You found that on Google?

Gaining awareness about “Google Hackers”

Johnny Long
johnny@ihackstuff.com

HUGE DISCLAIMER!

- The print/CD version of this presentation is much smaller than the live version!

- The live version shows ***many more*** techniques and examples. After all, I can't leave a paper trail… =^P
- **DEFCON ATTENDEES**: This print version is the same as the Blackhat talk, but the live version is very different! I'm too lazy to make 2 print versions ;-)

What this is about

- We’ll be talking about how hackers can use Google to locate vulnerable targets and sensitive information
- This process has been termed “Google hacking”
- We will be blowing through the basics
  - After all, this is DEFCON! =)

Advanced Operators

- Google advanced operators help refine searches
- Advanced operators use a syntax such as the following:
  - operator:search_term
- Notice that there's no space between the operator, the colon, and the search term

Advanced Operators

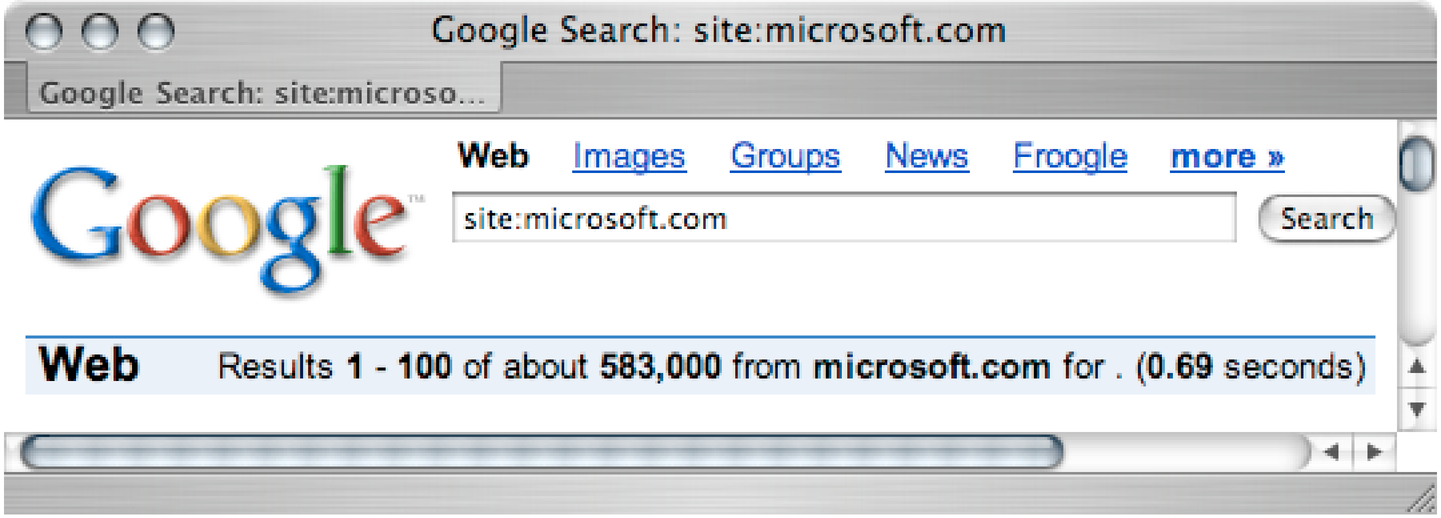
- site: restrict a search to a specific web site or domain
  - The web site to search must be supplied after the colon.
- filetype: search only within the text of a particular type of file
- link: search within hyperlinks
- cache: displays the version of a web page as it appeared when Google crawled the site
- intitle: search for a term in the title of a document
- inurl: search only within the URL (web address) of a document

Search Characters

- Some characters:
    - (+) force inclusion of a search term
    - (-) exclude a search term
    - (“) use quotes around search phrases
    - (.) a single-character wildcard
    - (*) any word

Site Crawling

- To find every web page Google has crawled for a specific site, use the site: operator


Google Search: site:microsoft.com
Google Search: site:microso...
Google
Web
Images
Groups
News
Froogle
more »
Search
Web

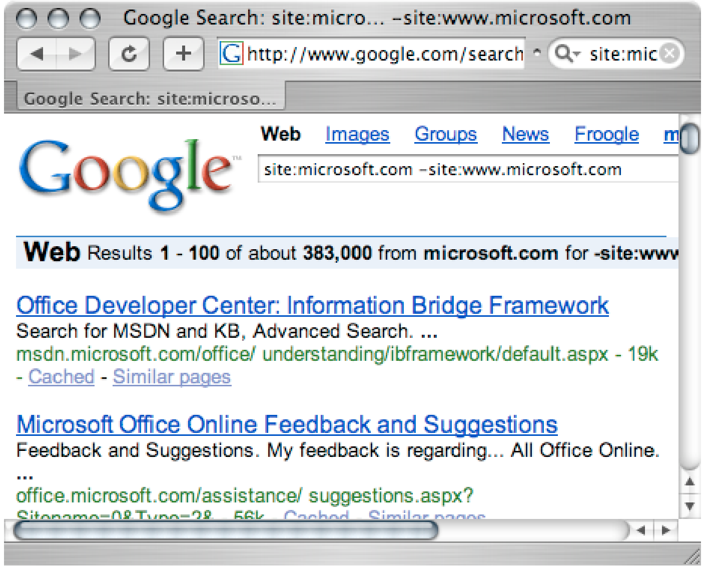
site:microsoft.com

Results **1** - **100** of about **583,000** from **microsoft.com** for . (**0.69** seconds)

site: microsoft.com

Server Crawling

- To locate additional servers, subtract common hostnames from the query


Google Search: site:micro... –site:www.microsoft.com
http://www.google.com/search
site:mic
Google Search: site:microso...
Google
Web
Images
Groups
News
Froogle
m

site:microsoft.com –site:www.microsoft.com

Web Results **1** - **100** of about **383,000** from **microsoft.com** for **-site:www**

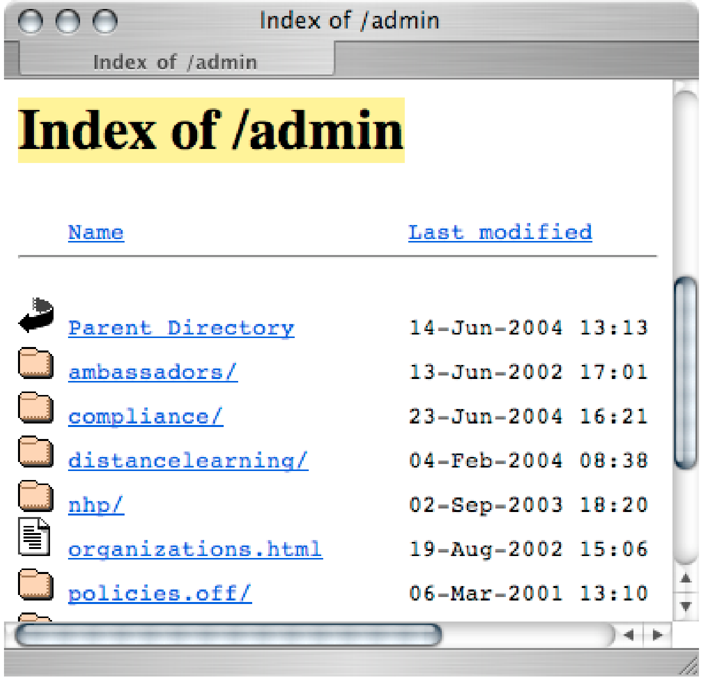
Office Developer Center: Information Bridge Framework
Search for MSDN and KB, Advanced Search. ...
msdn.microsoft.com/office/ understanding/ibframework/default.aspx - 19k - Cached - Similar pages

Microsoft Office Online Feedback and Suggestions
Feedback and Suggestions. My feedback is regarding... All Office Online. ...
office.microsoft.com/assistance/ suggestions.aspx?
Sitename=0&Type=2& - 56k - Cached - Similar pages

site: microsoft.com
-site:www.microsoft.com

Directory Listings

- Directory listings can be a source of great information



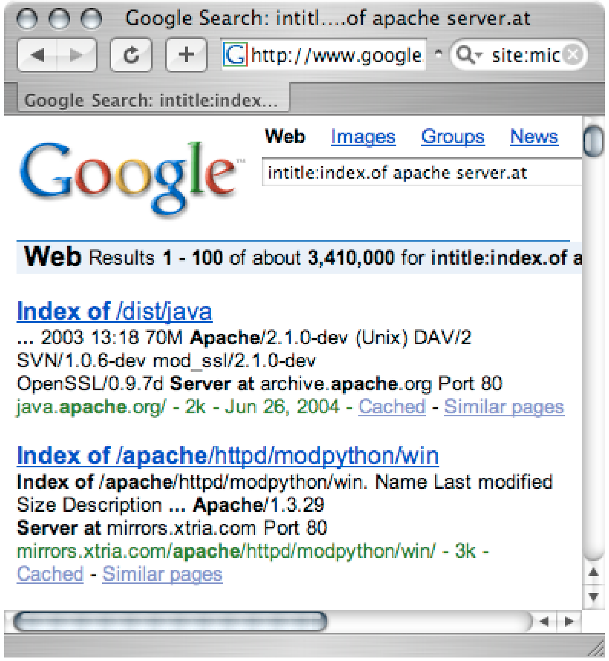
Index of /admin

```
     Name                             Last modified

     Parent Directory                 14-Jun-2004 13:13
     ambassadors/                     13-Jun-2002 17:01
     compliance/                      23-Jun-2004 16:21
     distancelearning/                04-Feb-2004 08:38
     nhp/                             02-Sep-2003 18:20
     organizations.html               19-Aug-2002 15:06
     policies.off/                    06-Mar-2001 13:10
```

intitle:index.of/admin

Directory Listings

- Directory listings can provide server version information


Google Search: intitl....of apache server.at
http://www.google
site:mic
Google Search: intitle:index...
Google
Web
Images
Groups
News
intitle:index.of apache server.at

Web Results **1** - **100** of about **3,410,000** for **intitle:index.of a**

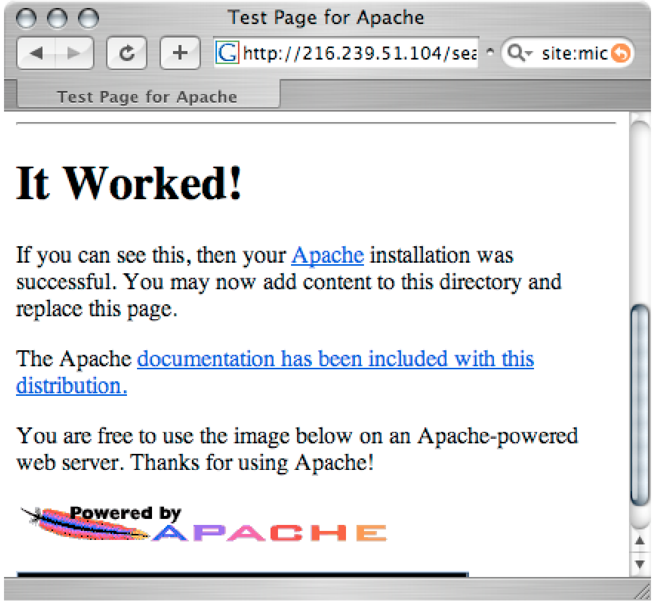
Index of /dist/java
... 2003 13:18 70M **Apache**/2.1.0-dev (Unix) DAV/2 SVN/1.0.6-dev mod_ssl/2.1.0-dev OpenSSL/0.9.7d **Server at** archive.**apache**.org Port 80
java.**apache**.org/ - 2k - Jun 26, 2004 - Cached - Similar pages

Index of /**apache**/httpd/modpython/win
Index of /**apache**/httpd/modpython/win. Name Last modified Size Description **... Apache**/1.3.29 **Server at** mirrors.xtria.com Port 80
mirrors.xtria.com/**apache**/httpd/modpython/win/ - 3k - Cached - Similar pages

intitle:index.of apache server.at

Default Server Pages

- Web servers with default pages can serve as juicy targets



It Worked!

If you can see this, then your Apache installation was successful. You may now add content to this directory and replace this page.

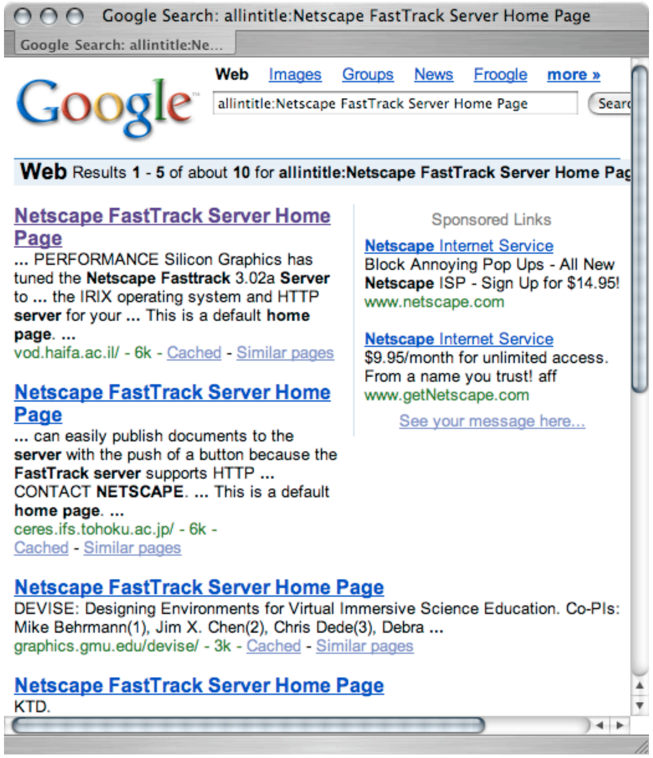
The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

intitle:test.page.for.apache “it worked”

Default Server Pages

- Web servers with default pages can serve as juicy targets


Google Search: allintitle:Netscape FastTrack Server Home Page
Google Search: allintitle:Ne...
Web
Images
Groups
News
Froogle
more »
allintitle:Netscape FastTrack Server Home Page
Searc

Web Results **1** - **5** of about **10** for **allintitle:Netscape FastTrack Server Home Pag**

Netscape FastTrack Server Home Page
... PERFORMANCE Silicon Graphics has tuned the **Netscape Fasttrack** 3.02a **Server** to ... the IRIX operating system and HTTP **server** for your ... This is a default **home page**. ...
vod.haifa.ac.il/ - 6k - Cached - Similar pages

Netscape FastTrack Server Home Page
... can easily publish documents to the **server** with the push of a button because the **FastTrack server** supports HTTP ... CONTACT **NETSCAPE**. ... This is a default **home page**. ...
ceres.ifs.tohoku.ac.jp/ - 6k - Cached - Similar pages

Netscape FastTrack Server Home Page
DEVISE: Designing Environments for Virtual Immersive Science Education. Co-PIs: Mike Behrmann(1), Jim X. Chen(2), Chris Dede(3), Debra ...
graphics.gmu.edu/devise/ - 3k - Cached - Similar pages

Netscape FastTrack Server Home Page
KTD.

Sponsored Links

Netscape Internet Service
Block Annoying Pop Ups - All New **Netscape** ISP - Sign Up for $14.95!
www.netscape.com

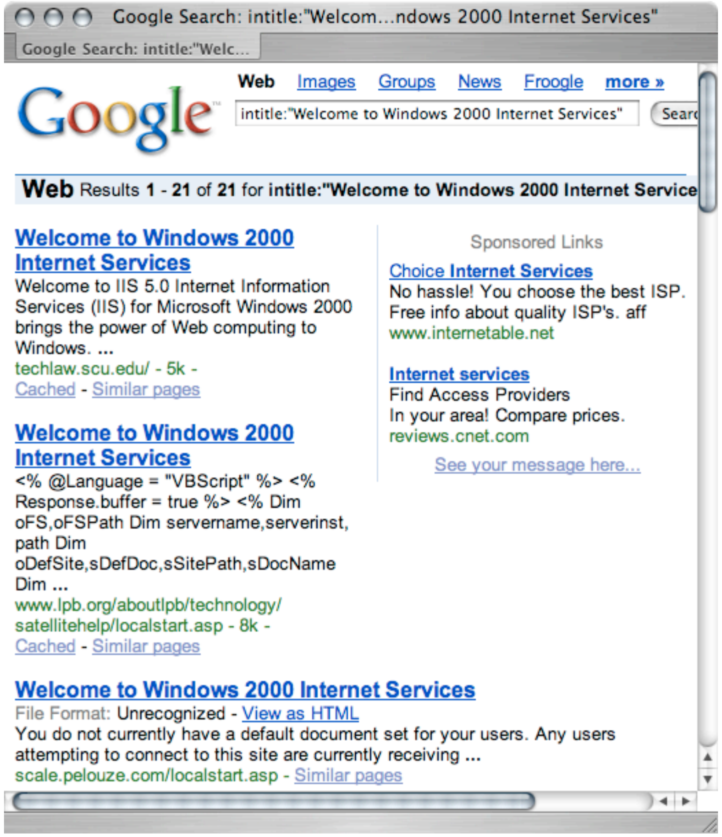
Netscape Internet Service
$9.95/month for unlimited access. From a name you trust! aff
www.getNetscape.com

See your message here...

allintitle:Netscape FastTrack Server Home Page

Default Server Pages

- Web servers with default pages can serve as juicy targets


Google Search: intitle:"Welcom...ndows 2000 Internet Services"
Google Search: intitle:"Welc...
Google
Web
Images
Groups
News
Froogle
more »
intitle:"Welcome to Windows 2000 Internet Services"
Searc

Web Results **1** - **21** of **21** for **intitle:"Welcome to Windows 2000 Internet Service**

Welcome to Windows 2000 Internet Services
Welcome to IIS 5.0 Internet Information Services (IIS) for Microsoft Windows 2000 brings the power of Web computing to Windows. ...
techlaw.scu.edu/ - 5k -
Cached - Similar pages

Welcome to Windows 2000 Internet Services
<% @Language = "VBScript" %> <% Response.buffer = true %> <% Dim oFS,oFSPath Dim servername,serverinst, path Dim oDefSite,sDefDoc,sSitePath,sDocName Dim ...
www.lpb.org/aboutlpb/technology/satellitehelp/localstart.asp - 8k -
Cached - Similar pages

Welcome to Windows 2000 Internet Services
File Format: Unrecognized - View as HTML
You do not currently have a default document set for your users. Any users attempting to connect to this site are currently receiving ...
scale.pelouze.com/localstart.asp - Similar pages

Sponsored Links

Choice Internet Services
No hassle! You choose the best ISP. Free info about quality ISP's. aff
www.internetable.net

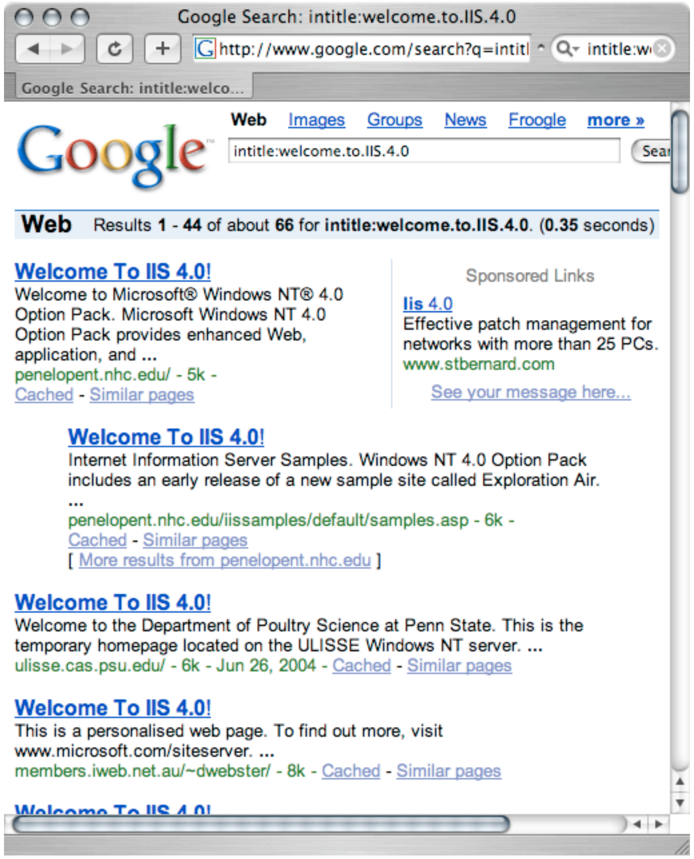
Internet services
Find Access Providers
In your area! Compare prices.
reviews.cnet.com

See your message here...

intitle:"Welcome to Windows 2000 Internet Services"

Default Server Pages

- Web servers with default pages can serve as juicy targets


Google Search: intitle:welcome.to.IIS.4.0
http://www.google.com/search?q=intitl
intitle:w
Google Search: intitle:welco...
Google
Web
Images
Groups
News
Froogle
more »
intitle:welcome.to.IIS.4.0
Sear

Web Results **1** - **44** of about **66** for **intitle:welcome.to.IIS.4.0**. (**0.35** seconds)

Welcome To IIS 4.0!
Welcome to Microsoft® Windows NT® 4.0 Option Pack. Microsoft Windows NT 4.0 Option Pack provides enhanced Web, application, and ...
penelopent.nhc.edu/ - 5k -
Cached - Similar pages

Sponsored Links

Iis 4.0
Effective patch management for networks with more than 25 PCs.
www.stbernard.com

See your message here...

Welcome To IIS 4.0!
Internet Information Server Samples. Windows NT 4.0 Option Pack includes an early release of a new sample site called Exploration Air. ...
penelopent.nhc.edu/iissamples/default/samples.asp - 6k -
Cached - Similar pages
[More results from penelopent.nhc.edu]

Welcome To IIS 4.0!
Welcome to the Department of Poultry Science at Penn State. This is the temporary homepage located on the ULISSE Windows NT server. ...
ulisse.cas.psu.edu/ - 6k - Jun 26, 2004 - Cached - Similar pages

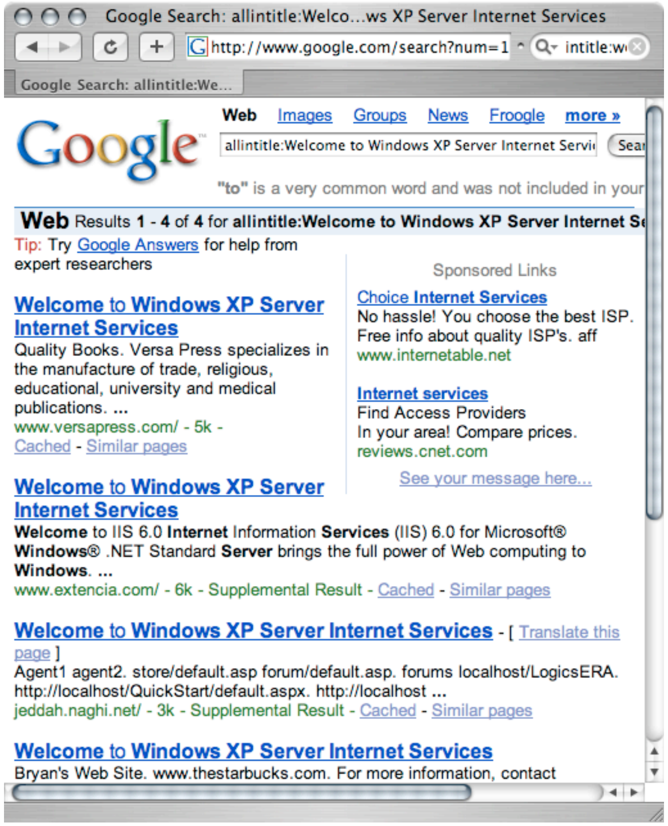
Welcome To IIS 4.0!
This is a personalised web page. To find out more, visit www.microsoft.com/siteserver. ...
members.iweb.net.au/~dwebster/ - 8k - Cached - Similar pages

Welcome To IIS 4.0!

intitle:welcome.to.IIS.4.0

Default Server Pages

- Web servers with default pages can serve as juicy targets


Google Search: allintitle:Welco...ws XP Server Internet Services
http://www.google.com/search?num=1
intitle:w
Google Search: allintitle:We...
Google
Web Images Groups News Froogle more »
allintitle:Welcome to Windows XP Server Internet Servi
Sear

"to" is a very common word and was not included in your

Web Results **1** - **4** of **4** for **allintitle:Welcome to Windows XP Server Internet S**

Tip: Try Google Answers for help from expert researchers

Welcome to Windows XP Server Internet Services
Quality Books. Versa Press specializes in the manufacture of trade, religious, educational, university and medical publications. ...
www.versapress.com/ - 5k - Cached - Similar pages

Welcome to Windows XP Server Internet Services
Welcome to IIS 6.0 **Internet** Information **Services** (IIS) 6.0 for Microsoft® **Windows**® .NET Standard **Server** brings the full power of Web computing to **Windows**. ...
www.extencia.com/ - 6k - Supplemental Result - Cached - Similar pages

Welcome to Windows XP Server Internet Services - [Translate this page]
Agent1 agent2. store/default.asp forum/default.asp. forums localhost/LogicsERA. http://localhost/QuickStart/default.aspx. http://localhost ...
jeddah.naghi.net/ - 3k - Supplemental Result - Cached - Similar pages

Welcome to Windows XP Server Internet Services
Bryan's Web Site. www.thestarbucks.com. For more information, contact

Sponsored Links

Choice Internet Services
No hassle! You choose the best ISP. Free info about quality ISP's. aff
www.internetable.net

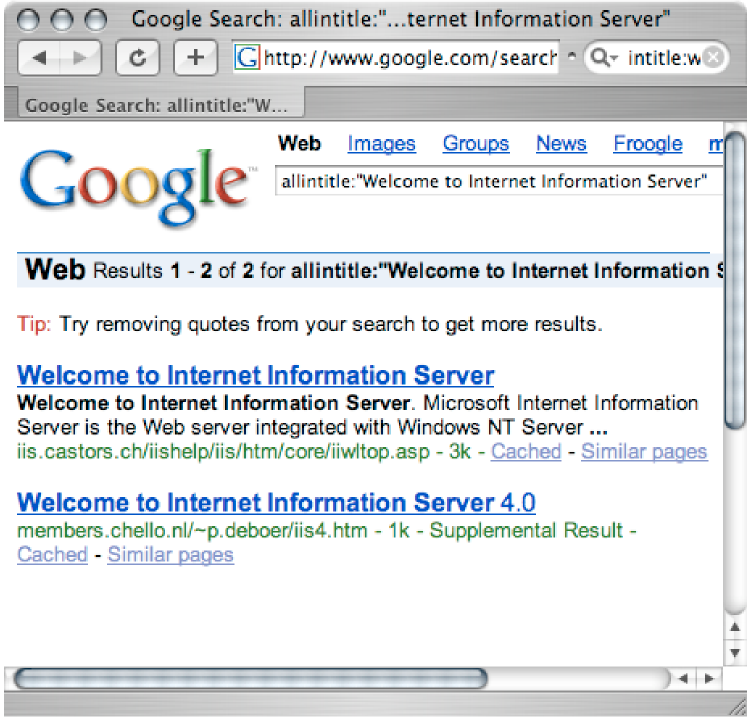
Internet services
Find Access Providers
In your area! Compare prices.
reviews.cnet.com

See your message here...

allintitle:Welcome to Windows XP Server Internet Services

Default Server Pages

- Web servers with default pages can serve as juicy targets


Google Search: allintitle:"...ternet Information Server"
http://www.google.com/search
intitle:w
Google Search: allintitle:"W...
Google
Web
Images
Groups
News
Froogle

allintitle:"Welcome to Internet Information Server"

Web Results **1** - **2** of **2** for **allintitle:"Welcome to Internet Information S**

Tip: Try removing quotes from your search to get more results.

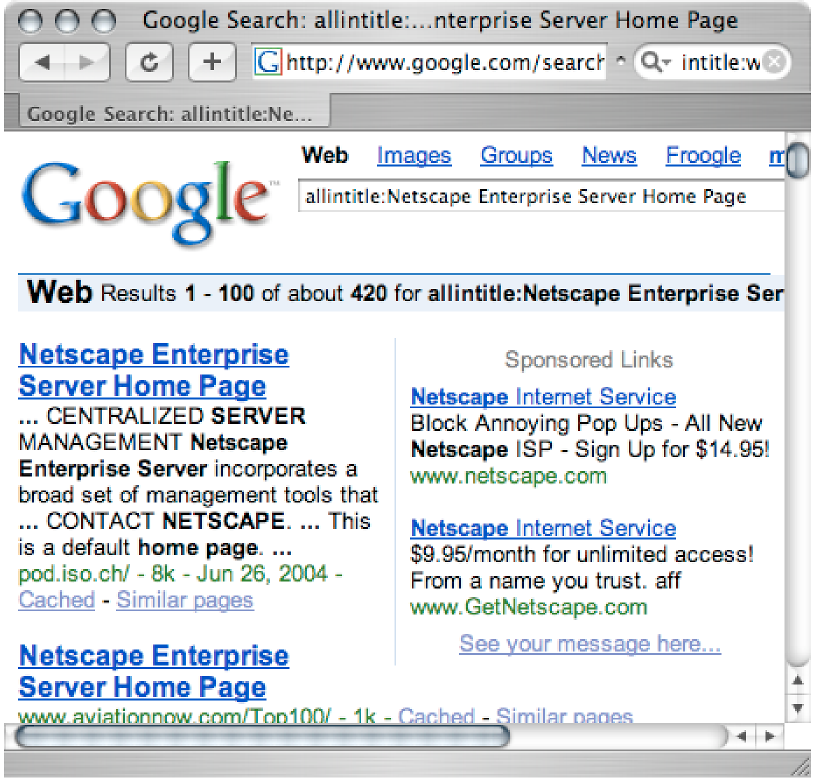
Welcome to Internet Information Server
Welcome to Internet Information Server. Microsoft Internet Information Server is the Web server integrated with Windows NT Server **...**
iis.castors.ch/iishelp/iis/htm/core/iiwltop.asp - 3k - Cached - Similar pages

Welcome to Internet Information Server 4.0
members.chello.nl/~p.deboer/iis4.htm - 1k - Supplemental Result - Cached - Similar pages

allintitle:"Welcome to Internet Information Server"

Default Server Pages

- Web servers with default pages can serve as juicy targets


Google Search: allintitle:...nterprise Server Home Page
http://www.google.com/search
intitle:w
Google Search: allintitle:Ne...
Google
Web
Images
Groups
News
Froogle
m

allintitle:Netscape Enterprise Server Home Page

Web Results **1** - **100** of about **420** for **allintitle:Netscape Enterprise Ser**

Netscape Enterprise Server Home Page
... CENTRALIZED **SERVER** MANAGEMENT **Netscape Enterprise Server** incorporates a broad set of management tools that ... CONTACT **NETSCAPE**. ... This is a default **home page**. ...
pod.iso.ch/ - 8k - Jun 26, 2004 - Cached - Similar pages

Netscape Enterprise Server Home Page
www.aviationnow.com/Top100/ - 1k - Cached - Similar pages

Sponsored Links

Netscape Internet Service
Block Annoying Pop Ups - All New **Netscape** ISP - Sign Up for $14.95!
www.netscape.com

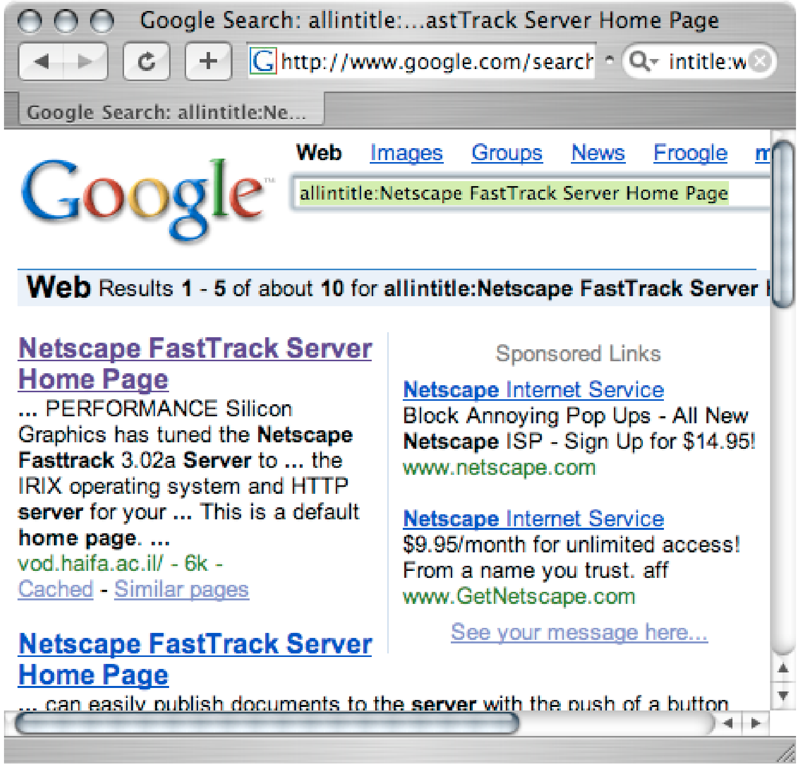
Netscape Internet Service
$9.95/month for unlimited access! From a name you trust. aff
www.GetNetscape.com

See your message here...

allintitle:Netscape Enterprise Server Home Page

Default Server Pages

- Web servers with default pages can serve as juicy targets


Google Search: allintitle:...astTrack Server Home Page
http://www.google.com/search
intitle:w
Google Search: allintitle:Ne...
Web
Images
Groups
News
Froogle
Google

allintitle:Netscape FastTrack Server Home Page

Web Results **1** - **5** of about **10** for **allintitle:Netscape FastTrack Server**

Netscape FastTrack Server Home Page
... PERFORMANCE Silicon Graphics has tuned the **Netscape Fasttrack** 3.02a **Server** to ... the IRIX operating system and HTTP **server** for your ... This is a default **home page**. ...
vod.haifa.ac.il/ - 6k -
Cached - Similar pages

Netscape FastTrack Server Home Page
... can easily publish documents to the **server** with the push of a button

Sponsored Links

Netscape Internet Service
Block Annoying Pop Ups - All New **Netscape** ISP - Sign Up for $14.95!
www.netscape.com

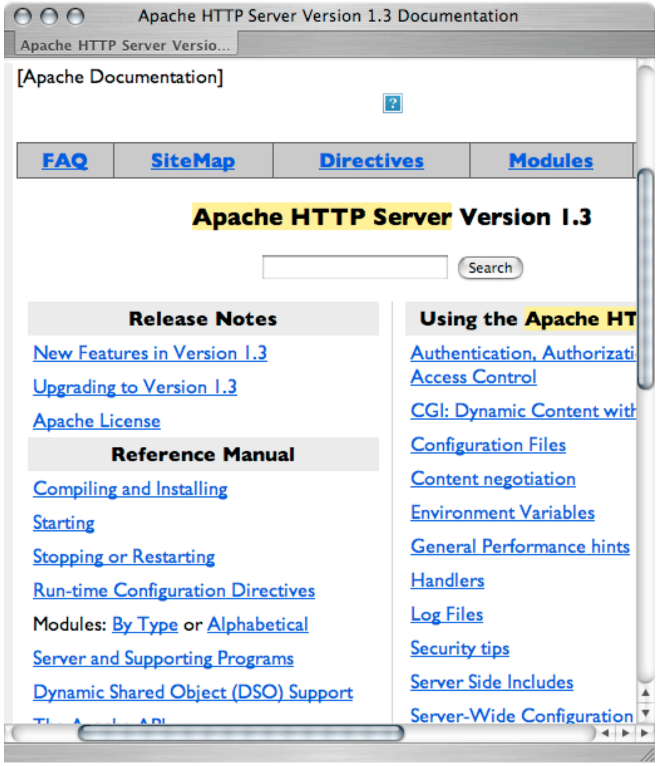
Netscape Internet Service
$9.95/month for unlimited access! From a name you trust. aff
www.GetNetscape.com

See your message here...

allintitle:Netscape FASTTRACK Server Home Page

Default Documents

- Servers can also be profiled via default manuals and documentation


Apache HTTP Server Version 1.3 Documentation
Apache HTTP Server Versio...
Search

[Apache Documentation]

FAQ	SiteMap	Directives	Modules

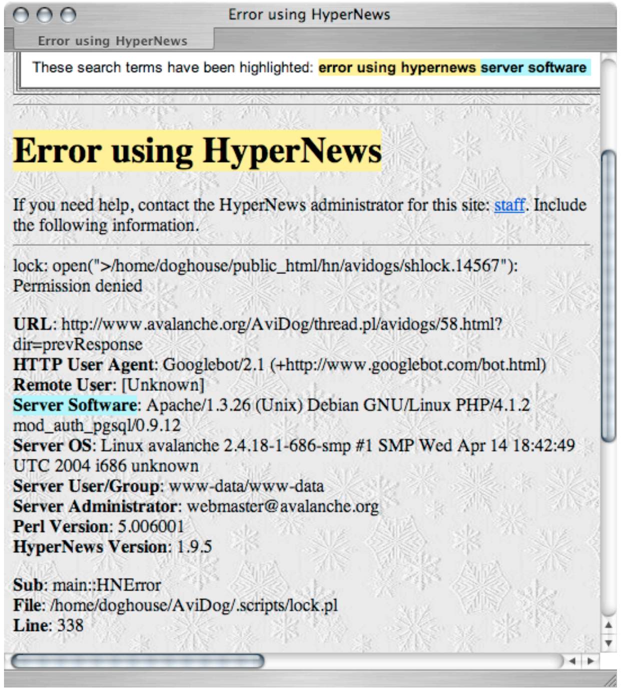
Apache HTTP Server Version 1.3

Release Notes	Using the Apache HT
New Features in Version 1.3	Authentication, Authorizati Access Control
Upgrading to Version 1.3	CGI: Dynamic Content wit
Apache License	Configuration Files
Reference Manual	Content negotiation
Compiling and Installing	Environment Variables
Starting	General Performance hints
Stopping or Restarting	Handlers
Run-time Configuration Directives	Log Files
Modules: By Type or Alphabetical	Security tips
Server and Supporting Programs	Server Side Includes
Dynamic Shared Object (DSO) Support	Server-Wide Configuration

intitle:"Apache HTTP Server" intitle:"documentation"

Error Messages

- Server profiling is easy with some error messages



These search terms have been highlighted: **error using hypernews server software**

Error using HyperNews

If you need help, contact the HyperNews administrator for this site: staff. Include the following information.

lock: open(">/home/doghouse/public_html/hn/avidogs/shlock.14567"): Permission denied

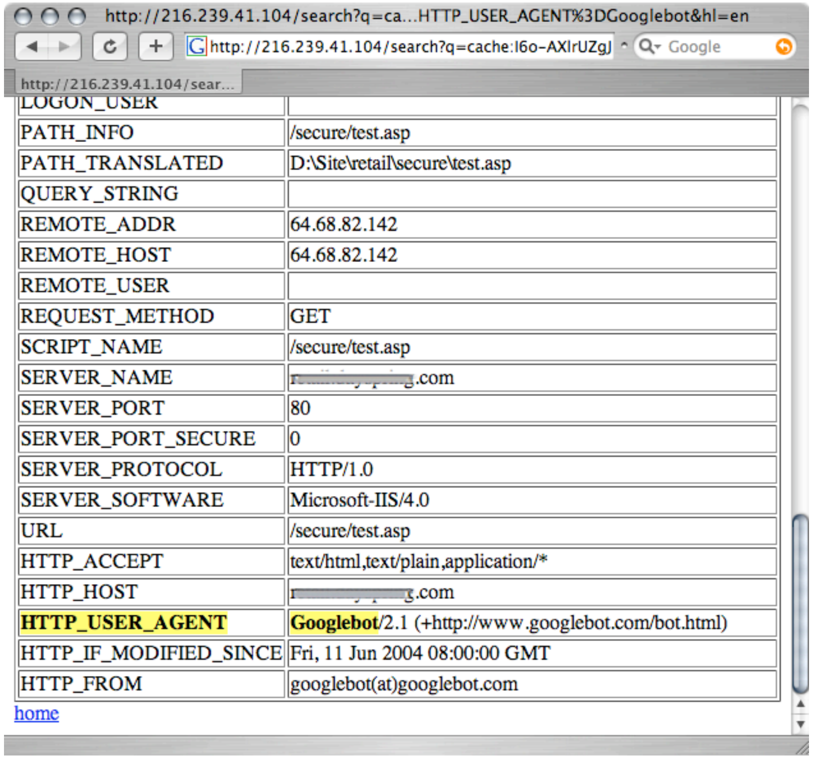
URL: http://www.avalanche.org/AviDog/thread.pl/avidogs/58.html?dir=prevResponse
HTTP User Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Remote User: [Unknown]
Server Software: Apache/1.3.26 (Unix) Debian GNU/Linux PHP/4.1.2 mod_auth_pgsql/0.9.12
Server OS: Linux avalanche 2.4.18-1-686-smp #1 SMP Wed Apr 14 18:42:49 UTC 2004 i686 unknown
Server User/Group: www-data/www-data
Server Administrator: webmaster@avalanche.org
Perl Version: 5.006001
HyperNews Version: 1.9.5

Sub: main::HNError
File: /home/doghouse/AviDog/.scripts/lock.pl
Line: 338

intitle:"Error using Hypernews" "Server Software"

Error Messages

- CGI environment vars provide a great deal of information
- The generic way to find these pages is by focusing on the trail left by the googlebot crawler



http://216.239.41.104/search?q=ca...HTTP_USER_AGENT%3DGooglebot&hl=en

http://216.239.41.104/search?q=cache:I6o-AXIrUZgJ

http://216.239.41.104/sear...

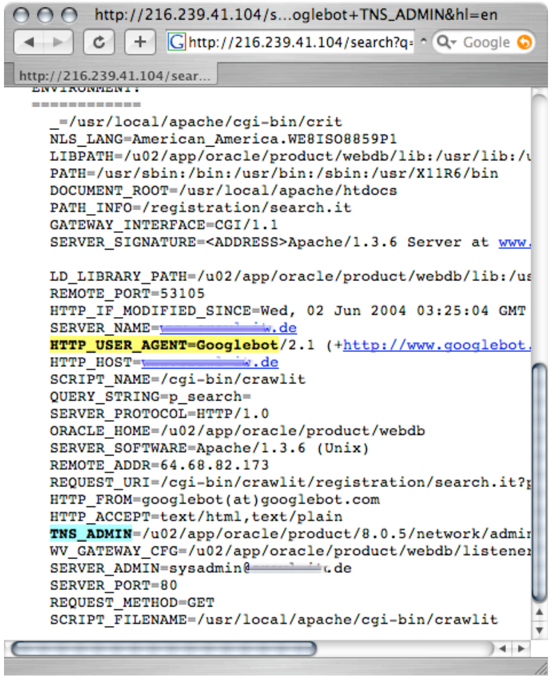
LOGON_USER	
PATH_INFO	/secure/test.asp
PATH_TRANSLATED	D:\Site\retail\secure\test.asp
QUERY_STRING	
REMOTE_ADDR	64.68.82.142
REMOTE_HOST	64.68.82.142
REMOTE_USER	
REQUEST_METHOD	GET
SCRIPT_NAME	/secure/test.asp
SERVER_NAME	[redacted].com
SERVER_PORT	80
SERVER_PORT_SECURE	0
SERVER_PROTOCOL	HTTP/1.0
SERVER_SOFTWARE	Microsoft-IIS/4.0
URL	/secure/test.asp
HTTP_ACCEPT	text/html,text/plain,application/*
HTTP_HOST	[redacted].com
HTTP_USER_AGENT	**Googlebot**/2.1 (+http://www.googlebot.com/bot.html)
HTTP_IF_MODIFIED_SINCE	Fri, 11 Jun 2004 08:00:00 GMT
HTTP_FROM	googlebot(at)googlebot.com

home

“HTTP_USER_AGENT=Googlebot”

Error Messages

- after a generic search, we can narrow down to the fields we find more interesting


http://216.239.41.104/s...oglebot+TNS_ADMIN&hl=en
http://216.239.41.104/search?q=
Google
http://216.239.41.104/sear...

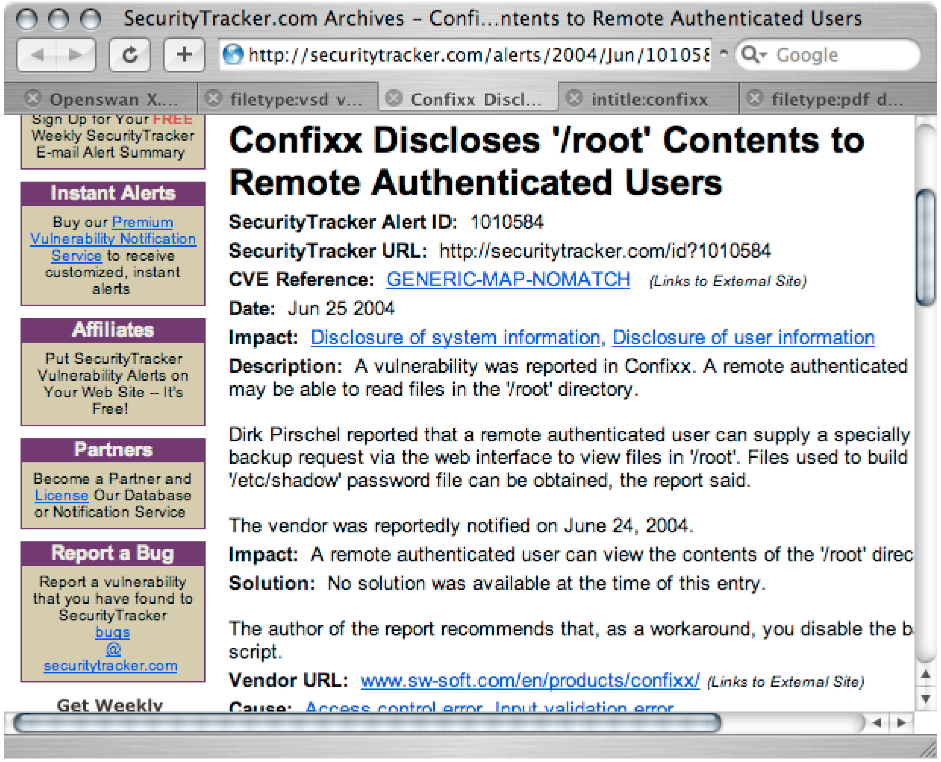
```
ENVIRONMENT:
============
  _=/usr/local/apache/cgi-bin/crit
  NLS_LANG=American_America.WE8ISO8859P1
  LIBPATH=/u02/app/oracle/product/webdb/lib:/usr/lib:/u
  PATH=/usr/sbin:/bin:/usr/bin:/sbin:/usr/X11R6/bin
  DOCUMENT_ROOT=/usr/local/apache/htdocs
  PATH_INFO=/registration/search.it
  GATEWAY_INTERFACE=CGI/1.1
  SERVER_SIGNATURE=<ADDRESS>Apache/1.3.6 Server at www.

  LD_LIBRARY_PATH=/u02/app/oracle/product/webdb/lib:/us
  REMOTE_PORT=53105
  HTTP_IF_MODIFIED_SINCE=Wed, 02 Jun 2004 03:25:04 GMT
  SERVER_NAME=[redacted]w.de
  HTTP_USER_AGENT=Googlebot/2.1 (+http://www.googlebot.
  HTTP_HOST=[redacted]w.de
  SCRIPT_NAME=/cgi-bin/crawlit
  QUERY_STRING=p_search=
  SERVER_PROTOCOL=HTTP/1.0
  ORACLE_HOME=/u02/app/oracle/product/webdb
  SERVER_SOFTWARE=Apache/1.3.6 (Unix)
  REMOTE_ADDR=64.68.82.173
  REQUEST_URI=/cgi-bin/crawlit/registration/search.it?p
  HTTP_FROM=googlebot(at)googlebot.com
  HTTP_ACCEPT=text/html,text/plain
  TNS_ADMIN=/u02/app/oracle/product/8.0.5/network/admin
  WV_GATEWAY_CFG=/u02/app/oracle/product/webdb/listener
  SERVER_ADMIN=sysadmin@[redacted].de
  SERVER_PORT=80
  REQUEST_METHOD=GET
  SCRIPT_FILENAME=/usr/local/apache/cgi-bin/crawlit
```

“HTTP_USER_AGENT=Googlebot”
TNS_ADMIN

Vulnerability Trolling

- Many attackers find vulnerable targets via Google

- A typical security advisory may look like this:


SecurityTracker.com Archives – Confi…ntents to Remote Authenticated Users
http://securitytracker.com/alerts/2004/Jun/10105
Google
Openswan X…
filetype:vsd v…
Confixx Discl…
intitle:confixx
filetype:pdf d…

Sign Up for Your FREE Weekly SecurityTracker E-mail Alert Summary

Instant Alerts

Buy our Premium Vulnerability Notification Service to receive customized, instant alerts

Affiliates

Put SecurityTracker Vulnerability Alerts on Your Web Site -- It's Free!

Partners

Become a Partner and License Our Database or Notification Service

Report a Bug

Report a vulnerability that you have found to SecurityTracker bugs @ securitytracker.com

Get Weekly

Confixx Discloses '/root' Contents to Remote Authenticated Users

SecurityTracker Alert ID: 1010584

SecurityTracker URL: http://securitytracker.com/id?1010584

CVE Reference: GENERIC-MAP-NOMATCH *(Links to External Site)*

Date: Jun 25 2004

Impact: Disclosure of system information, Disclosure of user information

Description: A vulnerability was reported in Confixx. A remote authenticated may be able to read files in the '/root' directory.

Dirk Pirschel reported that a remote authenticated user can supply a specially backup request via the web interface to view files in '/root'. Files used to build '/etc/shadow' password file can be obtained, the report said.

The vendor was reportedly notified on June 24, 2004.

Impact: A remote authenticated user can view the contents of the '/root' direc

Solution: No solution was available at the time of this entry.

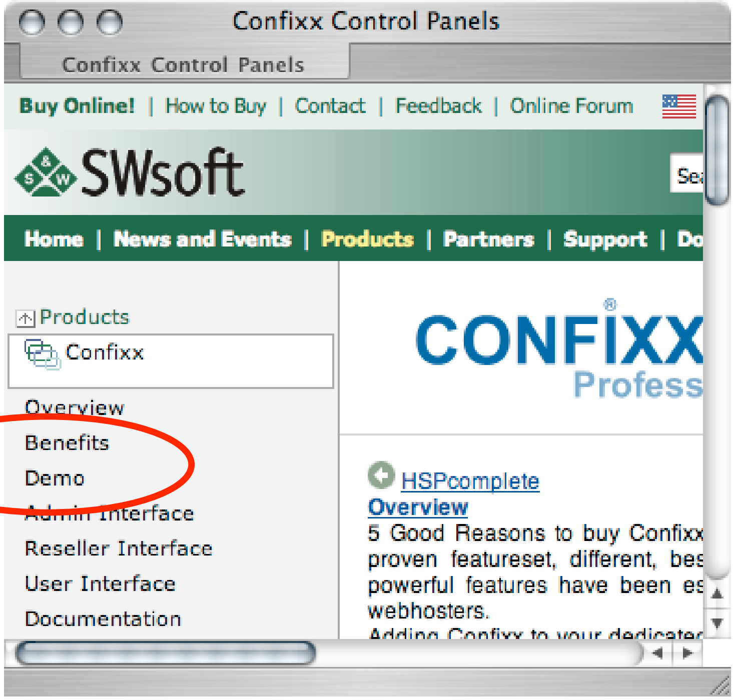
The author of the report recommends that, as a workaround, you disable the b script.

Vendor URL: www.sw-soft.com/en/products/confixx/ *(Links to External Site)*

Cause: Access control error, Input validation error

Vulnerability Trolling

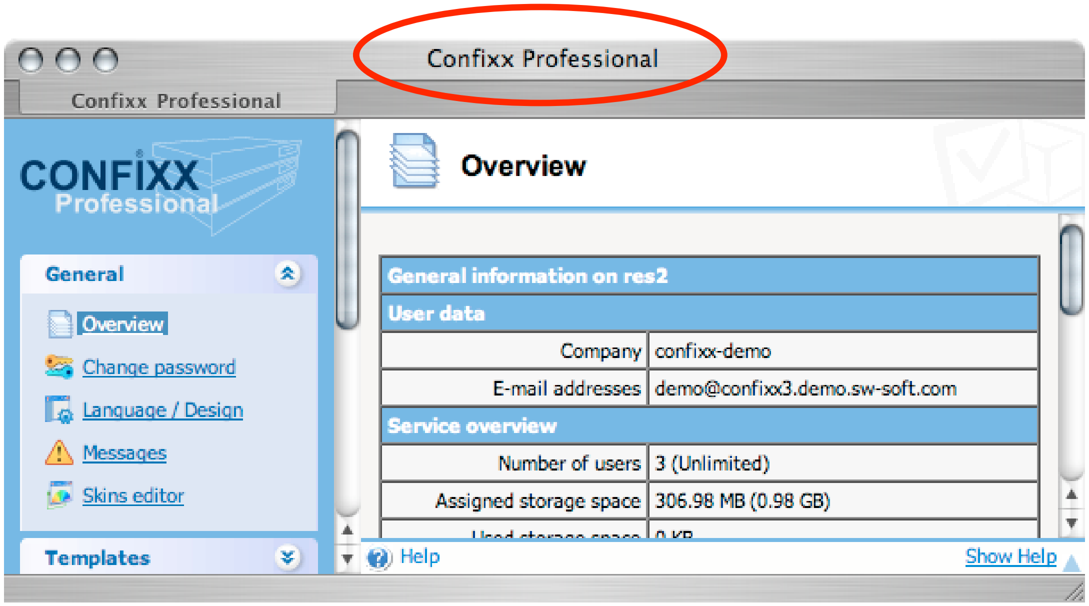
- A quick browse of the vendor's website reveals a demo of the product



5 Good Reasons to buy Confixx proven featureset, different, bes powerful features have been es webhosters.
Adding Confixx to your dedicated

Vulnerability Trolling

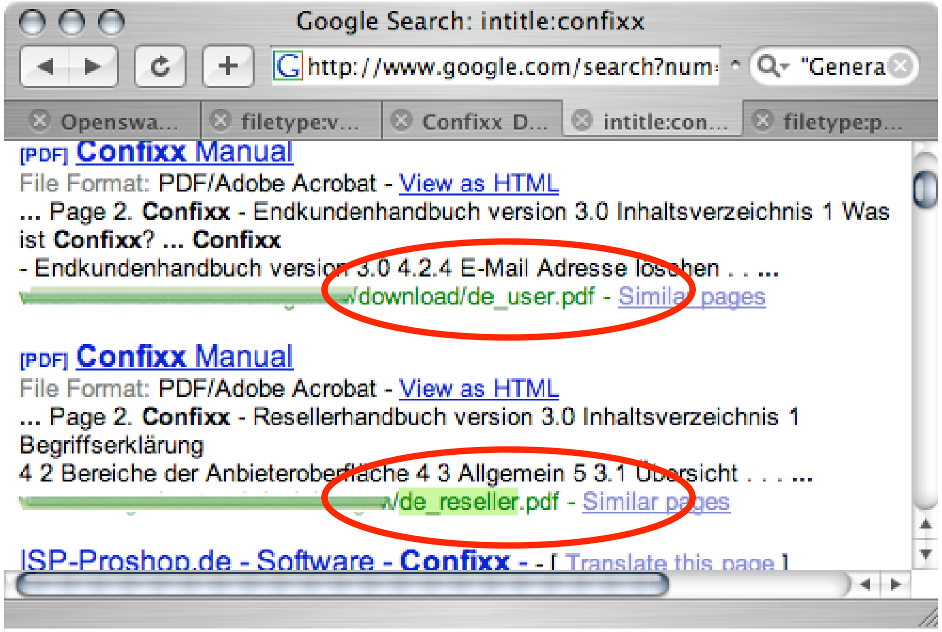
- The demo page suggests one method for finding targets



General information on res2	
User data	
Company	confixx-demo
E-mail addresses	demo@confixx3.demo.sw-soft.com
Service overview	
Number of users	3 (Unlimited)
Assigned storage space	306.98 MB (0.98 GB)
Used storage space	0 KB

Vulnerability Trolling

- A quick intitle: search suggests more vectors…


Google Search: intitle:confixx
http://www.google.com/search?num=
"Genera
Openswa…
filetype:v…
Confixx D…
intitle:con…
filetype:p…

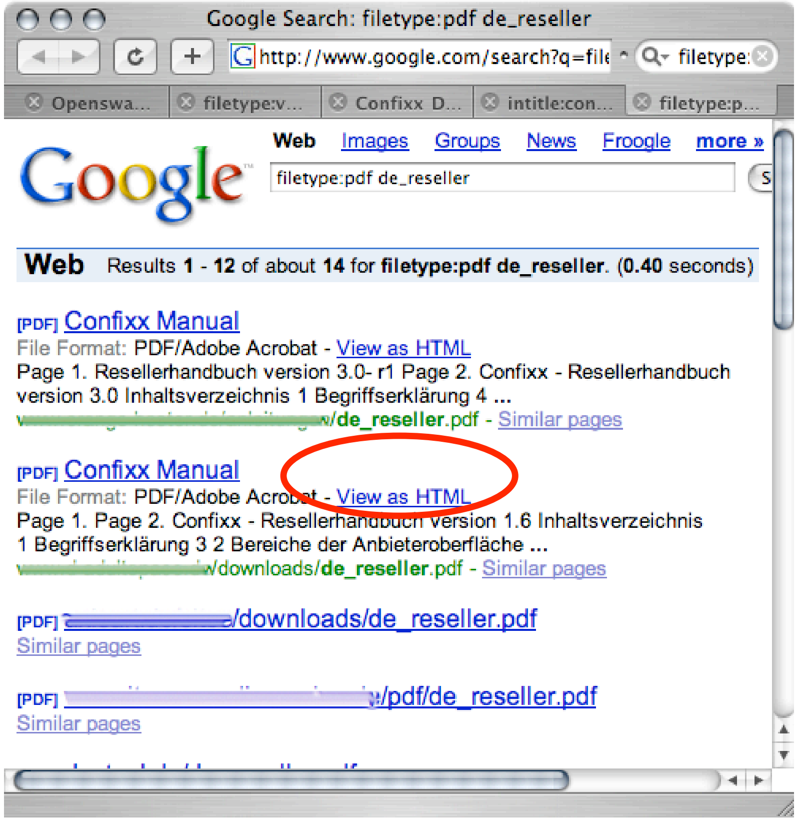
[PDF] **Confixx** Manual
File Format: PDF/Adobe Acrobat - View as HTML
... Page 2. **Confixx** - Endkundenhandbuch version 3.0 Inhaltsverzeichnis 1 Was ist **Confixx**? ... **Confixx** - Endkundenhandbuch version 3.0 4.2.4 E-Mail Adresse loschen . . . ...
[redacted]/download/de_user.pdf - Similar pages

[PDF] **Confixx** Manual
File Format: PDF/Adobe Acrobat - View as HTML
... Page 2. **Confixx** - Resellerhandbuch version 3.0 Inhaltsverzeichnis 1 Begriffserklärung
4 2 Bereiche der Anbieteroberfläche 4 3 Allgemein 5 3.1 Übersicht . . . ...
[redacted]/de_reseller.pdf - Similar pages

ISP-Proshop.de - Software - **Confixx** - - [Translate this page]

Vulnerability Trolling

- This search finds the documentation included with the product
- These sites are probably poorly configured



Web Results **1** - **12** of about **14** for **filetype:pdf de_reseller**. (**0.40** seconds)

[PDF] Confixx Manual
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. Resellerhandbuch version 3.0- r1 Page 2. Confixx - Resellerhandbuch version 3.0 Inhaltsverzeichnis 1 Begriffserklärung 4 ...
[redacted]/**de_reseller**.pdf - Similar pages

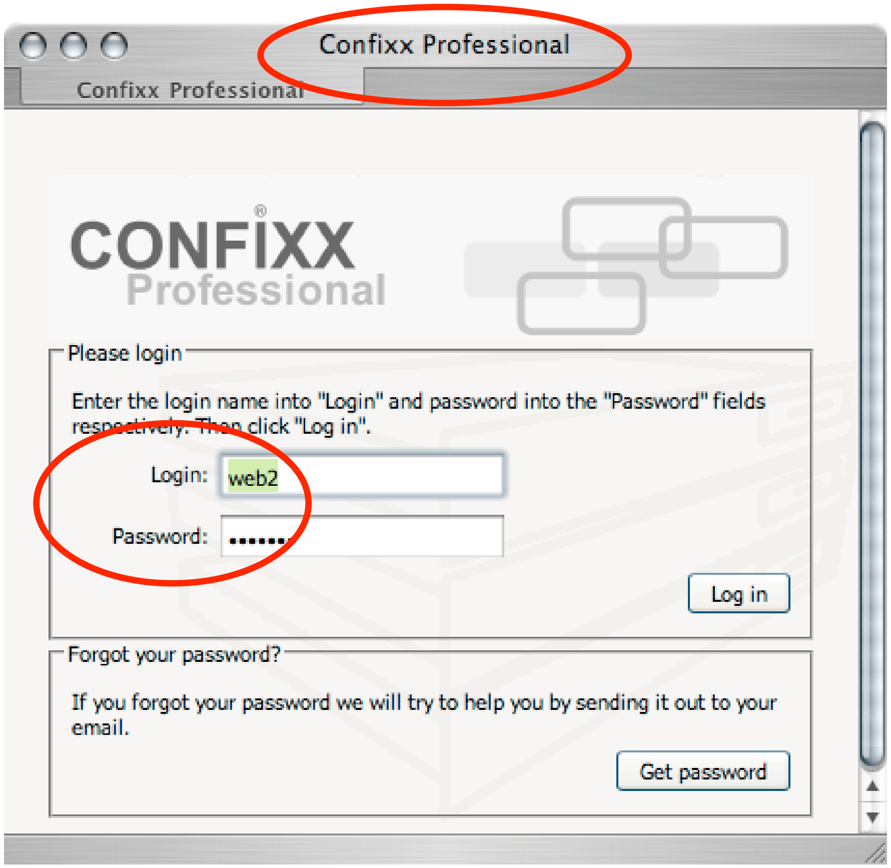
[PDF] Confixx Manual
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. Page 2. Confixx - Resellerhandbuch version 1.6 Inhaltsverzeichnis 1 Begriffserklärung 3 2 Bereiche der Anbieteroberfläche ...
[redacted]/downloads/**de_reseller**.pdf - Similar pages

[PDF] [redacted]/downloads/de_reseller.pdf
Similar pages

[PDF] [redacted]/pdf/de_reseller.pdf
Similar pages

Vulnerability Trolling

- Other searches are easy to discover as well…



Please login

Enter the login name into "Login" and password into the "Password" fields respectively. Then click "Log in".

Login: web2

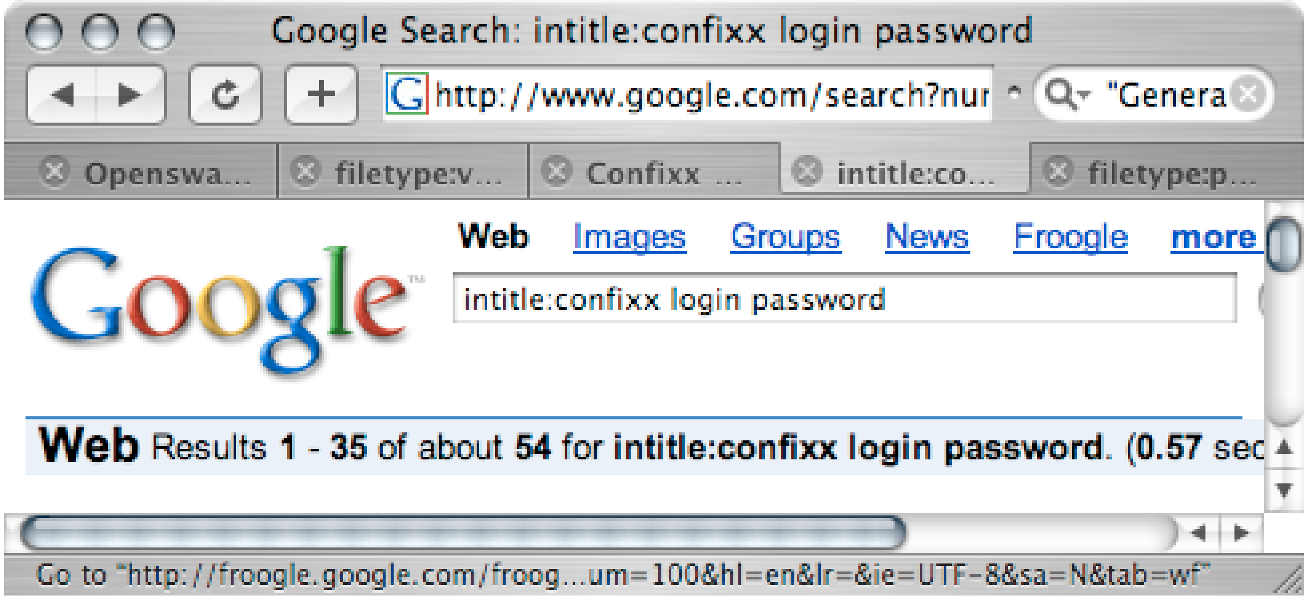
Password: •••••••

Forgot your password?

If you forgot your password we will try to help you by sending it out to your email.

Vulnerability Trolling

- Other searches are easy to discover as well…



Google Search: intitle:confixx login password

http://www.google.com/search?nur

"Genera

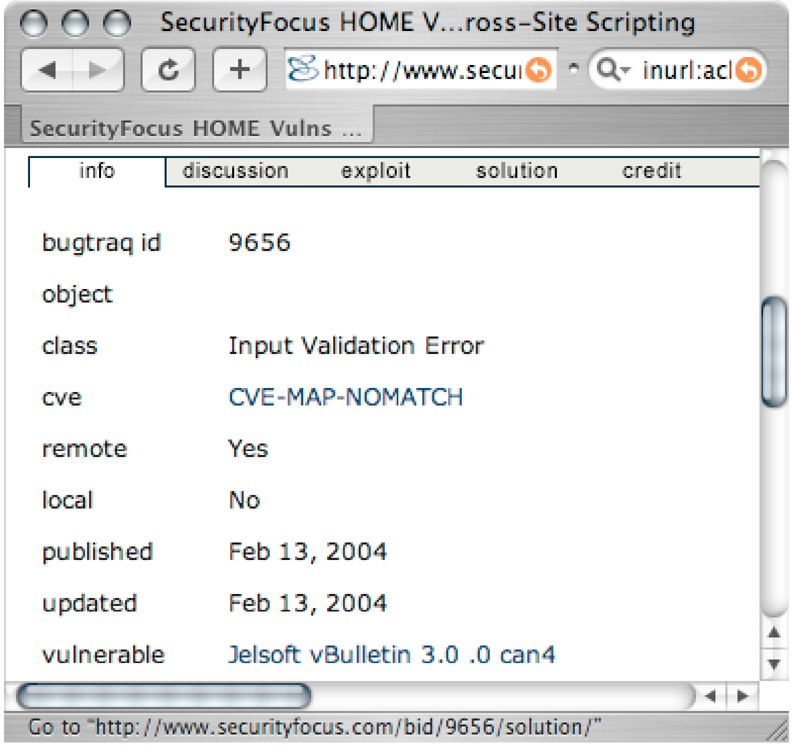
intitle:confixx login password

Web Results **1** - **35** of about **54** for **intitle:confixx login password**. (**0.57** sec

Go to "http://froogle.google.com/froog...um=100&hl=en&lr=&ie=UTF-8&sa=N&tab=wf"

Vulnerability Trolling

- Many times, a good search string is much simpler to come up with
- Consider this advisory:

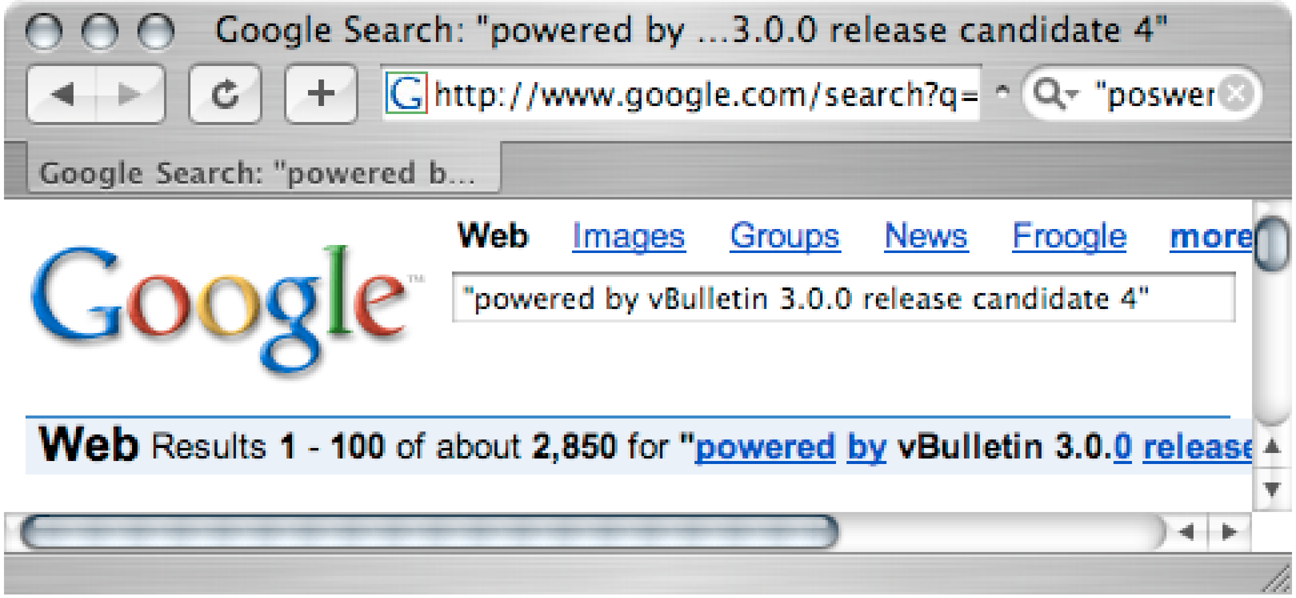

SecurityFocus HOME V...ross-Site Scripting
http://www.secu
inurl:acl
SecurityFocus HOME Vulns ...
info
discussion
exploit
solution
credit

bugtraq id	9656
object	
class	Input Validation Error
cve	CVE-MAP-NOMATCH
remote	Yes
local	No
published	Feb 13, 2004
updated	Feb 13, 2004
vulnerable	Jelsoft vBulletin 3.0 .0 can4

Go to "http://www.securityfocus.com/bid/9656/solution/"

Vulnerability Trolling

- A creative search finds vulnerable targets



Google Search: "powered by ...3.0.0 release candidate 4"

http://www.google.com/search?q=

"poswer

Google Search: "powered b...

"powered by vBulletin 3.0.0 release candidate 4"

Web Results 1 - 100 of about 2,850 for "powered by vBulletin 3.0.0 release

CGI Scanning

- In order to locate web vulnerabilities on a larger scale, many attacker will use a ‘CGI’ scanner
- Most scanners read a data file and query target web servers looking for the vulnerable files

CGI Scanning

- A CGI scanner’s vulnerability file…

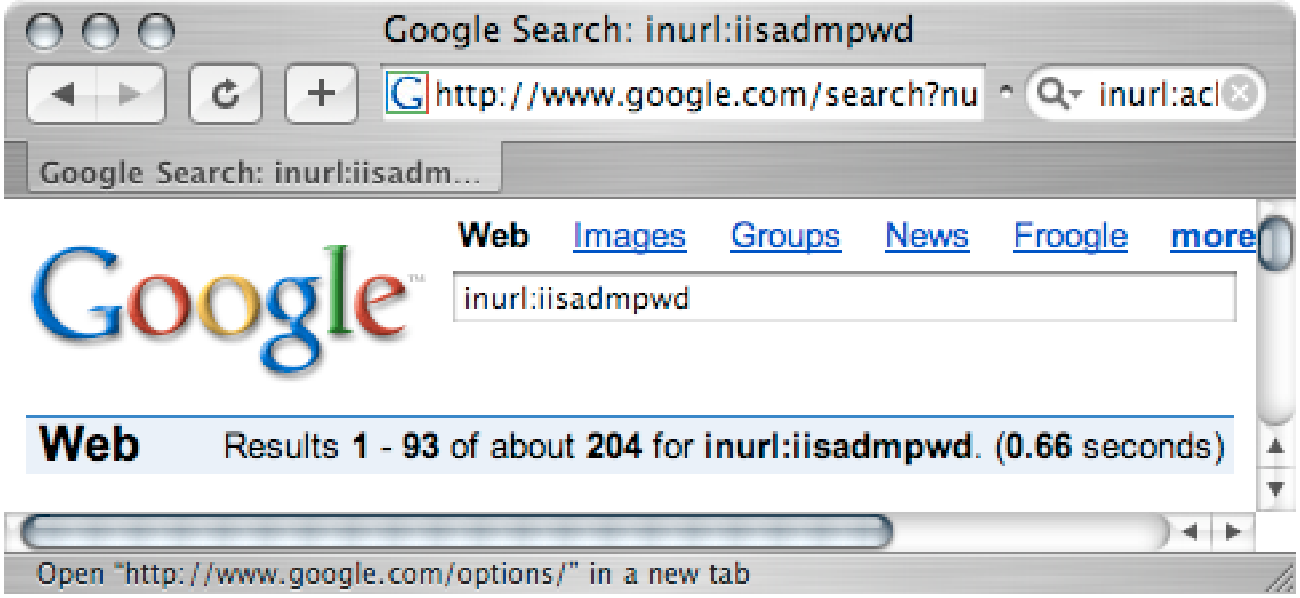
```
/iisadmpwd/
/iisadmpwd/achg.htr
/iisadmpwd/aexp.htr
/iisadmpwd/aexp2.htr
/iisadmpwd/aexp2b.htr
```

- can be converted to Google queries in a number of different ways:

```
inurl;/iisadmpwd/
inurl;/iisadmpwd/achg.htr
inurl;/iisadmpwd/aexp.htr
inurl;/iisadmpwd/aexp2.htr
inurl;/iisadmpwd/aexp2b.htr
```

Vulnerability Trolling

- Regardless of the age of the vulerability, there are usually vulnerable targets



Google Search: inurl:iisadmpwd

http://www.google.com/search?nu

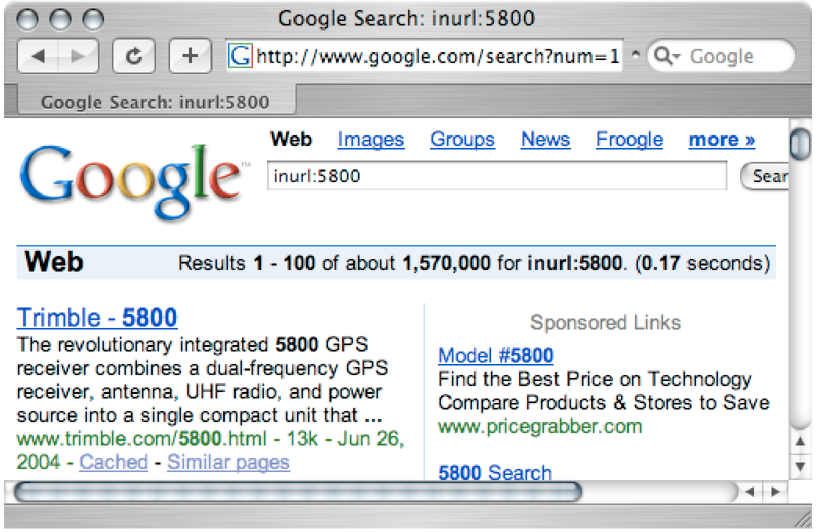
inurl:iisadmpwd

Web Results 1 - 93 of about 204 for inurl:iisadmpwd. (0.66 seconds)

Open "http://www.google.com/options/" in a new tab

Port Scanning

- Although port numbers are sometimes found in the url, there's no easy way to scan just for a port number… the results are much too copious


Google Search: inurl:5800
http://www.google.com/search?num=1
Google
Google Search: inurl:5800
Google
Web
Images
Groups
News
Froogle
more »
inurl:5800
Sear

Web Results **1** - **100** of about **1,570,000** for **inurl:5800**. (**0.17** seconds)

Trimble - **5800**
The revolutionary integrated **5800** GPS receiver combines a dual-frequency GPS receiver, antenna, UHF radio, and power source into a single compact unit that ...
www.trimble.com/**5800**.html - 13k - Jun 26, 2004 - Cached - Similar pages

Sponsored Links

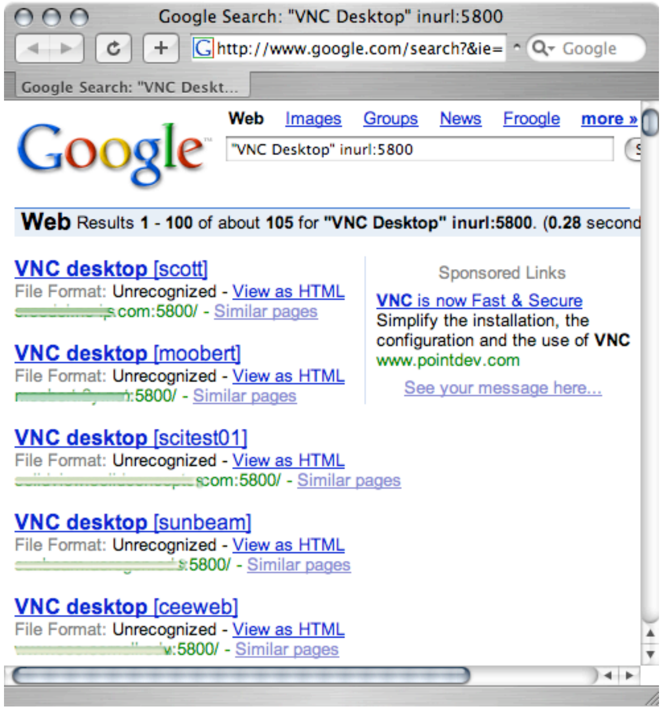
Model **#5800**
Find the Best Price on Technology Compare Products & Stores to Save
www.pricegrabber.com

5800 Search

inurl:5800

Port Scanning

- We can use creative queries to sniff out services that may be listening on particular ports
- VNC Desktop, port 5800


Google Search: "VNC Desktop" inurl:5800
http://www.google.com/search?&ie=
Google
Google Search: "VNC Deskt...
Web
Images
Groups
News
Froogle
more »
"VNC Desktop" inurl:5800

Web Results **1** - **100** of about **105** for **"VNC Desktop" inurl:5800**. (**0.28** second

VNC desktop [scott]
File Format: Unrecognized - View as HTML
[redacted]s.com:5800/ - Similar pages

VNC desktop [moobert]
File Format: Unrecognized - View as HTML
[redacted]:5800/ - Similar pages

VNC desktop [scitest01]
File Format: Unrecognized - View as HTML
[redacted]com:5800/ - Similar pages

VNC desktop [sunbeam]
File Format: Unrecognized - View as HTML
[redacted]:5800/ - Similar pages

VNC desktop [ceeweb]
File Format: Unrecognized - View as HTML
[redacted]v:5800/ - Similar pages

Sponsored Links

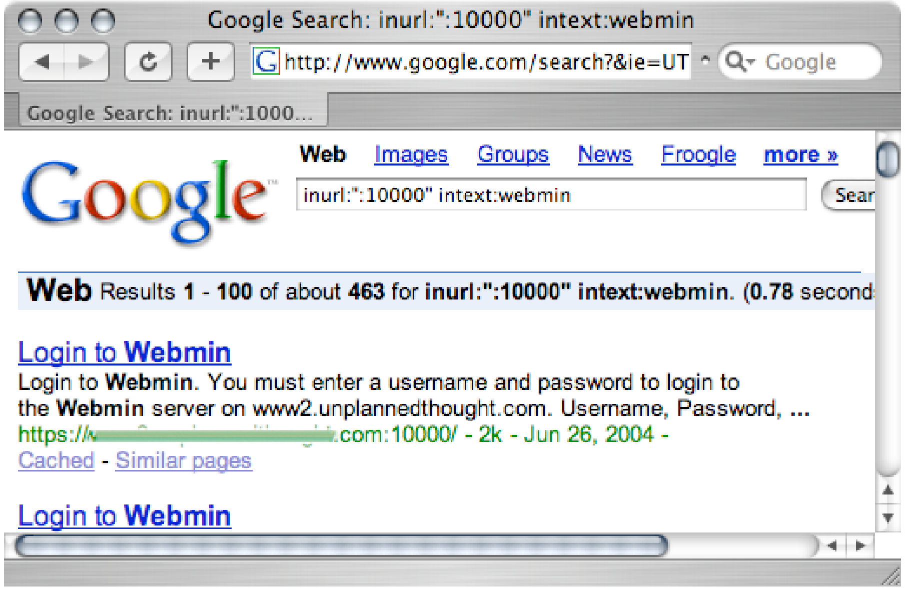
VNC is now Fast & Secure
Simplify the installation, the configuration and the use of **VNC**
www.pointdev.com

See your message here...

"VNC Desktop" inurl:5800

Port Scanning

- Webmin, port 10000


Google Search: inurl:":10000" intext:webmin
http://www.google.com/search?&ie=UT
Google
Google Search: inurl:":1000...
Web
Images
Groups
News
Froogle
more »
inurl:":10000" intext:webmin
Sear

Web Results **1** - **100** of about **463** for **inurl:":10000" intext:webmin**. (**0.78** second

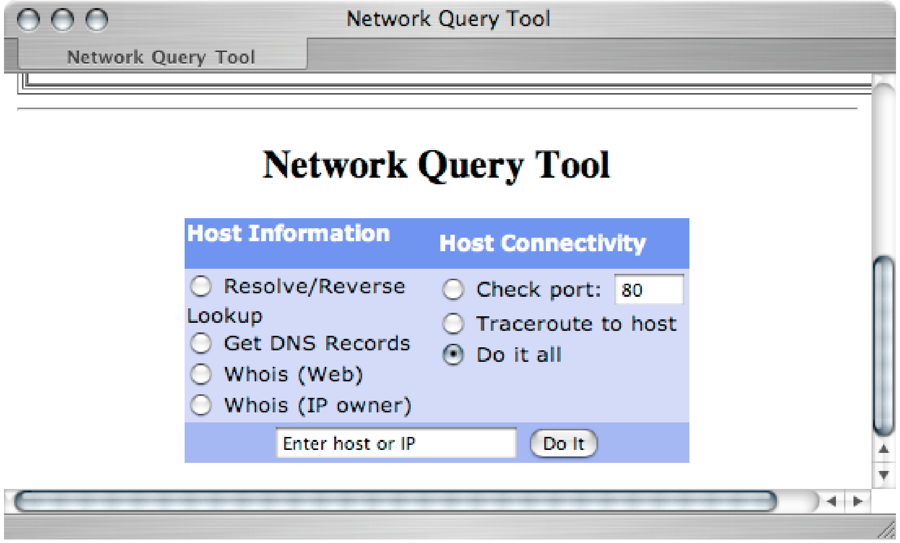
[Login to **Webmin**](#)
Login to **Webmin**. You must enter a username and password to login to the **Webmin** server on www2.unplannedthought.com. Username, Password, **...**
https://[redacted].com:10000/ - 2k - Jun 26, 2004 -
[Cached](#) - [Similar pages](#)

[Login to **Webmin**](#)

inurl:webmin inurl:10000

Port Scanning

- Google can be used to find sites to do the portscanning for you
- Consider the Network Query Tool

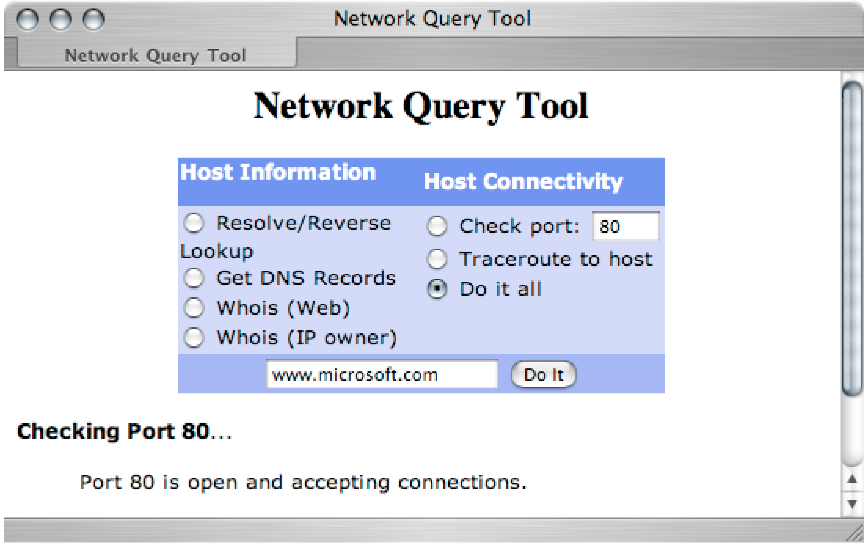


Network Query Tool

Host Information	Host Connectivity
○ Resolve/Reverse Lookup	○ Check port: 80
○ Get DNS Records	○ Traceroute to host
○ Whois (Web)	● Do it all
○ Whois (IP owner)	

Port Scanning

- NQT allows web users to perform traceroutes, rdns lookups and port scans.
- This is the NQT program checking port 80 on www.microsoft.com:



Network Query Tool

Host Information

○ Resolve/Reverse Lookup
○ Get DNS Records
○ Whois (Web)
○ Whois (IP owner)

Host Connectivity

○ Check port: 80
○ Traceroute to host
● Do it all

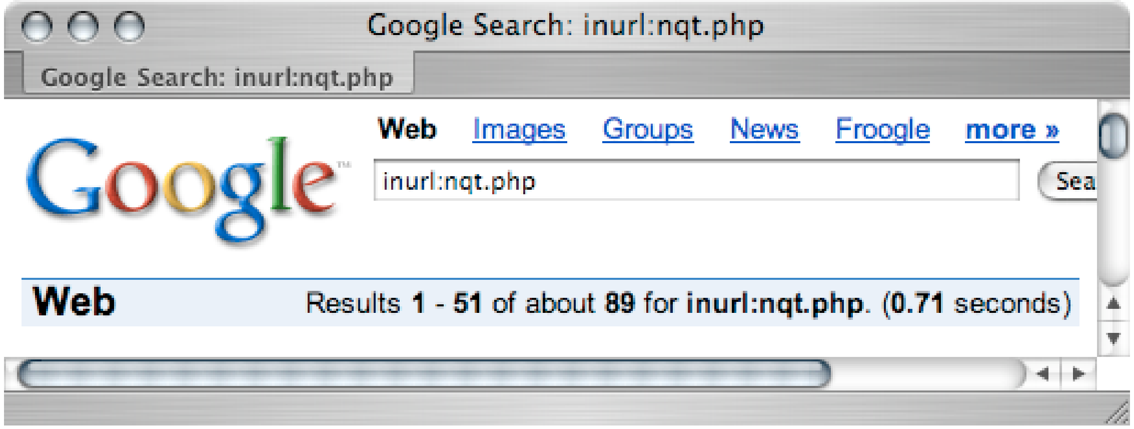
www.microsoft.com

Checking Port 80...

Port 80 is open and accepting connections.

Port Scanning

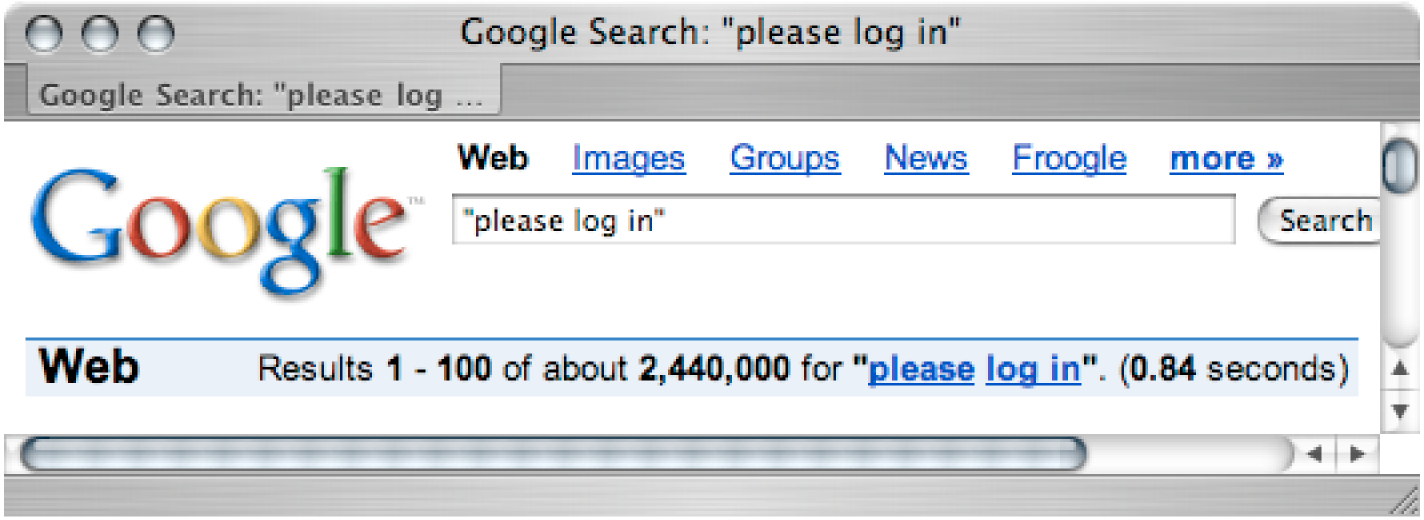
- Google can be used to locate servers running the NQT program, nqt.php
- Once servers are harvested, they can be used to perform port scans (usually through a web proxy)
- NQT also allows remote posts, so that more than one port can be checked at a time



Results **1** - **51** of about **89** for **inurl:nqt.php**. (**0.71** seconds)

Login Portals

- The most generic of login portals

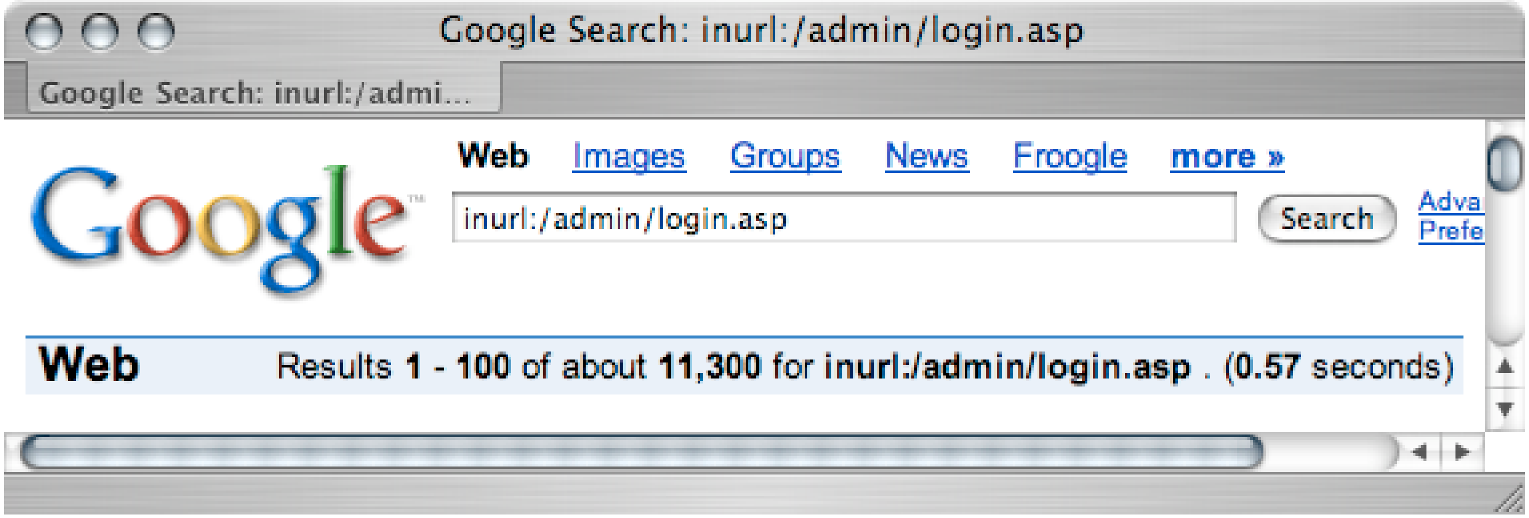

Google Search: "please log in"
Google Search: "please log ...
Google
Web
Images
Groups
News
Froogle
more »
Search

"please log in"

Web Results **1** - **100** of about **2,440,000** for "**please log in**". (**0.84** seconds)

Login Portals

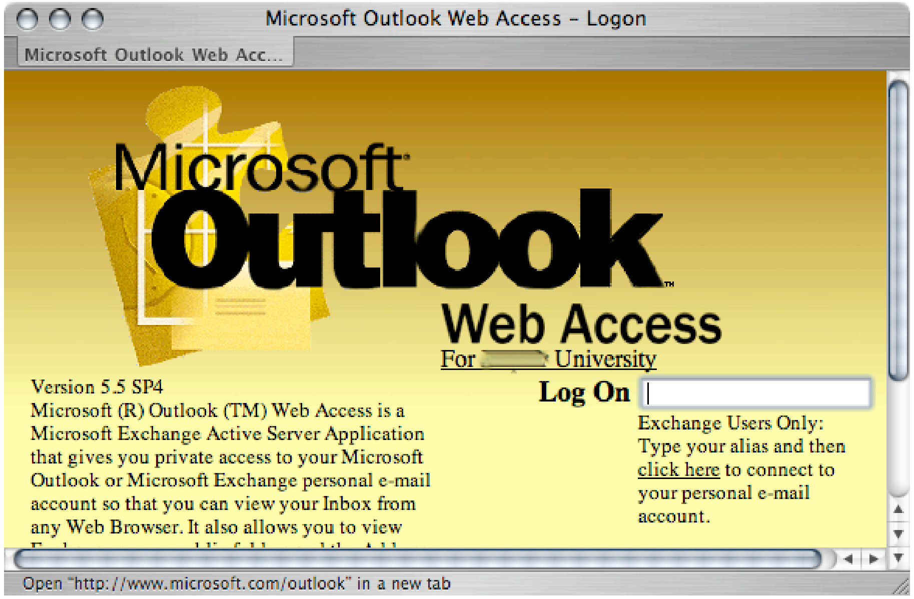
- Another very generic portal



Results **1** - **100** of about **11,300** for **inurl:/admin/login.asp** . (**0.57** seconds)

Login Portals

- Microsoft Outlook Web Access


Microsoft Outlook Web Access – Logon
Microsoft Outlook Web Acc...
Microsoft Outlook Web Access

For [redacted] University

Log On

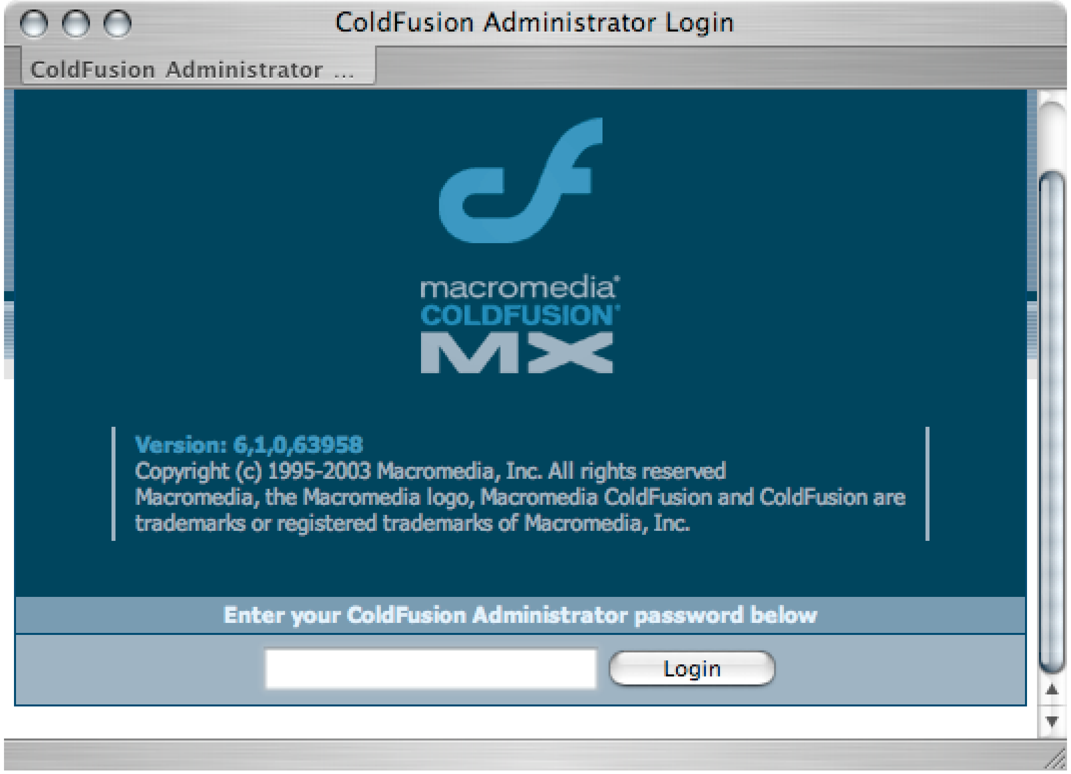
Version 5.5 SP4
Microsoft (R) Outlook (TM) Web Access is a Microsoft Exchange Active Server Application that gives you private access to your Microsoft Outlook or Microsoft Exchange personal e-mail account so that you can view your Inbox from any Web Browser. It also allows you to view

Exchange Users Only:
Type your alias and then click here to connect to your personal e-mail account.

Open "http://www.microsoft.com/outlook" in a new tab

Login Portals

- Coldfusion Admin Page

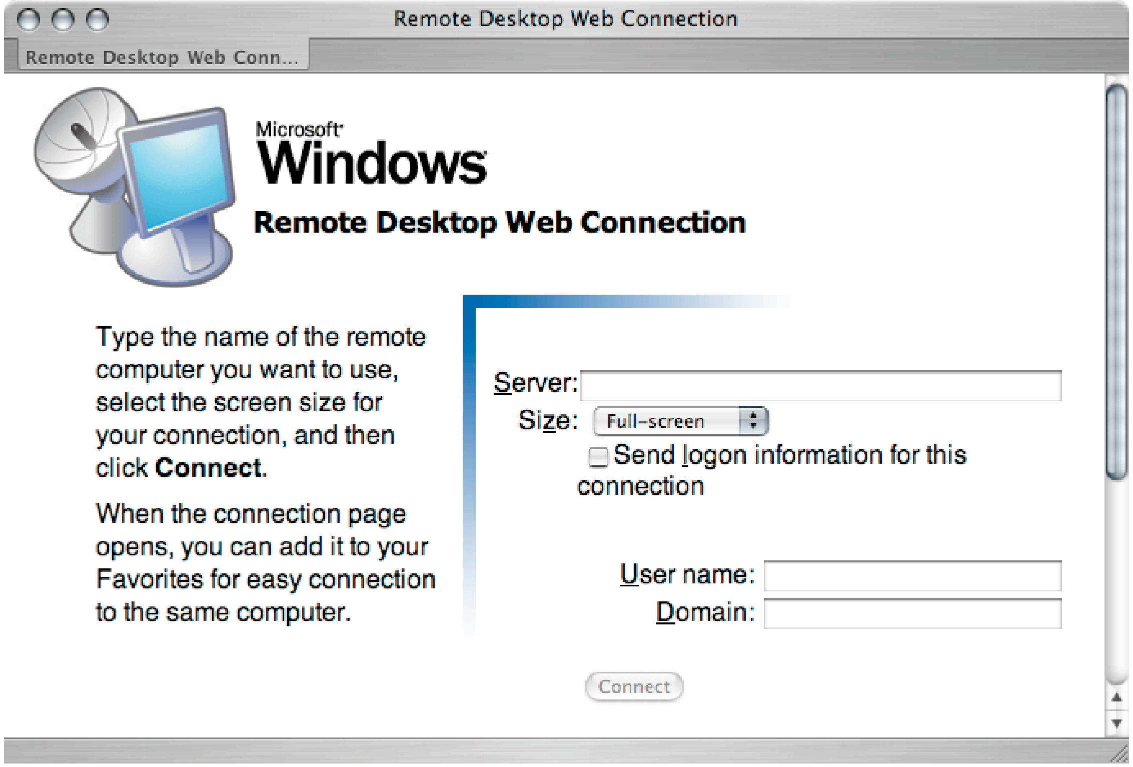


Version: 6,1,0,63958
Copyright (c) 1995-2003 Macromedia, Inc. All rights reserved
Macromedia, the Macromedia logo, Macromedia ColdFusion and ColdFusion are trademarks or registered trademarks of Macromedia, Inc.

Enter your ColdFusion Administrator password below

Login Portals

- Windows Remote Desktop



Remote Desktop Web Connection
Remote Desktop Web Conn...
Microsoft
Windows
Remote Desktop Web Connection

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

When the connection page opens, you can add it to your Favorites for easy connection to the same computer.

Server:

Size: Full-screen

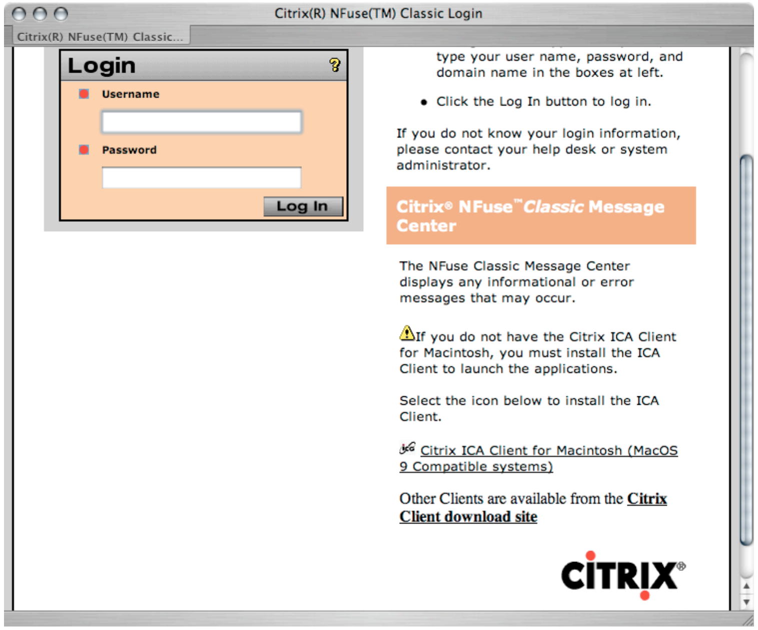
□ Send logon information for this connection

User name:

Domain:

Login Portals

- Citrix Metaframe


Citrix(R) NFuse(TM) Classic Login
Citrix(R) NFuse(TM) Classic...
Login
Username
Password
Log In

type your user name, password, and domain name in the boxes at left.

- Click the Log In button to log in.

If you do not know your login information, please contact your help desk or system administrator.

Citrix® NFuse™ *Classic* Message Center

The NFuse Classic Message Center displays any informational or error messages that may occur.

⚠If you do not have the Citrix ICA Client for Macintosh, you must install the ICA Client to launch the applications.

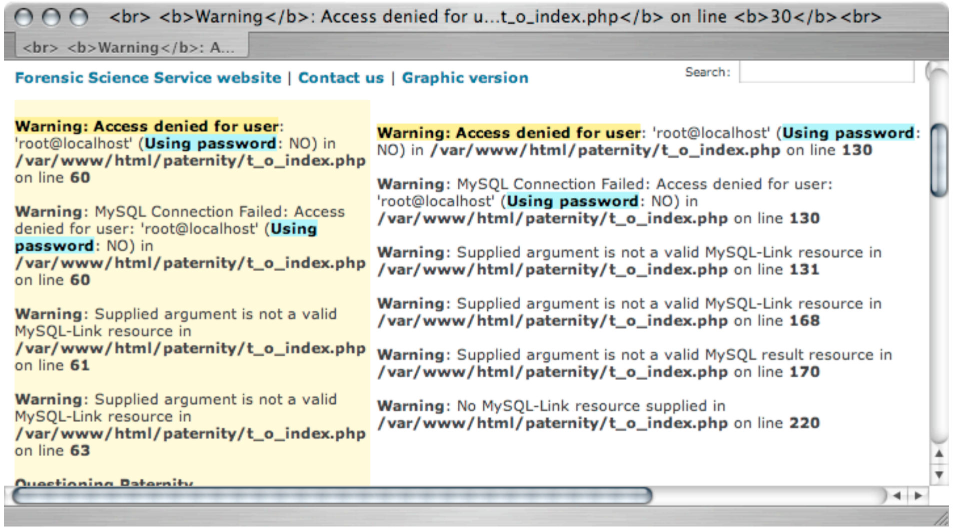
Select the icon below to install the ICA Client.

Citrix ICA Client for Macintosh (MacOS 9 Compatible systems)

Other Clients are available from the **Citrix Client download site**

SQL Information

- Gathering SQL usernames is simple with this search



 <b>Warning</b>: Access denied for u...t_o_index.php</b> on line <b>30</b>

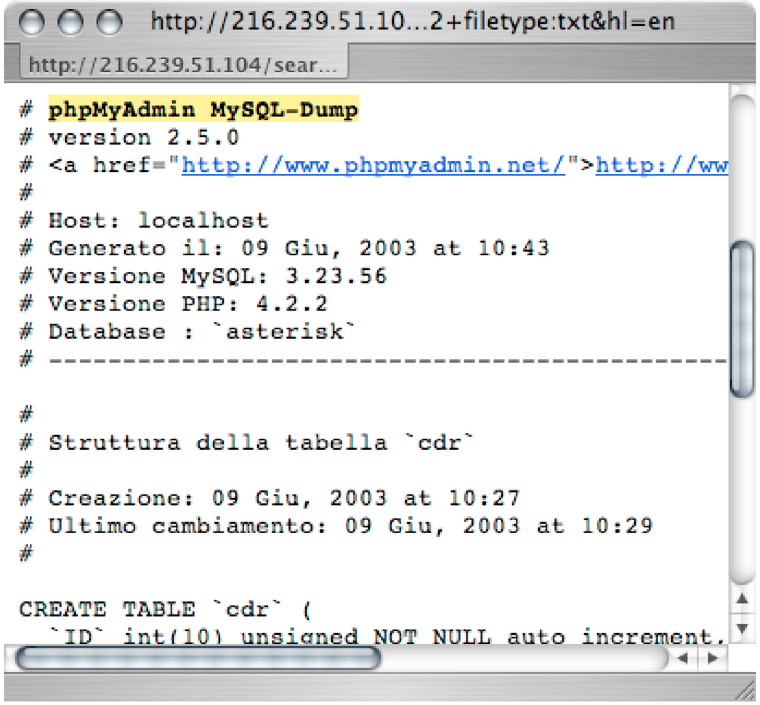
 <b>Warning</b>: A...
Forensic Science Service website | Contact us | Graphic version
Search:

```
Warning: Access denied for user:
'root@localhost' (Using password: NO) in
/var/www/html/paternity/t_o_index.php
on line 60

Warning: MySQL Connection Failed: Access
denied for user: 'root@localhost' (Using
password: NO) in
/var/www/html/paternity/t_o_index.php
on line 60

Warning: Supplied argument is not a valid
MySQL-Link resource in
/var/www/html/paternity/t_o_index.php
on line 61

Warning: Supplied argument is not a valid
MySQL-Link resource in
/var/www/html/paternity/t_o_index.php
on line 63

Questioning Paternity
```

```
Warning: Access denied for user: 'root@localhost' (Using password:
NO) in /var/www/html/paternity/t_o_index.php on line 130

Warning: MySQL Connection Failed: Access denied for user:
'root@localhost' (Using password: NO) in
/var/www/html/paternity/t_o_index.php on line 130

Warning: Supplied argument is not a valid MySQL-Link resource in
/var/www/html/paternity/t_o_index.php on line 131

Warning: Supplied argument is not a valid MySQL-Link resource in
/var/www/html/paternity/t_o_index.php on line 168

Warning: Supplied argument is not a valid MySQL result resource in
/var/www/html/paternity/t_o_index.php on line 170

Warning: No MySQL-Link resource supplied in
/var/www/html/paternity/t_o_index.php on line 220
```

SQL Information

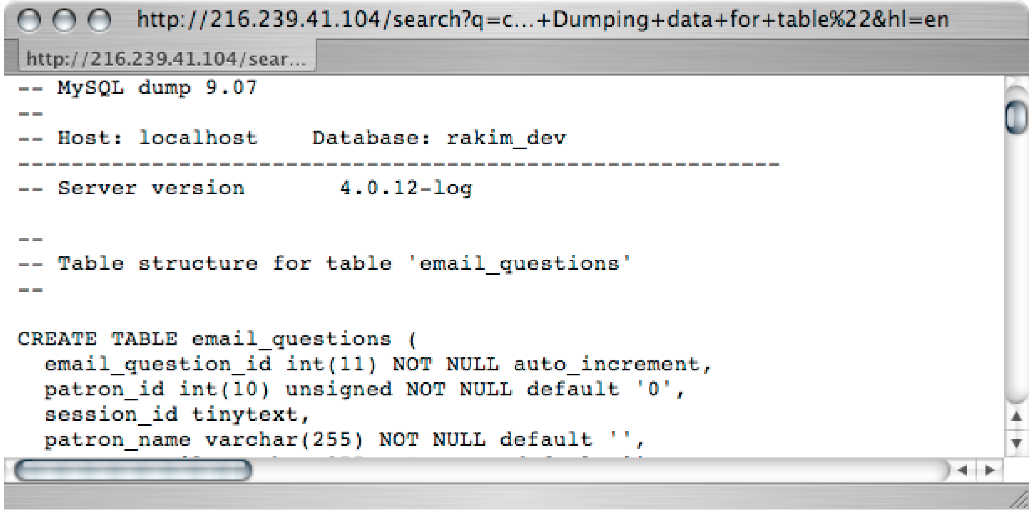
- This is an SQL dump made by phpmyadmin


http://216.239.51.10...2+filetype:txt&hl=en
http://216.239.51.104/sear...

```
# phpMyAdmin MySQL-Dump
# version 2.5.0
# <a href="http://www.phpmyadmin.net/">http://ww
#
# Host: localhost
# Generato il: 09 Giu, 2003 at 10:43
# Versione MySQL: 3.23.56
# Versione PHP: 4.2.2
# Database : `asterisk`
# --------------------------------------------

#
# Struttura della tabella `cdr`
#
# Creazione: 09 Giu, 2003 at 10:27
# Ultimo cambiamento: 09 Giu, 2003 at 10:29
#

CREATE TABLE `cdr` (
  `ID` int(10) unsigned NOT NULL auto_increment,
```

SQL Information

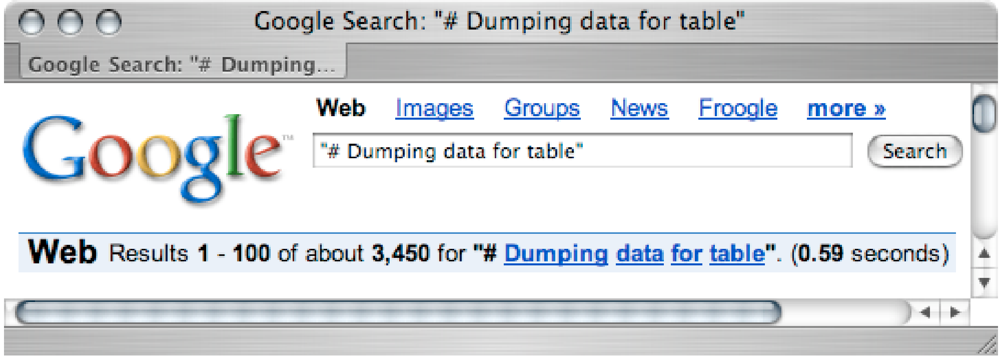
- This is a complete database schema dump, essentially a complete database backup


http://216.239.41.104/search?q=c...+Dumping+data+for+table%22&hl=en
http://216.239.41.104/sear...

```
-- MySQL dump 9.07
--
-- Host: localhost    Database: rakim_dev
---------------------------------------------------------
-- Server version       4.0.12-log

--
-- Table structure for table 'email_questions'
--

CREATE TABLE email_questions (
  email_question_id int(11) NOT NULL auto_increment,
  patron_id int(10) unsigned NOT NULL default '0',
  session_id tinytext,
  patron_name varchar(255) NOT NULL default '',
```

SQL Information

- This query will locate SQL schemas on the web



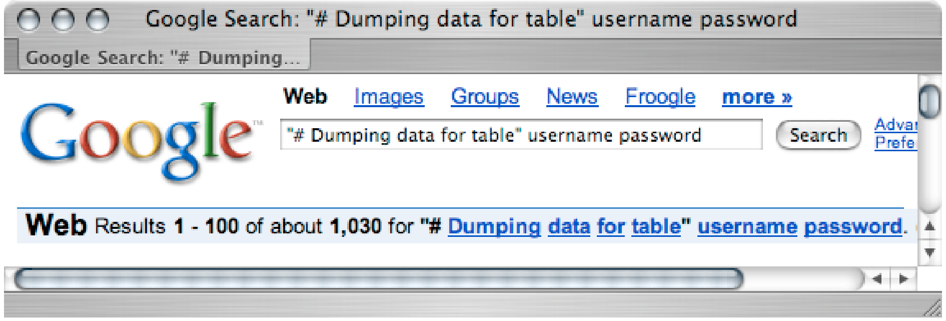
Google Search: "# Dumping data for table"

"# Dumping data for table"

Web Results 1 - 100 of about 3,450 for "# Dumping data for table". (0.59 seconds)

SQL Information

- In addition, this query finds the words username and password inside the SQL dump



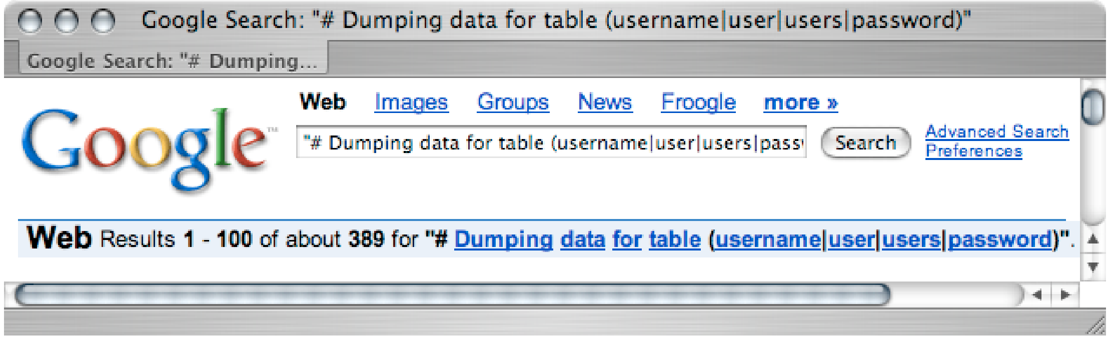
Google Search: "# Dumping data for table" username password

"# Dumping data for table" username password

Web Results 1 - 100 of about 1,030 for "# Dumping data for table" username password.

SQL Information

- This potent query finds SQL dumps wither username, user, users or password as a table name



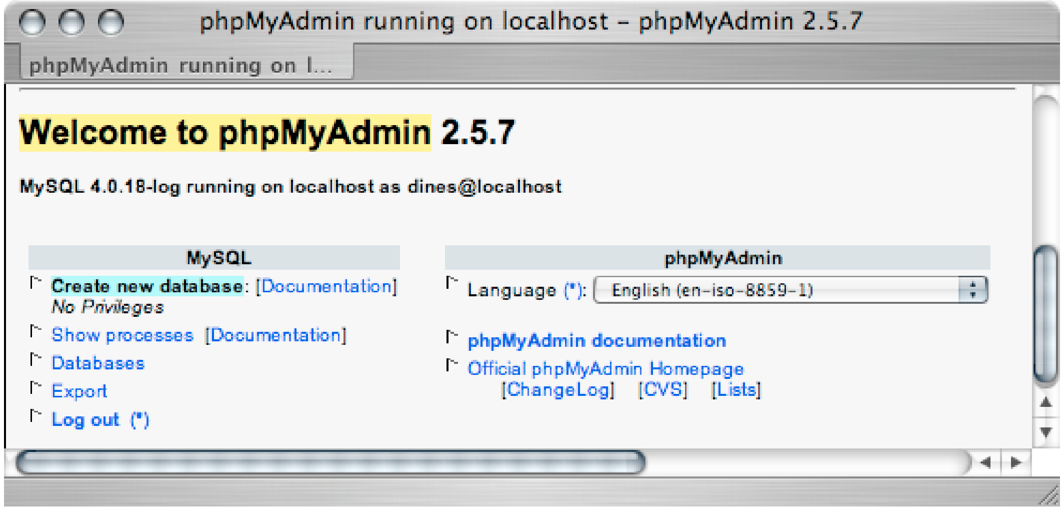
Google Search: "# Dumping data for table (username|user|users|password)"

"# Dumping data for table (username|user|users|pass

Web Results 1 - 100 of about 389 for "# Dumping data for table (username|user|users|password)".

SQL Information

- This graphical front-end to SQL is mis-configured to allow anyone admin access



phpMyAdmin running on localhost – phpMyAdmin 2.5.7

Welcome to phpMyAdmin 2.5.7

MySQL 4.0.18-log running on localhost as dines@localhost

MySQL

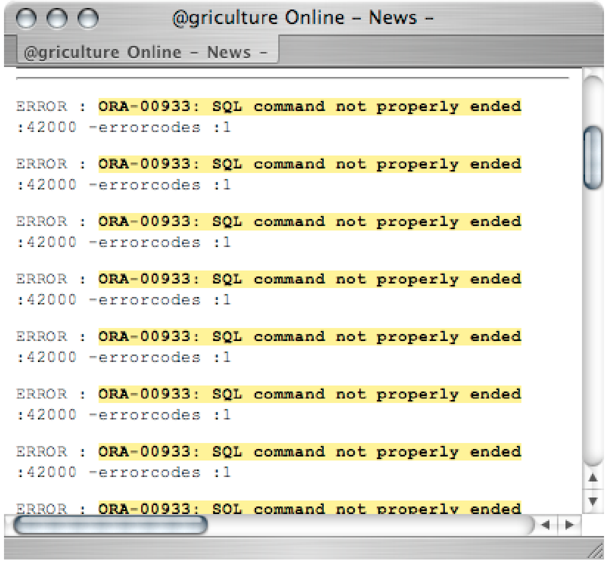
- **Create new database**: [Documentation]
  No Privileges
- Show processes [Documentation]
- Databases
- Export
- **Log out** (*)

phpMyAdmin

- Language (*): English (en-iso-8859-1)
- **phpMyAdmin documentation**
- Official phpMyAdmin Homepage
  [ChangeLog] [CVS] [Lists]

SQL Information

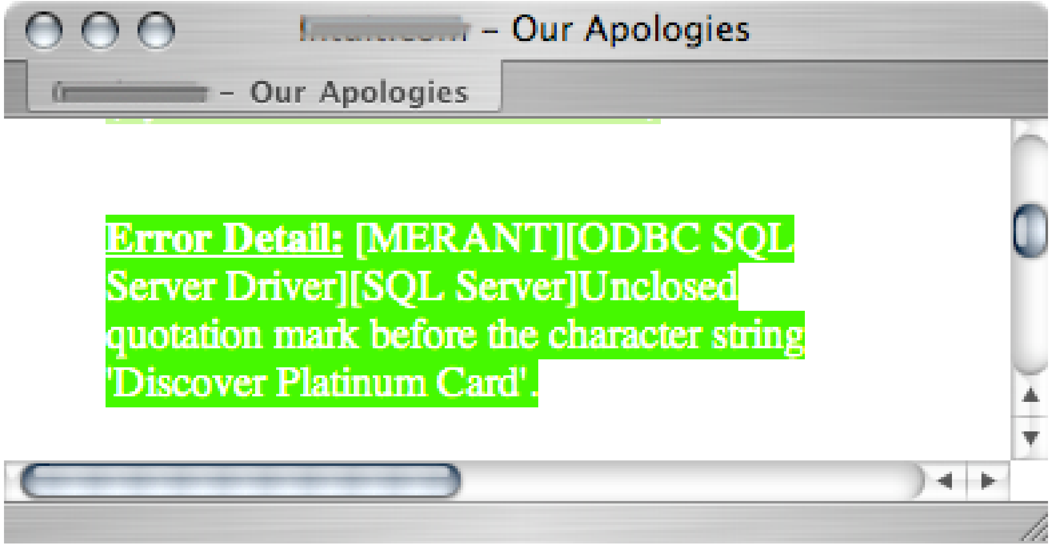
- This search can be used by hackers to find SQL injection targets



```
ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
:42000 -errorcodes :1

ERROR : ORA-00933: SQL command not properly ended
```

SQL Information

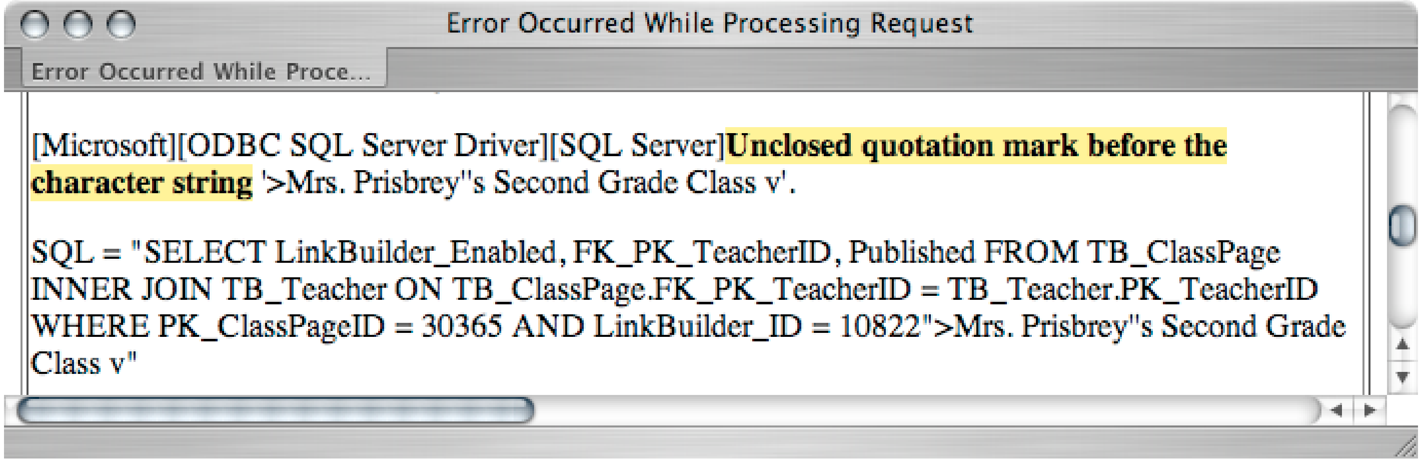
- …another SQL injection target…



Error Detail: [MERANT][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string 'Discover Platinum Card'.

SQL Information

- ..and another…



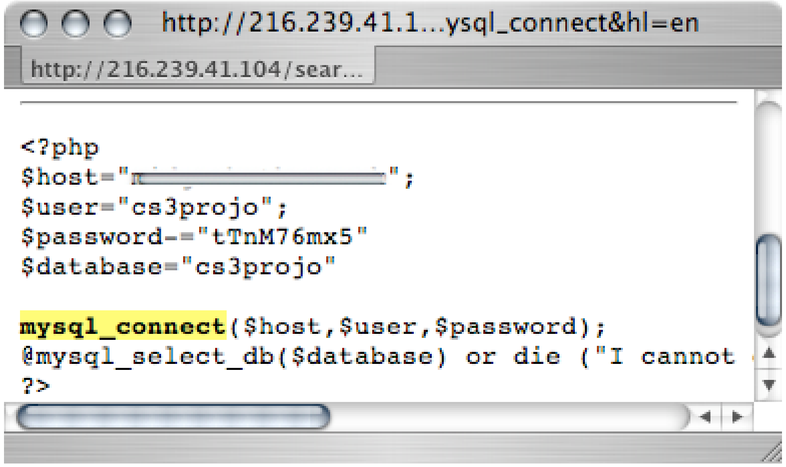
Error Occurred While Processing Request
Error Occurred While Proce…

[Microsoft][ODBC SQL Server Driver][SQL Server]**Unclosed quotation mark before the character string** '>Mrs. Prisbrey''s Second Grade Class v'.

SQL = "SELECT LinkBuilder_Enabled, FK_PK_TeacherID, Published FROM TB_ClassPage INNER JOIN TB_Teacher ON TB_ClassPage.FK_PK_TeacherID = TB_Teacher.PK_TeacherID WHERE PK_ClassPageID = 30365 AND LinkBuilder_ID = 10822">Mrs. Prisbrey''s Second Grade Class v"

SQL Information

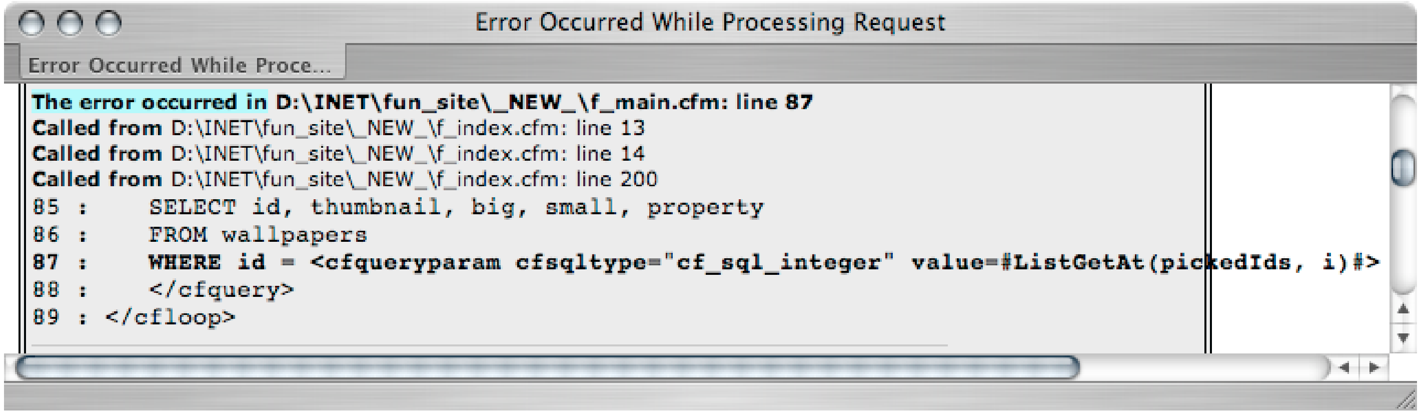
- the mysql_connect function makes a database query with a supplied username and password
- This file should not be on the web


http://216.239.41.1...ysql_connect&hl=en
http://216.239.41.104/sear...

```
<?php
$host="[redacted]";
$user="cs3projo";
$password-="tTnM76mx5"
$database="cs3projo"

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

SQL Information

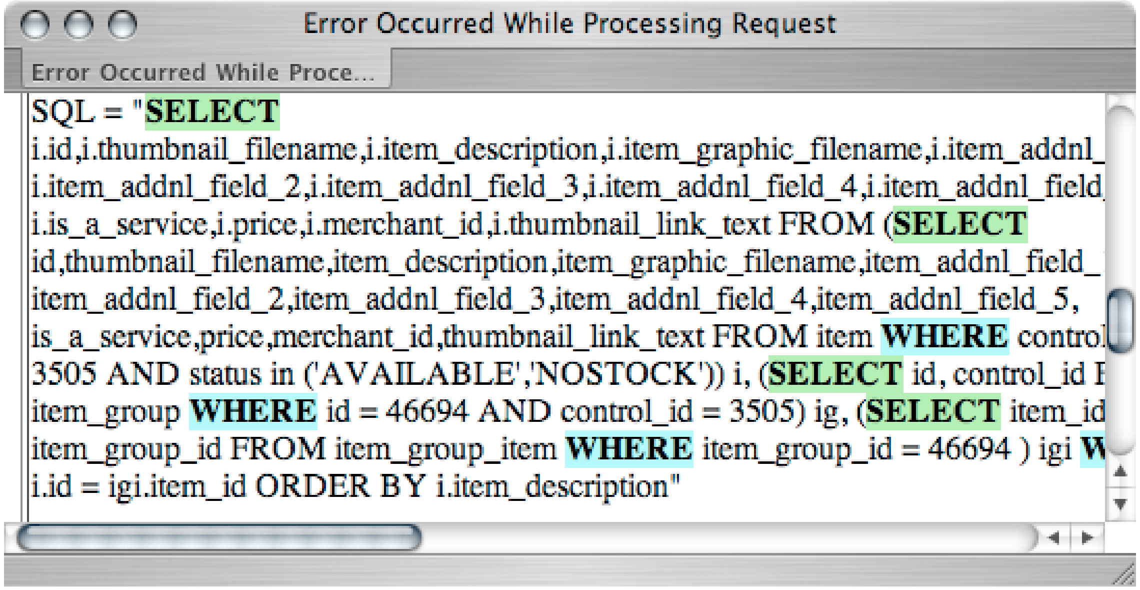
- In most cases, there's nothing better for an SQL injector than a complete line of SQL source code…


Error Occurred While Processing Request
Error Occurred While Proce...

```
The error occurred in D:\INET\fun_site\_NEW_\f_main.cfm: line 87
Called from D:\INET\fun_site\_NEW_\f_index.cfm: line 13
Called from D:\INET\fun_site\_NEW_\f_index.cfm: line 14
Called from D:\INET\fun_site\_NEW_\f_index.cfm: line 200
85 :     SELECT id, thumbnail, big, small, property
86 :     FROM wallpapers
87 :     WHERE id = <cfqueryparam cfsqltype="cf_sql_integer" value=#ListGetAt(pickedIds, i)#>
88 :     </cfquery>
89 :  </cfloop>
```

SQL Information

- …except for really long lines of SQL code…



Error Occurred While Processing Request
Error Occurred While Proce…

```
SQL = "SELECT
i.id,i.thumbnail_filename,i.item_description,i.item_graphic_filename,i.item_addnl_
i.item_addnl_field_2,i.item_addnl_field_3,i.item_addnl_field_4,i.item_addnl_field
i.is_a_service,i.price,i.merchant_id,i.thumbnail_link_text FROM (SELECT
id,thumbnail_filename,item_description,item_graphic_filename,item_addnl_field_
item_addnl_field_2,item_addnl_field_3,item_addnl_field_4,item_addnl_field_5,
is_a_service,price,merchant_id,thumbnail_link_text FROM item WHERE control
3505 AND status in ('AVAILABLE','NOSTOCK')) i, (SELECT id, control_id F
item_group WHERE id = 46694 AND control_id = 3505) ig, (SELECT item_id
item_group_id FROM item_group_item WHERE item_group_id = 46694 ) igi W
i.id = igi.item_id ORDER BY i.item_description"
```

Examples

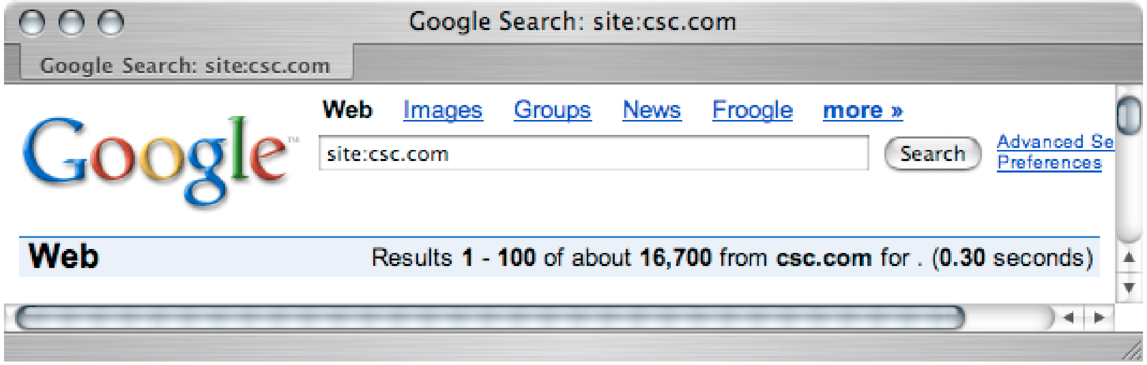
- *** LIVE EXAMPLES REMOVED FROM PRINT VERSION***

Prevention

- Do not put sensitive data on your web site, even temporarily
- Proactively check your web presence with Google on a regular basis
- Use sites like http://johnny.ihackstuff.com to keep up on the latest “Google Hacks”

Prevention

- Use site: queries against each of your web hosts
- Don’t forget about hosts that do not have DNS names



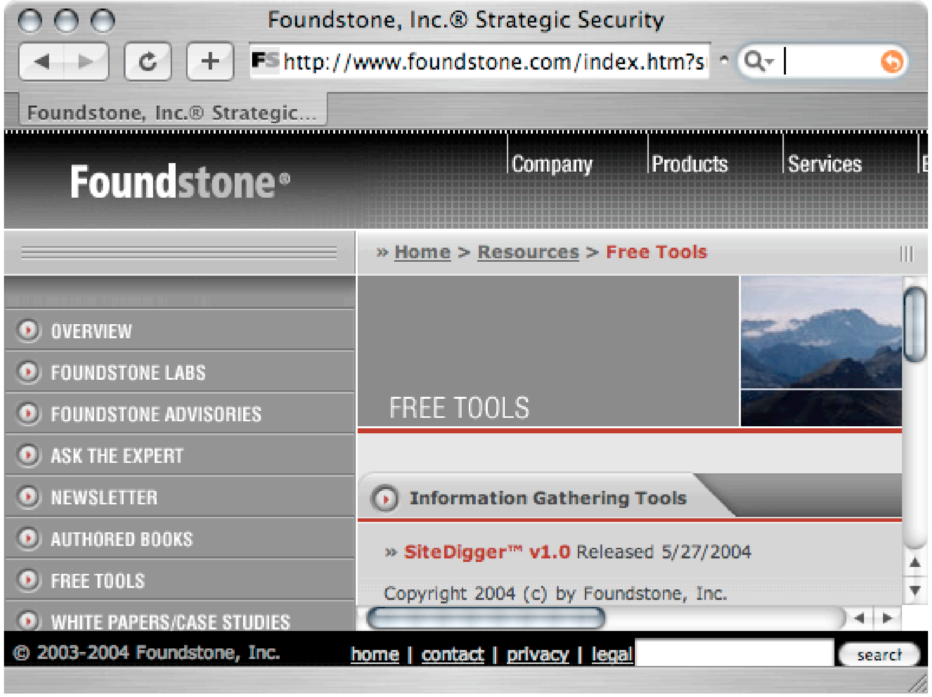
site:csc.com

Web Results **1** - **100** of about **16,700** from **csc.com** for . (**0.30** seconds)

- Scan each result page, ensuring that each and every page it supposed to be in Google’s database

Prevention

- Automate your scans with tools like sitedigger by Foundstone


Foundstone, Inc.® Strategic Security
http://www.foundstone.com/index.htm?s
Foundstone, Inc.® Strategic...
Foundstone®
Company
Products
Services
» Home > Resources > Free Tools
OVERVIEW
FOUNDSTONE LABS
FOUNDSTONE ADVISORIES
ASK THE EXPERT
NEWSLETTER
AUTHORED BOOKS
FREE TOOLS
WHITE PAPERS/CASE STUDIES
FREE TOOLS
Information Gathering Tools
home | contact | privacy | legal
search

» SiteDigger™ v1.0 Released 5/27/2004

Copyright 2004 (c) by Foundstone, Inc.

© 2003-2004 Foundstone, Inc.

Presentation Materials

- This is a condensed version of the actual presentation given at the event
- For more information, please see: http://johnny.ihackstuff.com
- e-mail: johnny@ihackstuff.com

Thanks

- Thanks to God for the gift of life.
- Thanks to my wife for the gift of love.
- Thanks to my kids for the gift of laughter.
- Thanks to my friends for filling in the blanks.