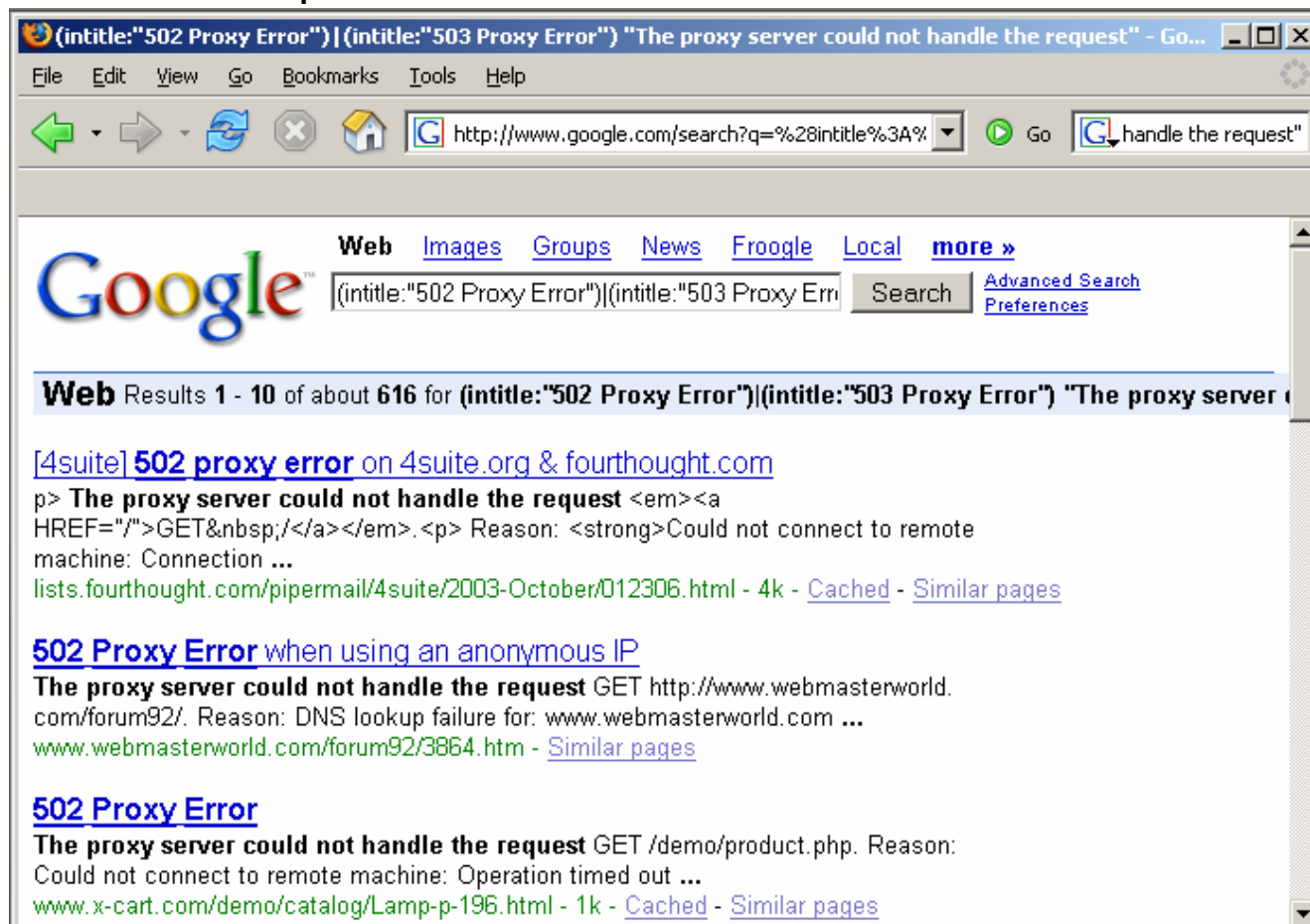
Yet another port scanner

- "server status" "enter domain below"



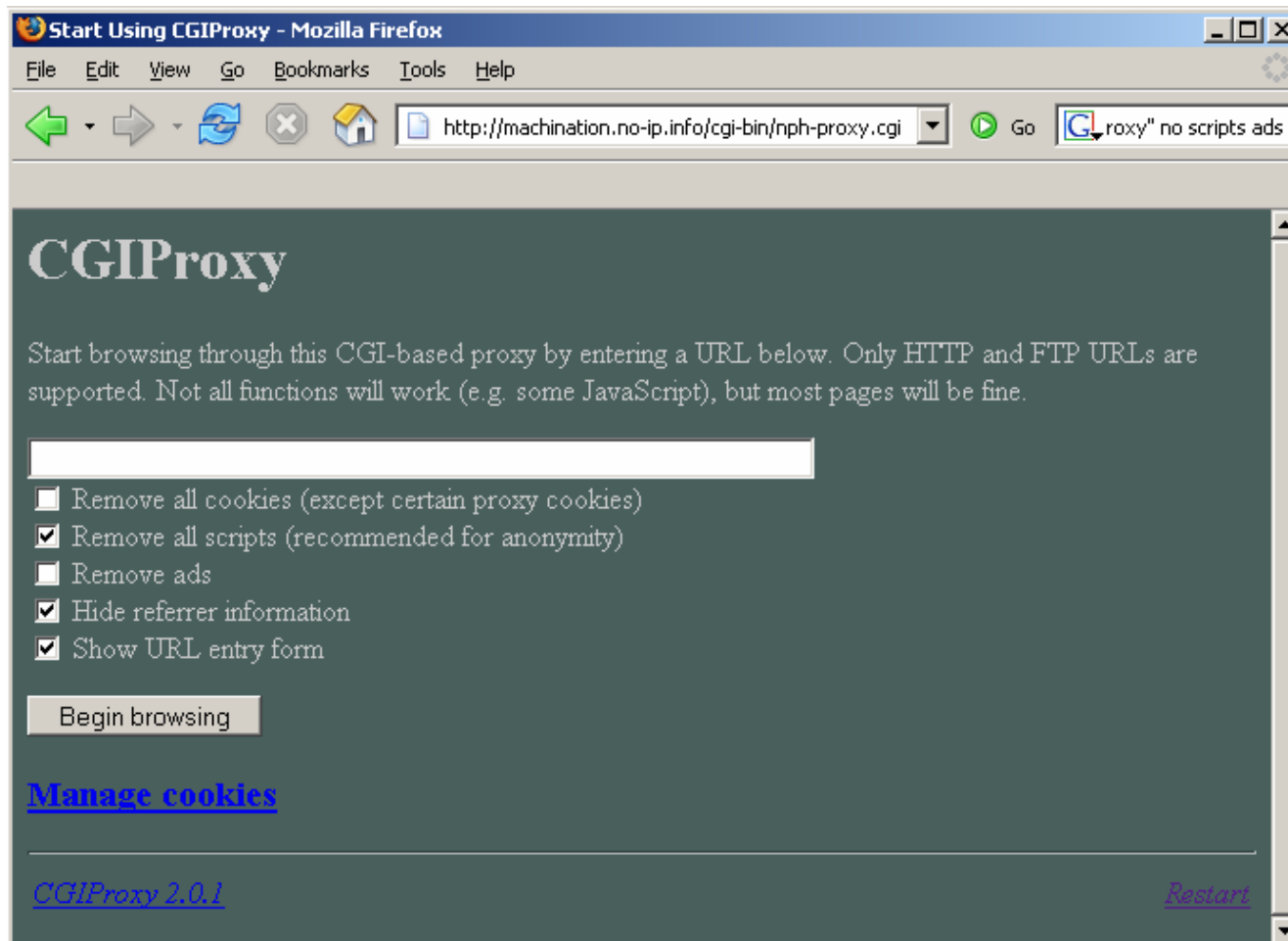
Locating proxy servers

- (intitle:"502 Proxy Error")|(intitle:"503 Proxy Error") "The proxy server could not handle the request"



CGIProxy

- intitle:"start using cgiproxy" no scripts ads



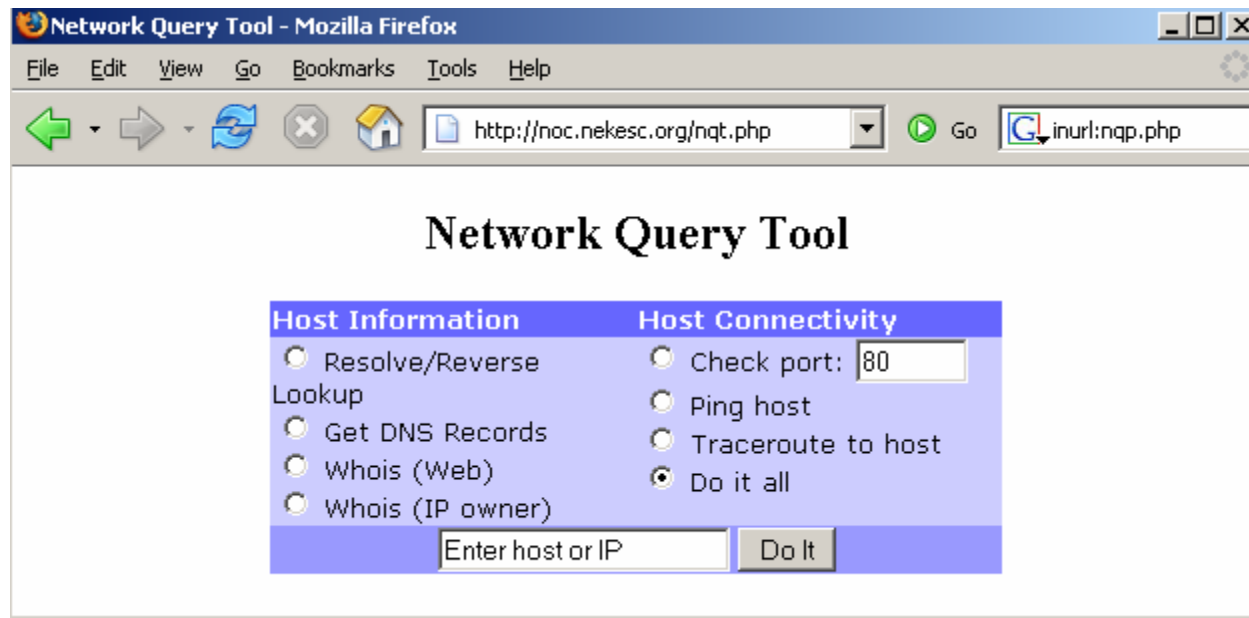
WebUtil

■ inurl:webutil.pl



Network Query Tool

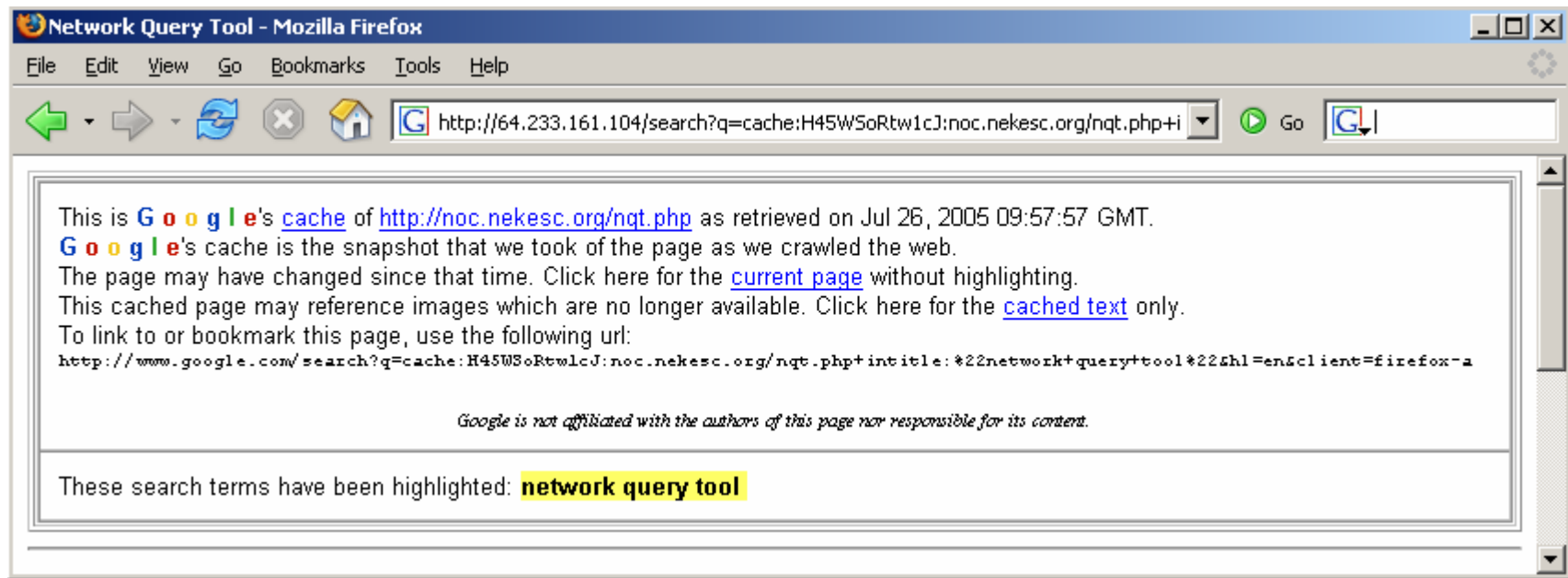
- intitle:"network query tool"



The screenshot shows a Mozilla Firefox browser window titled "Network Query Tool - Mozilla Firefox". The address bar contains the URL "http://noc.nekesc.org/nqt.php". The page content is titled "Network Query Tool" and features two main sections: "Host Information" and "Host Connectivity".

Host Information	Host Connectivity
<input type="radio"/> Resolve/Reverse Lookup	<input type="radio"/> Check port: <input type="text" value="80"/>
<input type="radio"/> Get DNS Records	<input type="radio"/> Ping host
<input type="radio"/> Whois (Web)	<input type="radio"/> Traceroute to host
<input type="radio"/> Whois (IP owner)	<input checked="" type="radio"/> Do it all
<input type="text" value="Enter host or IP"/> <input type="button" value="Do It"/>	

Cache is your friend!





Zero-packet Recon

- The point is, Google can be used as an interesting, low-profile alternative to traditional recon techniques. We've used Google queries for low profile alternatives to
 - DNS resolution
 - Unix service queries
 - Network Recon
 - Web-based proxy services
 - Web crawling via cache



Directory Listings, a Google hackers best friend!

- intitle:"index of" "last modified"
 - Virtual file server, can reveal sensitive files web surfers shouldn't see
 - Index listings provide an x-ray into the system. Just because our target doesn't necessarily have directory listings, other sites with the same web apps might. This is handy!

- This helps narrow down server structure when we know which applications are installed...



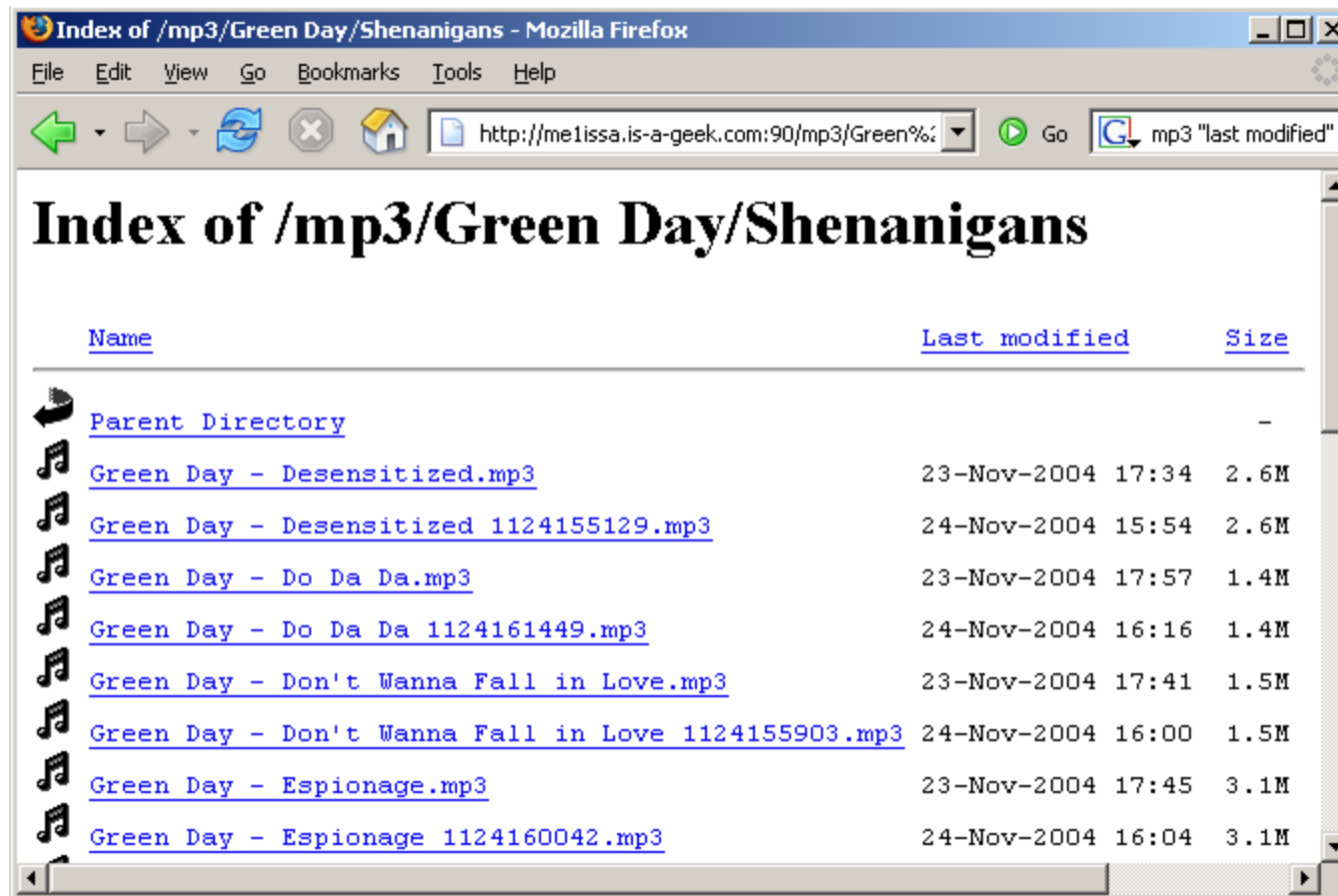


Who needs Kazaa?

- Peer to peer applications use non-standard ports.
- Not always possible to install with given access.
- P2P Ports can be blocked at the firewall level.

Google to the rescue!

- intitle:"index.of" Green Day mp3 last modified



The screenshot shows a Mozilla Firefox browser window with the title "Index of /mp3/Green Day/Shenanigans". The address bar displays the URL "http://me1issa.is-a-geek.com:90/mp3/Green%?". The search bar contains the query "mp3 'last modified'". The main content area shows a table of files with columns for Name, Last modified, and Size. The files listed are Green Day mp3 tracks, including "Desensitized.mp3", "Do Da Da.mp3", "Don't Wanna Fall in Love.mp3", and "Espionage.mp3".

Name	Last modified	Size
Parent Directory		-
Green Day - Desensitized.mp3	23-Nov-2004 17:34	2.6M
Green Day - Desensitized 1124155129.mp3	24-Nov-2004 15:54	2.6M
Green Day - Do Da Da.mp3	23-Nov-2004 17:57	1.4M
Green Day - Do Da Da 1124161449.mp3	24-Nov-2004 16:16	1.4M
Green Day - Don't Wanna Fall in Love.mp3	23-Nov-2004 17:41	1.5M
Green Day - Don't Wanna Fall in Love 1124155903.mp3	24-Nov-2004 16:00	1.5M
Green Day - Espionage.mp3	23-Nov-2004 17:45	3.1M
Green Day - Espionage 1124160042.mp3	24-Nov-2004 16:04	3.1M



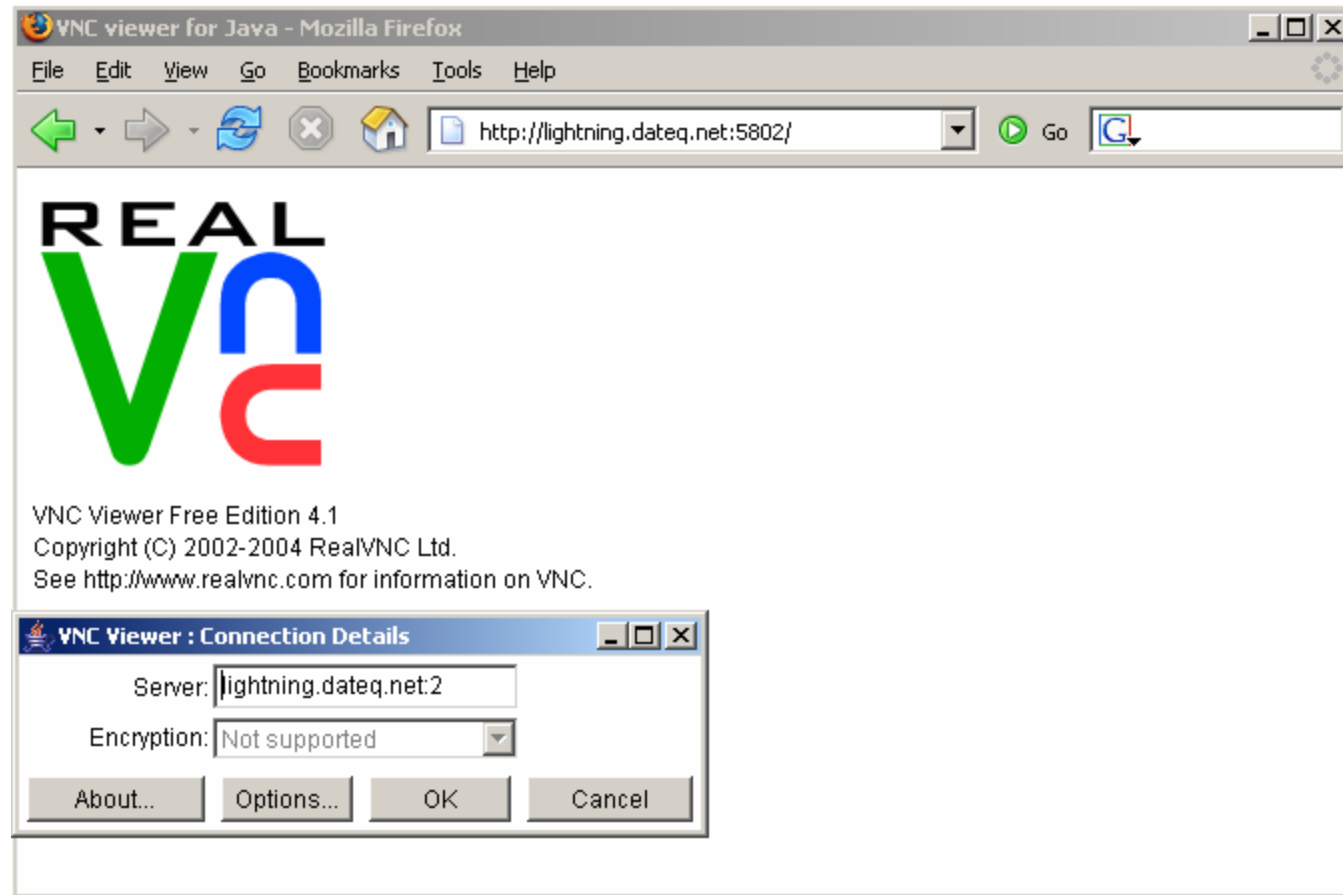
Google Hacking Showcase, 2005!

Let the games begin!

Each of these screenshots were found using nothing but Google.

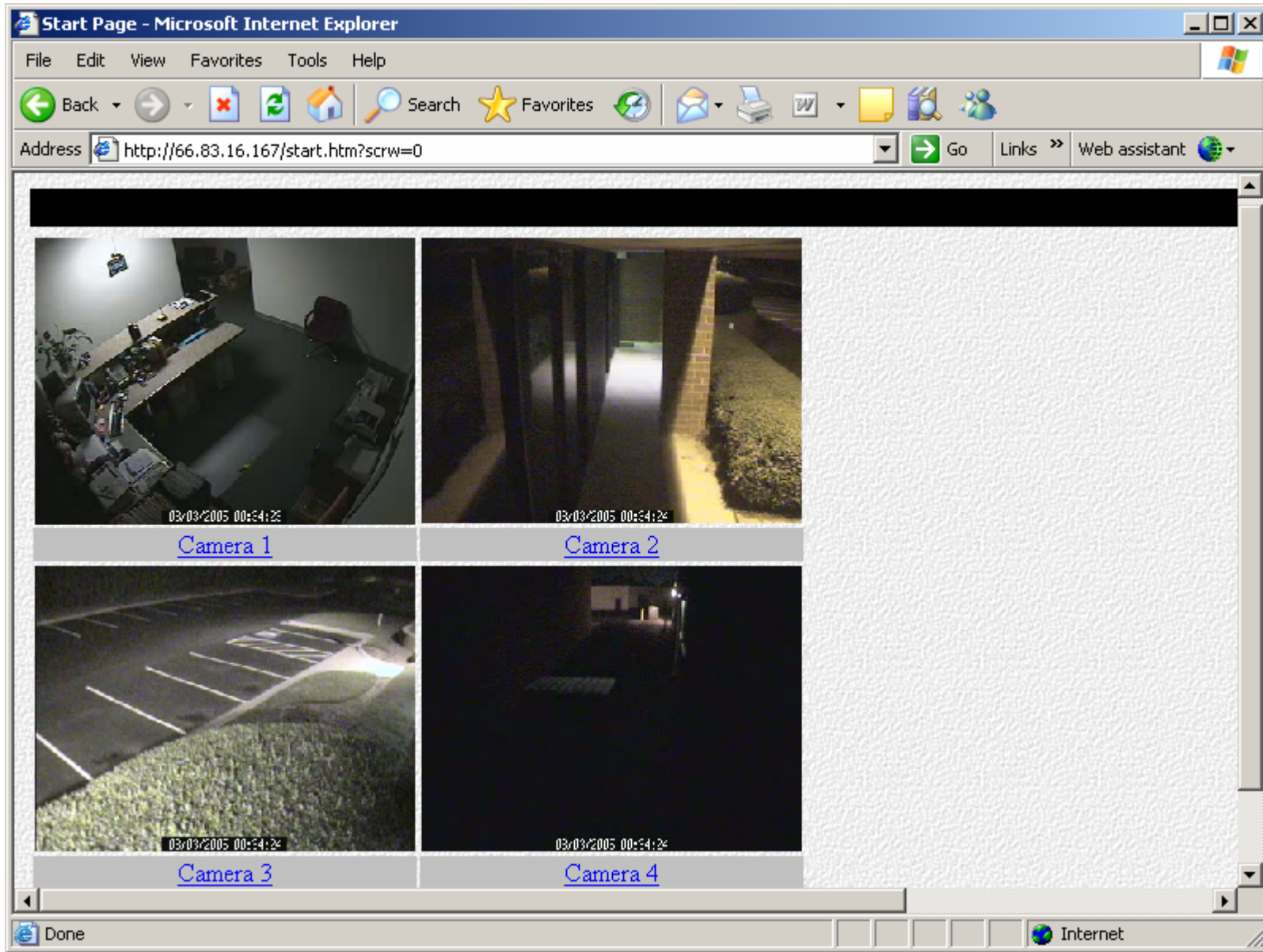
Here's some of the best of the worst:

intitle:"VNC Viewer for Java"

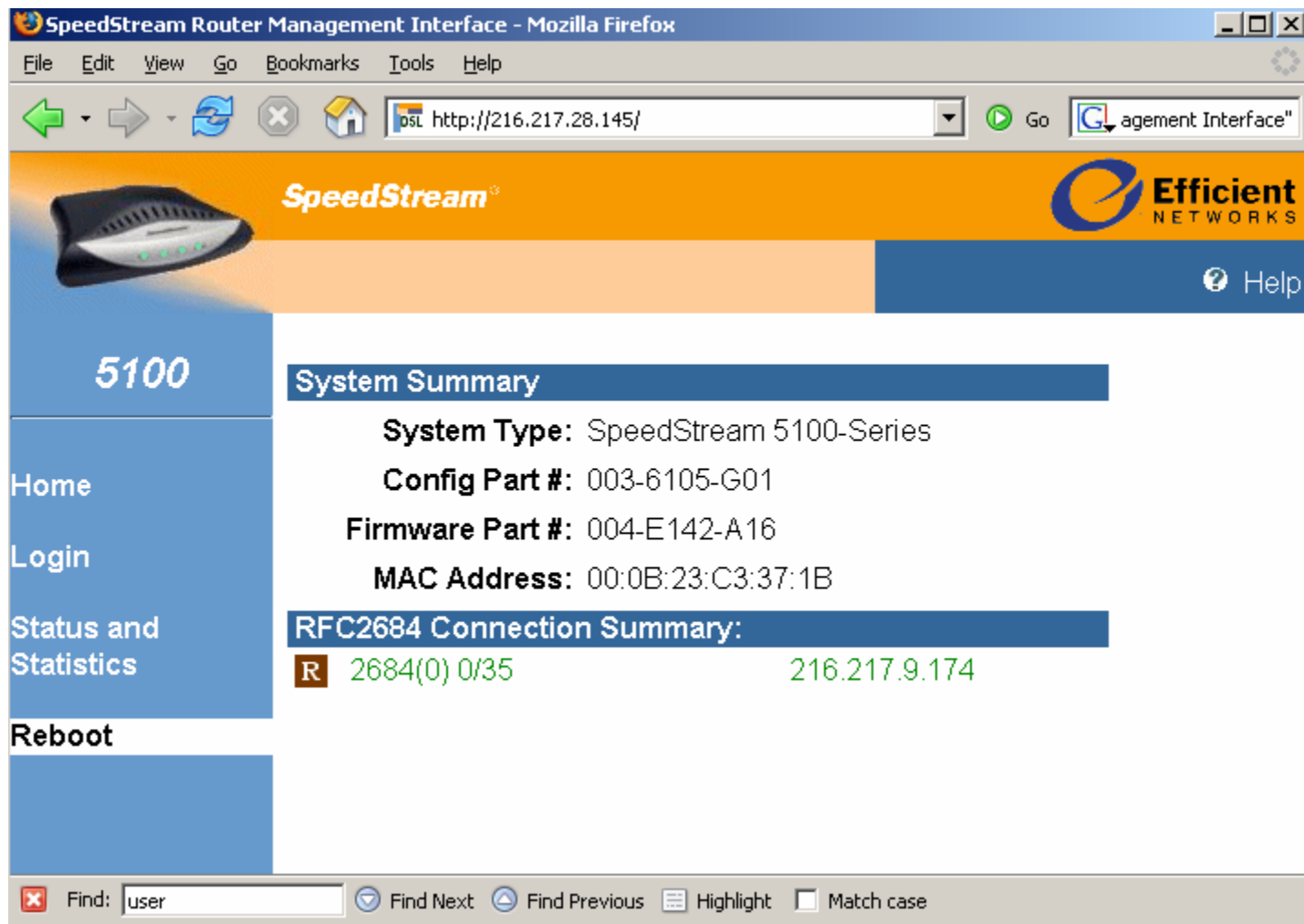


intitle:"toshiba network camera - user login"





intitle:"Speedstream Router Management Interface"



intitle:"Setup Home" "You will need to log in before"
"change" "settings"

Router Setup Home - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.mezco.com/ Go "change" "settings"

BELKIN Cable/DSL Gateway Router Setup Utility

Home | Help | Login Internet Status: **No Connection**

LAN Setup

- LAN Settings
- DHCP Client List

Internet WAN

- Connection Type
- DNS
- MAC Address

Wireless

- Channel and SSID
- Encryption
- Use as Access Point

Firewall

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

Utilities

- Parental Control
- Restart Router

Status

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

Version Info	
Firmware Version	v2.00.002
Boot Version	v0.00.010
Hardware	R01
Serial No.	S425027987

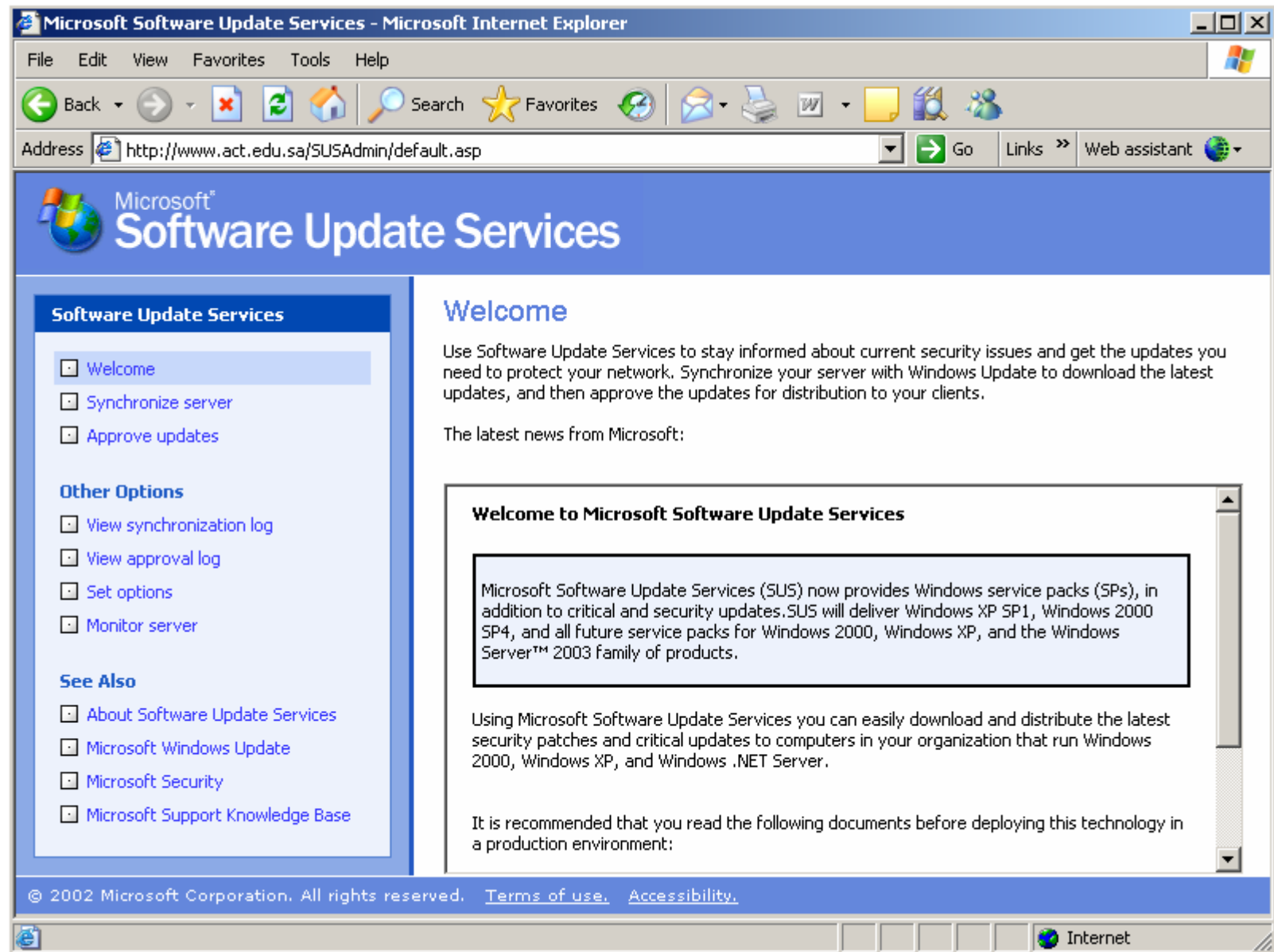
LAN Settings	
LAN/WLAN MAC	00-30-BD-CA-FD-14
IP address	192.168.2.1
Subnet mask	255.255.255.0
DHCP Server	Disabled

Internet Settings	
WAN MAC address	00-30-BD-CA-FD-15
Connection Type	STATIC
Subnet mask	255.255.255.0
Wan IP	66.9.153.201
Default gateway	66.9.153.1
DNS Address	160.79.5.130

Features	
NAT	Enabled
Firewall Settings	Disabled
SSID	Zukerman
Encryption	128-Auto

Find: user Find Next Find Previous Highlight Match case

inurl:SUSAdmin intitle:"Microsoft Software Update Services"



"set up administrator user" inurl:pivot

Pivot » setup - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.stefanleur.nl/blog/pivot/ Go

Pivot

Set up the Administrator User

Username:

Password:

Password (confirm):

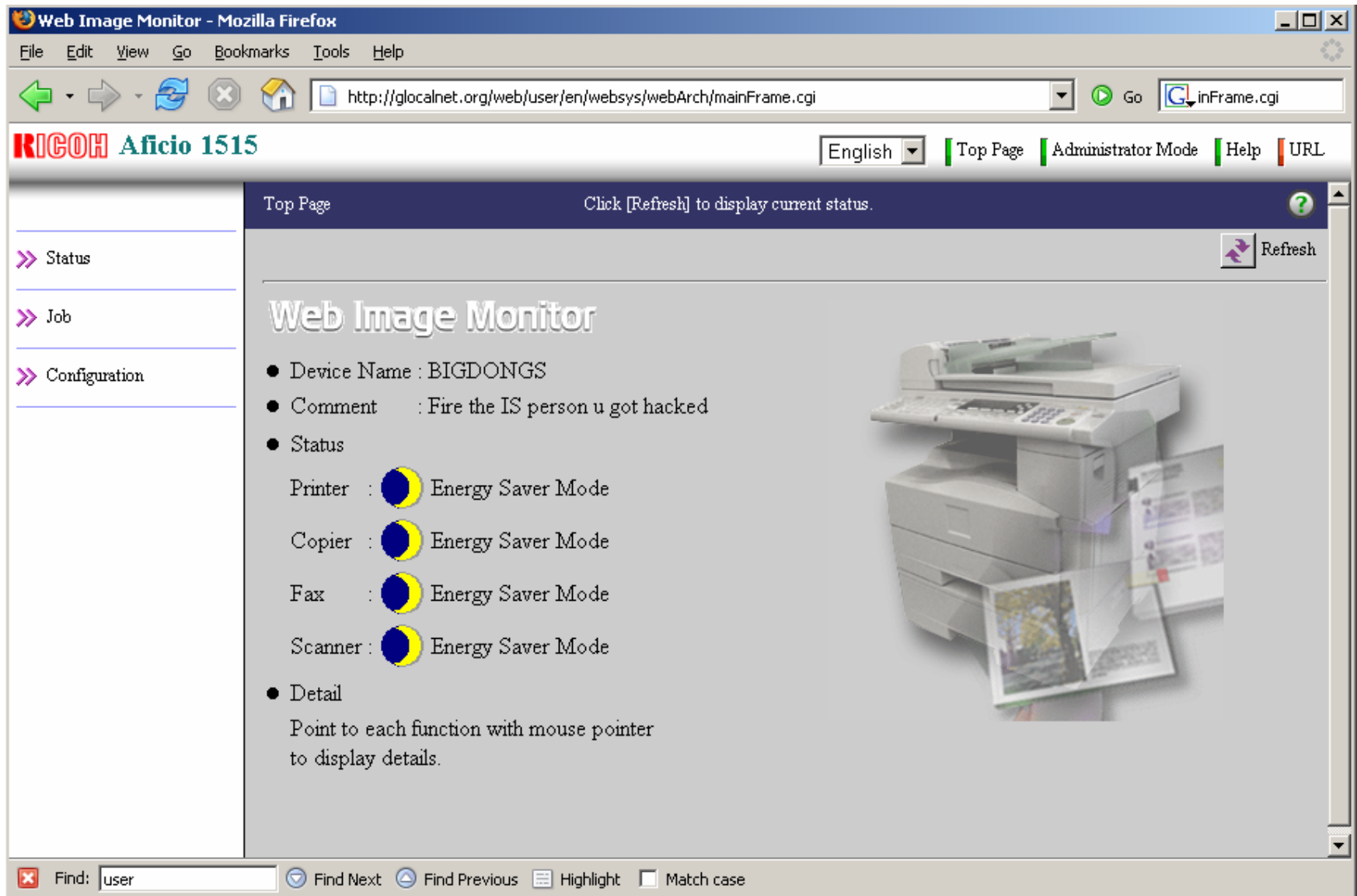
Email:

Nickname:

[proceed to login](#)

Find: user Find Next Find Previous Highlight Match case

inurl:webArch/MainFrame.cgi



intitle:"EpsonNet WebAssist" intitle:"Rev"

EpsonNet WebAssist Rev.4.1bE - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://kerr.udg.es/ Go Assist" intitle:"Rev"

[Home] [Help] [About WebAssist] [Link to EPSON] [Favorite]

EpsonNet WebAssist

Information

Printer

- Device
- Consumables
- Input
- Print
- Emulation
- Interface

Network

- General
- NetWare
- TCP/IP
- AppleTalk
- NetBEUI
- IPP
- SNMP

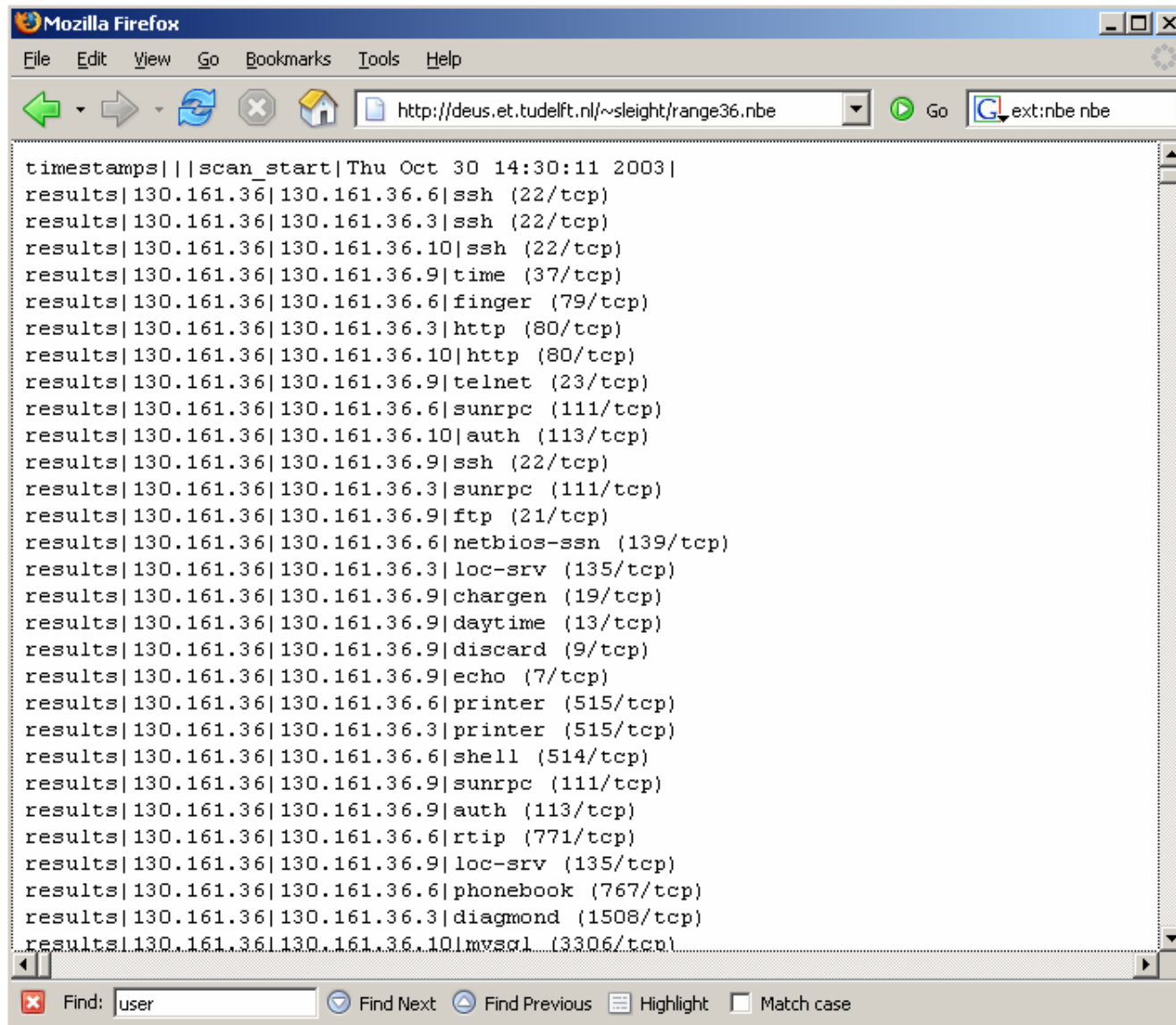
Configuration

TCP/IP

Get IP Address	Manual
IP Address	130.206.124.187
Subnet Mask	255.255.254.0
Default Gateway	130.206.124.1
Use a private IP address when an IP address cannot be assigned by the DHCP server.	Disable
Set by PING	Disable
Universal Plug and Play	Disable
Universal Plug and Play Device Name	AL-C1900-99139D

Find: user Find Next Find Previous Highlight Match case

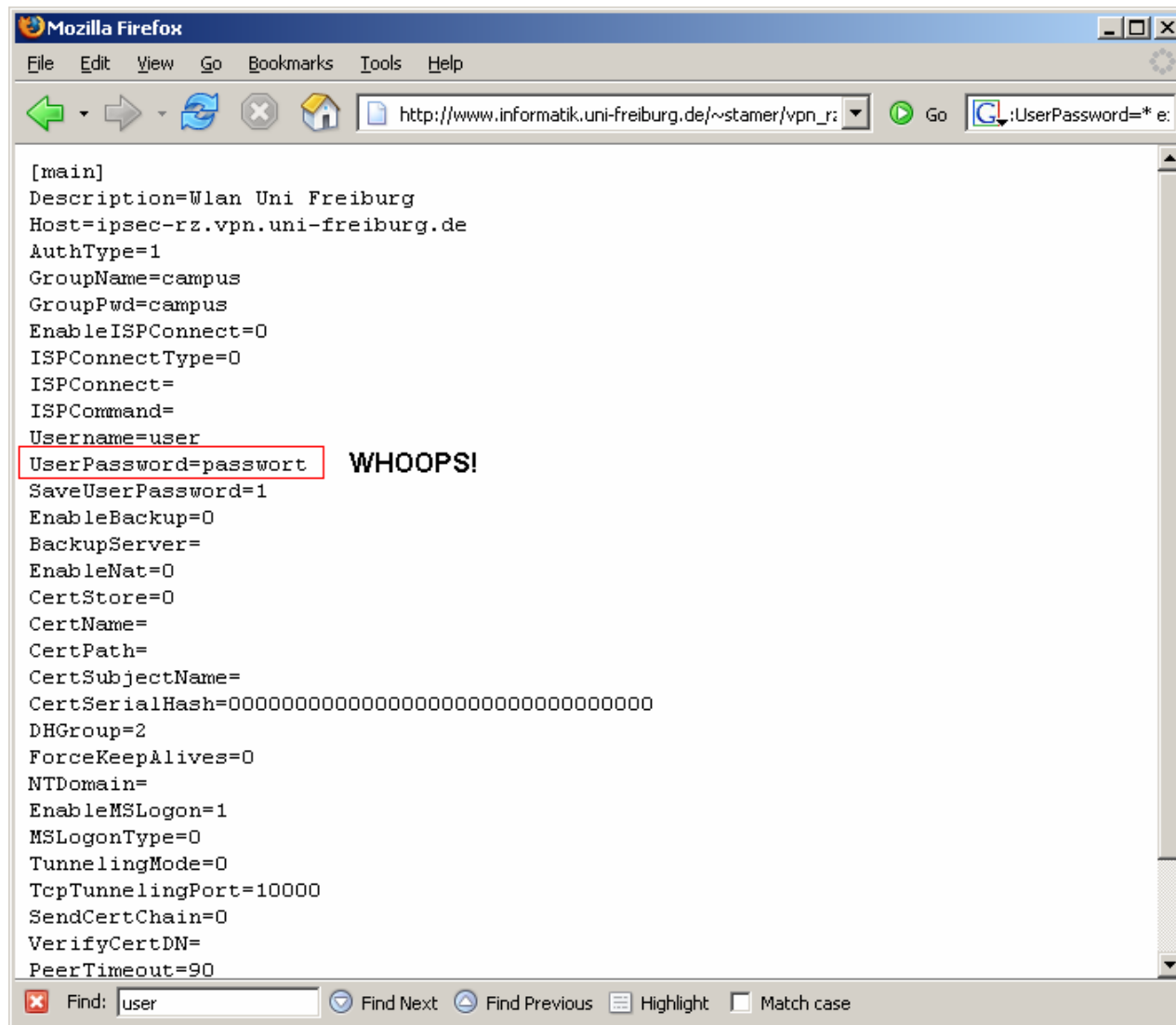
Nessus Scan output! ext:nbe nbe



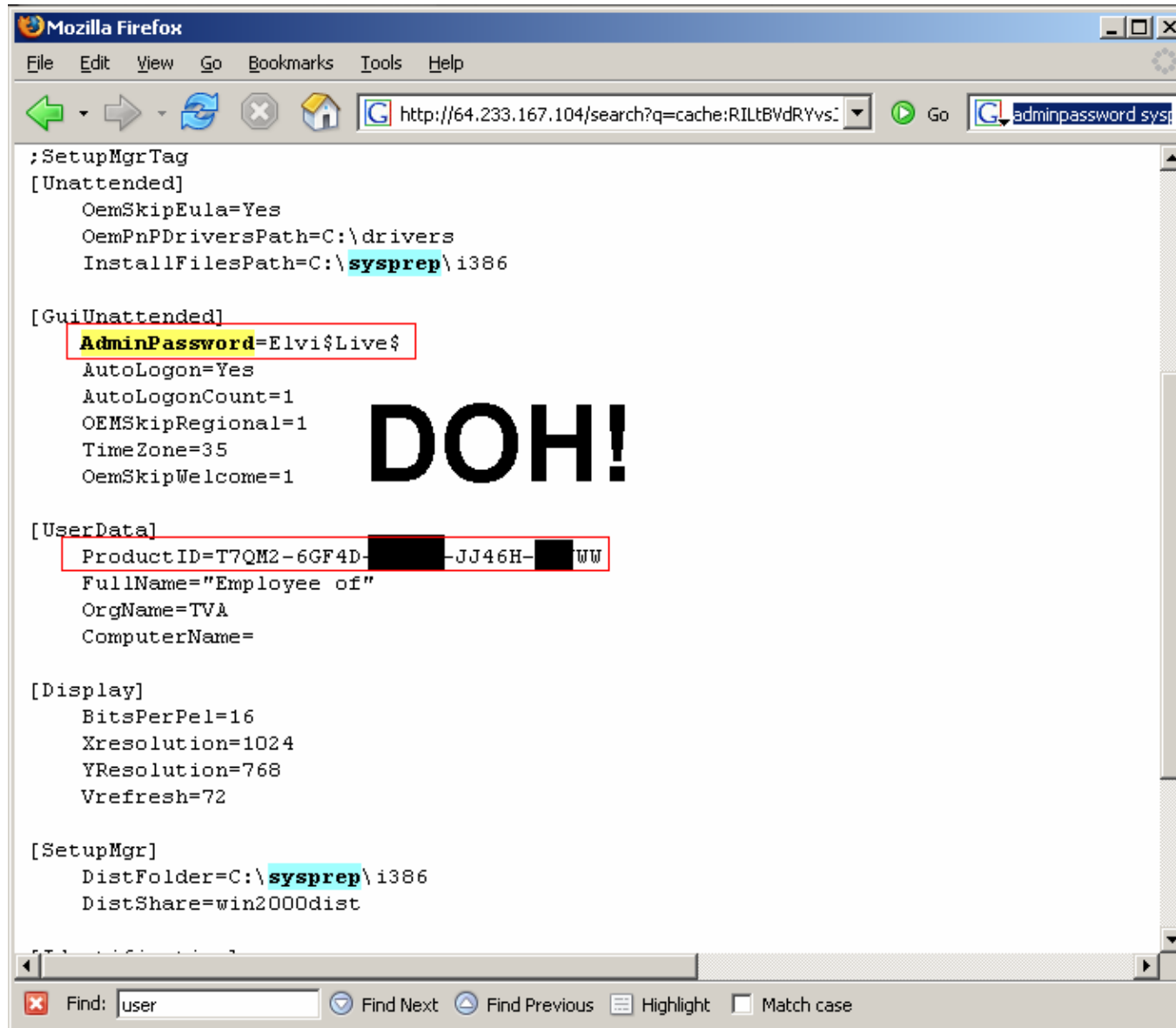
```
timestamps||scan_start|Thu Oct 30 14:30:11 2003|
results|130.161.36|130.161.36.6|ssh (22/tcp)
results|130.161.36|130.161.36.3|ssh (22/tcp)
results|130.161.36|130.161.36.10|ssh (22/tcp)
results|130.161.36|130.161.36.9|time (37/tcp)
results|130.161.36|130.161.36.6|finger (79/tcp)
results|130.161.36|130.161.36.3|http (80/tcp)
results|130.161.36|130.161.36.10|http (80/tcp)
results|130.161.36|130.161.36.9|telnet (23/tcp)
results|130.161.36|130.161.36.6|sunrpc (111/tcp)
results|130.161.36|130.161.36.10|auth (113/tcp)
results|130.161.36|130.161.36.9|ssh (22/tcp)
results|130.161.36|130.161.36.3|sunrpc (111/tcp)
results|130.161.36|130.161.36.9|ftp (21/tcp)
results|130.161.36|130.161.36.6|netbios-ssn (139/tcp)
results|130.161.36|130.161.36.3|loc-srv (135/tcp)
results|130.161.36|130.161.36.9|chargen (19/tcp)
results|130.161.36|130.161.36.9|daytime (13/tcp)
results|130.161.36|130.161.36.9|discard (9/tcp)
results|130.161.36|130.161.36.9|echo (7/tcp)
results|130.161.36|130.161.36.6|printer (515/tcp)
results|130.161.36|130.161.36.3|printer (515/tcp)
results|130.161.36|130.161.36.6|shell (514/tcp)
results|130.161.36|130.161.36.9|sunrpc (111/tcp)
results|130.161.36|130.161.36.9|auth (113/tcp)
results|130.161.36|130.161.36.6|rtip (771/tcp)
results|130.161.36|130.161.36.9|loc-srv (135/tcp)
results|130.161.36|130.161.36.6|phonebook (767/tcp)
results|130.161.36|130.161.36.3|diagmond (1508/tcp)
results|130.161.36|130.161.36.10|mvsq (3306/tcp)
```

VPN User Profiles

intext:Host=*. * intext:UserPassword=* ext:pcf



adminpassword sysprep filetype:inf



```
;SetupMgrTag
[Unattended]
    OemSkipEula=Yes
    OemPnPDriversPath=C:\drivers
    InstallFilesPath=C:\sysprep\i386

[GuiUnattended]
    AdminPassword=Elvi$Live$
    AutoLogon=Yes
    AutoLogonCount=1
    OEMSkipRegional=1
    TimeZone=35
    OemSkipWelcome=1

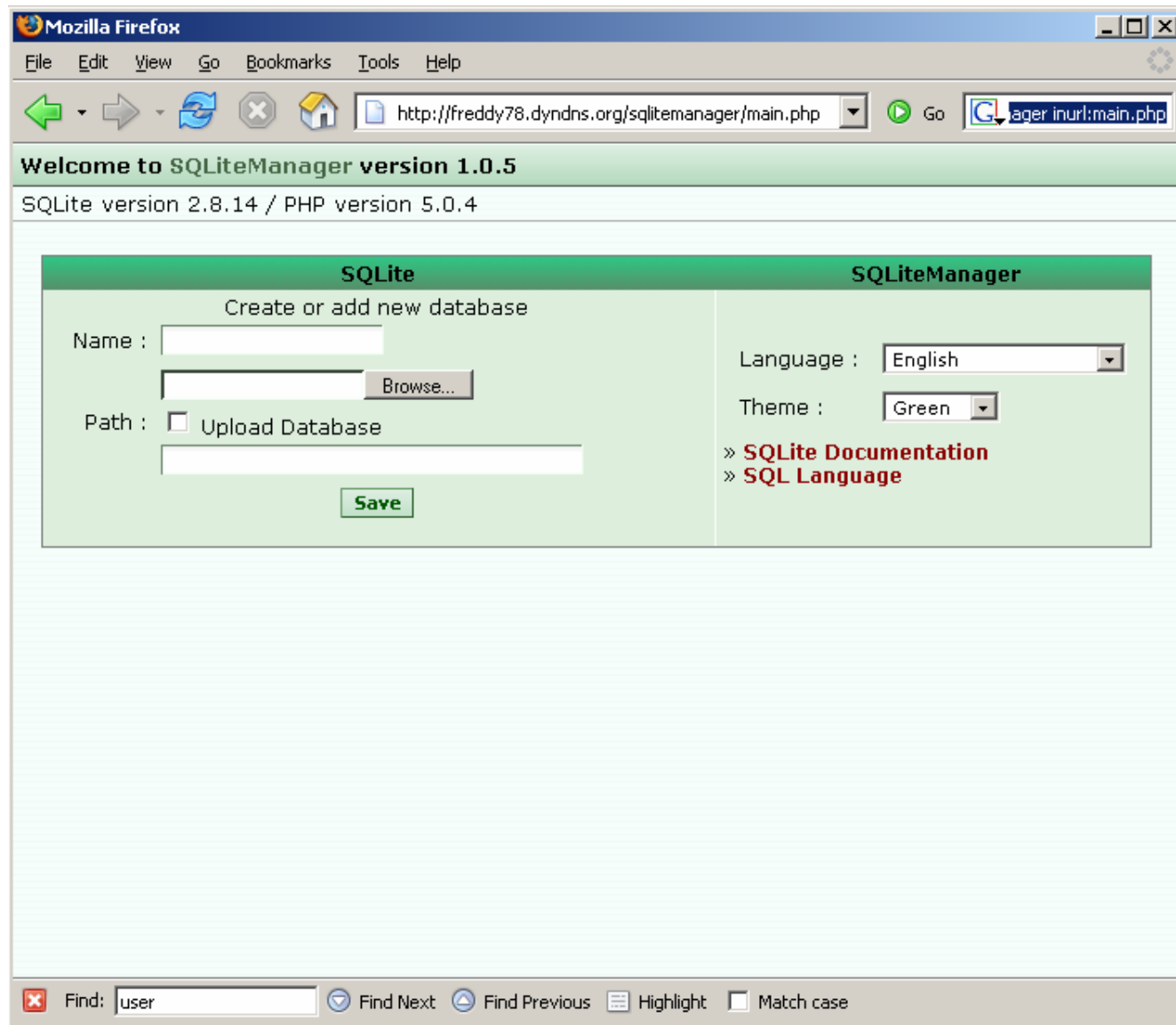
[UserData]
    ProductID=T7QM2-6GF4D- -JJ46H- WW
    FullName="Employee of"
    OrgName=TVA
    ComputerName=

[Display]
    BitsPerPel=16
    Xresolution=1024
    Yresolution=768
    Vrefresh=72

[SetupMgr]
    DistFolder=C:\sysprep\i386
    DistShare=win2000dist
```

Find: user Find Next Find Previous Highlight Match case

intext:SQLiteManager inurl:main.php



intitle:phpMyAdmin "Welcome to phpMyAdmin "*" "running on * as root@*"

The screenshot shows a web browser window with the address bar displaying "www.sulsters.net >> localhost | phpMyAdmin 2.6.0-pl2 - Mozilla Firefox". The browser's menu bar includes File, Edit, View, Go, Bookmarks, Tools, and Help. The address bar contains a search icon, a back icon, a forward icon, a refresh icon, a home icon, and a search icon. The search bar contains the text "ing on * as root@*". The main content area displays the title "Welcome to phpMyAdmin 2.6.0-pl2" and the text "MySQL 3.23.58 running on localhost as root@localhost". Below this, there are two main sections: "MySQL" and "phpMyAdmin". The "MySQL" section contains a "Create new database" form with a text input field and a "Create" button. Below this are several links: "Show MySQL runtime information", "Show MySQL system variables Documentation", "Show processes Documentation", "Reload MySQL Documentation", "Privileges", "Databases", and "Export". The "phpMyAdmin" section contains a "Language" dropdown menu set to "English (en-iso-8859-1)", a "Theme / Style" dropdown menu set to "Original", and several links: "phpMyAdmin documentation", "Show PHP information", "Official phpMyAdmin Homepage", "[ChangeLog]", "[CVS]", and "[Lists]". At the bottom of the page, a red-bordered box contains the following text: "Your configuration file contains settings (root with no password) that correspond to the default MySQL privileged account. Your MySQL server is running with this default, is open to intrusion, and you really should fix this security hole."

www.sulsters.net >> localhost | phpMyAdmin 2.6.0-pl2 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

ing on * as root@*

phpMyAdmin - Logo

Welcome to phpMyAdmin 2.6.0-pl2

MySQL 3.23.58 running on localhost as root@localhost

MySQL

Create new database [Documentation](#)

[Show MySQL runtime information](#)

☐ [Show MySQL system variables Documentation](#)

☐ [Show processes Documentation](#)

☐ [Reload MySQL Documentation](#)

☐ [Privileges](#)

☐ [Databases](#)

☐ [Export](#)

phpMyAdmin

☐ Language

☐ Theme / Style:

☐ [phpMyAdmin documentation](#)

☐ [Show PHP information](#)

☐ [Official phpMyAdmin Homepage](#)

[\[ChangeLog\]](#) [\[CVS\]](#) [\[Lists\]](#)

Your configuration file contains settings (root with no password) that correspond to the default MySQL privileged account. Your MySQL server is running with this default, is open to intrusion, and you really should fix this security hole.

intitle:"Sipura.SPA.Configuration" -.pdf

Sipura SPA Configuration - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://home.surreality.us:8080/advanced

Configuration" -.pdf

SIPURA
technology, inc.

Sipura Phone Adapter Configuration

Router Voice

Status Wan Setup Lan Setup Application Admin Login basic | advanced

Product Information

Product Name:	SPA-2100	Serial Number:	88013SE07587
Software Version:	2.0.5(a)	Hardware Version:	1.0.0(8970)
MAC Address:	000E08EA7C42	Client Certificate:	Installed
Customization:	Customized		

System Status

Current Time:	8/3/2005 01:29:38	Elapsed Time:	01:29:49
Wan Connection Type:	DHCP	Current IP:	69.160.159.112
Host Name:	sipura	Domain:	broadvoice.com
Current Netmask:	255.255.254.0	Current Gateway:	69.160.158.1
Primary DNS:	147.135.0.6		
Secondary DNS:	147.135.8.6		
LAN IP Address:	172.16.0.1	Broadcast Pkts Sent:	2
Broadcast Bytes Sent:	684	Broadcast Pkts Recv:	169298
Broadcast Bytes Recv:	10197078	Broadcast Pkts Dropped:	0
Broadcast Bytes Dropped:	0		

Undo All Changes Submit All Changes

Admin Login basic | advanced


Copyright © 2003 Sipura Technology. All Rights Reserved.

intitle:"EverFocus" intitle:"Applet"


EverFocus EDSR Applet (1.4) - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

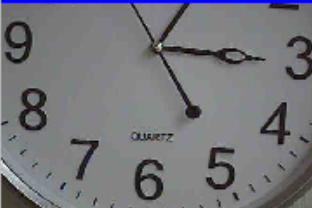
Camera 1 2005/08/03 15:03:04




Camera 2 2005/08/03 15:03:05




Camera 3 2005/08/03 15:03:08




Camera 4 2005/08/03 15:03:08




Camera 5 2005/08/03 15:03:11




Camera 6 2005/08/03 15:03:12




Camera 7 2005/08/03 15:02:43




Camera 8 2005/08/03 15:03:15




Camera 9 2005/08/03 15:03:17




Camera 10 2005/08/03 15:02:51




Camera 11 2005/08/03 15:02:55




Camera 12 2005/08/03 15:02:58




Camera 13 2005/08/03 15:02:30




Camera 14 2005/08/03 15:02:59



Camera 15 2005/08/03 15:03:03



Camera 16 2005/08/03 15:02:33





☒ BY SEGMENT LIST

☐ BY ALARM LIST

☐ BY DATE TIME

☐ PTZ CONTROL

Play

Refresh

LIVE

2005/08/03 15:03:17

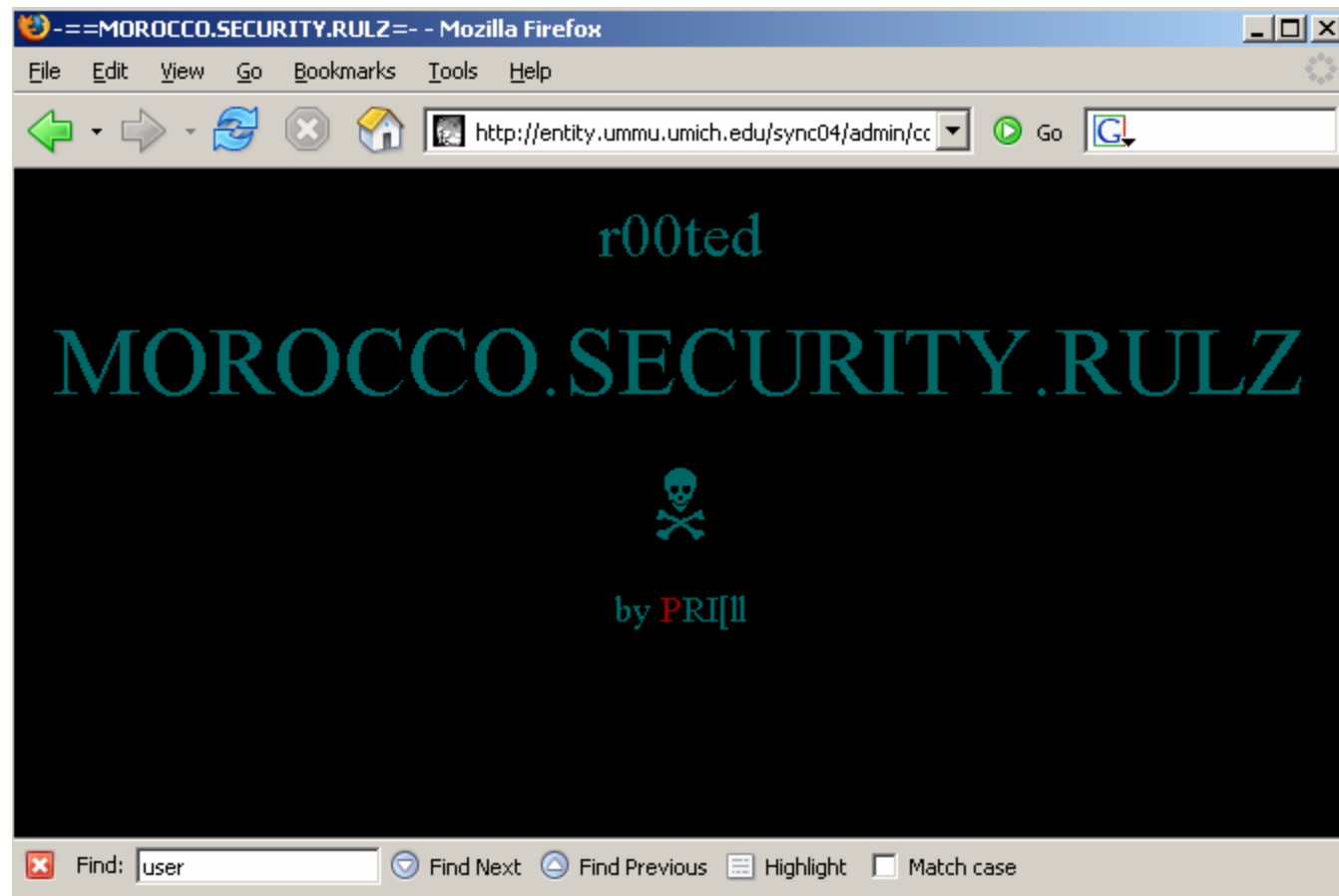








Even UMich is vulnerable...



intitle:"TANDBERG" "This page requires a frame capable browser!" site:umich.edu

POLYCOM

Network Statistics
Advanced Statistics
Remote Control
Call Log
Home

Setup System Diagnostics Admin Home Place a Call View a Presentation Select a Presentation

System Name: Media Union PolyCom Three

Address Book Global Address Book Manual Dial

Univ. of Michigan CR3
Polycom Japan IP
Polycom Milpitas Lobby
Polycom Milpitas USA
Polycom Southern Europe
Shared Codec UM
UMN Geology and Geophysics Lab
Univ. of Michigan CR3
vidconf.rcat.utoronto.ca

Name: Univ. of Michigan CR3

384 141.213.30.154

Call this Site

NEAR FAR

H.323 Number: Cause Code:

1P GK

javascript:DisplayEntry('localaddr', 29)

intitle:"Big Brother - Status" inurl:bb

yellow : Big Brother - Status @ Tue Aug 2 23:48:02 EDT 2005 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://pythagoras.its.umd.umich.edu/bb/Sun/S Go edu inurl:robots.txt

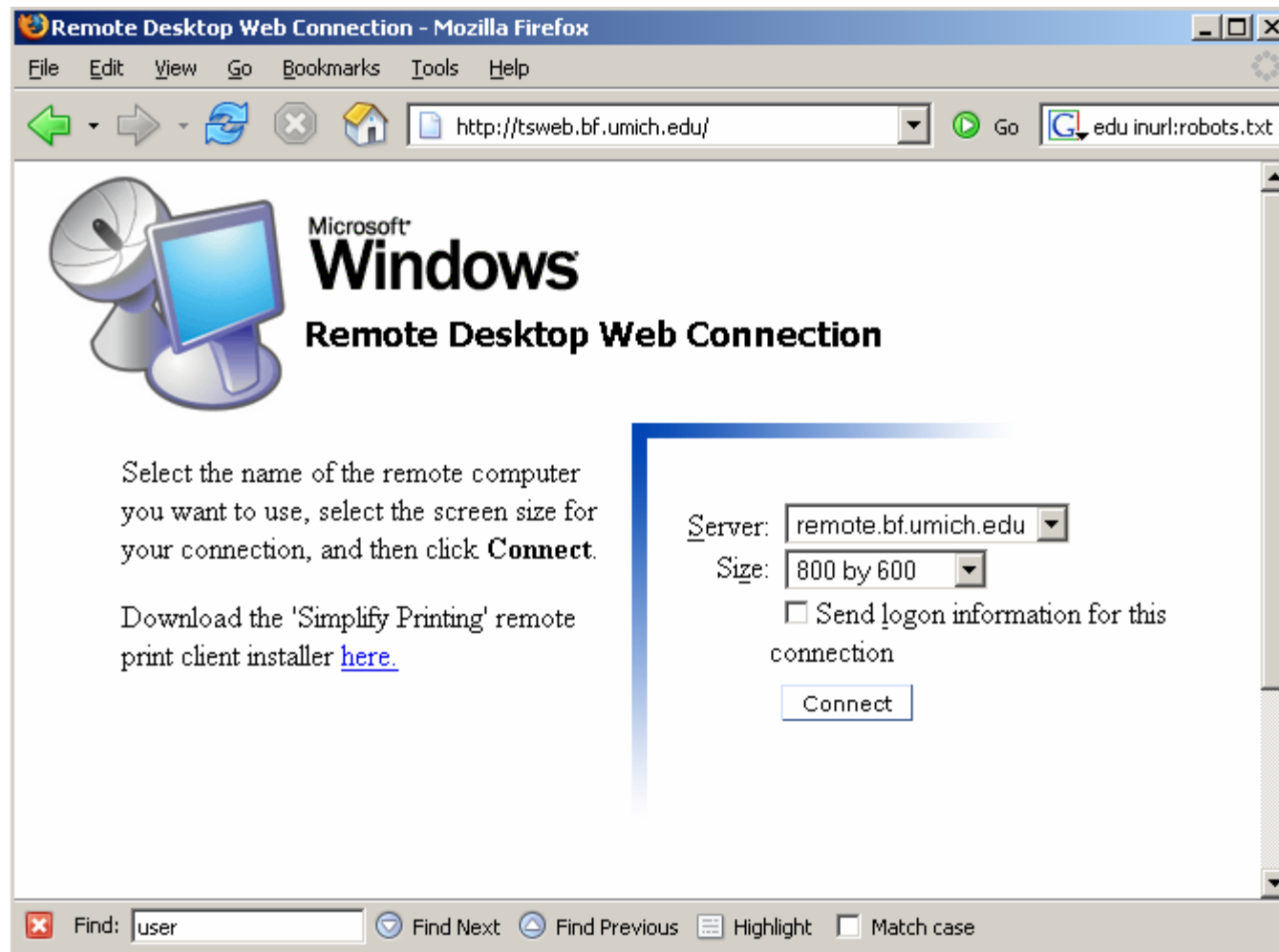
big brother last update
Tue Aug 2 23:48:02 EDT 2005

To be installed

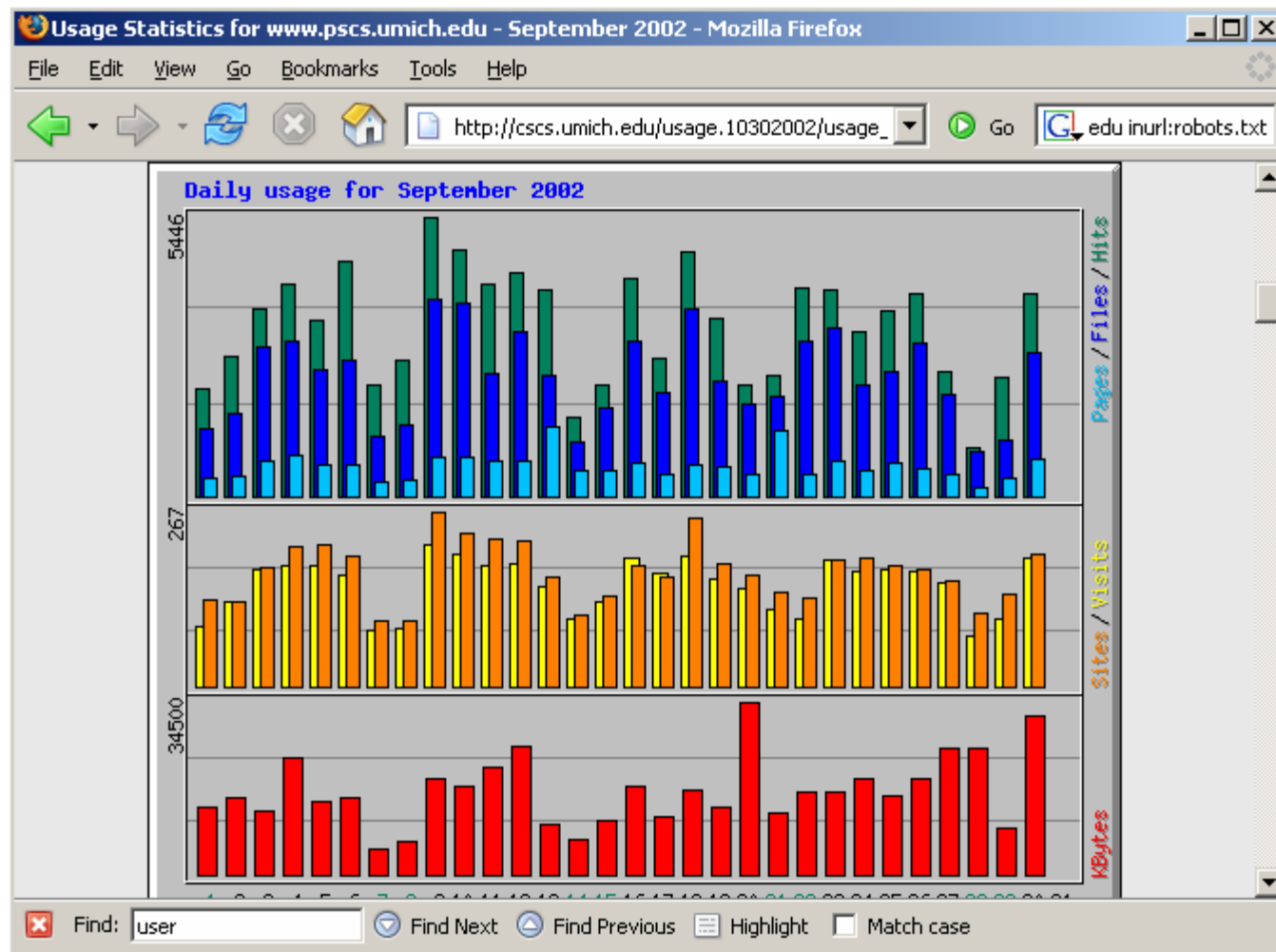
	conn	cpu	disk	msgs	procs	ssh
mars.umd.umich.edu						-
backup.its.umd.umich.edu		-	-	-	-	
vega.umd.umich.edu		-	-	-	-	-
compassion.its.umd.umich.edu		-	-	-	-	
spica.its.umd.umich.edu		-	-	-	-	-

Find: user Find Next Find Previous Highlight Match case

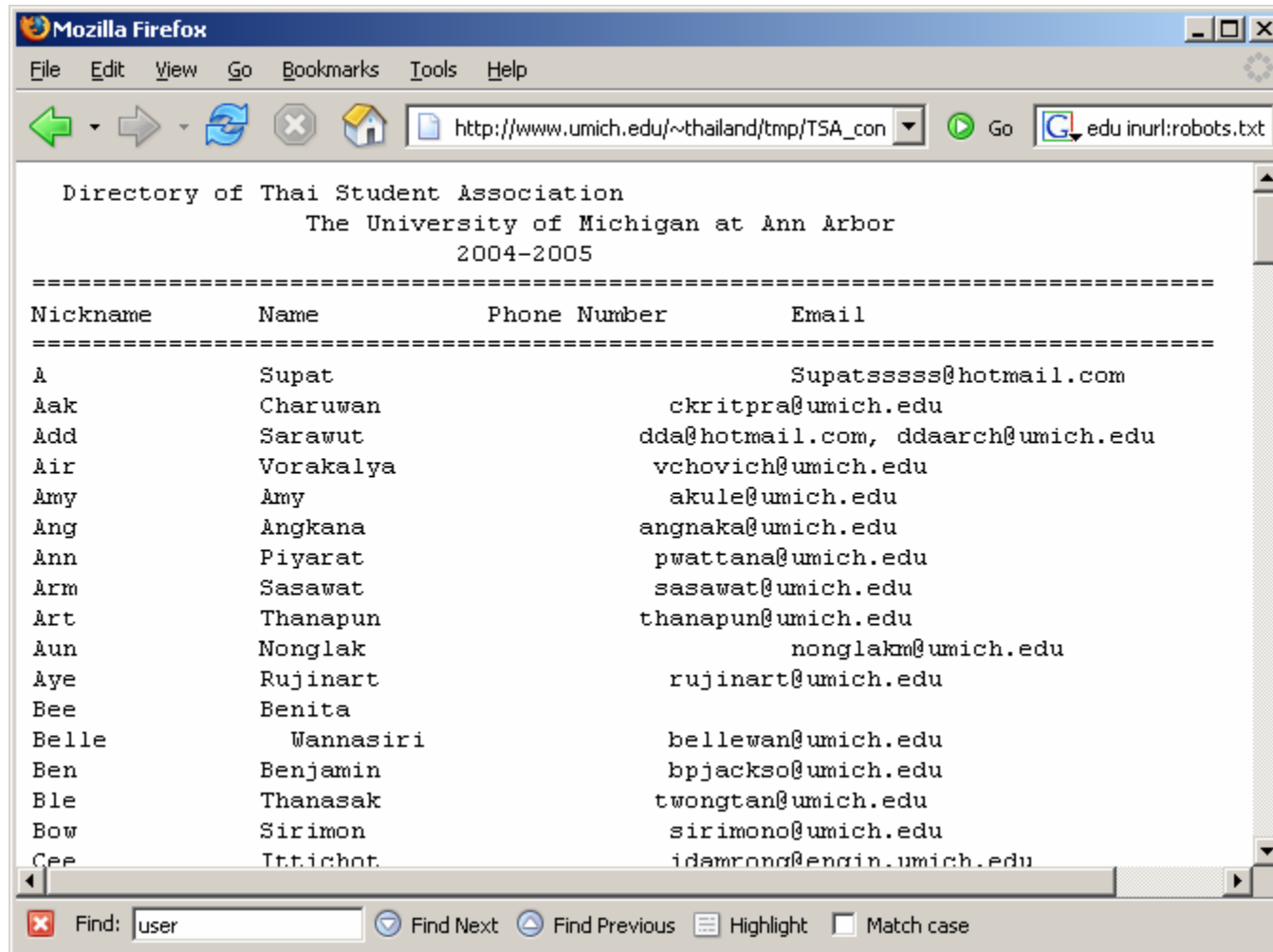
intitle:Remote.Desktop.Web.Connection inurl:tsweb



+intext:"webalizer" +intext:"Total
Usernames" +intext:"Usage Statistics for"



inurl:/tmp



"please log in"

www.biokids.umich.edu - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.biokids.umich.edu/login_form Go edu inurl:robots.txt

Please log in

Search:

To access this part of the site, you need to log in with your username and password.

User Name:

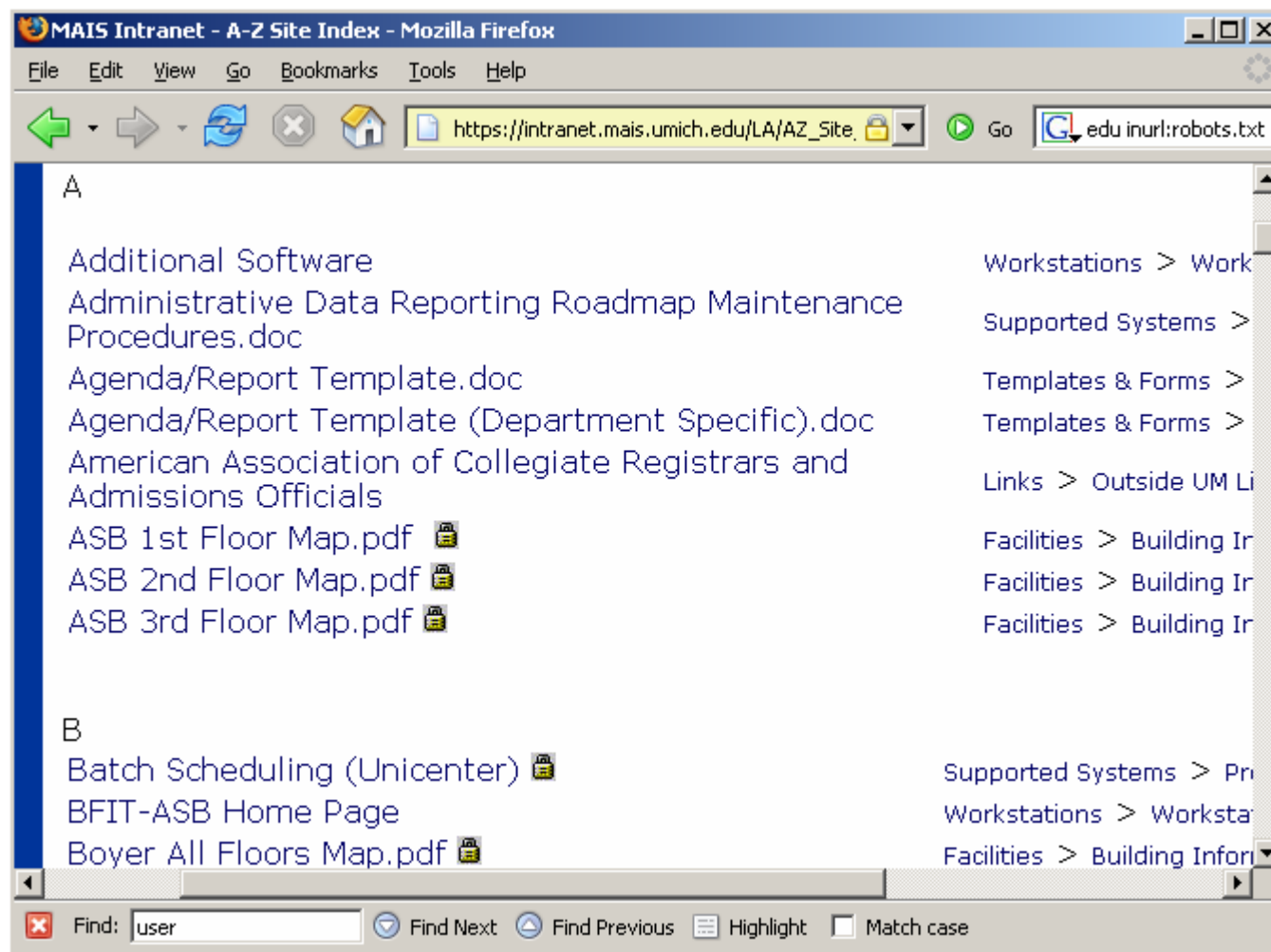
Password:

☒ Remember my name.
Setting the 'Remember my name' option will create a cookie with your username. When you log in later, your user name will already be filled in for you.

Forgotten your password? [Click here](#) to have it mailed to you.

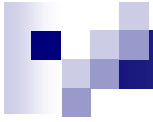
Find: user Find Next Find Previous Highlight Match case

intitle:intranet inurl:intranet +intext:"human resources"



inurl:"exchange/logon.asp" OR intitle:"Microsoft Outlook Web Access - Logon"





- My personal favorite...

site:umich.edu filetype:mbox

Mozilla Firefox
File Edit View Go Bookmarks Tools Help

http://[REDACTED].umich.edu/pipermail/mailman.mbox/mailman.mbox

.COM Gmail - Inbox http://mbox/mailman.mbox

List-Subscribe: <http://fp2.fp.med.umich.edu/mailman/listinfo/mailman>,
<mailto:mailman-request@fp2.fp.med.umich.edu?subject=subscribe>
X-List-Received-Date: Wed, 07 Jul 2004 23:44:45 -0000

-----92453380050713374==
Content-Type: multipart/signed; micalg=sha1; boundary=Apple-Mail-17--732470900;
protocol="application/pkcs7-signature"

--Apple-Mail-17--732470900
Content-Transfer-Encoding: 7bit
Content-Type: text/plain;
charset=US-ASCII;
format=flowed

I believe this is up and running. Instructions on administering the
mailman server can be found at:

<http://staff.imsa.edu/~ckolar/mailman/mailman-admin-quickref-0.2.html>
<http://staff.imsa.edu/~ckolar/mailman/mailman-administration-v2.html>
<http://www.gnu.org/software/mailman/site.html>
<http://www.gnu.org/software/mailman/mailman-member/index.html>

mailman@[REDACTED].umich.edu is the admin user with the password gobblue.

--Jason
--Apple-Mail-17--732470900



So, what can be done?

■ Preventative maintenance

- ☐ Disable directory listings if you do not need them.
- ☐ Password protect sensitive directories
- ☐ Robots.txt
 - But don't let Google crawl it ;)
- ☐ Don't use default passwords!
 - Do I really need to say this?
- ☐ Google's removal page
 - <http://www.google.com/remove.html>



Go hack yourself, pal!

- Wikto from Sensepost.
- Athena
- Gooscan
 - Note: Gooscan violates Google's TOS
 - You really do not want Google pissed at you. Remember Old Yeller? Sadder than that.

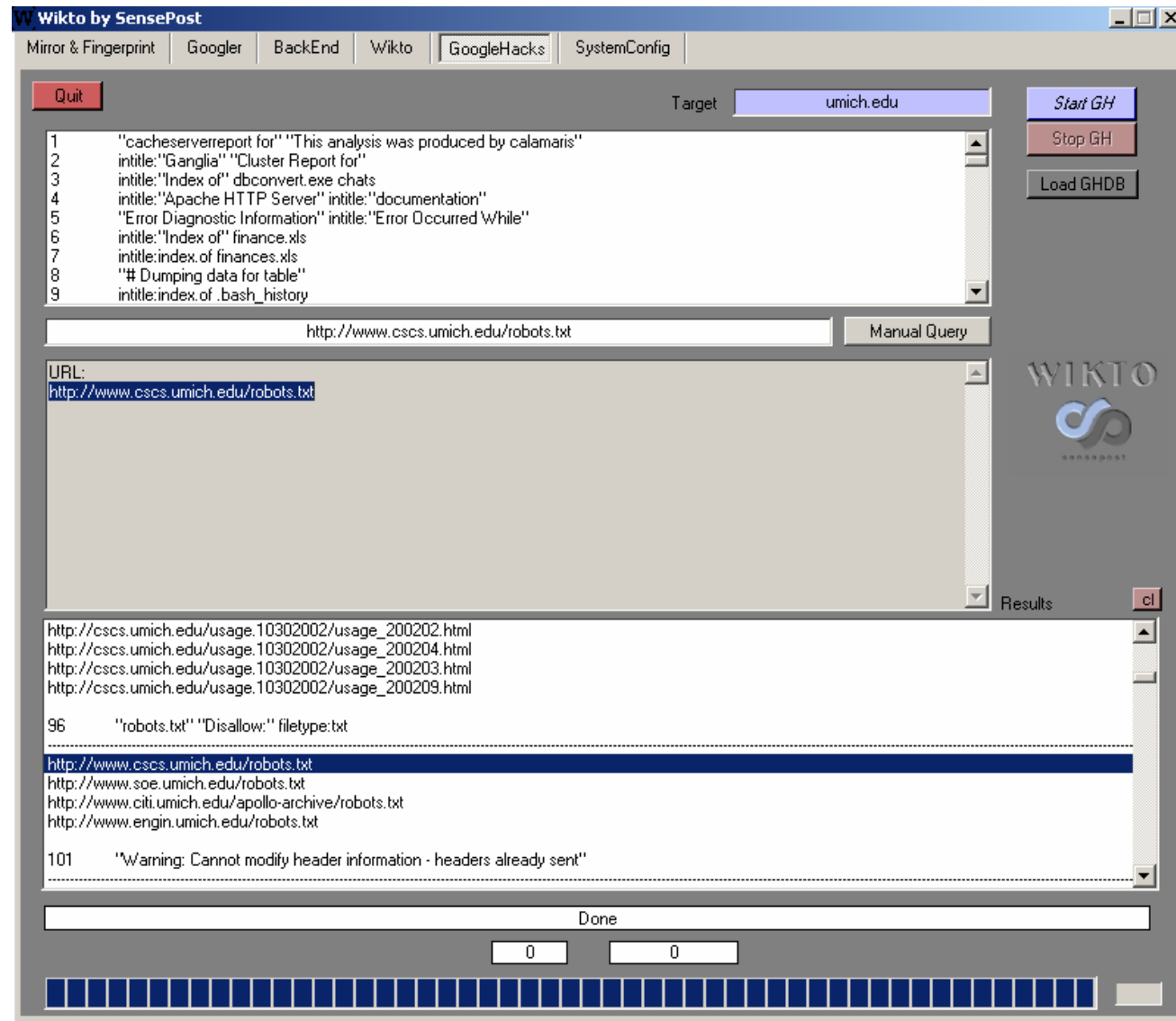


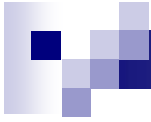
WIKTO, by Sensepost

- Automates Google Hack Scanning
- Available for free from www.sensepost.com
- Requires a valid Google API Key
- Designed to allow site owners to test themselves for vulnerabilities



Wikto





Thanks!

- UMich for having me out
- Johnny Long for being a mentor and a friend
- The whole team at <http://johnny.ihackstuff.com>
- The endless (misguided?) loving support of my family and friends, and co-workers
- The 7-11 by my house, for always being there for me when I need them.

Without the help of all of these people and more, none of this would be possible and I might still be jockeying tapes at the video store.