

# Scanning the interwebs

Hunting for that vulnerable web application

B E Y O N D   A V A I L A B I L I T Y

Sean Arries  
Security Engineer  
Terremark Worldwide



## About Me

- Member of the Terremark's Threat Intelligence Team, an offensive intelligence division of Secure Information Services. The Team provides clients around the world with rapid incident response, forensics, and other critical security services including evaluating security posture through vulnerability assessments and penetration testing. The team is also tasked with staying up to date with the latest threats in the Information Security world.
- With 12 years of experience in the securities/technology field, I have led, as well as been a part of numerous consulting projects in the areas of system, network, and web-based vulnerability assessment, security audits, computer forensics, and secure computing design. I have also been instrumental in locating and responsibly disclosing numerous harmful zero-day vulnerabilities.

## What I am trying to convey.

- None of the concepts in this presentation are new..
- This is about designing an attack methodology that is extremely efficient.
- This is a very common attack pattern used today by blackhats to penetrate an organization.
- Methodology of a penetration test is just as important as the tools used or the 0day in your arsenal.



## Why we need to know this....

- Most organizations today use some form of 'known' web application. Whether its an open source or closed source application.
- These applications are the gate keepers to the internal network.
- Understanding how to find vulnerable web applications has a couple side effects.
  - Discovering a detailed inventory of what an organization has exposed to the internet
  - Aids in creating a comprehensive web application planning and assessment methodology

## What type of organizations?

- Basically anyone with a large web presence.
- Government organizations
- Universities / Colleges
- ISP / Datacenters / Hosting Providers
- This methodology was developed while performing pentests and protecting customers at Terremark.

*I like to call it protecting customers from themselves.*

# TATICS

- GOOGLE DORKS!
  - site:
  - filetype:
  - inurl:



- Sub-Domain Brute forcer
- Whois / host / Netblocks
- Bing IP reverse
- Web Application Finger Printing

```
#  
# The following results may also be obtained via:  
# http://whois.arin.net/rest/nets;q=72.14.253.104?showDetails=true&  
#  
NetRange:      72.14.192.0 - 72.14.255.255  
CIDR:          72.14.192.0/18  
OriginAS:  
NetName:       GOOGLE  
NetHandle:     NET-72-14-192-0-1  
Parent:        NET-72-0-0-0-0  
NetType:       Direct Allocation  
NameServer:    NS2.GOOGLE.COM  
NameServer:    NS3.GOOGLE.COM  
NameServer:    NS4.GOOGLE.COM  
NameServer:    NS1.GOOGLE.COM  
RegDate:       2004-11-10  
Updated:       2007-04-10  
Ref:           http://whois.arin.net/rest/net/NET-72-14-192-0-1
```

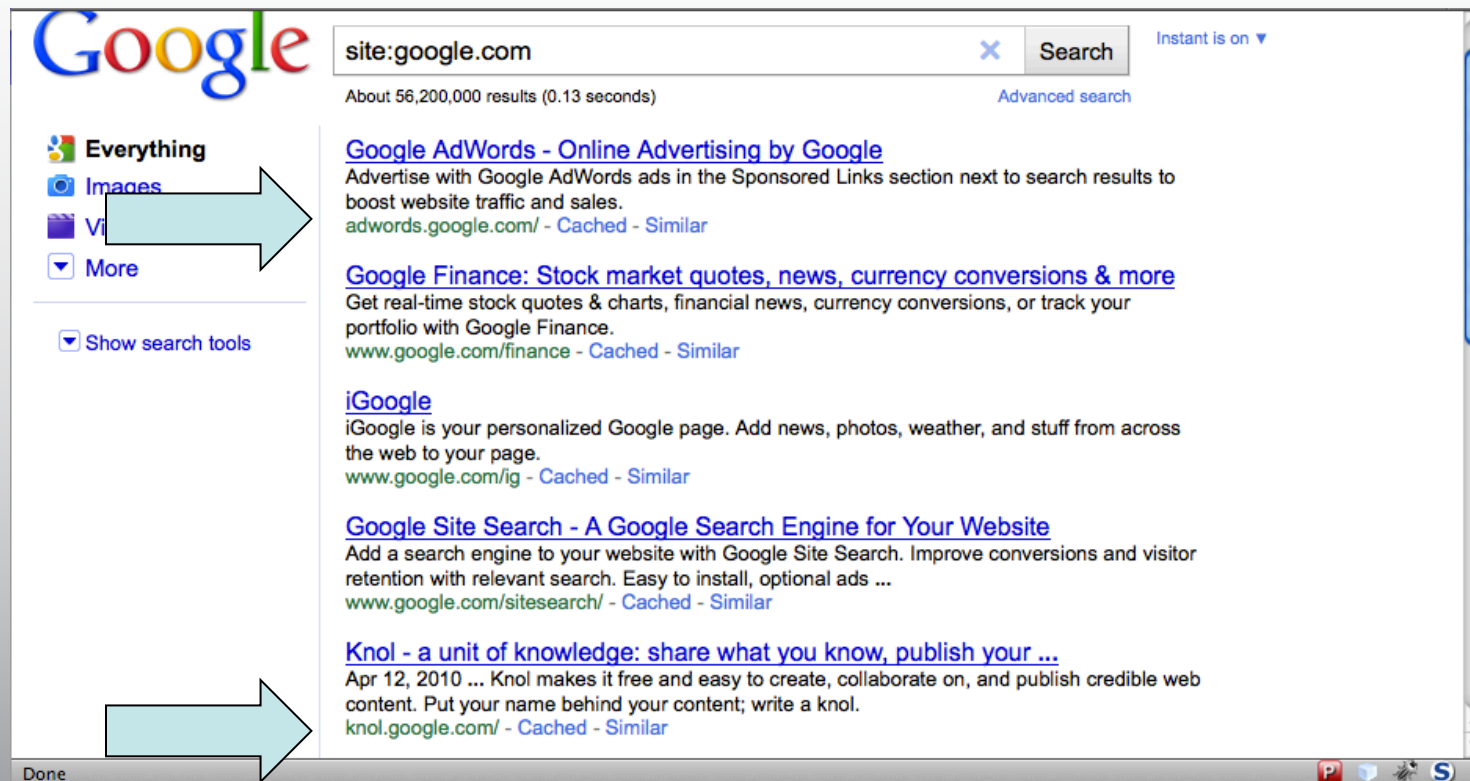
# METHODOLOGY

NOW LET'S PUT TOGETHER A GOOD METHODOLOGY  
FOR ALL THIS INFORMATION GATHERING

- 1. FINDING SUBDOMAINS
- 2. FINDING NETBLOCKS
- 3. FINDING WEBSERVERS
- 4. FIND ALL VHOSTED DOMAINS
- 5. WEB APPLICATION FINGERPRINTING
- 6. VULNERABILITY INFORMATION

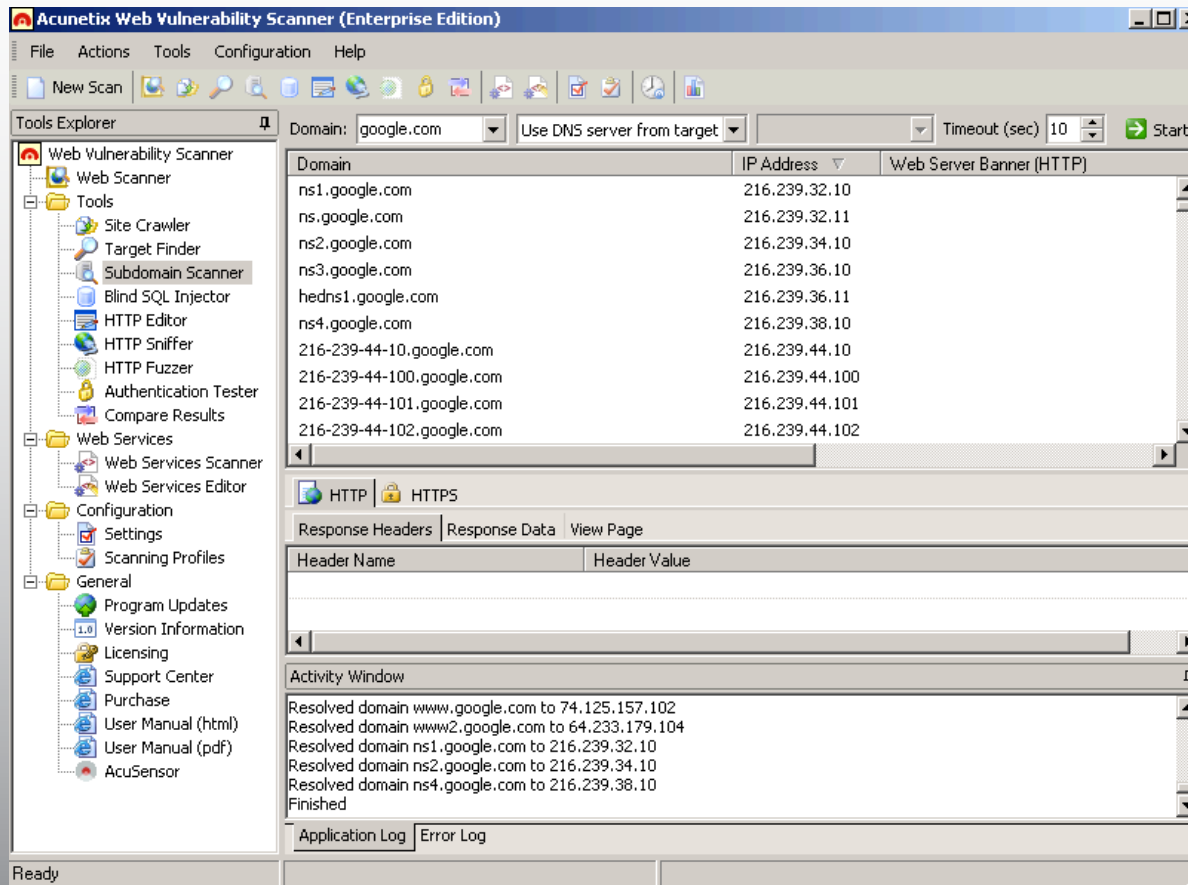
# Finding Subdomains

- Google Dorks - site: | inurl: | filetype: | intext: | intitle:
- Use your dorks to find subdomains



## Finding Subdomains cont...

- Use a sub-domain brute forcer
  - Code one in your scripting language of choice
  - Acunetix has one built in



[+] Bruting: google.com

[+] Threads: 20

[+] Words Loaded: 1906

=> Domains: 82 | Finished/Total: 1906/1906 | Complete 100%

[+] Sub-Domains Found

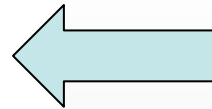


```
72.14.204.147 : academico.google.com
72.14.204.112 : ads.google.com
72.14.204.102 : alerts.google.com
72.14.204.147 : ap.google.com
72.14.204.102 : apps.google.com
66.249.89.104 : asia.google.com
72.14.204.191 : blog.google.com
72.14.204.102 : calendar.google.com
72.14.204.102 : catalog.google.com
72.14.204.101 : code.google.com
72.14.204.102 : d.google.com
72.14.204.102 : dir.google.com
72.14.204.102 : directory.google.com
72.14.204.102 : docs.google.com
72.14.204.147 : download.google.com
72.14.204.147 : downloads.google.com
72.14.204.102 : earth.google.com
72.14.204.102 : email.google.com
72.14.204.102 : europe.google.com
74.125.54.213 : feeds.google.com
72.14.204.147 : gd.google.com
74.125.227.46 : gg.google.com
72.14.204.102 : gmail.google.com
72.14.204.100 : group.google.com
```

# FINDING NETBLOCKS

- HOST

```
x@demonico:~$ host www.google.com
www.google.com is an alias for www.l.google.com.
www.l.google.com has address 74.125.45.106
www.l.google.com has address 74.125.45.147
www.l.google.com has address 74.125.45.99
www.l.google.com has address 74.125.45.103
www.l.google.com has address 74.125.45.104
www.l.google.com has address 74.125.45.105
x@demonico:~$
```



- WHOIS

```
x@demonico:~$ whois 74.125.45.99
#
# Query terms are ambiguous. The query is assumed to be:
# "n 74.125.45.99"
#
# Use "?" to get help.
#
#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=74.125.45.99?showDetails=true&showARIN=false
#
NetRange:      74.125.0.0 - 74.125.255.255
CIDR:          74.125.0.0/16
OriginAS:
NetName:       GOOGLE
NetHandle:     NET-74-125-0-0-1
Parent:        NET-74-0-0-0-0
NetType:       Direct Allocation
NameServer:    NS2.GOOGLE.COM
NameServer:    NS3.GOOGLE.COM
NameServer:    NS4.GOOGLE.COM
NameServer:    NS1.GOOGLE.COM
RegDate:       2007-03-13
Updated:       2007-05-22
Ref:           http://whois.arin.net/rest/net/NET-74-125-0-0-1
```



# FINDING WEBSERVERS

- NMAP
  - Best option
- Acunetix
  - Has a built in webserver finder
- WebInspect
  - Has a built in webserver finder
- Write your own script to do it..
  - Very easy and free also



This little guy is awesome

```
nmap -p80,443 -PN -oG google.com 74.125.45.0/24 |  
grep nothingtoseehere ; cat google.com |grep open |  
awk '{print $2}' > iplist.txt
```

```
x@demonico:~$ nmap -p80,443 -PN -oG google.com 74.125.45.0/24 | grep nothingtoseehere ; cat google.com |grep open  
Host: 74.125.45.17 (yx-in-f17.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.18 (yx-in-f18.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.19 (yx-in-f19.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.24 (yx-in-f24.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.32 (yx-in-f32.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.33 (yx-in-f33.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.34 (yx-in-f34.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.35 (yx-in-f35.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.36 (yx-in-f36.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.37 (yx-in-f37.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.38 (yx-in-f38.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.39 (yx-in-f39.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.40 (yx-in-f40.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.41 (yx-in-f41.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.42 (yx-in-f42.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.43 (yx-in-f43.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.44 (yx-in-f44.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.45 (yx-in-f45.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.46 (yx-in-f46.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.47 (yx-in-f47.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.48 (yx-in-f48.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.49 (yx-in-f49.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.50 (yx-in-f50.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.51 (yx-in-f51.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///  
Host: 74.125.45.52 (yx-in-f52.1e100.net) Ports: 80/open/tcp/http///, 443/open/tcp/https///
```

## FIND VIRTUAL HOSTED DOMAINS

- Currently, there are no commercial applications capable of doing this.
- There are a bunch of websites that do this.
  - <http://www.yougetsignal.com/tools/web-sites-on-web-server/>
  - <http://ip2web.web-max.ca/>
  - <http://bing.com> -- IP:74.125.45.17
- Bing is the way to go.
  - Bing has a API for programmer interface
  - <http://www.bing.com/developers> ←signup for your api key
  - I developed a python script to do this...
  - [sarries@hexsec.com](mailto:sarries@hexsec.com) email me if you want a copy

```
x@demonico:~$ ./ip2vhost.py iplist.txt
## ip2vhost through bing ##
##      Sean Arries      ##
#####

[+] finding vhosts for 111 IP's
[*] please wait...
[+] 1647 found!

0-oo.googlecode.com
1.bp.blogspot.com
100artisindonesia.blogspot.com
10khours.appspot.com
16.gmodules.com
2.bp.blogspot.com
3.bp.blogspot.com
31stentourage-nvk.appspot.com
3ceam.googlecode.com
3g-nokia.blogspot.com
4.bp.blogspot.com
6-4-2.blogspot.com
69sixty-nine.blogspot.com
74.125.45.100
74.125.45.101
74.125.45.102
74.125.45.105
74.125.45.113
74.125.45.147
74.125.45.99
9tm49u91btpu7le36r63p2sj07equiv5p.spreadsheets.gmodules.com
aatif.jaiku.com
addictionandrecoverynews.blogspot.com
adewale.jaiku.com
adirob.blogspot.com
adriansjournal.blogspot.com
adsense.google.com
adult-future.blogspot.com
adwords.google.co.uk
adwords.google.com
adwords.google.com.tr
adwords.google.de
```

# DETERMINE THE WEB APPLICATION RUNNING

- WhatWeb by Andrew Horton
  - Developed in Ruby
  - Detects over 250 web applications
  - Very active development
  - First public tool of its type
  - Carries out detection via simple regex detection
  - Does md5 matching
  - Does version detection
  - Has the function to crawl a site for other web applications
  - Can load a list vhosts 😊
- Very light impact. Nothing more than a request to the index page, is required to determine most web applications

x@demonic:~/pen/apps/whatweb-0.4.5\$ ./whatweb -i vhosts.txt

Attachment Move Junk Unread Categorize Follow Up Filters Contacts Search

http:// ERROR: bad URI (absolute but no path): http://

http://talky.l.google.com [302] Title[302 Moved], RedirectLocation[http://www.google.com/talk/], MD5[b31888224b72e5248b487e89445b6e00], Tag-Hash[ab

http://t13n.googlecode.com [301] HTTPServer[Apache], Title[301 Moved Permanently], RedirectLocation[http://code.google.com/p/t13n/], MD5[5be7a0852ce

http://syntaxhighlighter.googlecode.com [301] HTTPServer[Apache], Title[301 Moved Permanently], RedirectLocation[http://code.google.com/p/syntaxhig

5070ffce75]

http://svfobject.googlecode.com [301] HTTPServer[Apache], Title[301 Moved Permanently], RedirectLocation[http://code.google.com/p/svfobject/], MD5[4b

http://tabtomidi.appspot.com [200] Title[Tab to MIDI: Convert drum tabs to MIDI files], HTML5, HTTPServer[Google Frontend], JQuery, Header-Hash[7255

d6521b7e6bb33106a1e0e1634c3c0e5]

http://code.google.com/p/t13n [301] HTTPServer[codesite], UncommonHeaders[x-content-type-options,x-ss-protection], Title[301 Moved], RedirectLocat

ash[d3eb3e30e27ecb5b0263fa0e56ecb392]

http://sumpumptips.blogspot.com [200] UncommonHeaders[x-content-type-options,x-ss-protection], Google-Analytics[urchin][633524], HTTPServer[GSE],

84], Tag-Hash[2f2734e7863decefb2f70c66817f58e], Header-Hash[138d3e543aafc78289511a6cfffca0a06f], Footer-Hash[b0dd321032ec1e0c71cb8537d7acd359]

http://swimsuitmodeling.blogspot.com [200] AtomFeed[http://www.blogger.com/favicon.ico], Blogger, UncommonHeaders[x-content-type-options,x-ss-prob

RSSFeed[http://www.blogger.com/favicon.ico], OpenID, probably WordPress, Tag-Hash[d9ce7511a7b9ab47632c3e5a9ff563e4], Header-Hash[4aa795f868076cc6f

http://straymarks.net [302] HTTPServer[sffe], UncommonHeaders[x-content-type-options,x-ss-protection], Title[302 Moved], RedirectLocation[http://w

d8af9e36fe611d26]

http://suggestqueries.google.com [302] HTTPServer[sffe], UncommonHeaders[x-content-type-options,x-ss-protection], Title[302 Moved], RedirectLocati

1135d6dede9d8af9e36fe611d26]

http://support.google.com [301] HTTPServer[GSE], UncommonHeaders[x-content-type-options,x-frame-options,x-ss-protection], Title[Moved Permanently]

er-Hash[6fe1270d660d387b70f1908ab9cf35f5]

http://tjmhalfred.blogspot.com [200] AtomFeed[http://www.blogger.com/favicon.ico], Blogger, Title[Musings, Ramblings, and Things Left Unsaid], HT

ader-Hash[bbf8926772685de2b2614bb45b28a168], Tag-Hash[0729c24f213729e5bae378afb96b14f5], Footer-Hash[bff9de13592bf36a1e37b86b7a6dbd1a], MD5[d374f62f

http://stocksforbeginners.blogspot.com [200] AtomFeed[http://www.blogger.com/favicon.ico], Blogger, Title[Online Stock Trading for Beginners and Tr

protection], Header-Hash[bc59d5861012bfa7afe8711fbd8c8d31], Tag-Hash[3cb3fe7e187bcb7aee5651c9f50f3536], Footer-Hash[36744c5fbaf9a8af9acb07a35d0106a

http://stilldottie.blogspot.com [200] AdobeFlash, AtomFeed[http://www.blogger.com/favicon.ico], Blogger, Title[still dottie's diy tutorials, fashion

te@gmail.com], UncommonHeaders[x-content-type-options,x-ss-protection], Header-Hash[70e4a95949cdd1f850063b118e06154e], Tag-Hash[0866ec2e512c8e67af9

http://tarannowar.blogspot.com [200] AtomFeed[http://www.blogger.com/favicon.ico], Blogger, Cookies[blogger\_TID], Title[Future Husbands And Wives I

s[x-content-type-options,x-ss-protection], MD5[cf9296a91a95b6a5f141921283677fae], Tag-Hash[bfec7d230bc5807ff532b9bda4cd00b3], Footer-Hash[73db84f59

http://stevesregionalnewscaps.blogspot.com [200] AtomFeed[http://www.blogger.com/favicon.ico], Blogger, Title[Steve's Regional News Caps], HTML5, H

ss-protection], Header-Hash[36d271a63c70a54050205698798499e8], Tag-Hash[0b7942e269e0ad011552eb2b5eec34b0], Footer-Hash[ecf41af2a4e7e52eb86607877867

http://surfridercapolicy.blogspot.com [200] AdobeFlash, UncommonHeaders[x-content-type-options,x-ss-protection], HTTPServer[GSE], Title[Surfrider I

ger], MD5[9b4bbe5c1cdca87efabc5a63330e4462], Tag-Hash[743a0dae9bf4d1f213486968b444758b], Header-Hash[935b89aea814aa16d61aa74a457e1fc7], Footer-Hash

http://steppenraven.blogspot.com [200] AdobeFlash, AtomFeed[http://www.blogger.com/favicon.ico], Blogger, probably WordPress, HTTPServer[GSE], Unco

OpenID, PoweredBy[BannerFans.com], Mailto[dalibor.komaromi@gmail.com], Tag-Hash[1cc6f8468cf19f67c87e7108be24dad9], MD5[833ed3aad4b5af1f7c52722c2c7

http://statecollegeparealestate.blogspot.com [200] AtomFeed[http://www.blogger.com/favicon.ico], Blogger, Title[State College PA Real Estate], HTTP

er-Hash[f4d3cd8ddc60e23581fdd175196dad4e2], Tag-Hash[d19721560899c79a87738b4256b1ed6c], Footer-Hash[fe9c44a7d712e487b53e33c5306e66eb], MD5[956824c0f

http://code.google.com/p/t13n/ [200] Cookies[PREF], Title[t13n - Project Hosting on Google Code], HTTPServer[codesite], Mailto[transliteration-sup

b9aae], Tag-Hash[32b58da952df94426f4941c9d98d774c], Footer-Hash[10f55a21adebd4db41fd8d7d2ad70830], MD5[61aa0b25a023fb7773fcdf4d53f06d40] from my IP

http://static4.orkut.com [404] Title[404 Not Found], HTTPServer[orkut\_static\_fe], MD5[fc7aa91bb4ab99b9ad574c4c339c40b5], Header-Hash[66fc0f429e1ea72

## VULNERBILITY INFORMATION

- Now that we know what's out there, it's time to find some vulnerabilities for those web applications
- <http://cve.mitre.org/>
- <http://www.exploit-db.com/>
- <http://osvdb.org/>
- My favorite... Audit the application and find new 0day for yourself.



[HOME](#) > [CVE](#) > [SEARCH RESULTS](#)**About CVE**[Terminology](#)[Documents](#)[FAQs](#)**CVE List**[About CVE Identifiers](#)[Obtain a CVE Identifier](#)[Search CVE](#)[Search NVD](#)**CVE In Use**[CVE Adoption](#)[CVE-Compatible Products](#)[NVD for CVE Fix](#)[Information](#)[More . . .](#)**News & Events**[Calendar](#)[Free Newsletter](#)**Community**[CVE Editorial Board](#)[Sponsor](#)**Contact Us**[Search the Site](#)

## Search Results

There are **192** CVE entries or candidates that match your search.

Name	Description
<a href="#">CVE-2010-2924</a>	SQL injection vulnerability in myLDlinker.php in the myLinksDump Plugin 1.2 for WordPress allows remote attackers to execute arbitrary SQL comma these details are obtained from third party information.
<a href="#">CVE-2010-1186</a>	Cross-site scripting (XSS) vulnerability in xml/media-rss.php in the NextGEN Gallery plugin before 1.5.2 for WordPress allows remote attackers to inject parameter.
<a href="#">CVE-2010-0682</a>	WordPress 2.9 before 2.9.2 allows remote authenticated users to read trash posts from other authors via a direct request with a modified p parameter.
<a href="#">CVE-2010-0673</a>	SQL injection vulnerability in cplphoto.php in the Copperleaf Photolog plugin 0.16, and possibly earlier, for WordPress allows remote attackers to execute parameter.
<a href="#">CVE-2009-4748</a>	SQL injection vulnerability in mycategoryorder.php in the My Category Order plugin 2.8 and earlier for WordPress allows remote attackers to execute parameter in an act_OrderCategories action to wp-admin/post-new.php.
<a href="#">CVE-2009-4672</a>	Directory traversal vulnerability in main.php in the WP-Lytebox plugin 1.3 for WordPress allows remote attackers to include and execute arbitrary local
<a href="#">CVE-2009-4424</a>	SQL injection vulnerability in results.php in the Pyrmont plugin 2 for WordPress allows remote attackers to execute arbitrary SQL commands via the id
<a href="#">CVE-2009-4170</a>	WP-Cumulus Plug-in 1.20 for WordPress, and possibly other versions, allows remote attackers to obtain sensitive information via a crafted request to i parameters, which reveals the installation path in an error message.
<a href="#">CVE-2009-4169</a>	Cross-site scripting (XSS) vulnerability in wp-cumulus.php in the WP-Cumulus Plug-in before 1.22 for WordPress allows remote attackers to inject arbitrary vectors.
<a href="#">CVE-2009-4168</a>	Cross-site scripting (XSS) vulnerability in Roy Tanck tagcloud.swf, as used in the WP-Cumulus plugin before 1.23 for WordPress and the Joomla! mod attackers to inject arbitrary web script or HTML via the tagcloud parameter in a tags action. Cross-site scripting (XSS) vulnerability in tagcloud.swf in t WordPress allows remote attackers to inject arbitrary web script or HTML via the tagcloud parameter.
<a href="#">CVE-2009-3891</a>	Cross-site scripting (XSS) vulnerability in wp-admin/press-this.php in WordPress before 2.8.6 allows remote authenticated users to inject arbitrary web selection variable).
<a href="#">CVE-2009-3890</a>	Unrestricted file upload vulnerability in the wp_check_filetype function in wp-includes/functions.php in WordPress before 2.8.6, when a certain config Apache HTTP Server is enabled, allows remote authenticated users to execute arbitrary code by posting an attachment with a multiple-extension file a direct request to a wp-content/uploads/ pathname, as demonstrated by a .php.jpg filename.

- Thanks for attending.
  - Questions?

