Exploiting & Defending Against Search Engine Attacks

Nish Bhalla
Founder, Security Compass

Introduction

Nish Bhalla, Application Security Consultant

- Founder, Security Compass
- Over 10 years industry experience
- “Hacking Exposed: Web Applications – IInd”, “Buffer Overflow Attacks: Detect, Exploit & Prevent”, “HackNotes: Network Security” and others.
- Speaker : "Reverse Engineering Conference“ in Montreal, "HackInTheBox" in Malaysia and "ISC2 Security" Conference in Las Vegas, New York etc.
- Developer and Trainer of Application Security Courses
- Brining field work done for various fortune 500 and large software houses into class rooms

Agenda

Web Application Review Methodology

Search Engine Basics

Google Hacking

Web Application Review Methodology

- Threat Analysis
- Architecture Review
- Application Review

Threat Analysis

- What is Threat Analysis?

- Threat Analysis or threat modeling is the process of systematically deriving the **key threats** relevant to an application in order to efficiently **identify** and **mitigate** potential **security weaknesses** before deployment

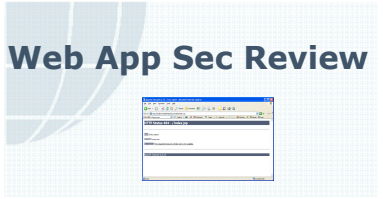
- It is a method to determine the unique threats that an application might face; it is a systematic method of finding security issues in an application by **forcing developers to think like an attacker**

- Security staff can **focus** their resources on the most important issues an application faces after performing this activity

Web Architecture Review

- Design Review: Understand what the thought process was when the application was originally designed
- More often than not the design and the end product are two completely different applications
- Architecture Review: Evaluate the deployed application's architecture and implementation in a real world scenario

Web Application Review



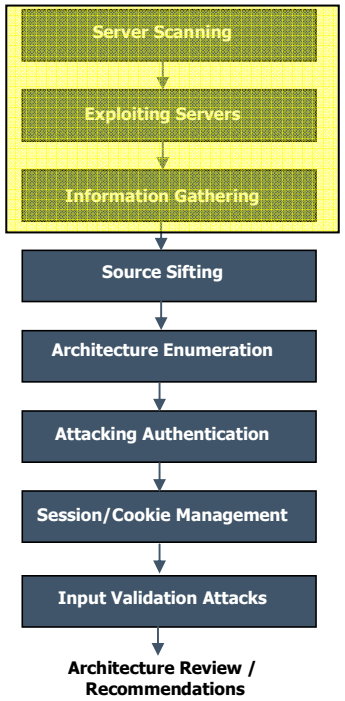
- Web application security reviews determine the security state of a web or eCommerce implementation, identifying potential weaknesses and recommending improvements

- Our methodology breaks web application reviews into the following major steps:

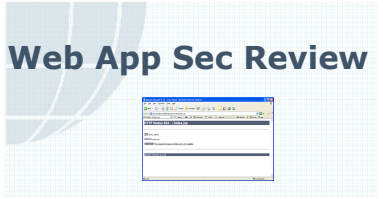
1. Server Scanning- Scan the Internet-facing servers for default installs and missing patches

2. Exploiting Servers- Determine what depth an attacker from the Internet can gain access to in the network by exploiting server vulnerabilities (This step involves running exploits and is taken after coordinating with the client)

3. Information Gathering- Gain a better understanding of the application by browsing the website as a typical user. This includes mirroring the site and searching for information about the application on the Internet ("Google Mining")



Web Application Review



4. Source Sifting- Review the source for key elements such as interesting comments, hard-coded user names, etc.

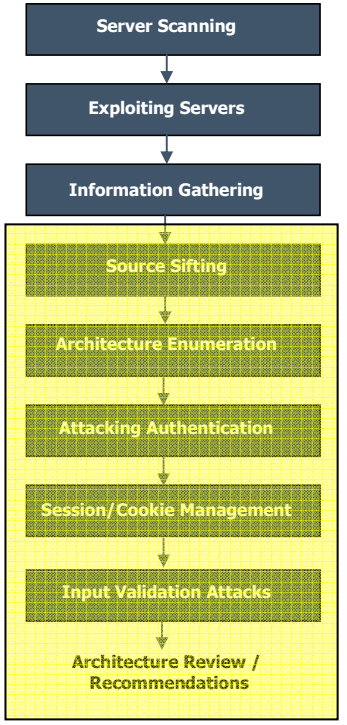
5. Architecture Enumeration- Develop an architecture diagram of the application outlining the technologies used

6. Attacking Authentication- Attempt to brute-force and bypass authentication mechanisms

7. Session / Cookie Management- Attempt to exploit session management vulnerabilities and manipulate client cookies

8. Input Validation Attacks- Input validation is critical to effective application security testing. Not performing input validation in multiple areas could lead to a variety of attacks

9. Architecture Review- Perform an architecture review using all the information gathered



Agenda

Web Application Review Methodology

Search Engine Basics

Google Hacking

PAST / PRESENT / FUTURE ?!

- Passwords
  - Default / no passwords /easy to guess passwords ..
- Misconfiguration
  - default / samples / improper ACLs ..
- Buffer overflows
  - Badly written applications either provided by vendor or otherwise ..
- Web Application Vulnerabilities
  - SQL Injection / XSS ..
- Search Engine
  - Search engines help find all of the above problems and more, much more …

Search Engines

- www.google.com
- www.vivisimo.com
- www.msnsearch.com
- www.yahoo.com
- www.altavista.com
- www.filesearching.com
- www.archive.org

Search Engines - Information

There is too much information on the web. There have been multiple attempts to organize this information using search engine technologies.

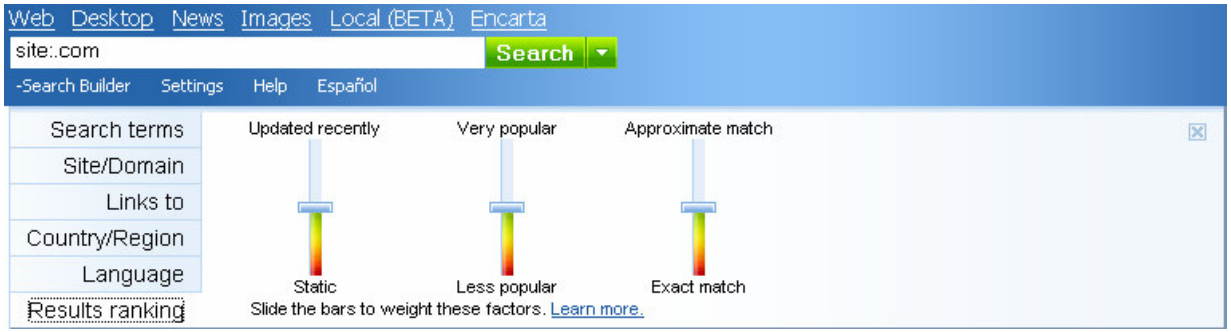
Yahoo uses directory service

Metacrawler uses metatags

Google/Msn use keywords and links

Search Engine - Basics

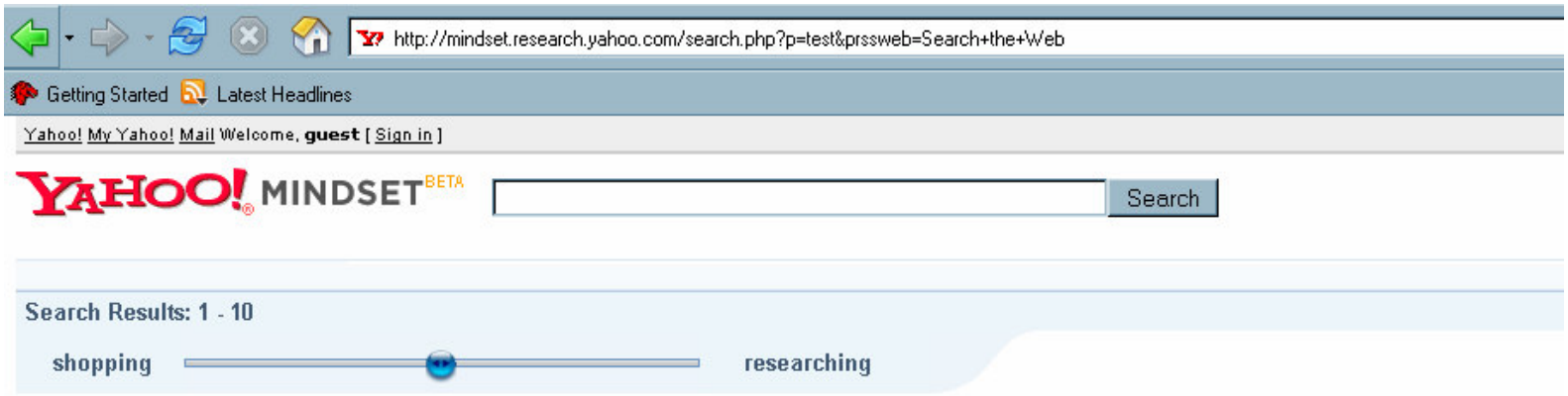
- Basic Searching Techniques (MSN)
  - Site:
  - Search All the terms/any of the terms/exact phrase



Search Engine - Basics

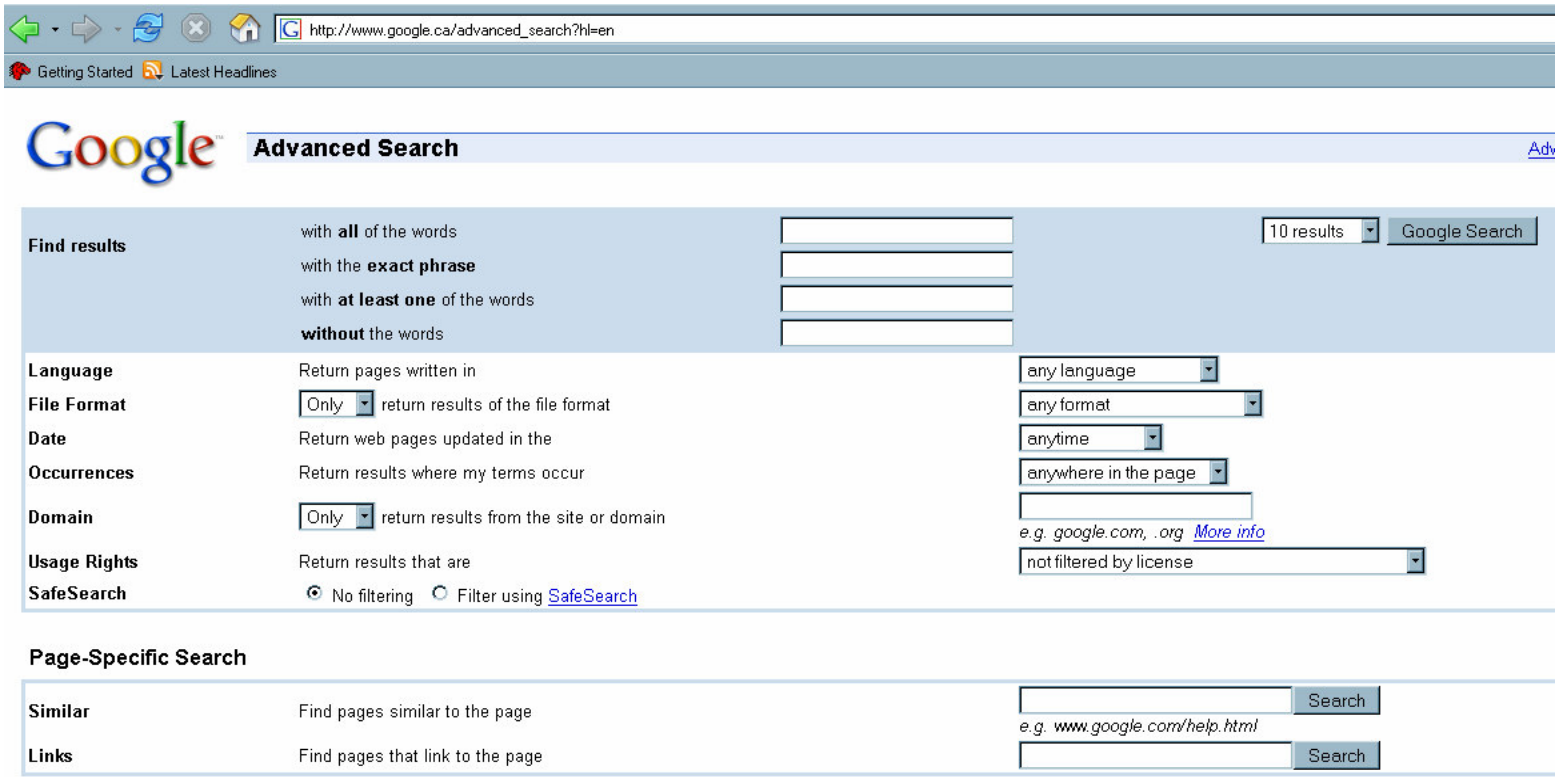
- Basic Searching Techniques (Yahoo)
  - intitle:
  - inurl:
  - Advanced: Filetype / Update Past few months / File Format

- http://mindset.research.yahoo.com/



Search Engine - Basics

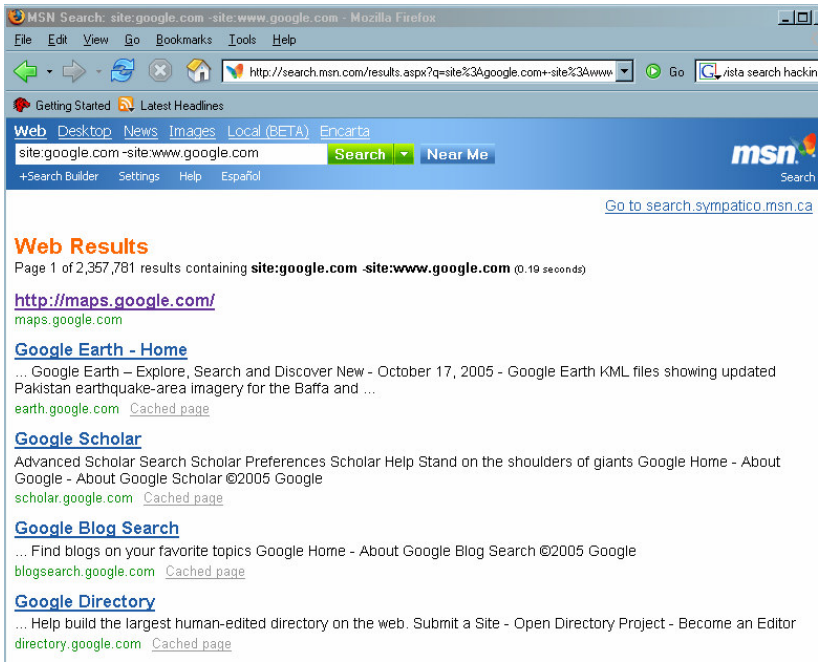
- Basic Searching Techniques (Google)
  - Site:
  - Filetype:
  - Daterange:
  - Numrange:

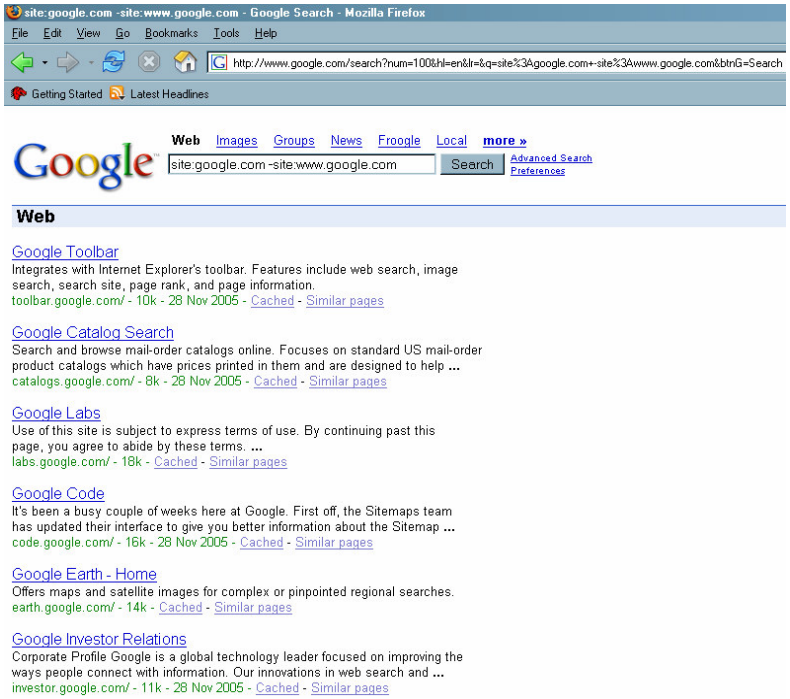


Search Engine - Basics

link:www.securitycompass.com

site:google.com –site:www.google.com

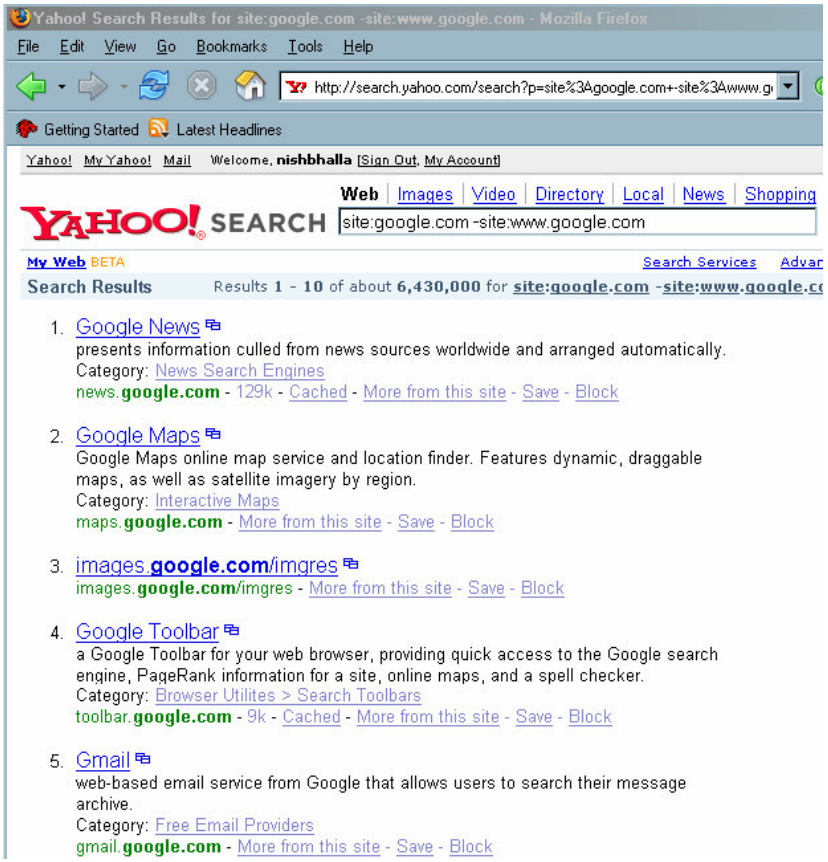


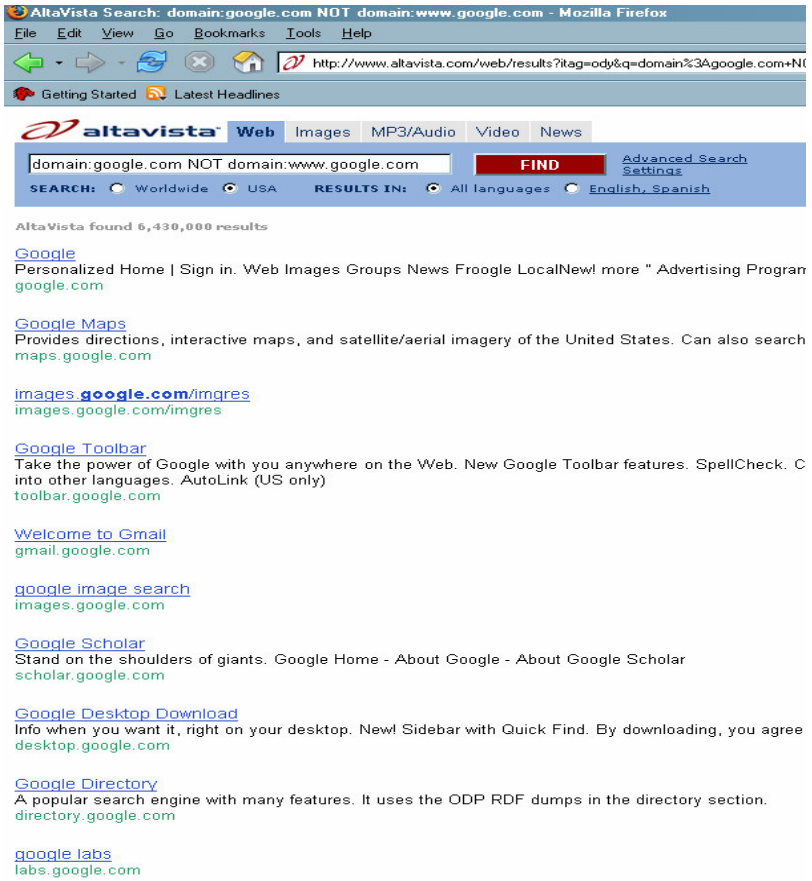


Search Engine - Basics

link:www.securitycompass.com

domain:google.com NOT domain:www.google.com





Agenda

Web Application Review Methodology

Search Engine Basics

Google Hacking

Search Engine - “Google Hacking”

- All about knowing how to search.

- Lets see some examples with various search engines.
- Agenda:
  - Port Scan
  - Server Identification / Profile (IIS/Apache/Tomcat/..)
  - Gather Information
  - Vulnerability Scan Reports (Information left by auditors / hackers for us).
  - Find other points of entry (Login Portals / Terminal Servers)
  - Database Injection
  - Devices (Firewalls/Routers/Virus/Phone/Webex/Print)

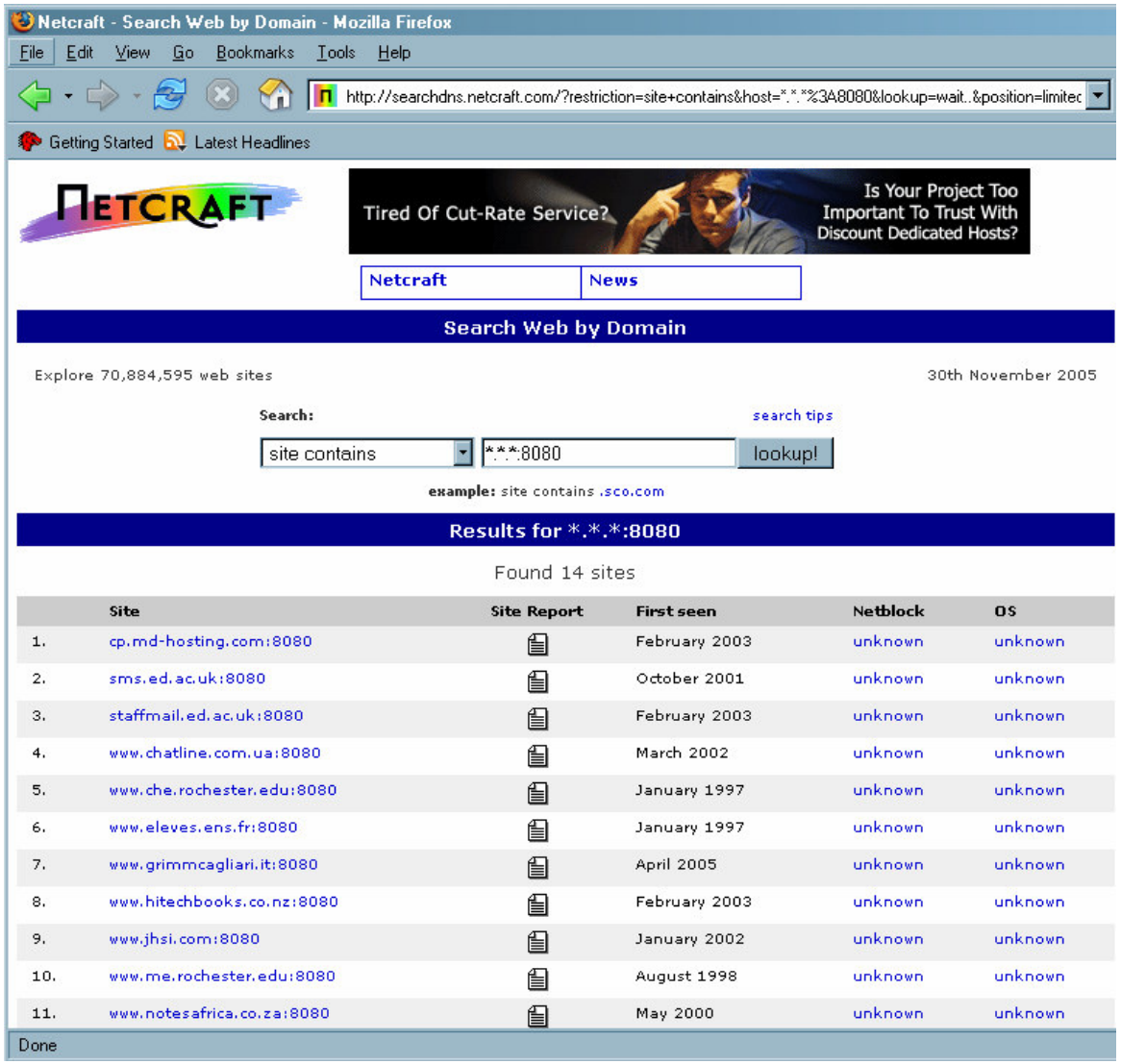
Port Scan

- Port Scan
  - inurl:8080
  - inurl:8081
  - inurl:2506/jana-admin
  - inurl:21
  - inurl:3889
  - (inurl:8888 | inurl:8889)
  - (inurl:81-cobalt | inurl:cgi-bin/.cobalt)
  - url:8080

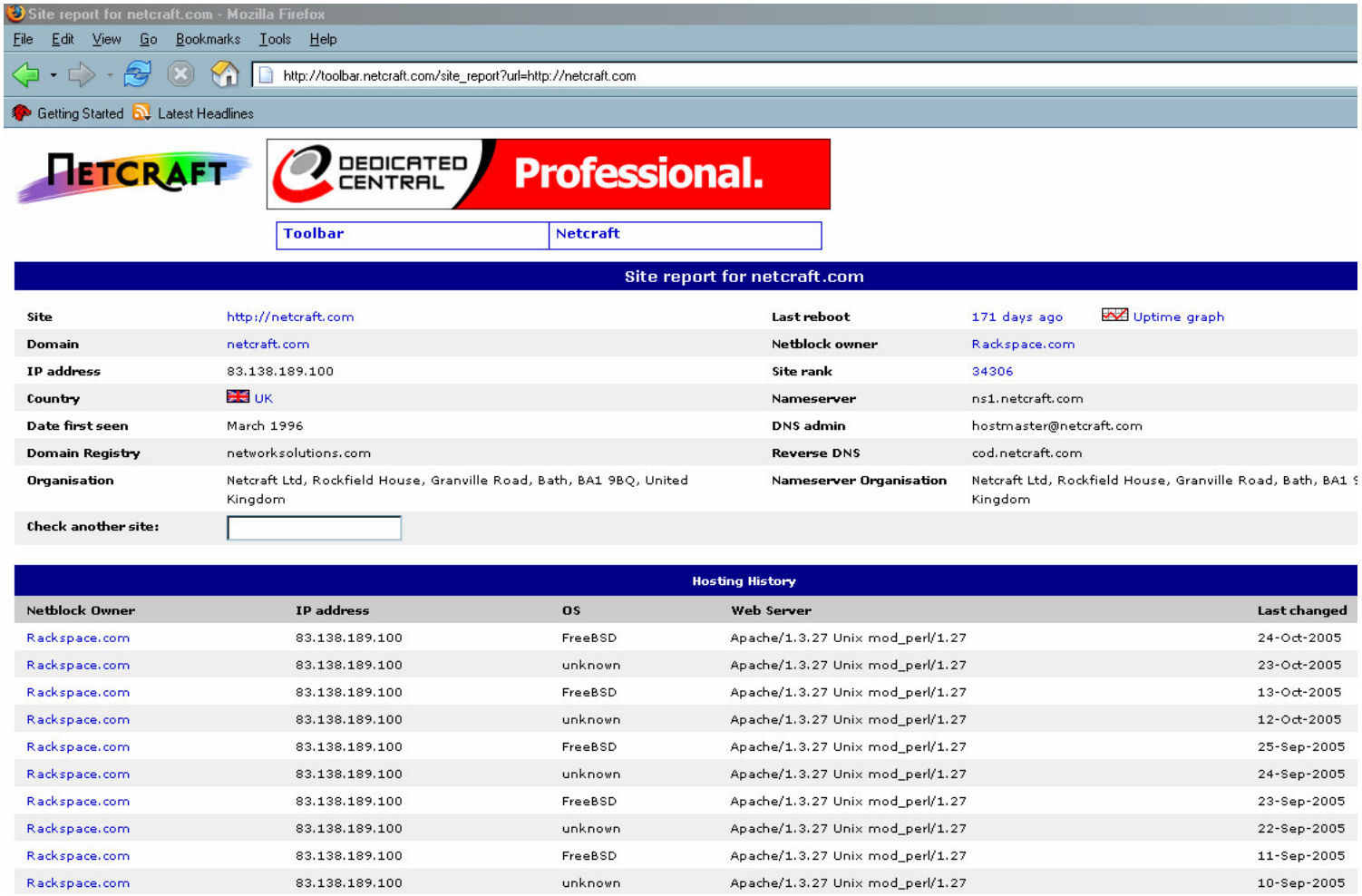
Note:
pipe | or the keyword OR depends on search engine
url or the inurl depends on search engine

Port Scan

Then there is
www.netcraft.com



Server Identification



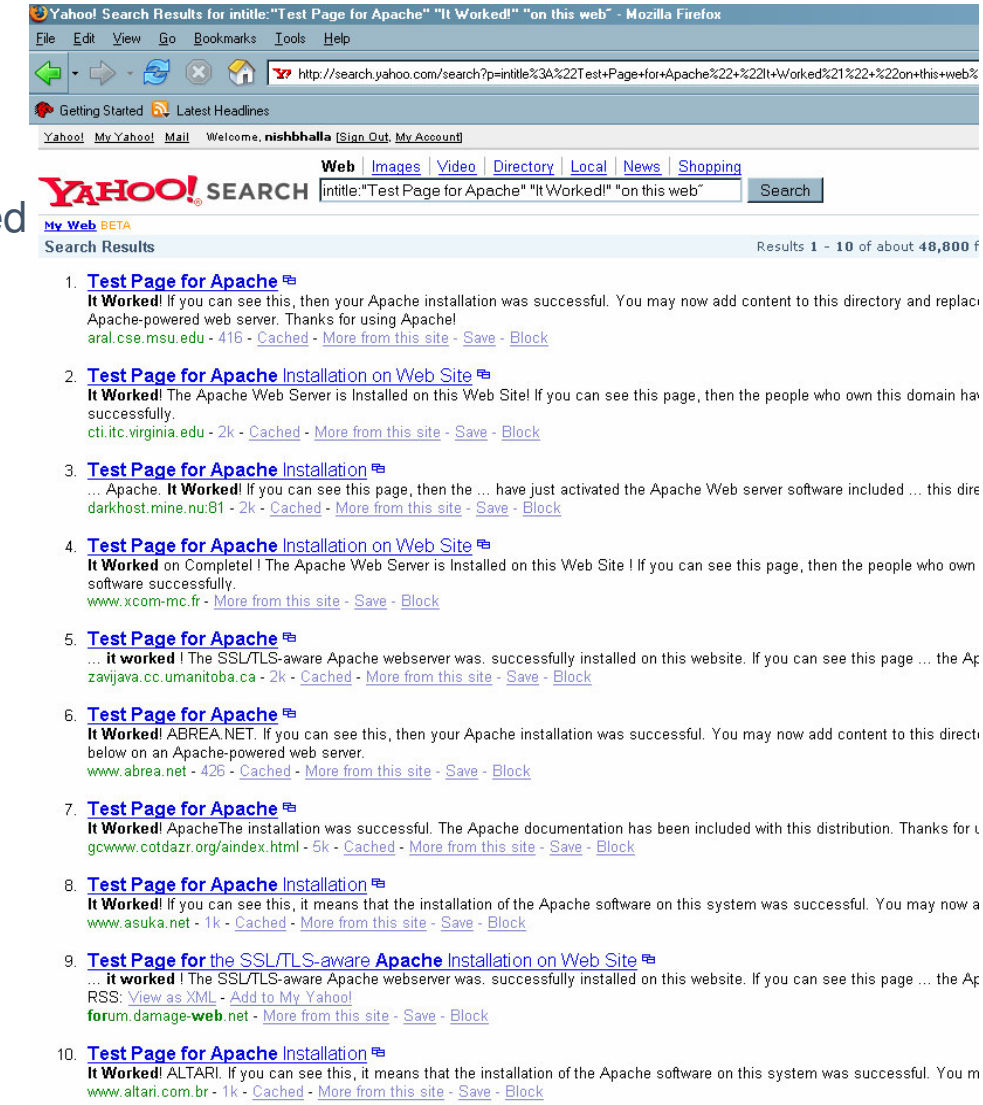
Server Identification

"Microsoft-IIS/5.0 server at"

"JRun Web Server" intitle:index.of

"OmniHTTPd/2.10" intitle:index.of

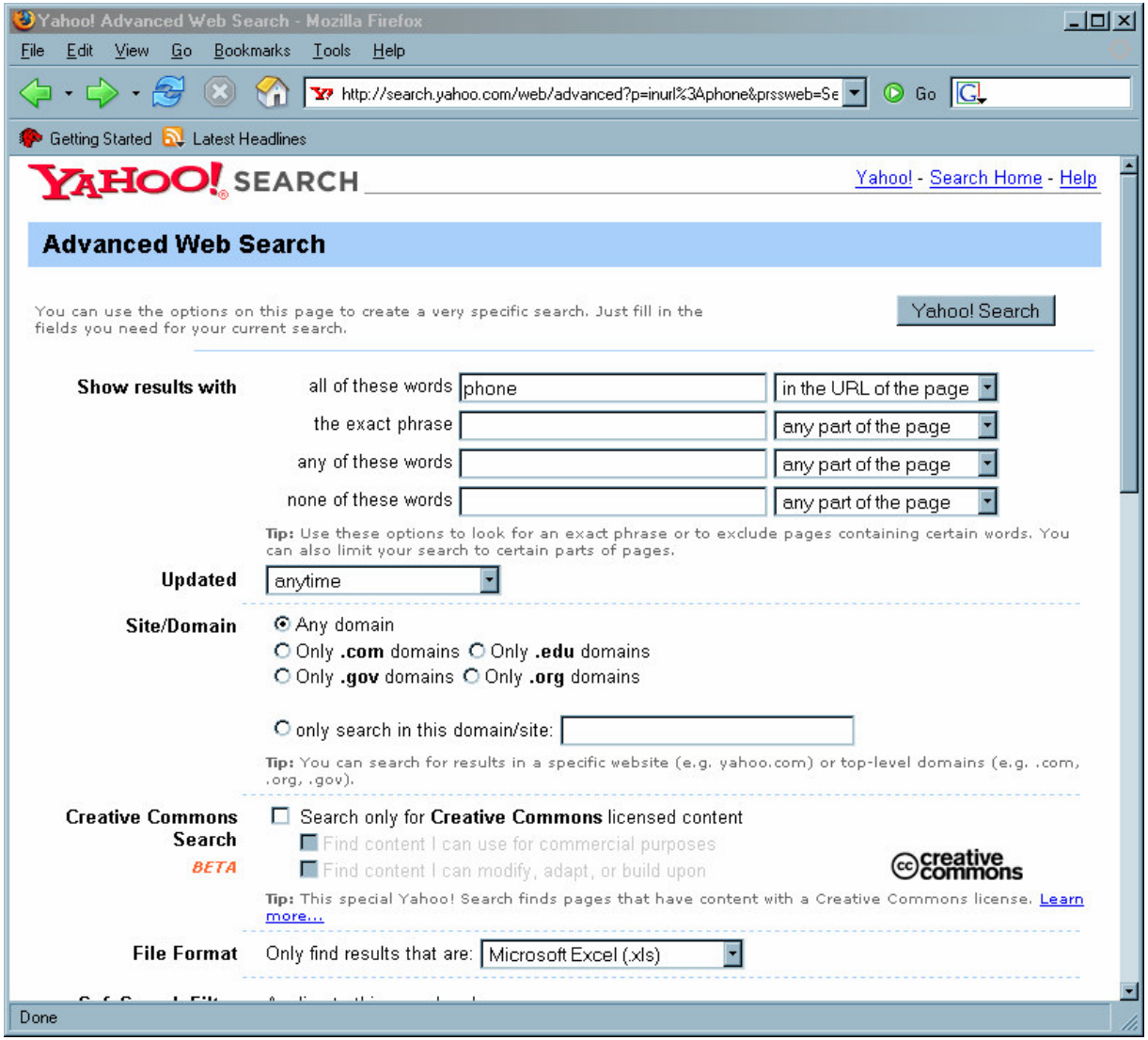
intitle: “Test Page for Apache” “It Worked” “on this web”



Gather Information

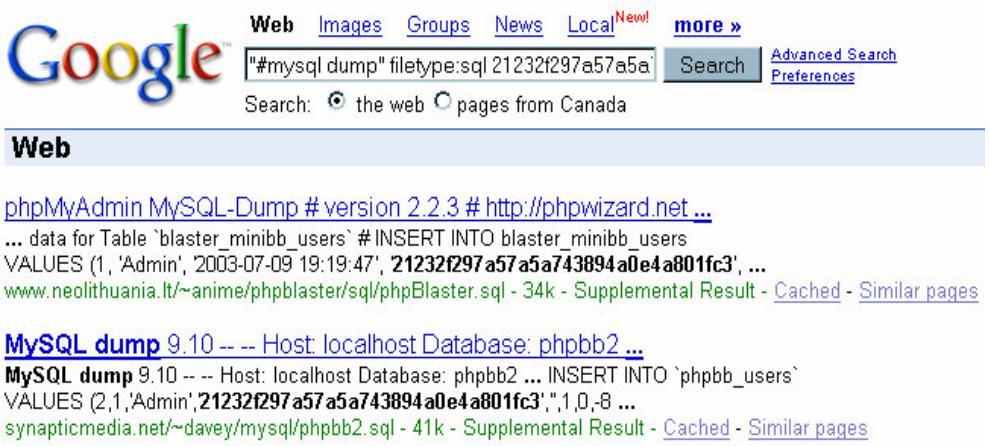
- File Format: xls
- phone | contact | Email
- @securitycompass.com

- Phone Book Search Through whitepages.com / yellowpages.com or google
- pb=f&q=(555)+555-5555



Gather Information

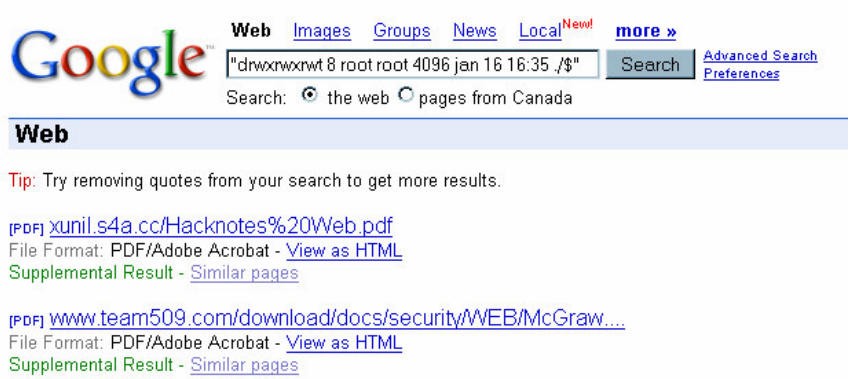
- Directories:
  - "index of cgi-bin“
  - intitle:"Index of /CFIDE/" administrator
  - "index of/" "ws_ftp.ini" "parent directory"
- Files:
  - filetype:pst inurl:"outlook.pst“
  - allinurl:"/.htaccess" filetype:htaccess
  - "#mysql dump" filetype:sql 21232f297a57a5a743894a0e4a801fc3
  - "#-FrontPage-" inurl:service.pwd
  - "not for distribution" confidential
  - ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:confidential salary | intext:"budget approved") inurl:confidential

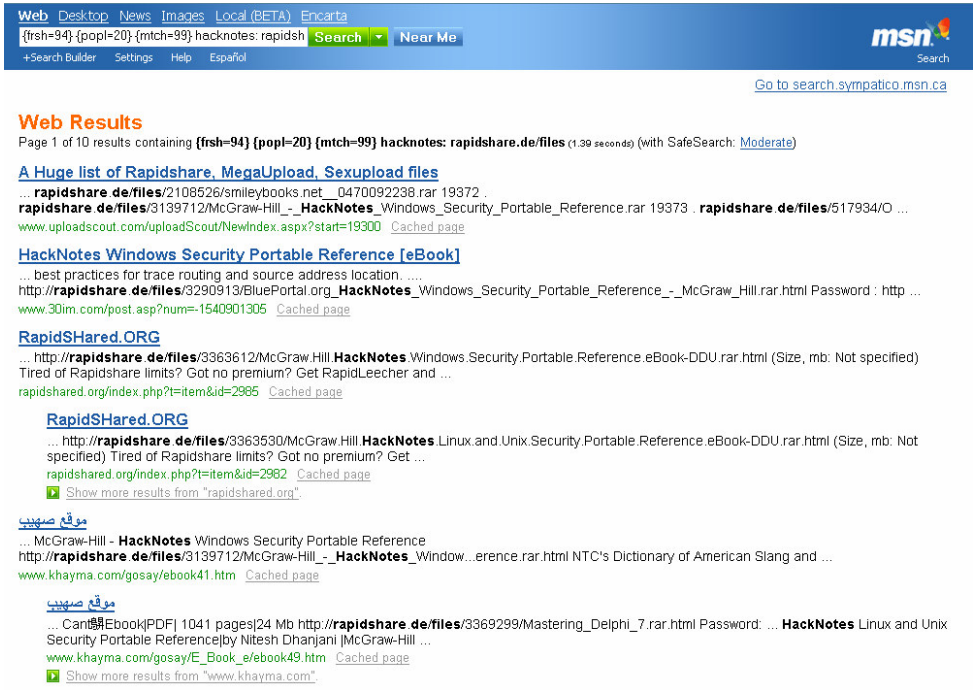


Gather Information

- What about books or mp3 which is illegal to download Kaza / emule /e-donkey and other P2P software OR
- Contents of books "drwxrwxrwt 8 root root 4096 jan 16 16:35 ./$“
- MSNSearch

{frsh=94} {popl=20} {mtch=99} hacknotes: rapidshare.de/files





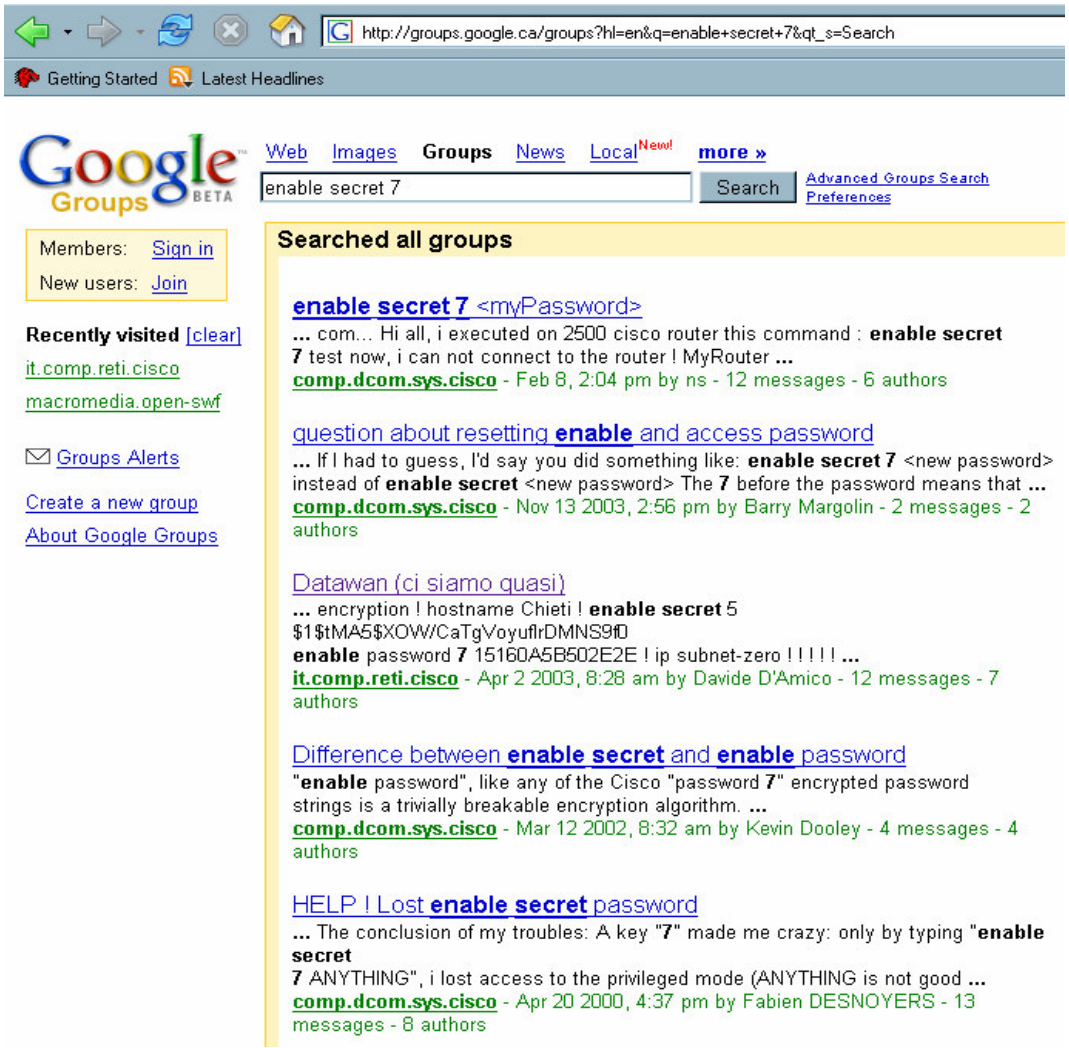
Gather Information

groups.google.com

- System configuration
- Resumes
- Troubleshooting apps
- Coding issues

Decryptor

- http://www.alcrypto.co.uk/cisco/



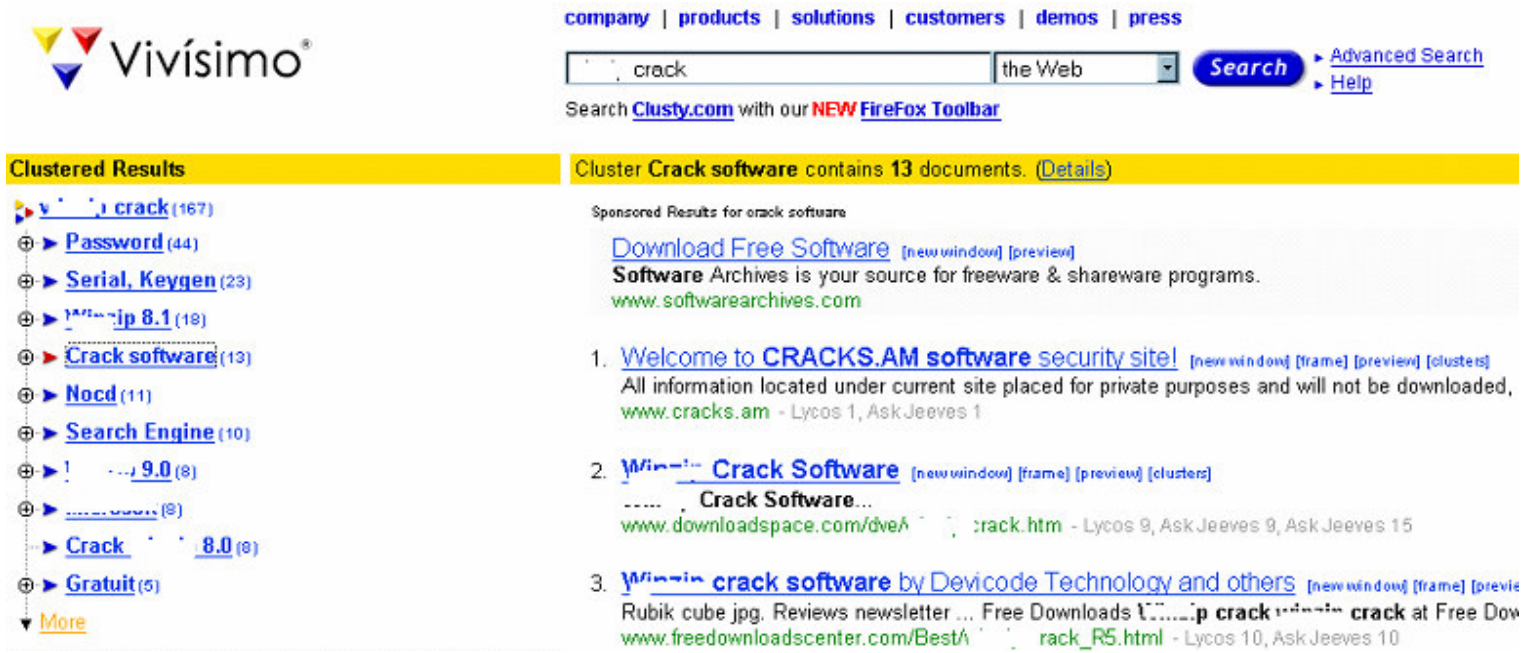
P2P Search

Google

- (intitle:"index of")+("/ebooks"|"/book") +(chm | pdf)
- intitle:"index of" AND ("wares" | "warez" | "appz" | "gamez" | "cracked") ("nfo" OR "rar" OR "zip") “parent directory“

YAHOO

- intitle:"index of" intitle:"/music" mp3 OR mov OR avi OR asf OR asx OR avi OR wav OR wma -htm -html -asp -aspx -jsp –php



Vulnerability Scan Reports

Hackers and Auditors to the rescue.

- intitle:"Nessus Scan Report" "This file was generated by Nessus“
- "Host Vulnerability Summary Report"

File Edit View Go Bookmarks Tools Help

http://www.infosecwriters.com/projects/osscan/sp3.htm

Getting Started Latest Headlines

This scan was performed using Nessus 2.0 and NMAP.

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these th

Hosts which where alive and responding during test	1
Number of security holes found	4
Number of security warnings found	15

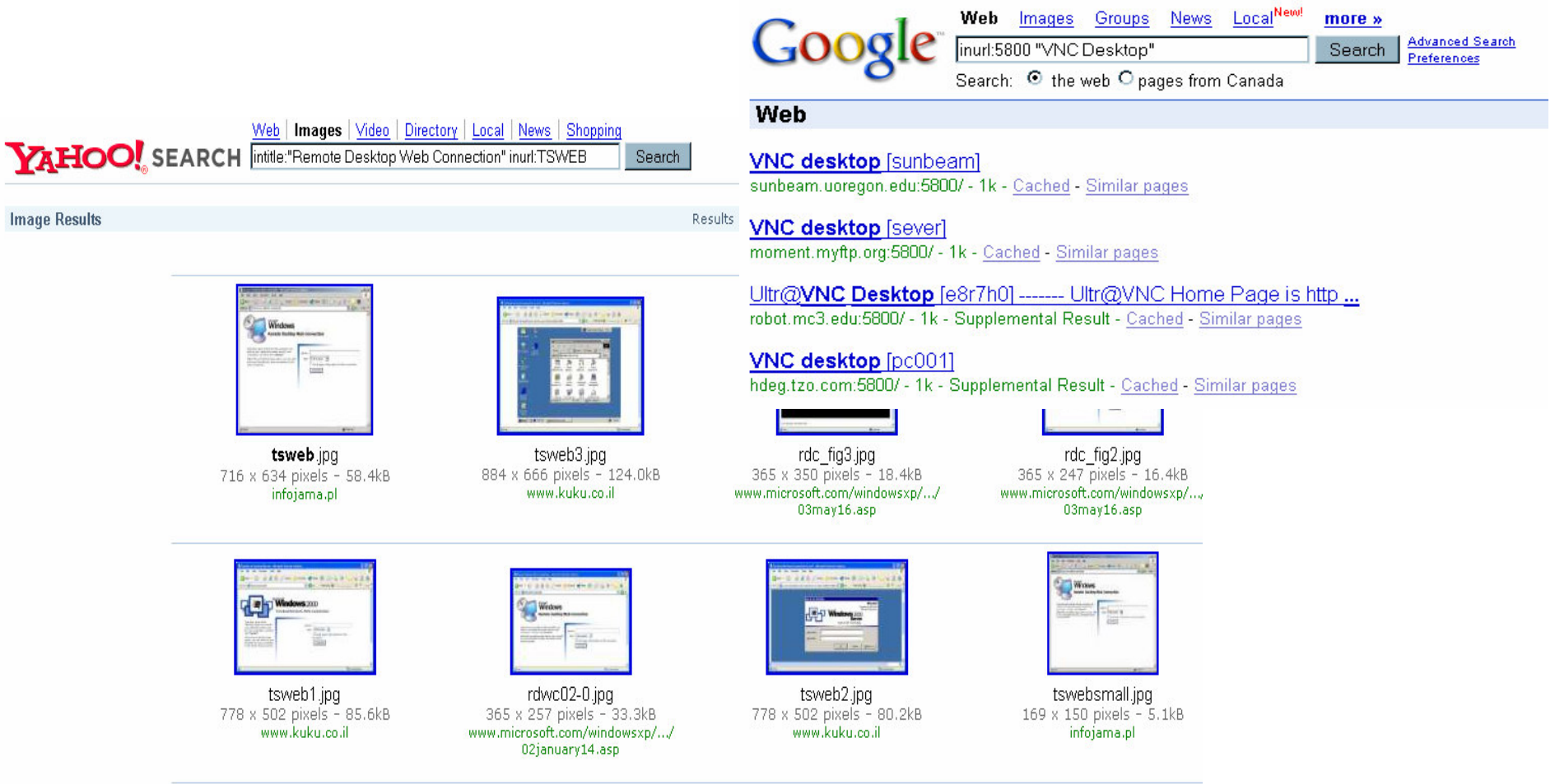
Host(s)	Possible Issue
151.108.232.190	Security hole(s) found

[return to top]

Address of Host	Port/Service	Issue regarding Port
151.108.232.190	smtp (25/tcp)	Security notes found
151.108.232.190	http (80/tcp)	Security hole found
151.108.232.190	loc-srv (135/tcp)	Security warning(s) found
151.108.232.190	netbios-ssn (139/tcp)	Security hole found
151.108.232.190	https (443/tcp)	Security notes found
151.108.232.190	microsoft-ds (445/tcp)	Security notes found
151.108.232.190	LSA-or-nterm (1026/tcp)	Security notes found
151.108.232.190	NFS-or-IIS (1025/tcp)	Security notes found
151.108.232.190	ms-lsa (1029/tcp)	Security notes found
151.108.232.190	unknown (2803/tcp)	Security notes found
151.108.232.190	msdtc (3372/tcp)	Security notes found
151.108.232.190	general/udp	Security notes found
151.108.232.190	general/icmp	Security warning(s) found
151.108.232.190	general/tcp	Security warning(s) found
151.108.232.190	netbios-ns (137/udp)	Security warning(s) found
151.108.232.190	iad1 (1030/udp)	Security notes found
151.108.232.190	unknown (1027/udp)	Security notes found

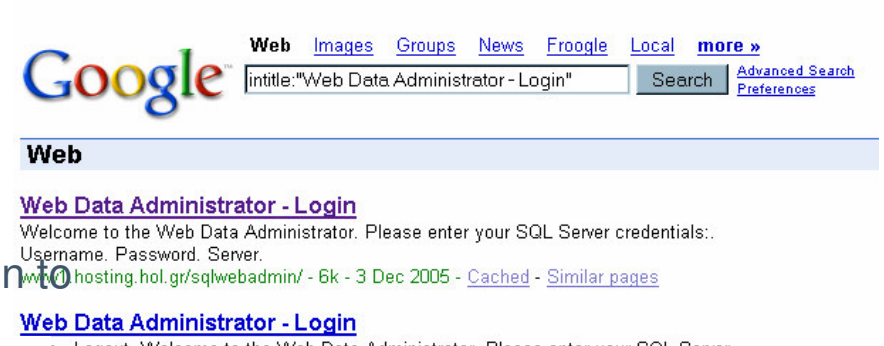
Login Portals

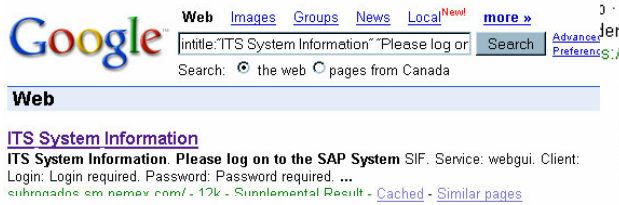
- VNC / Remote Desktop are some of the common remote connection services used to connect to internal systems.

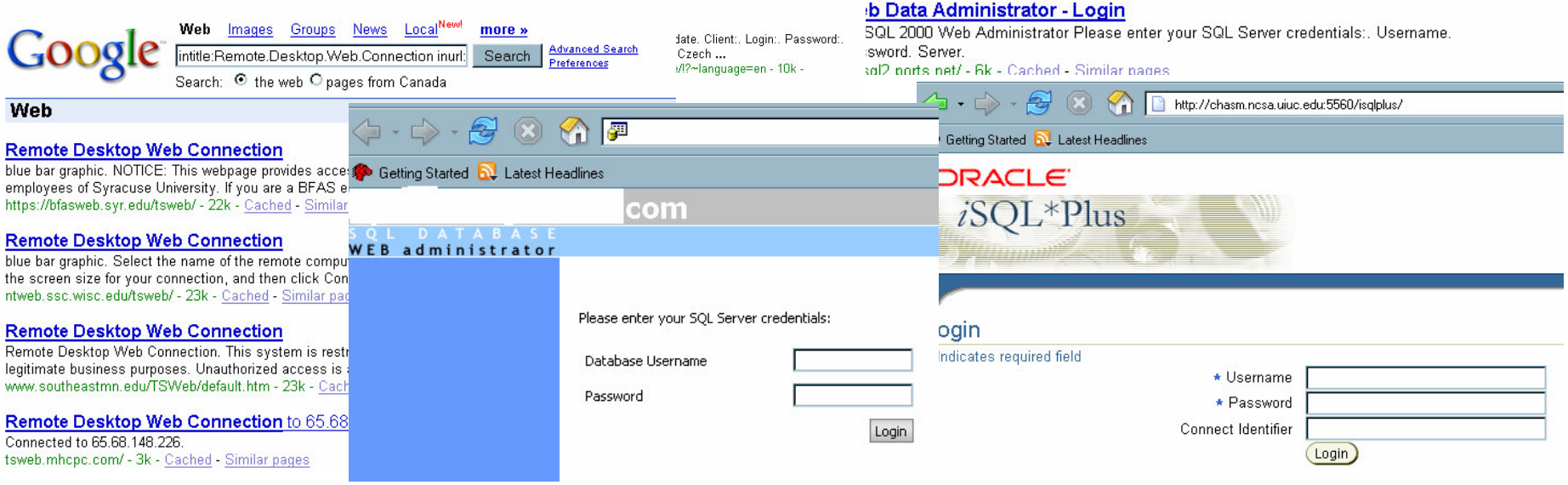


Login Portal

- Intitle:" Web Data Administrator – Login"
- "iSQL*Plus Release“
- intitle:Remote.Desktop.Web.Connection inurl:tsweb
- intitle:"ITS System Information" "Please log on to the SAP System"







Database Error

- "[SQL Server Driver][SQL Server]Line 1: Incorrect syntax near" -forum -thread – showthread
- "ORA-12541: TNS:no listener" intitle:"error occurred“
- “MySQL error with query”

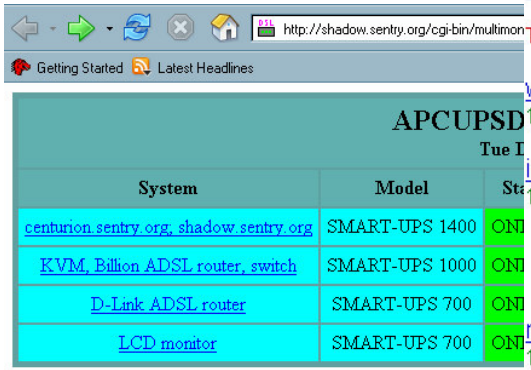
Devices

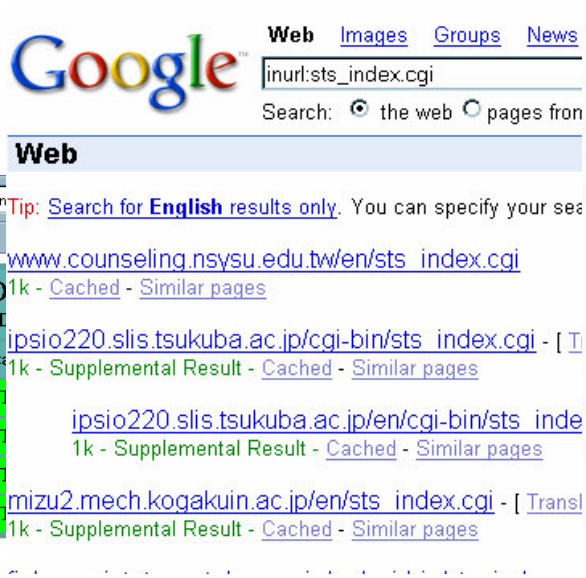
Webcam

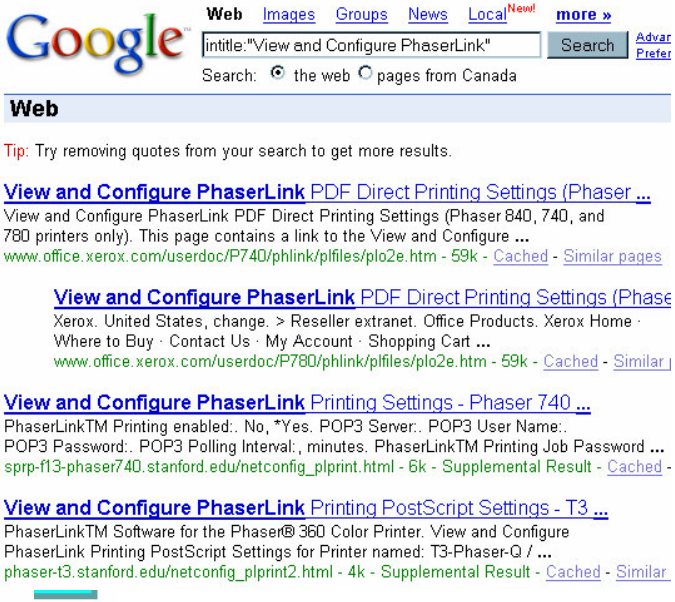
- intitle:snc-z20 inurl:home/
- inurl:indexFrame.shtml Axis

Printers

- inurl:sts_index.cgi
- intitle:"View and Configure PhaserLink" Power
- intitle:multimon UPS status page PBX
- intitle:"start.managing.the.device" remote pbx access







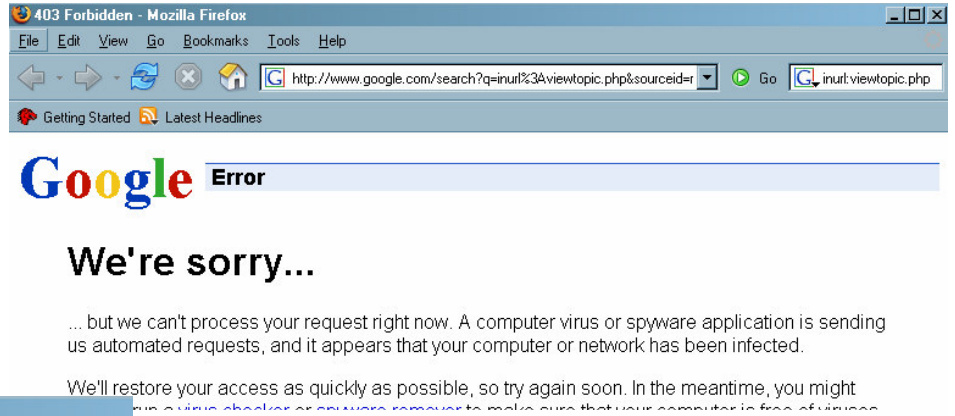
Misc

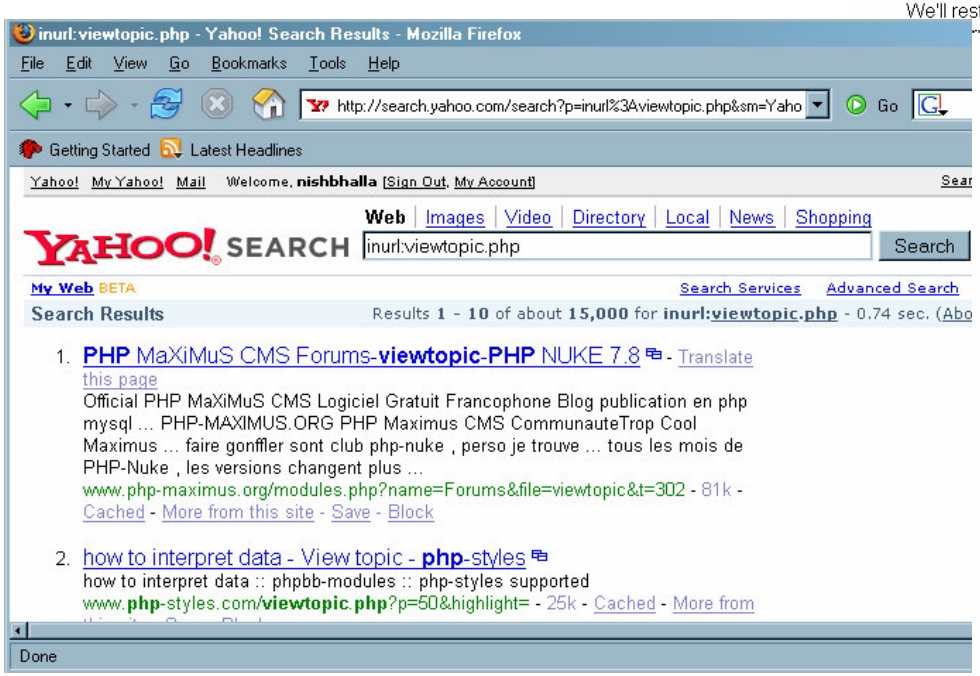
Google blocks some searches

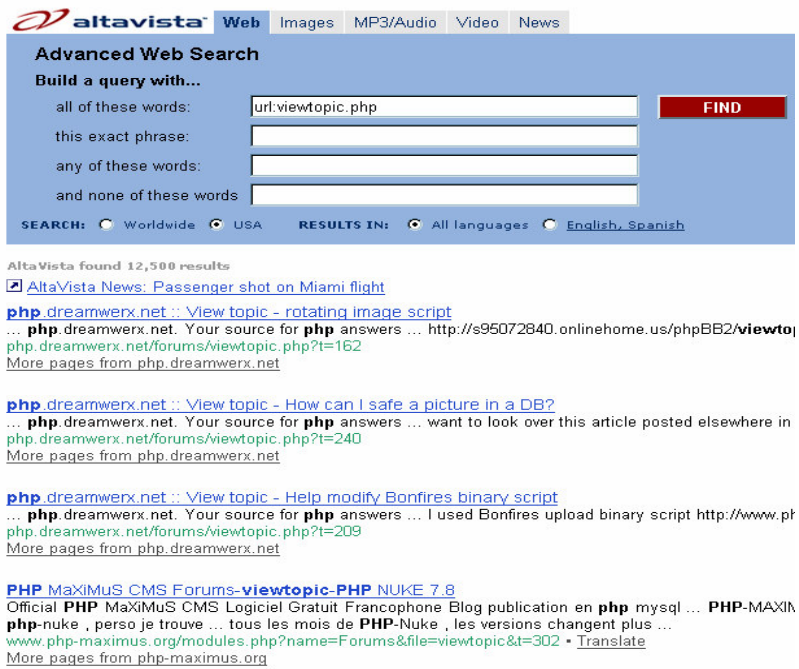
- Inurl:viewtopic.php

But there are other search engines which will respond like yahoo altavista vivisimo.

- Inurl:viewtopic.php







Search Engines

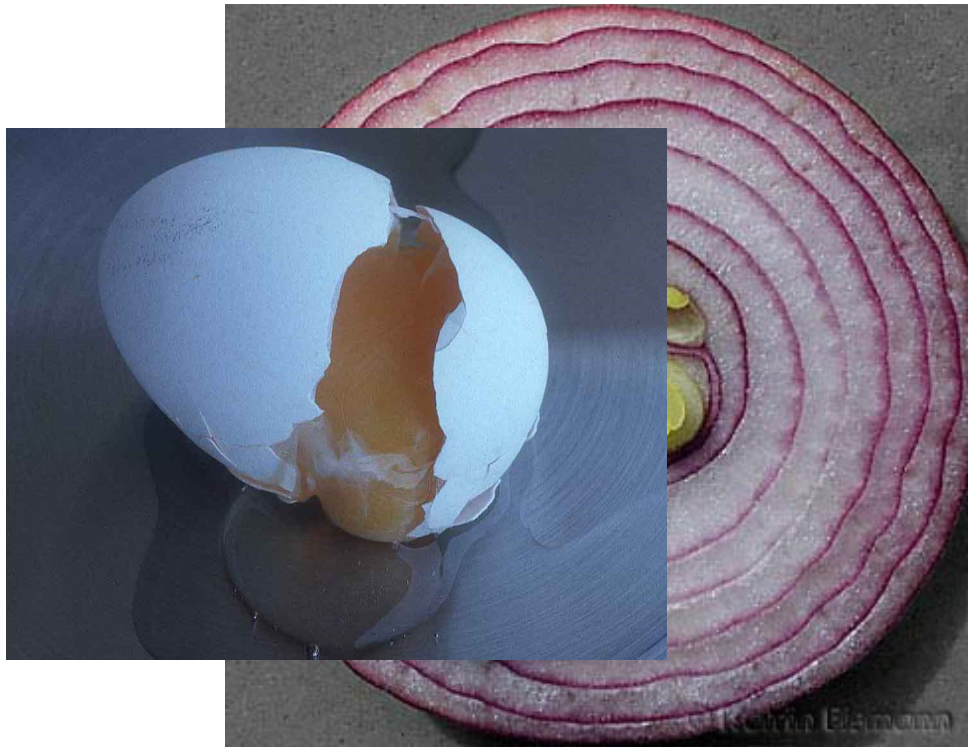
- Accessing PII
  - Credit Card
  - Social Security Number / Social Insurance Number
  - Phone Numbers
  - Home Address
  - Mothers' Maiden Name
  - Disaster Relief Sites
    - Katrina People Finder
    - September 11th People Finder

Can You Defend ?

- To a large extent
- Robots.txt
- Archive.org ?

http://web.archive.org/web/20040202071327/www.atstake.com/research/reports/

- Awareness Programs
- Search Engine Hacking Challenges
- Comments in Code
- Onion Not Egg Model

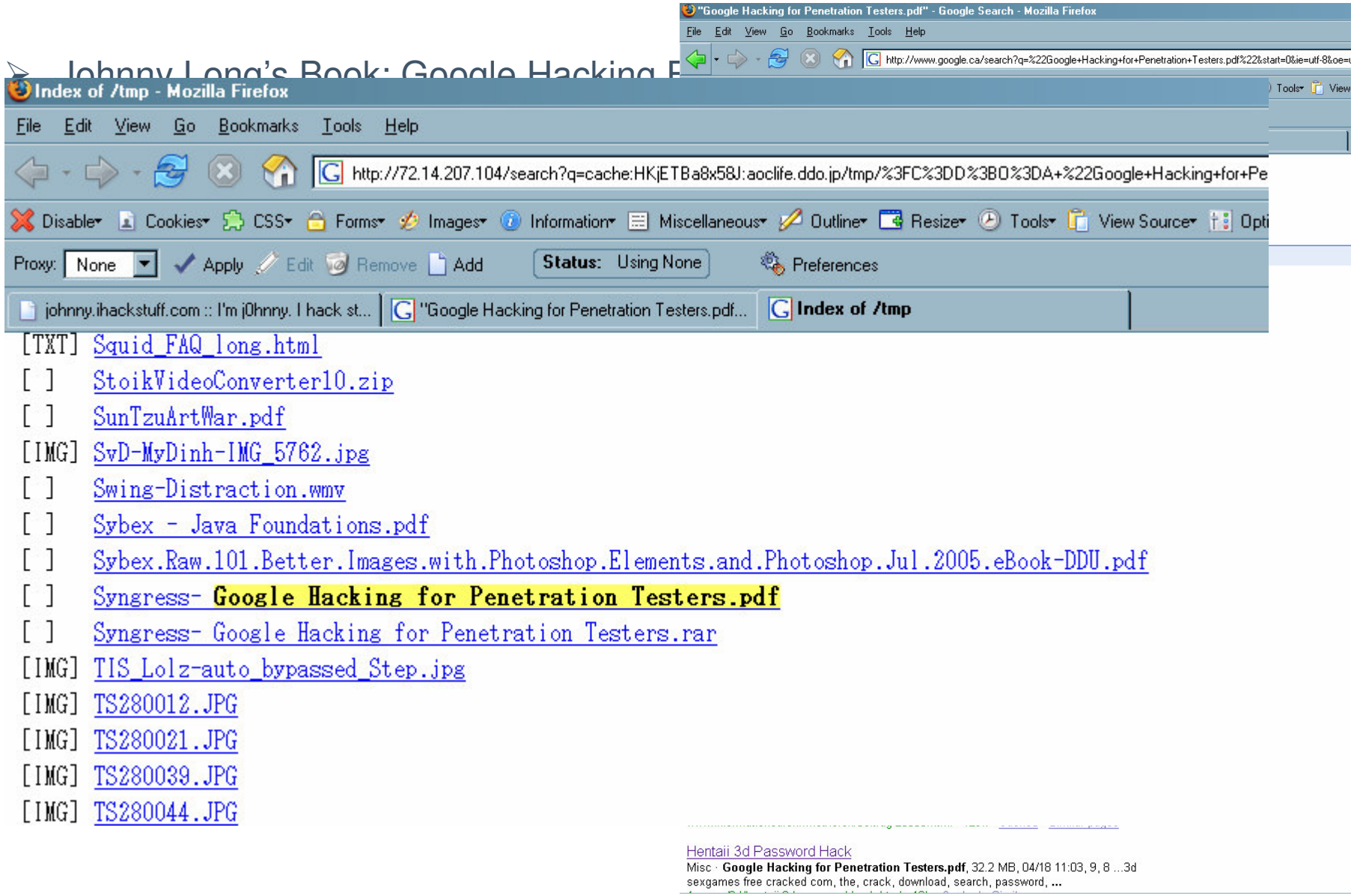


Automated Tools

- Automated Tools:
  - Perl Scripts (goolink.pl)
  - Php scripts (onlamp)
  - SiteDigger
  - Wikto (Integrated Nikto & Google Scanner)

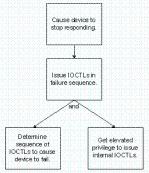
References

- Johnny Long's Book: Google Hacking F

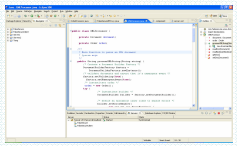


Application Consulting Services

- We offer four distinct consulting services for Application Security:

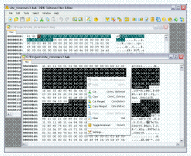


Threat Analysis

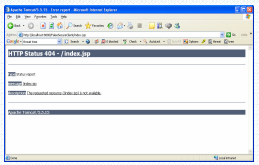


App Code Review

Product Review

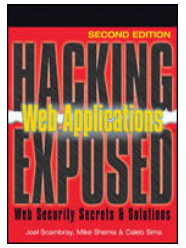


Web App Sec Review

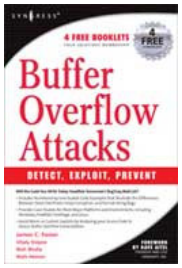


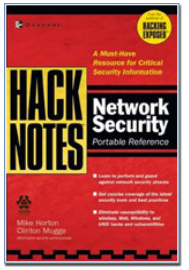
Security Compass Profile

- Our consultants have serviced large (Fortune 500) and medium sized companies across most major industries
- We have worked for major security players, including Foundstone and Deloitte

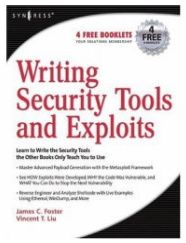


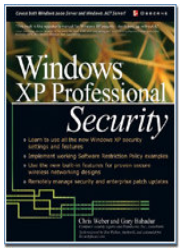
- We have co-authored or contributed to several security books, including:
  - Buffer Overflow Attacks: Detect, Exploit & Prevent
  - Windows XP Professional Security
  - HackNotes: Network Security
  - Writing Security Tools and Exploits
  - Hacking Exposed: Web Applications, 2nd Edition





- We have presented at and continue to present at security conferences, including:
  - Reverse Engineering Conference 2005 in Montreal; HackInTheBox 2005 in Malaysia; ISC2's Infosec Conferences in Las Vegas, NYC, Toronto & DC; CSI NetSec; DallasCon; ToorCon; and Freenix.





- We present and contribute to open source projects:
  - Chair at OWASP Toronto, Presented at OWASP Toronto, Contributed to YASSP Project (Lead by SANS and Xerox), Botan Crypto library, Cutlas P2P network & VNCCrack

Contact Info:

- Nishchal Bhalla

Founder, Security Compass
Nish Bhalla (Nish@securitycompass.com)
Toronto, Ontario: 647.722.4883
Shrewsbury, New Jersey: 201.390.9198