



# Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing

16 FEB 2011 – HackCon 2011 – Oslo, Norway



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
- Advanced Defenses
  - Google/Bing Hacking Alerts
- Other OSINT Attack Techniques
- Future Directions



# Goals

DROP KNOWLEDGE ON YOU

- *To improve* Google Hacking
  - Attacks and defenses
  - Advanced tools and techniques
- *To think differently* about exposures in publicly available sources
- To blow your mind!



# Introduction/ Background

GETTING UP TO SPEED





# Open Source Intelligence

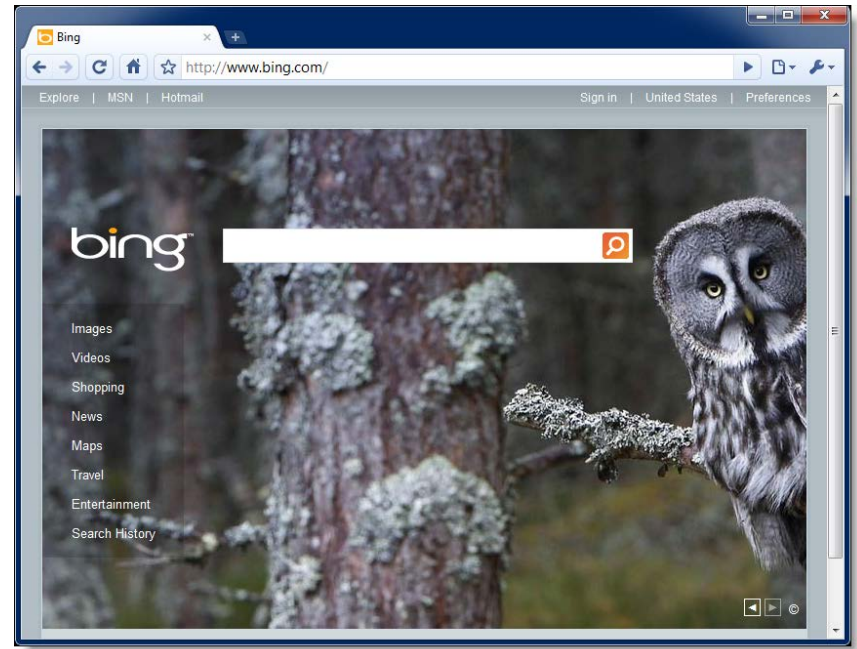
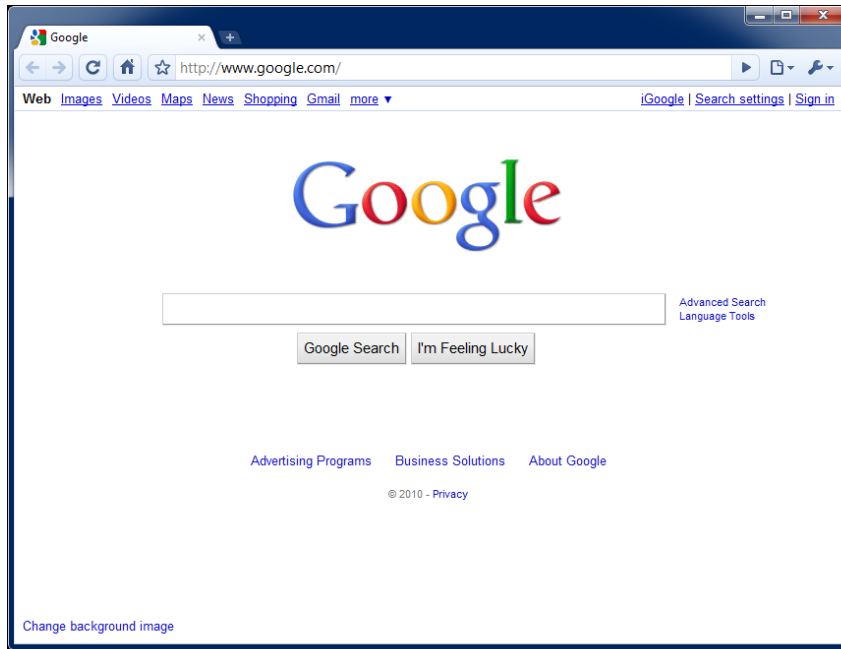
SEARCHING PUBLIC SOURCES

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)



# Attack Targets

GOOGLE HACKING DATABASE

## Old School Examples

- Error Messages
  - `filetype:asp + "[ODBC SQL"`
  - `"Warning: mysql_query()" "invalid query"`
- Files containing passwords
  - `inurl:passlist.txt`



# Quick History

## GOOGLE HACKING RECAP

Dates	Event
2004	Google Hacking Database (GHDB) begins
May 2004	Foundstone SiteDigger v1 released
2005	Google Hacking v1 released by Johnny Long
Jan. 2005	Foundstone SiteDigger v2 released
Feb. 13, 2005	Google Hack HoneyPot first release
Jan. 10, 2005	MSNPawn v1.0 released
Dec. 5, 2006	Google stops issuing Google SOAP API keys
...	...



# Quick History

## GOOGLE HACKING RECAP

Dates	Event
Mar. 2007	Bing disables inurl: link: and linkdomain:
Nov. 2, 2007	Google Hacking v2 released
Mar. 2008	cDc Goolag - gui tool released
Sept. 7, 2009	Google shuts down SOAP Search API
Nov. 2009	Binging tool released
Dec. 1, 2009	FoundStone SiteDigger v 3.0 released
2010	Googlag.org disappears



# Advanced Attacks

WHAT YOU SHOULD KNOW






# New Toolkit

STACH & LIU TOOLS




## Google Diggity

- Uses Google AJAX API
  - Not blocked by Google bot detection
  - Does not violate Terms of Service
-  • Can leverage **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 Toolkit



GOOGLEDIGGITY

Search Diggity

File Options Help

GoogleDiggity BingDiggity

Advanced Simple

SCAN Cancel

Sites/Domains  Add

stachliu.com [Remove]

Google Custom Search ID: [Create](#)

Import Clear

Category	Subcategory	Search String	Page Title	URL	Cache URL
Custom	Custom	site:stachliu.c	Stach & Li	<a href="http://www.stachliu.com/">http://www.stachliu.com/</a>	<a href="http://www.google.com/search?">http://www.google.com/search?</a>
Custom	Custom	site:stachliu.c	Lord of the Bin	<a href="http://www.stachliu.com/slides/">http://www.stachliu.com/slides/</a>	<a href="http://www.google.com/search?">http://www.google.com/search?</a>
Custom	Custom	site:stachliu.c	APPLicATIOn So	<a href="http://www.stachliu.com/brochu">http://www.stachliu.com/brochu</a>	<a href="http://www.google.com/search?">http://www.google.com/search?</a>
Custom	Custom	site:stachliu.c	Lord of the Bin	<a href="http://www.stachliu.com/slides/">http://www.stachliu.com/slides/</a>	<a href="http://www.google.com/search?">http://www.google.com/search?</a>
Custom	Custom	site:stachliu.c	News « Stach 8	<a href="http://www.stachliu.com/index.p">http://www.stachliu.com/index.p</a>	<a href="http://www.google.com/search?">http://www.google.com/search?</a>
Custom	Custom	site:stachliu.c	Secure Web AP	<a href="http://www.stachliu.com/brochu">http://www.stachliu.com/brochu</a>	<a href="http://www.google.com/search?">http://www.google.com/search?</a>

Output Selected Result

```
Advanced Scan started. [9/13/2010 10:47:40 PM]
Search Safety: Moderate.
Unlimited results per query.
Not using Custom Search ID.
Found 41 result(s) for query: " " [stachliu.com].
Total Results: 41.
Scan Complete. [9/13/2010 10:47:41 PM]
```

Google Status: Ready Bing Status: Ready

# New Toolkit



## BINGDIGGITY

The screenshot shows the Search Diggity application window. The interface includes a menu bar (File, Options, Help), a tabbed interface with 'GoogleDiggity' and 'BingDiggity', and a main workspace. The workspace has a 'Query Appender' on the left, a 'SCAN' button, and a 'Bing 2.0 API Key' field. Below the API key is a table of search results. The 'Output' section at the bottom shows the scan results for the selected IP.

Category	Subcategory	Search String	Page Title	URL
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	Google Hacking Diggity Project	<a href="http://www.stachliu.com/index.php/resources/tools/goo">http://www.stachliu.com/index.php/resources/tools/goo</a>
Custom	Custom	ip:98.129.200.37	Tools « Stach & Liu	<a href="http://www.stachliu.com/index.php/resources/tools/">http://www.stachliu.com/index.php/resources/tools/</a>
Custom	Custom	ip:98.129.200.37	Training « Stach & Liu	<a href="http://www.stachliu.com/index.php/training/">http://www.stachliu.com/index.php/training/</a>
Custom	Custom	ip:98.129.200.37	Webinars « Stach & Liu	<a href="http://www.stachliu.com/index.php/resources/webinars/">http://www.stachliu.com/index.php/resources/webinars/</a>
Custom	Custom	ip:98.129.200.37	Management & Advisory Board	<a href="http://www.stachliu.com/index.php/company/managem">http://www.stachliu.com/index.php/company/managem</a>
Custom	Custom	ip:98.129.200.37	Clients & Partners « Stach & Liu	<a href="http://www.stachliu.com/index.php/company/clients-par">http://www.stachliu.com/index.php/company/clients-par</a>

**Output Selected Result**

```
Advanced Scan started. [9/13/2010 10:37:10 PM]
Adult Option: Moderate
Maximum 200 results per query.
Using Custom Search ID: 2136A2334B9A25C0C8B7C73B899461F9367F8FD32.
Found 32 result(s) for query: " " [98.129.200.37].
Total Results: 32.
Scan Complete. [9/13/2010 10:37:12 PM]
```





# New Toolkit

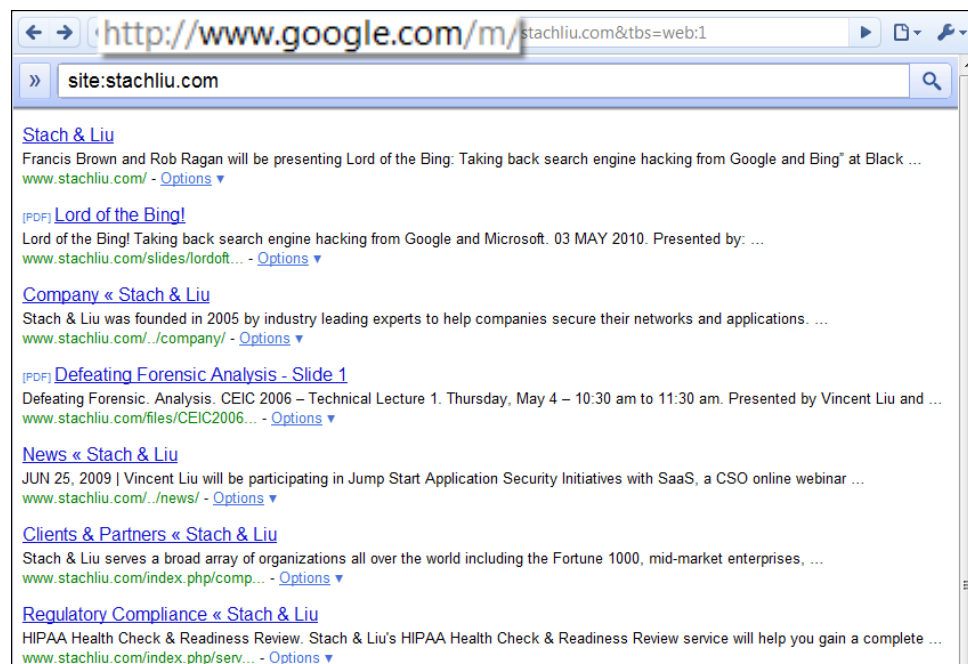


STACH & LIU TOOLS

## 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 Hack Databases

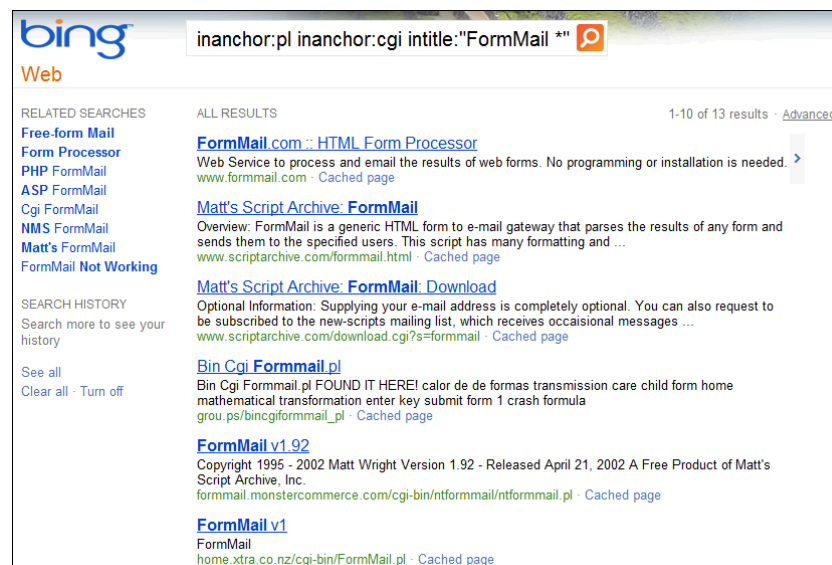
## ATTACK QUERIES

### 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"`



# BaiduDiggity

CHINA SEARCH ENGINE



- COMING SOON!

**COMING SOON**



# Google Custom Search

NORWAY SEARCH ENGINE

A screenshot of a web browser displaying a Google Custom Search page. The browser's address bar shows the URL `www.google.com/cse/home?cx=013931441997728635234:w6kfuwsuxj4`, which is highlighted with a red box and a callout bubble labeled "Google CSE ID". The page title is "Norway - Google Custom Search". Below the title is a search input field containing the text "test" and a "Search" button. Underneath is a section titled "Search engine details" which includes the text "searches sites including: \*.no/\*" (highlighted with a red box and a callout bubble labeled "Results filtered for \*.no - Norway sites."), "Last updated: February 16, 2011", and several links: "Add this search engine to your Google homepage", "Add this search engine to your blog or page", and "Create your own Custom Search Engine". At the bottom, there is a copyright notice: "©2008 Google - Google Home - About Google - Privacy Policy".



NEW GOOGLE HACKING TOOLS

**DEMO**



# 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



# 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



# Advanced Defenses

PROTECT YO NECK







# Existing Defenses

"HACK YOURSELF"



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





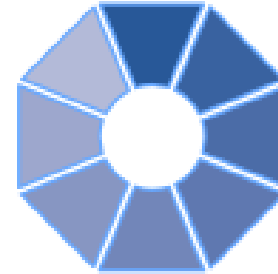
# Advanced Defenses

NEW HOT SIZZLE



Stach & Liu now proudly presents:

- Google Hacking Alerts
- Bing Hacking Alerts



# 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

stachliu0@gmail.com | [Settings](#) | [FAQ](#) | [Sign out](#)

**Google alerts** Manage your Alerts

GHDB regexes made into Google Alerts

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

Switch to [text emails](#) | [Export alerts](#)

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

# Google Hacking Alerts

ADVANCED DEFENSES



Google reader

All items (1000+)

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 - "acce..." (45)
- Google Alerts - "An i..." (1)
- Google Alerts - "ASP..." (5)

Google Alerts - "mysql error with query"

Show: 11 new items - all items

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.cmail as userid, c.cemail as email, ...  
[www.mi6.co.uk/mi6.php3/news/index.php?itemid...t...](#)

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

Several thousand GHDB/FSDDB vuln alerts generated each day

# Bing Hacking Alerts

ADVANCED DEFENSES



## Bing Hacking Alerts

- Bing searches with regexs from BHDB
- Leverage `&format=rss` directive to turn into update feeds
- Real-time vuln updates to **>900 Bing hack queries** via RSS

The screenshot shows a Google Reader interface with a search query: `Bing: intitle:"Snap Server" intitle:"Home" "Active Users" >>`. The feed displays several items, including:

- 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 publicat
- Snap Server FTP-SERVER [Home] - Flinn - Flinn OFF-Site Backup: Home - Folder for network shares/drive mapping:

The item "Snap Server FTP-SERVER [Home]" is expanded, showing details: "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".

A red callout box points to the feed with the text: "SNAP network attached storage servers exposed".



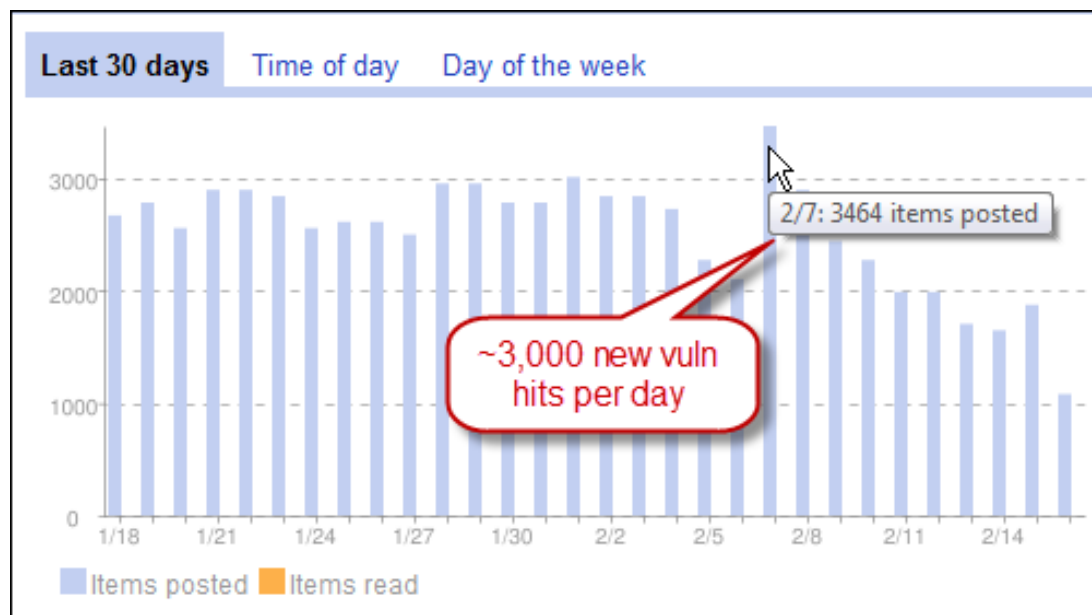
# Bing/Google Alerts

LIVE VULNERABILITY FEEDS



World's Largest Live Vulnerability Repository

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



# Bing/Google Alerts

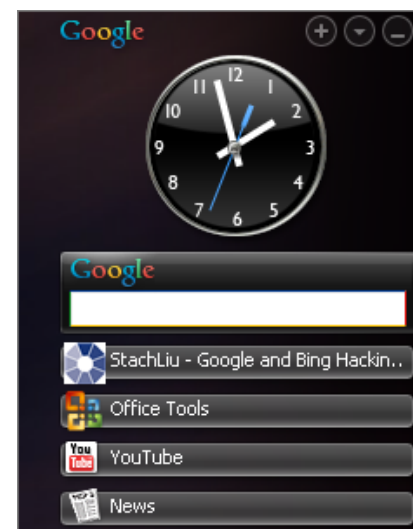
THICK CLIENTS TOOLS



## 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:
  - Google Desktop Gadget
    - OS independent client
  - Droid app (coming soon)

**COMING SOON**



ADVANCED DEFENSE TOOLS

DEMO



# New Defenses

"GOOGLE/BING HACK ALERTS"



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





# Other OSINT Attacks

WHAT YOU SHOULD KNOW



# Google Apps Explosion

SO MANY APPLICATIONS TO ABUSE

Google alerts

Google reader

Google™  
PhoneBook

Google custom search

Google™  
trends

Google buzz 

Google™  
code search labs

Google™ code

Google health

Google calendar

Google news

Google™ public data explorer  
labs

Google docs

Google™ Insights for Search  
beta

Google™ wave  
preview 

Google blogs

Google maps

Google groups



# Google Code Search

## VULNS IN OPEN SOURCE CODE

- Regex search for vulnerabilities in public code
- 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 are displayed under the heading "Code". A red callout box points to the search query, stating "reply\_id is SQL injectable querystring parameter". 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>×çôâ£°ô»óÐ,ÁîÃôÃ×÷ôß°í¹ùÀíô±²ÁÄÜí±³ôâ,ôìù×ó."

57: strSql = "SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çôâ£°ô»óÐ,ÁîÃôÃ×÷ôß°í¹ùÀíô±²ÁÄÜí±³ôâ,ôìù×ó."
```

The code snippet shows a SQL injection vulnerability where the `reply_id` parameter is used in a querystring parameter without proper sanitization. The search results also show the source URL: [www.cnarts.net/eweb/download/software/bbs/tradeforum.zip](http://www.cnarts.net/eweb/download/software/bbs/tradeforum.zip) - Unknown - ASP - [More from tradeforum.zip »](#)



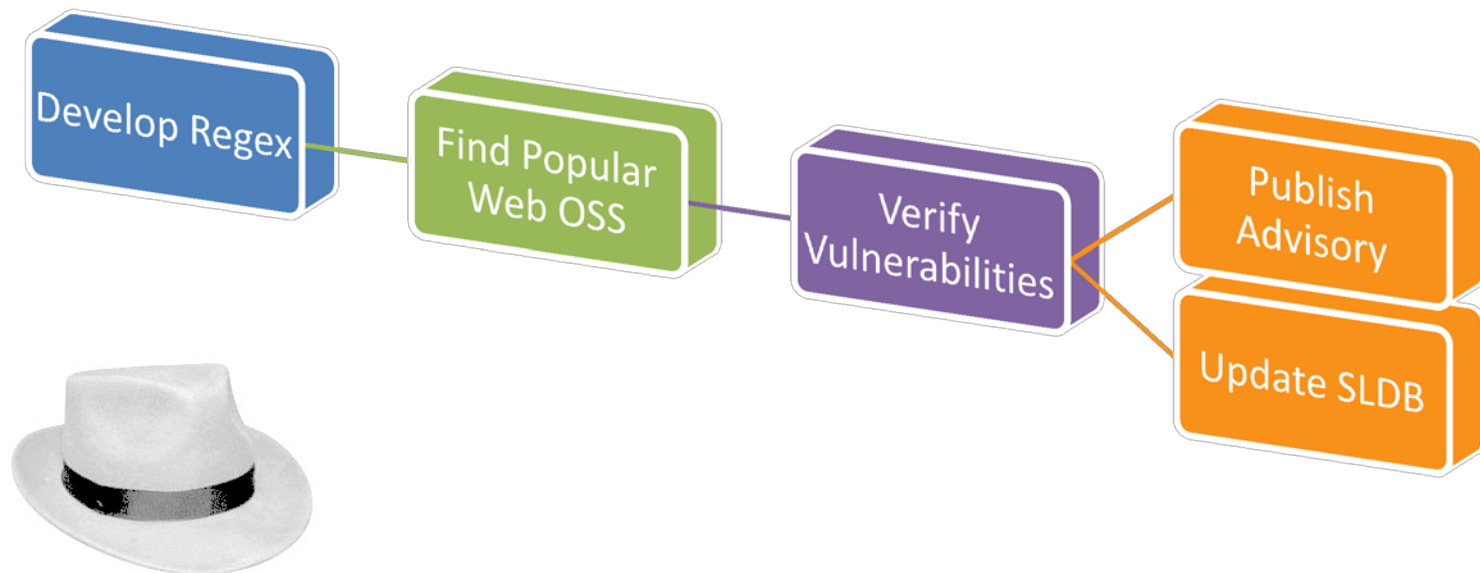
GOOGLE CODE SEARCH HACKING  
**DEMO**



# Google Code Search



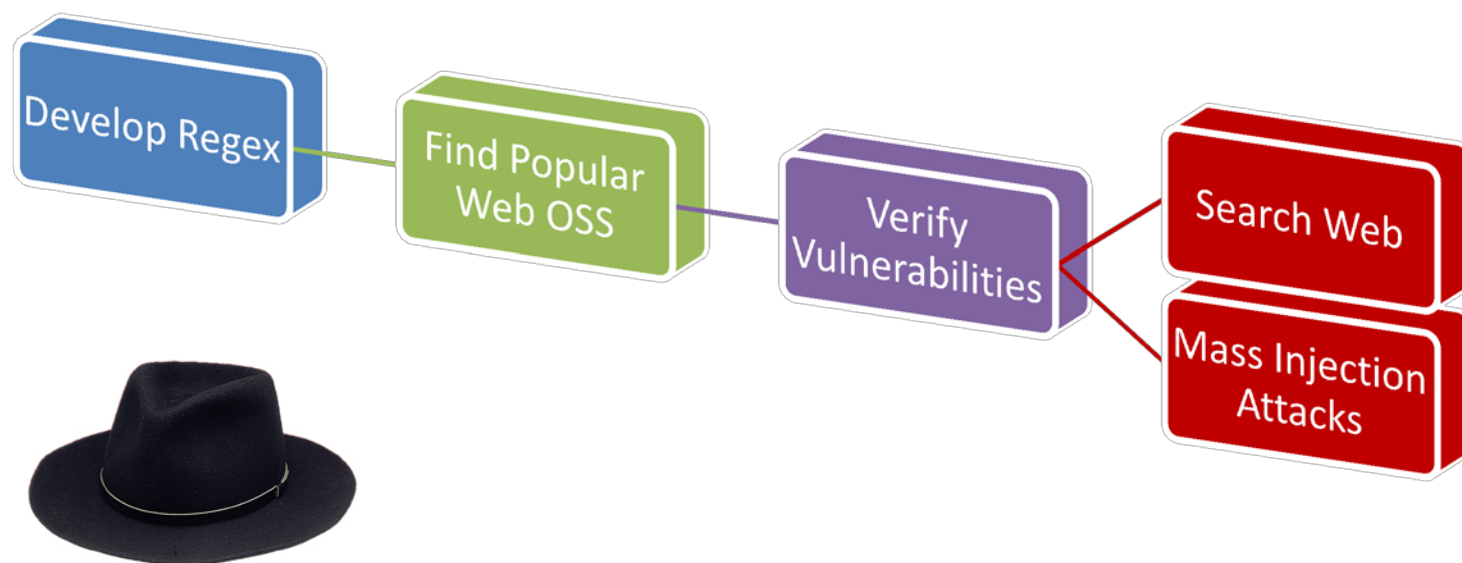
VULNS IN OPEN SOURCE CODE





# Google Code Search

VULNS IN OPEN SOURCE CODE



# Black Hat SEO



## SEARCH ENGINE OPTIMIZATION

- Use popular search topics du jour
- Pollute results with links to badware
- Increase chances of a successful attack





# Google Trends



## BLACK HAT SEO RECON

Google Insights for Search beta [Help](#) | [Sign in](#) | [Download as CSV](#) | [English \(US\)](#)

**Compare by**

- Search terms
- Locations
- Time Ranges

**Search terms**

Tip: Use a comma as shorthand to add comparison items. (tennis, squash)

- All search terms

**Filter**

Web Search

United States | All subregions | All metros

2004 - present

All Categories

**Top Google searches over past 6 years**

**Web Search Interest**

United States, 2004 - present

**Search terms**

**Top searches**

1. [lyrics](#)
2. [you](#)
3. [yahoo](#)

**Lada Gaga, Rihanna lyrics sites used to foist Java exploit**

Dan Kaplan April 14, 2010

PRINT | EMAIL | REPRINT | PERMISSIONS | FONT SIZE: A | A | A

As expected, virus writers now are actively exploiting a zero-day Sun  
vulnerable info routers through drive

RELATED ARTICLES

**Fake lyrics web sites setup to appear in Google search results, infect you with malware upon clicking**

**Top Google searches over past 6 years**

# Malware Ads



## BLACK HAT ADS

**bing** adobe reader

Web Web News

RELATED SEARCHES  
Adobe Reader 0Day  
Adobe Reader Free Download  
Adobe Reader 7 Free Download  
Adobe Acrobat Reader 8.1  
Adobe Reader Plugin  
Adobe Reader 10  
Free Adobe Reader for XP  
Java

SEARCH HISTORY  
adobe reader  
See all  
Clear all · Turn off

ALL RESULTS 1-10 of 54,900,000 results · [Advanced](#)

**Reader 9.0 -Official Site** Sponsored sites  
[www.PDF-Format.com](http://www.PDF-Format.com) · Open, Create & Edit PDF Files! Official Site (Recommended Download)

**Adobe Acrobat 9 Download**  
[AdobeAcrobat.PDF-Software.com](http://AdobeAcrobat.PDF-Software.com) · Ultra Fast Acrobat Download - Latest Version 100% Guaranteed

**Adobe Reader Download**  
[AdobeProReader10.com/Free](http://AdobeProReader10.com/Free) · New **Adobe Reader** Official Version. 100% Support. Free Download!

**Adobe Acrobat 9.3 Version**  
[www.PDF-9-D0wnload.com](http://www.PDF-9-D0wnload.com) · Download **Adobe** PDF Latest Version Ultra Fast 100% Guaranteed!

**Adobe - Adobe Reader**  
Download **Adobe Reader** to view, print and collaborate on PDF files.  
[get.adobe.com/reader](http://get.adobe.com/reader) · Cached page

Get Flash Player      Adobe - Adobe Air  
Adobe - Adobe Reader      Adobe - Adobe Reader Accessibility  
Show more results from [get.adobe.com](http://get.adobe.com)



# Defenses

## BLACKHAT SEO DEFENSES

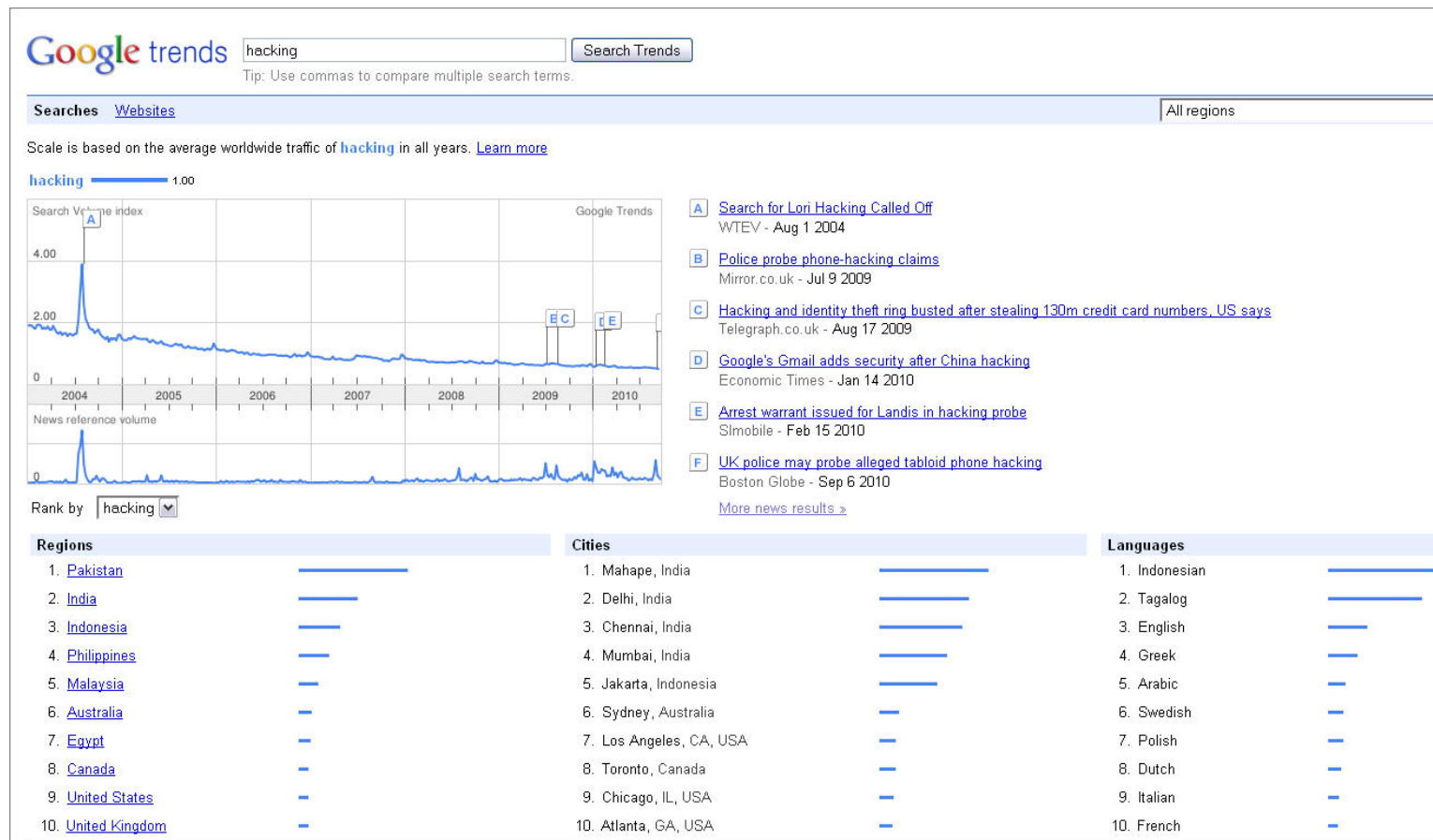
- Malware Warning Filters
  - Google Safe Browsing
  - Microsoft SmartScreen Filter
  - Yahoo Search Scan
- Sandbox Software
  - Sandboxie ([sandboxie.com](http://sandboxie.com))
  - Dell KACE - Secure Browser
  - Office 2010 (Protected Mode)
  - Adobe Reader Sandbox (Protected Mode)
- No-script and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



# Google Trends



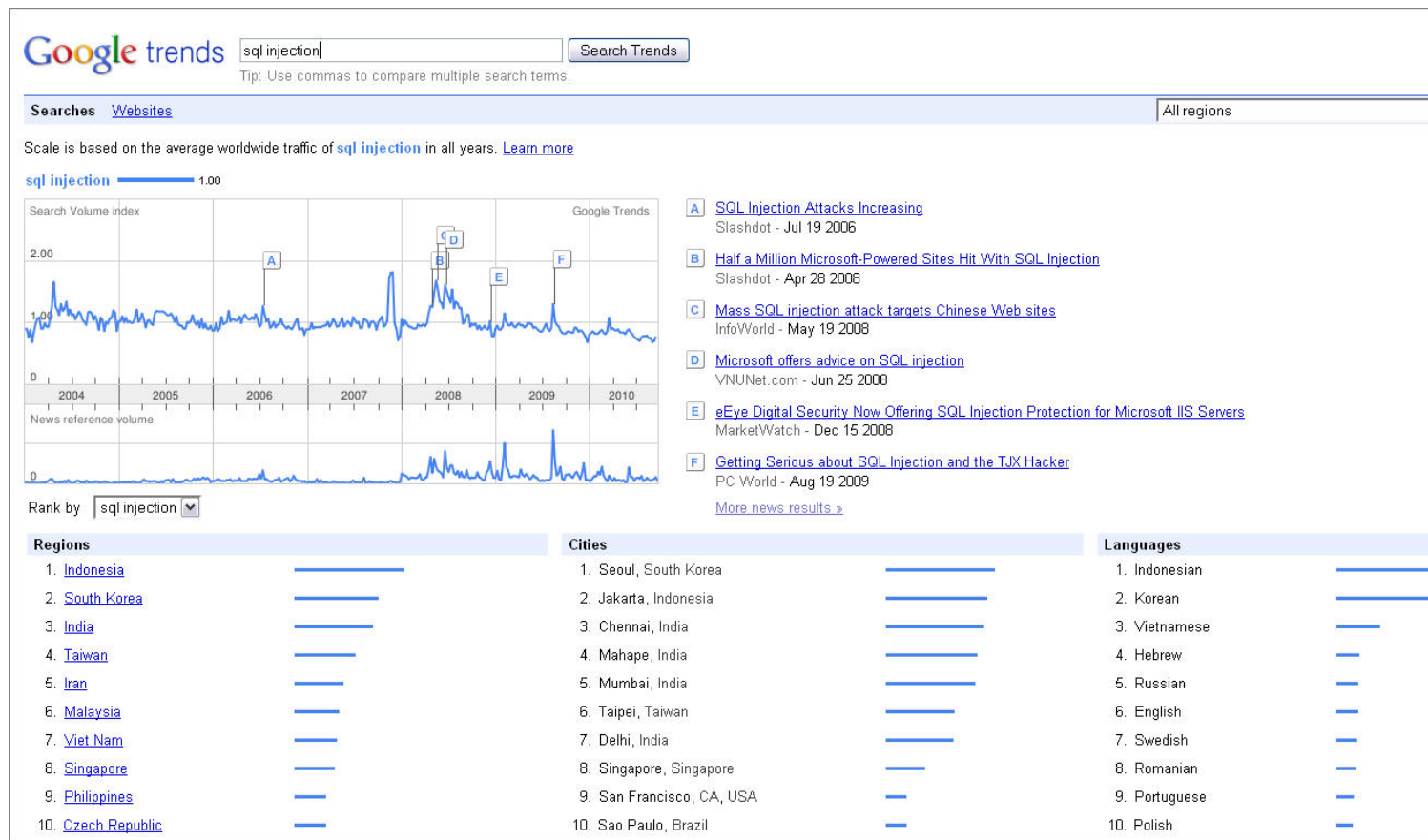
## OTHER INTERESTING



# Google Trends



## OTHER INTERESTING



# Google Trends



## PREDICTING ELECTIONS

**Slashdot** NEWS FOR NERDS. STUFF THAT MATTERS.

▶ **Stories** [Recent](#) [Popular](#) [Search](#)

**Technology: Predicting Election Results With Google**

Posted by samzenpus on Sunday October 31, @11:38AM  
from the future-search dept.

destinyland writes

"Google announced they've searched its 'Insights for Search' tool, which co 'Looking at the most popular searches their official blog reported, adding, 'w foreclosures, as well as immigration a some candidate's predicted vote total error for other candidates. 'Oddly en contest [in Florida], where the break

The Official **Google** Blog | Insights from Googlers into our products, technology, and the Google culture.

### Searching your way to the ballot box

10/27/2010 02:54:00 PM

With less than a week left until the U.S. 2010 midterm elections, interest is heating up around the country—in polling places, close races and hot political issues. We thought we'd peek into the search data to see what we could find about what kinds of info people are looking for as they get ready to go to the ballot box next Tuesday. We used a combination of [Insights for Search](#) and internal tools to dis...



# Mass Injection Attacks

MALWARE GONE WILD

## Malware Distribution Woes

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

### Massive Malware Hits Media Web Sites

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

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

June 10, 2010

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=225600247>

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

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



From: [www.itworld.com](http://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](http://servicewomen.org) and [intijobs.org](http://intijobs.org).

# Future Direction

PREDICTIONS







# Predictions



## FUTURE DIRECTIONS

### Data Explosion

- More data indexed, searchable
- Real-time, streaming updates
- Faster, more robust search interfaces

### Google Involvement

- Filtering of search results
- Better GH detection and tool blocking

### Renewed Tool Dev

- Google Ajax API based
- Bing/Yahoo/other engines
  - Search engine aggregators
- Google Code and Other Open Source Repositories
  - MS CodePlex, SourceForge, ...
- More automation in tools
  - Real-time detection and exploitation
  - Google worms

# Real-time Updates

FUTURE DIRECTIONS



Google obama Search [Advanced Search](#)

Web > Updates [Hide options](#) Results 1 - 10 of about 4 for obama. (0.58 seconds)

[All results](#)  
[Images](#)  
[Videos](#)  
[News](#)  
[Blogs](#)  
**Updates**  
[Books](#)  
[Discussions](#)

[Any time](#)  
Latest  
[Reset options](#)

2010 > April > 20 - 21

7am 1pm 7pm 1am

New results will appear below as they become available. [Pause](#)

Helen Thomas on her one question for **Obama**  
[YouTube - Helen Thomas on her one question for Obama](#) - youtube.com

[Idanah](#) - **Twitter** - 1 minute ago

**Obama** falters on immigration reform promises  
#usnews #news  
reform, Obama's priorities shift -  
latimes.com - latimes.com

[filterednews](#) - **Twitter** - 1 minute ago

**Top links**

[Obama to discuss Supreme Court pick with party leaders - CNN.com](#)  
President **Obama** is expected to meet with key Republican and Democratic leaders Wednesday to discuss a replacement for retiring Supreme ...  
<http://www.cnn.com/2010/.../jobama.../index.html>  
[All mentions >](#)

[Obama Supreme Court Pick: President Talking With Possible High ...](#)  
WASHINGTON — Pushing forward with one of his most consequential decisions, President Barack **Obama** has begun informal talks with ...  
<http://www.huffingtonpost.com/.../jobama-supreme->

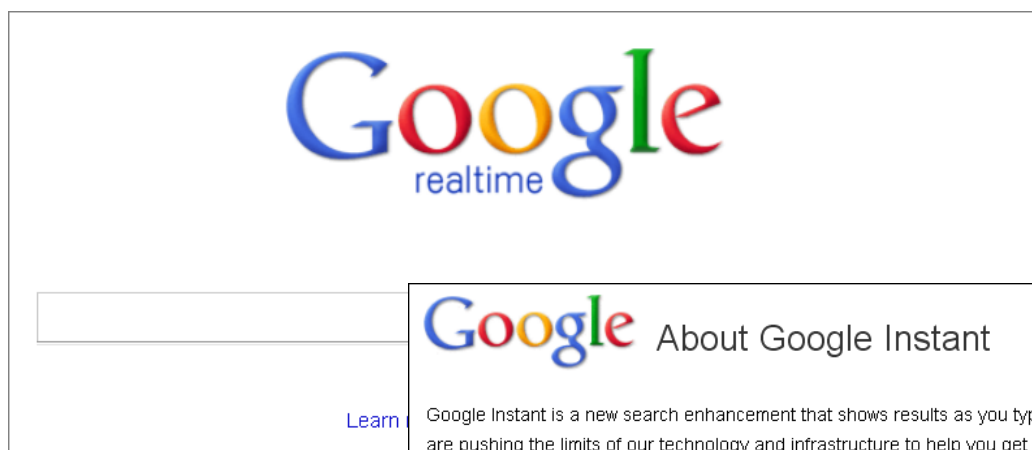
Real-time updates!



# Predictions Update



GOOGLE REALTIME/INSTANT



[Learn](#)

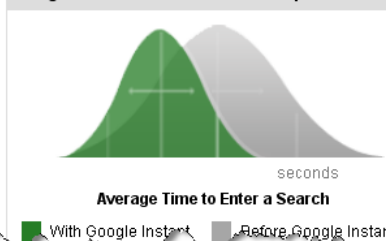
## Google About Google Instant

Google Instant is a new search enhancement that shows results as you type. We are pushing the limits of our technology and infrastructure to help you get better search results, faster. Our key technical insight was that people type slowly, but read quickly, typically taking 300 milliseconds between keystrokes, but only 30 milliseconds (a tenth of the time!) to glance at another part of the page. This means that you can scan a results page while you type.

The most obvious change is that you get to the right content much faster than before because you don't have to finish typing your full search term, or even press "search." Another shift is that seeing results as you type helps you formulate a better search term by providing instant feedback. You can now adapt your search on the fly until the results match exactly what you want. In time, we may wonder how search ever worked in any other way.

[Try It Now](#)  
or, [set Google as your homepage](#)

Google Instant can save 2.5 seconds per search





# Predictions Update

RENEWED TOOL DEV



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.



# Predictions Update

SEEMS STRANGELY FAMILIAR

## Google Safe Browsing Alerts for Network Administrators

- Google's new service which greatly resembles MalwareDiggity
- Imitation is the sincerest form of flattery...

The screenshot shows the Google Safe Browsing Alerts for Network Administrators interface. At the top, the title "Google Safe Browsing Alerts for Network Administrators" is displayed in green. Below the title, there is a navigation menu with "Home" and "Messages" options. The main content area is divided into two columns. The left column contains a "Home" section with a "Messages" link and a paragraph of text: "Safe Browsing Alerts for Network Administrators allows autonomous system (AS) administrators to register to receive Google Safe Browsing notifications. The goal is to provide network administrators with information of malicious content that is being hosted on their networks." The right column contains a "Home" section with a "Messages" link and a notification: "You have no recent notification". Below this, there is a text input field with the placeholder "Enter the AS you'd like to manage." and a "Google Online Security Blog" section with the text "The latest news and insights from Google on security and safety on the Internet". At the bottom, there is a "Safe Browsing Alerts for Network Administrators" section with a date and time stamp "Tuesday, September 28, 2010 1:30 PM" and a post by "Nav Jagpal and Ke Wang, Security Team". The post text reads: "Google has been working hard to protect its users from malicious web pages, and also to help webmasters keep their websites clean. When we find malicious content on websites, we [attempt to notify](#) their webmasters via email about the bad URLs. There is even a [Webmaster Tools feature](#) that helps webmasters identify specific malicious content that has been surreptitiously added to their sites, so that they can clean up their site and help prevent it from being compromised in the future."

# Sensitive Info Mashup



GOOGLE MAPS + SENSITIVE INFO DISCLOSURE

Base Zip: 30342  
do zip search

30342  
30319  
30326  
31119  
30358

Select Zips: 30358  
Ref Name: none  
Show Packages

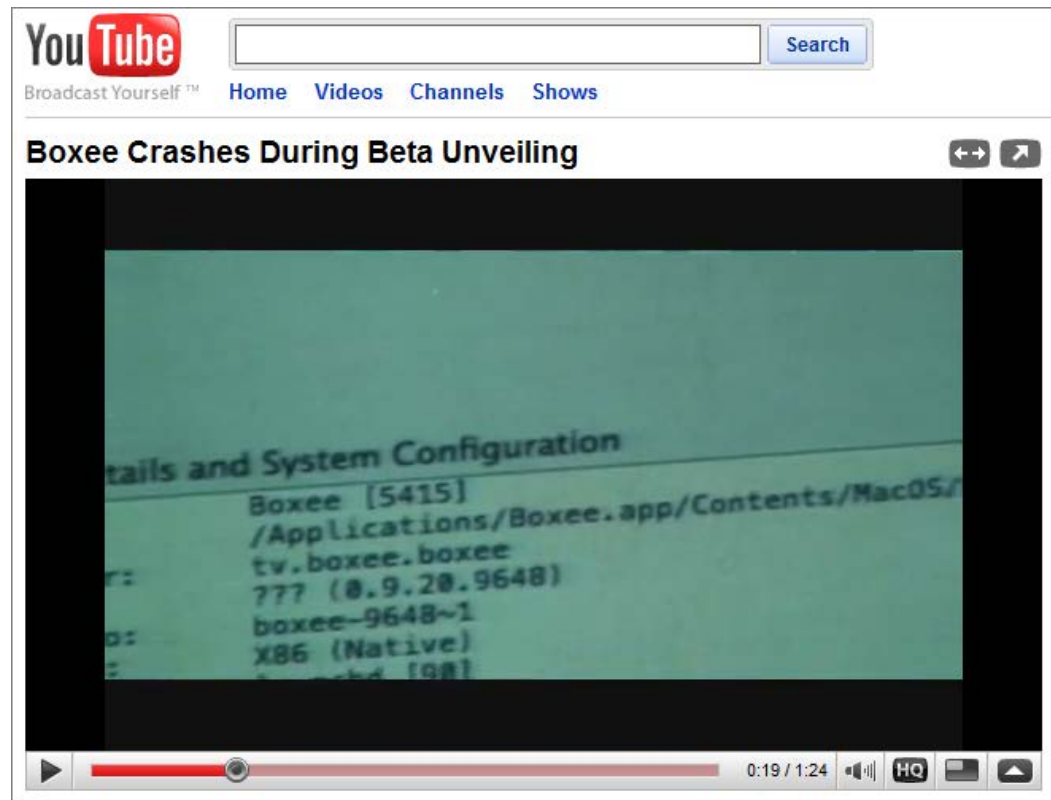
Tracking Number: 1Z W19 6XS  
03 4952 676 9  
Address: 5667 PEACHTREE  
DUNWOODY RD NE  
ATLANTA, GA 30342 US.  
Reference String: none.

Find: urls   Next   Previous   Highlight all   Match case

# Youtube Info Leak



YOUTUBE + SENSITIVE INFO DISCLOSURE





# WikiLeaks Auto-Generator



## FUTURE DIRECTIONS

OpenDLP 0.2.5 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

localhost https://localhost/OpenDLP/viewrest

Most Visited Getting Started Latest Headlines

OpenDLP 0.2.5

OpenDLP 0.2.5

- Main
- Profiles
- Regular Expressions
- Scans
  - Start New Scan
  - View Scans/Results
  - Export Scan Results
  - Delete Scan Results
- False Positives
- Logs
- OpenDLP Homepage

### View Results

Results for 192.168.170.134 (WIN2K3BOX):

Profile	test
Status	finished
Step	3: Done
Files Done	1
Files Total	1
Bytes Done	0
Bytes Total	13
Progress	<div style="width: 100%;"><div style="width: 100%;"></div></div>
Percentage	100%
Completion Time	
Total Findings	1
False Positives	0
Valid Findings	1
Updated	00:00:53 ago
Pause	N/A
Resume	N/A
Stop and Uninstall	N/A

#	Regex	Pattern	File (click to download)	Byte offset	False?
1	Social_Security_Number_dashes	666-66-6666	<a href="#">c:\badstuff\test.txt</a>	0	<input type="checkbox"/>

Mark Selected as False Positives



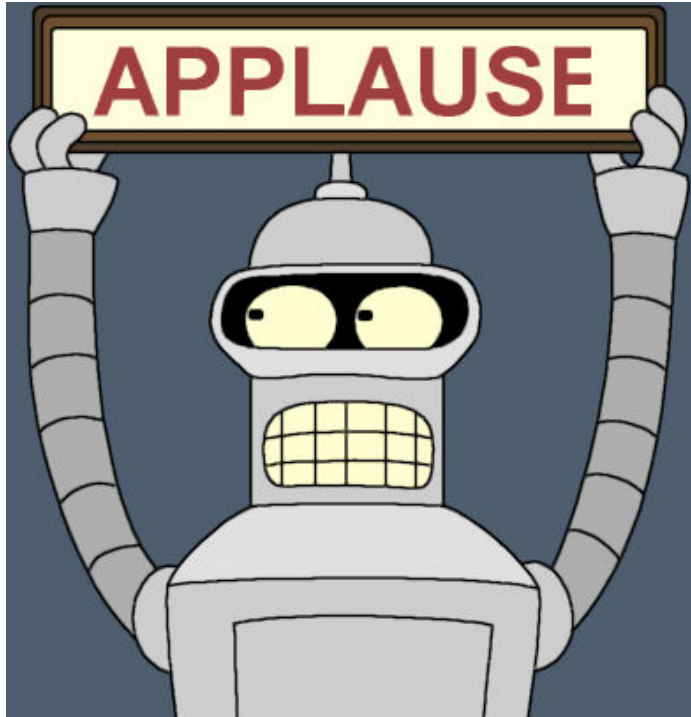




Questions?  
Ask us something  
We'll try to answer it.

For more info:  
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/>