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

[Image of a Google search interface with query parameters: intitle:"i hack stuff" inurl:"hackstuff" intext:"navigate"]

- Business Solutions - About Google

©2009 Google - Searching 6,058,044,051 web pages
Advanced Google Searching

http://johnny.ihackstuff.com

intitle:"I hack stuff"
inurl:"ihackstuff"

intext:"navigate"

Navigate

Home
Who's Johnny?
The Forums
downloads
Google Hacking
Database (GHD8)
photo/art
web links
site search

Blackhat USA / Defcon 2005

Posted by: jJohnny - 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: Zbrothers, Renegade334, Roslof and the Sansploit Crew, Andrew and the Syngress crew, Mudge, Dan Kaminsky, Kevin Mitnick, Richard Thiemer, Thor, Blue Boar, Jay Beale, Tom Parker, Grifter, Caeser, 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.
Google Hacking Basics

Putting advanced operators together in intelligent ways can cause a seemingly innocuous query…
Google Hacking Basics

...can have **devastating** results!
Basic Domain Crawling

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

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

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 ...
webvcs.itcs.umich.edu/jobnet/job_posting.php/postingnumber=045873 - 6k - Cached - Similar pages

UMMA 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!
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
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
Directory Transversal

- inurl:"php?page=" inurl:html
Directory Transversal

This...

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!
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?
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"
PHP Ping

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

Enter ip address or FQDN to ping

YOUR INPUT: johnny.ihackstuff.com
PING johnny.ihackstuff.com (216.133.72.171) from 24.81.102.254 : 56(84) bytes of data.
64 bytes from earth.nexus.net (216.133.72.171): icmp_seq=1 ttl=54 time=120 ms
64 bytes from earth.nexus.net (216.133.72.171): icmp_seq=2 ttl=54 time=115 ms
64 bytes from earth.nexus.net (216.133.72.171): icmp_seq=3 ttl=54 time=113 ms
64 bytes from earth.nexus.net (216.133.72.171): icmp_seq=4 ttl=54 time=117 ms

--- johnny.ihackstuff.com ping statistics ---
4 packets transmitted, 4 received, 0% loss, time 3037ms
rtt min/avg/max/mdev = 113.325/116.670/120.751/2.766 ms
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"
CGIPProxy

- intitle:"start using cgiproxy" no scripts ads

CGIPProxy

Start browsing through this CGI-based proxy by entering a URL below. Only HTTP and FTP URLs are supported. Not all functions will work (e.g. some JavaScript), but most pages will be fine.

- Remove all cookies (except certain proxy cookies)
- Remove all scripts (recommended for anonymity)
- Remove ads
- Hide referrer information
- Show URL entry form

Begin browsing

Manage cookies

CGIProxy 2.0.1
WebUtil

"inurl:webutil.pl"

WebUtil Version: 2.7

By The Puppet Master

Make Your Choice Below

Note: Depending on present net traffic and the speed of your link.
Some of these commands may take a long time. Patience is a virtue.

- ping
- traceroute
- whois
- finger
- netlookup
- host
- chquery
- dig
- calendar
- uptime

WebUtil © Copyright 1998-2001 The Puppet Master
Parseform.pl is © Copyright The CGI/Perl Cookbook
Network Query Tool

- intitle:"network query tool"
Cache is your friend!

This is Google's cache of http://ncc.nekesc.org/nqt.php as retrieved on Jul 26, 2005 09:57:57 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:


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

These search terms have been highlighted: network query tool
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...

<table>
<thead>
<tr>
<th>Name</th>
<th>Last Modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/</td>
<td>07-Feb-2005 17:48</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>common.php</td>
<td>13-May-2002 17:18</td>
<td>5.4K</td>
<td></td>
</tr>
<tr>
<td>config.php</td>
<td>24-Mar-2003 20:44</td>
<td>282</td>
<td></td>
</tr>
<tr>
<td>contrib/</td>
<td>07-Feb-2005 17:40</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>db/</td>
<td>07-Feb-2005 17:49</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>docs/</td>
<td>07-Feb-2005 17:49</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>extension.inc</td>
<td>04-Apr-2002 15:52</td>
<td>835</td>
<td></td>
</tr>
<tr>
<td>faq.php</td>
<td>31-Mar-2002 03:06</td>
<td>3.7K</td>
<td></td>
</tr>
<tr>
<td>groundrhn</td>
<td>20-May-2002 04:21</td>
<td>46K</td>
<td></td>
</tr>
</tbody>
</table>
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
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"
You will need to log in before you can change any settings.
Welcome

Use Software Update Services to stay informed about current security issues and get the updates you need to protect your network. Synchronize your server with Windows Update to download the latest updates, and then approve the updates for distribution to your clients.

The latest news from Microsoft:

Welcome to Microsoft Software Update Services

Microsoft Software Update Services (SUS) now provides Windows service packs (SPs), in addition to critical and security updates. SUS will deliver Windows XP SP1, Windows 2000 SP4, and all future service packs for Windows 2000, Windows XP, and the Windows Server™ 2003 family of products.

Using Microsoft Software Update Services you can easily download and distribute the latest security patches and critical updates to computers in your organization that run Windows 2000, Windows XP, and Windows .NET Server.

It is recommended that you read the following documents before deploying this technology in a production environment:
"set up administrator user" inurl:pivot
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.
<table>
<thead>
<tr>
<th>TCP/IP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Get IP Address</td>
<td>Manual</td>
</tr>
<tr>
<td>IP Address</td>
<td>130.206.124.187</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.254.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>130.206.124.1</td>
</tr>
<tr>
<td>Use a private IP address when an IP address cannot be assigned by the DHCP server</td>
<td>Disable</td>
</tr>
<tr>
<td>Set by PING</td>
<td>Disable</td>
</tr>
</tbody>
</table>

- Universal Plug and Play
- Universal Plug and Play Device Name: AL-C1900-99139D
Nessus Scan output! ext:nbe nbe
VPN User Profiles

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

[main]
Description=Ulan Uni Freiburg
Host=ipsec-r2.vpn.uni-freiburg.de
AuthType=1
GroupName= campus
GroupPwd=campus
EnableISPCConnect=0
ISPCConnectType=0
ISPCConnect=
ISPCCommand=
Username=user
UserPassword=password  WHOOOPS!
SaveUserPassword=1
EnableBackup=0
BackupServer=
EnableNet=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DGroup=2
FsockKeepAlives=0
NDomain=
EnableMSLogon=1
MSLogonType=0
TunnelingMode=0
TcpTunnelingPort=10000
SendCertChain=0
VerifyCertID=
PeerTimeout=90

Find: user Find Next Find Previous Highlight Match case
adminpassword sysprep filetype:inf

DOH!
Welcome to SQLiteManager version 1.0.5
SQLite version 2.8.14 / PHP version 5.0.4

<table>
<thead>
<tr>
<th>SQLite</th>
<th>SQLiteManager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>Language: English</td>
</tr>
<tr>
<td>Path:</td>
<td>Theme: Green</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Create or add new database</td>
<td>» SQLite Documentation</td>
</tr>
<tr>
<td></td>
<td>» SQL Language</td>
</tr>
</tbody>
</table>

![SQLiteManager in action](image.png)
Welcome to phpMyAdmin 2.6.0-pl2
MySQL 3.23.58 running on localhost as root@localhost

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.
### Product Information

<table>
<thead>
<tr>
<th>Product Name:</th>
<th>SPA-2100</th>
<th>Serial Number:</th>
<th>800135E07587</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Version:</td>
<td>2.0.5(a)</td>
<td>Hardware Version:</td>
<td>1.8.0(8970)</td>
</tr>
<tr>
<td>MAC Address:</td>
<td>000E06EA7C42</td>
<td>Client Certificate:</td>
<td>Installed</td>
</tr>
<tr>
<td>Customization:</td>
<td>Customized</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### System Status

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Wan Connection Type:</td>
<td>DHCP</td>
<td>Current IP:</td>
<td>69.160.139.112</td>
</tr>
<tr>
<td>Host Name:</td>
<td>sipura</td>
<td>Domain:</td>
<td>broadvoice.com</td>
</tr>
<tr>
<td>Current Netmask:</td>
<td>255.255.254.0</td>
<td>Current Gateway:</td>
<td>69.160.158.1</td>
</tr>
<tr>
<td>Primary DNS:</td>
<td>147.135.0.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary DNS:</td>
<td>147.135.8.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN IP Address:</td>
<td>172.16.0.1</td>
<td>Broadcast Pkt:</td>
<td>2</td>
</tr>
<tr>
<td>Broadcast Bytes Sent:</td>
<td>684</td>
<td>Broadcast Pkt: Rev:</td>
<td>169298</td>
</tr>
<tr>
<td>Broadcast Bytes Recv:</td>
<td>10197078</td>
<td>Broadcast Pkt: Dropped:</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast Bytes Dropped:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Even UMich is vulnerable...

r00ted

MOROCCO SECURITY RULZ

by PRI[ll]
intitle:"TANDBERG" "This page requires a frame capable browser!" site:umich.edu
To be installed

- mars.umd.umich.edu
- backup.its.umd.umich.edu
- vega.umd.umich.edu
- compassion.its.umd.umich.edu
- spica.its.umd.umich.edu
Remote Desktop Web Connection

Select the name of the remote computer you want to use, select the screen size for your connection, and then click Connect.

Download the 'Simplify Printing' remote print client installer here.
Usage Statistics for www.pscs.umich.edu - September 2002 - Mozilla Firefox

Daily usage for September 2002

- intext:"webalizer"
- intext:"Total Usernames"
- intext:"Usage Statistics for"
### Directory of Thai Student Association
**The University of Michigan at Ann Arbor**
**2004-2005**

<table>
<thead>
<tr>
<th>Nickname</th>
<th>Name</th>
<th>Phone Number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Supat</td>
<td></td>
<td><a href="mailto:Supatsssss@hotmail.com">Supatsssss@hotmail.com</a></td>
</tr>
<tr>
<td>Aak</td>
<td>Charuwan</td>
<td></td>
<td><a href="mailto:ckritpra@umich.edu">ckritpra@umich.edu</a></td>
</tr>
<tr>
<td>Add</td>
<td>Saravut</td>
<td></td>
<td><a href="mailto:dda@hotmail.com">dda@hotmail.com</a>, <a href="mailto:ddaarch@umich.edu">ddaarch@umich.edu</a></td>
</tr>
<tr>
<td>Air</td>
<td>Vorakalya</td>
<td></td>
<td><a href="mailto:vchcvich@umich.edu">vchcvich@umich.edu</a></td>
</tr>
<tr>
<td>Amy</td>
<td>Amy</td>
<td></td>
<td><a href="mailto:akule@umich.edu">akule@umich.edu</a></td>
</tr>
<tr>
<td>Ang</td>
<td>Angkana</td>
<td></td>
<td><a href="mailto:angnaka@umich.edu">angnaka@umich.edu</a></td>
</tr>
<tr>
<td>Ann</td>
<td>Piyarat</td>
<td></td>
<td><a href="mailto:pwattana@umich.edu">pwattana@umich.edu</a></td>
</tr>
<tr>
<td>Arm</td>
<td>Sasawat</td>
<td></td>
<td><a href="mailto:sassawat@umich.edu">sassawat@umich.edu</a></td>
</tr>
<tr>
<td>Art</td>
<td>Thanopun</td>
<td></td>
<td><a href="mailto:thanopun@umich.edu">thanopun@umich.edu</a></td>
</tr>
<tr>
<td>Aun</td>
<td>Nonglak</td>
<td></td>
<td><a href="mailto:nonglakm@umich.edu">nonglakm@umich.edu</a></td>
</tr>
<tr>
<td>Aye</td>
<td>Rujinart</td>
<td></td>
<td><a href="mailto:rujinart@umich.edu">rujinart@umich.edu</a></td>
</tr>
<tr>
<td>Bee</td>
<td>Benita</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belle</td>
<td>Wanwasiri</td>
<td></td>
<td><a href="mailto:bellewan@umich.edu">bellewan@umich.edu</a></td>
</tr>
<tr>
<td>Ben</td>
<td>Benjamin</td>
<td></td>
<td><a href="mailto:bpjackson@umich.edu">bpjackson@umich.edu</a></td>
</tr>
<tr>
<td>Ble</td>
<td>Thanasak</td>
<td></td>
<td><a href="mailto:twongtan3@umich.edu">twongtan3@umich.edu</a></td>
</tr>
<tr>
<td>Bow</td>
<td>Sirimon</td>
<td></td>
<td><a href="mailto:sirimon0@umich.edu">sirimon0@umich.edu</a></td>
</tr>
<tr>
<td>Cee</td>
<td>Ittrichot</td>
<td></td>
<td><a href="mailto:idomin20@engin.umich.edu">idomin20@engin.umich.edu</a></td>
</tr>
</tbody>
</table>
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.

Log in

Forgotten your password? Click here to have it mailed to you.
intitle:intranet inurl:intranet +intext:"human resources"
inurl:"exchange/logon.asp" OR intitle:"Microsoft Outlook Web Access - Logon"
My personal favorite…
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

mailman:umich.edu is the admin user with the password goblue.

--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
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.