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

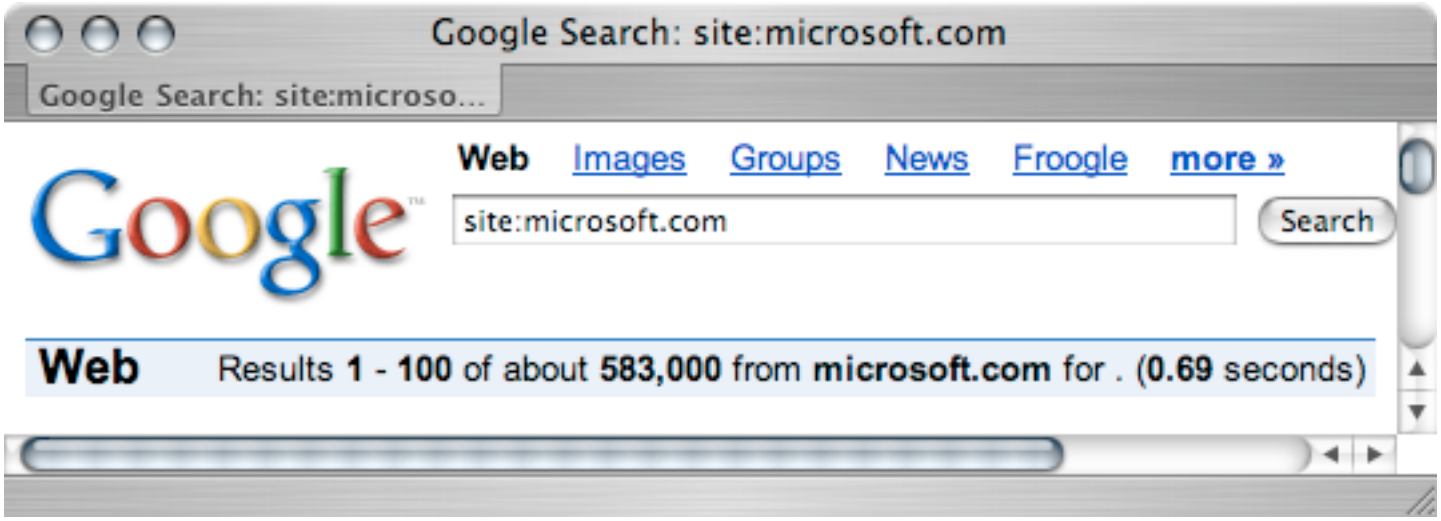
- site: restrict a search to a specific web site or domain
  - The web site to search must be supplied after the colon.
- filetype: search only within the text of a particular type of file
- link: search within hyperlinks
- cache: displays the version of a web page as it appeared when Google crawled 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

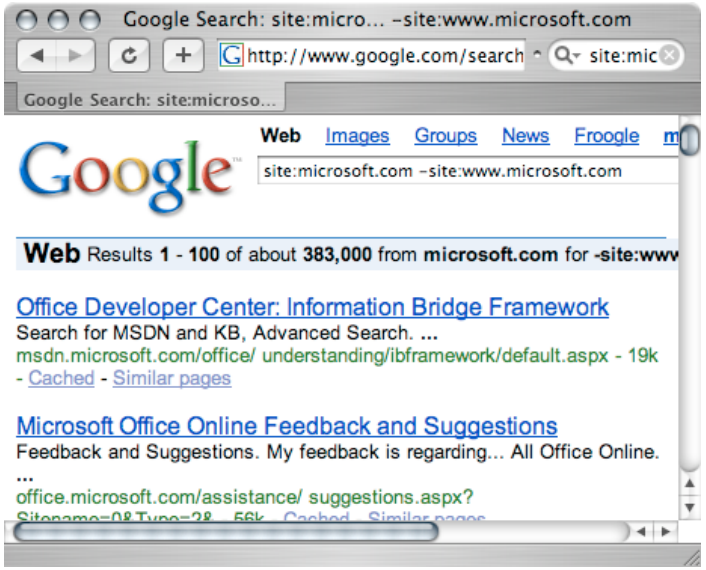
- To find every web page Google has crawled for a specific site, use the site: operator



site: microsoft.com

Server Crawling

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



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

Directory Listings

- Directory listings can be a source of great information



intitle:index.of/admin

Directory Listings

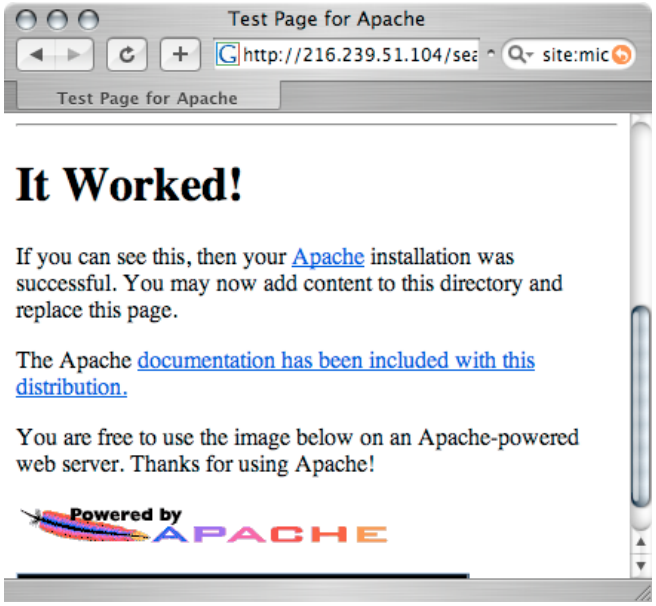
- Directory listings can provide server version information



intitle:index.of apache server.at

Default Server Pages

- Web servers with default pages can serve as juicy targets



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

Default Server Pages

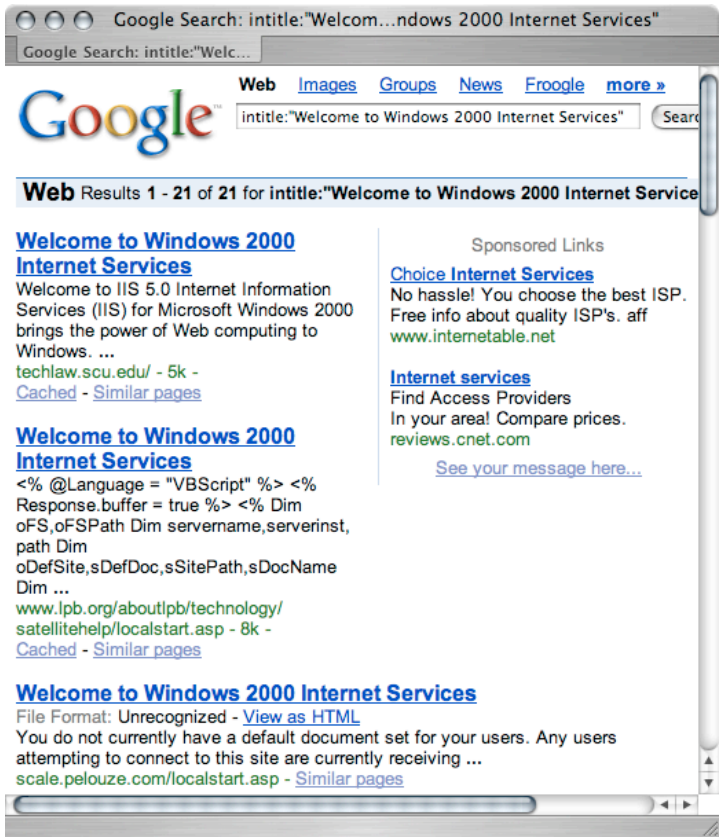
- Web servers with default pages can serve as juicy targets



allintitle:Netscape FastTrack Server Home Page

Default Server Pages

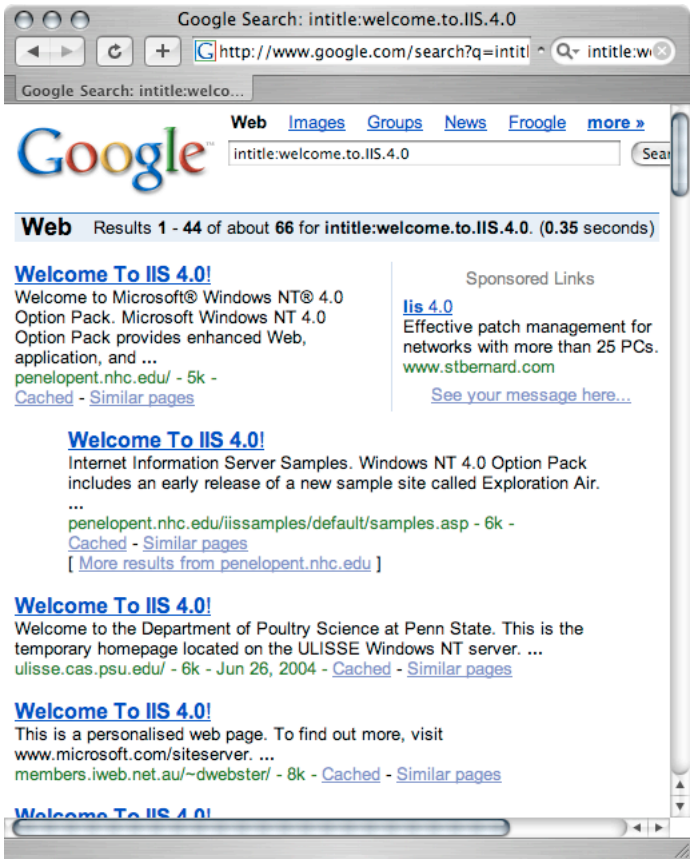
- Web servers with default pages can serve as juicy targets



intitle:"Welcome to Windows 2000 Internet Services"

Default Server Pages

- Web servers with default pages can serve as juicy targets



intitle:welcome.to.IIS.4.0

Default Server Pages

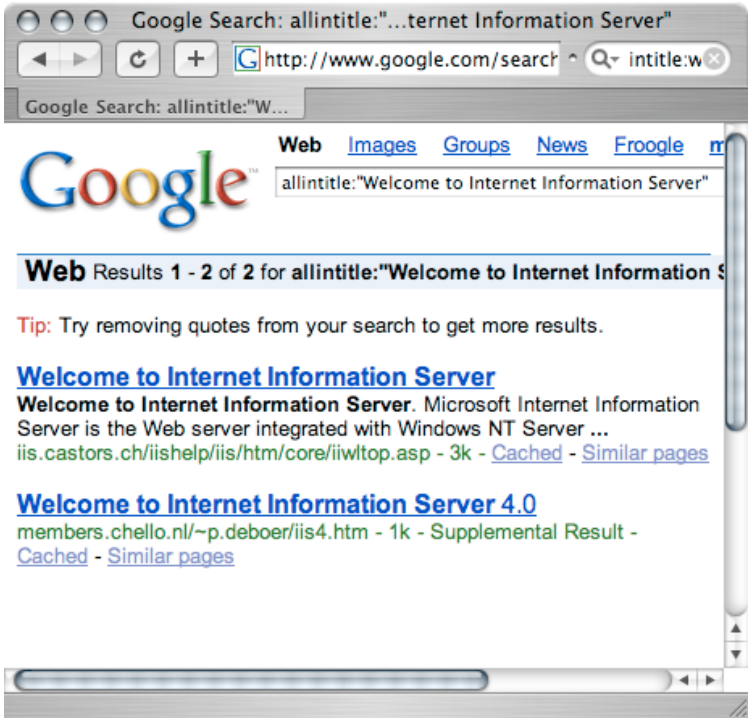
- Web servers with default pages can serve as juicy targets



allintitle:Welcome to Windows XP Server Internet Services

Default Server Pages

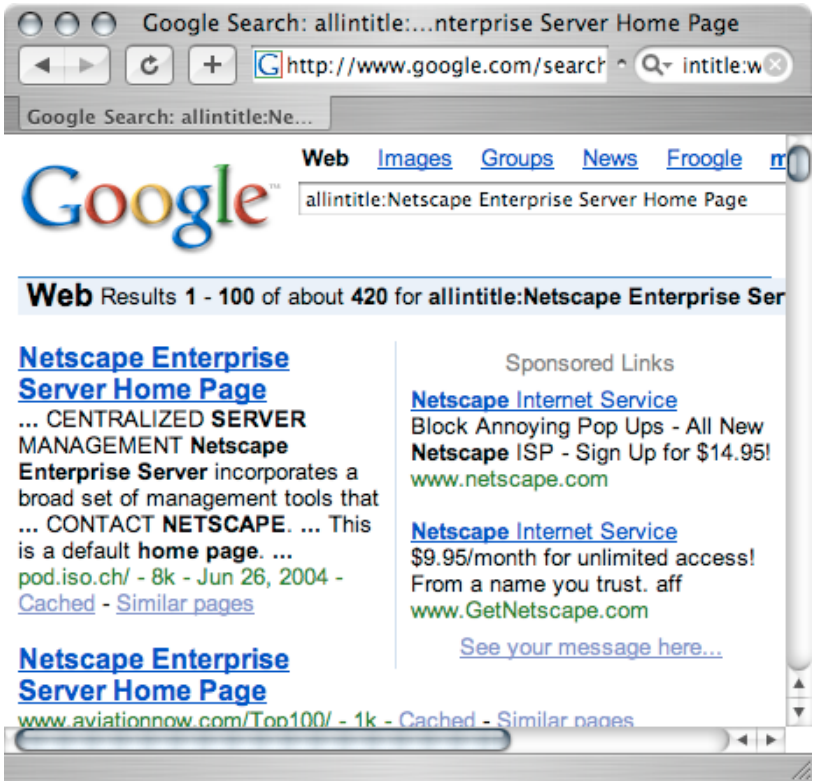
- Web servers with default pages can serve as juicy targets



allintitle:"Welcome to Internet Information Server"

Default Server Pages

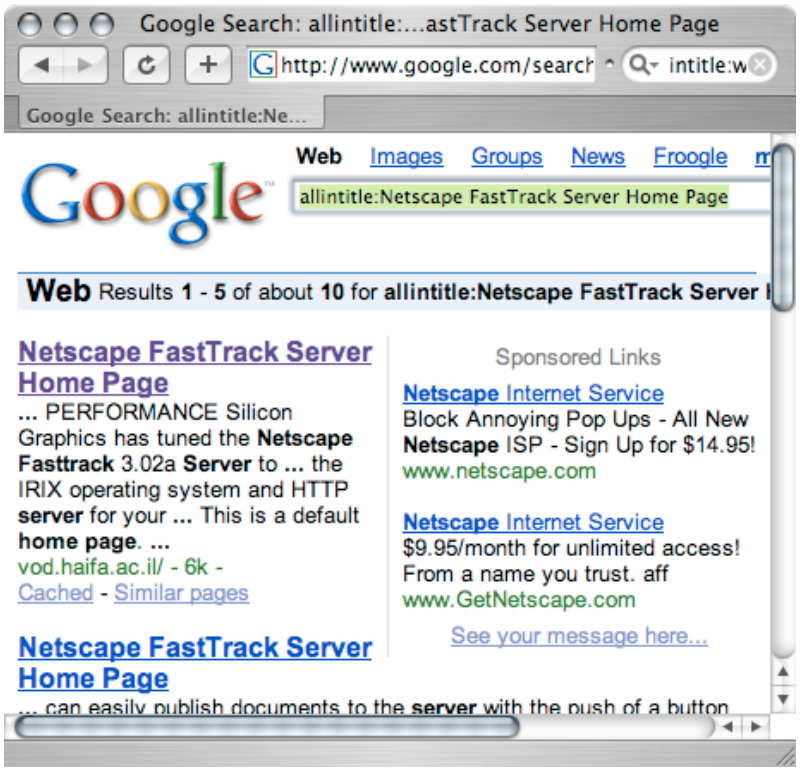
- Web servers with default pages can serve as juicy targets



allintitle:Netscape Enterprise Server Home Page

Default Server Pages

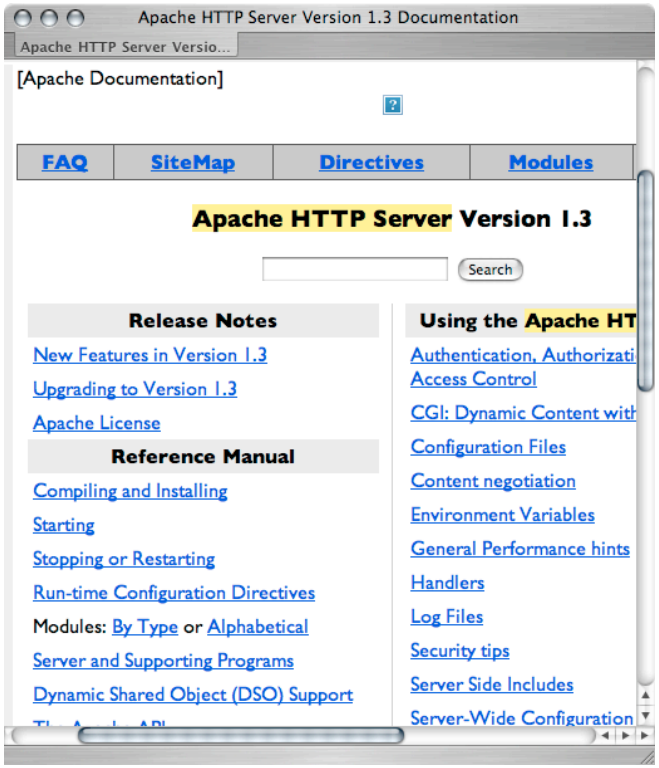
- Web servers with default pages can serve as juicy targets



allintitle:Netscape FASTTRACK Server Home Page

Default Documents

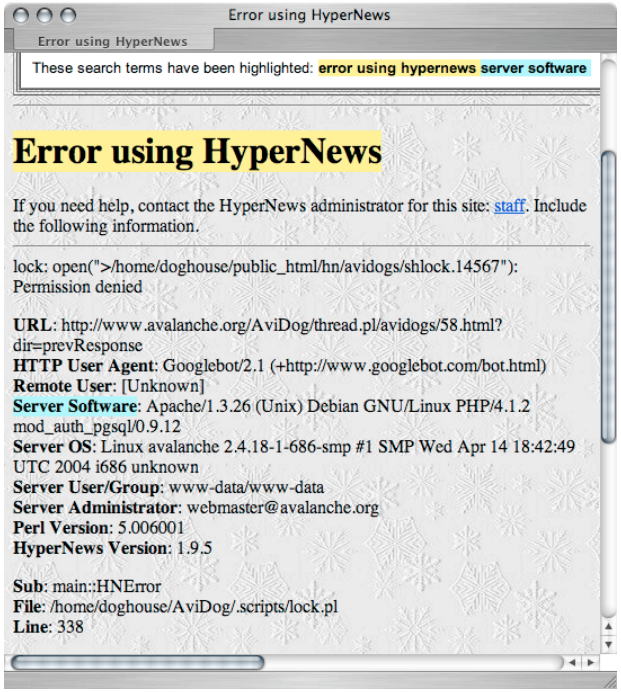
- Servers can also be profiled via default manuals and documentation



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

Error Messages

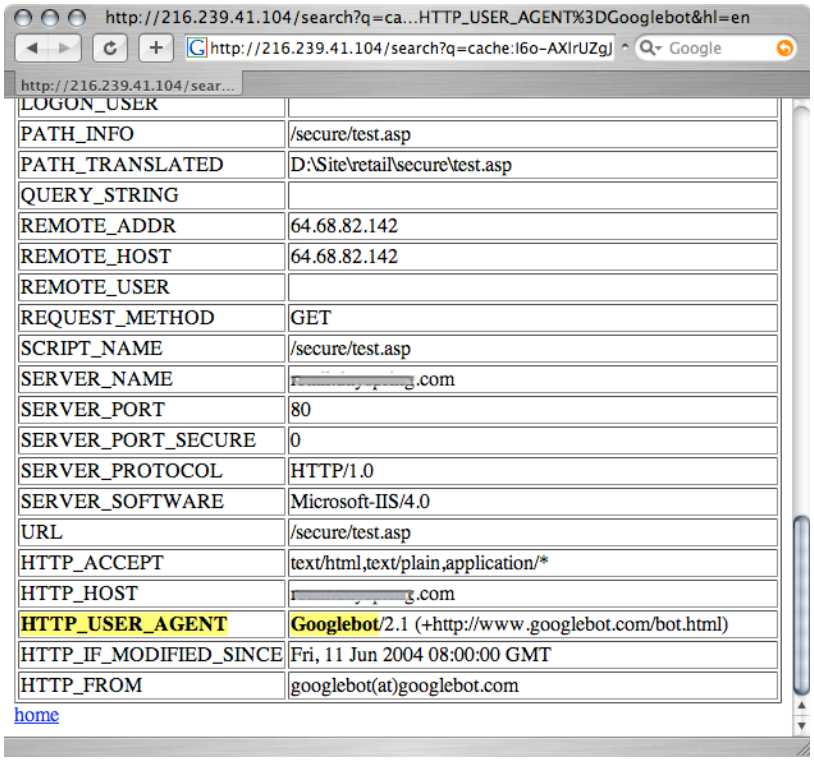
- Server profiling is easy with some error messages



intitle:"Error using Hypernews" "Server Software"

Error Messages

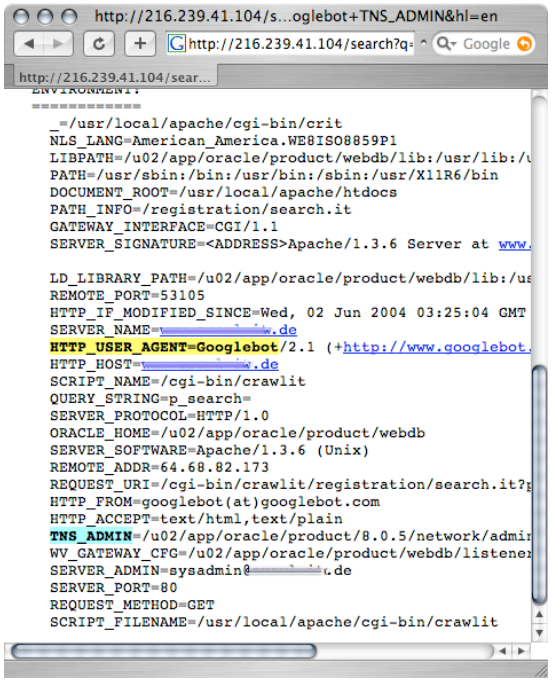
- CGI environment vars provide a great deal of information
- The generic way to find these pages is by focusing on the trail left by the googlebot crawler



"HTTP_USER_AGENT=Googlebot"

Error Messages

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

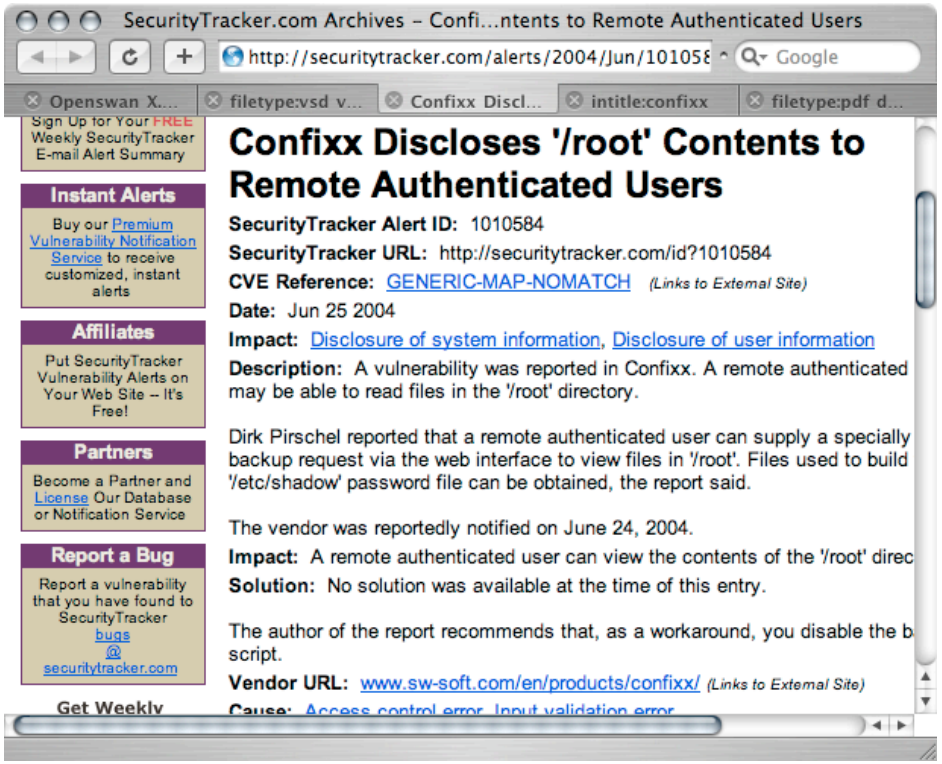


“HTTP_USER_AGENT=Googlebot”
TNS_ADMIN

Vulnerability Trolling

- Many attackers find vulnerable targets via Google

- A typical security advisory may look like this:



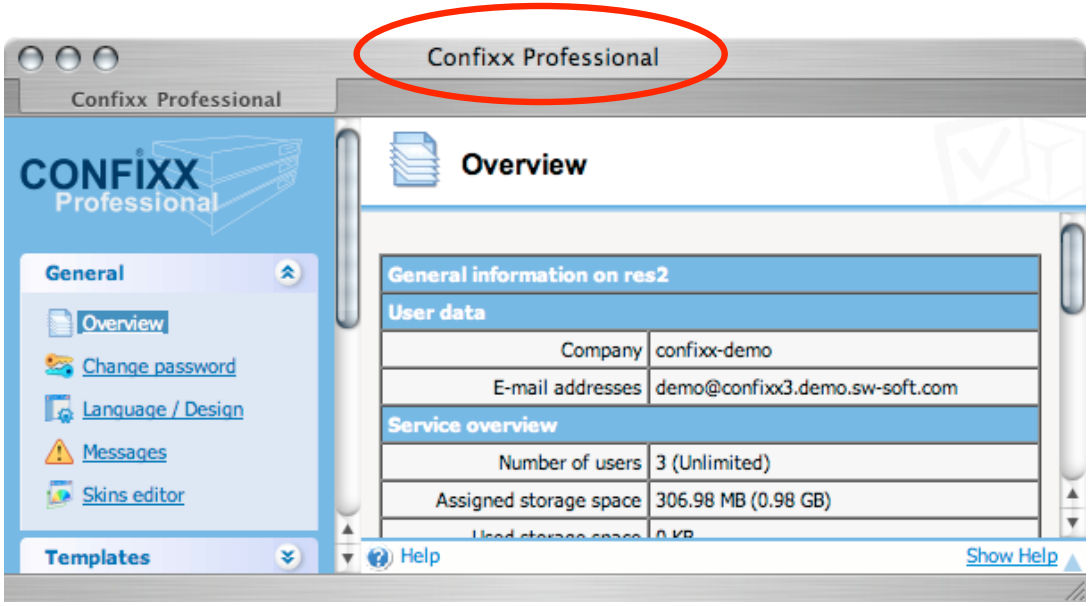
Vulnerability Trolling

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



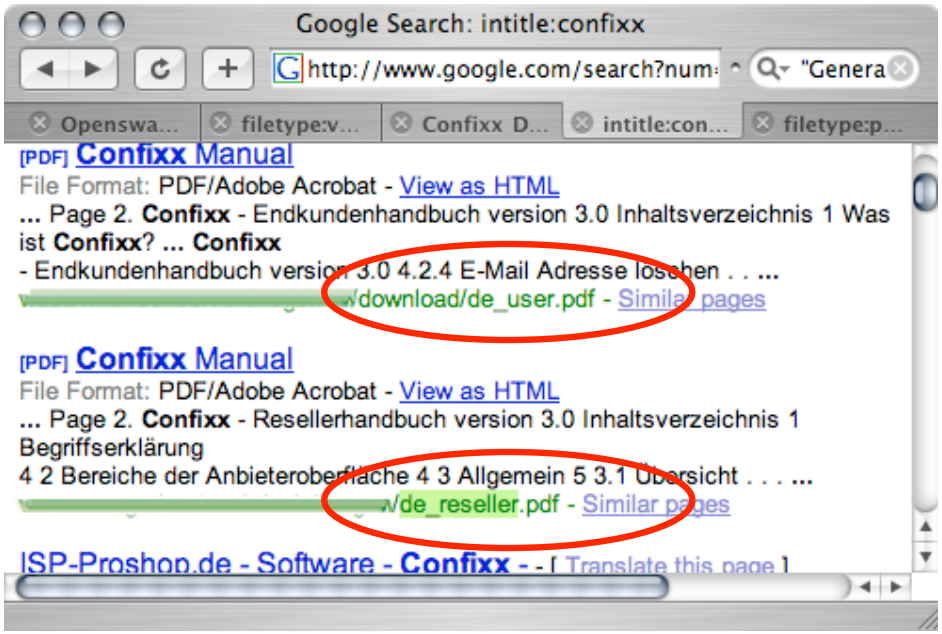
Vulnerability Trolling

- The demo page suggests one method for finding targets



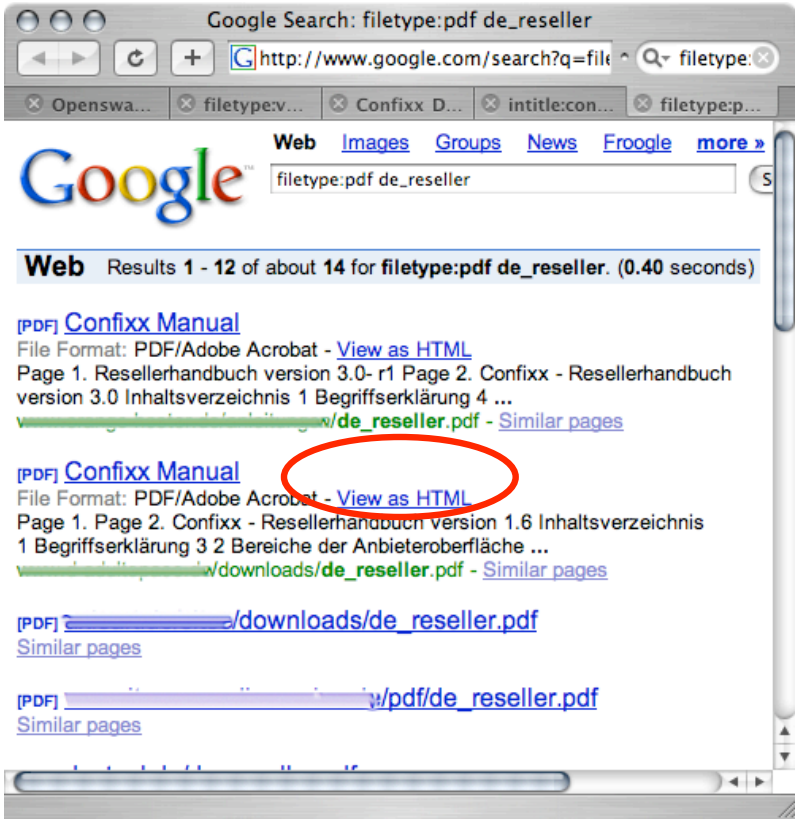
Vulnerability Trolling

- A quick intitle: search suggests more vectors…



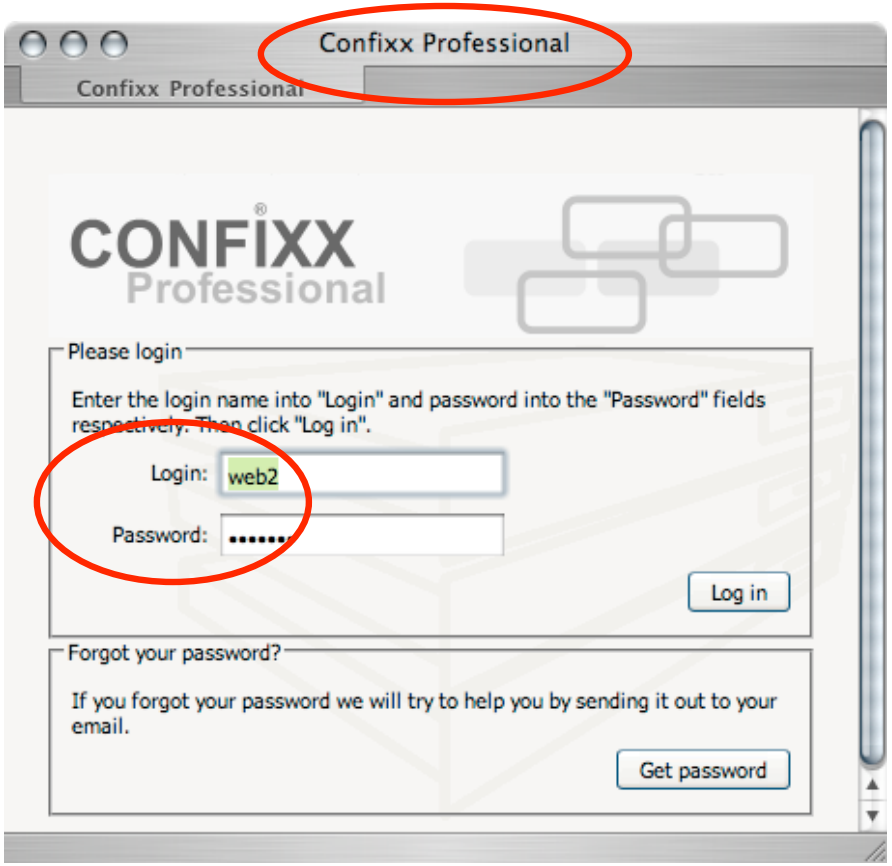
Vulnerability Trolling

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



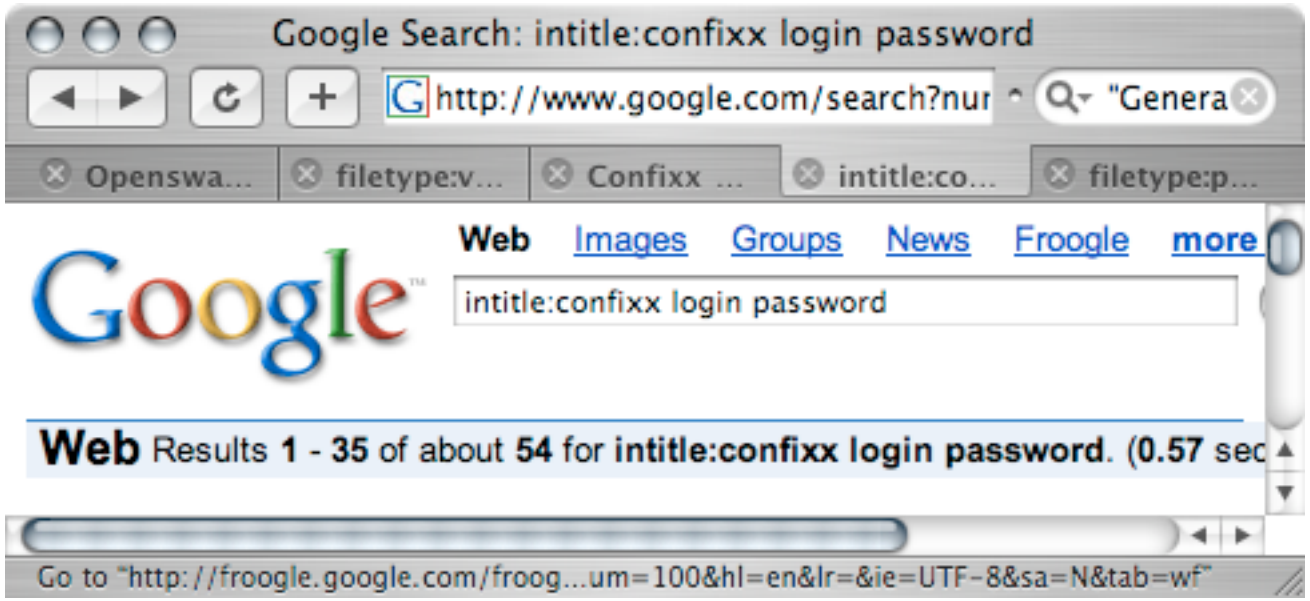
Vulnerability Trolling

- Other searches are easy to discover as well…



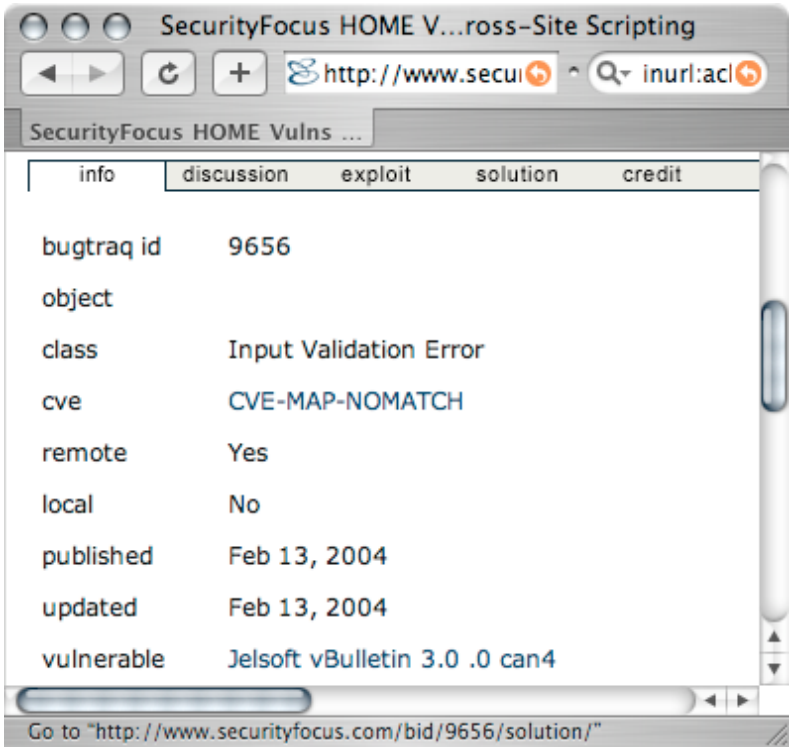
Vulnerability Trolling

- Other searches are easy to discover as well…



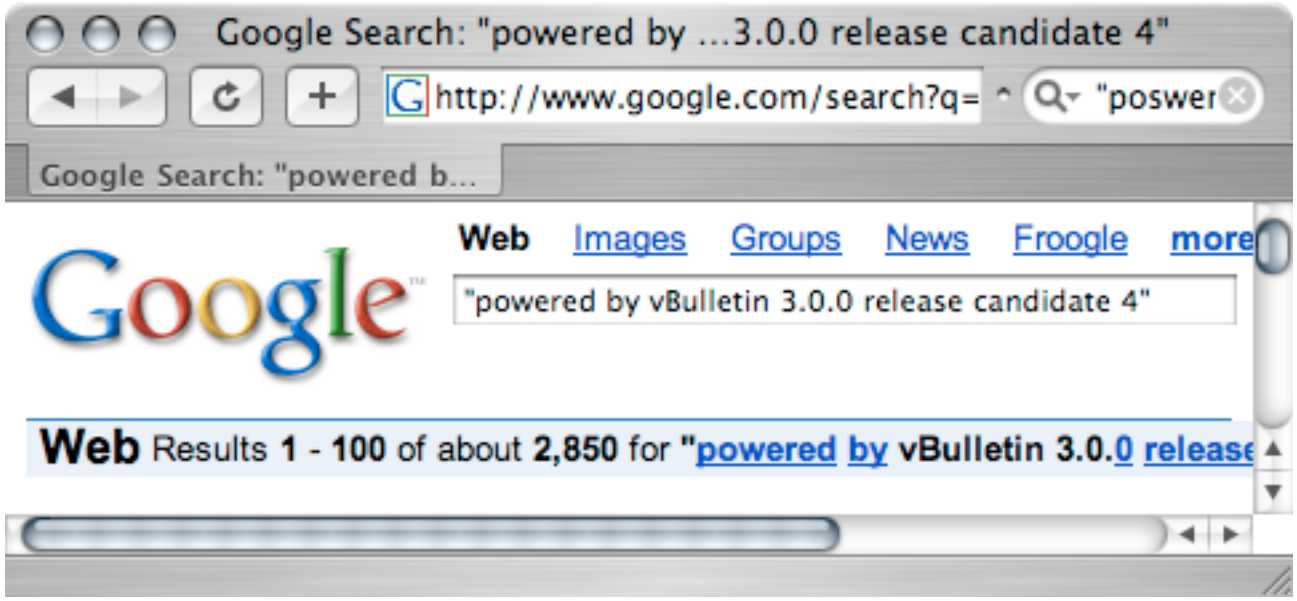
Vulnerability Trolling

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



Vulnerability Trolling

- A creative search finds vulnerable targets



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…

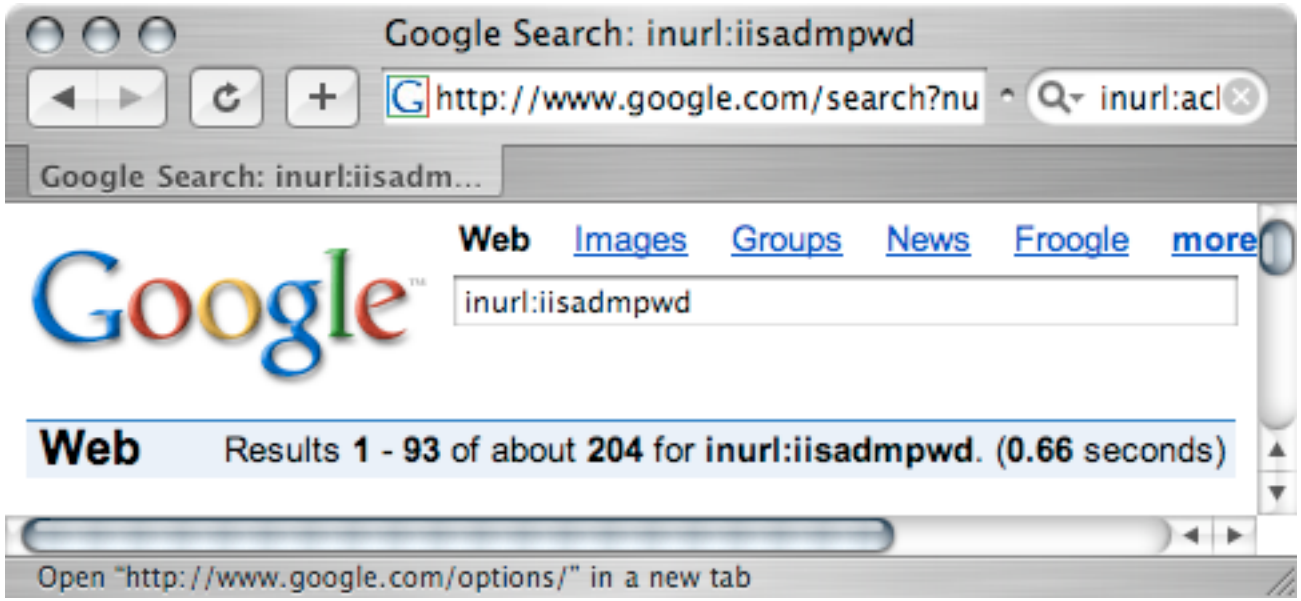
```
/iisadmpwd/
/iisadmpwd/achg.htr
/iisadmpwd/aexp.htr
/iisadmpwd/aexp2.htr
/iisadmpwd/aexp2b.htr
```

- 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
```

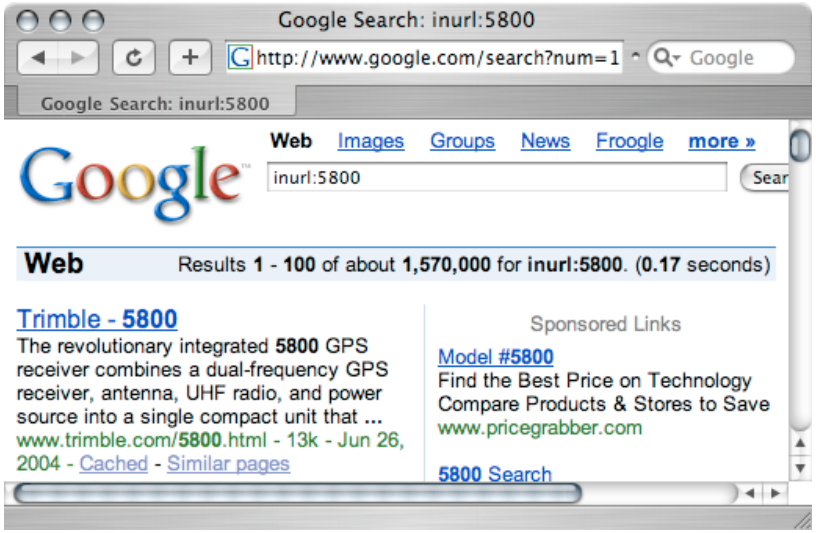
Vulnerability Trolling

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



Port Scanning

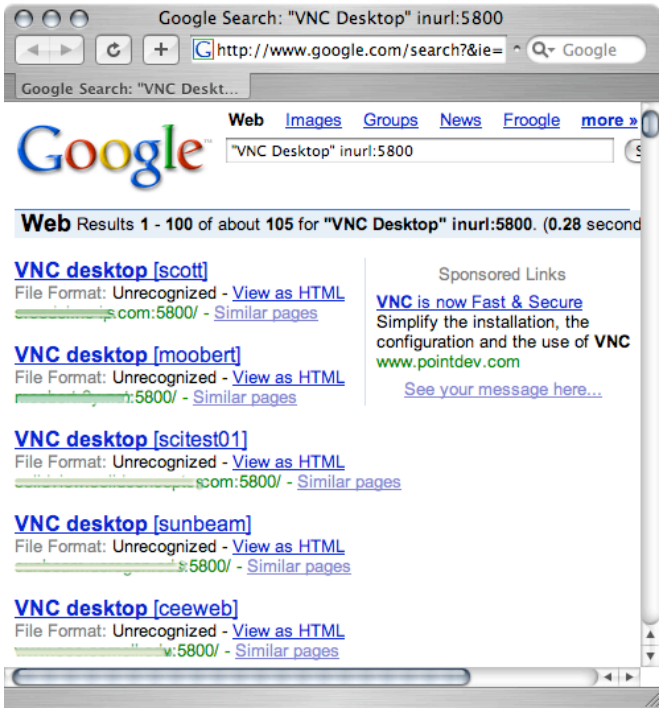
- Although port numbers are sometimes found in the url, there's no easy way to scan just for a port number… the results are much too copious



inurl:5800

Port Scanning

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



"VNC Desktop" inurl:5800

Port Scanning

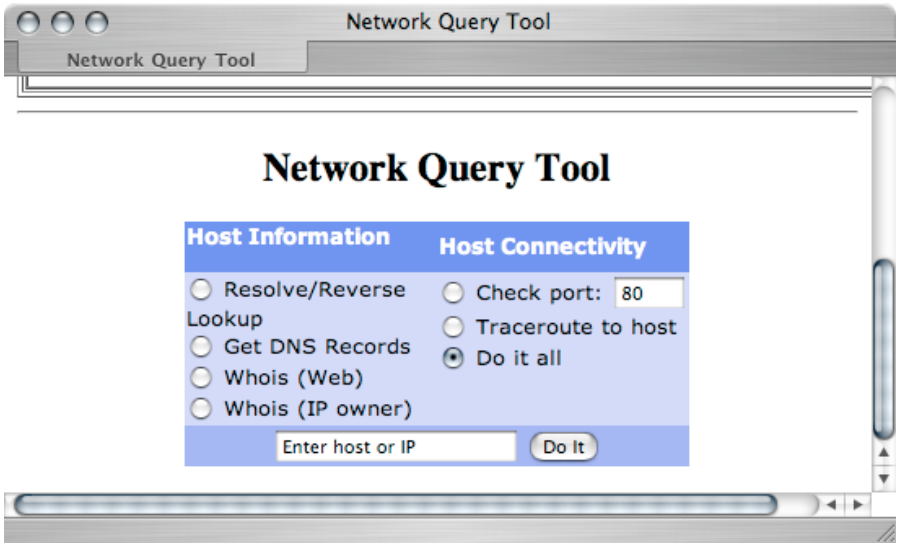
- Webmin, port 10000



inurl:webmin inurl:10000

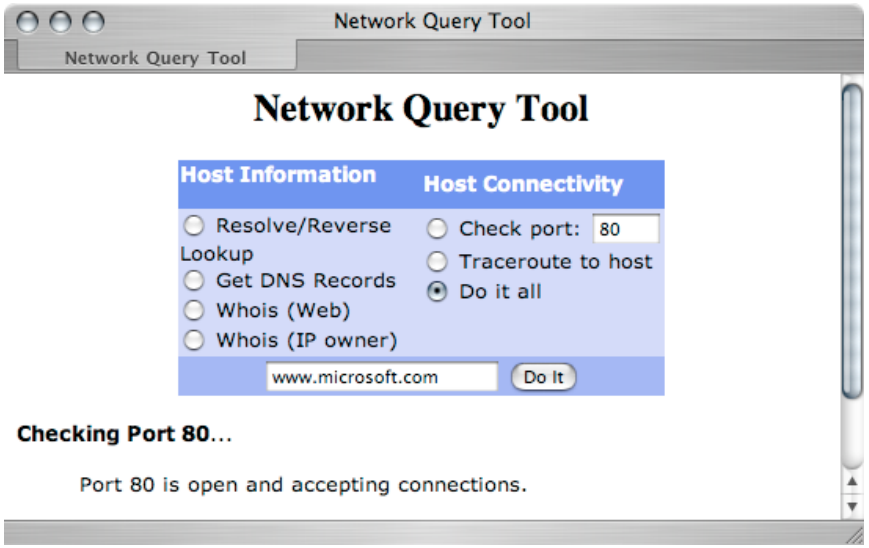
Port Scanning

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



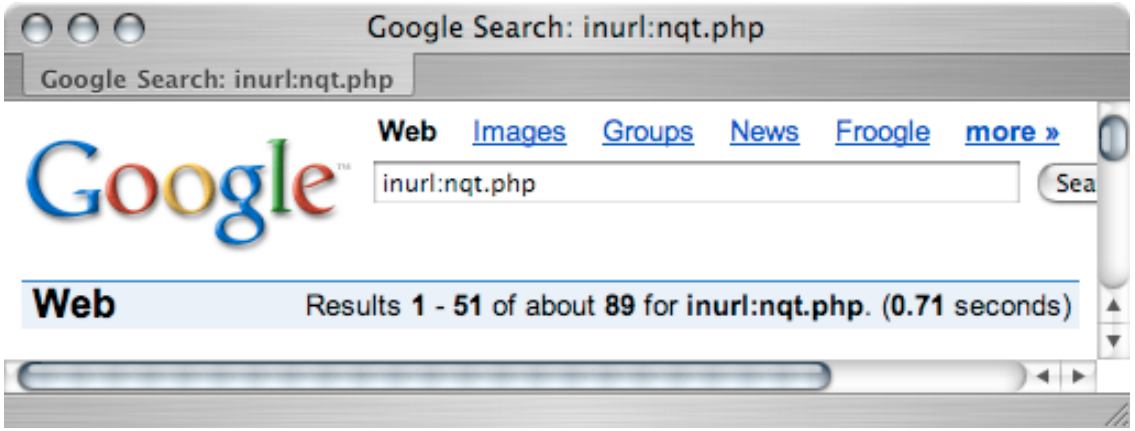
Port Scanning

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



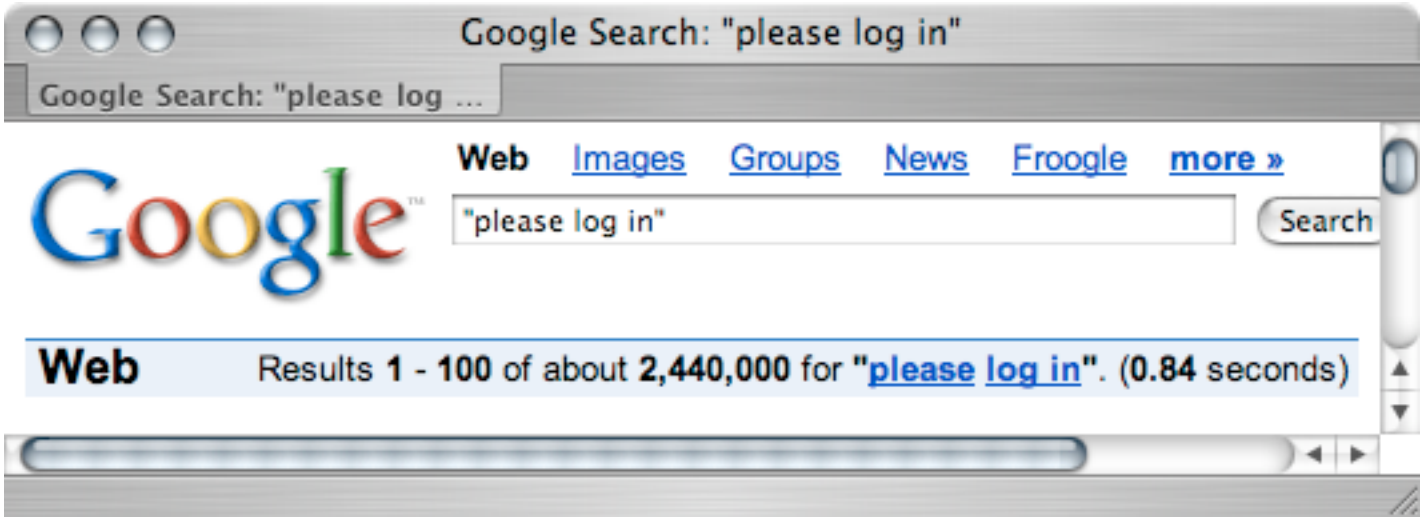
Port Scanning

- 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



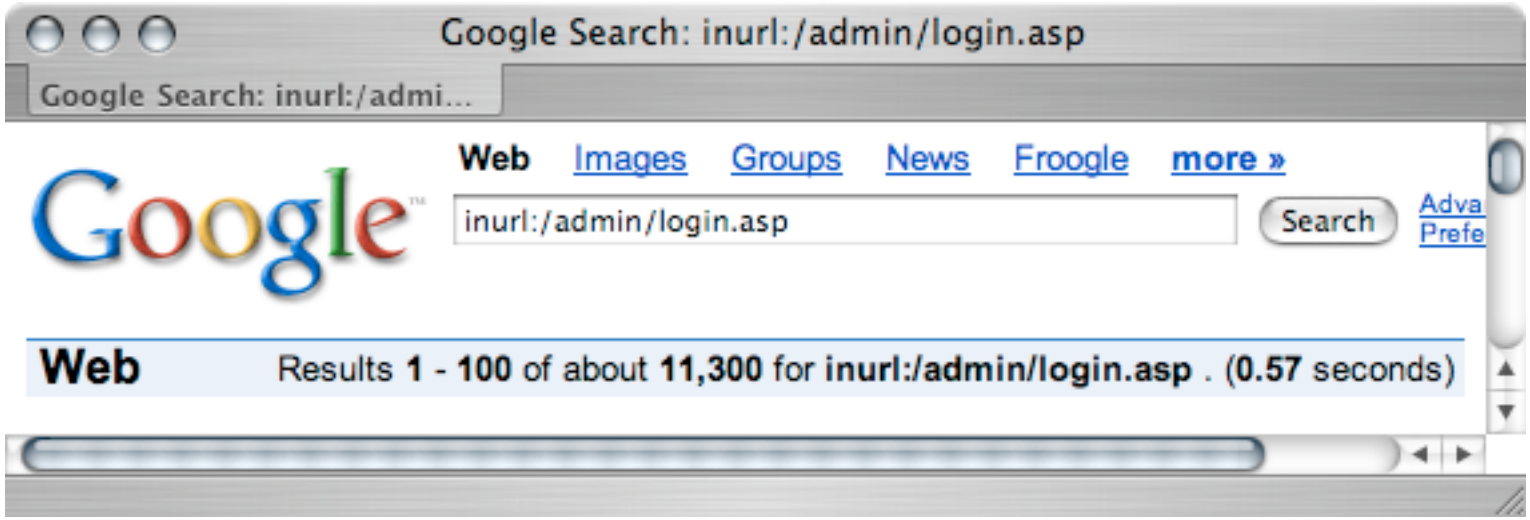
Login Portals

- The most generic of login portals



Login Portals

- Another very generic portal



Login Portals

- Microsoft Outlook Web Access



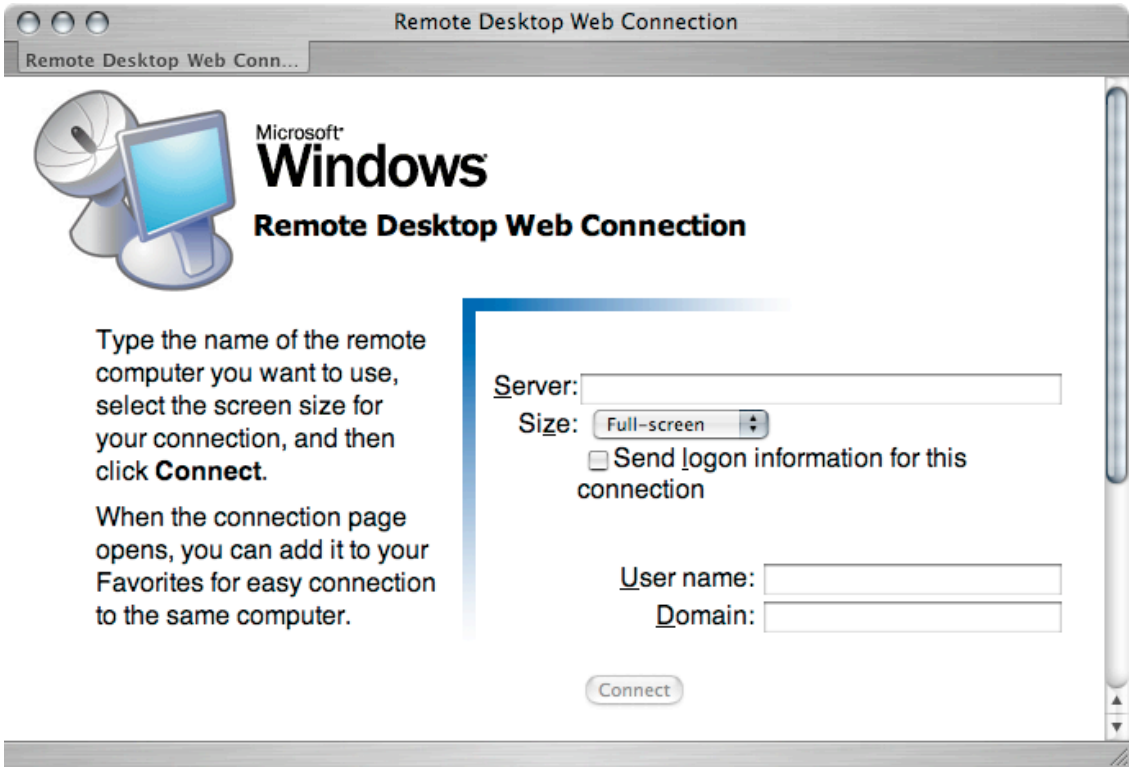
Login Portals

- Coldfusion Admin Page



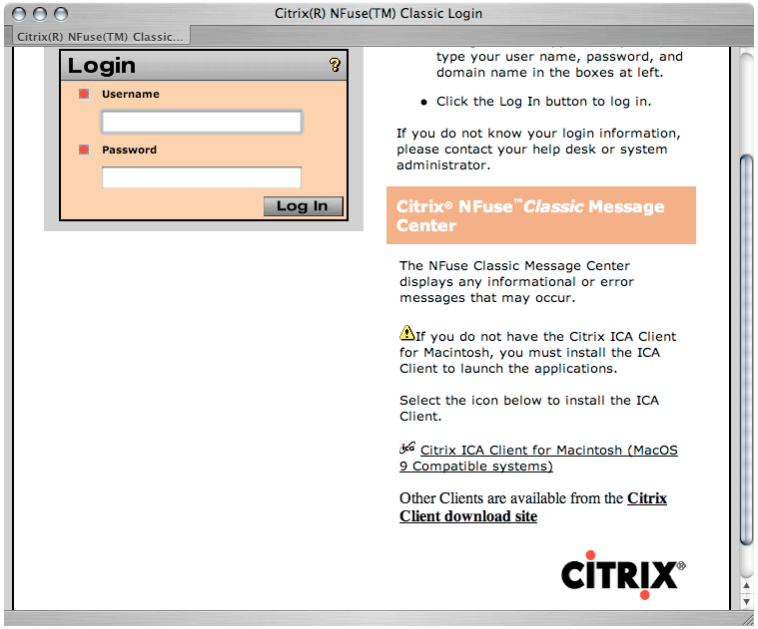
Login Portals

- Windows Remote Desktop



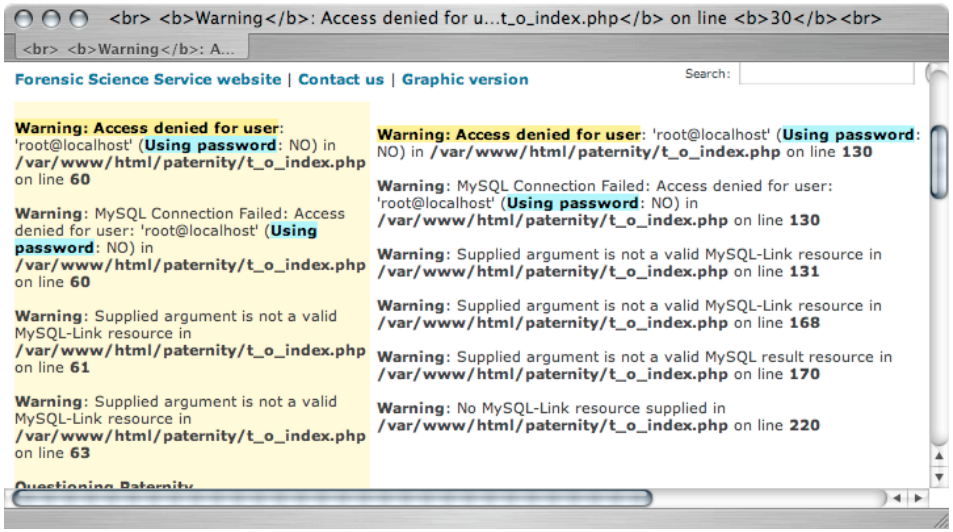
Login Portals

- Citrix Metaframe



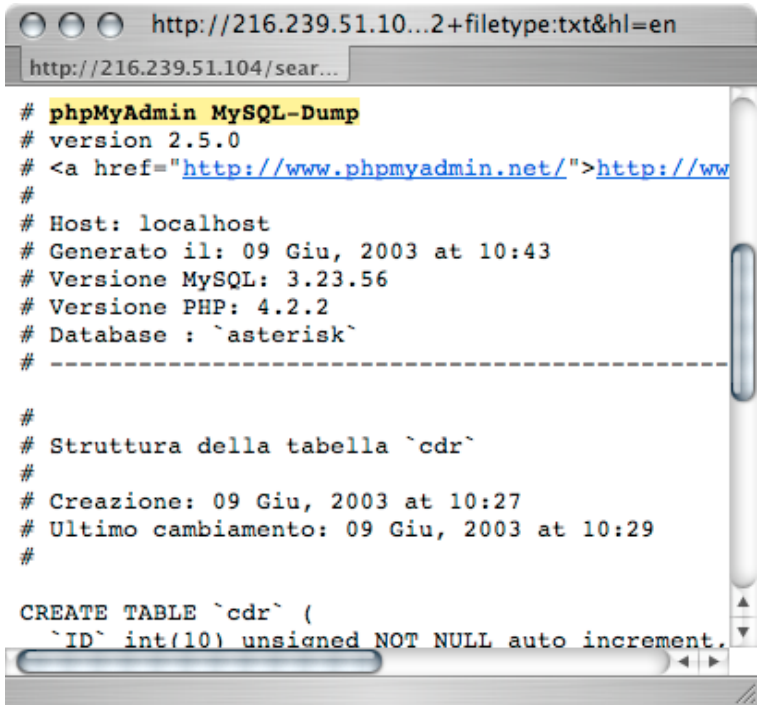
SQL Information

- Gathering SQL usernames is simple with this search



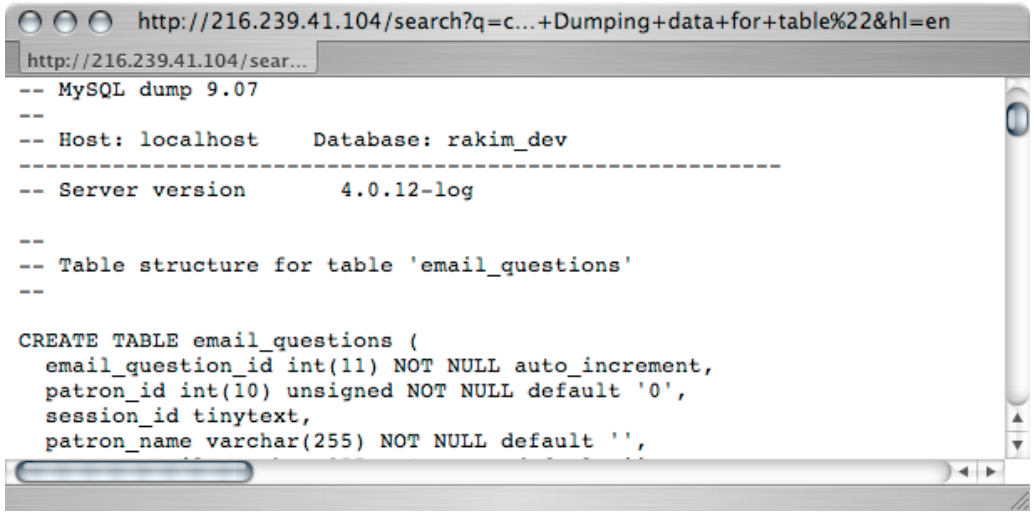
SQL Information

- This is an SQL dump made by phpmyadmin



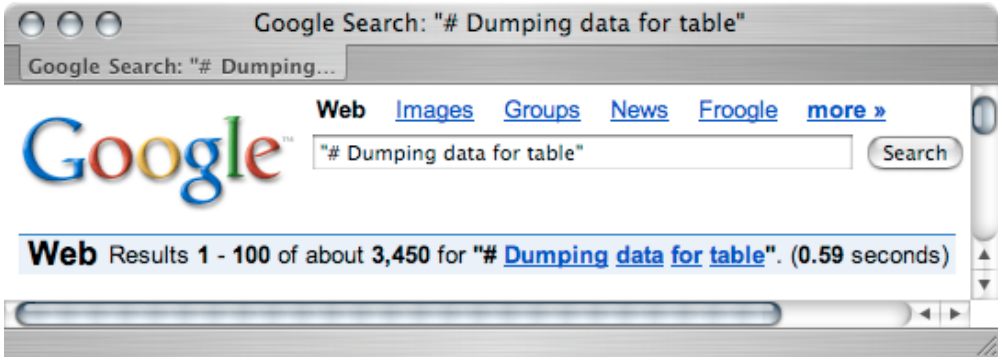
SQL Information

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



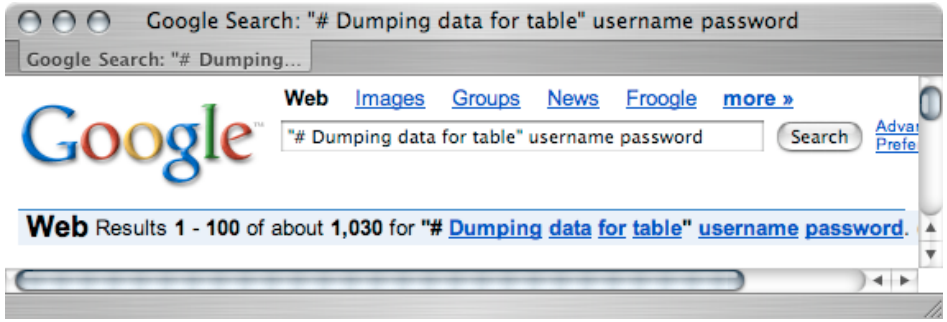
SQL Information

- This query will locate SQL schemas on the web



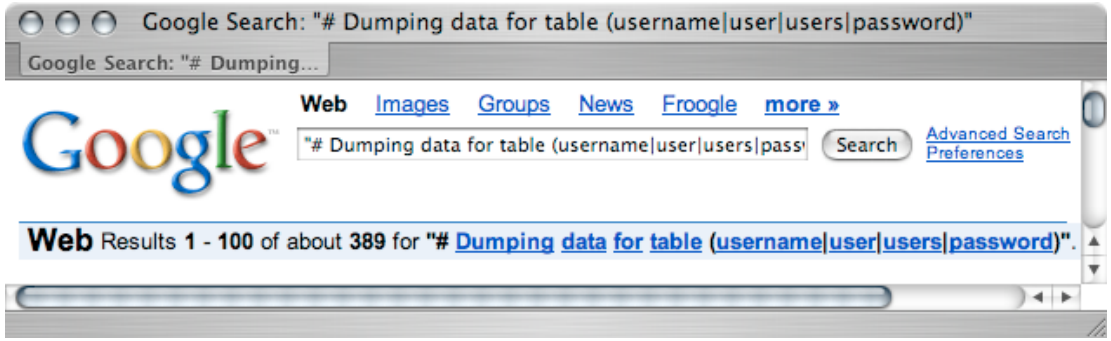
SQL Information

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



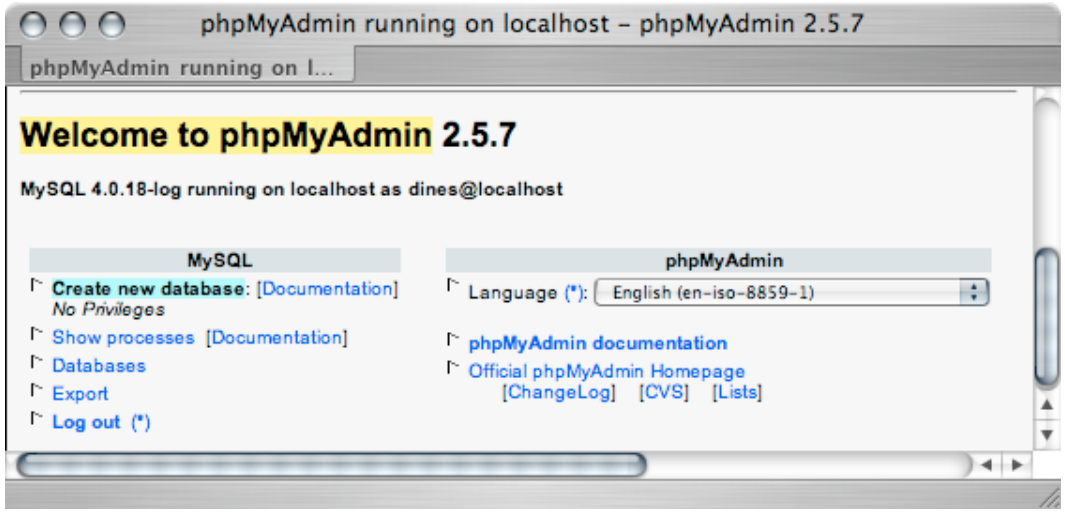
SQL Information

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



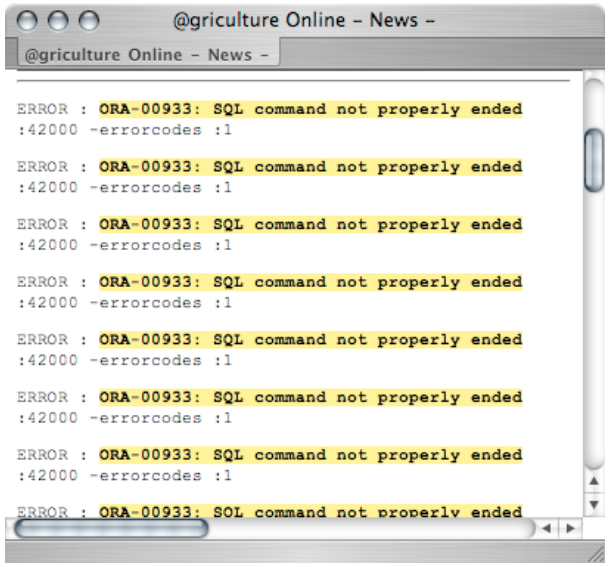
SQL Information

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



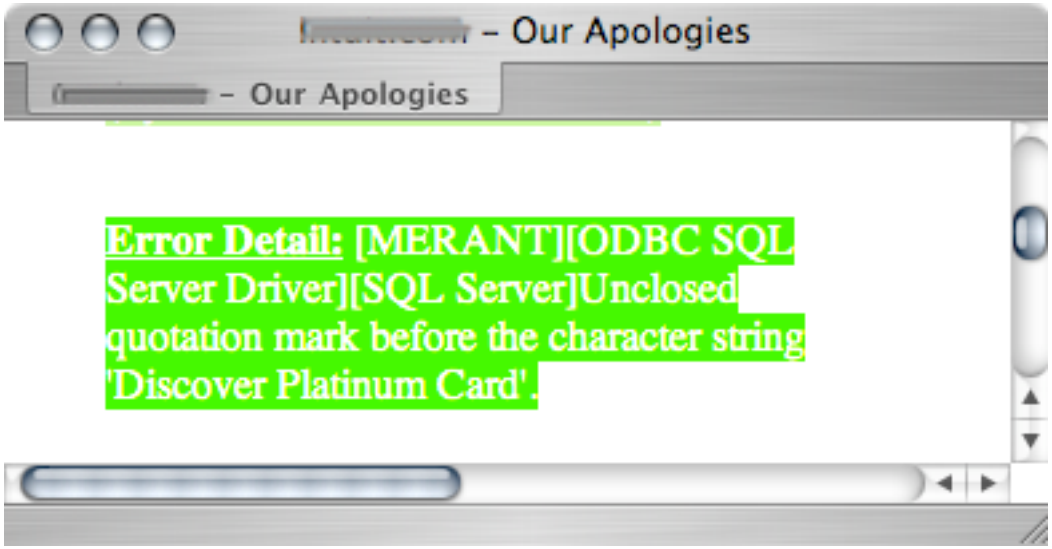
SQL Information

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



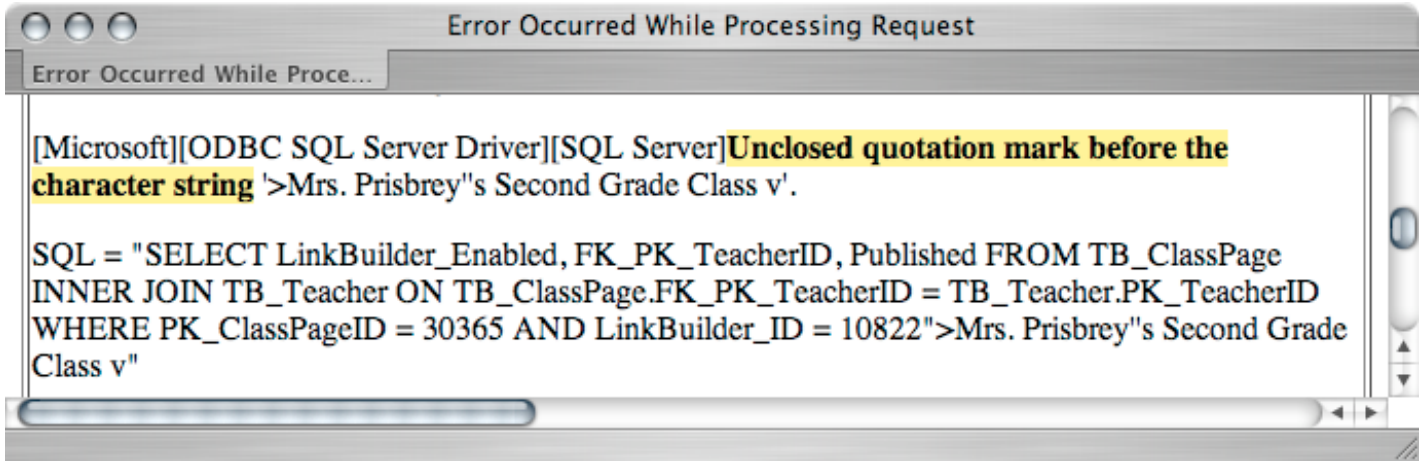
SQL Information

- …another SQL injection target…



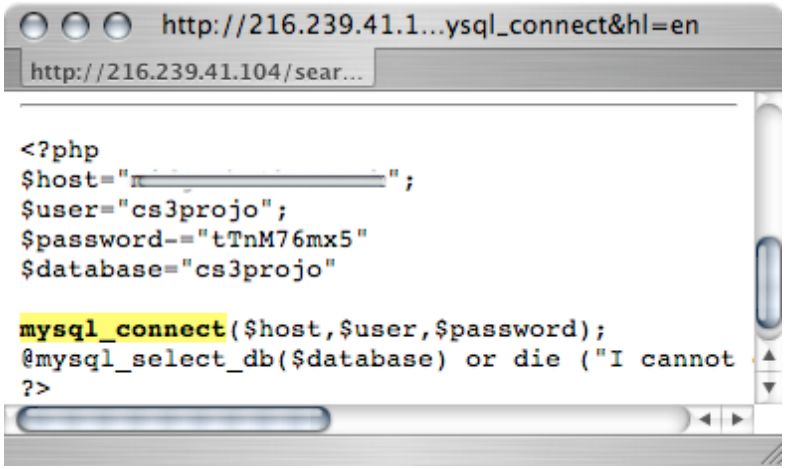
SQL Information

- ..and another…



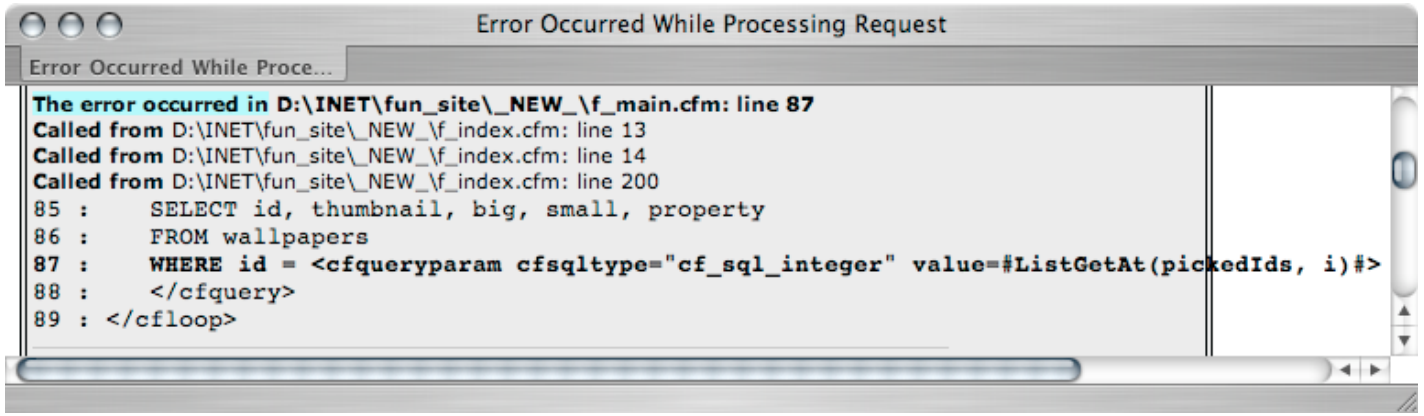
SQL Information

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



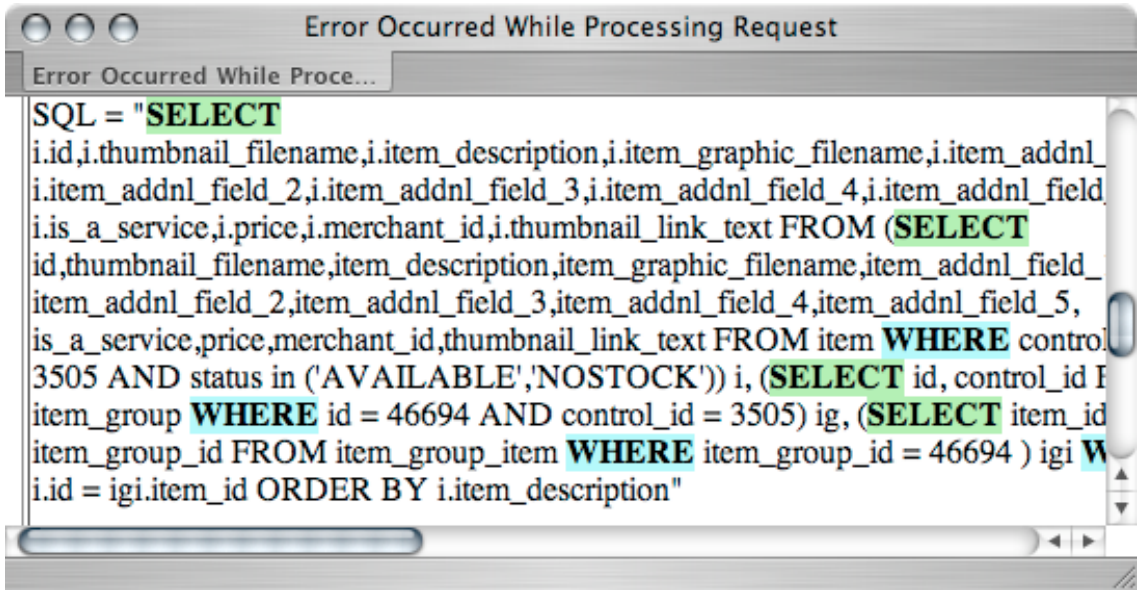
SQL Information

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



SQL Information

- …except for really long lines of SQL code…



Examples

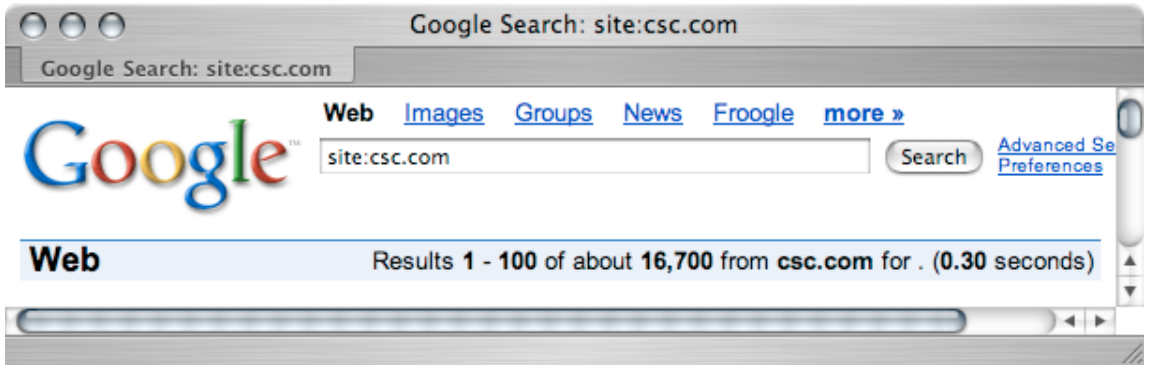
- *** LIVE EXAMPLES REMOVED FROM PRINT VERSION***

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

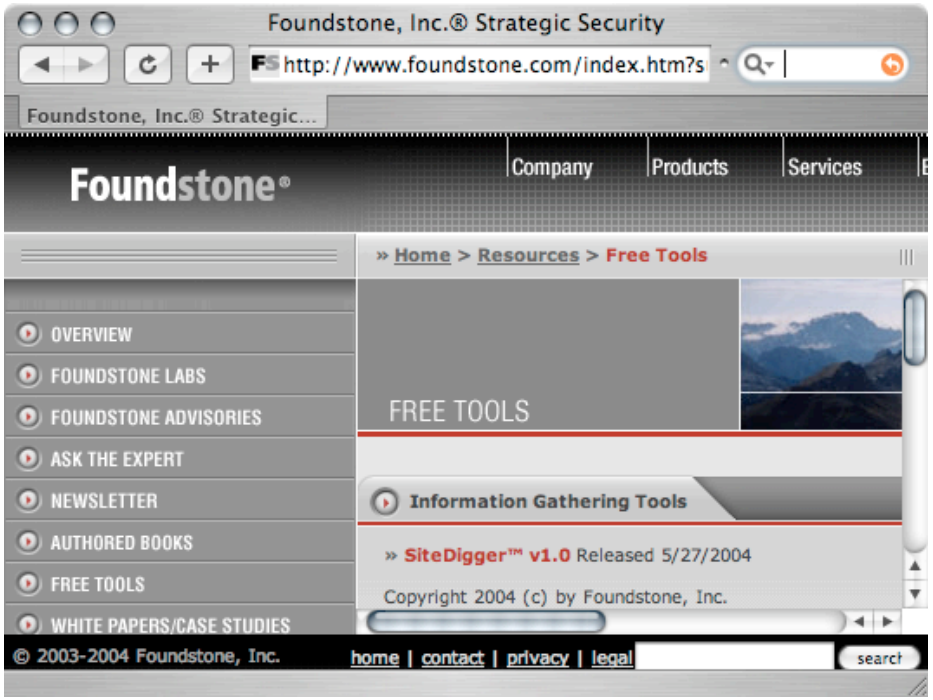
- Use site: queries against each of your web hosts
- Don’t forget about hosts that do not have DNS names



- 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



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.