Pulp Google Hacking

The Next Generation Search Engine Hacking Arsenal

3 August 2011 – Black Hat 2011 – Las Vegas, NV

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

• 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);
    }
}

STACH&LIU
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

Google Hacking search used by Kayla of LulzSec
## Quick History

### Google Hacking Recap

<table>
<thead>
<tr>
<th>Dates</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>Google Hacking Database (GHDB) begins</td>
</tr>
<tr>
<td>May 2004</td>
<td>Foundstone SiteDigger v1 released</td>
</tr>
<tr>
<td>2005</td>
<td>Google Hacking v1 released by Johnny Long</td>
</tr>
<tr>
<td>Jan 2005</td>
<td>Foundstone SiteDigger v2 released</td>
</tr>
<tr>
<td>Feb 13, 2005</td>
<td>Google Hack Honeypot first release</td>
</tr>
<tr>
<td>Jan 10, 2005</td>
<td>MSNPawn v1.0 released</td>
</tr>
<tr>
<td>Dec 5, 2006</td>
<td>Google stops issuing Google SOAP API keys</td>
</tr>
<tr>
<td>Mar 2007</td>
<td>Bing disables inurl: link: and linkdomain:</td>
</tr>
<tr>
<td>Nov 2, 2007</td>
<td>Google Hacking v2 released</td>
</tr>
</tbody>
</table>
Quick History...cont.

**Google Hacking Recap**

<table>
<thead>
<tr>
<th>Dates</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2008</td>
<td>cDc Goolag - gui tool released</td>
</tr>
<tr>
<td>Sept 7, 2009</td>
<td>Google shuts down SOAP Search API</td>
</tr>
<tr>
<td>Nov 2009</td>
<td>Binging tool released</td>
</tr>
<tr>
<td>Dec 1, 2009</td>
<td>FoundStone SiteDigger v 3.0 released</td>
</tr>
<tr>
<td>2010</td>
<td>Googlag.org disappears</td>
</tr>
<tr>
<td><strong>April 21, 2010</strong></td>
<td><strong>Google Hacking Diggity Project initial releases</strong></td>
</tr>
<tr>
<td>Nov 1, 2010</td>
<td>Google AJAX API slated for retirement</td>
</tr>
<tr>
<td>Nov 9, 2010</td>
<td>GHDB Reborn Announced – Exploit-db.com</td>
</tr>
<tr>
<td>July 2011</td>
<td>Bing ceases <code>&amp;format=rss</code> support</td>
</tr>
</tbody>
</table>
Advanced Attacks
WHAT YOU SHOULD KNOW
Diggity Core 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

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 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

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

Search Diggity

Google Diggity

CodeSearchDiggity BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity MalwareDiggity

Advanced Simple

Query Appender

Queries

FSDB GHDB

Advisories and Vi Error Messages

Files containing j Files containing p

Footholds Misc

Pages containing Pages containing Sensitive Directory Sensitive Online

Category Subcategory Search String Page Title URL


Output Selected Result


Google Status: Ready

Download Progress: Idle Open Folder
Bing Diggity

D I G G I T Y  C O R E  T O O L S

Demonstrating Bing's IP address reverse lookup feature
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"`
Hacking CSE’s

All Top Level Domains

Search engine details
All top level domains:
http://data.jana.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: 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`

<table>
<thead>
<tr>
<th>Code</th>
<th>Results 1 - 10 of about 2,000</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>post.asp</code></td>
<td>reply_id is SQL injectable querystring parameter</td>
</tr>
</tbody>
</table>

```html
45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br><br><br><br><br> آلأُلُحِّ، أَطَأَبَ الأَنَّا حُكْمَ أَلَّاَدَّ "
57: strSql = "SELECT T.Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br><br><br><br><br> آلأُلُحِّ، أَطَأَبَ الأَنَّا حُكْمَ أَلَّاَدَّ "

www.cnarts.net/web/download/software/bbs/tradeforum.zip - Unknown - ASP - More from tradeforum zip »
```
CodeSearch Diggity

Amazon Cloud Secret Keys

Amazon AWS Cloud keys stored in plaintext

STACH&LIU
NEW GOOGLE HACKING TOOLS

Bing LinkFromDomainDiggity
Bing LinkFromDomain

**DIGGITY TOOLKIT**

External links then sorted and extracted into: applications, host names, and domains

Bing’s linkfromdomain: directive used to find external links on your sites
Bing LinkFromDomain

FOOTPRINTING LARGE ORGANIZATIONS

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

DI G G I T Y  T O O L K I T

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=225232417

"Every time I load this site, I get malware," on Tuesday, referring to the Jerusalem Post.

Sure enough, the Web sites of the Jerusalem Post and the Association of Christian Schools were 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 Infopost.org.
Mass Injection Attacks

Malware Gone Wild

Malware Distribution Woes – LizaMoon – April 2011

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

---

Viral Scareware Infects Four Million Websites

posted by timothy on Saturday April 02, @04:55PM from the warning your computer may be at risk dept.

oxide7 writes

"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."
Mass Injection Attacks

Malware Distribution Woes – willysy.com - August 2011

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

Diggity Toolkit

NEW

STACH&LIU
Malware Diggity

**DIAGNOSTICS IN RESULTS**

![Safe Browsing diagnostic result](www.google.com/safebrowsing/diagnostic?site=sf.tastyr.com)

*What is the current listing status for sf.tastyr.com?*
Site is listed as suspicious - visiting this web site may harm your computer.

*What happened when Google visited this site?*
Of the 10 pages we tested on the site over the past 90 days, 1 page(s) resulted in malicious software being downloaded and installed without user consent. The last test was on 2011-09-08, and the last site was on 2011-09-08.

Malicious software includes 4 scripting exploit(s).
Malicious software is hosted on 1 domain(s), including **lizamoon.com/**.
This site was hosted on 1 network(s) including **AS174 (COGENT)**.

Page suspected to be malicious and associated with LizaMoon
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

- **filetype:doc**
  - 1-10 of 26,900,000 results - Advanced

Bing

- **filetype:pdf**
  - 1-10 of 146,000,000 results - Advanced
DLP Diggity
MORE DATA SEARCHABLE EVERY YEAR

Google Results for Common Docs

- **PDF**: 10,900,000
- **DOC**: 260,000,000
- **XLS**: 84,500,000
- **TXT**: 17,300,000
- **2004**
- **2007**
- **2011**

**2004**: 513,000,000
**2007**: 42,000,000
**2011**: 46,400,000
Search through downloaded files from GoogleDiggity and BingDiggity for data leaks such as SSNs, credit cards, etc.
NEW GOOGLE HACKING TOOLS

FlashDiggity
Flash Diggity

D I G G I T Y  T O O L K I T

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

Hardcoded usernames and passwords in cleartext in SWF file
NEW GOOGLE HACKING TOOLS

DEMO
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

Finding vulns in Chinese government sites
Advanced Defenses

PROTECT YOUR NECK
Traditional 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
Adv​anced 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

- 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 Hacking Alerts

ADVANCED DEFENSES

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

Several thousand GHDB/FSDK

val alerts generated each day
Bing Hacking Alerts

- Bing searches with regexs from BHDB
- Leverages \texttt{http://api.bing.com/rss.aspx}
- Real-time vuln updates to $>900$ Bing hack queries via RSS
Bing/Google Alerts

LIVE VULNERABILITY FEEDS

World’s Largest Live Vulnerability Repository
• Daily updates of ~3000 new hits per day
ADVANCED DEFENSE TOOLS

Diggity Alert Funple Bundle
FUNdle Bundle
ADVANCED DEFENSES

"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 6,376 feeds included in this bundle
Sign in to subscribe

Debris Removal - News & Information
via Google Alerts - inurl:"/_layouts/" filetype:asp+xsl trav 9/11/11

(New Hanover County) --- New Hanover County and municipal offices with representatives of the Federal Emergency Management Agency.
www.nhcgov/News_/-layouts/listform.aspx?

*Curriculum Vitae*
via Google Alerts - "phone ^ ^ ^" address " " e-mail "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...
hh2504.dcccd.edu/vita/0017421.pdf

3762 RSS feeds from GHDB, FSDB, SLDB all consolidated into 1 RSS feed using Google Reader bundles
SHODAN Alerts

FINDING SCADA SYSTEMS

Using SHODAN to find SCADA web admin interfaces
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
ADVANCED DEFENSE TOOLS

iDiggity Alerts
iDiggity Alerts

ADVANCED DEFENSES

iDiggity Alert URL
http://www.stachliu.com/tools/iDiggityAlerts.xml

Search Domains
Tap To Add a Domain
hp.com
milblogging.com

Startup Behavior
Search feeds OFF

STACH&LIU
iDiggity Alerts

ADVANCED DEFENSES

- Feed: GHDB-Files containing...
  - Google Alerts - "login: "*
    - "password= "*
    - filetype:xls
  - http://www.google.com/url?sa=X&q=http://h30499.www3.hp.com/hpeb/attachments/hpeb/sws-20/1044/1/Attack%2520Statuss.XLS&ct=ga&cad=CAcQARgBAEoATAAOABAxvOQ8QRIAlgAYgVib1VUw&cd=1IV50JjTxmg&usg=AFQjCNEzfN95HhqChmtMJRucbi1ZmKU-g

- Reminder:
  - Thursday (08-04) at 04:30 AM
  - Repeat Weekly: ON

- Actions:
  - Collapse All
  - Collapse 2 searches
  - Google Alerts - intitle:Index. of etc shadow
  - Google Alerts - "login: "p
    - "assword= "*
    - filetype:xls

- Search Again
- Email Results
- Cancel
New Defenses

“GOOGLE/BING HACK ALERTS”

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

3rd 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.

As Johnny is now pursing 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 “BeSickWittIt” 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/