

Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing

ToorCon 12 - 24 October 2010



Presented by:
Francis Brown
Stach & Liu, LLC
www.stachliu.com

Agenda

OVERVIEW

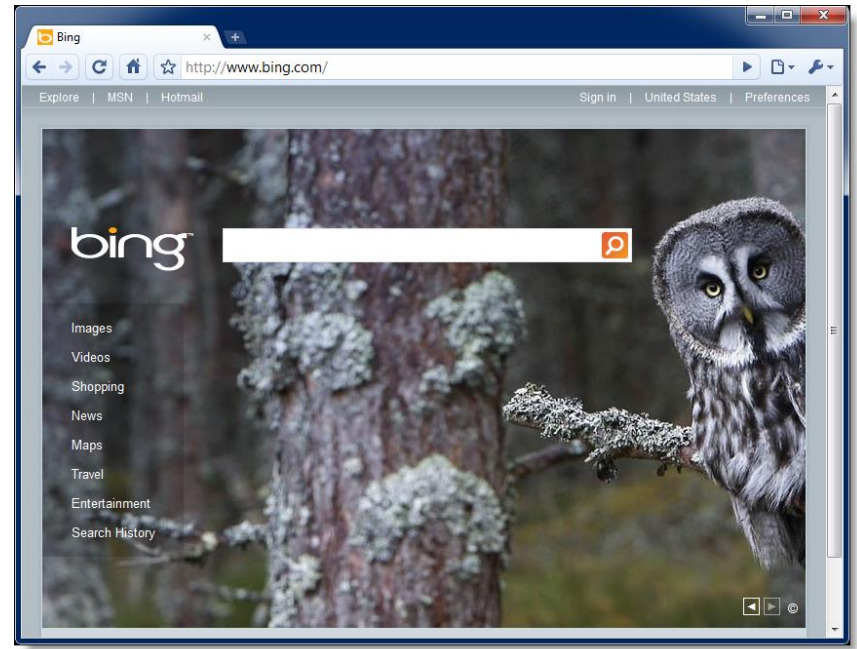
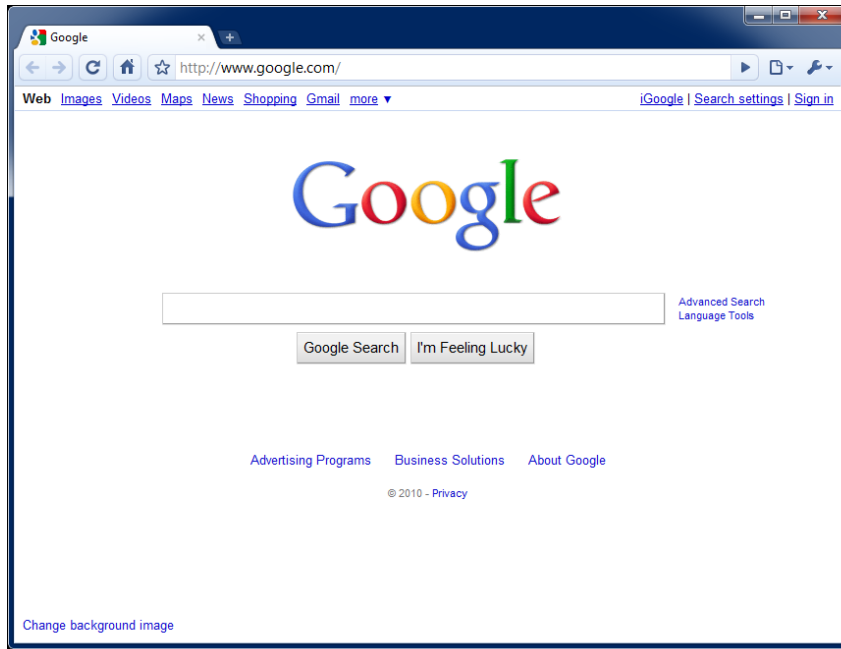
- Introduction/Background
- Advanced Attacks
 - Google/Bing Hacking
- Advanced Defenses
 - Google/Bing Hacking Alerts
- Demos (time permitting)

Introduction/ Background

GETTING UP TO SPEED

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`

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
June 3, 2009	Bing goes online
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

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

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

The screenshot displays the Search Diggity application window. The interface includes a menu bar (File, Options, Help), a toolbar with 'SCAN' and 'Cancel' buttons, and a 'Sites/Domains' list containing 'stachliu.com'. A 'Query Appender' and 'Queries' tree view are on the left. The main area shows a table of search results with columns for Category, Subcategory, Search String, Page Title, URL, and Cache URL. The 'Output' pane at the bottom shows the scan results.

Category	Subcategory	Search String	Page Title	URL	Cache URL
Custom	Custom	site:stachliu.c	Stach & Li	http://www.stachliu.com/	http://www.google.com/search?
Custom	Custom	site:stachliu.c	Lord of the Bin	http://www.stachliu.com/slides/	http://www.google.com/search?
Custom	Custom	site:stachliu.c	APPLiCATION So	http://www.stachliu.com/brochui	http://www.google.com/search?
Custom	Custom	site:stachliu.c	Lord of the Bin	http://www.stachliu.com/slides/t	http://www.google.com/search?
Custom	Custom	site:stachliu.c	News « Stach &	http://www.stachliu.com/index.p	http://www.google.com/search?
Custom	Custom	site:stachliu.c	Secure Web AP	http://www.stachliu.com/brochui	http://www.google.com/search?

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]
```

New Toolkit

BINGDIGGITY

The screenshot shows the Search Diggity application window. The interface includes a menu bar (File, Options, Help), a tabbed interface (GoogleDiggity, BingDiggity), and a main workspace. The workspace has a left sidebar with a tree view of search categories (e.g., BHDB, Advisories and Vulnerabilities, Backup Files, Configuration Management, Error Messages, Files containing javascript, Files containing perl, Files containing unix, Footholds, Misc, Pages containing, Pages containing, Privacy Related, Remote Administration, Reported Vulnerabilities, Sensitive Directories, Sensitive Online Information, Technology Profiles, Various Online Directories, Vulnerable Files). The main area contains a 'Query Appender' and 'Queries' list. A 'SCAN' button is visible. The 'Bing 2.0 API Key' is set to '37C73B99461F9367FBF'. The 'Sites/Domains/IPs' list contains '98.129.200.37'. The search results table is as follows:

Category	Subcategory	Search String	Page Title	URL
Custom	Custom	ip:98.129.200.37	Stach & Liu	http://www.stachliu.com/
Custom	Custom	ip:98.129.200.37	Google Hacking Diggity Project	http://www.stachliu.com/index.php/resources/tools/google-hacking-diggity/
Custom	Custom	ip:98.129.200.37	Tools « Stach & Liu	http://www.stachliu.com/index.php/resources/tools/
Custom	Custom	ip:98.129.200.37	Training « Stach & Liu	http://www.stachliu.com/index.php/training/
Custom	Custom	ip:98.129.200.37	Webinars « Stach & Liu	http://www.stachliu.com/index.php/resources/webinars/
Custom	Custom	ip:98.129.200.37	Management & Advisory Board	http://www.stachliu.com/index.php/company/management-advisory-board/
Custom	Custom	ip:98.129.200.37	Clients & Partners « Stach & Liu	http://www.stachliu.com/index.php/company/clients-partners/

The 'Output' tab shows the following text:

```
Advanced Scan started. [9/13/2010 10:37:10 PM]
Adult Option: Moderate
Maximum 200 results per query.
Using Custom Search ID: 2136A2334B9A25C0CB87C73B99461F9367FBFD32.
Found 32 result(s) for query: " " [98.129.200.37].
Total Results: 32.
Scan Complete. [9/13/2010 10:37:12 PM]
```

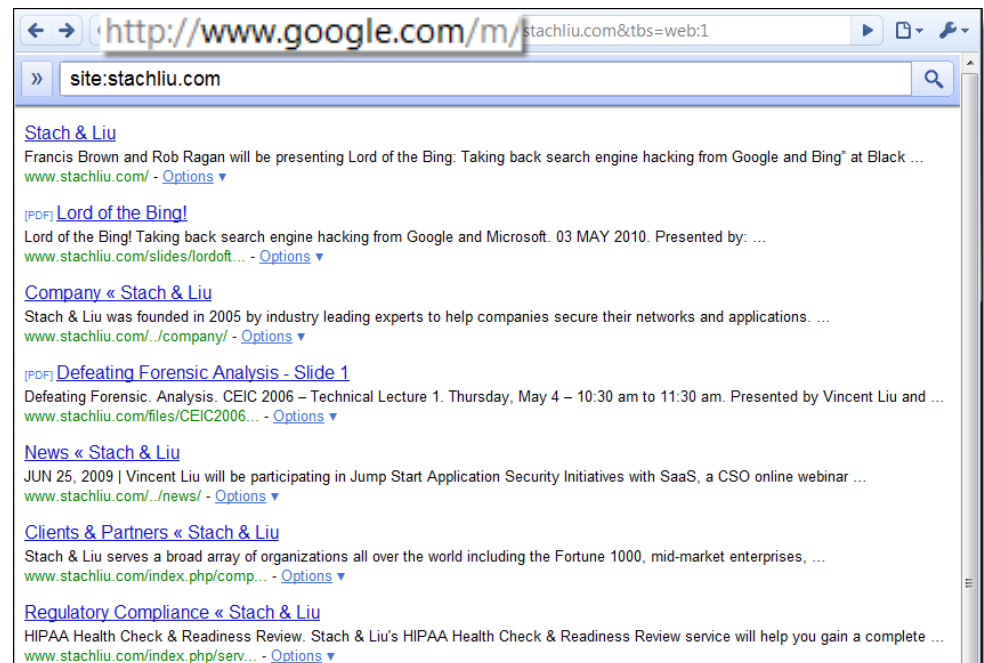
New Toolkit

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"`

The screenshot shows a Bing search results page. The search bar contains the query: `inanchor:pl inanchor:cgi intitle:'FormMail *''`. The search results are displayed in a list format. The first result is "FormMail.com :: HTML Form Processor" with a description: "Web Service to process and email the results of web forms. No programming or installation is needed." The second result is "Matt's Script Archive: FormMail" with a description: "Overview: FormMail is a generic HTML form to e-mail gateway that parses the results of any form and sends them to the specified users. This script has many formatting and ...". The third result is "Matt's Script Archive: FormMail: Download" with a description: "Optional Information: Supplying your e-mail address is completely optional. You can also request to be subscribed to the new-scripts mailing list, which receives occasional messages ...". The fourth result is "Bin Cgi Formmail.pl" with a description: "Bin Cgi Formmail.pl FOUND IT HERE! calor de de formas transmission care child form home mathematical transformation enter key submit form 1 crash formula". The fifth result is "FormMail v1.92" with a description: "Copyright 1995 - 2002 Matt Wright Version 1.92 - Released April 21, 2002 A Free Product of Matt's Script Archive, Inc.". The sixth result is "FormMail v1" with a description: "FormMail home.xtra.co.nz/cgi-bin/FormMail.pl".

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"

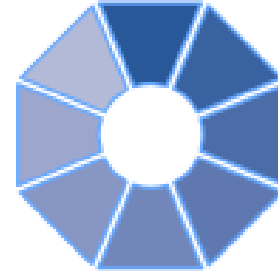
- ✓ Tools exist
- ✗ Convenient
- ✗ Real-time updates
- ✗ Multi-engine results
- ✗ Historical archived data
- ✗ Multi-domain searching

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 [Switch to text emails](#) | [Export 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 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	as-it-happens	up to 50 results	Feed View in Google Reader edit
<input type="checkbox"/> "# phpMyAdmin MySQL-Dump" "INSERT INTO" -"the"	Web	as-it-happens	up to 50 results	Feed View in Google Reader edit

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...

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

Google reader [Search] All items

+ Add a subscription

All items (1000+)

People you follow

Explore

Subscriptions

- BHDB-Advisories and V... (910)
- BHDB-Backup Files (50)
- BHDB-Configuration Ma... (207)
- BHDB-Error Messages (507)
- BHDB-Files containing... (607)
- BHDB-Files containing... (343)
- BHDB-Files containing... (50)
- BHDB-Footholds (45)
- BHDB-Misc (116)
- BHDB-Pages containing... (765)
- BHDB-Pages containing... (159)
- BHDB-Privacy Related (196)
- BHDB-Remote Administr... (36)
- BHDB-Reported Vulnera... (20)
- BHDB-Sensitive Direct... (200)

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

Snap Server FTP-SERVER [Home] »

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

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

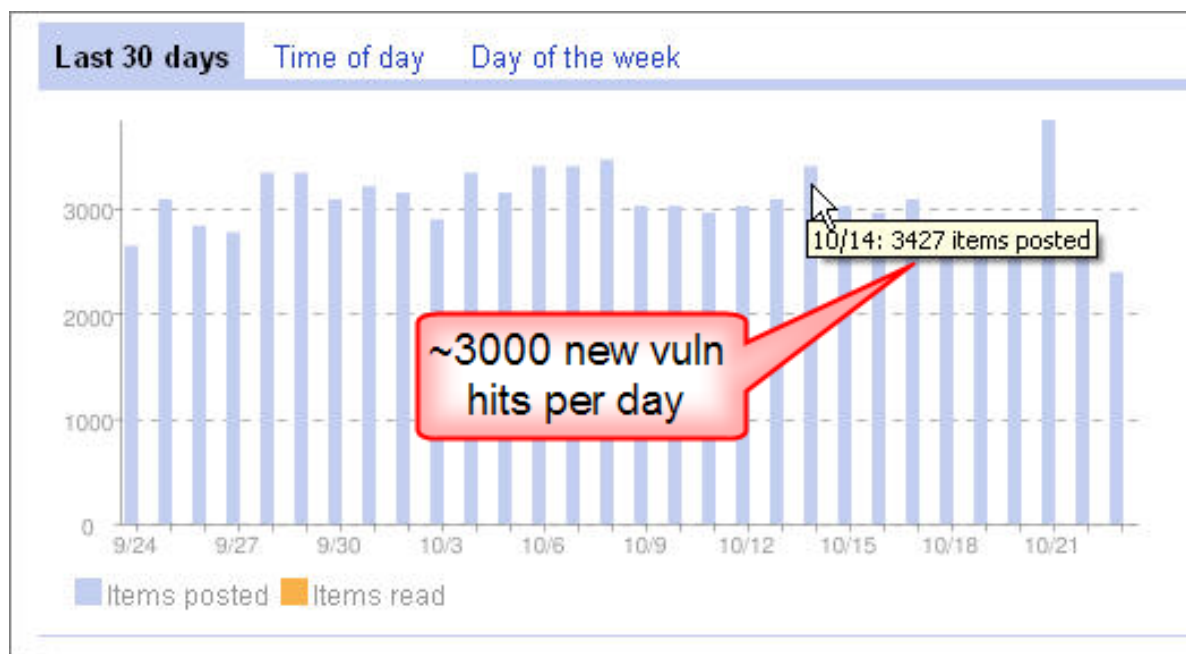
- ★ Snap Server XRAY7 [Home] - XRAY7 • Home
- ★ Snap Server SNAP205861 [Home] - SNAP205861 • Home

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)



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

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/>