



# Pulp Google Hacking

The Next Generation Search Engine Hacking Arsenal

02 April 2012 – InfoSec World 2012 – Orlando, FL



Presented by:

Francis Brown & Rob Ragan

Stach & Liu, LLC

[www.stachliu.com](http://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

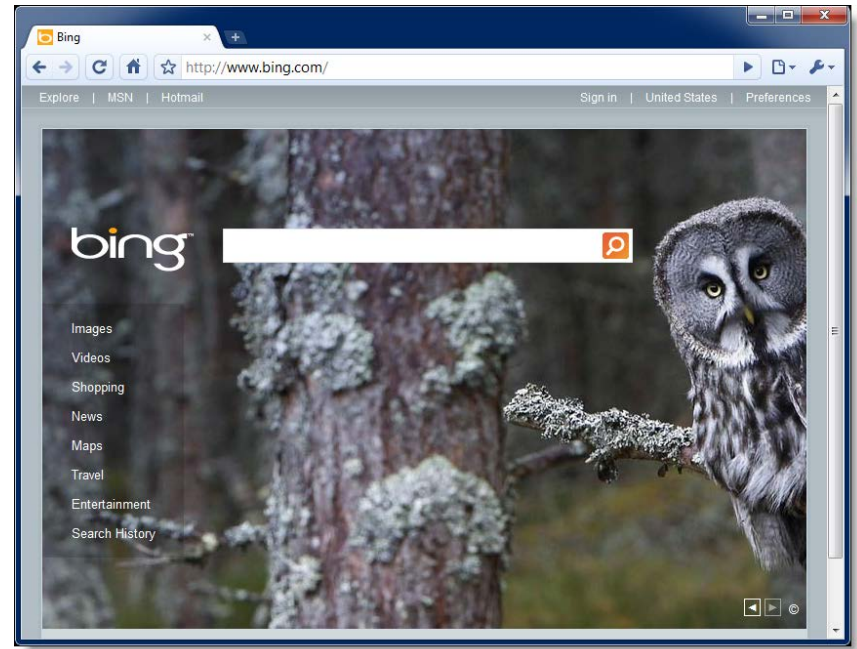
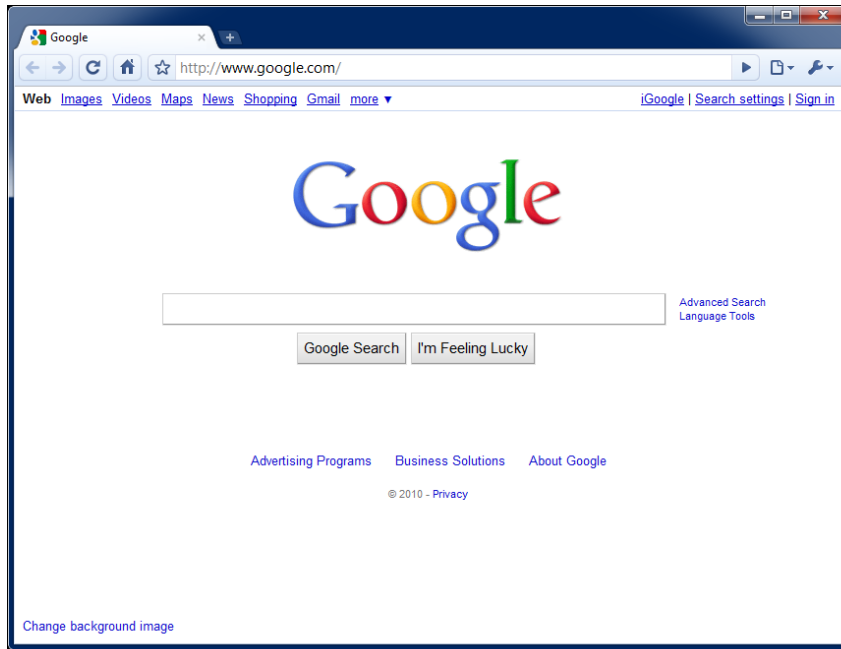
SEARCHING PUBLIC SOURCES

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



# 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

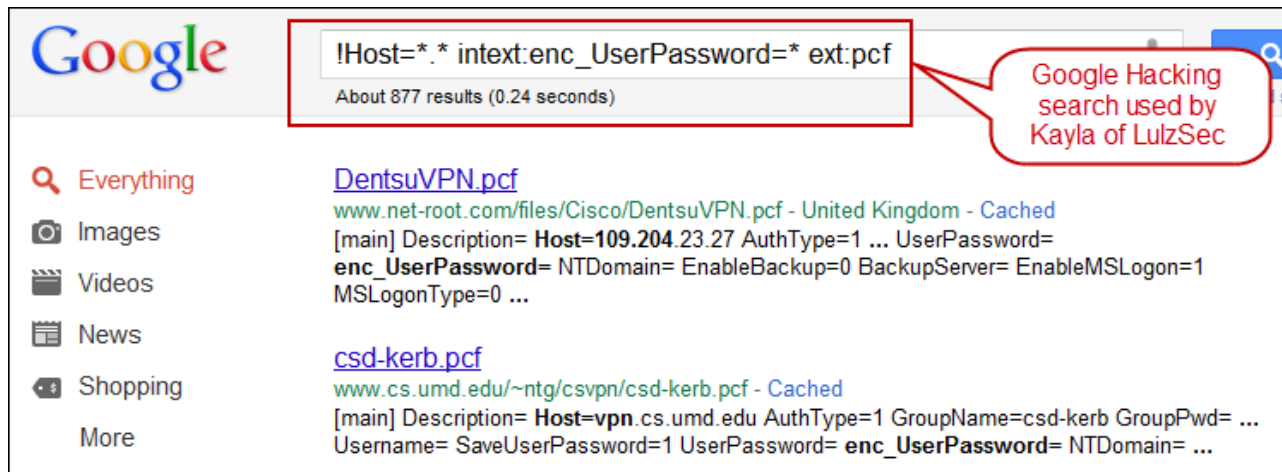
## REAL WORLD THREAT

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, with the first result being [DentsuVPN.pcf](#) from [www.net-root.com/files/Cisco/DentsuVPN.pcf](http://www.net-root.com/files/Cisco/DentsuVPN.pcf). 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 [csd-kerb.pcf](#) from [www.cs.umd.edu/~ntg/csvpn/csd-kerb.pcf](http://www.cs.umd.edu/~ntg/csvpn/csd-kerb.pcf). 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 search results, there are navigation links for "Everything", "Images", "Videos", "News", "Shopping", and "More". A red speech bubble points to the search bar with the text "Google Hacking search used by Kayla of LulzSec".

# Quick History

## GOOGLE HACKING RECAP





# 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



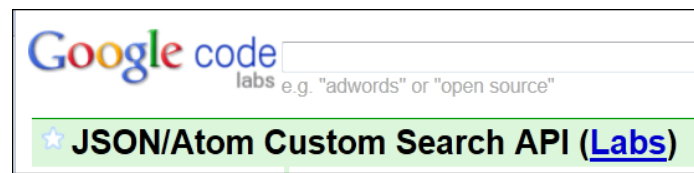


# New Features

## DIGGITY CORE TOOLS

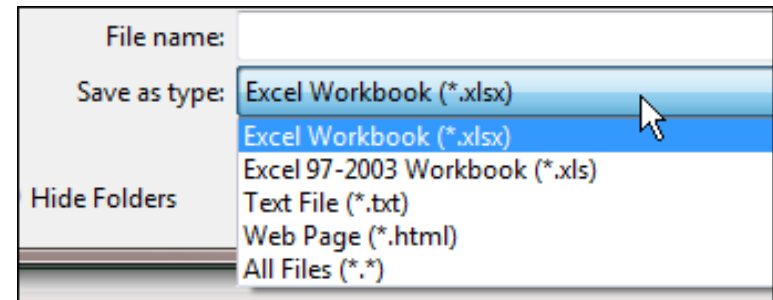
### Google Diggity - New API

- 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



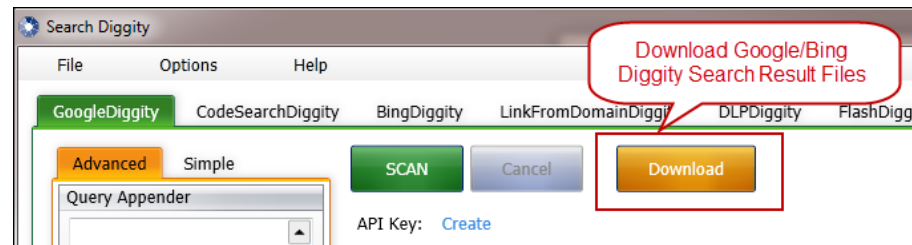


# New Features

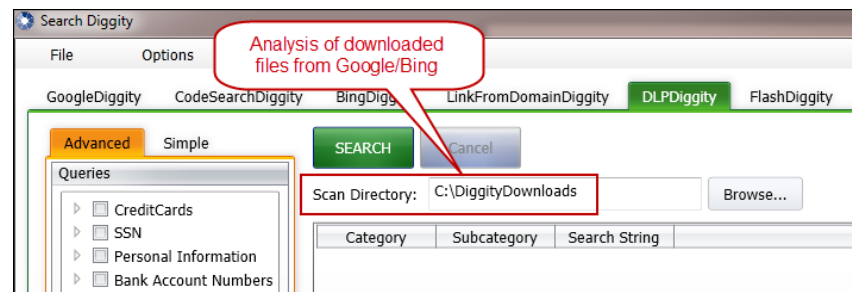
## DOWNLOAD BUTTON

### Download Buttons for Google/Bing Diggity

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

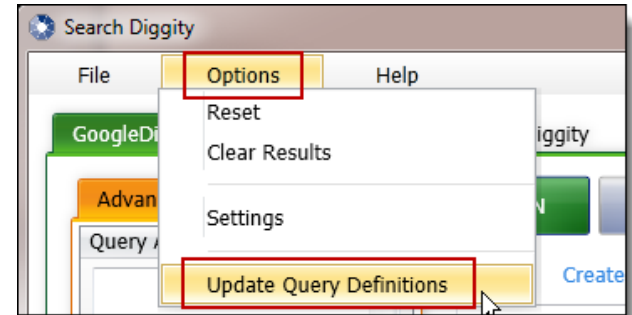


- Used by other tools for file download/analysis:
  - FlashDiggity, DLP Diggity, MalwareDiggity,...



# 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](http://www.stachliu.com/resources/tools/sharepoint-hacking-diggity-project/#SharePoint%20-%20GoogleDiggity%20Dictionary%20File)

Google  Search

About 98,300 results (0.21 seconds) [Advanced search](#)

- ▶ [Lists Web Service](#)
- POST /\_vti\_bin/lists.aspx HTTP/1.1 Host: www.wssdemo.com Content-Type: charset=utf-8 Content-Length: length SOAPAction: ...  
[www.wssdemo.com/\\_vti\\_bin/lists.aspx?op=GetListItems](http://www.wssdemo.com/_vti_bin/lists.aspx?op=GetListItems) - Cached - Similar
- [Lists Web Service](#)
- POST /\_vti\_bin/lists.aspx HTTP/1.1 Host: jubilee Content-Type: text/xml; charset=utf-8 Content-Length: length SOAPAction: ...  
[https://jubileeminneapolis.org/\\_vti\\_bin/lists.aspx](https://jubileeminneapolis.org/_vti_bin/lists.aspx)
- [Lists Web Service](#)
- POST /\_vti\_bin/lists.aspx HTTP/1.1 Host: www.votorantim.com Content-Type: text/xml; charset=utf-8 Content-Length: length SOAPAction: ...  
[www.votorantim.com/\\_vti\\_bin/lists.aspx?op=GetListItems](http://www.votorantim.com/_vti_bin/lists.aspx?op=GetListItems) - Cached

98,000 exposed SharePoint "\_vti\_bin/lists.aspx" filetype:asmx

Windows SharePoint Services  
*sharepoint Services*

# 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 bubble points to the search bar with the text: "GoogleDiggity automatically converts IP address ranges of different formats to site:10.1.\*.\* notation".

The search results include:

- [www.google.com/webmasters/](http://www.google.com/webmasters/) Do you own **216.75.\*.\***? Get indexing and r from Google.
- [Dallas Personal Injury Lawyer - 216.75.26.194/](http://216.75.26.194/)  
Freese & Goss PLLC is a newly-forme Richard A. Freese. Tim.
- [Paginas Tops del dia 216.75.7.67/topdia.php](http://216.75.7.67/topdia.php) Translate thi  
Una mujer de verdad siempre tiene su Piñera: "Y mis más condolencias a los

The 'sites/Domains/IP Ranges' panel is open, showing:

- Input field: sites/Domains/IP Ranges
- Buttons: Import, Clear, Add
- List of IP ranges:
  - 216.75.0.0/16 [Remove]
  - 216.75.26.1-216.75.26.255 [Remove]

A callout bubble points to the IP ranges with the text: "GoogleDiggity now can search IP address ranges".

# New Features

## TARGETING HTTP ADMIN CONSOLES

Searching for web admin interfaces on non-standard HTTP ports

The image displays two screenshots of Google search results. The left screenshot shows a search for `site:/com:*`, which returned approximately 681,000 results. A callout box points to the search query and another callout box points to the search results, stating: "All non-port 80/443 HTTP admin consoles for .com". The right screenshot shows a search for `site:/216.75.*:**`, which returned 16 results. A callout box points to the search query and another callout box points to the search results, stating: "IP address range search for HTTP admin interfaces on non-standard ports".

**Left Screenshot:**

- Search query: `site:/com:*`
- Results: About 681,000 results (0.06 seconds)
- Callout: All non-port 80/443 HTTP admin consoles for .com
- Visible results include:
  - [Twimbow - Colored Thought](https://www.twimbow.com:5223/)
  - [VastSpot.Com - Server](https://www.vastspot.com:81/)
  - [Davidsons Motors - Denver](https://davidsonsmotors.com:16)

**Right Screenshot:**

- Search query: `site:/216.75.*:**`
- Results: 16 results (0.06 seconds)
- Callout: IP address range search for HTTP admin interfaces on non-standard ports
- Visible results include:
  - [SmarterMail Login - SmarterMail](https://216.75.63.101:9998/)
  - [SHOUTcast Administrator](https://216.75.172.130:8015/)
  - [Prolinkweb - Web Mail](https://216.75.20.82:32000/mail/)

# 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 'Query Appender' and 'Queries' panels. The 'Queries' panel shows a tree view with 'GHDB' expanded, listing various search categories like 'Advisories and Vulnerabilities', 'Error Messages', etc. The main workspace contains a 'SCAN' button, a 'Download' button, and a 'Sites/Domains' list with 'stachliu.com' selected. Below this is a table of search results.

Category	Subcategory	Search String	Page Title	URL
Custom	Custom	site:stachliu.com	Stach & Liu	<a href="http://www.stachliu.com/">http://www.stachliu.com/</a>
Custom	Custom	site:stachliu.com	Services « Stach & Liu	<a href="http://www.stachliu.com/services/">http://www.stachliu.com/services/</a>
Custom	Custom	site:stachliu.com	Resources « Stach & Liu	<a href="http://www.stachliu.com/resources/">http://www.stachliu.com/resources/</a>
Custom	Custom	site:stachliu.com	Company « Stach & Liu	<a href="http://www.stachliu.com/company/">http://www.stachliu.com/company/</a>

The 'Output' panel shows the following text:

```
Using API Key: ALZAsyDIIUASIVNLC-aw_1IuzFNU7tDUC-9qKI-EURDM.  
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 shows '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 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	<a href="http://www.stachliu.com/">http://www.stachliu.com/</a>
Custom	Custom	ip:98.129.200.37	Lord of the Bin	<a href="http://www.stachliu.com/slides/lordofthebing.pdf">http://www.stachliu.com/slides/lordofthebing.pdf</a>
Custom	Custom	ip:98.129.200.37	Lord of the Bin	<a href="http://www.stachliu.com/slides/bh2010-lordofthebing.pdf">http://www.stachliu.com/slides/bh2010-lordofthebing.pdf</a>
Custom	Custom	ip:98.129.200.37	Secure Web A f	<a href="http://www.stachliu.com/brochures/securewebappdevjava.pdf">http://www.stachliu.com/brochures/securewebappdevjava.pdf</a>
Custom	Custom	ip:98.129.200.37	Google Hacking	<a href="http://www.stachliu.com/resources/tools/google-hacking-diggity-project/">http://www.stachliu.com/resources/tools/google-hacking-diggity-project/</a>
Custom	Custom	ip:98.129.200.37	Tools « Stach &	<a href="http://www.stachliu.com/resources/tools/">http://www.stachliu.com/resources/tools/</a>

**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

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 SQL Server User Group Terminal Server User Profiles Users Server 2003 Terminal Server Users Create SQL Server User

**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 interface. The search query is `select.*from.*request\..QUERYSTRING`. The search results show a file named `post.asp` with the following code snippet:

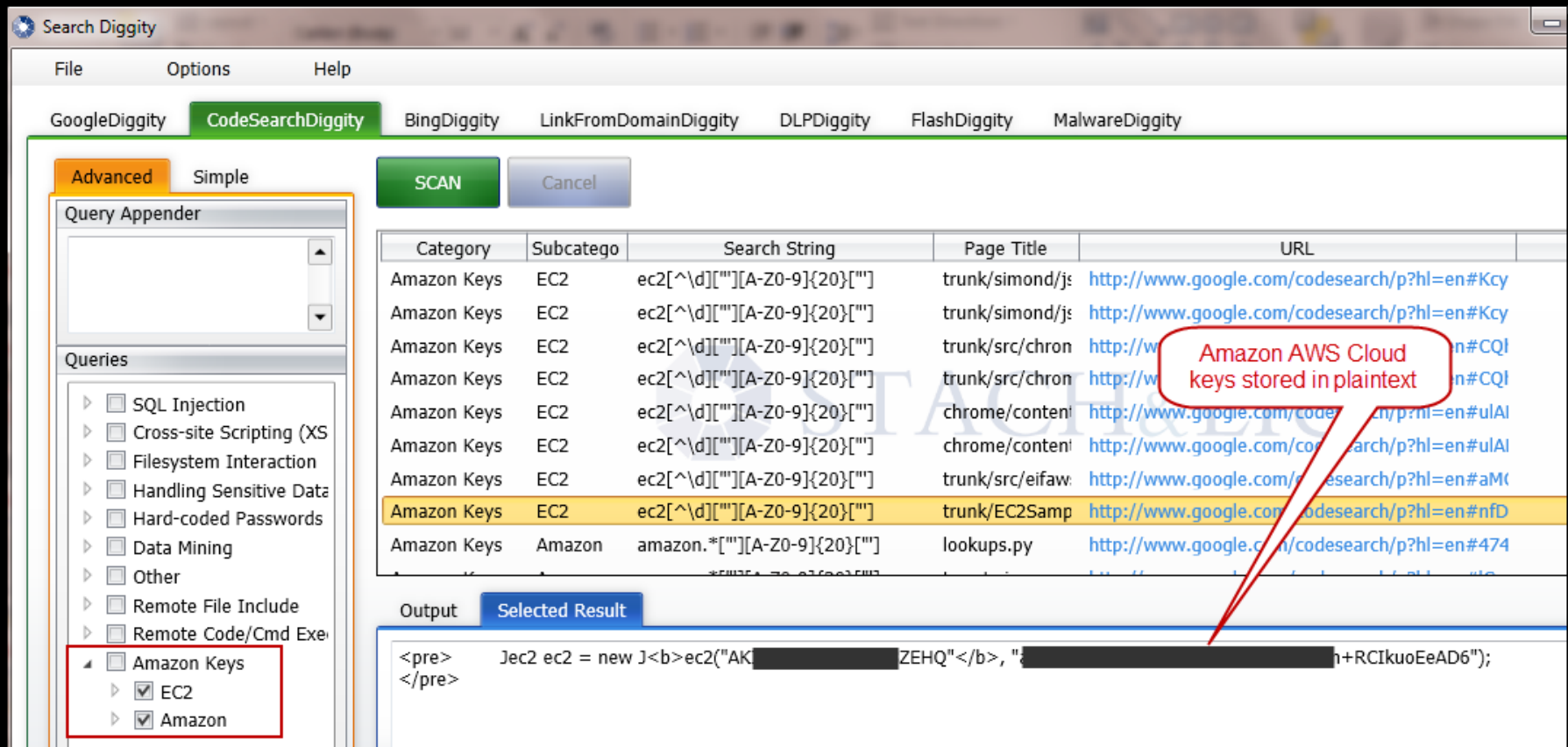
```
45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ĀĪĀŌĀ×÷Ōß°Í¹ÙÀĪŌ†²ĀĀŪ†ā₄Ōā,øĭŭ×ó."

57: strSql = "SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ĀĪĀŌĀ×÷Ōß°Í¹ÙÀĪŌ†²ĀĀŪ†ā₄Ōā,øĭŭ×ó."
```

A red callout box points to the `reply_id` parameter in the first query string, stating: `reply_id` is SQL injectable querystring parameter. The search results also show the URL `www.cnarts.net/eweb/download/software/bbs/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:

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

# Cloud Docs Exposures

PUBLIC CLOUD SEARCHING

Public cloud storage document exposures



Dropbox

Google docs

Google search results for the query: `intext:"name" intext:"address" intext:"taxpayer" site:dl.dropbox.com`. The search returned 7 results in 0.23 seconds. A callout bubble points to the search query with the text: "Looking for sensitive data leaks in Dropbox cloud storage". One of the search results is a PDF file named "W-9" with the URL `https://dl.dropbox.com/s/.../CTMUN_W9_Request_For_TaxID.pdf?...`. A second search is shown below, with the query: `site:live.com "skydrive" ext:dmp`. A callout bubble points to this search with the text: "Database dump files on Microsoft SkyDrive". The results for this search include "Windows Live SkyDrive" links to files like `https://skydrive.live.com/embedicon.../Open 060510-38688-01.dmp` and `https://skydrive.live.com/embedicon.../Open 122509-26520-01.dmp`.

Google search results for the query: `intext:"enable password" inurl:docid site:docs.google.com`. The search returned 4 results in 0.13 seconds. A callout bubble points to the search query with the text: "Cisco config files with passwords in Google Docs files". The search results include several Google Docs links, such as `https://docs.google.com/View?docid=0AbKTT...1...1...`. One of the results contains the text: `boot-end-marker ! enable secret 5 $1$BHsg$izpAqHDULzEWCqfP/leT/ enable password 7 0455254C5F765C ! no aaa new-model. system mtu routing 1500 ...`. Another result contains: `enable secret 5 $1$P6du$.NRbLzz5WIKER5mgw.t7r enable password 7 000A3D4C540C1B ! no aaa new-model. system mtu routing 1500. ip subnet-zero ...`. A third result contains: `logging buffered 51200 warnings. enable secret 5 $1$.7NSRu28/DDfSHrAgq5bhUFz enable password 7 151C2546547D25 ! no aaa new-model ! resource ...`. The search is performed from the location "Tempe, AZ".



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 (redacted), 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 shows '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, showing 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' section 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]'. The tool logo 'linkfromdomaindiggity' is visible in the bottom right corner.

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

# DLP Diggity



# DLP Diggity

LOTS OF FILES TO DATA MINE

Google search results for `filetype:pdf`. The search returned approximately 513,000,000 results in 0.25 seconds.

Google search results for `filetype:doc`. The search returned approximately 84,500,000 results in 0.10 seconds.

Google search results for `filetype:xls`. The search returned approximately 17,300,000 results in 0.13 seconds.

Bing search results for `filetype:doc`. The search returned 1-10 of 26,900,000 results. The interface includes a search bar with the query, a 'Web' filter, and a 'More' dropdown menu.

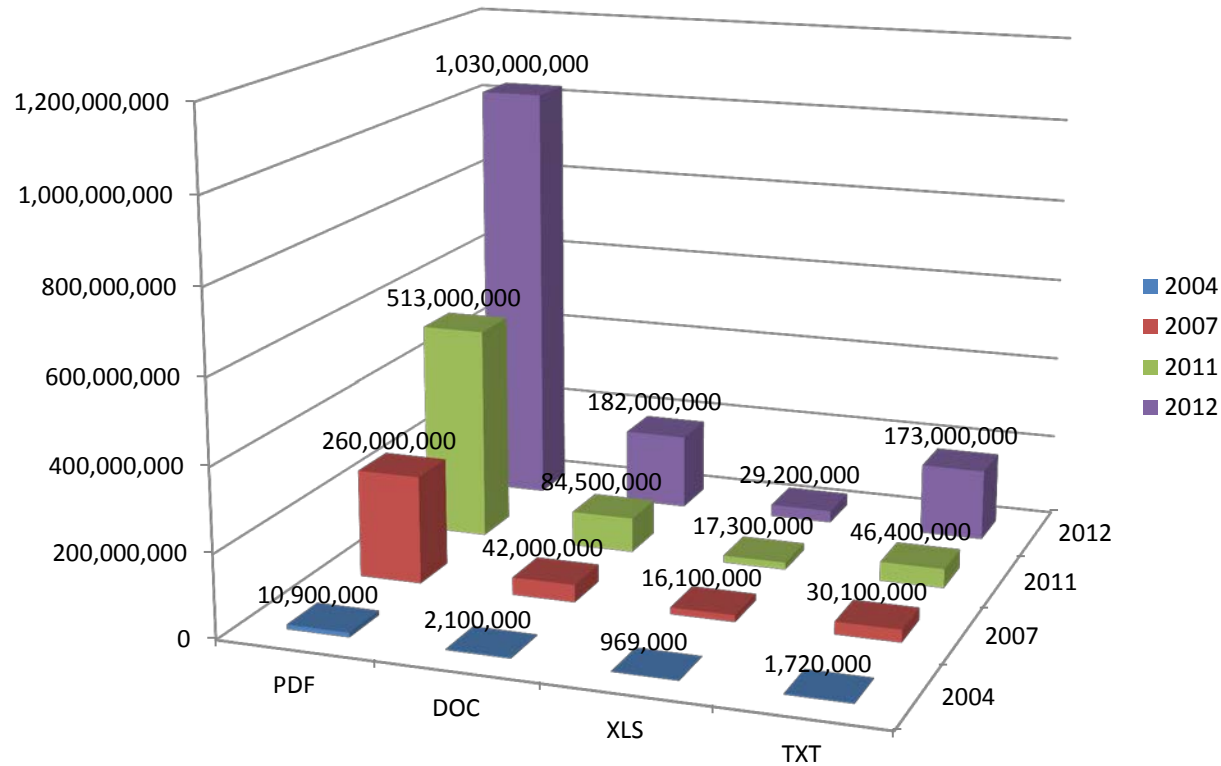
Bing search results for `filetype:pdf`. The search returned 1-10 of 146,000,000 results. The interface includes a search bar with the query, a 'Web' filter, and a 'More' dropdown menu.



# DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR

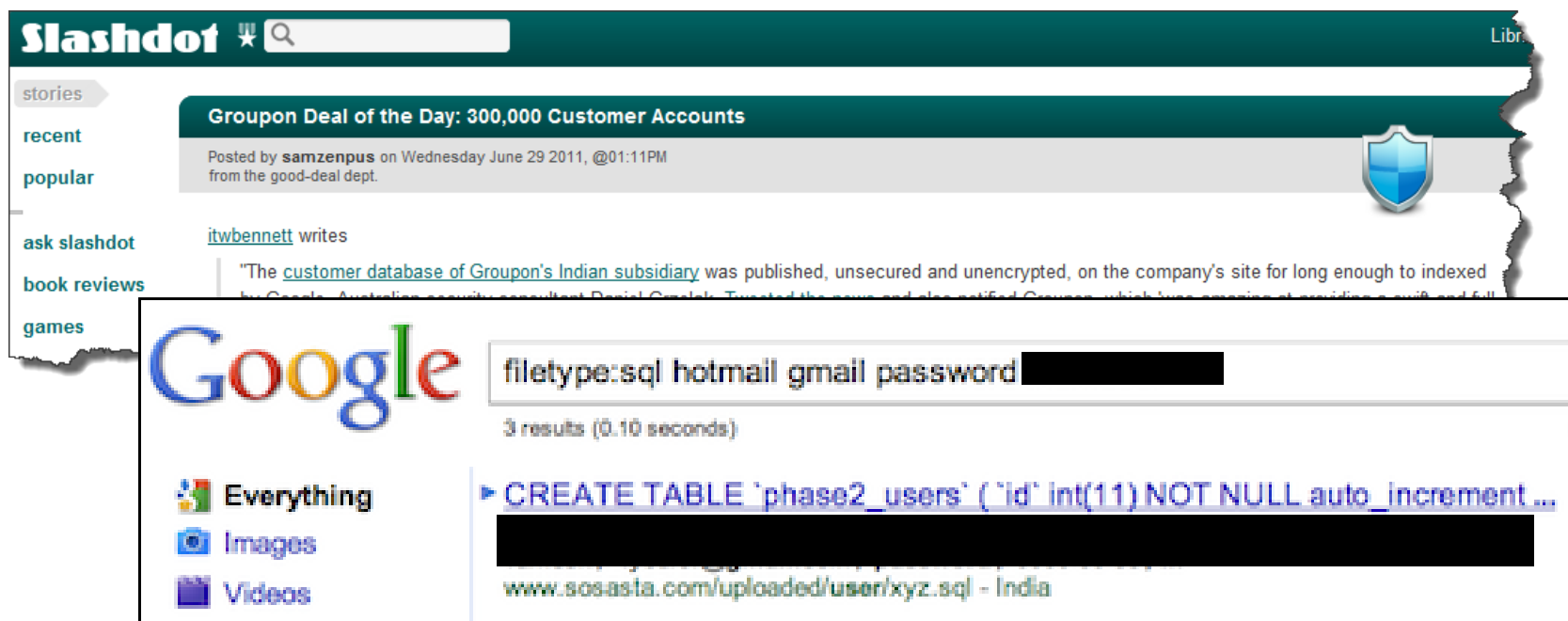
### Google Results for Common Docs



# Data Loss In The News

## MAJOR DATA LEAKS

- Groupon.com Leaks 300,000 users emails and passwords
  - `filetype:sql hotmail gmail password`



The image shows a screenshot of a Slashdot article titled "Groupon Deal of the Day: 300,000 Customer Accounts" posted by samzenpus on Wednesday June 29 2011. The article text mentions that the customer database of Groupon's Indian subsidiary was published, unsecured and unencrypted, on the company's site for long enough to be indexed by Google. A blue shield icon is visible on the right side of the article header.

Below the article is a Google search result for the query `filetype:sql hotmail gmail password`. The search shows 3 results in 0.10 seconds. The top result is a snippet from `www.sos-asta.com/uploaded/user/xyz.sql - India`, which includes the SQL command `CREATE TABLE 'phase2_users' ('id' int(11) NOT NULL auto_increment...`.

# Data Loss In The News

## MAJOR DATA LEAKS

- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet



# DLP Diggity

## DIGGITY TOOLKIT

The screenshot displays the DLP Diggity application interface. At the top, there are tabs for different 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 also 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:

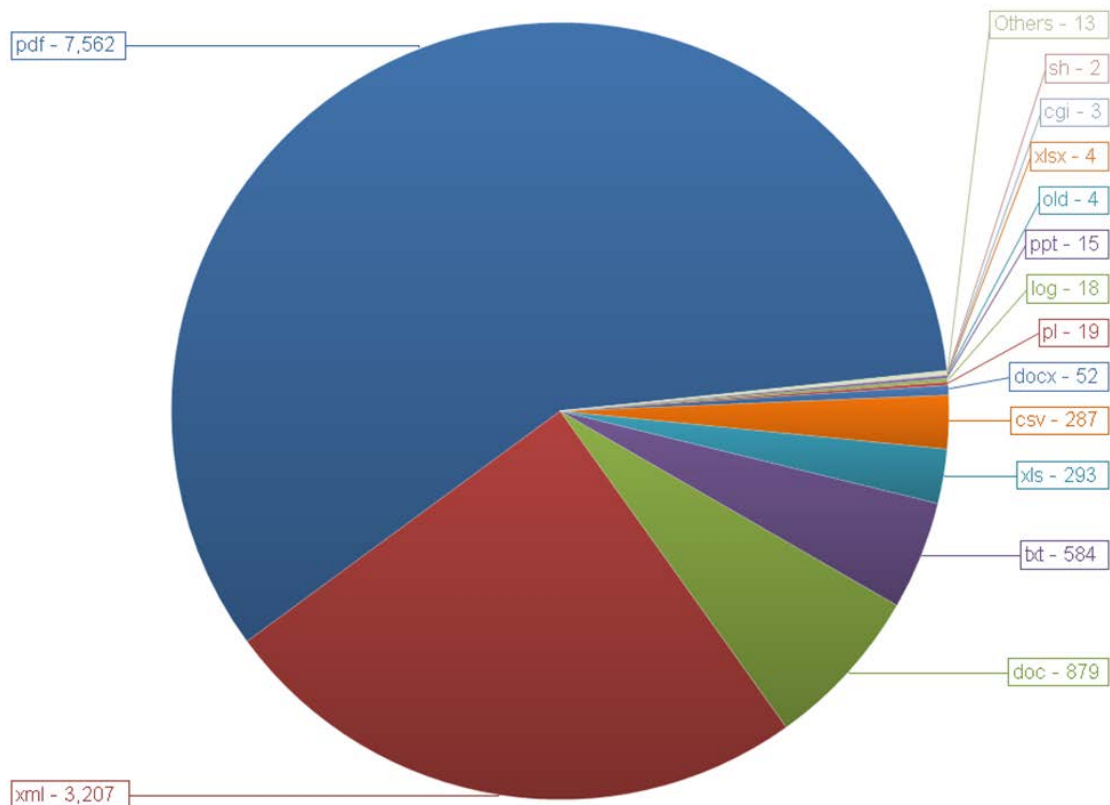
```
21 Jerry,  
22 This is Mary. I forgot to include my social security number in those clearance documents I su  
Would you mind adding it in for me? My SSN is 123-45-6789. Thanks a lot!  
23 - Mary  
24
```

# DLP Reporting

## PRACTICAL EXAMPLES

DLPDiggity - # of Files Analyzed per File Extension

Total = 12,943 files



# DLP Reporting

## PRACTICAL EXAMPLES

### Automagic Removal Process, DORK, GHDB, XSS.CX, Vulnerability Management, Best Practices

Updated October 8, 2011

#### Executive Summary

XSS.CX is an automated Anti-Phishing Execution Robot defined as a SCAP Expert System performing Vulnerability Execution, Risk Analysis and Reporting into the Public Domain for the public convenience and necessity of securing personally identifying information.

#### General Information

The Anti-Phishing Web Crawler publishes Vulnerable Host reports into the Public Domain which are then indexed Search Engines.

Companies with external facing Vulnerability Management Programs then identify the XSS.CX Report, resolving the vulnerability in the normal course of business.

www.google.com/cse/home?cx=008801388445696029762:5wl5jq9fxnc

Google custom search

XSS.CX Research

Google™ Site Search Search

Google CSE providing search access to XSS.CX vulnerability results

**Search engine details**

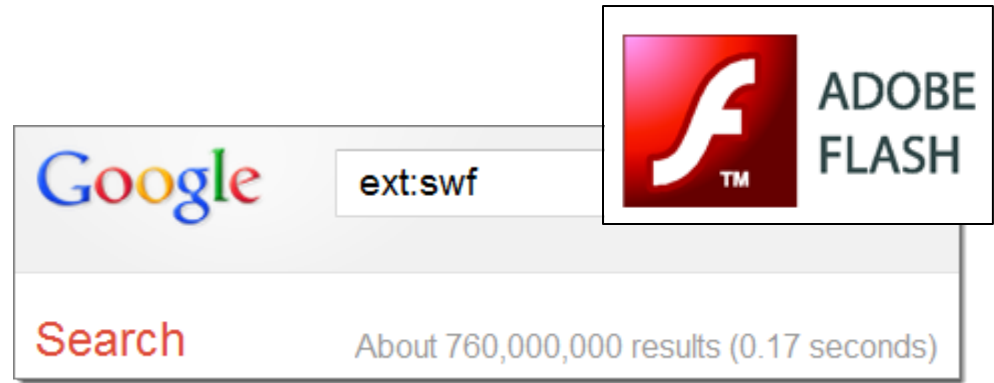
Proof of Concept CWE-79, CWE-89 and CWE-113 Reports for XSS, SQL Injection and HTTP Header Injection by Hoyt LLC Research

searches sites including: <http://xss.cx>, <http://www.cloudscan.me>

Keywords: XSS, SQL Injection, HTTP Header Injection, CWE-79, CWE-89, CWE-113, Hoyt LLC Research

Last updated: March 2, 2011



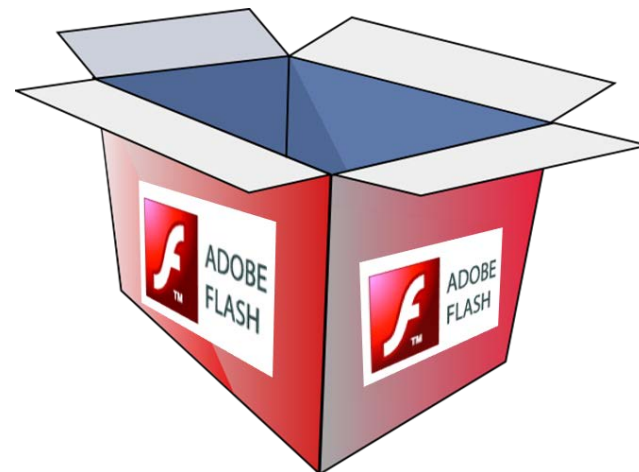


NEW GOOGLE HACKING TOOLS

# FlashDiggity

# FlashDiggity

## DIGGITY TOOLKIT



- Google/Bing 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 window. The 'FlashDiggity' tab is selected. The 'Advanced' search mode is active. 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 following code snippet:

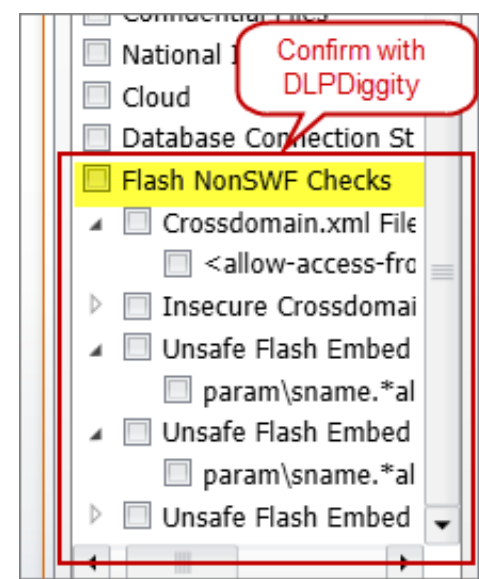
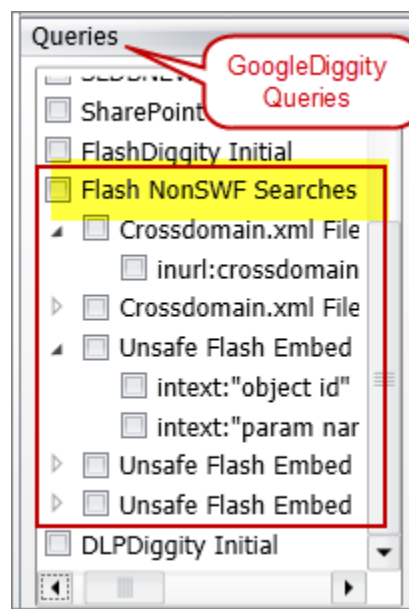
```
20 if (UserName.text == 'mizzico' && PassWord.text == 'furniture') {
21     getURL('http://www.dizzypixel.com/login/mizzico/login.html', _blank);
22     login_incorrect_alpha = 0;
23 } else {
24     if (UserName.text == 'sonya' && PassWord.text == 'paz') {
25         getURL('http://www.dizzypixel.com/login/sonyapaz/index.html',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

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

# Flash Non-SWF Hacking

## OTHER FLASH HACKING

- **Google/Bing for Non-SWF** files on target domains, but related to Flash. Example queries:
  - `inurl:crossdomain.xml ext:xml intext:"secure" intext:"false"`
  - `intext:"swf" intext:"param name" intext:"allowNetworking * all"`
- **Download** Non-SWF files to `C:\DiggityDownloads\`
- Use DLPDiggity to **analyze** for non-SWF Flash vulnerabilities, such as:
  - Crossdomain.xml Insecure Settings
    - Secure flag set to false
    - Open \* wildcard used
  - Unsafe Flash HTML Embed Settings:
    - AllowScriptAccess always
    - AllowNetworking all
    - AllowFullScreen true





NEW GOOGLE HACKING TOOLS

# Malware Diggity

# MalwareDiggity

## DIGGITY TOOLKIT

1. Leverages Bing's `linkfromdomain:` search operator 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 – 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-man-

When researchers from [Search Engine](#) search results suggested [search results](#) showed t

**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 is a sidebar with links for 'stories', 'recent', 'popular', 'ask slashdot', 'book reviews', 'games', and 'idle'. The main content area features a dark green header for the article 'Mysql.com Hacked, Made To Serve Malware', posted by 'Soulskill' on Monday, September 26, 2011, at 06:52 PM. Below this, the text reads 'Orome1 writes' followed by a quote: 'Mysql.com was compromised today, [redirecting visitors to a page serving malware](#). Security firm Armorize [detected the compromise through its website malware monitoring platform HackAlert](#) and has analyzed how...'. A red banner below the quote reads 'FILED UNDER: INSECURITY COMPLEX | SECURITY' and 'Hacked MySQL.com used to serve Windows malware'. The article is by 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.php	http://ecommerceparis.com/2011/index.php	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

INTERPARK 티켓

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	<a href="#">shentime.com</a>	Movies	6,100,000
902	<a href="#">ovi.com</a>	Mobile Apps & Ad	6,100,000
903	<a href="#">zumi.pl</a>	Business & P	6,100,000
904	<a href="#">natwest.com</a>	Banking	6,100,000
905	<a href="#">peixurbano.com.br</a>	Coupons & Discount Offers	6,100,000
906	<a href="#">soundcloud.com</a>	Music Equipment & Technology	6,100,000
907	<a href="#">interpark.com</a>	Shopping	6,100,000
908	<a href="#">hotpepper.jp</a>	Dining Guides	6,100,000

Links to michoo.co.kr

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

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 ~ 9월 3일(일) 15:00 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/](http://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/](http://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"**



# Malware Defenses

## BLACKHAT SEO DEFENSES

- Malware Warning Filters
  - Google Safe Browsing
  - Microsoft SmartScreen Filter
  - Yahoo Search Scan
- Sandbox Software
  - Sandboxie ([sandboxie.com](http://sandboxie.com))
  - Dell KACE - Secure Browser
  - Office 2010 (Protected Mode)
  - Adobe Reader Sandbox (Protected Mode)
- No-script and Ad-block browser plugins

# Advanced Defenses

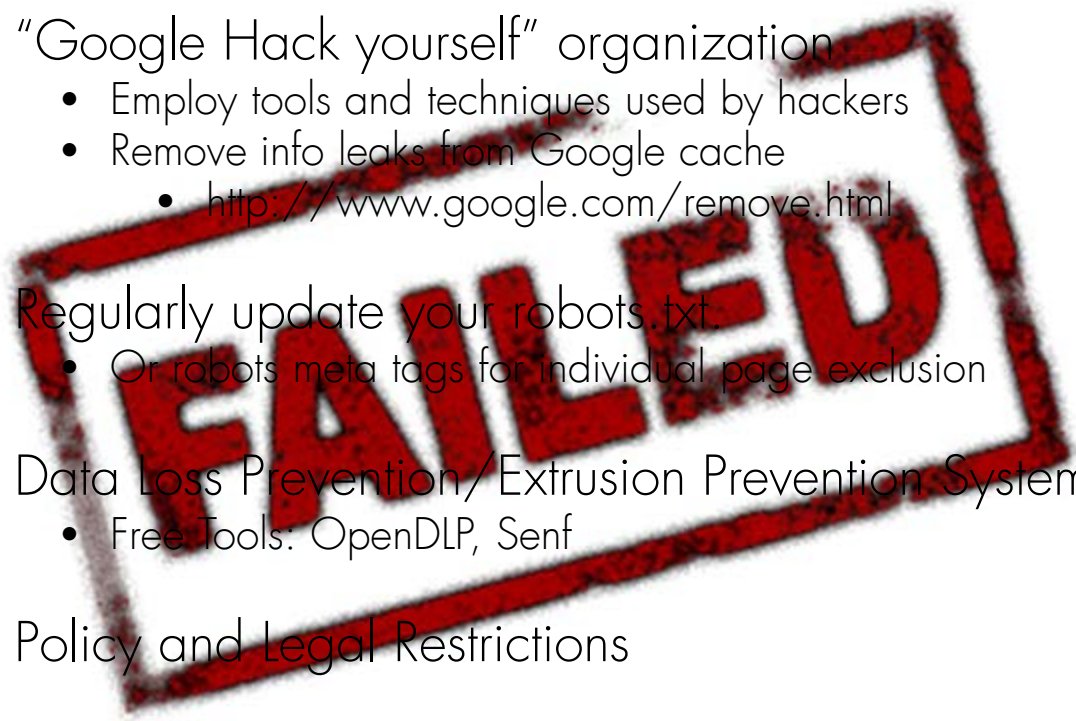
PROTECT YO NECK



# Traditional Defenses

## GOOGLE HACKING DEFENSES

- “Google Hack yourself” organization
  - Employ tools and techniques used by hackers
  - Remove info leaks from Google cache
    - <http://www.google.com/remove.html>
- 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

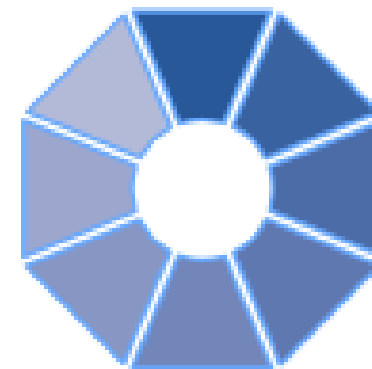
**FAILED**

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

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...](http://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

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 highlighted with a red box and has a callout bubble pointing to it. The callout bubble contains the text: "SNAP network attached storage servers exposed".

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

Feed items include:

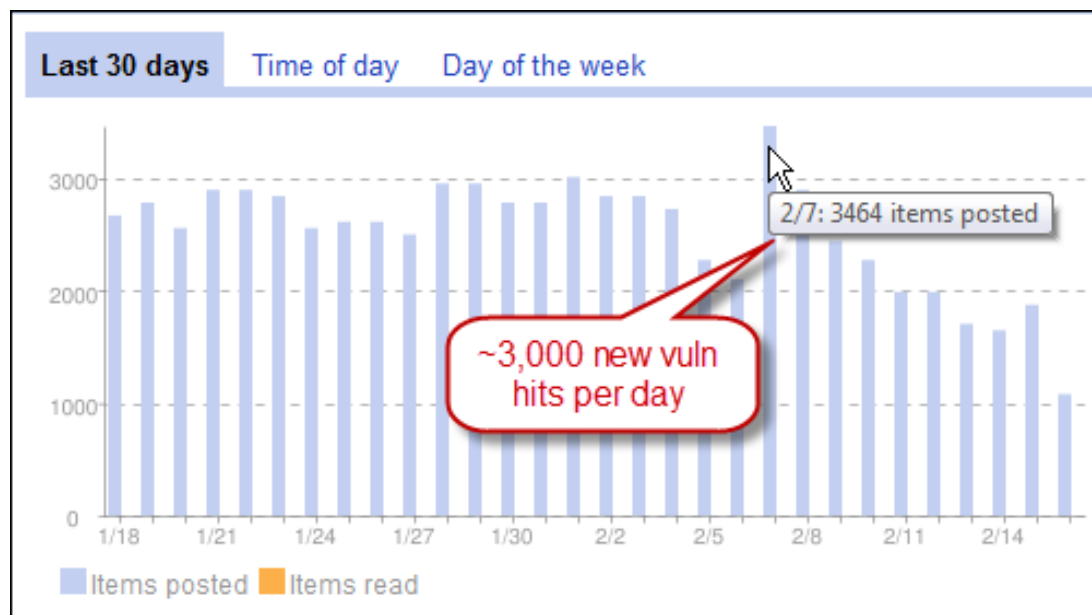
- Snap Server WELW-SNAP [Home] - WELW-SNAP • Home
- Snap Server CORESERVER [Home] - CORESERVER • Home
- Snap Server GSTI [Home] - GSTI • Home
- adsphotographer.com - SNAP55373 • Home
- Snap Server SNAP824929 [Home] - SNAP824929 • Home
- Snap Server SAINTSNAP [Home] - SAINTSNAP • Home
- Snap Server DIGITALDATA1 [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 personal Web Hosting: [msmcs.net](http://msmcs.net) - [www.msmcs.net](http://www.msmcs.net) PUB FTP
- Snap Server XRAY7 [Home] - XRAY7 • Home

# 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



 **Google reader 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

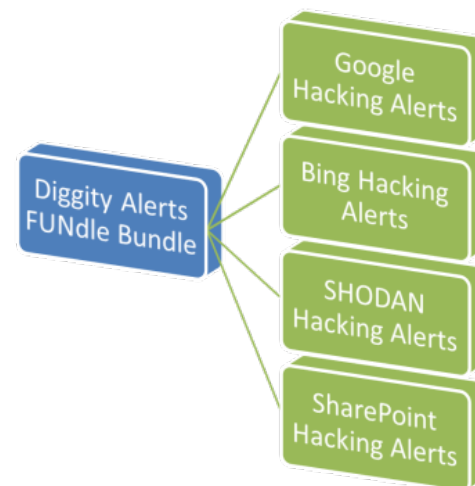
(New Hanover County)--- New Hanover County and municipal of ... with representatives of the Federal Emergency Management Agency ... [www.nhcgov.com/News/\\_layouts/listform.aspx?...](http://www.nhcgov.com/News/_layouts/listform.aspx?...)

**\*Curriculum Vitae\***

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

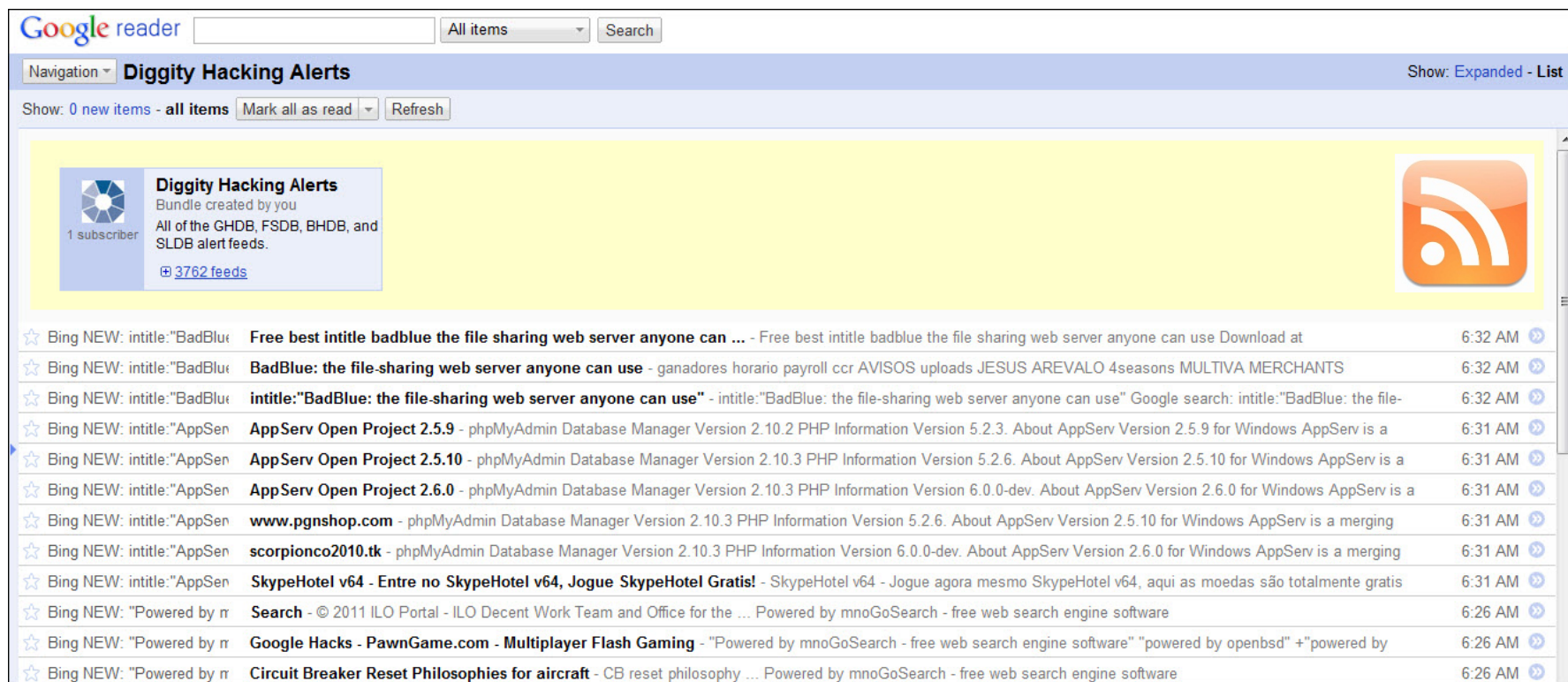
Work **Phone Number: 972-860-4130** for emergency only. **E-mail address:** [shavanal@dcccd.edu](mailto:shavanal@dcccd.edu). Education. I received my Associates in Arts and Sciences from ... [hb2504.dcccd.edu/vita/0017421.pdf](http://hb2504.dcccd.edu/vita/0017421.pdf)

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 for a feed named "Diggity Hacking Alerts". The feed is described as a bundle created by the user, containing all feeds from GHDB, FSDB, BHDB, and SLDB. It has 1 subscriber and 3762 feeds. The feed contains a list of news items, primarily about AppServ and BadBlue.

Source	Title	Time
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\\*](#) - [Google Alerts - intitle:index of passwd passwd bak](#)
- 4 [\\*Usage Statistics for\\* gui](#)
- 5 [\\*Usage Statistics for\\* tota](#)
- 6 [Phoca Forum • View topi](#)
- 7 [pongamos que hablo de](#)
- 8 [bomb wiz - MP3moo.com](#)
- 9 [sarrafyurdaer.com](#) - [Google](#)
- 0 [more...](#)
- # [mark these items as re](#)

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



The screenshot shows a Google Reader interface for the 'Diggity Hacking Alerts' feed. The feed title is 'Diggity Hacking Alerts' and it includes a '« Feeds' button and refresh/expand icons. The feed items are:

- ★ **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, 1027, 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...



[ult resource'](#)  
[esource"](#)



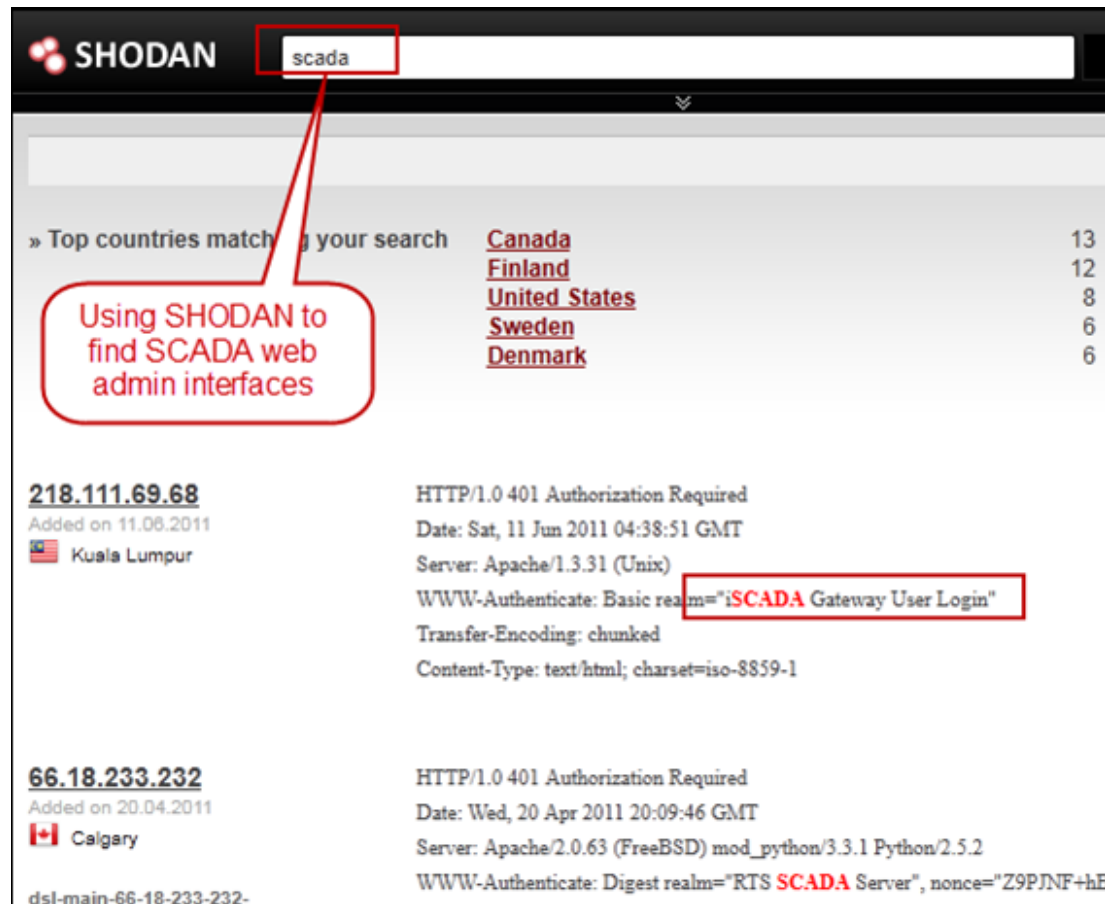
ADVANCED DEFENSE TOOLS

# SHODAN Alerts



# SHODAN Alerts


## FINDING SCADA SYSTEMS




SHODAN

» Top countries matching your search

<a href="#">Canada</a>	13
<a href="#">Finland</a>	12
<a href="#">United States</a>	8
<a href="#">Sweden</a>	6
<a href="#">Denmark</a>	6

**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-

Using SHODAN to find SCADA web admin interfaces

# 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

- ★ **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 displays two overlapping windows of the Alerts Diggity application. The background window shows the 'Subscribed Feeds' tab with a search bar containing 'milblogging.com' and an 'Add' button. The foreground window shows the 'Update' button pressed, resulting in a table of feed entries. A green notification window titled 'Hack Alerts Update' is overlaid on the bottom right, stating: 'Hack Alerts is up to date. 2 vulnerabilities were found.'

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

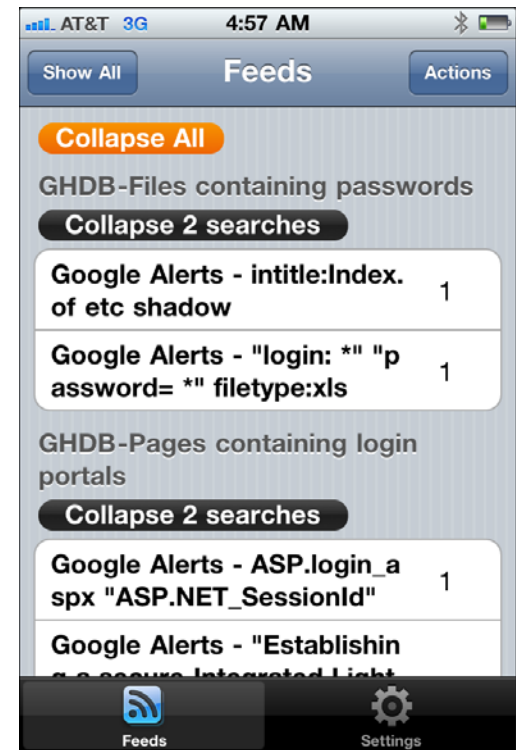
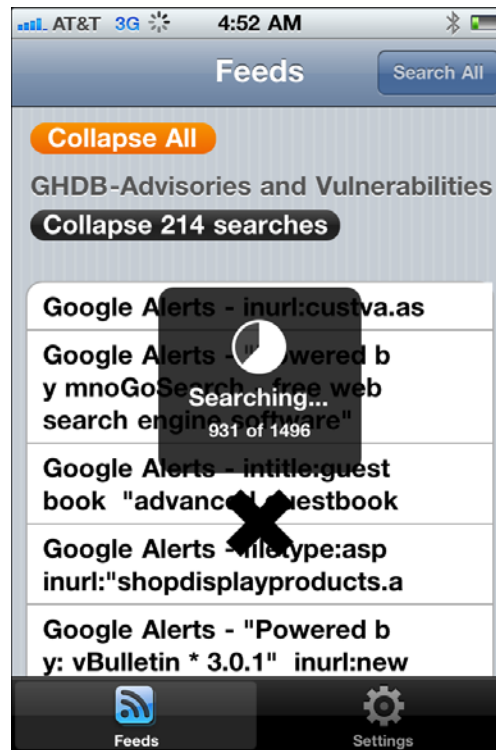
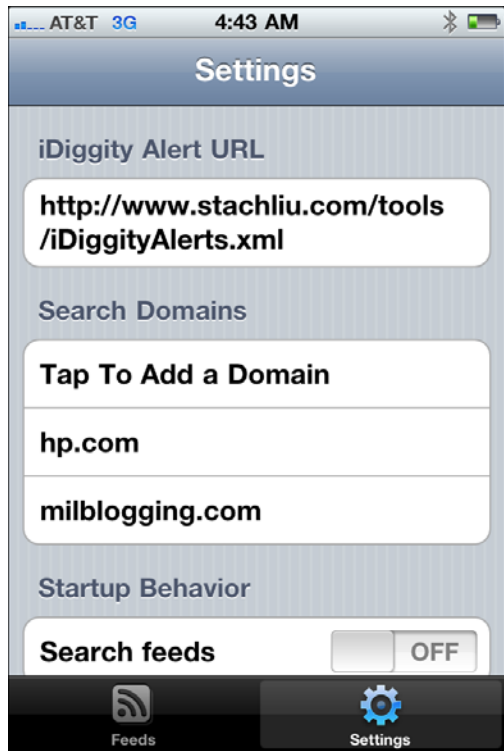


ADVANCED DEFENSE TOOLS

# iDiggity Alerts

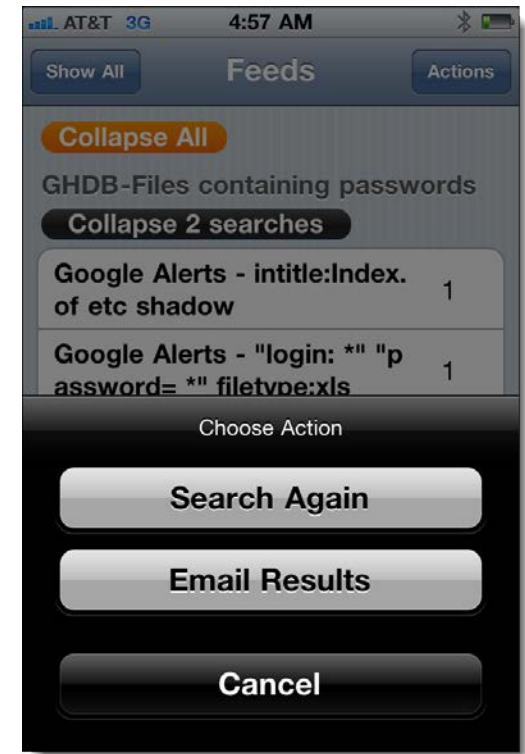
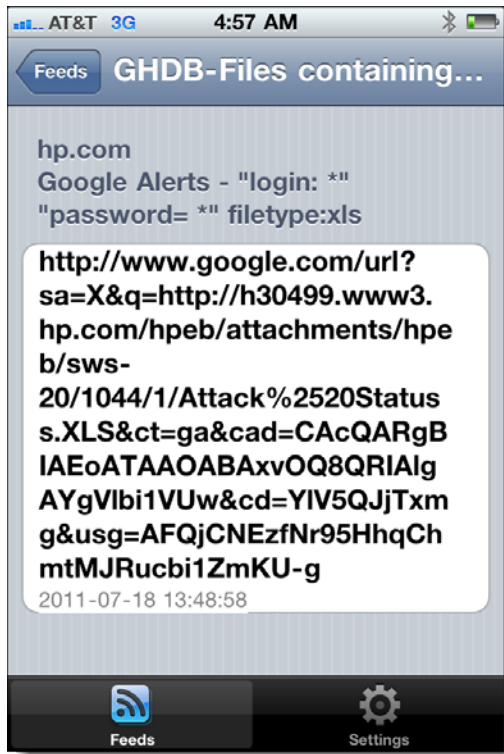
# iDiggity Alerts

## 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 <b>Data</b> 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 <b>Data</b> 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

World map showing red highlights indicating data locations or sources.



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

For more info:  
Fran Brown  
Rob Ragan (@sweepthatleg)  
Email: [contact@stachliu.com](mailto:contact@stachliu.com)  
Project: [diggity@stachliu.com](mailto:diggity@stachliu.com)  
Stach & Liu, LLC  
[www.stachliu.com](http://www.stachliu.com)



# Thank You

Stach & Liu Google Hacking Diggity Project info:

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