



Pulp Google Hacking

The Next Generation Search Engine Hacking Arsenal

26 October 2011 – Hacker Halted 2011 – Miami, FL



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



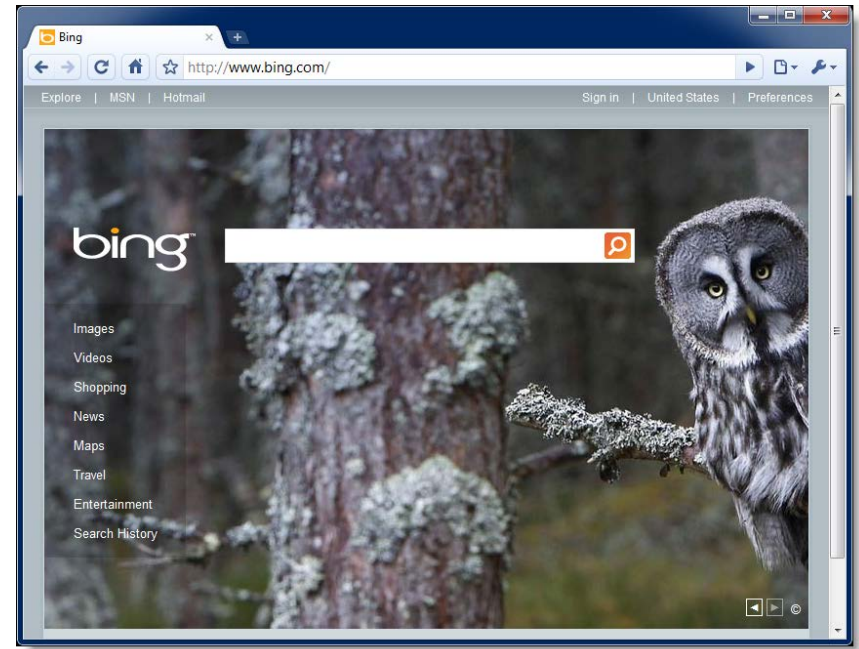
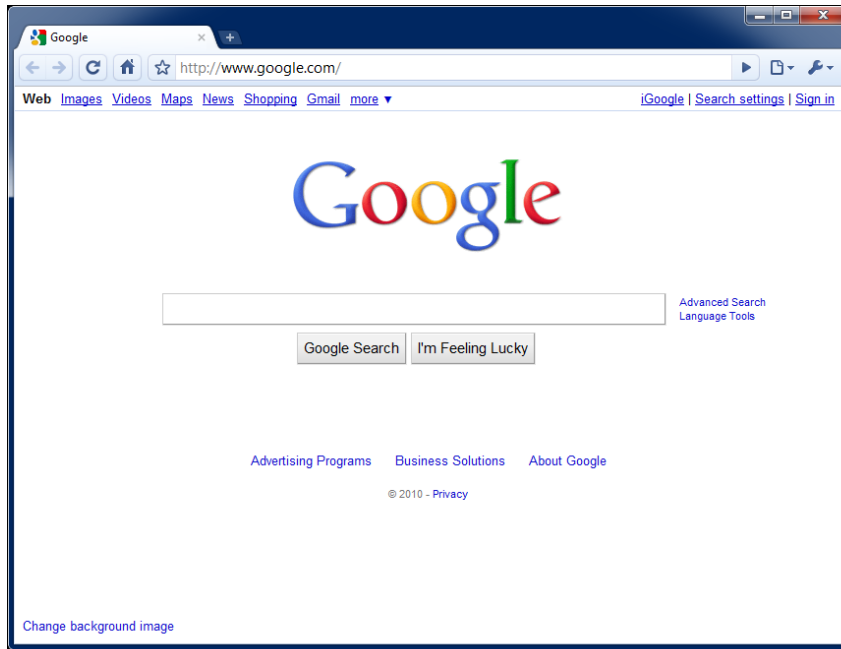
Open Source Intelligence

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

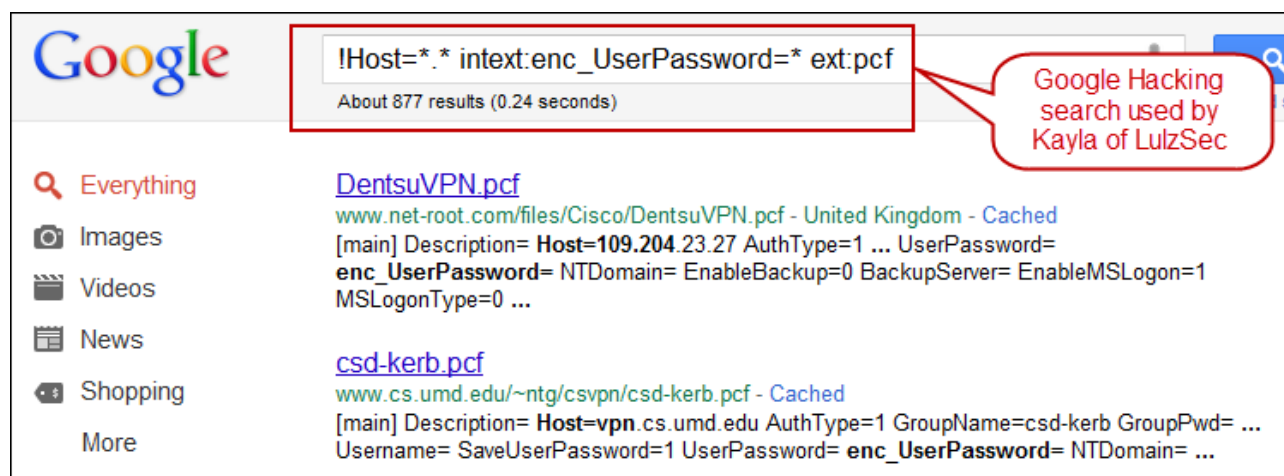
REAL WORLD THREAT

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 the URL 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 titled "csd-kerb.pcf" and is from the URL 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 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 2007	Bing disables inurl: link: and linkdomain:
Nov 2, 2007	Google Hacking v2 released



Quick History...cont.

GOOGLE HACKING RECAP

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



Advanced Attacks

WHAT YOU SHOULD KNOW



Diggity Core Tools

STACH & LIU TOOLS

Google Diggity

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



Bing Diggity

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



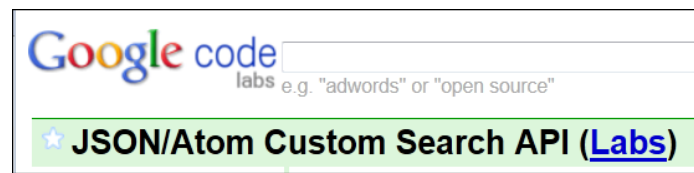


New Features

DIGGITY CORE TOOLS

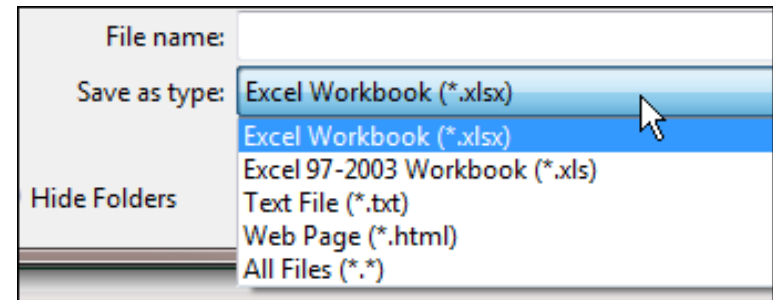
Google Diggity - New API

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



Misc. Feature Upgrades

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

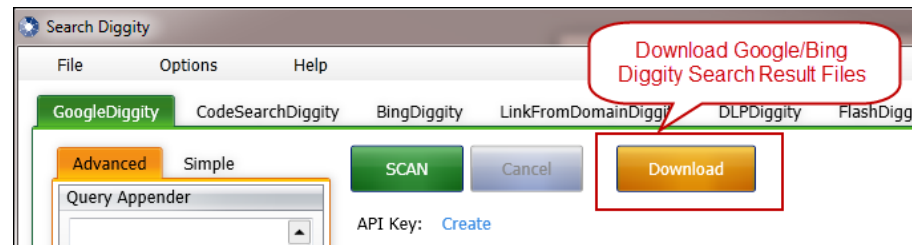


New Features

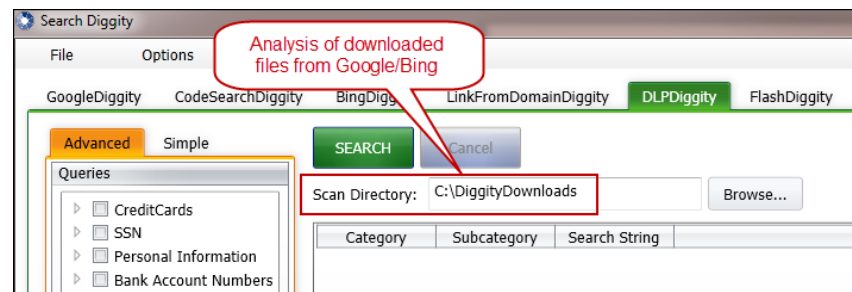
DOWNLOAD BUTTON

Download Buttons for Google/Bing Diggity

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

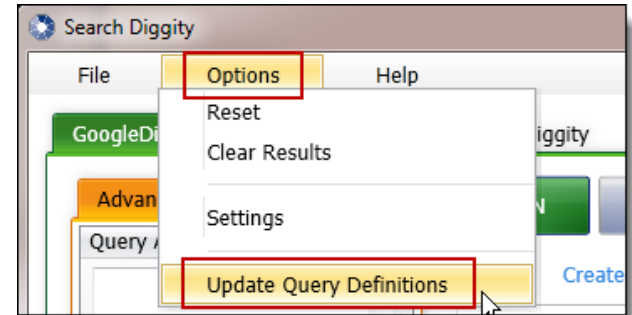


- Used by other tools for file download/analysis:
 - FlashDiggity, DLP Diggity, MalwareDiggity,...



New Features

AUTO-UPDATES



SLDB Updates in Progress

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



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 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

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 result for the query `select.*from.*request\..QUERYSTRING`. The search results page displays the following code snippet from a file named `post.asp`:

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

A red callout box points to the `reply_id` parameter in the SQL query, stating: `reply_id` is SQL injectable querystring parameter. The parameter is also circled in red in the code snippet.

Results 1 - 10 of about 2,000.

www.cnarts.net/eweb/download/software/bbs/tradeforum.zip - Unknown - ASP - [More from tradeforum.zip](#) »

CodeSearch Diggity

AMAZON CLOUD SECRET KEYS

The screenshot displays the CodeSearch Diggity application window. The interface includes a menu bar (File, Options, Help), a toolbar with buttons for 'SCAN' and 'Cancel', and a sidebar with a 'Query Appender' and a 'Queries' list. The 'Queries' list has 'Amazon Keys', 'EC2', and 'Amazon' checked. The main area shows a table of search results with columns for Category, Subcategory, Search String, Page Title, and URL. A red callout box points to a result with the URL 'http://www.google.com/codesearch/p?hl=en#nfD' and the page title 'trunk/EC2Samp'. Below the table, the 'Output' section shows a code snippet:

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

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

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



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 navigation bar. The interface includes a 'SCAN' button, a 'Cancel' button, a 'Bing 2.0 API Key' field with a 'Create' link, and a 'Domain' field containing 'stachliu.com'. Below these are tabs for 'URLs', 'Applications', 'Hosts', and 'Domains'. The 'URLs' tab is active, displaying a list of external links. A red callout box points to 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 URLs 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 status bars at the bottom indicate 'Google Status: Ready' and 'Bing Status: Ready'.

Bing LinkFromDomain

FOOTPRINTING LARGE ORGANIZATIONS

The screenshot shows the LinkFromDomainDiggity tool interface. The 'Query Appender' field contains 'site:gov.cn'. The 'Sites/Domains' field contains 'www.gov.cn'. The 'Hosts' tab is selected, displaying a list of hostnames: 2010.visithainan.gov.cn, app.mps.gov.cn, bg.mofcom.gov.cn, bjsat.gov.cn, bjyouth.gov.cn, catf.agri.gov.cn, and cc.fjkl.gov.cn. The 'Output' pane shows the 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]'.

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

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

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



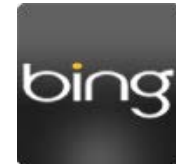
NEW GOOGLE HACKING TOOLS

Malware Diggity

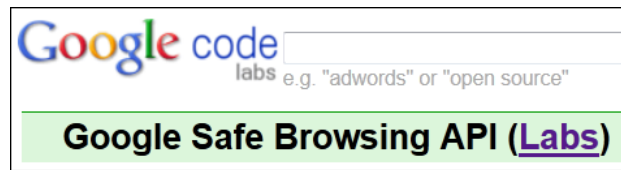
MalwareDiggity

DIGGITY TOOLKIT

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



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



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

Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – WSJ.com – June 2010

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

Massive Malware Hits Media Web Sites

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

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

June 10, 2010

URL: <http://www.informationweek.com/story/showArticle.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 Schools 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.

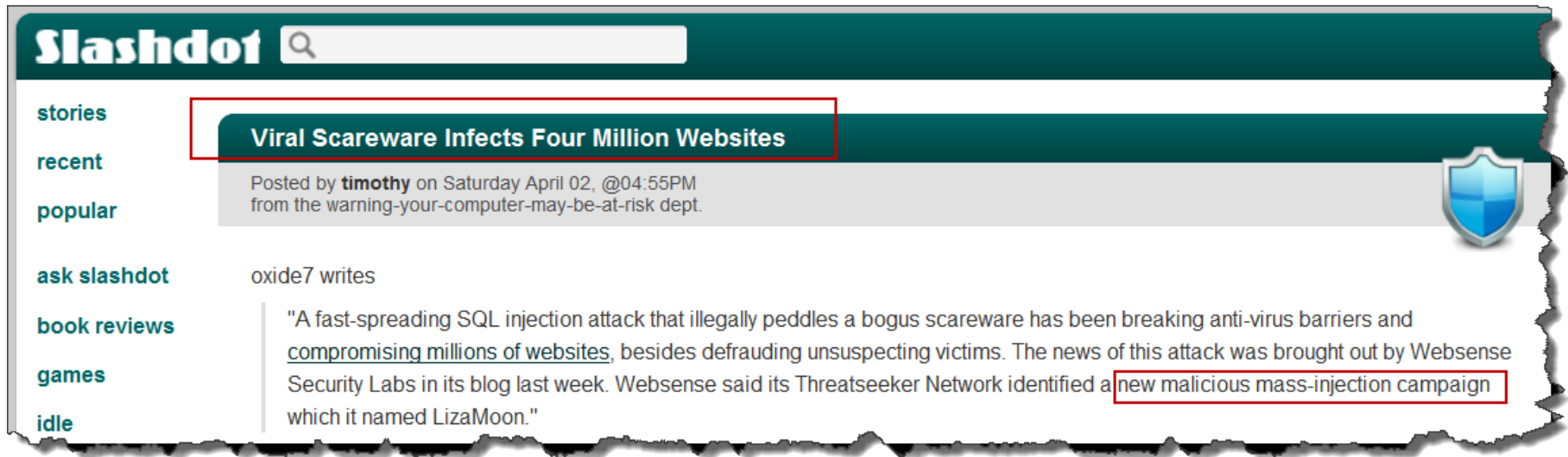
Estimates of the total number of compromised Web sites vary between 7,000 and 114,000, according to security experts. Other compromised sites include servicewomen.org and intijobs.org.

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 quote: '"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
osCommerce store-mar

When researchers from
search results suggeste
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 includes 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, @06:52PM from the high-profile-problems dept. The article text begins with 'Orome1 writes' and '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 across the article reads 'FILED UNDER: INSECURITY COMPLEX | SECURITY Hacked MySQL.com used to serve Windows malware'. Below this, the author is identified as 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 screenshot displays the DIGGITY TOOLKIT interface. On the left, there's a search bar with "www.michoo.co.kr" and a search button. Below it, search results are shown, including a link to "주공행장(酒公行狀) - 예매는 인터파크 - 인터파크 티켓" with a URL containing "interpark.com/ticket/". A callout bubble points to this link, stating "interpark.com does appear to have links to www.michoo.co.kr".

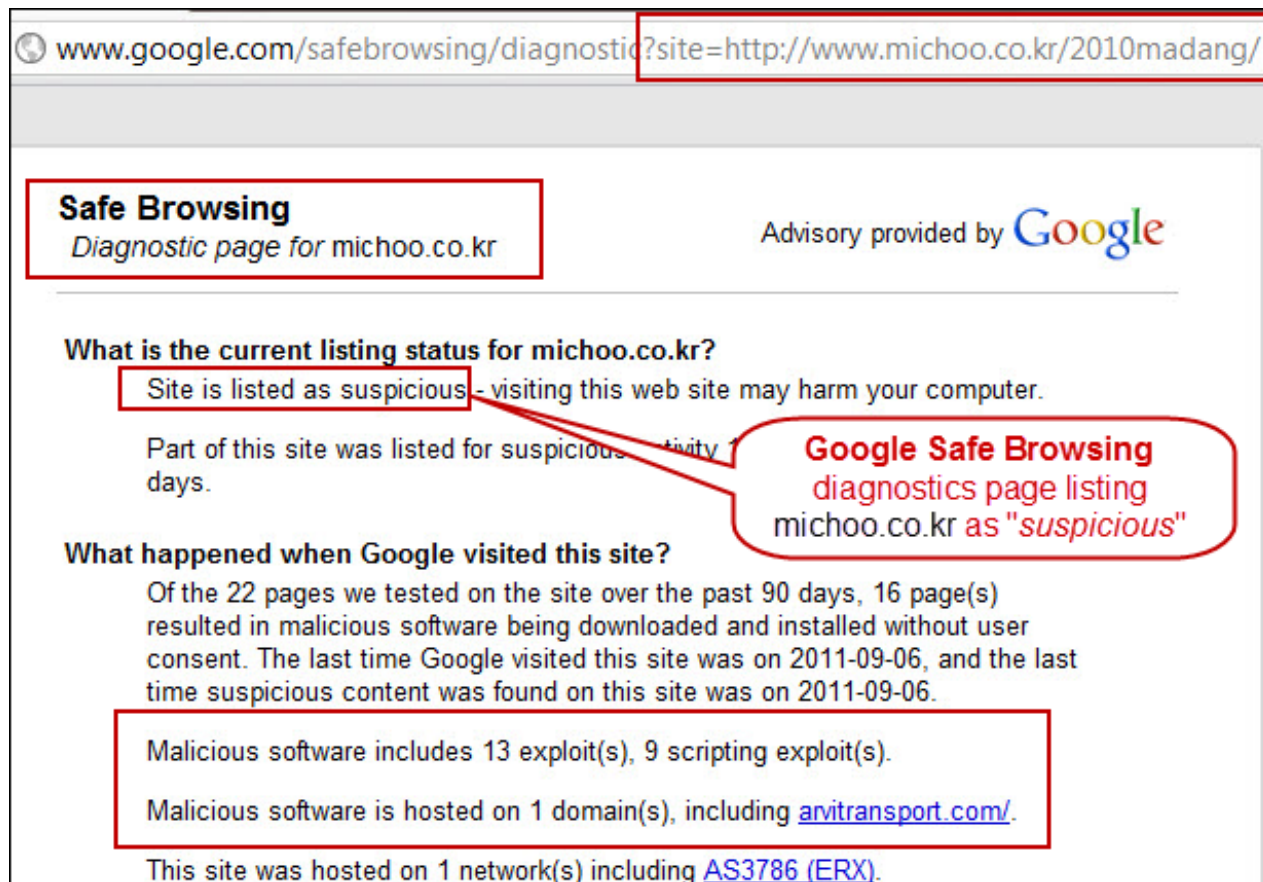
On the right, a table titled "The 1000 most-visited sites on the web" is shown. The table has columns for Rank, Site, Category, and Unique Visitors (users). The 907th site is "interpark.com" with 6,100,000 unique visitors. A callout bubble points to this row, stating "So, the 907th most popular site on the web has URL links to suspected malware sites".

Below the table, a section titled "알립니다" (Notice) contains information about a performance event. A callout bubble points to the URL "www.michoo.co.kr/zhaos", stating "Links to michoo.co.kr".

Rank	Site	Category	Unique Visitors (users)
901	shentime.com	Movies	6,100,000
902	ovi.com	Mobile Apps & Ad	6,100,000
903	zumi.pl	Business & P	6,100,000
904	natwest.com	Banking	6,100,000
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

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](#)

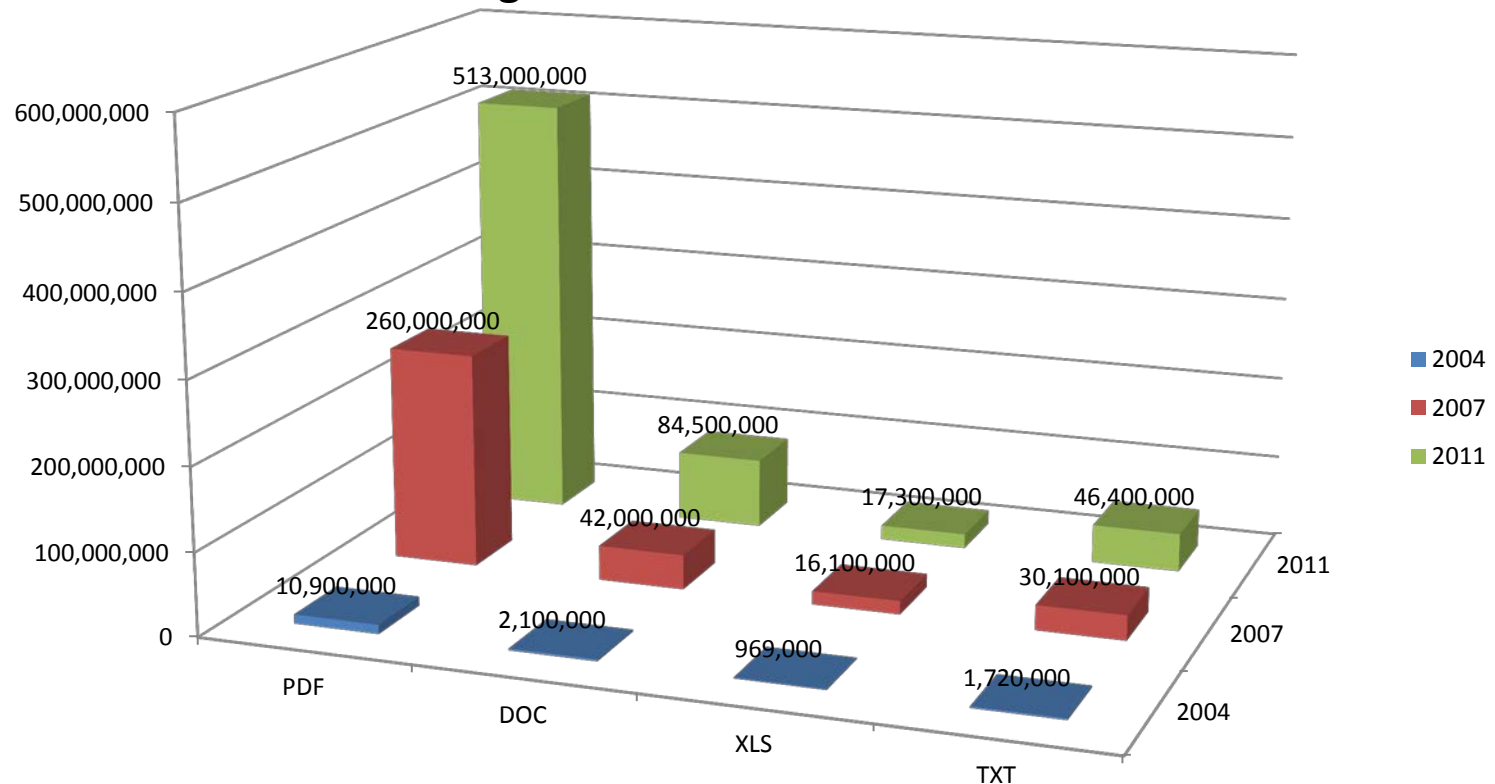
bing
Web
filetype:pdf
Web More
SEARCH HISTORY ALL RESULTS 1-10 of 146,000,000 results · [Advanced](#)



DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR

Google Results for Common Docs



DLP Diggity

DIGGITY TOOLKIT

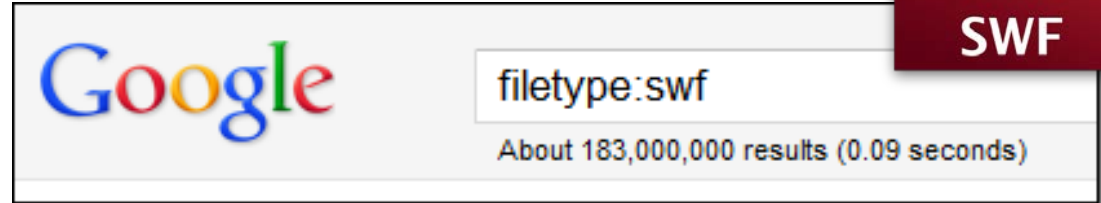
The screenshot displays the DLP Diggity application interface. At the top, there are tabs for different search engines: GoogleDiggity, CodeSearchDiggity, BingDiggity, LinkFromDomainDiggity, **DLPDiggity** (highlighted with a red box), FlashDiggity, and MalwareDiggity. Below the tabs, there are two buttons: "SEARCH" (green) and "Cancel" (grey). A "Scan Directory:" field contains the path "C:\DiggityDownloads" and a "Browse..." button. A table of search results is shown below, with the following columns: Category, Subcategory, Search String, and File. The table contains two rows, with the second row highlighted in yellow:

Category	Subcategory	Search String	File
SSN	Social Security	(ss(n)? social(\:	C:\DiggityDownloads\j...dio.txt
SSN	Social Security	(ss(n)? social(\:	C:\DiggityDownloads\PII...rial.doc

Below the table, there is a "Output" section with a "Selected Result" tab. The output text is as follows:

```
20
21   Jerry,
22   This is Mary. I forgot to include my social security number in those clearance documents I submitted.
23   Would you mind adding it in for me? My SSN is 123-45-6789. Thanks a lot!
24   - Mary
```

A red callout box points to the "Browse..." button and the search results table, containing the text: "Search through downloaded files from GoogleDiggity and BingDiggity for data leaks such as SSNs, credit cards, etc."



NEW GOOGLE HACKING TOOLS

FlashDiggity

Flash Diggity

DIGGITY TOOLKIT

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

The screenshot shows the FlashDiggity application interface. The 'FlashDiggity' tab is selected. The 'Advanced' search mode is active. The search 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 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".

NEW GOOGLE HACKING TOOLS

DEMO

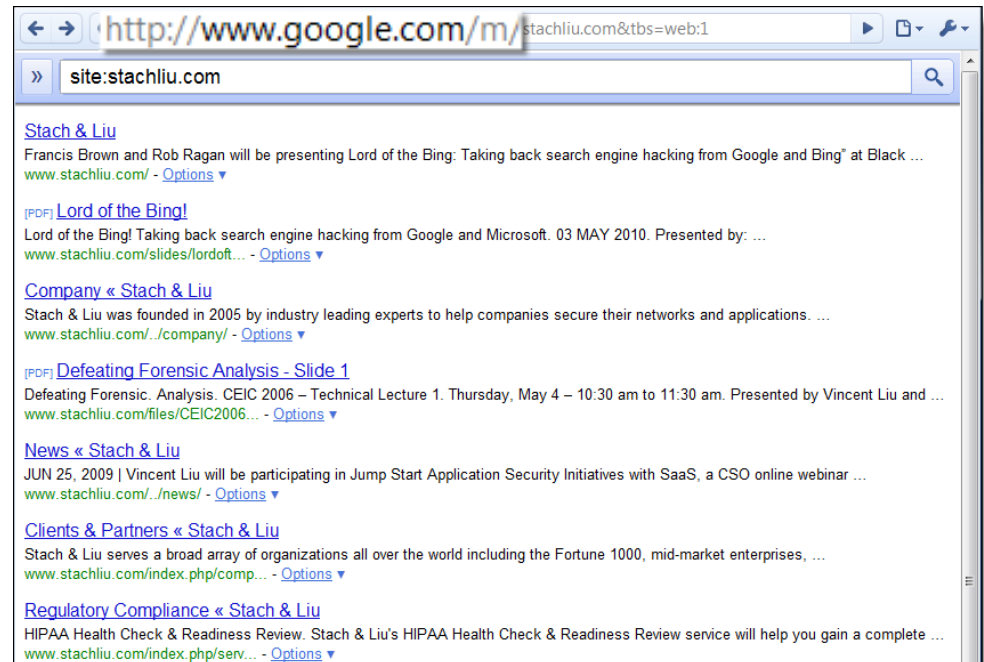
GoogleScrape Diggity

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



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



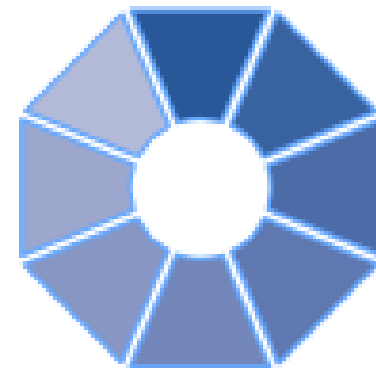


Advanced Defenses

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 feeds on the left and a main feed of items on the right. The main feed title is "Bing: intitle:'Snap Server' intitle:'Home' 'Active Users'". The feed contains several items, each with a star icon and a title. One item is highlighted with a blue background and a red callout box pointing to it. The callout box contains the text "SNAP network attached storage servers exposed".

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

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

- ★ Snap Server WELW-SNAP [Home] - WELW-SNAP • Home
- ★ Snap Server CORESERVER [Home] - CORESERVER • Home
- ★ Snap Server GSTI [Home] - GSTI • Home
- ★ adsphotographer.com - SNAP55373 • Home
- ★ Snap Server SNAP824929 [Home] - SNAP824929 • Home
- ★ Snap Server SAINTSNAP [Home] - SAINTSNAP • Home
- ★ Snap Server DIGITALDATA1 [Home] - BOT - Unavailable: folder does not exist. SHARE1: acesag - For ACES
- ★ Snap Server FTP-SERVER [Home] - Flinn - Flinn OFF-Site Backup: Home - Folder for network shares/drive r

Snap Server FTP-SERVER [Home]

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

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

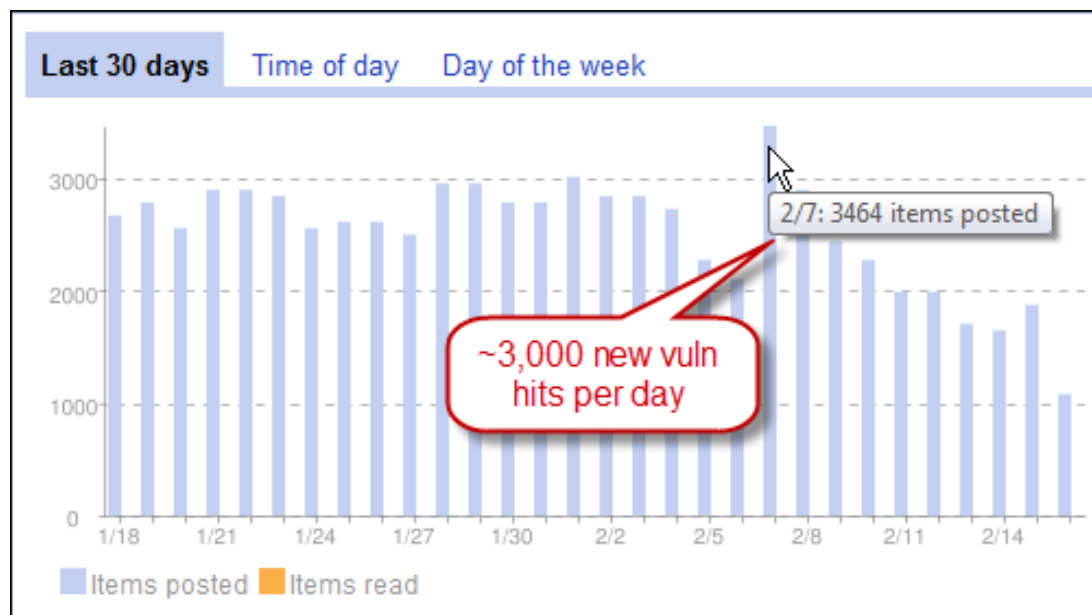
- ★ Snap Server XRAY7 [Home] - XRAY7 • Home

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

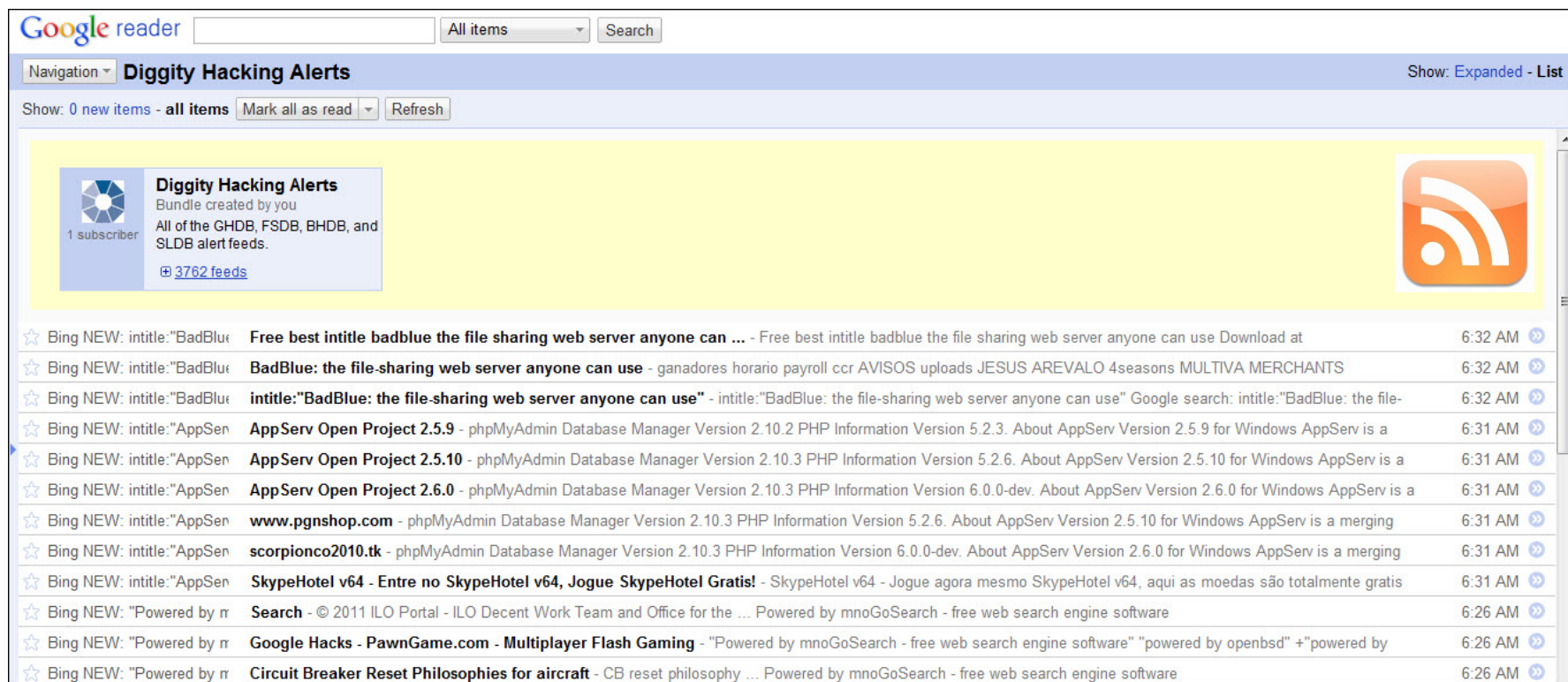
via Google Alerts - "phone * * * "address * * "e-mail" intitle:"curriculum vitae" by on 9/11/11

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 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 versions and other security-related topics.

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](#)
- 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"](#)

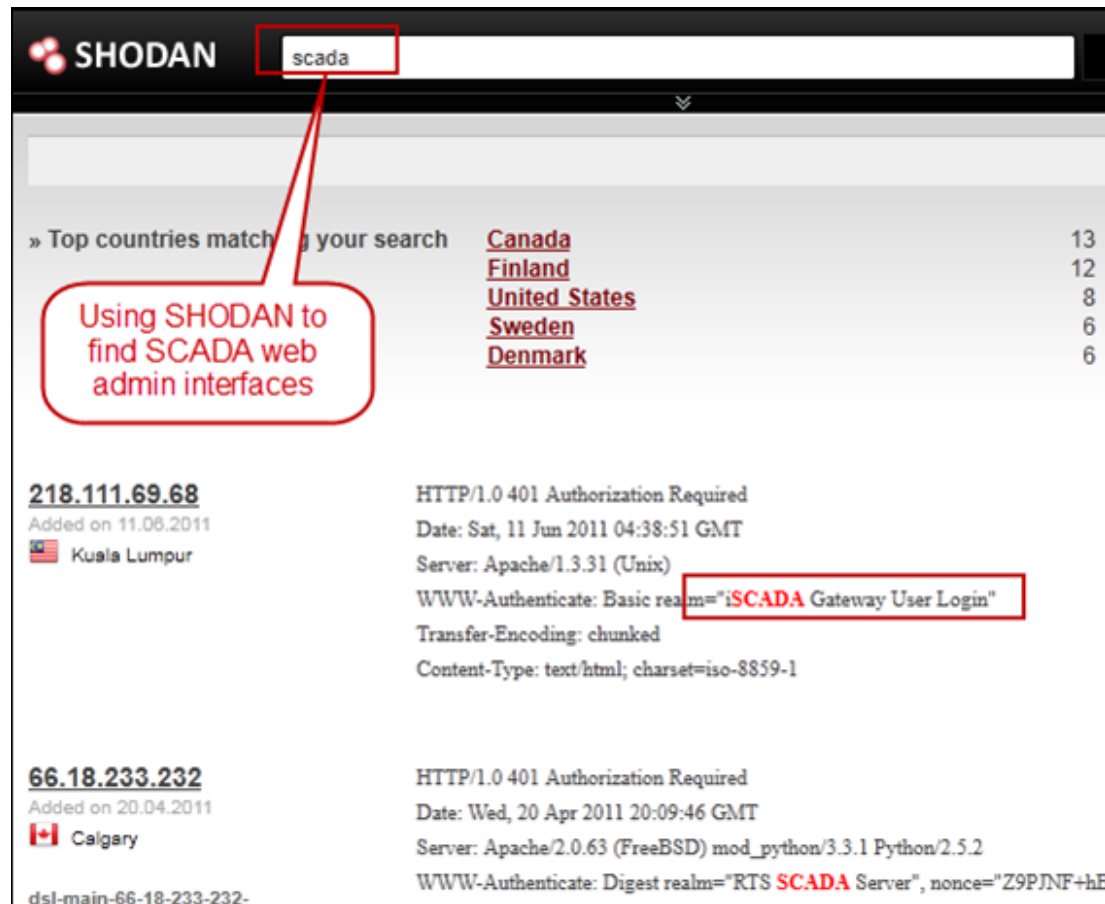


ADVANCED DEFENSE TOOLS

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 callout box points to the search bar with the text 'Using SHODAN to find SCADA web admin interfaces'. Below the search bar, a table lists top countries matching the search:

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

Two search results are shown below:

218.111.69.68
Added on 11.06.2011
Kuala Lumpur

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

66.18.233.232
Added on 20.04.2011
Calgary

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

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

SHODAN Alerts



SHODAN RSS FEEDS

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 screenshot displays the Alerts Diggity application interface. The main window has a menu bar with 'File' and 'Help', and a tabbed interface with 'All Alerts', 'Subscribed Feeds', 'Subscribed Domains', and 'Schedule'. A search bar is present with an 'Add' button. Below the search bar, the domain 'milblogging.com' is listed. A secondary window is overlaid on top, showing a table of alerts with columns for 'URL' and 'Publish Date'. The table contains several entries with blue hyperlinks and timestamps. 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

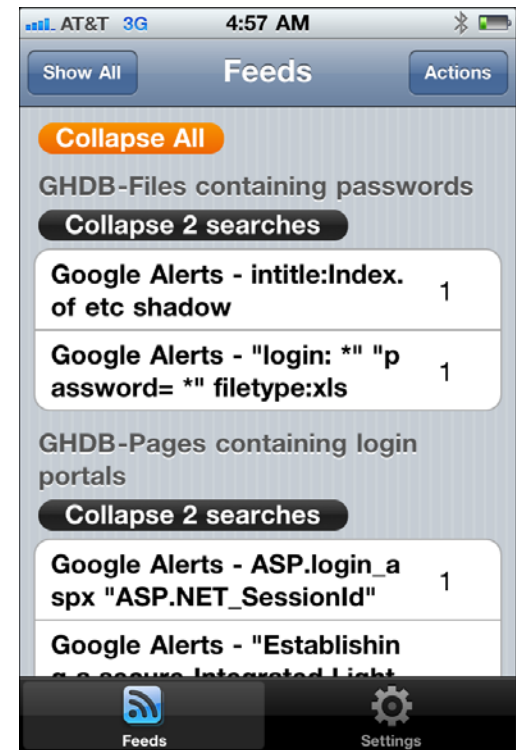
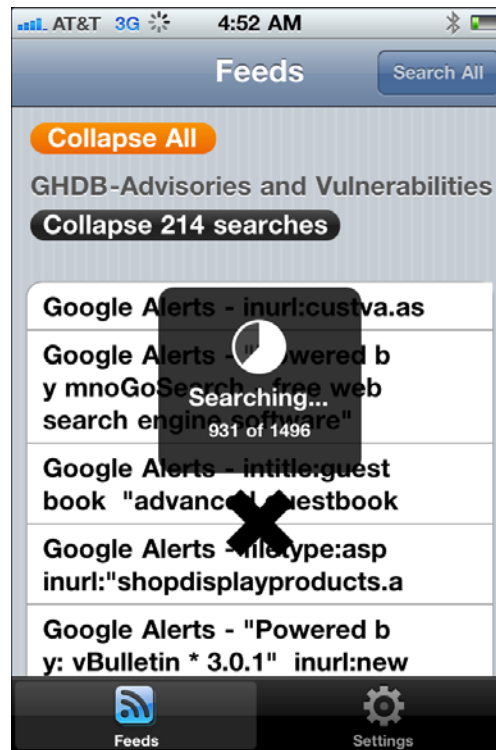
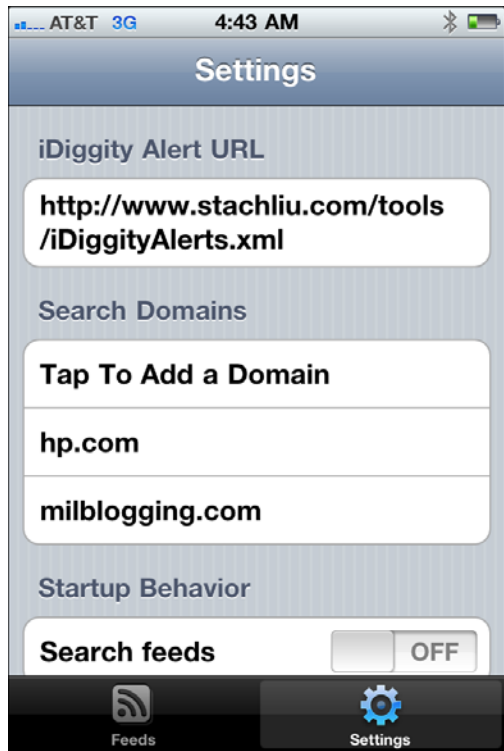


ADVANCED DEFENSE TOOLS

iDiggity Alerts

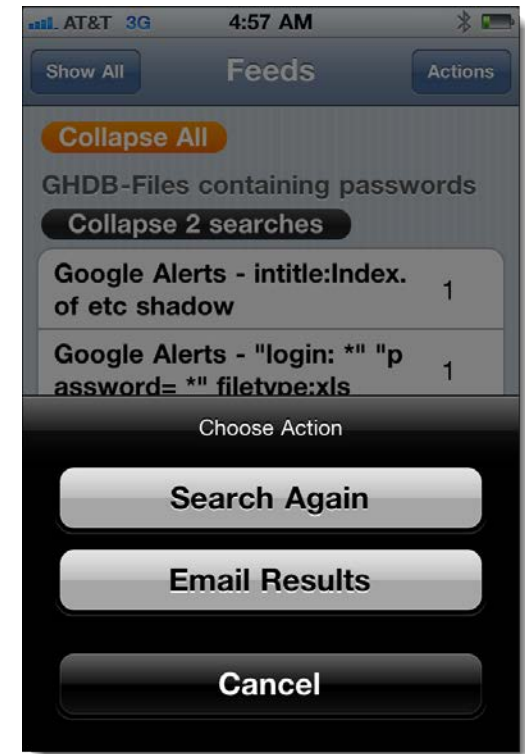
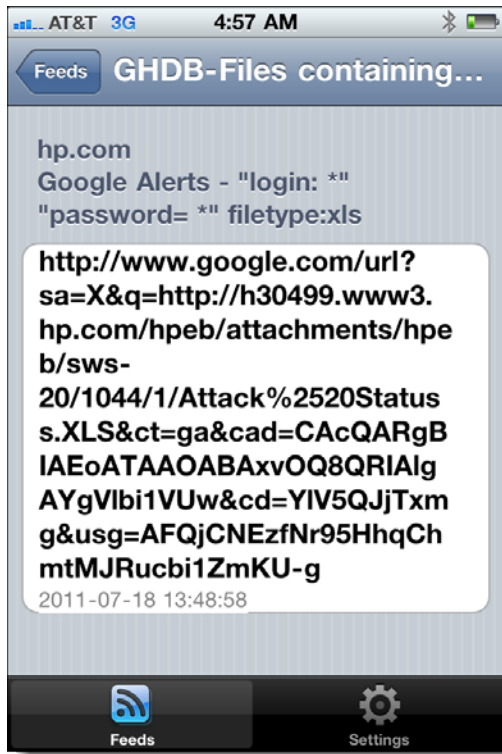
iDiggity Alerts

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 - 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

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.



Special Thanks

Oscar "The Bull" Salazar
Brad "BeSickWittlt" Sickles
Nick "King Luscious" Harbin
Prajakta "The Flasher" Jagdale
Ruihai "Ninja" Fang
Jason "Blk-majik" Lash



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

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



Thank You

Stach & Liu Google Hacking Diggity Project info:

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