

Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing

8 October 2010



Presented by:
Rob Ragan
Stach & Liu, LLC
www.stachliu.com

Goals

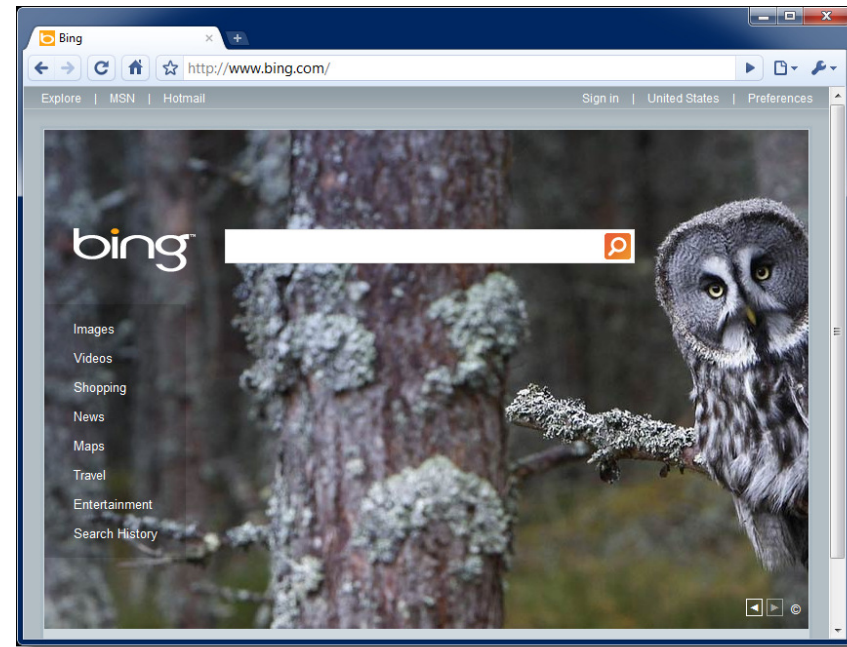
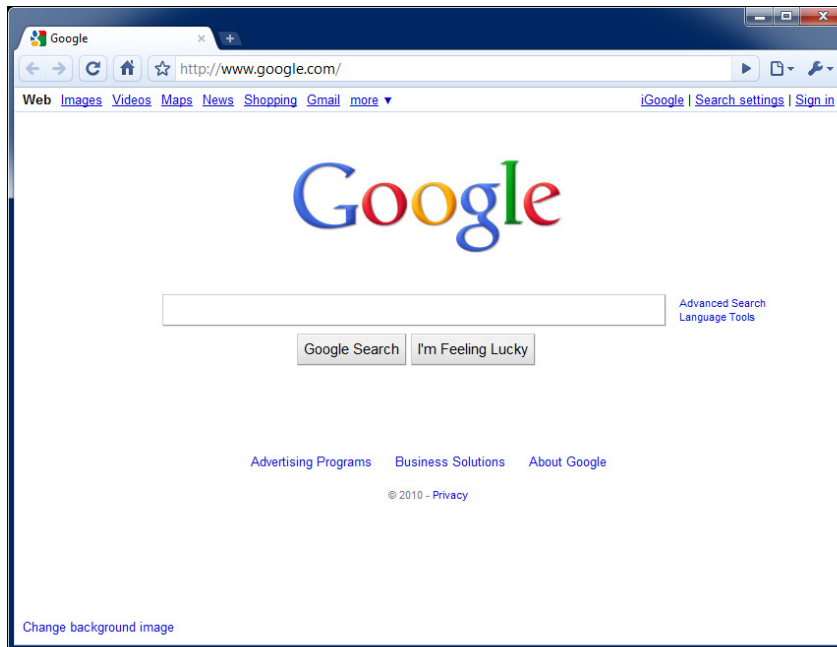
DESIRED OUTCOME

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



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)

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`

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

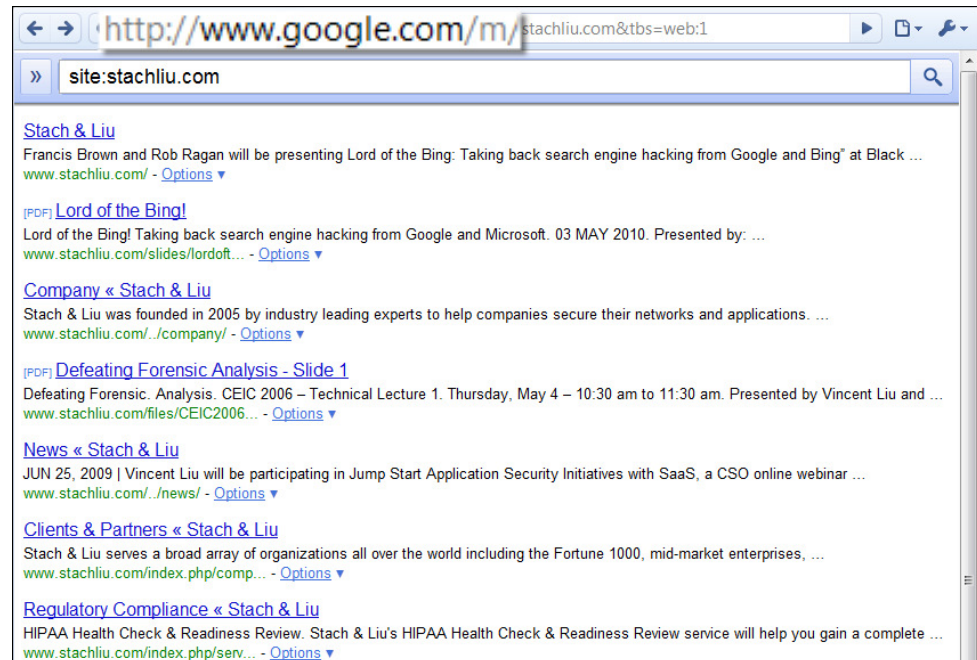
New Toolkit

STACH & LIU TOOLS



GoogleScape Diggity

- Uses Google mobile interface
 - Light-weight, no advertisements or extras
 - *Violates* Terms of Service
- Automatically leverages valid open proxies
- Spoofs User-agent and Referer headers
- Random **&userip=** value



New Hack Databases



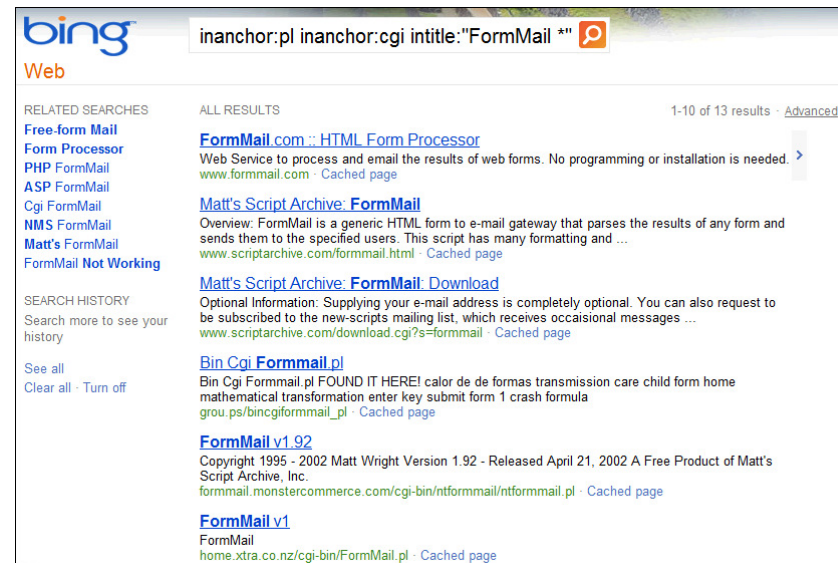
ATTACK QUERIES

BHDB – Bing Hacking Data Base

- First ever Bing Hacking database
- Bing has limitations that make it difficult to create vuln search queries
 - Bing disabled the **link:** and **linkdomain:** directives to combat abuse in March 2007
 - Does not support **ext:** or **inurl:**
 - The **filetype:** functionality is limited

Example - Bing vulnerability search:

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



New Hack Databases



ATTACK QUERIES

SLDB - Stach & Liu Data Base

- New Google/Bing hacking searches in active development by the S&L team

SLDB Examples

- `ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:confidential salary | intext:"budget approved") inurl:confidential`
- `(filetype:mail | filetype:eml | filetype:mbox | filetype:mbx) intext:password|subject`
- `filetype:sql "insert into" (pass|passwd|password)`
- `!Host=*. * intext:enc_UserPassword=* ext:pcf`
- `"your password is" filetype:log`



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

Google alerts Manage your Alerts stachliu0@gmail.com | Settings | FAQ | Sign out

GHDB regexs made into Google Alerts

Your Google Alerts

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

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+)

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 error with query" (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 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.cmail as userid, c.cemail as email, ...
www.mi6.co.uk/mi6.php3/news/index.php?itemid...t...

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
- Leverage `&format=rss` directive to turn into update feeds

Google reader All items

Navigation **Bing: "mysql error with query" »** Show: [Expanded](#) - [List](#)

Show: [5 new items](#) - [all items](#) [show details](#)

☆ www.kloosterman.be - mysql error with query SELECT p.pfile as pfile, e.event as event FROM	Apr 13, 2010	»
☆ The Shadow Project - Blog - mysql error with query SELECT COUNT(*) FROM nucleus_comment as c WHERE	Apr 13, 2010	»
☆ Hou-Hou Blog : tunisie blogs - mysql error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody	Apr 13, 2010	»
☆ Hou-Hou Blog : tunisie - mysql error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody as	Apr 13, 2010	»
☆ www.radiosonic.it - mysql error with query SELECT * FROM nucleus_config: Table 'Sql99301_1.nucleus_config'	Apr 13, 2010	»
☆ Hou-Hou Blog : george bush - mysql error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody as	Apr 7, 2010	»
☆ PHP /MYSQL - Error with query - ClanTemplates - PHP /MYSQL - Error with query Programming ... Programming Got	Apr 5, 2010	»
☆ www.tutje.nl - mysql error with query SELECT * FROM nucleus_config: Table 'poiplgqn_tutje.nucleus_config' doesn't exist	Apr 5, 2010	»

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



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

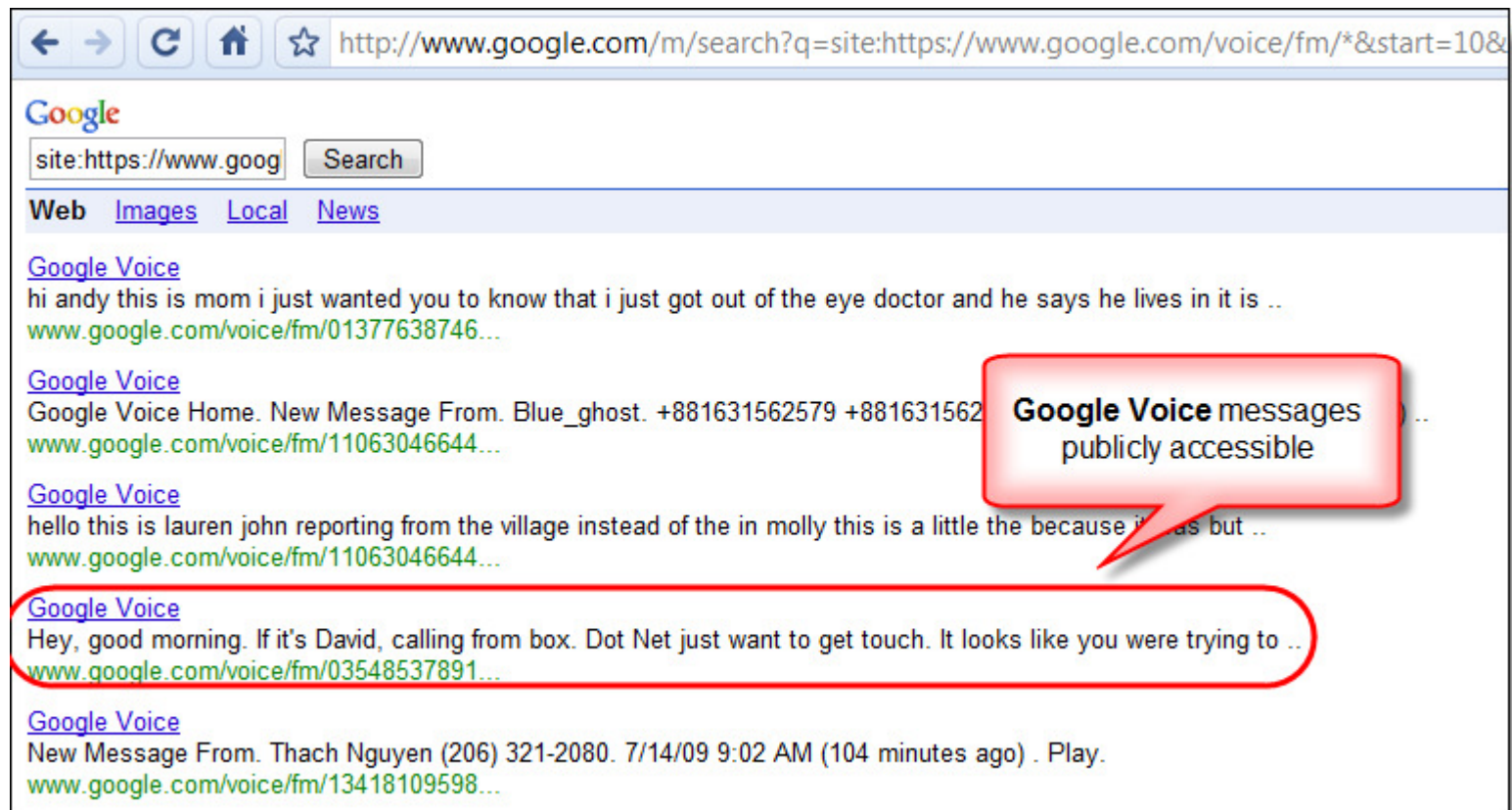
Google maps

Google groups

Google Voice



PARTY LINE



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 interface includes the Google Code Search Labs logo, a search bar with the query, and a 'Search' button. Below the search bar, the results are displayed. The first result is for a file named `post.asp`. The code snippet shows two lines of ASP code: `45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")` and `46: msg = "

×çôâ£°Ö»ÓÐ,ÃîÃôÃ×÷-ôß°í±ÙÀíô±²ÅÄÜ±â±ôâ,ôìû×ó."`. A red speech bubble points to the `reply_id` parameter in the first line, stating "reply_id is SQL injectable querystring parameter". The search results also show the number of results found: "Results 1 - 10 of about 2,000".

Code

Results 1 - 10 of about 2,000.

[post.asp](#)

```
45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br>×çôâ£°Ö»ÓÐ,ÃîÃôÃ×÷-ôß°í±ÙÀíô±²ÅÄÜ±â±ôâ,ôìû×ó."
```

```
57: strSql = "SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çôâ£°Ö»ÓÐ,ÃîÃôÃ×÷-ôß°í±ÙÀíô±²ÅÄÜ±â±ôâ,ôìû×ó."
```

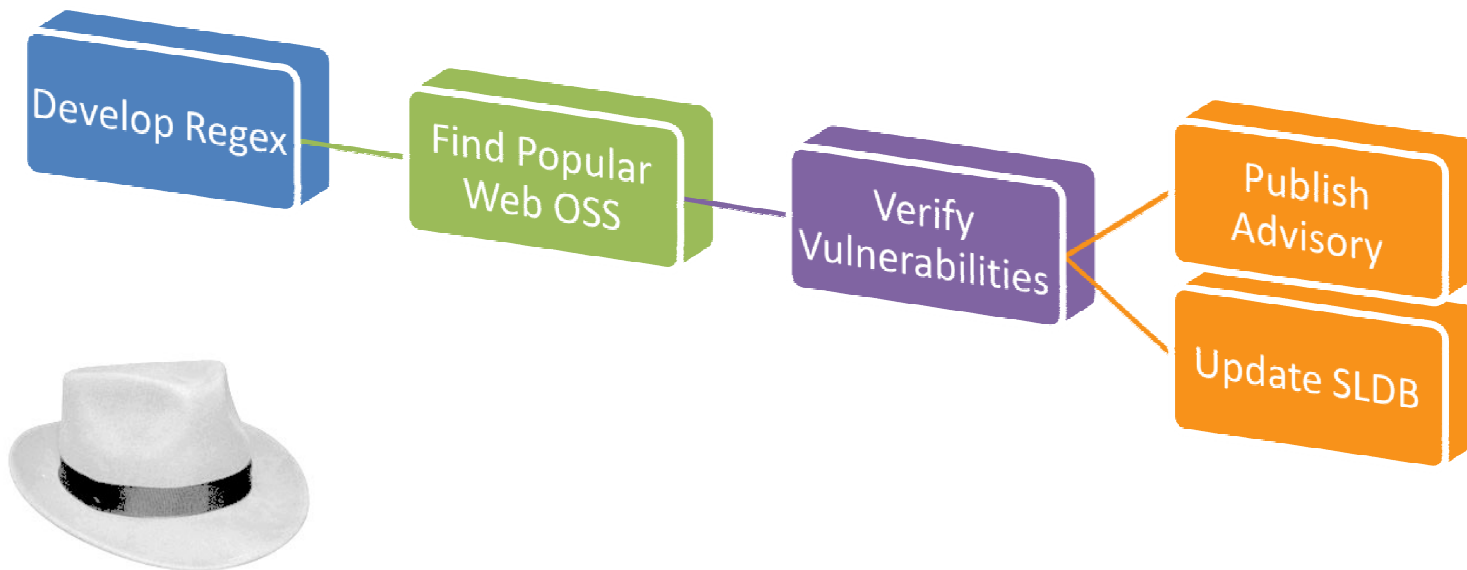
www.cnarts.net/eweb/download/software/bbs/tradeforum.zip - Unknown - ASP - [More from tradeforum.zip](#) »

GOOGLE CODE SEARCH HACKING DEMO

Google Code Search



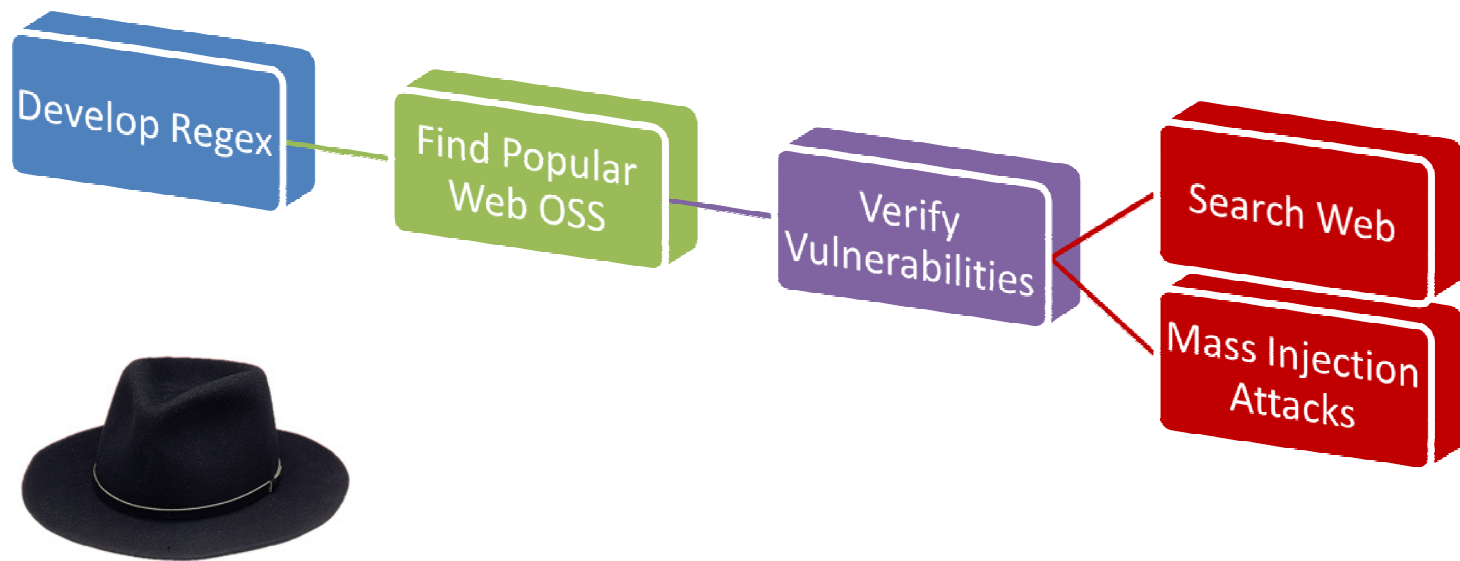
VULNS IN OPEN SOURCE CODE



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

Search

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... routers through drive

RELATED ARTICLES

Top Google searches over past 6 years

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



Defenses



BLACKHAT SEO DEFENSES

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



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/ebayArticle.jhtml?articleID=225600347>

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

Sure enough, the Web sites of the *Jer* and the Association of Christian Scho sites serving malware to viewers.

From: www.itworld.com

Mass Web attack hits Wall Street Journal, Jerusalem Post

by Robert McMillan

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

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



Malware Browser Filters



URL BLACK LIST

Protecting users from known threats

- Joint effort to protect customers from known malware and phishing links

Reported Attack Site!

This web site at 91.205.233.31 has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#) [Why was this site blocked?](#)

[Ignore this warning](#)

Inconvenient Truth



DICKHEAD ALERTS

Malware Black List Woes

- Average web administrator has no idea when their site gets black listed



Advanced Defenses

PROTECT YO NECK



Malware Diggity

ADVANCED DEFENSES



Malware Diggity

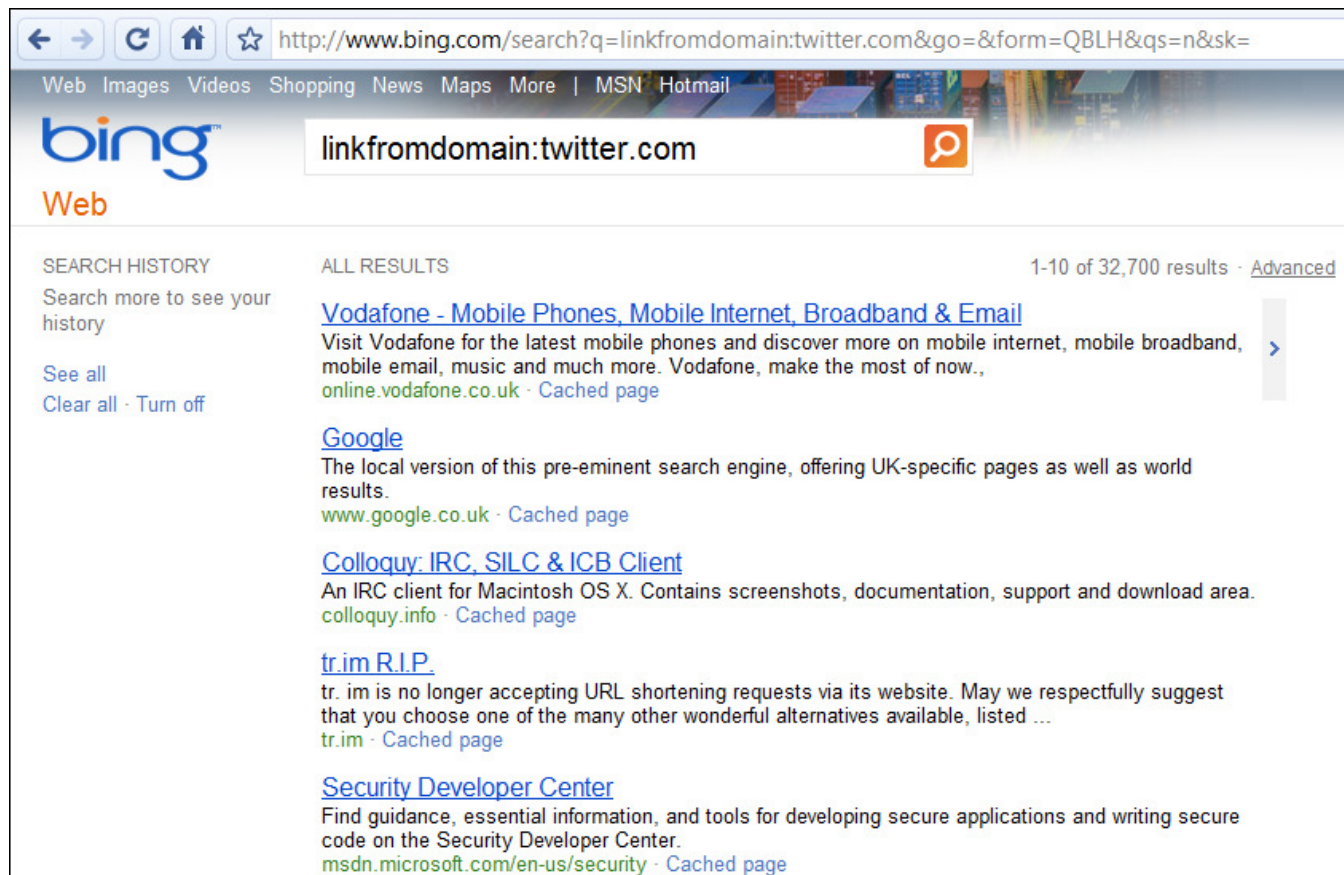
- Uses Bing's **linkfromdomain:** directive to *identify off-site links* of the domain(s) you wish to monitor
- Compares to *known malware sites/domains*
 - Alerts if site is compromised and now distributing malware
 - Monitors new Google Trends links

Malware Diggity Alerts

- Leverages the Bing '**&format=rss**' directive, to *actively monitor new off-site links* of your site as they appear
- Immediately lets you know if you have been compromised by one of these mass injection attacks or if your site has been black listed

Malware Diggity

ADVANCED DEFENSES



Malware Diggity

ADVANCED DEFENSES



YAHOO!

SITE EXPLORER

Site Explorer

- Add to MySites
- My Sites
- Submit Your Site
- Preferences
- Blog
- Badge
- Web Service API
- Feedback

Results

Pages (70) **Inlinks (4,130)** Show Inlinks: to:

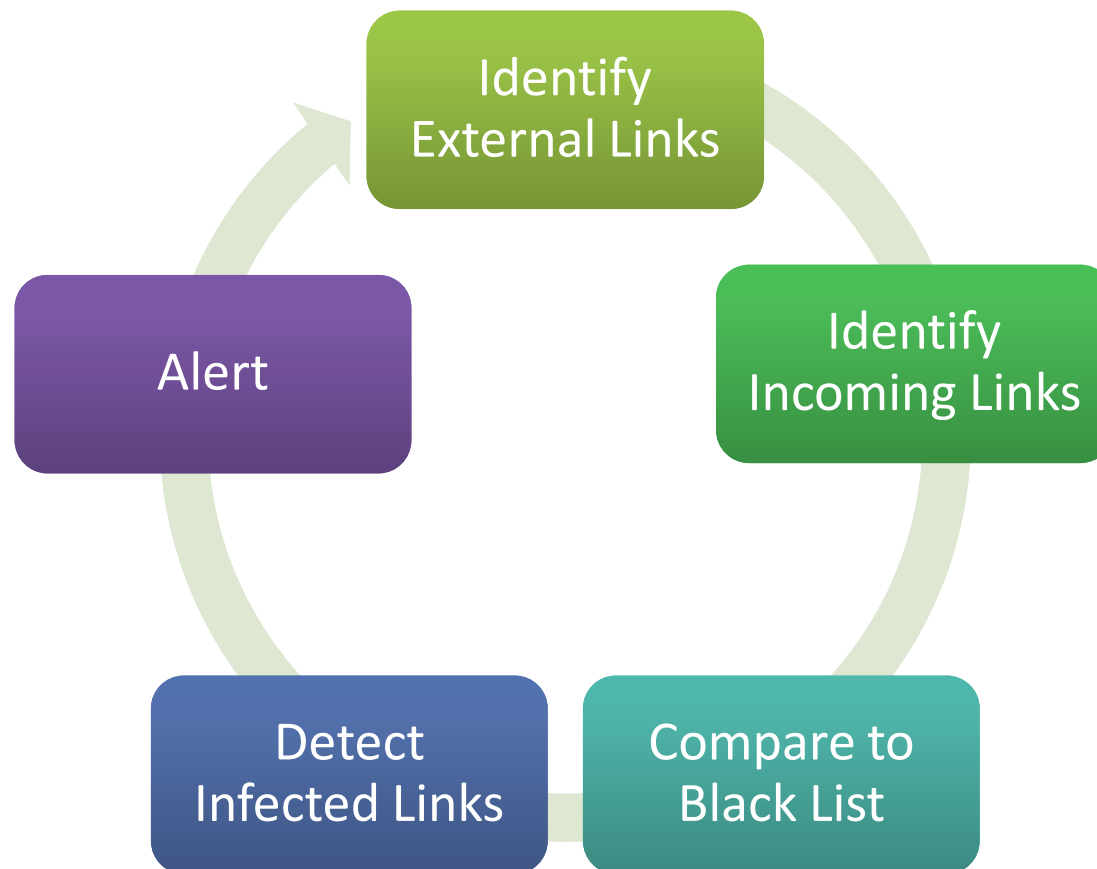
Result details:

[Submit webpage or Site Feed](#) | [Export first 1000 results to TSV](#)

1.	Unofficial MD5 text/html http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html - 12k - cache	<input type="button" value="Explore"/>
2.	Offensive Computing Community Malicious code research and ... text/html http://www.offensivecomputing.net/ - 35k - cache	<input type="button" value="Explore"/>
3.	Approved Scanning Vendors text/html https://www.pcisecuritystandards.org/pdfs/asv_report.html - 34k - cache	<input type="button" value="Explore"/>
4.	Peter Selinger: MD5 Collision Demo text/html http://www.mscs.dal.ca/~selinger/md5collision/ - 13k - cache	<input type="button" value="Explore"/>
5.	Microsoft BlueHat Blog - Site Home - TechNet Blogs text/html http://blogs.technet.com/b/bluehat/ - 140k - cache	<input type="button" value="Explore"/>
6.	Checkmarx Source Code Analysis Technologies text/html http://www.checkmarx.com/ - 48k - cache	<input type="button" value="Explore"/>
7.	Black Hat USA Spotlight: ATL Killbit Bypass - Microsoft ... text/html http://blogs.technet.com/b/bluehat/archive/2009/07/27/black-hat-usa-atl-killbit-bypass.aspx - 151k - cache	<input type="button" value="Explore"/>

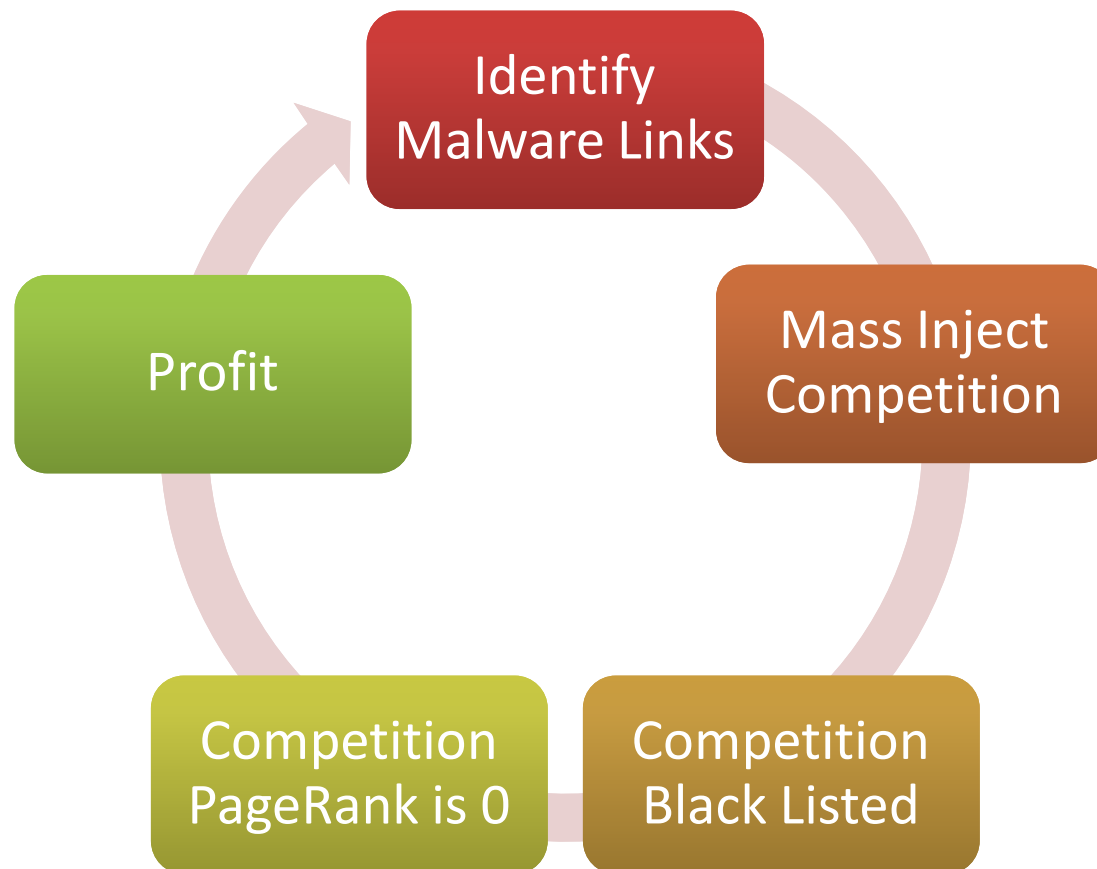
Malware Monitoring

INFECTION DETECTION



Search Engine deOptimization

BLACK LIST YOUR FOES



Safe Browsing Alerts

ADVANCED DEFENSES



Google Safe Browsing Alerts for Network Administrators

Home
[Messages](#)

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.

[Malware Forum](#)

Home
Messages

You have no recent notification emails. Once you add and verify an AS,

Enter the AS you'd like to manage.

Continue

Future Direction

PREDICTIONS



Google policy is to get
right up to the creepy line
and **not** cross it.

– Eric Schmidt
Google CEO

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
 - Customized search engines
- Google Code and Other Open Source Repositories
 - MS CodePlex, SourceForge, ...
- More automation in tools
 - Real-time detection and exploitation
 - Google worms

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

For more info:

Email: contact@stachliu.com

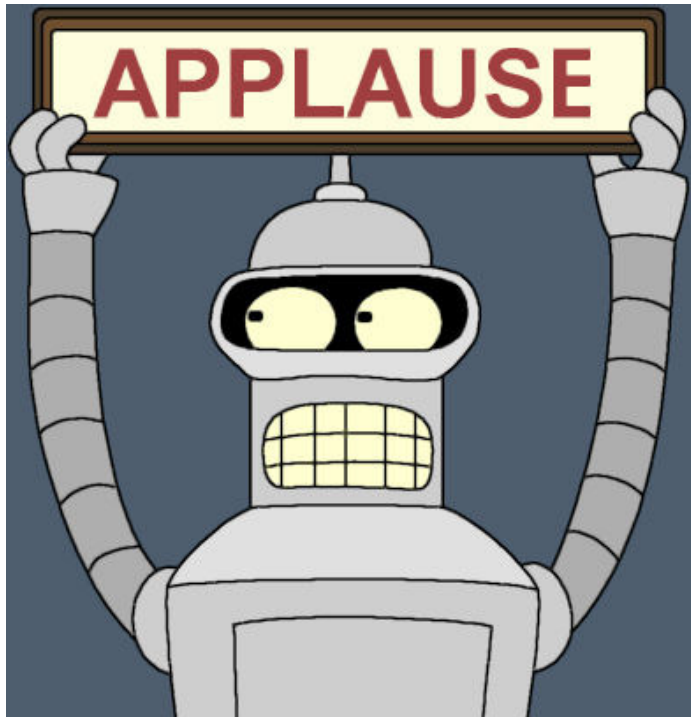
Project: diggity@stachliu.com

Stach & Liu, LLC

www.stachliu.com



Thank You



Stach & Liu Project info:

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