



Pulp Google Hacking

The Next Generation Search Engine Hacking Arsenal

09 December 2011 – BayThreat 2011 – San Francisco, CA



Presented by:
Francis Brown
Stach & Liu, LLC
www.stachliu.com

Agenda

OVERVIEW

- Introduction/Background
- Advanced Attacks
 - Google/Bing Hacking - Core Tools
 - **NEW** Diggity Attack Tools
- Advanced Defenses
 - Google/Bing Hacking Alert RSS Feeds
 - **NEW** Diggity Alert Feeds and Updates
 - **NEW** Diggity Alert RSS Feed Client Tools
- Future Directions



Introduction/ Background

GETTING UP TO SPEED





Open Source Intelligence

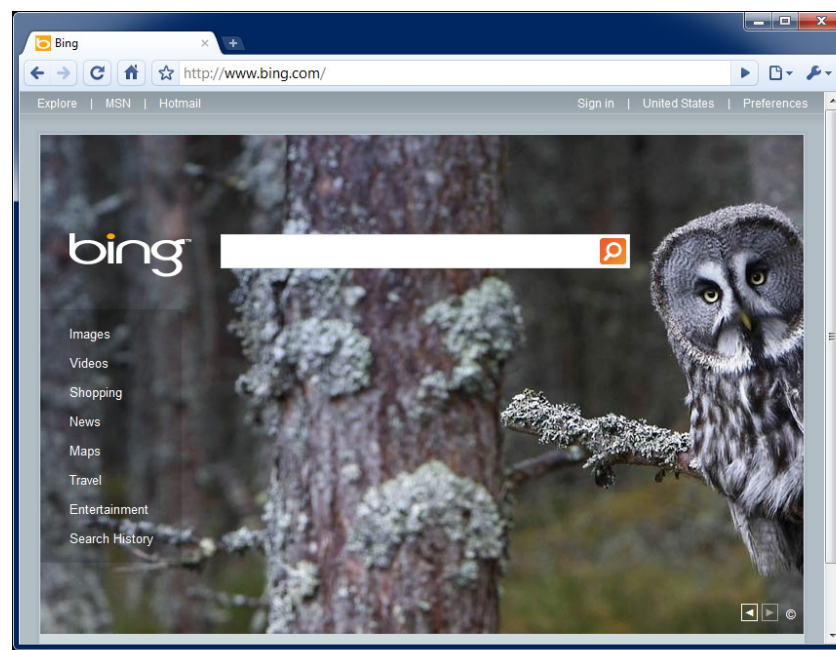
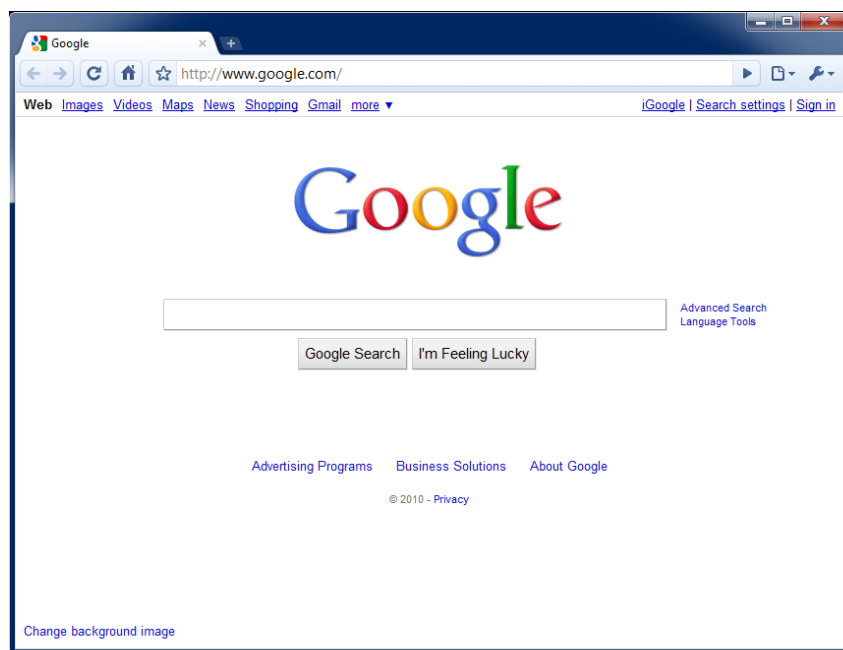
SEARCHING PUBLIC SOURCES

OSINT – is a form of intelligence collection management that involves finding, selecting, and acquiring information from *publicly available* sources and analyzing it to *produce actionable intelligence*.



Google/Bing Hacking

SEARCH ENGINE ATTACKS





Google/Bing Hacking

SEARCH ENGINE ATTACKS

Bing's source leaked!



```
class Bing {  
    public static string Search(string  
        query)  
    {  
        return Google.Search(query);  
    }  
}
```



Attack Targets

GOOGLE HACKING DATABASE

- Advisories and Vulnerabilities (215)
- Error Messages (58)
- Files containing juicy info (230)
- Files containing passwords (135)
- Files containing usernames (15)
- Footholds (21)
- Pages containing login portals (232)
- Pages containing network or vulnerability data (59)
- Sensitive Directories (61)
- Sensitive Online Shopping Info (9)
- Various Online Devices (201)
- Vulnerable Files (57)
- Vulnerable Servers (48)
- Web Server Detection (72)



Google Hacking = Lulz

REAL WORLD THREAT

LulzSec and Anonymous believed to use Google Hacking as a primary means of identifying vulnerable targets.



Their releases have nothing to do with their goals or their lulz. It's purely based on whatever they find with their "google hacking" queries and then release it.

- A-Team, 28 June 2011



Google Hacking = Lulz

REAL WORLD THREAT

22:14 <@kayla> Sooooo...using the link above and the *google hack string*.
!Host=. * intext:enc_UserPassword=* ext:pcf* Take your pick of VPNs you
want access too. Ugghh.. *Aaron Barr CEO HBGary Federal Inc.*

22:15 <@kayla> download the pcf file

22:16 <@kayla> then use *http://www.unix-ag.uni-kl.de/~massar/bin/cisco-decode?enc=* to clear text it

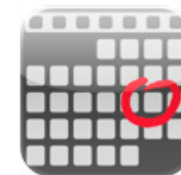
22:16 <@kayla> = *free VPN*



The screenshot shows a Google search interface. The search bar contains the query `!Host=*. * intext:enc_UserPassword=* ext:pcf`. Below the search bar, it indicates "About 877 results (0.24 seconds)". On the left side, there are navigation links for "Everything", "Images", "Videos", "News", "Shopping", and "More". The search results list two items:

- DentsuVPN.pcf**
www.net-root.com/files/Cisco/DentsuVPN.pcf - United Kingdom - Cached
[main] Description= **Host=109.204.23.27** AuthType=1 ... UserPassword=**enc_UserPassword=** NTDomain= EnableBackup=0 BackupServer= EnableMSLogon=1 MSLogonType=0 ...
- csd-kerb.pcf**
www.cs.umd.edu/~ntg/csvpn/csd-kerb.pcf - Cached
[main] Description= **Host=vpn.cs.umd.edu** AuthType=1 GroupName=csd-kerb GroupPwd= ... Username= SaveUserPassword=1 UserPassword= **enc_UserPassword=** NTDomain= ...

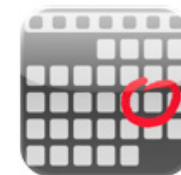
A red callout bubble points to the search bar with the text "Google Hacking search used by Kayla of LulzSec".



Quick History

GOOGLE HACKING RECAP

Dates	Event
2004	Google Hacking Database (GHDB) begins
May 2004	Foundstone SiteDigger v1 released
Jan 2005	Foundstone SiteDigger v2 released
Feb 13, 2005	Google Hack HoneyPot first release
Feb 20, 2005	Google Hacking v1 released by Johnny Long
Jan 10, 2006	MSNPawn v1.0 released by NetSquare
Dec 5, 2006	Google stops issuing Google SOAP API keys
Mar 2007	Bing disables inurl: link: and linkdomain:
Nov 2, 2007	Google Hacking v2 released



Quick History...cont.

GOOGLE HACKING RECAP

Dates	Event
Mar 2008	cDc Goolag - gui tool released
Sept 7, 2009	Google shuts down SOAP Search API
Nov 2009	Binging tool released by Blueinfy
Dec 1, 2009	FoundStone SiteDigger v 3.0 released
2010	Googlag.org disappears
April 21, 2010	Google Hacking Diggity Project initial releases
Nov 1, 2010	Google AJAX API slated for retirement
Nov 9, 2010	GHDB Reborn Announced – Exploit-db.com
July 2011	Bing ceases <code>&format=rss'</code> support



Advanced Attacks

WHAT YOU SHOULD KNOW






Diggity Core Tools

STACH & LIU TOOLS



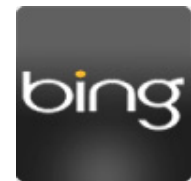
Google Diggity

- Uses **Google JSON/ATOM API** 
 - Not blocked by Google bot detection
 - Does not violate Terms of Service
- Required to use **Google custom search**



Bing Diggity

- Uses Bing 2.0 SOAP API
- Company/Webapp Profiling
 - Enumerate: URLs, IP-to-virtual hosts, etc.
- Bing Hacking Database (BHDB)
 - Vulnerability search queries in Bing format





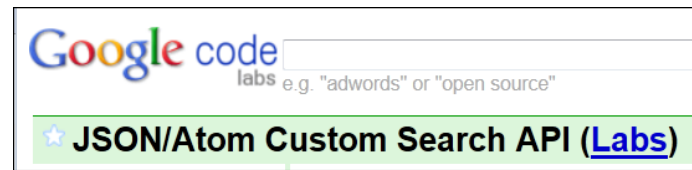
New Features



DIGGITY CORE TOOLS

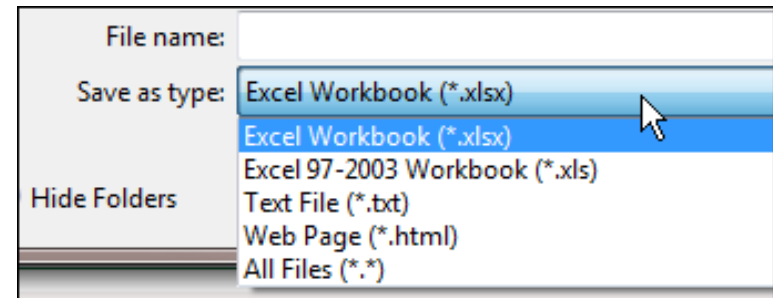
Google Diggity - New API

- Updated to use **Google JSON/ATOM API**
- Due to deprecated Google AJAX API



Misc. Feature Upgrades

- Auto-update for dictionaries
- Output export formats
 - Now also XLS and HTML
- Help File – chm file added



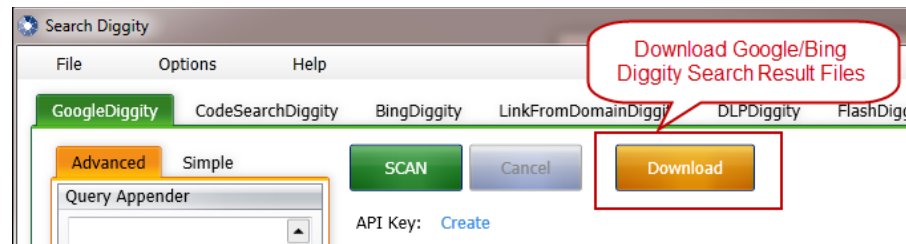
New Features



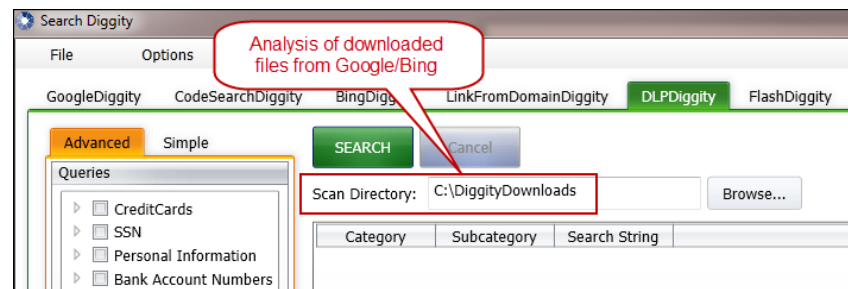
DOWNLOAD BUTTON

Download Buttons for Google/Bing Diggity

- Download actual files from Google/Bing search results
 - Downloads to default: `C:\DiggityDownloads\`



- Used by other tools for file download/analysis:
 - FlashDiggity, DLP Diggity, MalwareDiggity,...

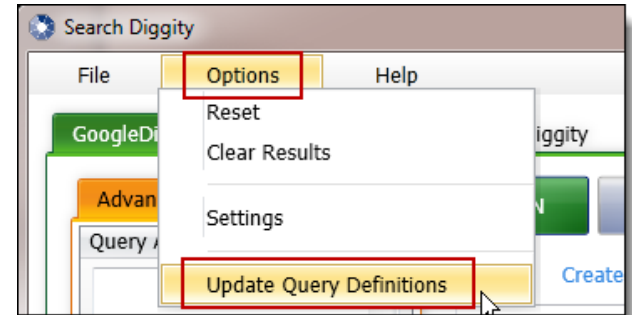




New Features

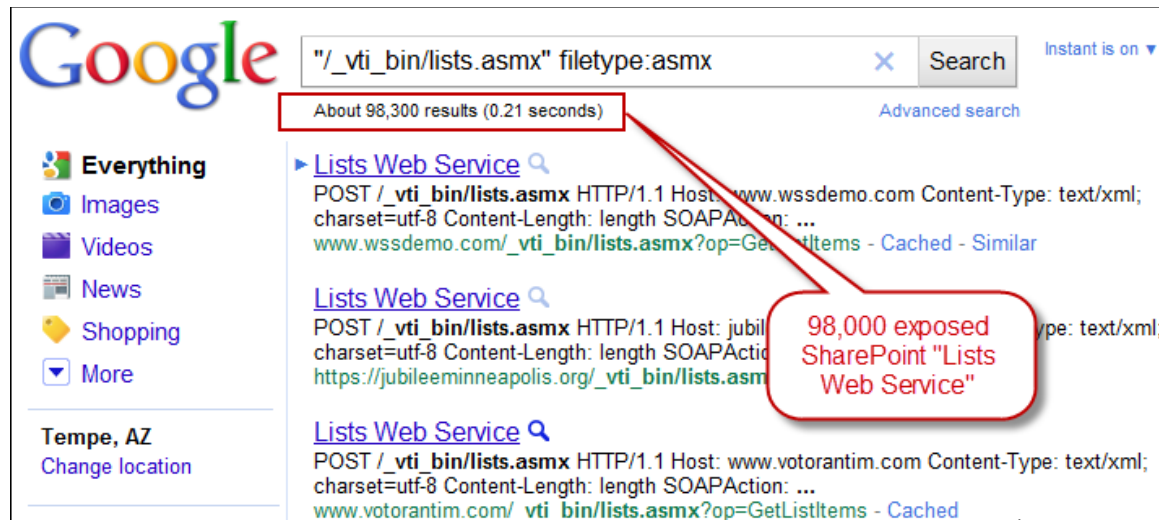


AUTO-UPDATES



SLDB Updates in Progress

- Example: SharePoint Google Dictionary
 - <http://www.stachliu.com/resources/tools/sharepoint-hacking-diggity-project/#SharePoint> – GoogleDiggity Dictionary File





Dictionary Updates



3RD PARTY INTEGRATION

New maintainers of the GHDB – 09 Nov 2010

- <http://www.exploit-db.com/google-hacking-database-reborn/>

Google Hacking Database Reborn

9th November 2010 - by admin

The incredible amount of information continuously leaked onto the Internet, and therefore accessible by Google, is of great use to penetration testers around the world. Johnny Long of [Hackers for Charity](#) started the Google Hacking Database (GHDB) to serve as a repository for search terms, called Google-Dorks, that expose sensitive information, vulnerabilities, passwords, and much more.

GOOGLE
HACKING-DATABASE

As Johnny is now pursuing his [mission in Uganda](#), he has graciously allowed us at The Exploit Database to pick up where the GHDB left off and resurrect it. It is with great excitement that we announce that the [GHDB](#) is now being hosted by us and actively maintained again. This will allow us to tie the GHDB directly into our database of exploits providing the most current information possible.

Google Diggity

DIGGITY CORE TOOLS



The screenshot shows the Google Diggity application window. The interface includes a menu bar (File, Options, Help), a toolbar with 'SCAN', 'Cancel', and 'Download' buttons, and a 'Sites/Domains' list containing 'stachliu.com'. The 'Advanced' tab is selected, showing a 'Query Appender' and a tree view of 'Queries' with categories like FSDB, GHDB, and Advisories and Vulnerabilities. The 'Output' pane displays the results of a scan, including the API key, scan start time, number of results found, and scan completion time.

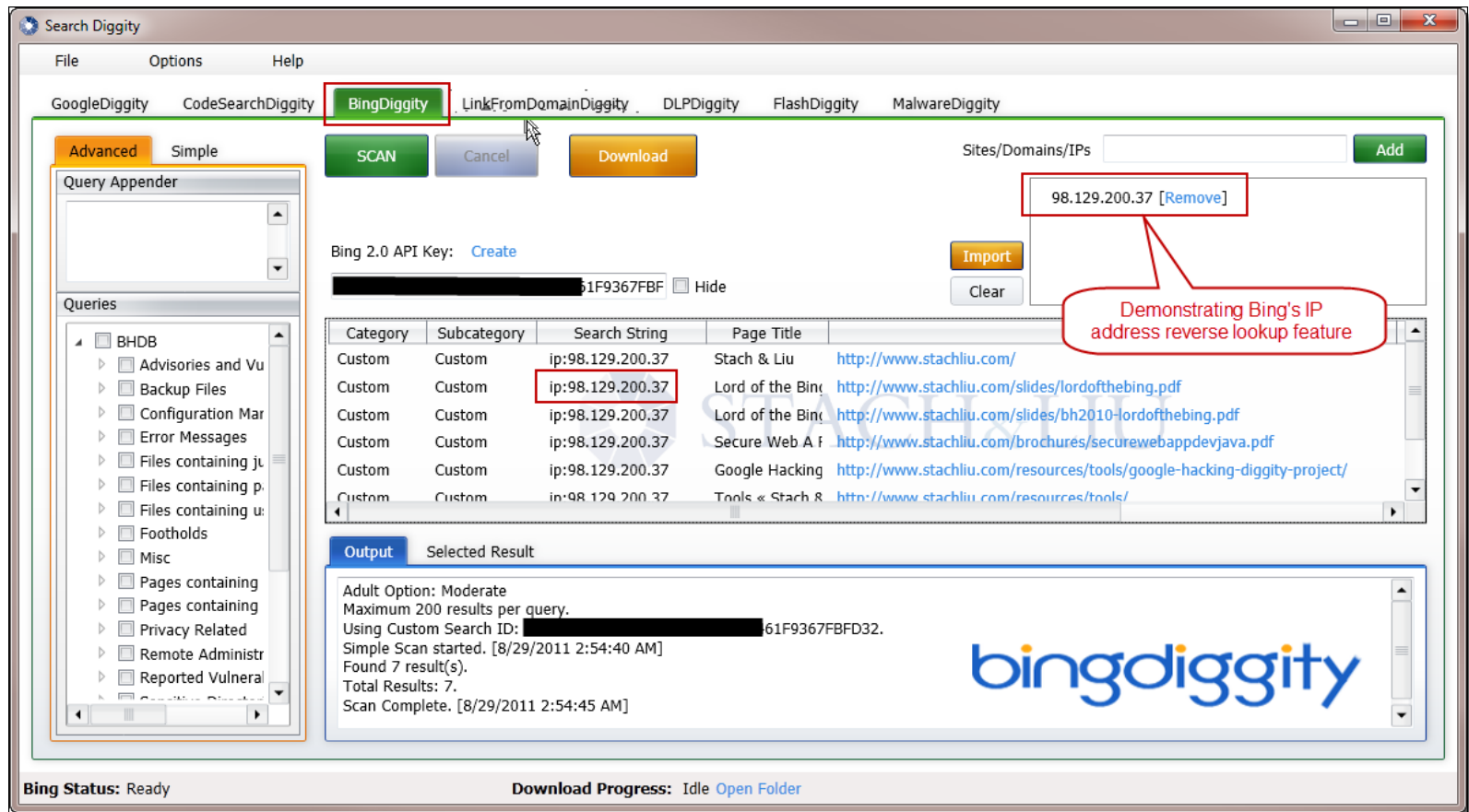
Category	Subcategory	Search String	Page Title	URL
Custom	Custom	site:stachliu.com	Stach & Liu	http://www.stachliu.com/
Custom	Custom	site:stachliu.com	Services « Stac	http://www.stachliu.com/services/
Custom	Custom	site:stachliu.com	Resources « St	http://www.stachliu.com/resources/
Custom	Custom	site:stachliu.com	Company « Sta	http://www.stachliu.com/company/

Output Selected Result

```
Using API Key: AIzaSyDIIUASIVNLE-aw_jIuzFRUz7BUC-9qK1EUKDM.  
Simple Scan started. [8/3/2011 3:39:44 AM]  
Found 45 result(s).  
Total Results: 45.  
Scan Complete. [8/3/2011 3:39:54 AM]
```

Bing Diggity

DIGGITY CORE TOOLS



The screenshot shows the Bing Diggity application window. The 'BingDiggity' tab is active. The interface includes a menu bar (File, Options, Help), a toolbar with 'SCAN', 'Cancel', and 'Download' buttons, and a search input field containing '98.129.200.37'. Below the search field, there is a 'Bing 2.0 API Key' field with a 'Create' link and a 'Hide' checkbox. A table of search results is displayed, with the IP '98.129.200.37' highlighted in red in the 'Search String' column. A red callout bubble points to the IP in the search field with the text 'Demonstrating Bing's IP address reverse lookup feature'. The 'Output' section at the bottom shows the scan results, including the API key and the number of results found.

Category	Subcategory	Search String	Page Title
Custom	Custom	ip:98.129.200.37	Stach & Liu http://www.stachliu.com/
Custom	Custom	ip:98.129.200.37	Lord of the Bin http://www.stachliu.com/slides/lordofthebing.pdf
Custom	Custom	ip:98.129.200.37	Lord of the Bin http://www.stachliu.com/slides/bh2010-lordofthebing.pdf
Custom	Custom	ip:98.129.200.37	Secure Web A f http://www.stachliu.com/brochures/securewebappdevjava.pdf
Custom	Custom	ip:98.129.200.37	Google Hacking http://www.stachliu.com/resources/tools/google-hacking-diggity-project/
Custom	Custom	ip:98.129.200.37	Tools « Stach & Liu http://www.stachliu.com/resources/tools/

Output Selected Result

Adult Option: Moderate
Maximum 200 results per query.
Using Custom Search ID: [REDACTED]61F9367FBFD32.
Simple Scan started. [8/29/2011 2:54:40 AM]
Found 7 result(s).
Total Results: 7.
Scan Complete. [8/29/2011 2:54:45 AM]

Bing Status: Ready **Download Progress:** Idle [Open Folder](#)



Bing Hacking Database



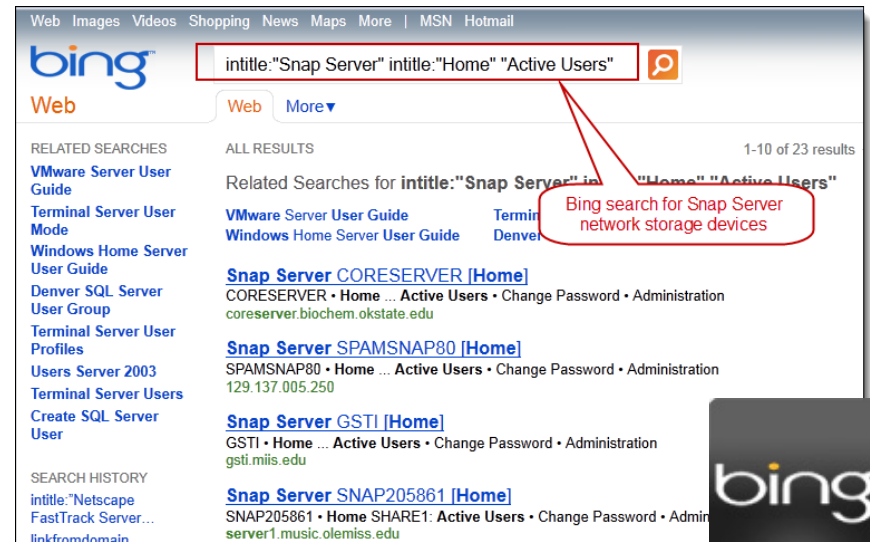
STACH & LIU TOOLS

BHDB – Bing Hacking Data Base

- First ever Bing hacking database
- Bing hacking limitations
 - Disabled **inurl:**, **link:** and **linkdomain:** directives in March 2007
 - No support for **ext:**, **allintitle:**, **allinurl:**
 - Limited **filetype:** functionality
 - Only 12 extensions supported

Example - Bing vulnerability search:

- GHDB query
 - "allintitle:Netscape FastTrack Server Home Page"
- BHDB version
 - intitle:"Netscape FastTrack Server Home Page"





Hacking CSE's



ALL TOP LEVEL DOMAINS

GoogleDiggity

Google custom search

All Top Level Domains


Google™ Custom Search

Search engine details

All top level domains:
<http://data.iana.org/TLD/tlds-alpha-by-domain.txt>

searches sites including: *.ZW/*, *.ZM/*, *.ZA/*, *.YT/*, *.YE/*

Last updated: July 21, 2011

Add this search engine to your [Google homepage](#): 

[Add this search engine to your blog or webpage »](#)

[Create your own Custom Search Engine »](#)



NEW GOOGLE HACKING TOOLS

Code Search Diggity

Google Code Search



VULNS IN OPEN SOURCE CODE

- Regex search for vulnerabilities in indexed public code, including popular open source code repositories:



- Example: SQL Injection in ASP querystring
 - `select.*from.*request\..QUERYSTRING`

The screenshot shows a Google Code Search result for the query `select.*from.*request\..QUERYSTRING`. The search results page displays the file `post.asp` with the following code snippet:

```
45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ÄÏÄÖÂ×÷Öß°í¹ÙÀíÔ±²ÄÄÜ±à±Öâ,òìú×ó."

57: strSql = "SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ÄÏÄÖÂ×÷Öß°í¹ÙÀíÔ±²ÄÄÜ±à±Öâ,òìú×ó."
```

A red callout box points to the `reply_id` parameter in the first line of code, stating: `reply_id` is SQL injectable querystring parameter. The search results also show the URL `www.cnarts.net/eweb/download/software/bbs/tradeforum.zip` and the text "Unknown - ASP - More from tradeforum.zip »".

CodeSearch Diggity

AMAZON CLOUD SECRET KEYS



Search Diggity

File Options Help

GoogleDiggity **CodeSearchDiggity** BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity MalwareDiggity

Advanced Simple

SCAN Cancel

Category	Subcatogo	Search String	Page Title	URL
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/simond/j	http://www.google.com/codesearch/p?hl=en#Kcy
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/simond/j	http://www.google.com/codesearch/p?hl=en#Kcy
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/chron	http://www.google.com/codesearch/p?hl=en#CQl
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/chron	http://www.google.com/codesearch/p?hl=en#CQl
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	chrome/content	http://www.google.com/codesearch/p?hl=en#ulAl
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	chrome/content	http://www.google.com/codesearch/p?hl=en#ulAl
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/eifaw	http://www.google.com/codesearch/p?hl=en#aM
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/EC2Samp	http://www.google.com/codesearch/p?hl=en#nfD
Amazon Keys	Amazon	amazon.*[A-Z0-9]{20}	lookups.py	http://www.google.com/codesearch/p?hl=en#474

Amazon AWS Cloud keys stored in plaintext

Output Selected Result

```
<pre>
Jec2 ec2 = new J<b>ec2("AK[REDACTED]ZEHQ"</b>, "[REDACTED]+RCIkuoEeAD6");
</pre>
```




Cloud Security

NO PROMISES...NONE

Amazon AWS Customer Agreement

- <http://aws.amazon.com/agreement/#10>

10. Disclaimers.

No guarantee of confidentiality, integrity, or availability (the CIA security triad) of your data in any way

THE SERVICE OFFERINGS ARE PROVIDED "AS IS." WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.



NEW GOOGLE HACKING TOOLS

Bing LinkFromDomainDiggity

Bing LinkFromDomain

DIGGITY TOOLKIT



The screenshot shows the Search Diggity application window. The 'LinkFromDomain' tool is selected in the top menu. The interface includes a 'SCAN' button, a 'Cancel' button, a 'Bing 2.0 API Key' field with a 'Create' link, and a 'Domain' field containing 'stachliu.com'. Below these are tabs for 'URLs', 'Applications', 'Hosts', and 'Domains'. The 'URLs' tab is active, displaying a list of external links. A red callout box points to this list with the text: 'External links then sorted and extracted into: applications, host names, and domains'. Another red callout box points to the 'URLs' tab with the text: 'Bing's linkfromdomain: directive used to find external links on your sites'. The 'Output' section at the bottom shows the following text: 'Maximum 200...', 'Using Custom Search ID: [redacted]9367FBFD32.', 'Found 25 result(s) for query: "linkfromdomain:stachliu.com".', 'Total Results: 25.', and 'Scan Complete. [4/21/2011 1:01:30 AM]'. The status bar at the bottom indicates 'Google Status: Ready' and 'Bing Status: Ready'.

Bing LinkFromDomain



FOOTPRINTING LARGE ORGANIZATIONS

The screenshot shows the LinkFromDomainDiggity tool interface. The 'Query Appender' field contains 'site:gov.cn'. The 'Sites/Domains' field contains 'www.gov.cn'. The 'Hosts' tab is selected, displaying a list of hostnames: 2010.visithainan.gov.cn, app.mps.gov.cn, bg.mofcom.gov.cn, bjsat.gov.cn, bjyouth.gov.cn, catf.agri.gov.cn, and cc.fjkl.gov.cn. The 'Output' pane shows the search results: 'Using [redacted] F9367FBFD32. Advanced Scan started. [9/10/2011 2:16:54 PM] Found 445 result(s) for query: "linkfromdomain:www.gov.cn site:gov.cn". Total Results: 445. Scan Complete. [9/10/2011 2:17:26 PM]'.

1. Running Bing's linkfromdomain:www.gov.cn to get list of off-site links from China's government main website

2. Also filtering results to just those also part of the gov.cn domain

3. Results in large list of other valid Chinese government hostnames on the gov.cn domain.



NEW GOOGLE HACKING TOOLS

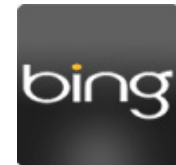
Malware Diggity

MalwareDiggity



DIGGITY TOOLKIT

1. Leverages Bing's `linkfromdomain`: search directive to find **off-site links of target** applications/domains



2. Runs off-site links against **Google's Safe Browsing API** to determine if any are malware distribution sites



3. Return results that identify malware sites that your web applications are directly linking to



Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – WSJ.com – June 2010

- Popular websites victimized, become malware distribution sites to their own customers

Massive Malware Hits Media Web Sites

Security researchers estimate that roughly 7,000 Web pages were compromised in a SQL injection attack this week, including *The Wall Street Journal* and *Jerusalem Post*.

By Mathew J. Schwartz, [InformationWeek](#)

June 10, 2010

URL: <http://www.informationweek.com/story/showArticle.jstpl?articleID=225600347>

"Every time I load Jpost site, I get nas on Tuesday, referring to the Jerusalem

Sure enough, the Web sites of the *Jerusalem Post* and the Association of Christian Scholars sites serving malware to viewers.



From: www.itworld.com

Mass Web attack hits Wall Street Journal, Jerusalem Post

by Robert McMillan

June 9, 2010 —Internet users have been hit by a widespread Web attack that has compromised thousands of Web sites, including Web pages belonging to the Wall Street Journal and the Jerusalem Post.

Estimates of the total number of compromised Web sites vary between 7,000 and 114,000, according to security experts. Other compromised sites include servicewomen.org and intjobs.org.

Mass Injection Attacks



MALWARE GONE WILD

Malware Distribution Woes – LizaMoon – April 2011

- Popular websites victimized, become malware distribution sites to their own customers

The screenshot shows a Slashdot article page. The article title is "Viral Scareware Infects Four Million Websites", highlighted with a red box. The author is "oxide7" and the post was made on Saturday April 02, @04:55PM. The article text describes a fast-spreading SQL injection attack that illegally peddles a bogus scareware, compromising millions of websites. A red box highlights the phrase "new malicious mass-injection campaign" in the text. A blue shield icon is visible on the right side of the article content. In the background, a keyboard key labeled "Install Malware" is visible.

Slashdot

stories **Viral Scareware Infects Four Million Websites**

recent

popular

ask slashdot

book reviews

games

idle

Posted by **timothy** on Saturday April 02, @04:55PM from the warning-your-computer-may-be-at-risk dept.

oxide7 writes

"A fast-spreading SQL injection attack that illegally peddles a bogus scareware has been breaking anti-virus barriers and compromising millions of websites, besides defrauding unsuspecting victims. The news of this attack was brought out by Websense Security Labs in its blog last week. Websense said its Threatseeker Network identified a **new malicious mass-injection campaign** which it named LizaMoon."

Mass Injection Attacks



MALWARE GONE WILD

Malware Distribution Woes – willysy.com - August 2011

- Popular websites victimized, become malware distribution sites to their own customers

Malware attack spreads to 5 million pages (and counting)

Unpatched sites turn on visitors

By [Dan Goodin in San Francisco](#) • [Get more from this author](#)

Posted in [Malware](#), 2nd August 2011 18:07 GMT

An attack that targets a popular online commerce application has infected almost 5 million webpages with scripts that attempt to install malware on their visitors' computers.

The mass attack, which targets [osCommerce](#) store-management software, was first reported in late July. When researchers from [Armorize](#) searched for search results suggested by the search results showed that

Armorize Malware Blog



willysy.com Mass Injection ongoing, over 8 million infected pages, targets osCommerce sites

POSTED BY: CHRIS ON 7.25.2011 / CATEGORIES: [DRIVE-BY DOWNLOAD](#), [HACKALERT](#), [MASS INJECTION](#), [OSCOMMERCE](#), [WEB MALWARE](#)





Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – mysql.com - Sept2011

- Popular websites victimized, become malware distribution sites to their own customers

The image shows a screenshot of a Slashdot article. The article title is "Hacked MySQL.com used to serve Windows malware". The author is Elinor Mills, dated September 26, 2011. The article text mentions that MySQL.com was compromised and redirected visitors to a page serving malware. A keyboard key labeled "Install Malware" is overlaid on the right side of the screenshot. The Slashdot logo and navigation menu are visible on the left.

Malware Diggity

DIGGITY TOOLKIT



GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity **MalwareDiggity**

SCAN Cancel

Bing 2.0 API Key: [Create](#)
[Redacted]361463C6A

Google Safe Browsing API Key: [Create](#)
[Redacted]Qd1Qj0mx

Sites/Domains:

Import **Clear**

facebook.com [Remove]
youtube.com [Remove]
yahoo.com [Remove]
live.com [Remove]

Searching Top 1000 most visited web sites on the Internet for 3rd party malware links

Target Domain	Offsite URL	Offsite App	Diagnostic URL	Type
yoo7.com	http://www.resalh.com	http://www.resalh.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.resalh.com%2f	Malware
jxedt.com	http://www.cqgj.net	http://www.cqgj.net	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.cqgj.net%2f	Malware
jxedt.com	http://www.fit.sh.cn	http://www.fit.sh.cn	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.fit.sh.cn%2f	Malware
groupon.ru	http://www.vipspanadom.kiev.ua	http://www.vipspanadom.kiev.ua	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.vipspanadom.kiev.ua%2f	Malware
uuu9.com	http://www.mymym.com	http://www.mymym.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.mymym.com%2f	Malware
pole-emploi.fr	http://ecommerceparis.com	http://ecommerceparis.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fecommerceparis.com%2f20	Malware
pole-emploi.fr	http://ecommerceparis.com/2011/index.p	http://ecommerceparis.com/2011/index.p	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fecommerceparis.com%2f20	Malware
newgrounds.com	http://www.pornno.com	http://www.pornno.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.pornno.com%2f	Malware
battle.net	http://www.mymym.com	http://www.mymym.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.mymym.com%2f	Malware
hankooki.com	http://nbinside.com	http://nbinside.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.nbinside.com%2f	Malware
interpark.com	http://www.michoo.co.kr	http://www.michoo.co.kr	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.michoo.co.kr%2f2010	Malware
52pk.com	http://www.apforums.net	http://www.apforums.net	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.apforums.net%2f	Malware
sonyericsson.com	http://www.rock-your-mobile.com	http://www.rock-your-mobile.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.rock-your-mobile.com	Malware
nokerstrategv.com	http://www.canadaimmigrationvisa.com	http://www.canadaimmigrationvisa.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.canadaimmigrationvis	Malware

Example result: interpark.com (907th most visited site on web) is linking to michoo.co.kr (suspicious according to Google Safe Browsing API)

Google Safe Browsing diagnostic page for suspicious michoo.co.kr

Output

Found 1 result(s) for query: "malware:npr.org" [npr.org].
Found 0 result(s) for query: "malware:gamestop.com" [gamestop.com].
Found 0 result(s) for query: "malware:theweathernetwork.com" [theweathernetwork.com].
Total Results: 59.

Malware Diggity

DIGGITY TOOLKIT



INTERPARK 티켓

검색

유지컬

www.michoo.co.kr" site:interpark.com

Search Page 2 of about 29 results (0.09 seconds)

interpark.com does appear to have links to www.michoo.co.kr

Everything ▶ 주공행장(酒公行狀) - 예매는 인터파크 - 인터파크 티켓 - [Trans ticket.interpark.com/ticket/Goods/GoodsInfo.asp?GoodsCode...]

Images ... 년 3월 17일(금) ~ 3월 26일(일) 평일 19:30 / 토 16:00, 19:30 / 일 15:00 주 후원: 한국문화예술위원회 · 문의: 02-747-5161

www.michoo.co.kr ...

관람등급: 만 7세이상 (?)
관람시간: -
기본가: -

월드와이드 | Country

The 1000 most-visited sites on the web

Learn more about this list

Rank	Site	Category	Unique Visitors (users)
901	shentime.com	Movies	6,100,000
902	ovi.com	Mobile Apps & Ad	
903	zumi.pl	Business & P	
904	natwest.com	Banking	
905	peixurbano.com.br	Coupons & Discount Offers	6,100,000
906	soundcloud.com	Music Equipment & Technology	6,100,000
907	interpark.com	Shopping	6,100,000
908	hotpepper.jp	Dining Guides	6,100,000

So, the 907th most popular site on the web has URL links to suspected malware sites

Links to michoo.co.kr

알립니다

일시: 2006년 9월 3일(일) ~ 14일(목) [평일 19:30 / 토 15:00, 19:30 / 일 15:00]
주최: 극단미추
문의: 02-747-5161
홈페이지: www.michoo.co.kr/zhaos
■ 프리뷰 할인: 9월 2일(토) 7시 30분 ~ 10시 전석 15,000원
■ 조기예매할인: 전석 각 10,000원 할인

Google

"www.michoo.co.kr" site:interpark.com

Search Page 2 of about 29 results (0.09 seconds)

interpark.com does appear to have links to www.michoo.co.kr

Everything ▶ 주공행장(酒公行狀) - 예매는 인터파크 - 인터파크 티켓 - [Trans ticket.interpark.com/ticket/Goods/GoodsInfo.asp?GoodsCode...]

Images ... 년 3월 17일(금) ~ 3월 26일(일) 평일 19:30 / 토 16:00, 19:30 / 일 15:00 주 후원: 한국문화예술위원회 · 문의: 02-747-5161

www.michoo.co.kr ...

Worldwide | Country

The 1000 most-visited sites on the web

Learn more about this list

Rank	Site	Category	Unique Visitors (users)
901	shentime.com	Movies	6,100,000
902	ovi.com	Mobile Apps & Ad	
903	zumi.pl	Business & P	
904	natwest.com	Banking	
905	peixurbano.com.br	Coupons & Discount Offers	6,100,000
906	soundcloud.com	Music Equipment & Technology	6,100,000
907	interpark.com	Shopping	6,100,000
908	hotpepper.jp	Dining Guides	6,100,000

So, the 907th most popular site on the web has URL links to suspected malware sites

Links to michoo.co.kr

알립니다

일시: 2006년 9월 3일(일) ~ 14일(목) [평일 19:30 / 토 15:00, 19:30 / 일 15:00]
주최: 극단미추
문의: 02-747-5161
홈페이지: www.michoo.co.kr/zhaos
■ 프리뷰 할인: 9월 2일(토) 7시 30분 ~ 10시 전석 15,000원
■ 조기예매할인: 전석 각 10,000원 할인

Malware Diggity



DIAGNOSTICS IN RESULTS

www.google.com/safebrowsing/diagnostic?site=http://www.michoo.co.kr/2010madang/

Safe Browsing
Diagnostic page for michoo.co.kr

Advisory provided by Google

What is the current listing status for michoo.co.kr?
Site is listed as **suspicious** - visiting this web site may harm your computer.
Part of this site was listed for suspicious activity 7 days.

What happened when Google visited this site?
Of the 22 pages we tested on the site over the past 90 days, 16 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2011-09-06, and the last time suspicious content was found on this site was on 2011-09-06.

Malicious software includes 13 exploit(s), 9 scripting exploit(s).
Malicious software is hosted on 1 domain(s), including avitransport.com/.
This site was hosted on 1 network(s) including [AS3786 \(ERX\)](#).

Google Safe Browsing diagnostics page listing michoo.co.kr as "suspicious"



NEW GOOGLE HACKING TOOLS

DLP Diggity



DLP Diggity



LOTS OF FILES TO DATA MINE

Google

filetype:pdf

About 513,000,000 results (0.25 seconds)

Google

filetype:doc

About 84,500,000 results (0.10 seconds)

Google

filetype:xls

About 17,300,000 results (0.13 seconds)

bing

filetype:doc

Web More

SEARCH HISTORY ALL RESULTS 1-10 of 26,900,000 results · [Advanced](#)

bing

filetype:pdf

Web More

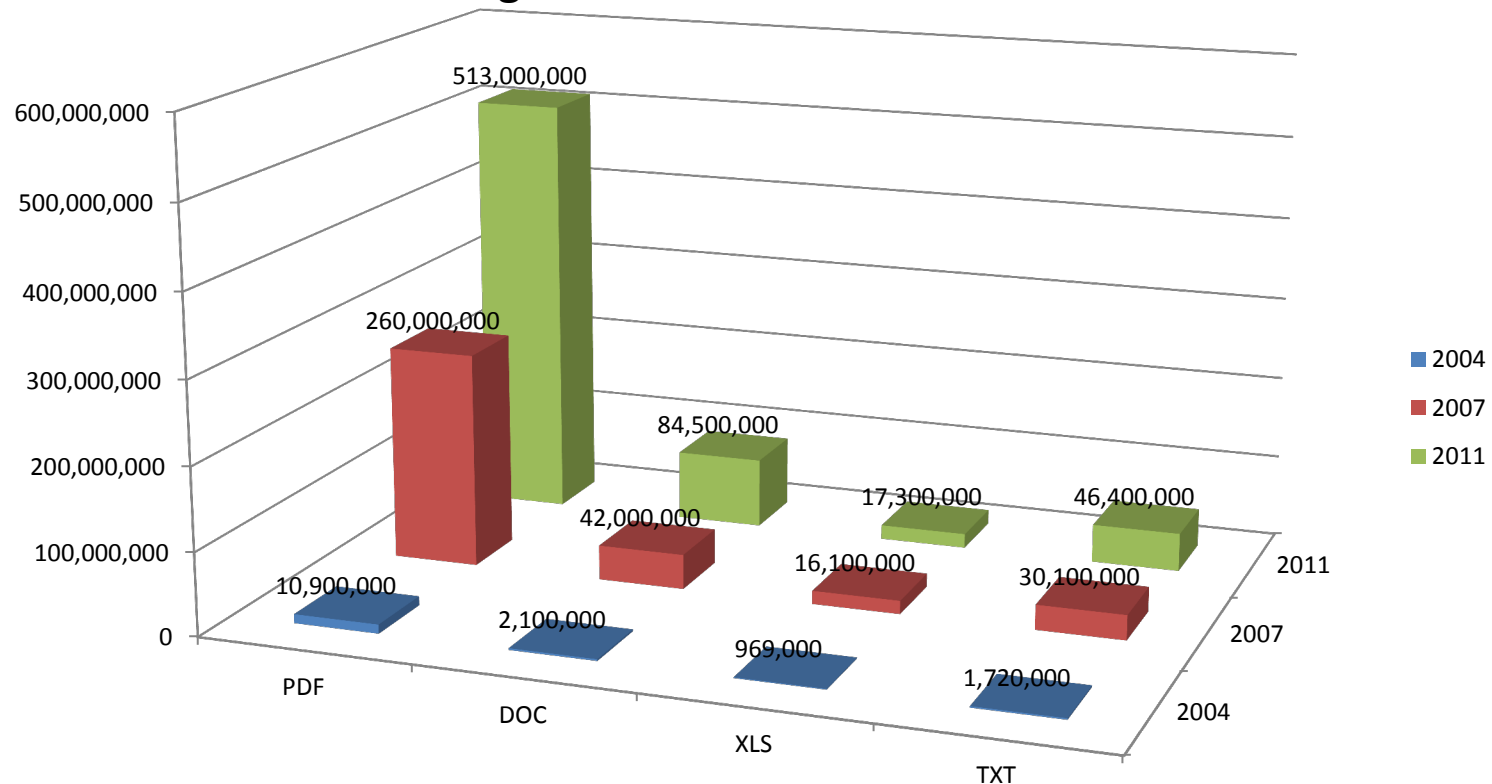
SEARCH HISTORY ALL RESULTS 1-10 of 146,000,000 results · [Advanced](#)



DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR

Google Results for Common Docs



DLP Diggity

DIGGITY TOOLKIT



GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity **DLPDiggity** FlashDiggity Mal...

Advanced Simple **SEARCH** Cancel

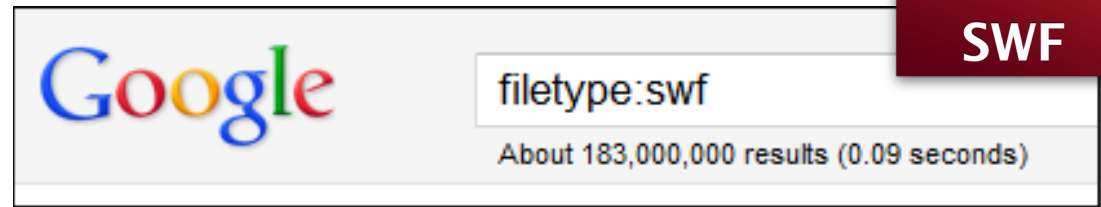
Scan Directory: C:\DiggityDownloads\ Browse...

Category	Subcategory	Search String	File
SSN	Social Security	[^A-Za-z0-9_]([0-6])d{	C:\DiggityDownloads\PIITutorial.doc
SSN	SSN LANL	(ss(n)? social(\s*securi	C:\DiggityDownloads\PIITutorial.doc

Output Selected Result

```
21 Jerry,
22 This is Mary. I forgot to include my social security number in those clearance documents I su
Would you mind adding it in for me? My SSN is 123-45-6789. Thanks a lot!
23 - Mary
24
```

Search through downloaded files from GoogleDiggity and BingDiggity for data leaks such as SSNs, credit cards, etc.



NEW GOOGLE HACKING TOOLS

FlashDiggity

Flash Diggity

DIGGITY TOOLKIT



- **Google** for SWF files on target domains
 - Example search: `filetype:swf site:example.com`
- **Download** SWF files to `C:\DiggityDownloads\`
- **Disassemble** SWF files and **analyze** for Flash vulnerabilities



GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity DLPDiggity **FlashDiggity** MalwareDiggity

Advanced Simple

SEARCH Cancel

Scan Directory: C:\DiggityDownloads Browse...

Category	Subcategory	Search String	File Path
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_13 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]

Output Selected Result

```
20 if (UserName.text == 'mizzico' && PassWord.text == 'furniture') {
21   getURL('http://www.dizzypixel.com/login/mizzico/login.html', '_blank');
22   login_incorrect_alpha = 0;
23 } else {
24   if (UserName.text == 'sonya' && PassWord.text == 'paz') {
25     getURL('http://www.dizzypixel.com/login/sonyapaz/index.html', 'blank');
```

Hardcoded usernames and passwords in cleartext in SWF file



NEW GOOGLE HACKING TOOLS

DEMO

GoogleScrape Diggity

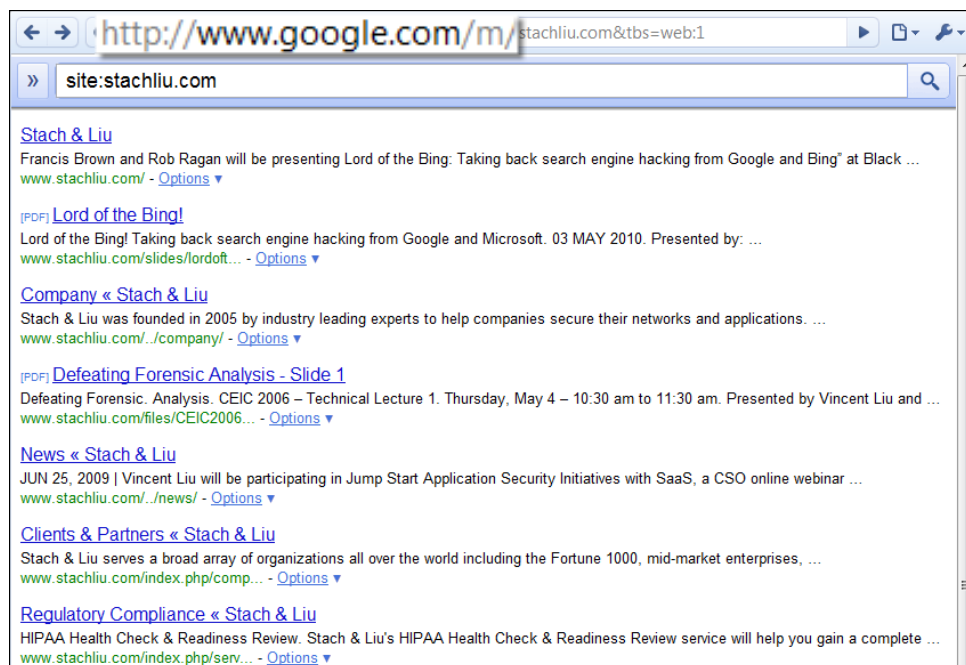
DIGGITY TOOLKIT



GoogleScrape Diggity

- Uses Google mobile interface
 - Light-weight, no advertisements
 - *Violates* Terms of Service
- Bot detection avoidance
 - Distributed via proxies
 - Spoofs User-agent and Referer headers
 - Random `&userip=` value
 - Across Google servers

COMING SOON





NEW GOOGLE HACKING TOOLS

Baidu Diggity

BaiduDiggity

CHINA SEARCH ENGINE



- Fighting back

COMING SOON

百度搜索_"supplied argu... x

www.baidu.com/s?bs=intitle%3A"Snap+Server"+intitle%3A"Home"+"Active+Use

Baidu 百度 新闻 网页 贴吧 知道 MP3 图片 视频 地图 更多

"supplied argument is not a valid MySQL result resource" site:gov.cn 百度一下

去掉""获得更多 [supplied argument is not a valid MySQL result resource site:gov.cn](#) 的搜索结果(于双引号)

信息内容添加

: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in D:\apache\phpmysql\htdocs\news\adm\newgl\newstj.php on line 11
[www.xjpi.gov.cn/news/adm/newgl/newstj.php](#) 2011-...

[中山市五桂山区办事处信息网](#)
Warning: mysql_free_result(): supplied argument is not a valid MySQL result resource in E:\site\phpsite\wgs\public\navigation.php on line 18...
[www.wuguishan.gov.cn/zhzx/zhzx_content.ph](#) ... 2011-2-17 - 百度快照

[堵河水电专业气象服务](#)
: mysql_num_rows(): supplied argument is not a valid MySQL result resource in E:\wwwroot\qxfw-shiyan.gov\web\duhe\inc_online.php...
[qxfw.shiyan.gov.cn/duhe/sdgk_dianzhan_xin](#) ... 2011-4-14 - 百度快照

[中山市五桂山区办事处信息网](#)
Warning: mysql_free_result(): supplied argument is not a valid MySQL result resource in E:\

Finding vulns in Chinese government sites

Advanced Defenses

PROTECT YO NECK

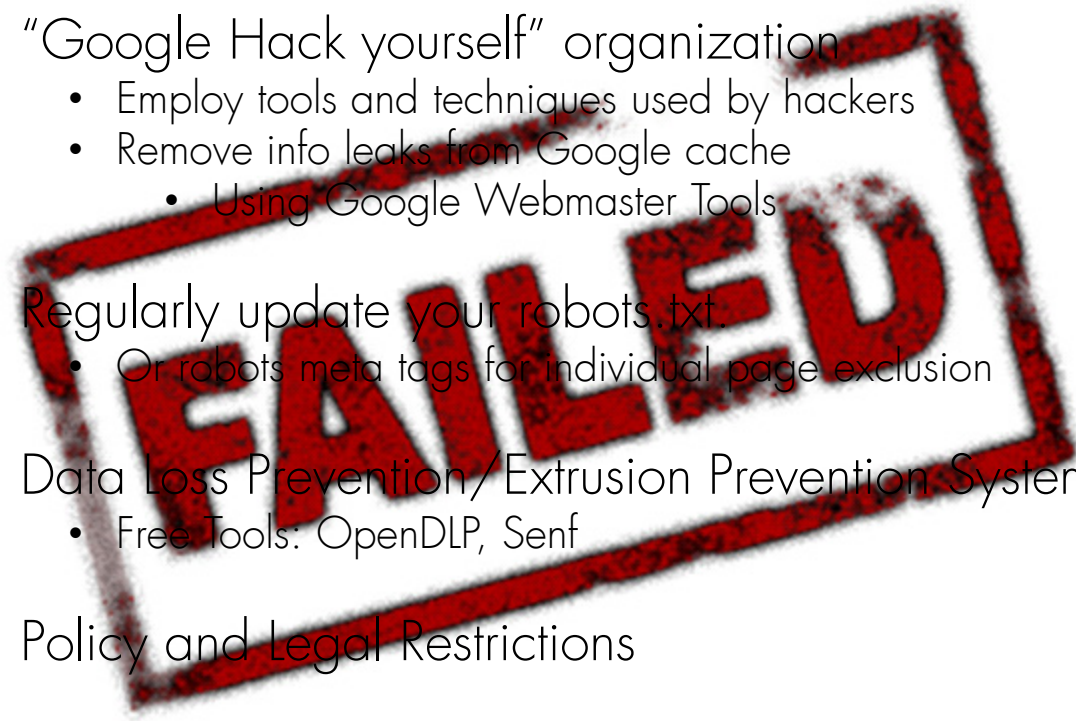




Traditional Defenses

GOOGLE HACKING DEFENSES

- “Google Hack yourself” organization
 - Employ tools and techniques used by hackers
 - Remove info leaks from Google cache
 - Using Google Webmaster Tools
- Regularly update your robots.txt
 - Or robots meta tags for individual page exclusion
- Data Loss Prevention/Extrusion Prevention Systems
 - Free Tools: OpenDLP, Senf
- Policy and Legal Restrictions





Existing Defenses

"HACK YOURSELF"



- ✓ Tools exist
- ✗ Convenient
- ✗ Real-time updates
- ✗ Multi-engine results
- ✗ Historical archived data
- ✗ Multi-domain searching



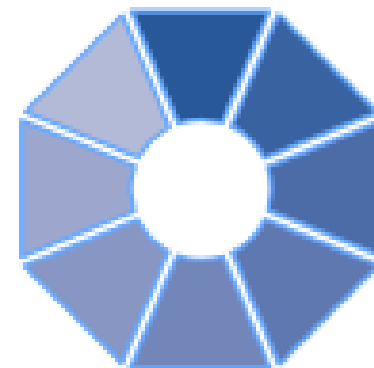
Advanced Defenses

NEW HOT SIZZLE



Stach & Liu now proudly presents:

- **Google and Bing Hacking Alerts**
 - SharePoint Hacking Alerts – 118 dorks
 - SHODAN Hacking Alerts – 26 dorks **NEW**
- **Diggity Alerts FUNdle Bundles** **NEW**
 - Consolidated alerts into 1 RSS feed
- **Alert Client Tools** **NEW**
 - Alert Diggity – Windows systray notifications
 - iDiggity Alerts – iPhone notification app



Google Hacking Alerts

ADVANCED DEFENSES



Google Hacking Alerts

- All hacking database queries using **Google alerts**
- Real-time vuln updates to >2400 hack queries via RSS
- Organized and available via **Google reader** importable file

Google alerts Manage your Alerts [email]@gmail.com | Settings | FAQ

Your Google Alerts

Search terms	Type	How often	Email length	Deliver to
<input type="checkbox"/> !Host=*.intext:enc_UserPassword=* ext:pcf	Web	as-it-happens	up to 50 results	Feed View in Google Reader
<input type="checkbox"/> "# Dumping data for table (username user users password)"	Web	as-it-happens	up to 50 results	Feed View in Google Reader
<input type="checkbox"/> "# Dumping data for table"	Web	as-it-happens	up to 50 results	Feed View in Google Reader
<input type="checkbox"/> "# phpMyAdmin MySQL-Dump" "INSERT INTO" -"the"	Web	as-it-happens	up to 50 results	Feed View in Google Reader

GHDB regexs made into Google Alerts

RSS Feeds generated that track new GHDB vulnerable pages in real-time

Google Hacking Alerts

ADVANCED DEFENSES



Google reader

All items (1000+)

People you follow

Explore

Subscriptions

- FSDB-Backup Files (195)
- FSDB-Configuration Ma... (371)
- FSDB-Error Messages (654)
- FSDB-Privacy Related (501)
- FSDB-Remote Administr... (102)
- FSDB-Reported Vulnera... (90)
- FSDB-Technology Profile (652)
- GHDB-Advisories and V... (1000+)
- GHDB-Error Messages (1000+)
- Google Alerts - "mySQ... (11)**
- Google Alerts - "A sv... (10)
- Google Alerts - "mySQL erro... with query" (11)
- Google Alerts - "acce... (45)
- Google Alerts - "An i... (1)
- Google Alerts - "ASP... (5)

Google Alerts - "mysql error with query"

Show: 11 new items - all items

Mark all as read

Refresh

Feed settings...

James Bond 007 :: MI6 - The Home Of James Bond

via [Google Alerts - "mysql error with query"](#)

mysql error with query SELECT c.citem as itemid, c.cnumber as commentid, c.cbody as body, c.cuser as user, c.cemail as userid, c.cemail as email, ...
www.mi6.co.uk/mi6.php3/news/index.php?itemid...

Add star Like Share Share with note Email Add tags

Several thousand GHDB/FSDDB vuln alerts generated each day

James Bond needs help!
mysql error page snippet conveniently provided in RSS summary

Bing Hacking Alerts

ADVANCED DEFENSES



Bing Hacking Alerts

- Bing searches with regexs from BHDB
- Leverages <http://api.bing.com/rss.aspx>
- Real-time vuln updates to >900 Bing hack queries via RSS

Google reader

All items Search

Add a subscription

All items (1000+)

People you follow

Explore

Subscriptions

BHDB-Advisories and V... (910)

BHDB-Backup Files (50)

BHDB-Configuration Ma... (207)

BHDB-Error Messages (507)

BHDB-Files containing... (607)

BHDB-Files containing... (343)

BHDB-Files containing... (50)

BHDB-Footholds (45)

BHDB-Misc (116)

BHDB-Pages containing... (765)

BHDB-Pages containing... (159)

BHDB-Privacy Related (196)

BHDB-Remote Administr... (36)

Bing: intitle:"Snap Server" intitle:"Home" "Active Users" »

Show: 0 new items - all items Mark all as read Refresh Feed settings...

★ Snap Server WELW-SNAP [Home] - WELW-SNAP • Home

★ Snap Server CORESERVER [Home] - CORESERVER • Home

★ Snap Server GSTI [Home] - GSTI • Home

★ adsphotographer.com - SNAP55373 • Home

★ Snap Server SNAP824929 [Home] - SNAP824929 • Home

★ Snap Server SAINTSNAP [Home] - SAINTSNAP • Home

★ Snap Server DIGITALDATA1 [Home] - BOT - Unavailable: folder does not exist. SHARE1: acesag - For ACES

Snap Server FTP-SERVER [Home]

Flinn - Flinn OFF-Site Backup: Home - Folder for network shares/drive mapping: MyHost - Folder for my perso
Web Hosting: msmcs.net - www.msmcs.net PUB FTP

★ Add star Like Share Share with note Email Keep unread Edit tags: BHDB-Various Online Dev

★ Snap Server XRAY7 [Home] - XRAY7 • Home

SNAP network attached storage servers exposed

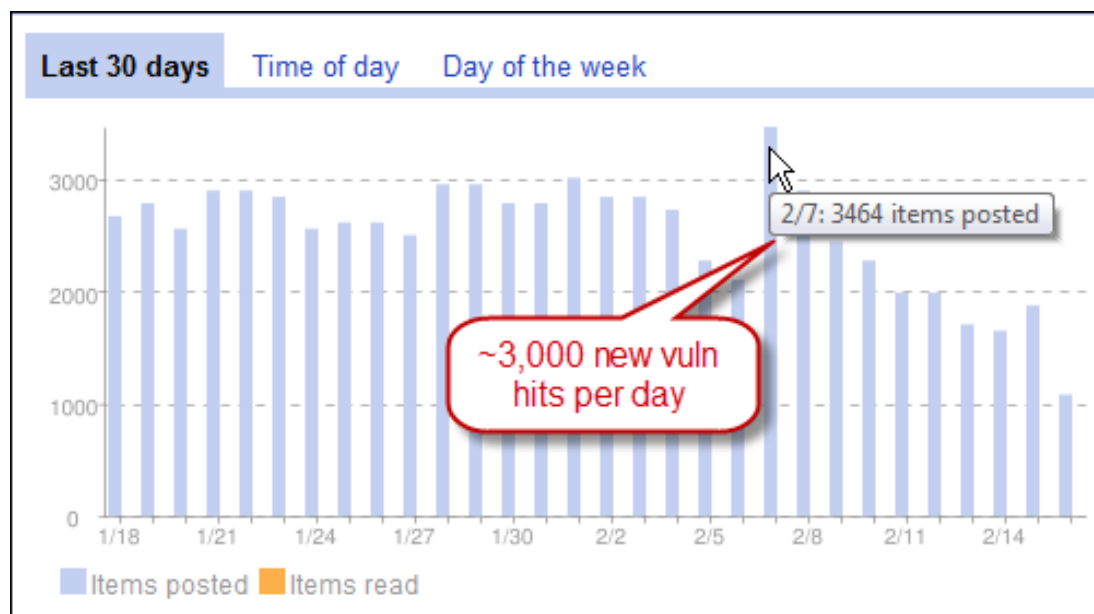
Bing/Google Alerts

LIVE VULNERABILITY FEEDS



World's Largest Live Vulnerability Repository

- Daily updates of *~3000 new hits per day*





Diggity Alerts 
One Feed to Rule Them All

ADVANCED DEFENSE TOOLS


Diggity Alert Fundle Bundle



FUNdle Bundle

ADVANCED DEFENSES



 **DIGGITY HACKING ALERTS**


"Diggity Hacking Alerts" bundle created by Stach

Description: All of the GHDB, FSDB, BHDB, and SLDB alert feeds.

A bundle is a collection of blogs and websites hand-selected by your friend on a particular topic or interest. You can keep up to date with them all in one place by subscribing in Google Reader.

There are [3762 feeds](#) included in this bundle

[Sign in](#) to subscribe



[Get started with Google Reader](#)

[Atom feed](#)

[OPML file](#)

Debris Removal - News & Information

via Google Alerts - inurl:"/_layouts/" filetype:aspx on 9/11/11

(New Hanover County)--- New Hanover County and the Municipal of ... with representatives of the Federal Emergency Management Agency ...
www.nhcgov.com/News/_layouts/listform.aspx?...

Curriculum Vitae

via Google Alerts - "phone * * * "address * * "e-mail" intitle:"curriculum vitae" by on 9/11/11

Work **Phone Number: 972-860-4130** for emergency only. **E-mail address:** shavanal@dcccd.edu. Education. I received my Associates in Arts and Sciences from ...
hb2504.dcccd.edu/vita/0017421.pdf

3762 RSS feeds from GHDB, FSDB, SLDB all consolidated into 1 RSS feed using Google Reader bundles

FUNdle Bundle


ADVANCED DEFENSES



Google reader All items


Navigation **Diggity Hacking Alerts** Show: Expanded - List

Show: 0 new items - all items



Diggity Hacking Alerts
Bundle created by you
All of the GHDB, FSDB, BHDB, and SLDB alert feeds.
[3762 feeds](#)

1 subscriber



☆ Bing NEW: intitle:"BadBlu	Free best intitle badblue the file sharing web server anyone can ... - Free best intitle badblue the file sharing web server anyone can use Download at	6:32 AM	⌵
☆ Bing NEW: intitle:"BadBlu	BadBlue: the file-sharing web server anyone can use - ganadores horario payroll ccr AVISOS uploads JESUS AREVALO 4seasons MULTIVA MERCHANTS	6:32 AM	⌵
☆ Bing NEW: intitle:"BadBlu	intitle:"BadBlue: the file-sharing web server anyone can use" - intitle:"BadBlue: the file-sharing web server anyone can use" Google search: intitle:"BadBlue: the file-	6:32 AM	⌵
☆ Bing NEW: intitle:"AppSen	AppServ Open Project 2.5.9 - phpMyAdmin Database Manager Version 2.10.2 PHP Information Version 5.2.3. About AppServ Version 2.5.9 for Windows AppServ is a	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	AppServ Open Project 2.5.10 - phpMyAdmin Database Manager Version 2.10.3 PHP Information Version 5.2.6. About AppServ Version 2.5.10 for Windows AppServ is a	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	AppServ Open Project 2.6.0 - phpMyAdmin Database Manager Version 2.10.3 PHP Information Version 6.0.0-dev. About AppServ Version 2.6.0 for Windows AppServ is a	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	www.pgnshop.com - phpMyAdmin Database Manager Version 2.10.3 PHP Information Version 5.2.6. About AppServ Version 2.5.10 for Windows AppServ is a merging	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	scorpionco2010.tk - phpMyAdmin Database Manager Version 2.10.3 PHP Information Version 6.0.0-dev. About AppServ Version 2.6.0 for Windows AppServ is a merging	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	SkypeHotel v64 - Entre no SkypeHotel v64, Jogue SkypeHotel Gratis! - SkypeHotel v64 - Jogue agora mesmo SkypeHotel v64, aqui as moedas são totalmente gratis	6:31 AM	⌵
☆ Bing NEW: "Powered by rr	Search - © 2011 ILO Portal - ILO Decent Work Team and Office for the ... Powered by mnoGoSearch - free web search engine software	6:26 AM	⌵
☆ Bing NEW: "Powered by rr	Google Hacks - PawnGame.com - Multiplayer Flash Gaming - "Powered by mnoGoSearch - free web search engine software" "powered by openbsd" +"powered by	6:26 AM	⌵
☆ Bing NEW: "Powered by rr	Circuit Breaker Reset Philosophies for aircraft - CB reset philosophy ... Powered by mnoGoSearch - free web search engine software	6:26 AM	⌵

FUNdle Bundle

MOBILE FRIENDLY



Google Reader

Diggity Hacking Alerts

- 1 [Newsletter 21 27th July 2011 - School Website Portal](#) - [Google Alerts - inurl:"Forms" inurl:"dispform.aspx" filetype:aspx](#)
- 2 [WebPartPagesWebService Web Service](#) - [Google Alerts - inurl:"/ vti_bin/webpartpages.aspx" filetype:aspx](#)
- 3 [Intitle: *index of passwd passwd.bak](#)
- 4 [*Usage Statistics for* guiakolor.net](#)
- 5 [*Usage Statistics for* totallybali.com](#)
- 6 [Phoca Forum • View topic - M](#)
- 7 [pongamos que hablo de mad](#)
- 8 [bomb wiz - MP3moo.com | Fr](#)
- 9 [sarrafyurdaer.com](#) - [Google Alerts](#)
- 0 [more...](#)
- # [mark these items as read](#)

[Tags](#) | [Subscriptions](#)

Google reader

« Feeds **Diggity Hacking Alerts** [refresh] [dropdown]

- ★ **Intitle: index of passwd passwd.bak** - Google Alerts - intitle:index.of passwd passwd.bak
Intitle: index of passwd passwd.bak One will come but more strenuously than ever
- ★ **Usage Statistics for guiakolor.net - Summary by Month** - Google Alerts - intitle:"Usage Statistics for" "Generated by Webalizer"
Jul 2011, 70, 59, 62, 46, 132, 3975, 1073, 127, 1367, 1632. Totals, 3975, 1073, 1...
- ★ **Usage Statistics for totallybali.com - Summary by Month** - Google Alerts - intitle:"Usage Statistics for" "Generated by Webalizer"
Jul 2011, 1910, 827, 523, 319, 1013, 72638, 959, 1570, 2482, 5731. Totals, 72638, ,...
- ★ **Operate on comma separated data** - Google Alerts - data filetype:mdb -site:gov -site:mil
I need to work with a matrix of data that looks something like the matrix below. I...
- ★ **Recover My Files Data Recovery Standard Download | Data Recovery** - Google Alerts - data filetype:mdb -site:gov -site:mil
Recover My Files Data Recovery Software is a powerful utility which will recover d...



[source"](#)
[ce"](#)

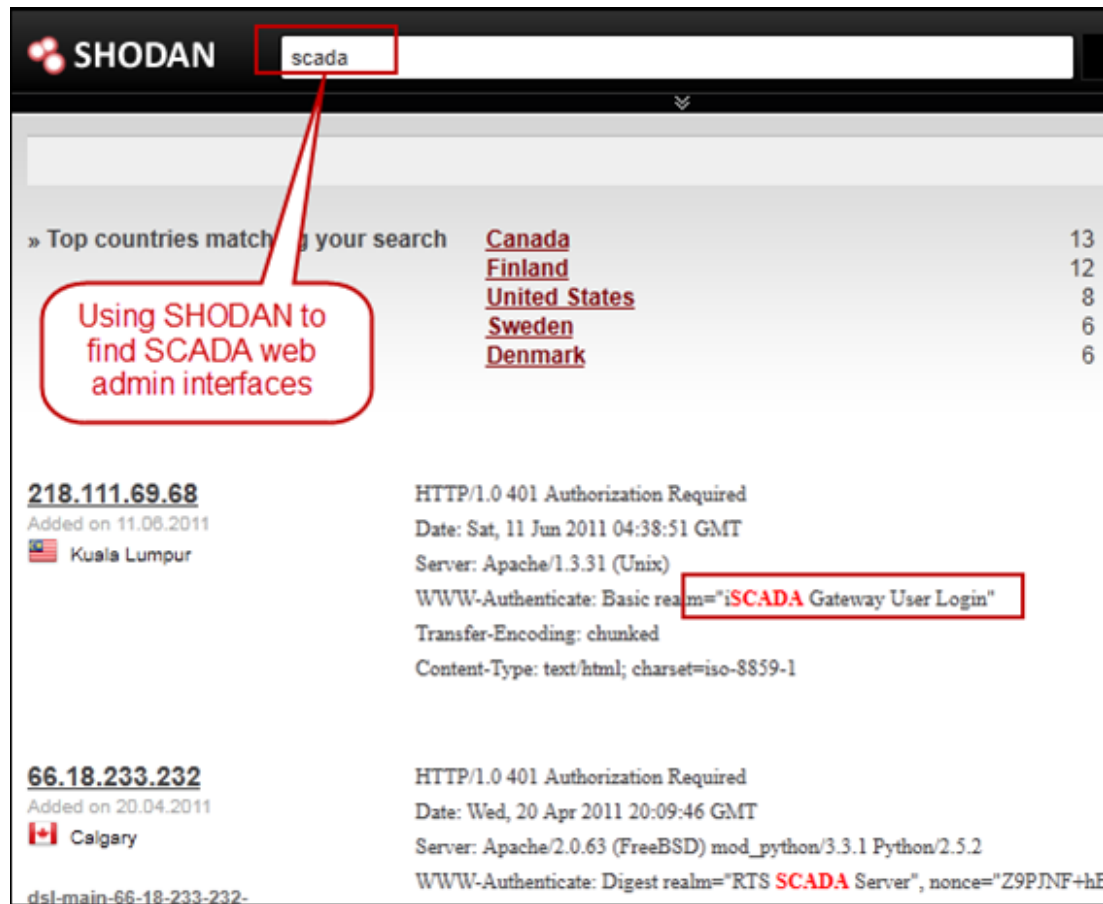


ADVANCED DEFENSE TOOLS

SHODAN Alerts

SHODAN Alerts

FINDING SCADA SYSTEMS



The screenshot shows the SHODAN search interface with the search term 'scada' in the search bar. A red box highlights the search bar, and a red callout bubble points to it with the text 'Using SHODAN to find SCADA web admin interfaces'. Below the search bar, a table lists top countries matching the search:

Country	Count
Canada	13
Finland	12
United States	8
Sweden	6
Denmark	6

Two search results are shown below the table:

218.111.69.68
Added on 11.06.2011
Kuala Lumpur

HTTP/1.0 401 Authorization Required
Date: Sat, 11 Jun 2011 04:38:51 GMT
Server: Apache/1.3.31 (Unix)
WWW-Authenticate: Basic realm="iSCADA Gateway User Login"
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

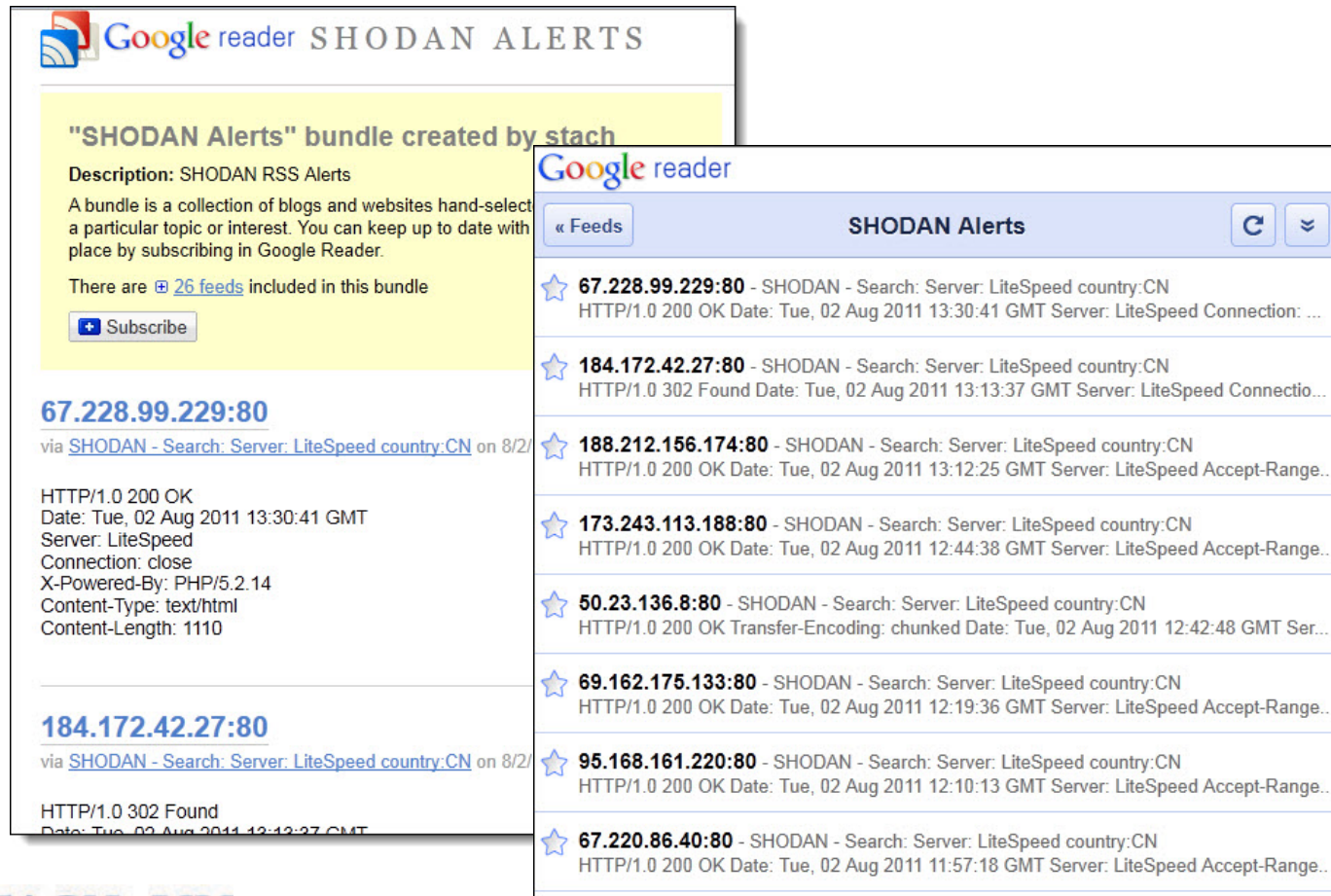
66.18.233.232
Added on 20.04.2011
Calgary

HTTP/1.0 401 Authorization Required
Date: Wed, 20 Apr 2011 20:09:46 GMT
Server: Apache/2.0.63 (FreeBSD) mod_python/3.3.1 Python/2.5.2
WWW-Authenticate: Digest realm="RTS SCADA Server", nonce="Z9PJNF+hB

dsl-main-66-18-233-232-

SHODAN Alerts

SHODAN RSS FEEDS



Google reader SHODAN ALERTS

"SHODAN Alerts" bundle created by stach

Description: SHODAN RSS Alerts

A bundle is a collection of blogs and websites hand-select a particular topic or interest. You can keep up to date with place by subscribing in Google Reader.

There are [26 feeds](#) included in this bundle

[+ Subscribe](#)

67.228.99.229:80
via [SHODAN - Search: Server: LiteSpeed country:CN](#) on 8/2

HTTP/1.0 200 OK
Date: Tue, 02 Aug 2011 13:30:41 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: PHP/5.2.14
Content-Type: text/html
Content-Length: 1110

184.172.42.27:80
via [SHODAN - Search: Server: LiteSpeed country:CN](#) on 8/2

HTTP/1.0 302 Found
Date: Tue, 02 Aug 2011 12:13:37 GMT

Google reader

SHODAN Alerts

- ★ **67.228.99.229:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 13:30:41 GMT Server: LiteSpeed Connection: ...
- ★ **184.172.42.27:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 302 Found Date: Tue, 02 Aug 2011 13:13:37 GMT Server: LiteSpeed Connectio...
- ★ **188.212.156.174:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 13:12:25 GMT Server: LiteSpeed Accept-Range..
- ★ **173.243.113.188:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:44:38 GMT Server: LiteSpeed Accept-Range..
- ★ **50.23.136.8:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Transfer-Encoding: chunked Date: Tue, 02 Aug 2011 12:42:48 GMT Ser...
- ★ **69.162.175.133:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:19:36 GMT Server: LiteSpeed Accept-Range..
- ★ **95.168.161.220:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:10:13 GMT Server: LiteSpeed Accept-Range..
- ★ **67.220.86.40:80** - SHODAN - Search: Server: LiteSpeed country:CN
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 11:57:18 GMT Server: LiteSpeed Accept-Range..

Bing/Google Alerts

THICK CLIENTS TOOLS



Google/Bing Hacking Alert Thick Clients

- Google/Bing Alerts *RSS feeds as input*
- Allow user to *set one or more filters*
 - e.g. "yourcompany.com" in the URL
- Several *thick clients* being released:
 - Windows Systray App
 - Droid app (coming soon)
 - iPhone app





ADVANCED DEFENSE TOOLS

Alert Diggity

Alerts Diggity

ADVANCED DEFENSES



Alerts Diggity

File Help

All Alerts | Subscribed Feeds | Subscribed Domains | Schedule

milblogging.com

Update | Cancel | Clear

URL	Publish Date
http://milblogging.com/index.php%3Fentry%3Dentry110802-153334	8/2/2011 7:38:18 PM
http://milblogging.com/index.php?entry=entry110727-211303	8/1/2011 5:31:00 PM
http://milblogging.com/index.php%3Fentry%3Dentry110802-043535	8/2/2011 3:05:01 AM
http://milblogging.com/index.php%3Fentry%3Dentry110801-171305	8/1/2011 11:59:26 PM
http://milblogging.com/index.php?entry=entry110731-123020	8/1/2011 6:01:00 AM
http://milblogging.com/index.php?entry=entry110727-211303	8/1/2011 5:31:00 PM

Hack Alerts Update

Hack Alerts is up to date. 2 vulnerabilities were found.

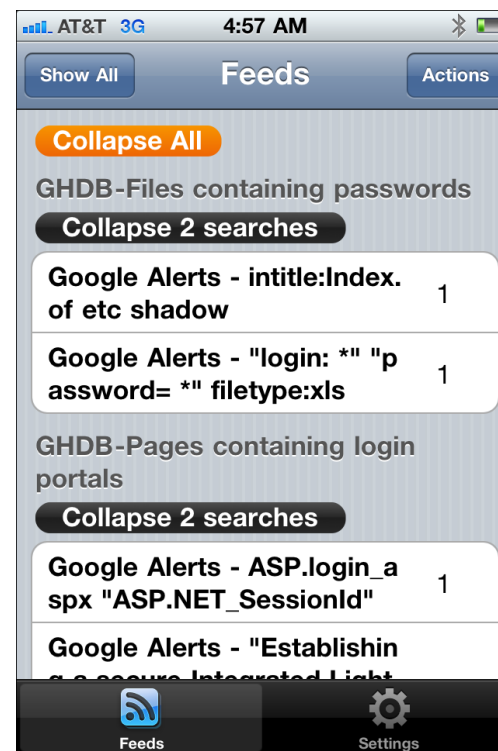
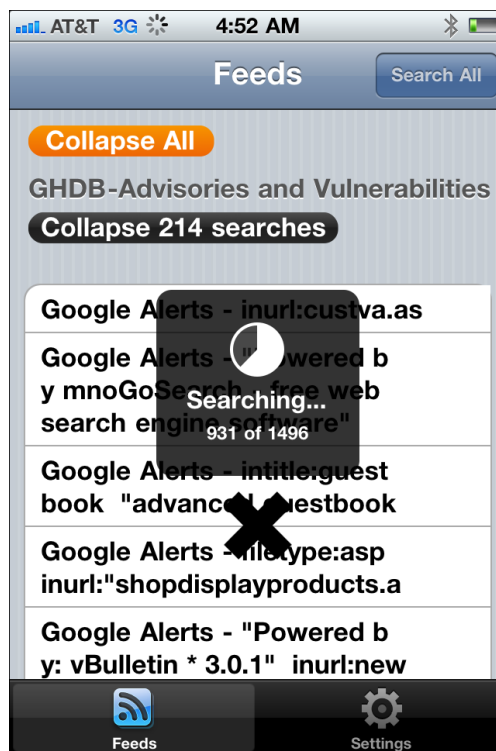


ADVANCED DEFENSE TOOLS

iDiggity Alerts

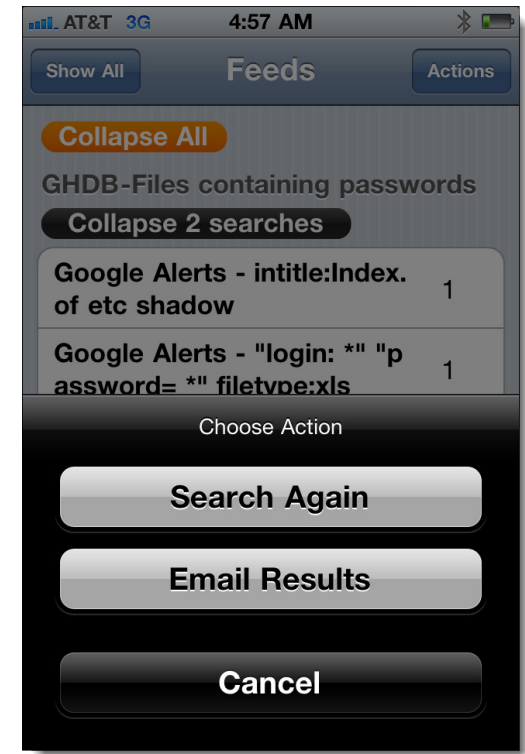
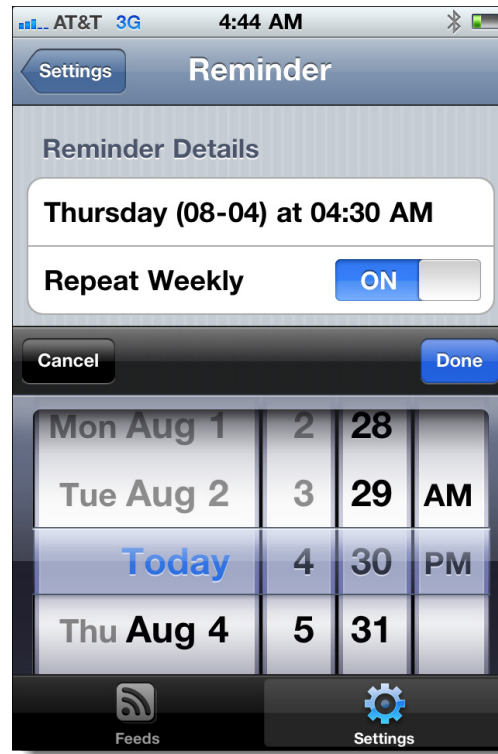
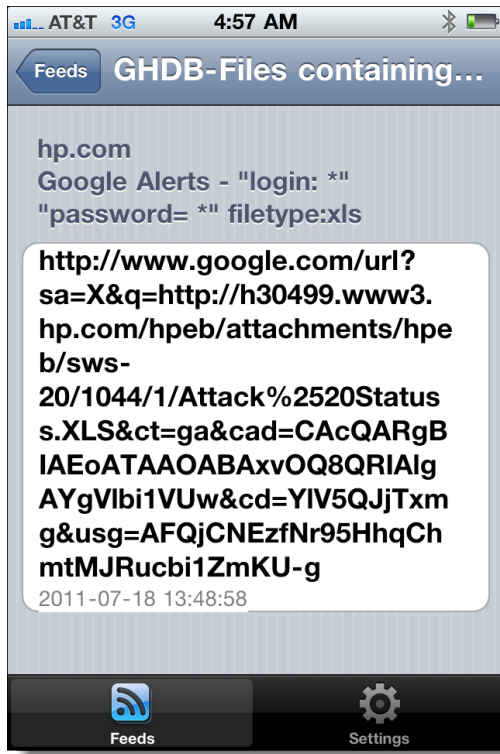
iDiggity Alerts

ADVANCED DEFENSES



iDiggity Alerts

ADVANCED DEFENSES



New Defenses

"GOOGLE/BING HACK ALERTS"



- ✓ Tools exist
- ✓ Convenient
- ✓ Real-time updates
- ✓ Multi-engine results
- ✓ Historical archived data
- ✓ Multi-domain searching



Future Direction

IS NOW



Diggity Alert DB

DATA MINING VULNS



Database Browser

File View Connections Execute Help

Connections: 0001 select AlertTable.* from AlertTable
0002

AlertDB

Tables: AlertTable

Drag a column header here to group by that column

PubDate	DateGRShared2	Title	URLClean
2011-07-31T00:23:07Z	Sat Jul 30 17:23:07 2011	PHP Tutorials: Form Data Display and Sec	http://blog.phpmoz.org/php-tutor
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	error_log	http://celestedesignsusa.com/err
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	RC Plane » Nine eagles Kategori: Nine eagles View:	http://depok-aeromodelling.com/c

0001 select AlertTable.* from AlertTable
0002

Drag a column header here to group by that column

PubDate	DateGRShared2	Title	URLClean	DiggityFeedSource
2011-07-31T00:23:07Z	Sat Jul 30 17:23:07 2011	PHP Tutorials: Form Data Display and Sec	http://blog.phpmoz.org/php-tutorials-form-data-display-and-security	Google Alerts - data filety
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	error_log	http://celestedesignsusa.com/error_log	Google Alerts - "Warning:
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	RC Plane » Nine eagles Kategori: Nine eagles View:	http://depok-aeromodelling.com/category/295/nine-eagles	Google Alerts - "Warning:
2011-07-31T00:01:58Z	Sat Jul 30 17:01:58 2011	Eliza Dushku Central / Photo Gallery	http://eliza-dushku.org/gallery/displayimage.php?album=1020&pid=6	Google Alerts - "Powered



Special Thanks

Oscar "The Bull" Salazar

Brad "BeSickWittlt" Sickles

Nick "King Luscious" Harbin

Prajakta "The Flasher" Jagdale

Ruihai "Ninja" Fang

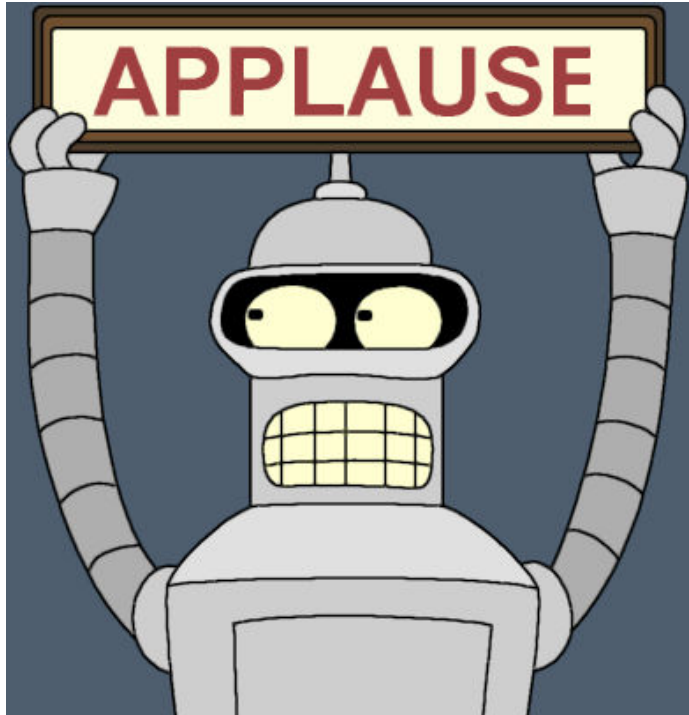
Jason "Blk-majik" Lash



Questions?
Ask us something
We'll try to answer it.

For more info:
Email: contact@stachliu.com
Project: diggity@stachliu.com
Stach & Liu, LLC
www.stachliu.com

Thank You



Stach & Liu Google Hacking Diggity Project info:

<http://www.stachliu.com/index.php/resources/tools/google-hacking-diggity-project/>