

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



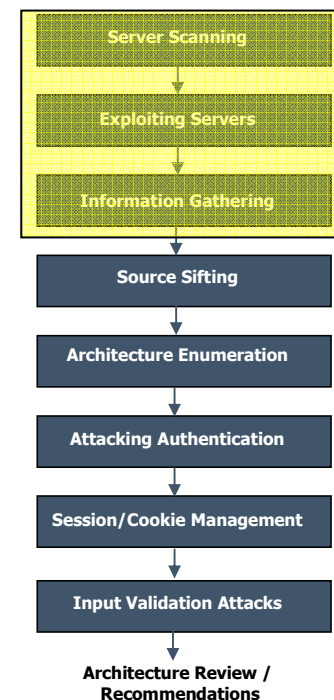
- Design Review: Understand what the thought process was when the application was originally designed
- More often than not the design and the end product are two completely different applications
- Architecture Review: Evaluate the deployed application's architecture and implementation in a real world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

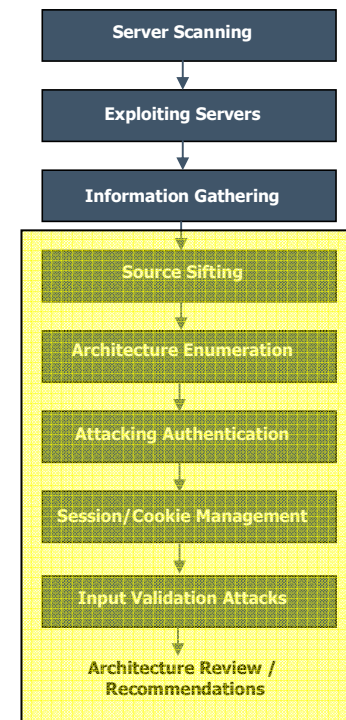
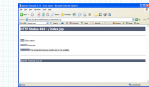


Web Application Review



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

Web App Sec Review



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

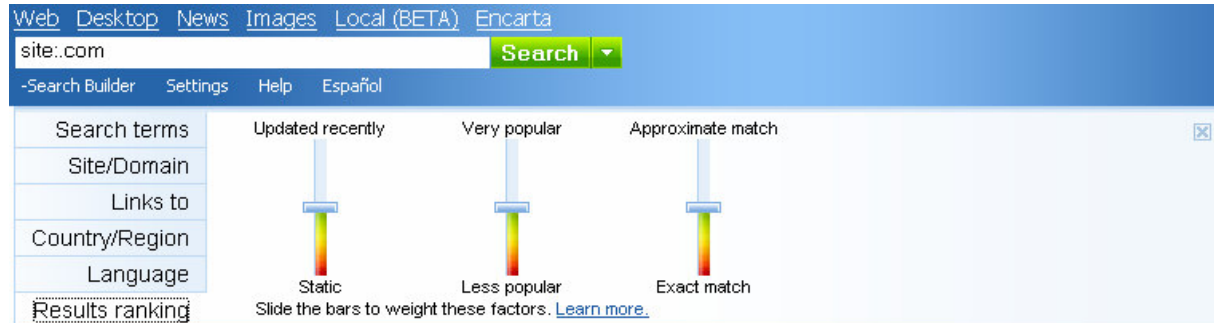


Search Engine - Basics



➤ Basic Searching Techniques (MSN)

- Site:
- Search All the terms/any of the terms/exact phrase



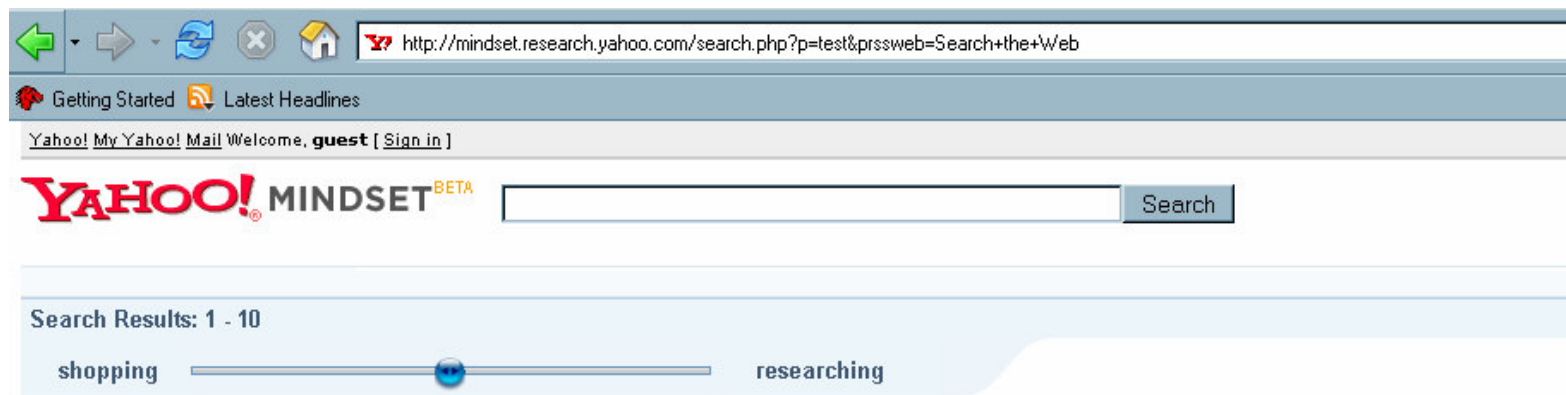
Search Engine - Basics



➤ Basic Searching Techniques (Yahoo)

- intitle:
- inurl:
- Advanced: Filetype / Update Past few months / File Format

➤ <http://mindset.research.yahoo.com/>

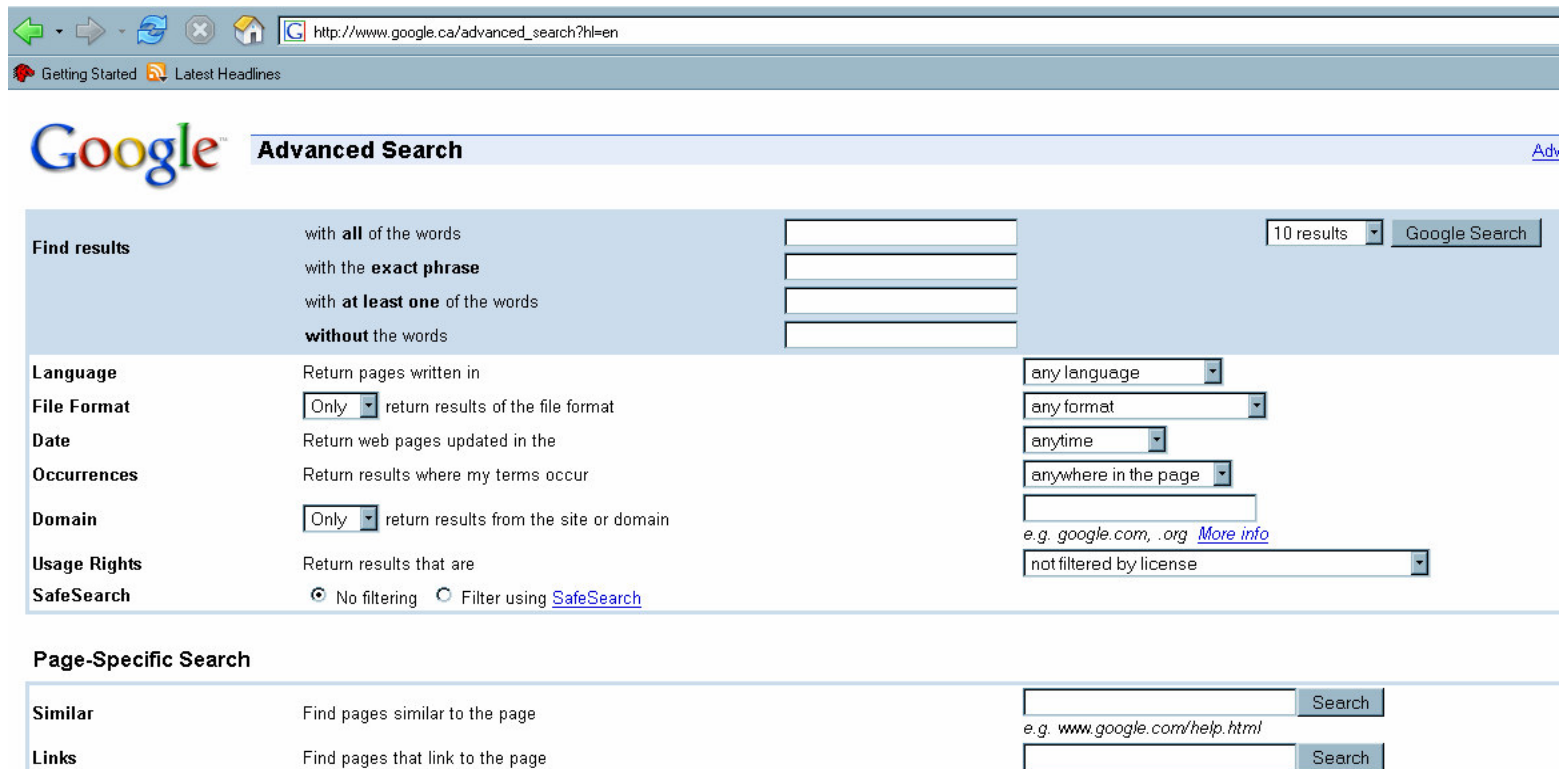


Search Engine - Basics



➤ Basic Searching Techniques (Google)

- Site:
- Filetype:
- Daterange:
- Numrange:



The screenshot shows the Google Advanced Search page in a web browser. The browser's address bar displays the URL `http://www.google.ca/advanced_search?hl=en`. Below the browser window, the Google logo is followed by the text "Advanced Search" and a link to "Adv".

The main search area is divided into two columns. The left column contains a list of search criteria with corresponding input fields:

- Find results**: A list of search criteria with corresponding input fields:
 - with **all** of the words
 - with the **exact phrase**
 - with **at least one** of the words
 - without** the words
- Language**: Return pages written in
- File Format**: Only return results of the file format
- Date**: Return web pages updated in the
- Occurrences**: Return results where my terms occur
- Domain**: Only return results from the site or domain
- Usage Rights**: Return results that are
- SafeSearch**: ☒ No filtering ☐ Filter using [SafeSearch](#)

The right column contains a list of search criteria with corresponding input fields:

- 10 results
- any language
- any format
- anytime
- anywhere in the page
-
- e.g. google.com, .org [More info](#)
- not filtered by license

Below the main search area, there is a section titled "Page-Specific Search" with two rows:

- Similar**: Find pages similar to the page
e.g. [www.google.com/help.html](#)
- Links**: Find pages that link to the page

Search Engine - Basics



link:www.securitycompass.com

site:google.com -site:www.google.com

MSN Search: site:google.com -site:www.google.com - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://search.msn.com/results.aspx?q=site%3Agoogle.com+site%3Awww.google.com

Getting Started Latest Headlines

Web Desktop News Images Local (BETA) Encarta

site:google.com -site:www.google.com Search Near Me

+Search Builder Settings Help Español

Go to search.sympatico.msn.ca

Web Results

Page 1 of 2,357,781 results containing **site:google.com -site:www.google.com** (0.19 seconds)

<http://maps.google.com/>
maps.google.com

Google Earth - Home
... Google Earth - Explore, Search and Discover New - October 17, 2005 - Google Earth KML files showing updated Pakistan earthquake-area imagery for the Baffa and ...
earth.google.com [Cached page](#)

Google Scholar
Advanced Scholar Search Scholar Preferences Scholar Help Stand on the shoulders of giants Google Home - About Google - About Google Scholar ©2005 Google
scholar.google.com [Cached page](#)

Google Blog Search
... Find blogs on your favorite topics Google Home - About Google Blog Search ©2005 Google
blogsearch.google.com [Cached page](#)

Google Directory
... Help build the largest human-edited directory on the web. Submit a Site - Open Directory Project - Become an Editor
directory.google.com [Cached page](#)

site:google.com -site:www.google.com - Google Search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.google.com/search?num=100&hl=en&lr=&q=site%3Agoogle.com+site%3Awww.google.com&btnG=Search

Getting Started Latest Headlines

Web Images Groups News Froogle Local more »

Google site:google.com -site:www.google.com Search [Advanced Search](#) [Preferences](#)

Web

Google Toolbar
Integrates with Internet Explorer's toolbar. Features include web search, image search, search site, page rank, and page information.
toolbar.google.com/ - 10k - 26 Nov 2005 - [Cached](#) - [Similar pages](#)

Google Catalog Search
Search and browse mail-order catalogs online. Focuses on standard US mail-order product catalogs which have prices printed in them and are designed to help ...
catalogs.google.com/ - 8k - 28 Nov 2005 - [Cached](#) - [Similar pages](#)

Google Labs
Use of this site is subject to express terms of use. By continuing past this page, you agree to abide by these terms. ...
labs.google.com/ - 18k - [Cached](#) - [Similar pages](#)

Google Code
It's been a busy couple of weeks here at Google. First off, the Sitemaps team has updated their interface to give you better information about the Sitemap ...
code.google.com/ - 16k - 28 Nov 2005 - [Cached](#) - [Similar pages](#)

Google Earth - Home
Offers maps and satellite images for complex or pinpointed regional searches.
earth.google.com/ - 14k - [Cached](#) - [Similar pages](#)

Google Investor Relations
Corporate Profile Google is a global technology leader focused on improving the ways people connect with information. Our innovations in web search and ...
investor.google.com/ - 11k - 28 Nov 2005 - [Cached](#) - [Similar pages](#)

Search Engine - Basics



link:www.securitycompass.com

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

Yahoo! Search Results for site:google.com -site:www.google.com - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://search.yahoo.com/search?p=site%3Agoogle.com+-site%3Awww.g...

Getting Started Latest Headlines

Yahoo! My Yahoo! Mail Welcome, nishbhalla [Sign Out, My Account]

Web Images Video Directory Local News Shopping

YAHOO! SEARCH site:google.com -site:www.google.com

My Web BETA Search Services Advan...

Search Results Results 1 - 10 of about 6,430,000 for site:google.com -site:www.google.c...

- [Google News](#)
presents information culled from news sources worldwide and arranged automatically.
Category: [News Search Engines](#)
[news.google.com](#) - 129k - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- [Google Maps](#)
Google Maps online map service and location finder. Features dynamic, draggable maps, as well as satellite imagery by region.
Category: [Interactive Maps](#)
[maps.google.com](#) - [More from this site](#) - [Save](#) - [Block](#)
- [images.google.com/imgres](#)
[images.google.com/imgres](#) - [More from this site](#) - [Save](#) - [Block](#)
- [Google Toolbar](#)
a Google Toolbar for your web browser, providing quick access to the Google search engine, PageRank information for a site, online maps, and a spell checker.
Category: [Browser Utilities > Search Toolbars](#)
[toolbar.google.com](#) - 9k - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- [Gmail](#)
web-based email service from Google that allows users to search their message archive.
Category: [Free Email Providers](#)
[gmail.google.com](#) - [More from this site](#) - [Save](#) - [Block](#)

AltaVista Search: domain:google.com NOT domain:www.google.com - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.altavista.com/web/results?itag=ody&q=domain%3Agoogle.com+NOT...

Getting Started Latest Headlines

altavista Web Images MP3/Audio Video News

domain:google.com NOT domain:www.google.com **FIND** [Advanced Search Settings](#)

SEARCH: ☐ Worldwide ☒ USA RESULTS IN: ☒ All languages ☐ English, Spanish

AltaVista found 6,430,000 results

[Google](#)
Personalized Home | Sign in. Web Images Groups News Froogle LocalNew! more " Advertising Program [google.com](#)

[Google Maps](#)
Provides directions, interactive maps, and satellite/aerial imagery of the United States. Can also search [maps.google.com](#)

[images.google.com/imgres](#)
[images.google.com/imgres](#)

[Google Toolbar](#)
Take the power of Google with you anywhere on the Web. New Google Toolbar features. SpellCheck. C into other languages. AutoLink (US only)
[toolbar.google.com](#)

[Welcome to Gmail](#)
[gmail.google.com](#)

[google image search](#)
[images.google.com](#)

[Google Scholar](#)
Stand on the shoulders of giants. Google Home - About Google - About Google Scholar
[scholar.google.com](#)

[Google Desktop Download](#)
Info when you want it, right on your desktop. New! Sidebar with Quick Find. By downloading, you agree [desktop.google.com](#)

[Google Directory](#)
A popular search engine with many features. It uses the ODP RDF dumps in the directory section.
[directory.google.com](#)

[google labs](#)
[labs.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

Netcraft - Search Web by Domain - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://searchdns.netcraft.com/?restriction=site+contains&host=*.*.3A8080&lookup=wait.&position=limited

Getting Started Latest Headlines

NETCRAFT

Tired Of Cut-Rate Service? Is Your Project Too Important To Trust With Discount Dedicated Hosts?

Netcraft News

Search Web by Domain

Explore 70,884,595 web sites 30th November 2005

Search: [search tips](#)

example: site contains .sco.com

Results for *.*.8080

Found 14 sites

	Site	Site Report	First seen	Netblock	OS
1.	cp.md-hosting.com:8080		February 2003	unknown	unknown
2.	sms.ed.ac.uk:8080		October 2001	unknown	unknown
3.	staffmail.ed.ac.uk:8080		February 2003	unknown	unknown
4.	www.chatline.com.ua:8080		March 2002	unknown	unknown
5.	www.che.rochester.edu:8080		January 1997	unknown	unknown
6.	www.eleves.ens.fr:8080		January 1997	unknown	unknown
7.	www.grimmcagliari.it:8080		April 2005	unknown	unknown
8.	www.hitechbooks.co.nz:8080		February 2003	unknown	unknown
9.	www.jhsi.com:8080		January 2002	unknown	unknown
10.	www.me.rochester.edu:8080		August 1998	unknown	unknown
11.	www.notesafrica.co.za:8080		May 2000	unknown	unknown

Done

www.securitycompass.com



Server Identification



Site report for netcraft.com - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://toolbar.netcraft.com/site_report?url=http://netcraft.com

Getting Started Latest Headlines

NETCRAFT **DEDICATED CENTRAL** **Professional.**

Toolbar Netcraft

Site report for netcraft.com

Site	http://netcraft.com	Last reboot	171 days ago Uptime graph
Domain	netcraft.com	Netblock owner	Rackspace.com
IP address	83.138.189.100	Site rank	34306
Country	UK	Nameserver	ns1.netcraft.com
Date first seen	March 1996	DNS admin	hostmaster@netcraft.com
Domain Registry	networksolutions.com	Reverse DNS	cod.netcraft.com
Organisation	Netcraft Ltd, Rockfield House, Granville Road, Bath, BA1 9BQ, United Kingdom	Nameserver Organisation	Netcraft Ltd, Rockfield House, Granville Road, Bath, BA1 9BQ, United Kingdom

Check another site:

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
Rackspace.com	83.138.189.100	FreeBSD	Apache/1.3.27 Unix mod_perl/1.27	24-Oct-2005
Rackspace.com	83.138.189.100	unknown	Apache/1.3.27 Unix mod_perl/1.27	23-Oct-2005
Rackspace.com	83.138.189.100	FreeBSD	Apache/1.3.27 Unix mod_perl/1.27	13-Oct-2005
Rackspace.com	83.138.189.100	unknown	Apache/1.3.27 Unix mod_perl/1.27	12-Oct-2005
Rackspace.com	83.138.189.100	FreeBSD	Apache/1.3.27 Unix mod_perl/1.27	25-Sep-2005
Rackspace.com	83.138.189.100	unknown	Apache/1.3.27 Unix mod_perl/1.27	24-Sep-2005
Rackspace.com	83.138.189.100	FreeBSD	Apache/1.3.27 Unix mod_perl/1.27	23-Sep-2005
Rackspace.com	83.138.189.100	unknown	Apache/1.3.27 Unix mod_perl/1.27	22-Sep-2005
Rackspace.com	83.138.189.100	FreeBSD	Apache/1.3.27 Unix mod_perl/1.27	11-Sep-2005
Rackspace.com	83.138.189.100	unknown	Apache/1.3.27 Unix mod_perl/1.27	10-Sep-2005

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"

Yahoo! Search Results for intitle:"Test Page for Apache" "It Worked!" "on this web" - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://search.yahoo.com/search?p=intitle%3A%22Test+Page+for+Apache%22%22+Worked%21%22+%22on+this+web%22

Getting Started Latest Headlines

Yahoo! My Yahoo! Mail Welcome, nishbhall (Sign Out, My Account)

Web Images Video Directory Local News Shopping

YAHOO! SEARCH intitle:"Test Page for Apache" "It Worked!" "on this web" Search

My Web BETA

Search Results Results 1 - 10 of about 48,800 f

- Test Page for Apache**
It Worked! If you can see this, then your Apache installation was successful. You may now add content to this directory and replace Apache-powered web server. Thanks for using Apache!
aral.cse.msu.edu - 416 - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for Apache Installation on Web Site**
It Worked! The Apache Web Server is Installed on this Web Site! If you can see this page, then the people who own this domain have successfully.
cti.itc.virginia.edu - 2k - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for Apache Installation**
... Apache. **It Worked!** If you can see this page, then the ... have just activated the Apache Web server software included ... this directory.
darkhost.mine.nu:81 - 2k - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for Apache Installation on Web Site**
It Worked! On Complete! The Apache Web Server is Installed on this Web Site! If you can see this page, then the people who own software successfully.
www.xcom-mc.fr - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for Apache**
... it worked! The SSL/TLS-aware Apache webserver was, successfully installed on this website. If you can see this page ... the Apache.
zavijava.cc.umanitoba.ca - 2k - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for Apache**
It Worked! ABREA.NET. If you can see this, then your Apache installation was successful. You may now add content to this directory below on an Apache-powered web server.
www.abrea.net - 426 - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for Apache**
It Worked! ApacheThe installation was successful. The Apache documentation has been included with this distribution. Thanks for using.
gcwww.cotdazr.org/aindex.html - 5k - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for Apache Installation**
It Worked! If you can see this, it means that the installation of the Apache software on this system was successful. You may now add content to this directory.
www.asuka.net - 1k - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for the SSL/TLS-aware Apache Installation on Web Site**
... it worked! The SSL/TLS-aware Apache webserver was, successfully installed on this website. If you can see this page ... the Apache.
RSS: [View as XML](#) - [Add to My Yahoo!](#)
forum.damage-web.net - [More from this site](#) - [Save](#) - [Block](#)
- Test Page for Apache Installation**
It Worked! ALTARI. If you can see this, it means that the installation of the Apache software on this system was successful. You may now add content to this directory.
www.altari.com.br - 1k - [Cached](#) - [More from this site](#) - [Save](#) - [Block](#)

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

Yahoo! Advanced Web Search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://search.yahoo.com/web/advanced?p=inurl%3Aphone&prssweb=Se

Getting Started Latest Headlines

YAHOO! SEARCH [Yahoo! - Search Home - Help](#)

Advanced Web Search

You can use the options on this page to create a very specific search. Just fill in the fields you need for your current search. [Yahoo! Search](#)

Show results with

all of these words	phone	in the URL of the page
the exact phrase		any part of the page
any of these words		any part of the page
none of these words		any part of the page

Updated anytime

Site/Domain

☒ Any domain
☐ Only .com domains ☐ Only .edu domains
☐ Only .gov domains ☐ Only .org domains

☐ only search in this domain/site:

Creative Commons Search **BETA**

☐ Search only for **Creative Commons** licensed content

☐ Find content I can use for commercial purposes

☐ Find content I can modify, adapt, or build upon

File Format Only find results that are: Microsoft Excel (.xls)

Done

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



Web Images Groups News Local ^{New!} more »
 Search [Advanced Search](#)
[Preferences](#)
 Search: ☒ the web ☐ pages from Canada

Web

[phpMyAdmin MySQL-Dump # version 2.2.3 # http://phpwizard.net ...](#)
 ... data for Table `blaster_minibb_users` # INSERT INTO blaster_minibb_users
 VALUES (1, 'Admin', '2003-07-09 19:19:47', '21232f297a57a5a743894a0e4a801fc3', ...
[www.neolithuania.lt/~anime/phpblaster/sql/phpBlaster.sql - 34k - Supplemental Result - Cached - Similar pages](#)

[MySQL dump 9.10 -- -- Host: localhost Database: phpbb2 ...](#)
 MySQL dump 9.10 -- -- Host: localhost Database: phpbb2 ... INSERT INTO `phpbb_users`
 VALUES (2,1,'Admin','21232f297a57a5a743894a0e4a801fc3','1,0,-8 ...
[synapticmedia.net/~davey/mysql/phpbb2.sql - 41k - Supplemental Result - Cached - Similar pages](#)

Web Images Video Directory Local News Shopping
YAHOO! SEARCH "#-FrontPage-" inurl:service.pwd
 My Web BETA
 Search Results

- <http://home.wanadoo.nl/paul.zoet/Scanners/Retina%202.0%20Network%20Scanner>
 ... [General] Name = **FrontPage** Password File - **Service.pwd** Description = The **service.pwd** fi
[home.wanadoo.nl/.../FrontPage Password File - Service.pwd.rth - 787 - Cached - More from thi](#)
- [pwd service](#)
 pwd service All Service Listings What are you looking for? Passware - Password Recovery Produ
 Database: **frontpage-pwd-service**(3391): **FrontPage** Extensions **service.pwd** file could ... Datab:
[directory-of-services.com/p/pwd.service.htm - 18k - Cached - More from this site - Save - Block](#)
- [vti_pvt service pwd](#)
 ... 2005_03 service pack 2 volenti o nolenti vti pvt **service pwd** service pack 2 volenti o nolenti ...
[www.publiweb.com/go/v/vti_pvt_service_pwd.html - 15k - Cached - More from this site - Save - B](#)
- http://www.cmsco.gr/vti_bin/shtml.dll/service.pwd
 Cannot run the **FrontPage** Server Extensions on this page: "**service.pwd**"
[www.cmsco.gr/vti_bin/shtml.dll/service.pwd - 107 - Cached - More from this site - Save - Block](#)
- http://conca.users.netlink.co.uk/vti_pvt/service.pwd
 # -**FrontPage**- juan:KIN.3BHTNuMII
[conca.users.netlink.co.uk/vti_pvt/service.pwd - 35 - Cached - More from this site - Save - Block](#)
- http://www.heyerlist.org/garderobe/vti_pvt/service.pwd
 # -**FrontPage**- ekendall:bYld1Sr73NLKq.louisa:5zm94d7cdDFiQ
[www.heyerlist.org/garderobe/vti_pvt/service.pwd - 35 - Cached - More from this site - Save - Blo](#)
- http://www.ltspe.edu/vti_pvt/service.pwd
 # -**FrontPage**- admin:J.V4Aq58IPfCg mstaples:u5jpa0V/qta7g
[www.ltspe.edu/vti_pvt/service.pwd - 57 - Cached - More from this site - Save - Block](#)
- http://www.agrarverlag.at/vti_pvt/service.pwd
 # -**FrontPage**- redak1:Vp3U6nYcC0lok
[www.agrarverlag.at/vti_pvt/service.pwd - 35 - Cached - More from this site - Save - Block](#)
- http://www.sbo.de/vti_pvt/service.pwd
 # -**FrontPage**- martin:AT8zF3AnDyDyc
[www.sbo.de/vti_pvt/service.pwd - 35 - Cached - More from this site - Save - Block](#)
- http://www.et.byu.edu/vti_pvt/service.pwd
 # -**FrontPage**- webmaster:b8IRc3dfOKAdk wizzo:NPjRI27BKUz7A
[www.et.byu.edu/vti_pvt/service.pwd - 58 - Cached - More from this site - Save - Block](#)



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

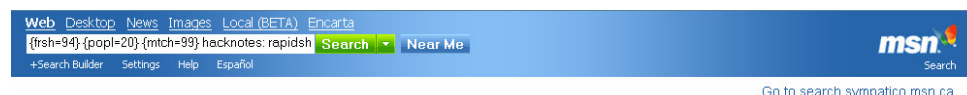


Web

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

[PDF] xunil.s4a.cc/Hacknotes%20Web.pdf
File Format: PDF/Adobe Acrobat - [View as HTML](#)
Supplemental Result - [Similar pages](#)

[PDF] www.team509.com/download/docs/security/WEB/McGraw...
File Format: PDF/Adobe Acrobat - [View as HTML](#)
Supplemental Result - [Similar pages](#)



Web Results

Page 1 of 10 results containing {frsh=94} {popl=20} {mtch=99} hacknotes: rapidshare.de/files (1.39 seconds) (with SafeSearch: [Moderate](#))

[A Huge list of Rapidshare, MegaUpload, Sexupload files](#)

... [rapidshare.de/files/2108526/smilebooks.net_0470092238.rar](#) 19372
[rapidshare.de/files/3139712/McGraw-Hill_-_HackNotes_Windows_Security_Portable_Reference.rar](#) 19373 . [rapidshare.de/files/517934/O...](#)
[www.uploadscout.com/uploadScout/NewIndex.aspx?start=19300](#) [Cached page](#)

[HackNotes Windows Security Portable Reference \[eBook\]](#)

... best practices for trace routing and source address location, ...
[http://rapidshare.de/files/3290913/BluePortal.org_HackNotes_Windows_Security_Portable_Reference_-_McGraw_Hill.rar.html](#) Password : http ...
[www.30im.com/post.asp?num=-1540901305](#) [Cached page](#)

[RapidSHARED.ORG](#)

... [http://rapidshare.de/files/3363612/McGraw.Hill.HackNotes.Windows.Security.Portable.Reference.eBook-DDU.rar.html](#) (Size, mb: Not specified)
Tired of Rapidshare limits? Got no premium? Get RapidLeecher and ...
[rapidshare.org/index.php?item&id=2985](#) [Cached page](#)

[RapidSHARED.ORG](#)

... [http://rapidshare.de/files/3363530/McGraw.Hill.HackNotes.Linux.and.Unix.Security.Portable.Reference.eBook-DDU.rar.html](#) (Size, mb: Not specified)
Tired of Rapidshare limits? Got no premium? Get ...
[rapidshare.org/index.php?item&id=2982](#) [Cached page](#)
[Show more results from "rapidshare.org".](#)

[موقع صهيبي](#)

... McGraw-Hill - [HackNotes Windows Security Portable Reference](#)
[http://rapidshare.de/files/3139712/McGraw-Hill_-_HackNotes_Window...erence.rar.html](#) NTC's Dictionary of American Slang and ...
[www.khayma.com/gosay/ebook41.htm](#) [Cached page](#)

[موقع صهيبي](#)

... Can't find eBook[PDF] 1041 pages|24 Mb [http://rapidshare.de/files/3369299/Mastering_Delphi_7.rar.html](#) Password: ... [HackNotes Linux and Unix Security Portable Reference](#) by Nitesh Dhanjani | McGraw-Hill ...
[www.khayma.com/gosay/E_Book_e/ebook49.htm](#) [Cached page](#)
[Show more results from "www.khayma.com".](#)



www.securitycompass.com



Gather Information



groups.google.com

- System configuration
- Resumes
- Troubleshooting apps
- Coding issues

Decryptor

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

The screenshot shows a web browser window with the address bar displaying http://groups.google.ca/groups?hl=en&q=enable+secret+7&qt_s=Search. The page features the Google Groups logo and navigation links for Web, Images, Groups, News, Local, and more. A search bar contains the text 'enable secret 7'. On the left sidebar, there are links for 'Members: Sign in', 'New users: Join', 'Recently visited' (with links to 'it.comp.reti.cisco' and 'macromedia.open-swf'), 'Groups Alerts', 'Create a new group', and 'About Google Groups'. The main content area, titled 'Searched all groups', lists several search results:

- enable secret 7 <myPassword>**
... com... Hi all, i executed on 2500 cisco router this command : **enable secret 7** test now, i can not connect to the router ! MyRouter ...
[comp.dcom.sys.cisco](#) - Feb 8, 2:04 pm by ns - 12 messages - 6 authors
- question about resetting enable and access password**
... If I had to guess, I'd say you did something like: **enable secret 7** <new password> instead of **enable secret** <new password> The **7** before the password means that ...
[comp.dcom.sys.cisco](#) - Nov 13 2003, 2:56 pm by Barry Margolin - 2 messages - 2 authors
- Datawan (ci siamo quasi)**
... encryption ! hostname Chieti ! **enable secret 5**
\$1\$tMA5\$XOW/CaTgVoyuflrDMNS9ID
enable password 7 15160A5B502E2E ! ip subnet-zero !!!!! ...
[it.comp.reti.cisco](#) - Apr 2 2003, 8:28 am by Davide D'Amico - 12 messages - 7 authors
- Difference between enable secret and enable password**
"enable password", like any of the Cisco "password 7" encrypted password strings is a trivially breakable encryption algorithm. ...
[comp.dcom.sys.cisco](#) - Mar 12 2002, 8:32 am by Kevin Dooley - 4 messages - 4 authors
- HELP ! Lost enable secret password**
... The conclusion of my troubles: A key "7" made me crazy: only by typing "enable secret 7 ANYTHING", i lost access to the privileged mode (ANYTHING is not good ...
[comp.dcom.sys.cisco](#) - Apr 20 2000, 4:37 pm by Fabien DESNOYERS - 13 messages - 8 authors

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

The screenshot shows the Vivísimo search engine interface. At the top, there's a navigation bar with links: company | products | solutions | customers | demos | press. Below this is a search bar containing the text 'crack' and a dropdown menu set to 'the Web'. A blue 'Search' button is next to the search bar, with links for 'Advanced Search' and 'Help'. Below the search bar, it says 'Search Clusty.com with our NEW FireFox Toolbar'. The main content area is divided into two columns. The left column, titled 'Clustered Results', lists various search results with expandable icons and counts: 'crack' (167), 'Password' (44), 'Serial, Keygen' (23), 'ip 8.1' (19), 'Crack software' (13), 'Nocd' (11), 'Search Engine' (10), '9.0' (8), '8.0' (8), and 'Crack' (8). A 'More' link is at the bottom of this list. The right column, titled 'Cluster Crack software contains 13 documents. (Details)', shows sponsored results for 'crack software'. It includes a link to 'Download Free Software' from 'Software Archives' and a list of three search results: 1. 'Welcome to CRACKS.AM software security site!', 2. 'Crack Software' from 'downloadspace.com', and 3. 'crack software by Devicod Technology and others' from 'freedownloadcenter.com'.

Vulnerability Scan Reports



Hackers and Auditors to the rescue.

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

Summary Statistics	
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.

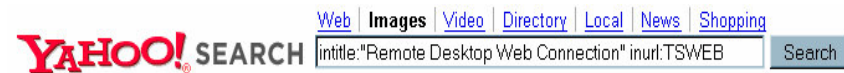


Image Results

Results



tsweb.jpg

716 x 634 pixels - 58.4kB
infojama.pl



tsweb3.jpg

884 x 666 pixels - 124.0kB
www.kuku.co.il



rdc_fig3.jpg

365 x 350 pixels - 18.4kB
www.microsoft.com/windowsxp/.../
03may16.asp



rdc_fig2.jpg

365 x 247 pixels - 16.4kB
www.microsoft.com/windowsxp/.../
03may16.asp



tsweb1.jpg

778 x 502 pixels - 85.6kB
www.kuku.co.il



rdwc02-0.jpg

365 x 257 pixels - 33.3kB
www.microsoft.com/windowsxp/.../
02january14.asp



tsweb2.jpg

778 x 502 pixels - 80.2kB
www.kuku.co.il



tswebsmall.jpg

169 x 150 pixels - 5.1kB
infojama.pl



Web Images Groups News Local ^{New!} more »

inurl:5800 "VNC Desktop"

Search

[Advanced Search](#)
[Preferences](#)

Search: ☒ the web ☐ pages from Canada

Web

[VNC desktop \[sunbeam\]](#)

[sunbeam.uoregon.edu:5800/](#) - 1k - [Cached](#) - [Similar pages](#)

[VNC desktop \[sever\]](#)

[moment.myftp.org:5800/](#) - 1k - [Cached](#) - [Similar pages](#)

[Ultr@VNC Desktop \[e8r7h0\] ----- Ultr@VNC Home Page is http ...](#)

[robot.mc3.edu:5800/](#) - 1k - [Supplemental Result](#) - [Cached](#) - [Similar pages](#)

[VNC desktop \[pc001\]](#)

[hdeg.tzo.com:5800/](#) - 1k - [Supplemental Result](#) - [Cached](#) - [Similar pages](#)

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"



Web

Web Data Administrator - Login

Welcome to the Web Data Administrator. Please enter your SQL Server credentials: Username. Password. Server.
www1.hosting.hol.gr/sqlwebadmin/ - 6k - 3 Dec 2005 - [Cached](#) - [Similar pages](#)

Web Data Administrator - Login

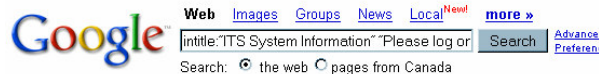
Logout. Welcome to the Web Data Administrator. Please enter your SQL Server credentials: Username. Password. Server. Select one ... SQL.ADHOST. ...
sqlmanager.adhost.com/ - 8k - [Cached](#) - [Similar pages](#)

Web Data Administrator - Login

Help - Logout. You are now logged out. Please enter your SQL Server credentials: Username. Password. Server. Select one ... SQL.ADHOST.COM, SQL1.ADHOST. ...
sqlmanager.adhost.com/Logout.aspx - 8k - [Cached](#) - [Similar pages](#)

Web Data Administrator - Login

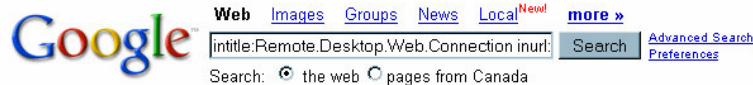
SQL 2000 Web Administrator Please enter your SQL Server credentials: Username. Password. Server.
sql2.norits.net/ - 6k - [Cached](#) - [Similar pages](#)



Web

ITS System Information

ITS System Information. Please log on to the SAP System SIF. Service: webgui. Client: Login: Login required. Password: Password required. ...
subnradine.cm.namex.com/ - 17k - [Supplemental Result](#) - [Cached](#) - [Similar pages](#)



Web

Remote Desktop Web Connection

Remote Desktop Web Connection. This system is restricted to legitimate business purposes. Unauthorized access is prohibited.
<https://bfasweb.syr.edu/tsweb/> - 22k - [Cached](#) - [Similar pages](#)

Remote Desktop Web Connection

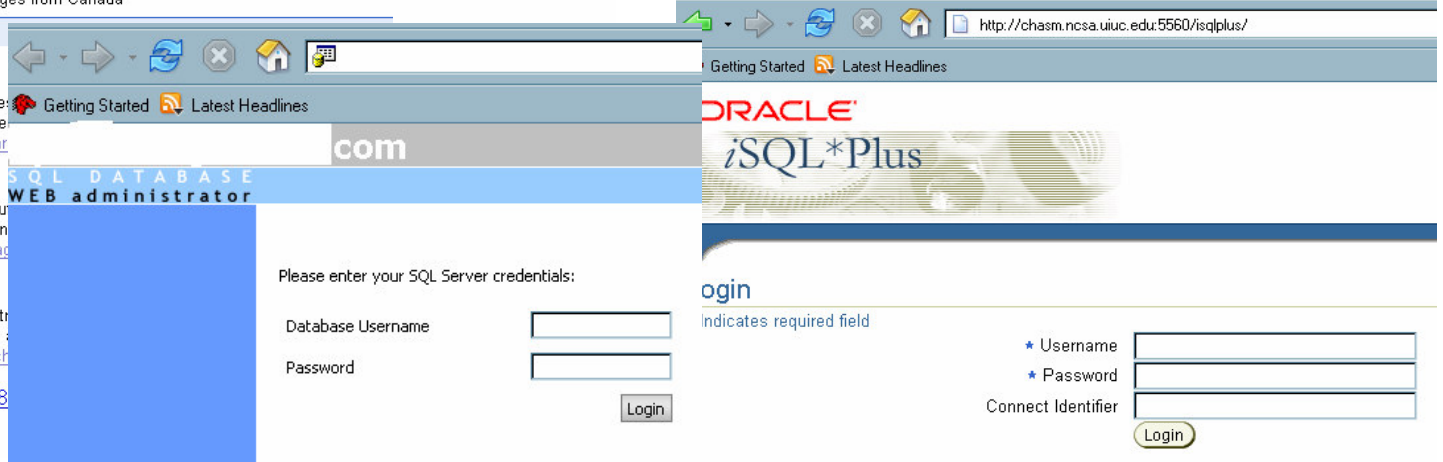
Remote Desktop Web Connection. This system is restricted to legitimate business purposes. Unauthorized access is prohibited.
ntweb.ssc.wisc.edu/tsweb/ - 23k - [Cached](#) - [Similar pages](#)

Remote Desktop Web Connection

Remote Desktop Web Connection. This system is restricted to legitimate business purposes. Unauthorized access is prohibited.
www.southeastmn.edu/TSWeb/default.htm - 23k - [Cached](#) - [Similar pages](#)

Remote Desktop Web Connection to 65.68.148.226

Connected to 65.68.148.226.
tsweb.mhpc.com/ - 3k - [Cached](#) - [Similar pages](#)



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"



Web Bilder Groups Verzeichnis News Froogle Mel
12541: TNS:no listener" intitle:"error occurred" Suche Erweitern
Web-Suche Suche Seiten auf Deutsch

Web

[Error Occurred While Processing Request](#) - [[Diese Seite übersetzen](#)]

... ORA-12541: TNS:no listener. The error occurred while processing an element with a general identifier of (CFQUERY), occupying document position (109:2) to (109:43) ...
[www.cbss.org/english/search/display.cfm?code=4024&Coll=FE_FEDSBIS_E - 2k - Zusätzliches Ergebnis](#)

[We're sorry, an error occurred](#) - [[Diese Seite übersetzen](#)]

... to connect: java.sql.SQLException: [MERANT][SequeLink JDBC Driver][ODBC Socket][Oracle][ODBC][Ora]ORA-12541: TNS:no listener The error occurred on line ...
[www.arinso.nl/whoweare/today_index.cfm - 3k - Zusätzliches Ergebnis](#) - [Im Cache](#) - [Ähnlich](#)

Mail

A Syntax Error Has Occurred

[12-05-2005 @ 16:48:12]

Error Number = 350

Error Message = Native SQL Error Code

Error Details = 350

C:\data\clients\meromall_demo\browse.html

SQL ALIAS="en" DBNAME="[removed]" LOGIN="[removed]" SQL="select id, name, parent, feature1, feature2 from category where active=1 and id=en_sectionid"

[Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect syntax near '!'.

select id, name, parent, feature1, feature2 from category where active=1 and id=en_sectionid

SQL Error: [Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect syntax near '!'.

SQL Statement: select id, name, parent, feature1, feature2 from category where active=1 and id=en_sectionid

XML Error: i_error_xml

SSL Error: i_error_cryptolib

Browser used: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915 Firefox/1.0.7
Error caused by IP: 206.248.149.8



Warning: mysql_connect(): Access denied for user: 'scraper@localhost' (T...

Warning: mysql_select_db(): supplied argument is not a valid MySQL-Link...

Warning: mysql_query(): Access denied for user: 'scraper@localhost' (T...

Warning: mysql_query(): A link to the database was not specified, using the default connection
Invalid command: SET FOOT



www.securitycompass.com



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



http://shadow.sentry.org/cgi-bin/multimon

Getting Started Latest Headlines

APCUPS

Tue I

System	Model	Sta
centurion.sentry.org, shadow.sentry.org	SMART-UPS 1400	ON
KVM, Billion ADSL router, switch	SMART-UPS 1000	ON
D-Link ADSL router	SMART-UPS 700	ON
LCD monitor	SMART-UPS 700	ON

Google

Web Images Groups News

inurl:sts_index.cgi

Search: the web pages from

Tip: Search for English results only. You can specify your search.

Web

www.counseling.nsysu.edu.tw/en/sts_index.cgi

1k - Cached - Similar pages

ipsio220.slis.tsukuba.ac.jp/cgi-bin/sts_index.cgi

1k - Supplemental Result - Cached - Similar pages

ipsio220.slis.tsukuba.ac.jp/en/cgi-bin/sts_index.cgi

1k - Supplemental Result - Cached - Similar pages

mizu2.mech.kogakuin.ac.jp/en/sts_index.cgi

1k - Supplemental Result - Cached - Similar pages

Google

Web Images Groups News Local more »

intitle:"View and Configure PhaserLink"

Search: the web pages from Canada

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

Web

View and Configure PhaserLink PDF Direct Printing Settings (Phaser ...

View and Configure PhaserLink PDF Direct Printing Settings (Phaser 840, 740, and 780 printers only). This page contains a link to the View and Configure ...

www.office.xerox.com/userdoc/P740/phlink/plfiles/plo2e.htm - 59k - Cached - Similar pages

View and Configure PhaserLink PDF Direct Printing Settings (Phase

Xerox. United States, change. > Reseller extranet. Office Products. Xerox Home · Where to Buy · Contact Us · My Account · Shopping Cart ...

www.office.xerox.com/userdoc/P780/phlink/plfiles/plo2e.htm - 59k - Cached - Similar

View and Configure PhaserLink Printing Settings - Phaser 740 ...

PhaserLinkTM Printing enabled.: No, *Yes. POP3 Server.: POP3 User Name.: POP3 Password.: POP3 Polling Interval.: minutes. PhaserLinkTM Printing Job Password ...

sprp-f13-phaser740.stanford.edu/netconfig_plprint.html - 6k - Supplemental Result - Cached -

View and Configure PhaserLink Printing PostScript Settings - T3 ...

PhaserLinkTM Software for the Phaser® 360 Color Printer. View and Configure PhaserLink Printing PostScript Settings for Printer named: T3-Phaser-Q / ...

phaser-t3.stanford.edu/netconfig_plprint2.html - 4k - Supplemental Result - Cached - Similar

Misc



Google blocks some searches

➤ `inurl:viewtopic.php`

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

➤ `inurl:viewtopic.php`

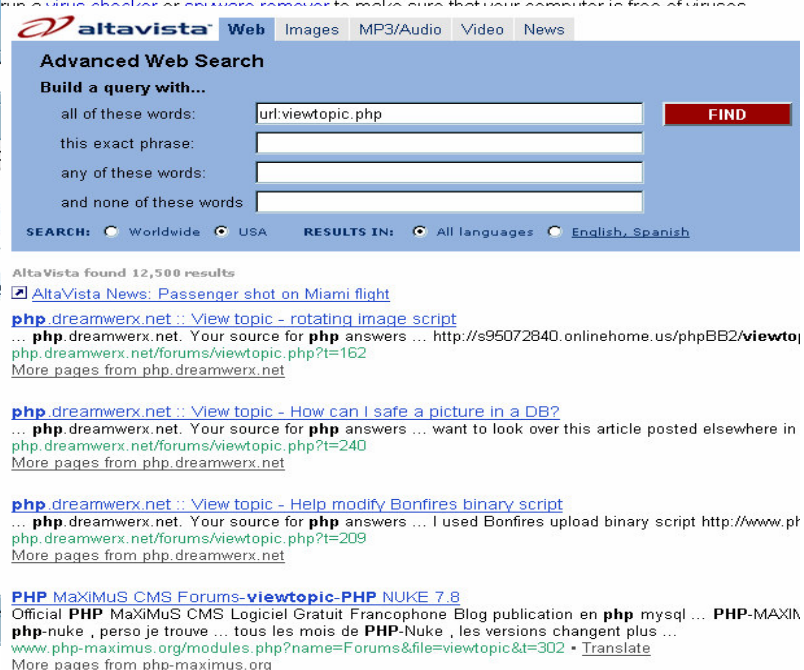
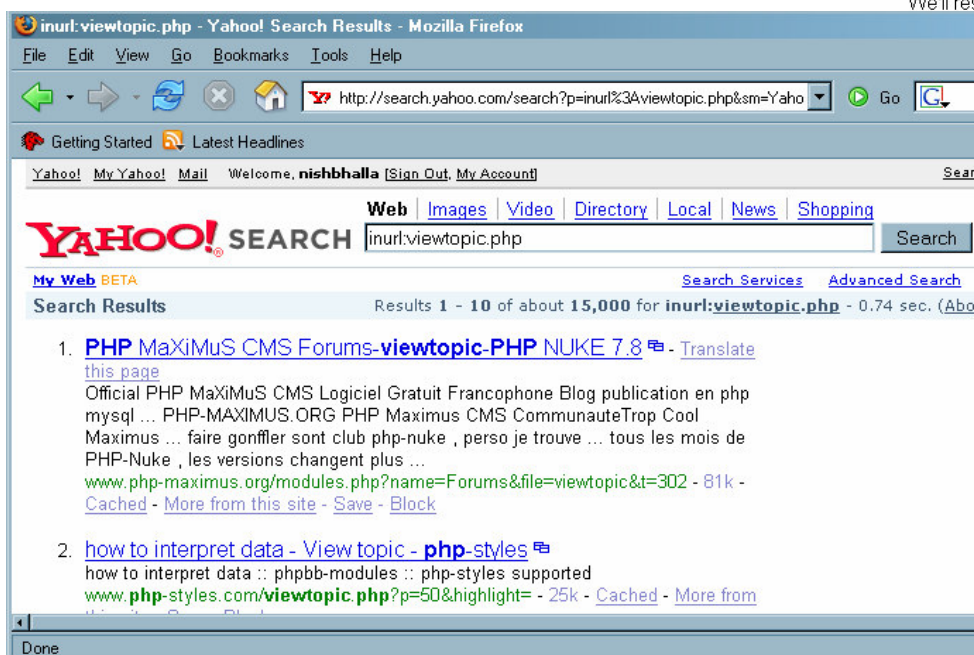


Google Error

We're sorry...

... but we can't process your request right now. A computer virus or spyware application is sending us automated requests, and it appears that your computer or network has been infected.

We'll restore your access as quickly as possible, so try again soon. In the meantime, you might run a virus checker or spyware remover to make sure that your computer is free of viruses.



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 ?

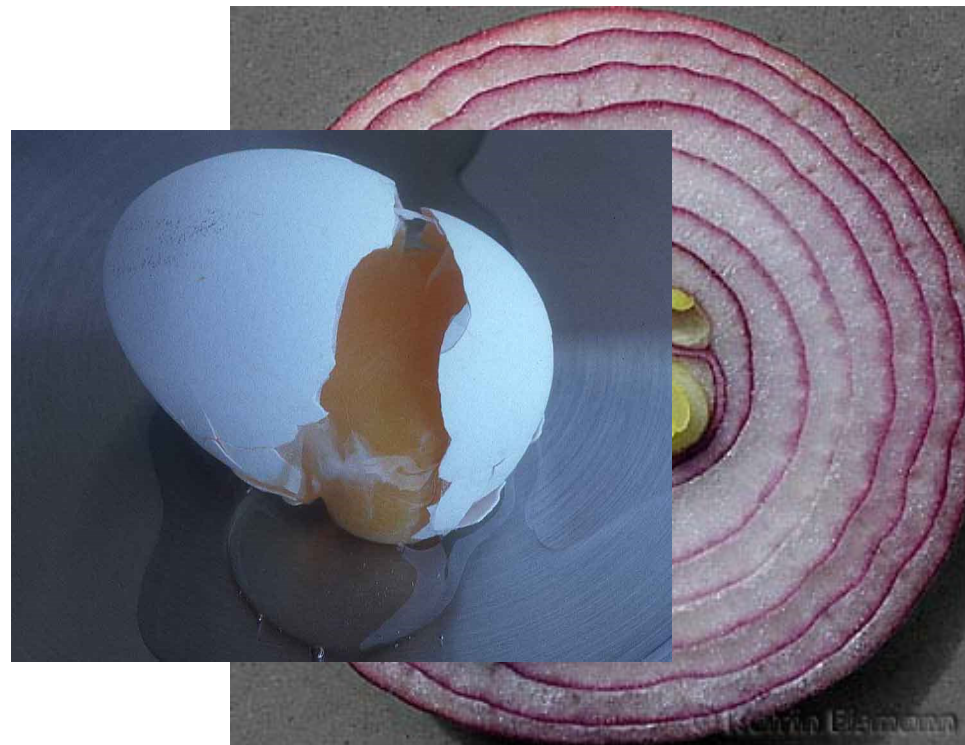
<http://web.archive.org/web/20040202071327/www.atstake.com/research/reports/>

➤ 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 For Penetration Testers

Index of /tmp - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://72.14.207.104/search?q=cache:HKjETBa8x58J:aoclife.ddo.jp/tmp/%3FC%3DD%3B0%3DA+%22Google+Hacking+for+Pe

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Opti

Proxy: None Apply Edit Remove Add Status: Using None Preferences

johnny.ihackstuff.com :: I'm j0hnny. I hack st... "Google Hacking for Penetration Testers.pdf" Index of /tmp

- [TXT] [Squid_FAQ_long.html](#)
- [] [StoikVideoConverter10.zip](#)
- [] [SunTzuArtWar.pdf](#)
- [IMG] [SvD-MyDinh-IMG_5762.jpg](#)
- [] [Swing-Distraction.wmv](#)
- [] [Sybex - Java Foundations.pdf](#)
- [] [Sybex.Raw.101.Better.Images.with.Photoshop.Elements.and.Photoshop.Jul.2005.eBook-DDU.pdf](#)
- [] [Syngress- Google Hacking for Penetration Testers.pdf](#)
- [] [Syngress- Google Hacking for Penetration Testers.rar](#)
- [IMG] [TIS_Lolz-auto_bypassed_Step.jpg](#)
- [IMG] [TS280012.JPG](#)
- [IMG] [TS280021.JPG](#)
- [IMG] [TS280039.JPG](#)
- [IMG] [TS280044.JPG](#)

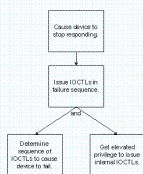
[Hentai 3d Password Hack](#)

Misc - [Google Hacking for Penetration Testers.pdf](#), 32.2 MB, 04/18 11:03, 9, 8 ...3d
sexgames free cracked com, the, crack, download, search, password, ...

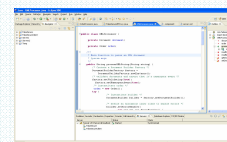
Application Consulting Services



- We offer four distinct consulting services for Application Security:

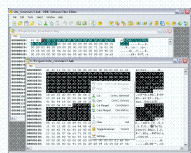


Threat Analysis

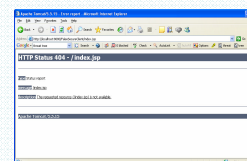


App Code Review

Product Review



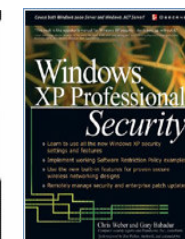
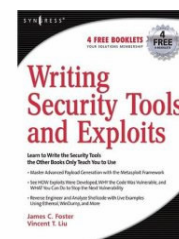
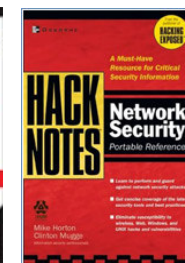
Web App Sec Review



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