



Pulp Google Hacking

The Next Generation Search Engine Hacking Arsenal

15 February 2012 – ISSA Los Angeles – Los Angeles, 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



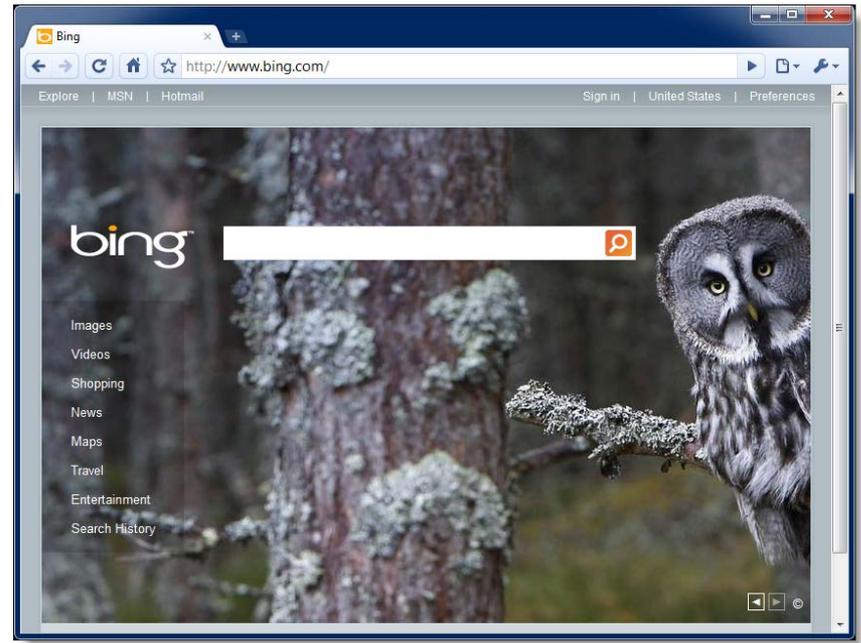
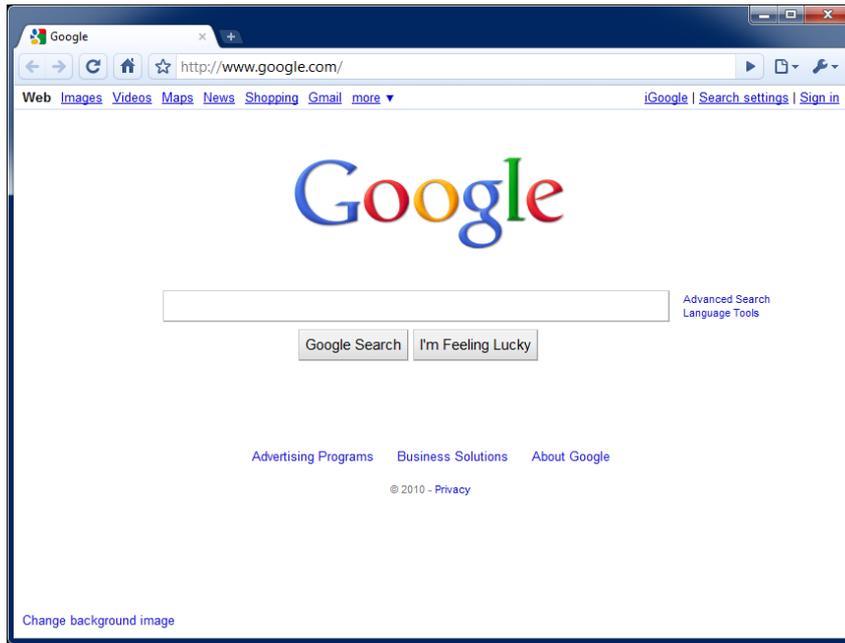
Open Source Intelligence

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

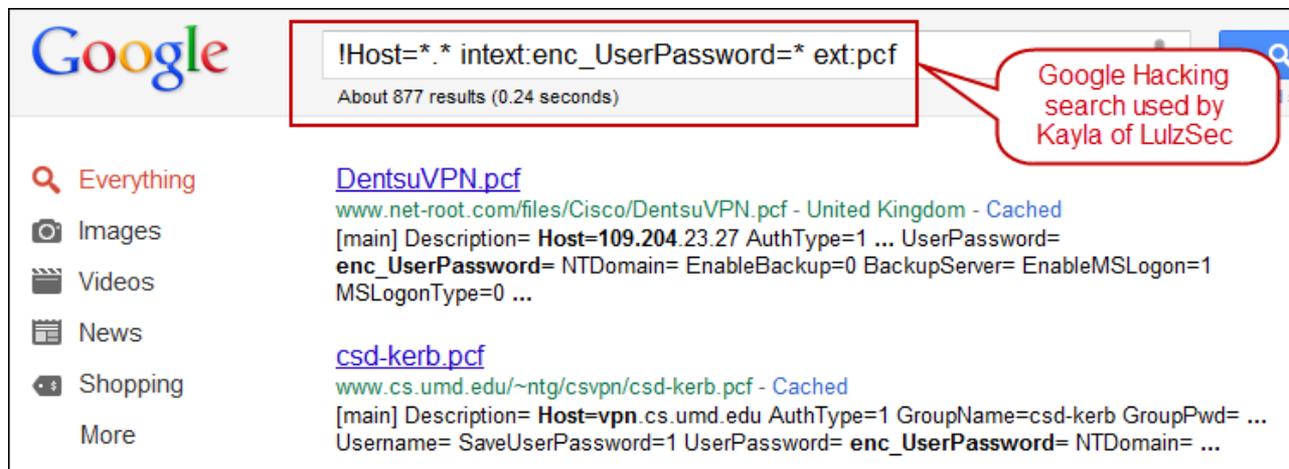
REAL WORLD THREAT

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)". The search results are listed on the right side of the page. The first result is titled "DentsuVPN.pcf" and is from "www.net-root.com/files/Cisco/DentsuVPN.pcf - United Kingdom - Cached". The description for this result is: "[main] Description= Host=109.204.23.27 AuthType=1 ... UserPassword= enc_UserPassword= NTDomain= EnableBackup=0 BackupServer= EnableMSLogon=1 MSLogonType=0 ...". The second result is titled "csd-kerb.pcf" and is from "www.cs.umd.edu/~ntg/csvpn/csd-kerb.pcf - Cached". The description for this result is: "[main] Description= Host=vpn.cs.umd.edu AuthType=1 GroupName=csd-kerb GroupPwd= ... Username= SaveUserPassword=1 UserPassword= enc_UserPassword= NTDomain= ...". On the left side of the page, there are navigation links for "Everything", "Images", "Videos", "News", "Shopping", and "More". A red speech bubble callout 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 29, 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
Jan 15, 2012	Google Code Search shuts down



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

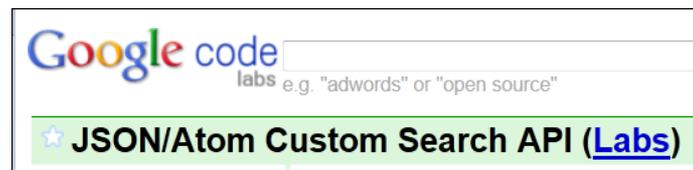


New Features

DIGGITY CORE TOOLS

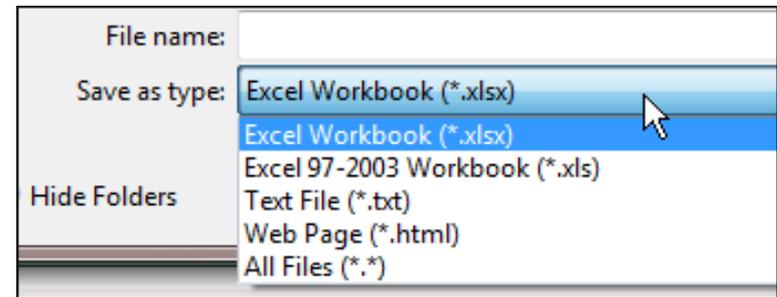
Google Diggity - New API

- 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

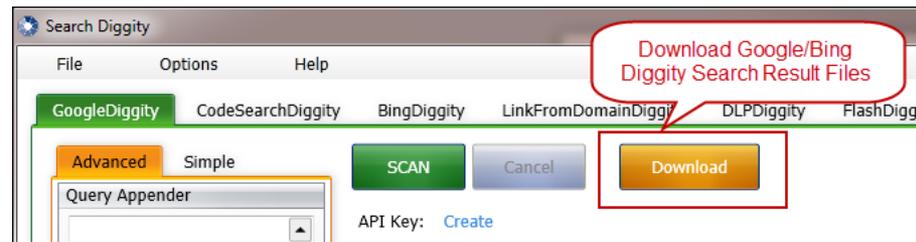


New Features

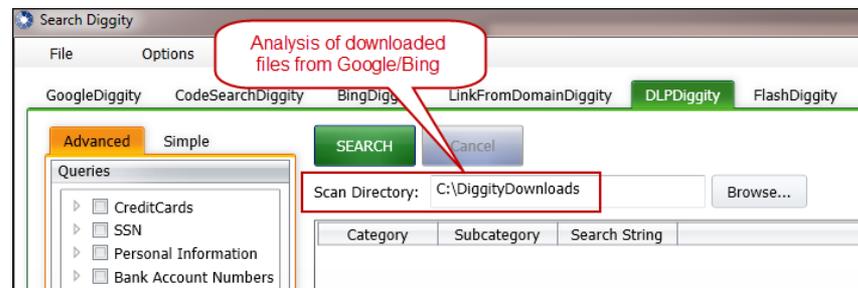
DOWNLOAD BUTTON

Download Buttons for Google/Bing Diggity

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

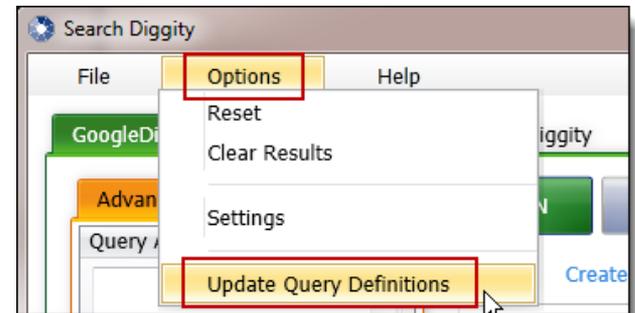


- Used by other tools for file download/analysis:
 - FlashDiggity, DLP Diggity, MalwareDiggity,...



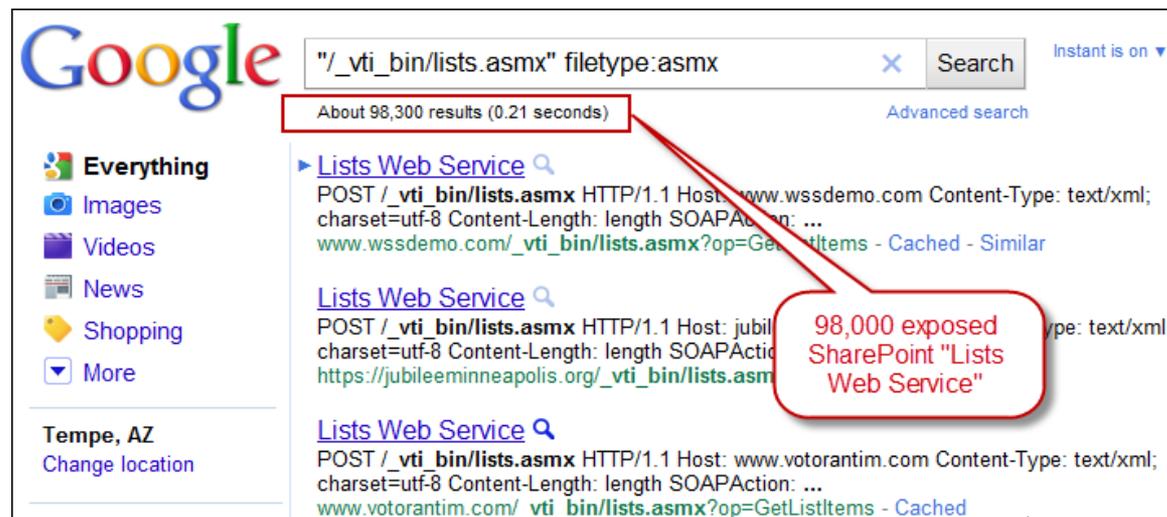
New Features

AUTO-UPDATES



SLDB Updates in Progress

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



New Features

IP ADDRESS RANGES

GoogleDiggity can now search for IP Address Ranges

The screenshot shows a Google search interface. The search bar contains the query `site:216.75.*.*`. A callout box points to this query with the text: "GoogleDiggity automatically converts IP address ranges of different formats to site:10.1.*.* notation".

The search results include a link for "Dallas Personal Injury Lawyer" with the IP address `216.75.26.194/` highlighted. Another result shows `216.75.7.67/topdia.php`.

An overlay window titled "sites/Domains/IP Ranges" is shown, containing a list of IP ranges: `216.75.0.0/16` and `216.75.26.1-216.75.26.255`, each with a "[Remove]" link. Below the list are "Import" and "Clear" buttons. A callout box points to this window with the text: "GoogleDiggity now can search IP address ranges".

Dictionary Updates

THIRD-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 displays the Google Diggity application window. The interface includes a menu bar (File, Options, Help), a tabbed interface with 'GoogleDiggity' selected, and a main workspace. On the left, there are sections for 'Query Appender' and a tree view of 'Queries' with 'GHDB' expanded. The central area features a 'SCAN' button, 'API Key' and 'Google Custom Search ID' fields, and a 'Sites/Domains' list containing 'stachliu.com'. Below this is a table of search results.

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/

The 'Output' section shows a log of the scan process:

```
Using API Key: ALZAsyDIIUASIVNLC-aw_1IuzFNU7tDUC-9qKI EORDM.  
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]
```

At the bottom, the status bar indicates 'Google Status: Ready' and 'Download Progress: Idle Open Folder'.

Bing Diggity

DIGGITY CORE TOOLS

The screenshot shows the Bing Diggity application window. The 'BingDiggity' tab is selected. 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. The main area displays a table of search results. A red box highlights the search string 'ip:98.129.200.37' in the second row. A red callout bubble points to the IP address in the search input 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 &	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"`

Web Images Videos Shopping News Maps More | MSN Hotmail

bing

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

Web More ▾

RELATED SEARCHES

- VMware Server User Guide
- Terminal Server User Mode
- Windows Home Server User Guide
- Denver SQL Server User Group
- Terminal Server User Profiles
- Users Server 2003
- Terminal Server Users
- Create SQL Server User

ALL RESULTS 1-10 of 23 results

Related Searches for intitle:"Snap Server" in "Home" "Active Users"

- VMware Server User Guide Terminal Server User Mode
- Windows Home Server User Guide Denver
- Snap Server CORESERVER [Home]**
CORESERVER • Home ... Active Users • Change Password • Administration
coreserver.biochem.okstate.edu
- Snap Server SPAMSNAP80 [Home]**
SPAMSNAP80 • Home ... Active Users • Change Password • Administration
129.137.005.250
- Snap Server GSTI [Home]**
GSTI • Home ... Active Users • Change Password • Administration
gsti.miis.edu
- Snap Server SNAP205861 [Home]**
SNAP205861 • Home SHARE1: Active Users • Change Password • Administration
server1.music.olemiss.edu

SEARCH HISTORY

- intitle:"Netscape
- FastTrack Server...
- linkfromdomain

bing



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 includes the Google Code Search logo, a search bar with the query, and a "Search" button. The results show a code snippet from a file named `post.asp`. The code snippet is as follows:

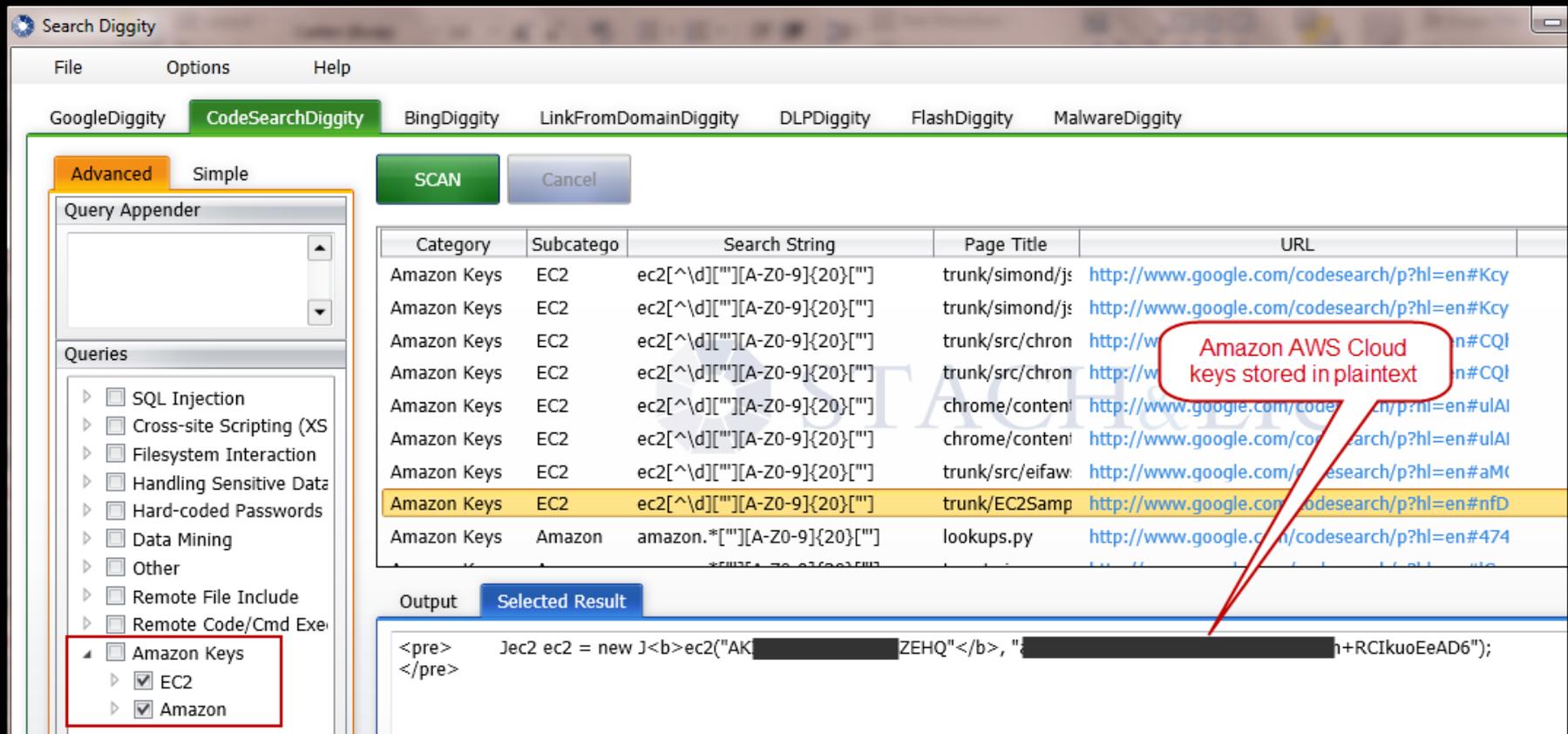
```
45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ÄÏÄÖÄ×÷Öß°Í¹ÙÀìÔ±²ÄÄÜ±à¼Öâ,øìû×ó."

57: strSql = "SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ÄÏÄÖÄ×÷Öß°Í¹ÙÀìÔ±²ÄÄÜ±à¼Öâ,øìû×ó."
```

A red speech bubble points to the `reply_id` parameter in the SQL query, 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



The screenshot shows the CodeSearch Diggity application window. The 'CodeSearchDiggity' tab is active. On the left, the 'Queries' list has 'Amazon Keys', 'EC2', and 'Amazon' checked. The main table displays search results with columns for Category, Subcategory, Search String, Page Title, and URL. A red callout box points to a result for 'Amazon Keys' in the 'EC2' category, with the text 'Amazon AWS Cloud keys stored in plaintext'. Below the table, the 'Selected Result' output shows a code snippet:

```

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



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.



linkFromDomainDiggity

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 (partially obscured), and a 'Domain' field containing 'stachliu.com'. Below the input fields 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 the 'URLs' tab with the text: 'Bing's linkfromdomain: directive used to find external links on your sites'. Another red callout box points to the list of links with the text: 'External links then sorted and extracted into: applications, host names, and domains'. The 'Output' section at the bottom shows the search results: 'Maximum 20...', '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 'linkfromdomaindiggity' logo is visible in the bottom right of the application window. The status bar at the bottom indicates 'Google Status: Ready' and 'Bing Status: Ready'.

Bing LinkFromDomain

FOOTPRINTING LARGE ORGANIZATIONS

The screenshot displays the LinkFromDomainDiggity tool interface. At the top, there are several tabs: GoogleDiggity, CodeSearchDiggity, BingDiggity, LinkFromDomainDiggity (highlighted), DLPDiggity, FlashDiggity, and MalwareDiggity. The main interface is divided into several sections:

- Query Appender:** Contains the search query `site:gov.cn`. A callout box points to this query with the text: "2. Also filtering results to just those also part of the gov.cn domain".
- Sites/Domains:** Contains a list of domains to scan, with `www.gov.cn` selected. A callout box points to this domain with the text: "1. Running Bing's linkfromdomain:www.gov.cn to get list of off-site links from China's government main website".
- Hosts:** A list of hostnames found in the results, including `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`. A callout box points to this list with the text: "3. Results in large list of other valid Chinese government hostnames on the gov.cn domain".
- Output:** Shows the scan 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]".

The tool's logo, "linkfromdomaindiggity", is visible in the bottom right corner of the interface.



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.jhtml?articleID=225600247>

"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.

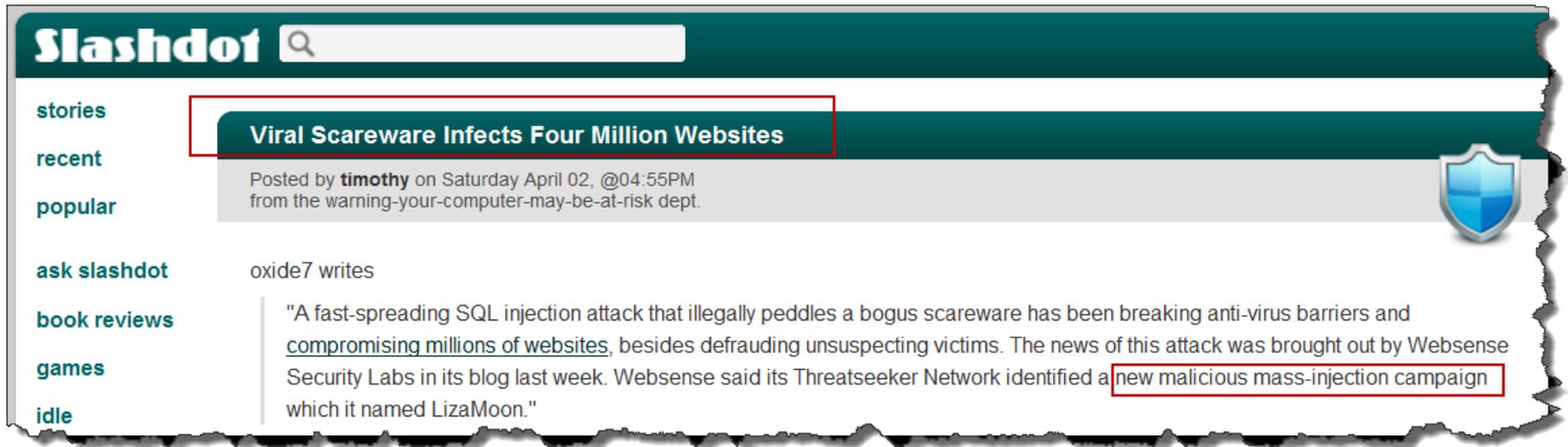
Estimates of the total number of compromised Web sites vary between 7,000 and 114,000, according to security experts. Other compromised sites include servicewomen.org and intijobs.org.

Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – LizaMoon – April 2011

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



The image shows a screenshot of a Slashdot article. The page has a dark green header with the 'Slashdot' logo and a search bar. On the left side, there is a navigation menu with links for 'stories', 'recent', 'popular', 'ask slashdot', 'book reviews', 'games', and 'idle'. The main content area features a headline 'Viral Scareware Infects Four Million Websites' in a dark green box. Below the headline, it says 'Posted by **timothy** on Saturday April 02, @04:55PM from the warning-your-computer-may-be-at-risk dept.' To the right of the text is a blue shield icon. The article body starts with 'oxide7 writes' followed by a paragraph: '"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."' The phrase 'new malicious mass-injection campaign' is highlighted with a red box.

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-managers,

When researchers from [Security](#) search results suggested that the search results showed that

Armorize Malware Blog



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

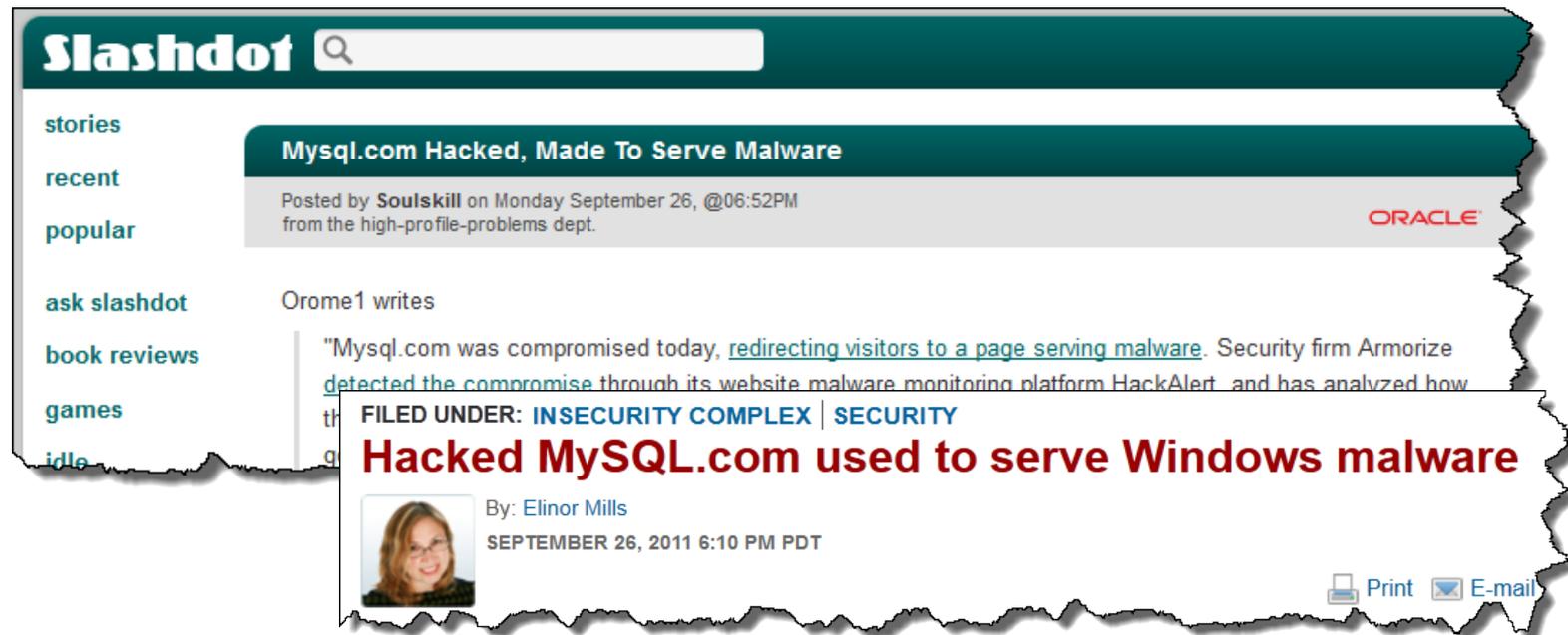
POSTED BY: CHRIS ON 7.25.2011 / CATEGORIES: [DRIVE-BY DOWNLOAD](#), [HACKALERT](#), [MASS INJECTION](#), [OSCOMMERCE](#), [WEB MALWARE](#)

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 top navigation bar is dark green with the 'Slashdot' logo and a search box. On the left, there are menu items: 'stories', 'recent', 'popular', 'ask slashdot', 'book reviews', 'games', and 'idle'. The main article header is 'Mysql.com Hacked, Made To Serve Malware', posted by 'Soulskill' on Monday, September 26, 2011 at 06:52 PM. The article text begins with 'Orome1 writes' and mentions that 'Mysql.com was compromised today, redirecting visitors to a page serving malware'. A red banner across the article reads 'FILED UNDER: INSECURITY COMPLEX | SECURITY' and 'Hacked MySQL.com used to serve Windows malware'. The author of this section is 'Elinor Mills', dated 'SEPTEMBER 26, 2011 6:10 PM PDT'. At the bottom right, there are 'Print' and 'E-mail' icons.

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

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

Import Clear

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

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

The image shows a composite of two web browser screenshots. The top screenshot is a Google search for "www.michoo.co.kr" on the interpark.com site. The search results show a link to a page on interpark.com with a URL containing "www.michoo.co.kr". A red callout bubble points to this link with the text: "interpark.com does appear to have links to www.michoo.co.kr".

The bottom screenshot shows a list titled "The 1000 most-visited sites on the web". The list includes the following data:

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

A red callout bubble points to the interpark.com entry in the list with the text: "So, the 907th most popular site on the web has URL links to suspected malware sites".

Other callouts in the image include: "Links to michoo.co.kr" pointing to a link in the bottom screenshot, and "www.michoo.co.kr ..." pointing to a link in the top screenshot.

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 \(ERX\)](http://AS3786).

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)

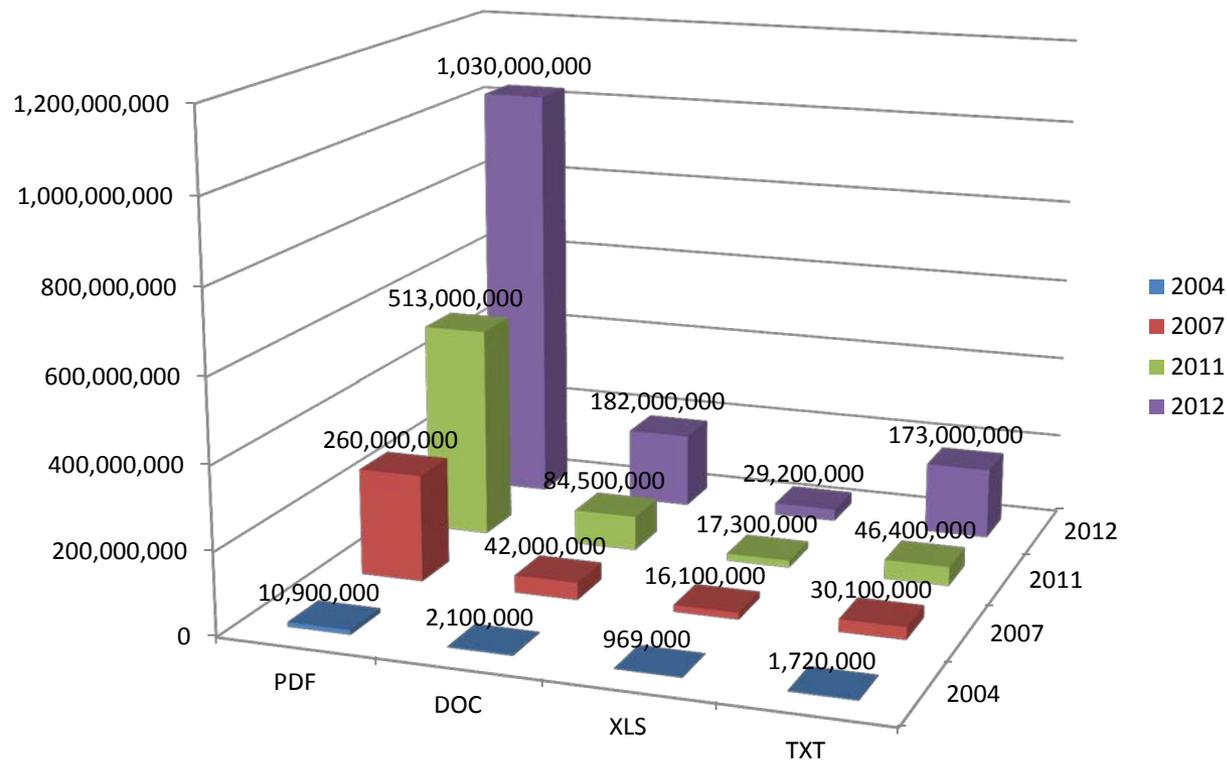
bing
Web
filetype:doc
Web More
SEARCH HISTORY ALL RESULTS 1-10 of 26,900,000 results · Advanced

bing
Web
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

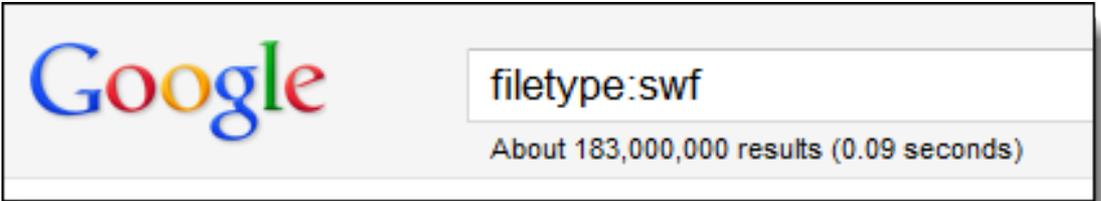
DIGGITY TOOLKIT

The screenshot displays the DLP Diggity application interface. At the top, there are tabs for various search engines: GoogleDiggity, CodeSearchDiggity, BingDiggity, LinkFromDomainDiggity, **DLPDiggity** (highlighted with a red box), FlashDiggity, and MalwareDiggity. Below the tabs, there are two modes: "Advanced" and "Simple". A "SEARCH" button is visible. The "Scan Directory" field is set to "C:\DiggityDownloads\" and is highlighted with a red box. A "Browse..." button is next to it. The main area shows a table of search results:

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

A red callout box points to the search results with the text: "Search through downloaded files from GoogleDiggity and BingDiggity for data leaks such as SSNs, credit cards, etc." Below the table, there is an "Output" section with a "Selected Result" tab. The output shows a snippet of text from a document:

```
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
```



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

The screenshot shows the FlashDiggity application interface. The 'FlashDiggity' tab is active. The 'Queries' list on the left includes 'Keywords' and 'User Account Info'. The 'Scan Directory' is set to 'C:\DiggityDownloads'. The search results table is as follows:

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]

The 'Output' section shows the 'Selected Result' for the highlighted row:

```
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);
```

A red callout box points to the code snippet with the text: "Hardcoded usernames and passwords in cleartext in SWF file".

NEW GOOGLE HACKING TOOLS

DEMO

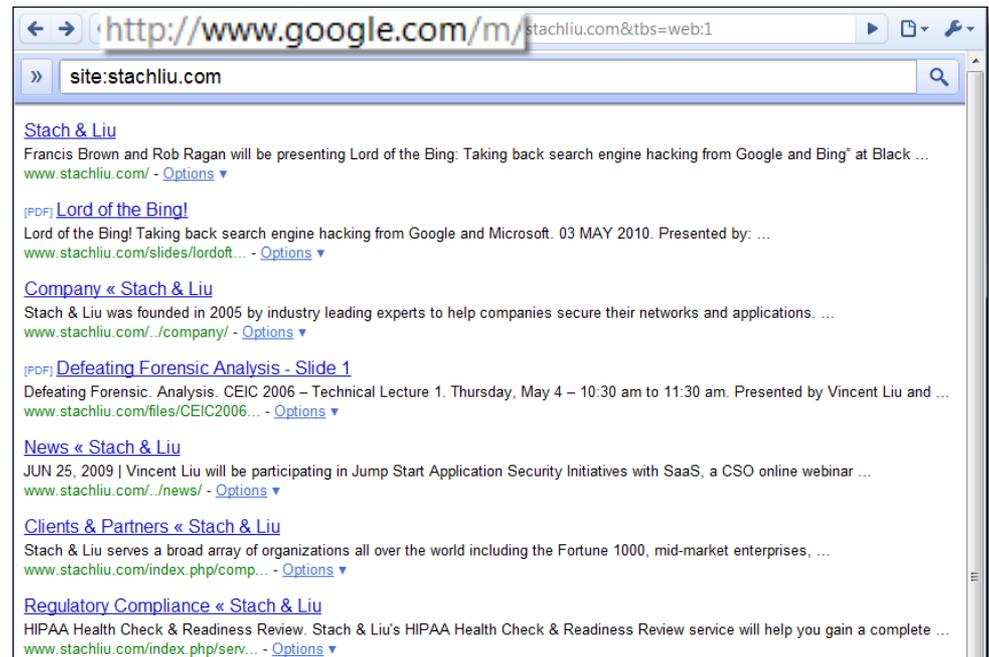
GoogleScrape Diggity

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



NON-DIGGITY ATTACK TOOLS

Other Search Hacking Tools

Maltego

INFORMATION GATHER TOOL

The screenshot displays the Maltego Client 3.0 BETA interface. The main window shows a network diagram with a central node 'guillaume.prigent@diateam.net' highlighted in light blue. This node is connected to several other nodes, including 'jean-baptiste.rouault@diateam.net', 'florian.vichot@diateam.net', 'frederic.paul@diateam.net', 'webmaster@diateam.net', 'actes.sstic.org', 'blog.hynesim.org', 'www.bridnet.fr', 'www.ossir.org', '2009.hack.lu', 'www.hynesim.fr', 'diateam.net', 'diateam.fr', and 'diateam.com'. A red arrow points from the central node to 'diateam.net'. The interface includes a top toolbar with 'Investigate' and 'Manage' tabs, a 'Palette' on the left with categories like 'Infrastructure' and 'Personal', and a 'Detail View' on the right showing information for 'actes.sstic.org'. The bottom status bar contains search and filter options.

theHarvester

FOOTPRINTING TOOL

- Gathers e-mail accounts, user names and hostnames, and subdomains

```
C:\theHarvester-ng-blackhat>python theHarvester.py

*****
*TheHarvester Ver. 2.1 (reborn) *
*Coded by Christian Martorella *
*Edge-Security Research *
*cmartorella@edge-security.com *
*****

Usage: theharvester options

-d: Domain to search or company name
-b: Data source (google,bing,bingapi,pgp,linkedin,google-profiles)
-s: Start in result number X (default 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS bruteforce for the domain name
-t: Perform a DNS TTL bruteforce
-e: Use this DNS server
-l: Limit the number of results (default is 100, goes from 50 to 1000)
-h: use SHODAN data source (default is google, goes from 100 to 1000, see option)

Examples: ./theharvester.py -d microsoft.com -l 500 -b google
          ./theharvester.py -d microsoft.com -b pgp
          ./theharvester.py -d microsoft -l 200 -b linkedin
```

theHarvester

theHarvester gathers: emails, subdomains, hosts, employee names, open ports and banners.

Searches different public sources, such as: Google, Bing, LinkedIn, PGP key servers and SHODAN

theHarvester

FOOTPRINTING EXAMPLE

```
C:\theHarvester>python theharvester.py -d microsoft.com -l 200 -b google -f microsoft.output.html
```

```
*****
*TheHarvester Ver. 2.1 (reborn) *
*Coded by Christian Martorella *
*Edge-Security Research *
*cmartorella@edge-security.com *
*****
```

```
[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
```

```
[+] Emails found:
-----
mikemr@microsoft.com
cnfrmpro@microsoft.com
wvblog@microsoft.com
nntp@microsoft.com
domains@microsoft.com
MVADean@e-mail.microsoft.com
```

```
[+] Hosts found in search engines:
-----
207.46.19.254:www.microsoft.com
207.46.225.250:support.microsoft.com
65.55.27.219:windowsupdate.microsoft.com
...
65.55.11.238:schemas.microsoft.com
65.52.103.84:connect.microsoft.com
```

```
[+] Proposed SET
-----
[]
Saving file
```

theHarvester-ng-blackhat/microsoft.output.html

theHarvester results for :microsoft.com

Dashboard:

14%	86%	0%	0%	0%
6	38	0	0	0
Emails	hosts	Vhost	TLD	Shodan

E-mails names found:

- mikemr@microsoft.com
- cnfrmpro@microsoft.com
- wvblog@microsoft.com
- nntp@microsoft.com
- domains@microsoft.com
- MVADean@e-mail.microsoft.com

Hosts found:

- 207.46.19.254:www.microsoft.com
- 207.46.225.250:support.microsoft.com

SHODAN



HACKER SEARCH ENGINE

- Indexed service banners for whole Internet for HTTP (Port 80), as well as some FTP (23), SSH (22) and Telnet (21) services

The screenshot shows the SHODAN search interface. The search bar contains the query `"Server:NAShttpd"`. Below the search bar, there is a section titled "» Top countries matching your search" with a list of countries and their counts:

Country	Count
Italy	20
China	14
United States	7
Spain	6
Greece	5

Below this list, there is a search result for the IP address **123.116.195.215**. The result includes the following information:

- Added on 06.02.2012
- Beijing
- HTTP/1.0 401 Unauthorized
- Server: NAShttpd
- Date: Mon, 06 Feb 2012 18:01:34 GMT
- WWW-Authenticate: Basic realm="Default USER:admin"
- Content-Type: text/html
- Connection: close

Red callout boxes highlight specific details: "NAS storage devices located" points to the IP address; "Default username is 'admin'" points to the WWW-Authenticate header value; and another box points to the search query.

PasteBin Leaks

PASSWORDS IN PASTEBIN.COM POSTS

- Twitter feed tracking passwords leaked via PasteBin

The image shows a Twitter feed on the left and a PasteBin post on the right. The Twitter feed features the profile of @PastebinLeaks, which is described as 'Glued to the leak' and focuses on 'Discovering leaks on Pastebin, web attacks and so on'. Two tweets are visible, both mentioning 'Possible Massive mail/pass leak' and providing links to PasteBin posts. A red callout bubble points to the tweets with the text: 'Twitter feed tracking public data leaks via PasteBin.com'. The PasteBin post on the right is titled 'http://biclopsgames.com (hacked)' and shows a list of user data from a MySQL database. A red callout bubble points to the data table with the text: 'Usernames, emails, and password hashes of compromised website posted to PasteBin.com'. The data table includes columns for 'username', 'user_password', and 'user_email'.

PasteBin Post Content:

```
1.
2. Target: http://biclopsgames.com/game.php?id=%Inject_Here%1
3. Date: 12/15/2011 11:17:28 PM
4. DB Detection: MySQL error based (
5. Method: GET
6. Type: Integer (Auto Detected)
7. Data Base: biclops_phpbb1
8. Table: phpbb_users
9. Total Rows: 341
10.
11. username user_password user_email
12. $voloch b35d1ac9729539d9f8ef87508e8b2be0 kirillwow79@mail.ru
13. &#28023;&#30423; 5e0ed8d03d765e4fb5128b6ba7bc8481
14. AaronFF cee3d5a7af23179acea3550fc6301300 EmbeveIcomo@mail.bij.
15. abadrabPype 1e3c47bf39af11993cfdc689693b7012 jeinso.n.wels
16. absurdism 297dbe7699dcfa60609bf9e667e2e4dc evolancia@gmail
17. Accichfueve adefb16336d900168c9bfc40af5b18ef lokorepaserna
```

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



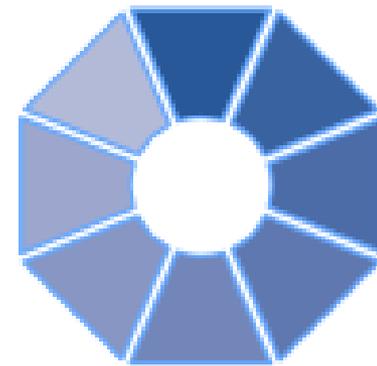


Advanced Defenses

NEW HOT SIZZLE

Stach & Liu now proudly presents:

- **Google and Bing Hacking Alerts**
 - SharePoint Hacking Alerts – 118 dorks
 - SHODAN Hacking Alerts – 26 dorks
- **Diggity Alerts FUNdle Bundles**
 - Consolidated alerts into 1 RSS feed
- **Alert Client Tools**
 - 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 regexes 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 - "mysql... (11)**
- Google Alerts - "A sv... (10)
- Google Alerts - "mysql error 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/FSDB 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

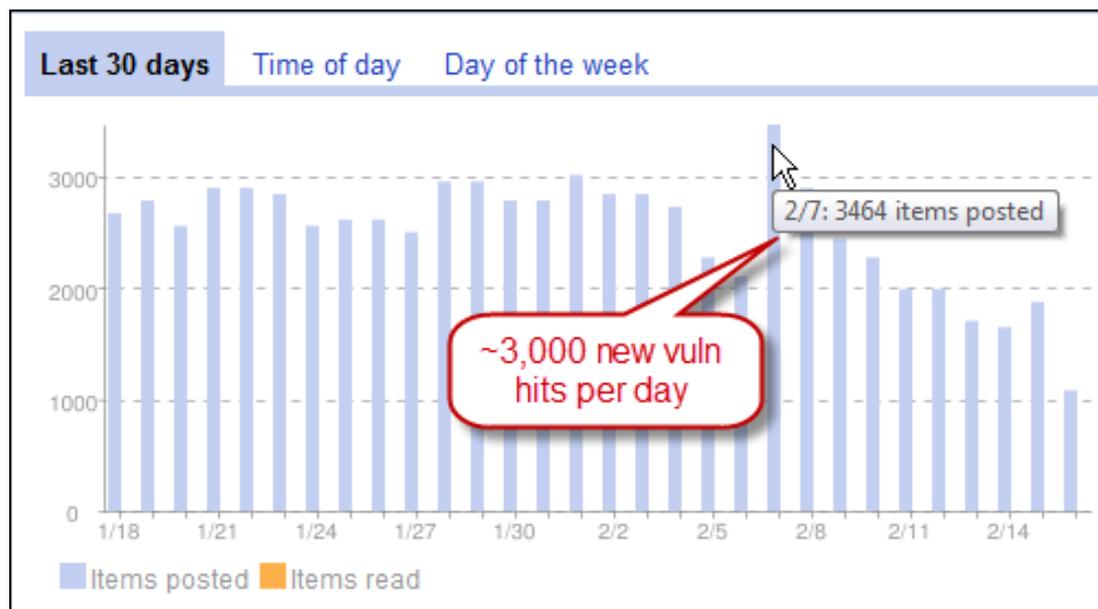
The screenshot shows a Google Reader interface with a list of RSS subscriptions on the left and a feed of items on the right. The top item in the feed is titled "Bing: intitle:'Snap Server' intitle:'Home' 'Active Users' >>". Below this, several items are listed, including "Snap Server WELW-SNAP [Home]", "Snap Server CORESERVER [Home]", "Snap Server GSTI [Home]", "adsphotographer.com - SNAP55373", "Snap Server SNAP824929 [Home]", "Snap Server SAINTSNAP [Home]", "Snap Server DIGITALDATA1 [Home]", and "Snap Server FTP-SERVER [Home]". A red callout box points to the "Snap Server FTP-SERVER [Home]" item with the text "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 Municipal of ... with representatives of the Federal Emergency Management Agency ... www.nhcgov.com/News/_layouts/listform.aspx?...

Curriculum Vitae

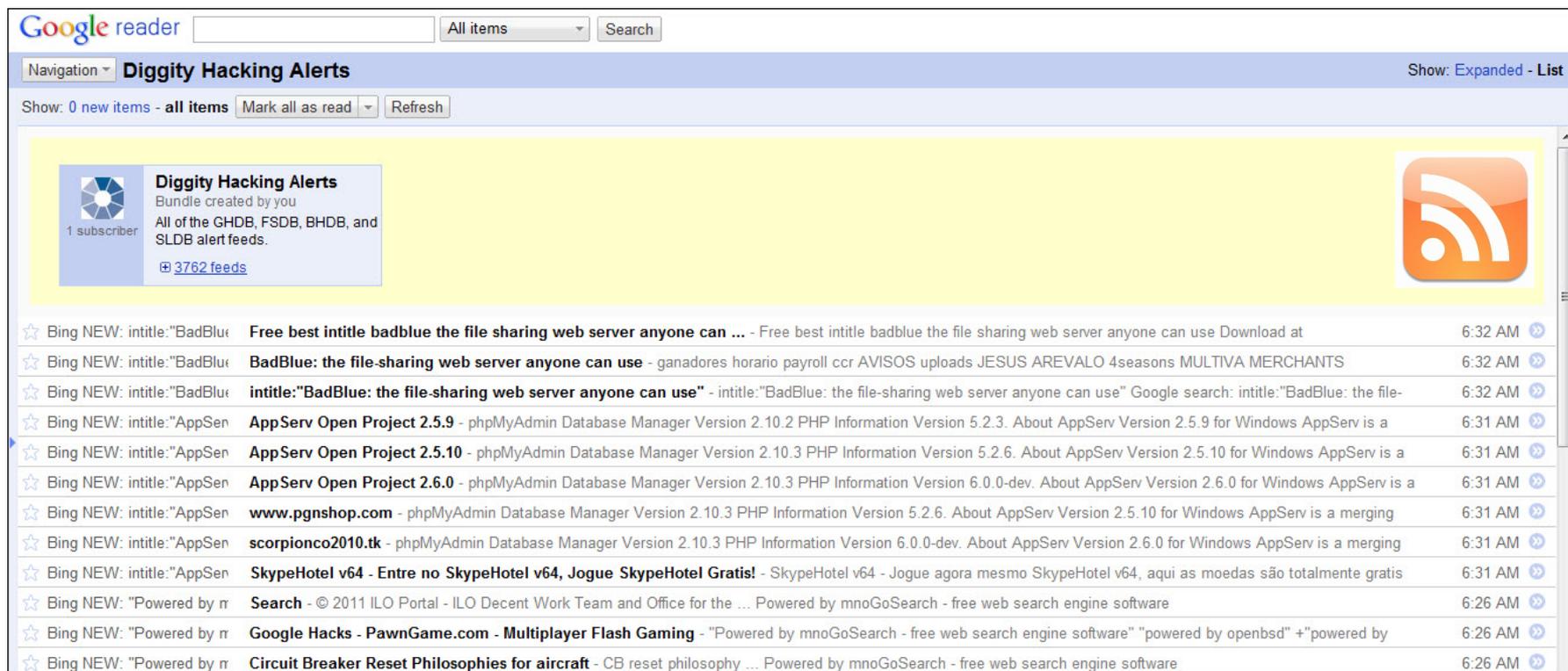
via Google Alerts - "phone * * * "address * * "e-mail" intitle:"curriculum vitae" by on 9/11/11

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



The screenshot shows a Google Reader interface. At the top, there's a search bar and a dropdown menu set to 'All items'. Below that, the feed title 'Diggity Hacking Alerts' is displayed, along with a 'Show: Expanded - List' option. The feed content includes a summary card for the bundle, which states it was created by the user, has 1 subscriber, and contains 3762 feeds. The main list of items includes several Bing News alerts about 'BadBlue' (a file-sharing web server) and 'AppServ Open Project' updates (versions 2.5.9, 2.5.10, and 2.6.0). Other items mention 'www.pgnshop.com', 'scorpionco2010.tk', and 'SkypeHotel v64'. The interface also features a navigation menu, a 'Mark all as read' button, and a 'Refresh' button.

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:asmx](#)
- 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



- ★ [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, 1127, 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, there is a table of top countries matching the search:

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

Below the table, two search results are shown. The first result is for IP address **218.111.69.68**, located in Kuala Lumpur, Malaysia. It was added on 11.06.2011. The HTTP headers for this result are:

- 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

The second result is for IP address **66.18.233.232**, located in Calgary, Canada. It was added on 20.04.2011. The HTTP headers for this result are:

- 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"

The URL for the second result is `dsl-main-66-18-233-232-`.

SHODAN Alerts



SHODAN RSS FEEDS

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 8/2/11

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 8/2/11

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

SHODAN Alerts

« Feeds 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

The image shows two overlapping windows of the Alerts Diggity application. The background window is in the 'Subscribed Feeds' tab and shows a search bar with 'milblogging.com' entered. The foreground window is also in the 'Subscribed Feeds' tab and displays a table of feeds with columns for 'URL' and 'Publish Date'. Below the table are 'Update', 'Cancel', and 'Clear' buttons. A green notification box in the bottom right corner reads: 'Hack Alerts Update' followed by 'Hack Alerts is up to date. 2 vulnerabilities were found.'

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

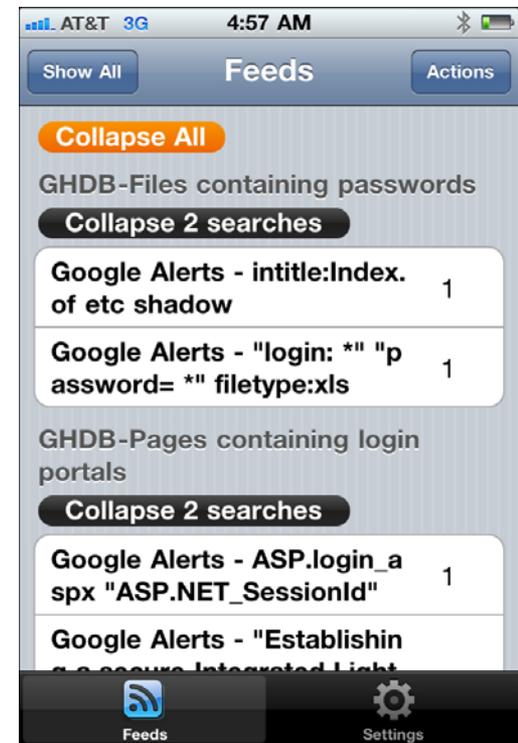
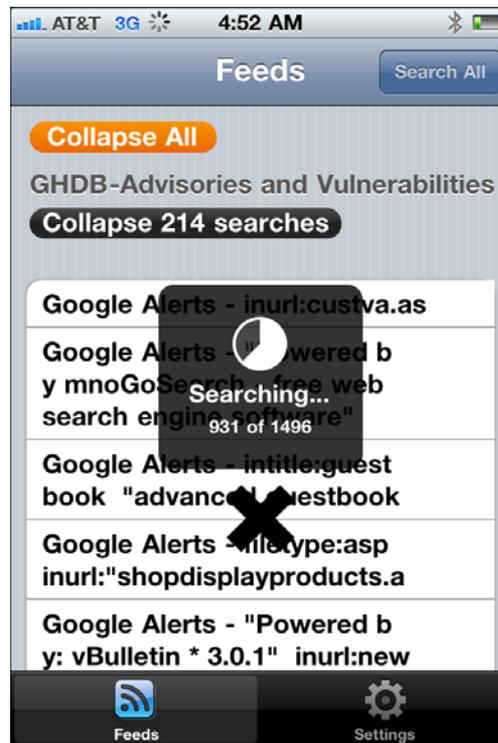


ADVANCED DEFENSE TOOLS

iDiggity Alerts

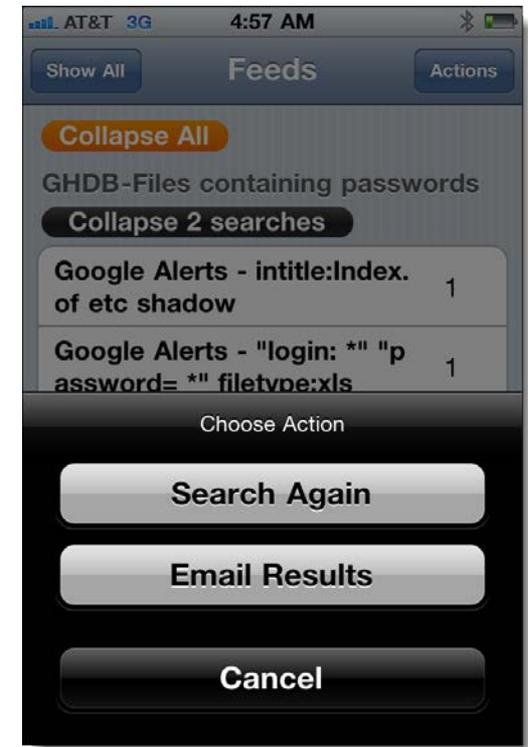
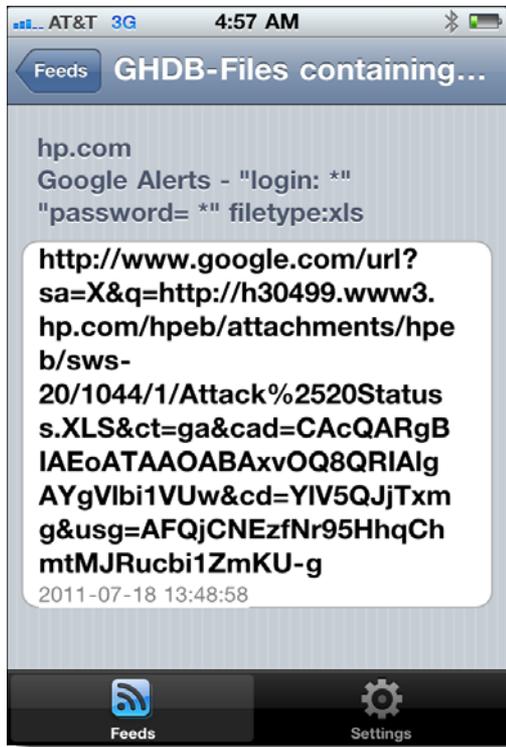
iDiggity Alerts

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 - "Warning: 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



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/>