"The Google Hacking Database: A Key Resource to Exposing Vulnerabilities"

Presented by:

Kiran Karnad
Mimos Berhad

Brought to you by:
Kiran Karnad

MIMOS Berhad

After more than sixteen years in software testing and implementation, Kiran Karnad found his true calling in penetration testing. Proudly calling himself a hands-on lead for information security, Kiran has worked with several Fortune 500 companies and mentored software test teams in multiple geographies. Currently leading the functional and security efforts at MIMOS, Kiran strives to identify process improvement opportunities throughout the organization and to implement them effectively.
The Google Hacking Database

Product Quality and Reliability Engineering Team
– Kiran Karnad, MIMOS Bhd

A Key Resource to exposing vulnerabilities
Disclaimer

This presentation is meant purely for ethical purposes.

Disclaimer

Neither MIMOS nor Kiran bear any responsibilities for any unethical usage of this material and training.
What’s This All About?

- Google & Bing Basics - OSINT
- Basic, Phrase, Advanced Search
- What’s Google Hacks All About?
- Sample Hacks
- Script for OS INT

In the Recent Past

- Sony
- Citibank
- Petrobras
- Google
- Apple
- eBay
- PayPal
- Facebook

If you are not hacked, you are not important!
What all can be hacked

- Network
- Hardware hacking
- Wireless
- Social Engineering
- Mobile
- Lock Picking
- Web hacking

What you don’t know might hurt…
OSINT – Let’s define

Intelligence collected from public sources

- Google
- Social Engines
- Details on next slide

OSINT Communities

- Government – FBI, CBI etc
- Military – Defence Intel Agency
- Homeland Security
- Business – Commercial, Competitor INT, BI
- Anonymous & LulzSec – shodan, GHDB

OSINT – Some methods

- Facebook
- Mobistealth
- Social Engineering
- Jobs DB
- Shodan
- StackOverflow
- Spokeo
- Recon-ng
- GHDB
GOOGLE HACKING

It's what you expose

How Google Works

Web spider

Builds index based on its own system of weighting

Encodes the data to save space

Builds list of words and notes where they were found

Stores data for users to access
Basic Search

Advanced Operators

Phrase Search

Search Types Supported

BASIC SEARCH

The most used type of search
So InSensitiVe

Web Images Maps Shopping More Search tools

About 1,590,000 results (0.38 seconds)

STARWest
starwest.technwell.com/
STARWEST is the premier event for software testers and quality assurance professionals—covering all your testing needs with 100+ learning and networking ...

5W 1H – Google doesn’t mind

Web Images Maps Shopping More Search tools

About 9,900,000 results (0.48 seconds)

Web Images Maps Shopping More Search tools

About 265,000,000 results (0.62 seconds)

Web Images Maps Shopping More Search tools

About 265,000,000 results (0.62 seconds)

Web Images Maps Shopping More Search tools

About 265,000,000 results (0.61 seconds)

Web Images Maps Shopping More Search tools

About 265,000,000 results (0.61 seconds)
Mark my Ten Words, that’s it

The reason for the previous results...

Google stems the results – singular, plural, verb etc etc

And is implied for each word

All word permutations and combinations

If more than 10 words are a must

Use wild card for ignored words – the, a, 5w 1h etc to have more words

> 10 words within the query are ignored
* Avoiding * 10-word limitation *

And I'm Always There

play squash

play and squash

and play and squash

play squash and
Now, try this… +the **

Search Types

General Search
- Not cAsE seNSitiVE
- No more than 10 keywords in a search
- Google ignores “a”, 5w1h, this, to, we
- AND is always implied
- Date of birth of Hugh Jackman

Phrase Search
- “Use quotes”
- Use + to force a term and – to exclude
- No space follows these signs
- See the SERPs for with and without quotes
PHRASE SEARCH

“More shrewd searches”

“Is there a difference?”

travel spots in Malaysia

About 8,870,000 results (0.31 seconds)  8.8 Million Results!

Ad related to travel spots in Malaysia

EGOLAND® Malaysia - Malaysia’s 1st International Theme Park
www.egoland.com/
Book Your Tickets Online Now!

“travel spots in Malaysia”

About 2,060 results (0.33 seconds)

travel - Where are good photography spots in Malaysia ...
photo.stackexchange.com/q/119240
November 1, 2012 - Aweopol has a list of travel spots in Malaysia, with photos from Flickr (so it can help visualize what kind of photos you can make). Malaysia
Force The Plus, Exclude The Minus

OR vs. AND
OR | or

A quick Recap

Operators

• Logical
  • OR – case sensitive

• Mathematical
  • + (must) and – (not) have special meaning

• No Stemming
  • OK: “It’s the end of the * as we know it”
  • KO: “American Psycho**” – wont give psychology or psychophysics
  • * represents a word, not the completion of a word
  • Period is a single character wild card

• Let’s try some
Intitle: starwest

inurl: starwest

Intext: starwest

Inanchor: starwest
Let's try one query:

http://www.google.com/#q=100000000..999999999+filetype:sql
Advanced Operators contd...

Try a space between the operator and the term and see the results count

More Advanced Operators
- Numrange:
- Daterange:
- Site:
- Related:
- Cache:
- Link:

Till now, we searched...

From now, we Hacked

B451c
Phr453
0p3r4t0r5

Fr0m n0w, w3 H4ck
So What?

- What can a hacker do with this info?
  - Go to [http://www.cvedetails.com](http://www.cvedetails.com)
  - Check vulnerabilities for Apache 2.2.16
  - Trigger Metasploit
Linux server installer files are obtained from
Files on AOL server.

Files on MIT server.

Query is: Intitle:index.of name size
Check out the site hypem.com in SERPS

Try directory traversal from any page, you can
download tons of music!

Their business is selling music online!
Our Learning Till Now...

Directory Listings

Show server version information

Useful for an attacker

\texttt{intitle:index.of server.at site:aol.com}

Finding Directory Listings

\texttt{intitle:index.of "parent directory"}

Piracy – MP3s

- \texttt{intitle:index.of mp3 jackson AND iso kaspersky}

Remember, Google stems!

<table>
<thead>
<tr>
<th>Index of /music/Michael Jackson</th>
<th>Index of /Soft_all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>ABBYY FineReader 9.0</td>
</tr>
<tr>
<td>ADOBE</td>
<td>Acrobat</td>
</tr>
<tr>
<td>Browser</td>
<td>CleanMem 2.3.0 (dimims.com).exe</td>
</tr>
<tr>
<td>CoreDraw Portable</td>
<td>DII Meter</td>
</tr>
<tr>
<td>DirectX</td>
<td>Diskkeeper 2011_Enterprise_Server_15.0.641.0_Final.632.cab</td>
</tr>
<tr>
<td>DJVu Soft</td>
<td>Download manager</td>
</tr>
<tr>
<td>File Format Converters.exe</td>
<td>FileType XP 4.1.2.1</td>
</tr>
<tr>
<td>GENUINE ADVANTAGE VALIDATION/</td>
<td>ItaloView</td>
</tr>
<tr>
<td>Kaspersky Anti-Virus/</td>
<td>Nero</td>
</tr>
<tr>
<td>Norton AntiVirus</td>
<td>Symantec Norton/</td>
</tr>
</tbody>
</table>
Piracy – MP3s

- `intitle:index.of mp3 jackson`
  - Yields 20+ pages of songs in mp3 format
  - No need to wait for website instructions!
  - Remember, Google stems!

- `intitle:index.of iso kaspersky`
  - Gets the AV installers from various websites
  - Most of them with professional key or cracks
  - Even beta versions are available

More Piracy – ISO

- `inurl:microsoft intitle:index.of filetype:iso`
  - Get MS ISO files from everywhere!
Johnny’s Disclaimer

“Note that actual exploitation of a found vulnerability crosses the ethical line, and is not considered mere web searching.”

Listing all the index pages...

Each of these pages can be hacked since the hacker knows the version and type for the App Server, Database & the Web Server.
Listing all the subdomains

HR Intranet with details on...

Some details a hacker gets from here:

- HR Forms and Policies
- New Staff Info
- Consultation
- Health Benefits
- Salary packaging
- Contact Person
- Office and Meeting Room Layout
- Emails and Phones
- Training
- Pay Calculation
PuTTY SSH Logs with juicy info

Web
Images
Maps
Shopping
More

PuTTY logs
https://2000lcl07.localhost/repo/attachment/20435/putty.log
PuTTY log 2011-05-13 10:32:45 and
PuTTY log 2011-05-15 10:32:45
Using username "admin"
Authenticating with public key "imported-generated-key"
SSH: keycheck done, next

Usernames and Passwords

Results here: d:\official\white papers\starwest2013\uname-pwd.xls
And uname-pwd2.xls
SQL Injectable Websites

The first query brought 38K results.

Just by reordering, we got 3.3 Mil in lesser time!

Each of these can be hacked with SQLI and all these are just PHP!

Our Learning Till Now...

Combining operators does the magic

Inurl:microsoft.com -inurl:www.microsoft.com

Inurl:intranet intitle:intranet +intext:”human resource”

Filetype:log username putty

inurl:admin intext:username= AND email= AND password= OR pass= filetype:xls

intitle:index.of inurl:admin

“Filetype:php inurl:id=”
Database Querying

This also enumerates all the tables via the SQL. So you know the connection details, IP and the tables!

Query to get mySQL connection details

Login, Password, Website – All in One!

The Query: filetype:xls "username | password"

One of the results on page 1:
http://teachersites.schoolworld.com/.../files/teachers%20passwords.xls

Number of results: 46500
Login, Password, Website – All in One!

The Query: filetype:xls "username | password"

One of the results on page 1:
http://teachersites.schoolworld.com/.../files/teachers%20passwords.xls

Number of results: 46500

A Quick Q

What do you think this query does?

inurl:"passes" OR inurl:"passwords" OR inurl:"credentials" -search -download -techsupt -git -games -gz -bypass -exe filetype:txt @yahoo.com OR @gmail OR @hotmail OR @rediff
Our Learning Till Now...

“filetype:phps mysql_connect”

filetype:xls "username | password"

inurl:"passes" OR inurl:"passwords" OR inurl:"credentials" -search -download -techsupt -git -games -gz -bypass -exe filetype:txt @yahoo.com OR @gmail OR @hotmail OR @rediff

NOT BORED YET?

Let's dig in some more!

Innovation for Life™
Which sites have been hacked?

All hacked sites have a `r00t.php`

inurl:`"r00t.php"

The Logs might help

Checking hacked website logs for more info

allintext:`"fs-admin.php"`
Must Tries

Hacked websites → inurl:”r00t.php”
Hacked logs → allintext:”fs-admin.php”
Finding login for portals → intitle:admin intitle:login
SSH usernames → filetype:log username putty
Getting user list → Inurl:admin inurl:userlist
Passwords! → filetype:pass pass intext:userid
SQL Passwords → filetype:sql password
Usernames → inurl:admin filetype:xls
Passwords → inurl:password filetype:xls
More!! → inurl:passwd filetype:xls (pdf, doc, mdb)

More Stuff!

intitle:"Index of" passwords modified
allinurl:auth_user_file.txt
"access denied for user" "using password"
"A syntax error has occurred" filetype:ihtml
allinurl: admin mdb
"ORA-00921: unexpected end of SQL command“
inurl:passlist.txt
"Index of /backup“
"Chatologica MetaSearch" "stack tracking:"
**Listings of what you want**

Change the word after the parent directory to what you want

- "parent directory " **DVDRip** -xxx -html -htm -php -shtml
  - opendivx -md5 -md5sums

- "parent directory " **Xvid** -xxx -html -htm -php -shtml
  - opendivx -md5 -md5sums

- "parent directory " **Gamez** -xxx -html -htm -php -shtml
  - opendivx -md5 -md5sums

- "parent directory " **MP3** -xxx -html -htm -php -shtml
  - opendivx -md5 -md5sums

- "parent directory " **Name of Singer or album** -xxx -html -htm -php -shtml -opendivx -md5 -md5sums

---

**CGI Scanner**

Google can be used as a CGI scanner.

The `index.of` or `inurl` searches are good tools to find vulnerable targets. For example, a Google search for this:

```
allinurl:/random_banner/index.cgi
```

Hurray! There are only four now... the broken random_banner program will cough up any file on that web server, including the password file...
**Passwords**

“# -FrontPage -inurl:service.pwd”

FrontPage passwords, very nice clean search

results listing:

“AutoCreate=TRUE password=*”

This searches the password for “Website Access Analyzer”, a Japanese software that creates web statistics. For those who can read Japanese, check out the author’s site at:

http://www.coara.or.jp/~passy/

“http://*:*@www” domainname

“http://*:*@www” gamespy or http://*:*@www”gamespy

Another way is by just typing:

“http://bob:bob@www”

---

**More Passwords – IRC and Access**

“sets mode: +k”

This search reveals channel keys (passwords) on IRC as revealed from IRC chat logs.

eggdrop filetype:user user

These are eggdrop config files. Avoiding a fullblown discussion about eggdrops and IRC bots, suffice it to say that this file contains usernames and passwords for IRC users.

allinurl: admin mdb

Not all of these pages are administrator’s access databases containing usernames, passwords and other sensitive information, but many are!
MySQL Passwords & ETC directory

intitle:"Index of" config.php

This search brings up sites with "config.php" files. To skip the technical discussion, this configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database.

intitle:index.of.etc

This search gets you access to the etc directory, where many, many, many types of password files can be found. This link is not as reliable, but crawling etc directories can be really fun!

Passwords in backup files

filetype:bak
inurl:"htaccess|passwd|shadow|htusers"

This will search for backup files (*.bak) created by some editors or even by the administrator himself (before activating a new version). Every attacker knows that changing the extension of a file on a web server can have ugly consequences.
Serial Numbers

Let's pretend you need a serial number for Windows XP Pro.

In the Google search bar type in just like this - "Windows XP Professional" 94FBR the key is the 94FBR code.. it was included with many MS Office registration codes so this will help you dramatically reduce the amount of 'fake' sites (usually pornography) that trick you. Or if you want to find the serial for WinZip 8.1 -

"WinZip 8.1" 94FBR

Credit Cards!!

Number Ranges to find Credit Card, SSN, Account Numbers

<table>
<thead>
<tr>
<th>Numbers</th>
<th>Amex: (15 digits)</th>
<th>300000000000000..399999999999999</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MC: (16 digits)</td>
<td>5178000000000000..517899999999999</td>
</tr>
<tr>
<td></td>
<td>Visa: (16 digits)</td>
<td>4356000000000000..435699999999999</td>
</tr>
</tbody>
</table>
Working Samples!

Credit Cards

--- Welcome to all of you in my service.
--- I save my site in CQV + 10 = direction on fixed words.
--- And I have unlimited many software makes good money.
--- Example:
  - Software for the bug and NSX kit in the Western Union.
  - Version: 1.1.1.3 (new update)
  - Software to open the balance in PayPal and Bank Connection
  - I did not sell well for my eldest, and my familiarity
  - I order more than 100 or daily + CVV.
  - There are all kinds of IC + CVV:
    Class, Basketook, Master, Master, fed, esp, full details
    Period: 10000 + + Rich valid still balance good price
  - And I have all kinds of about right track 1 / 2 fresh.

--- If you are a serious buyer, please add my Yahoo ID and contact me
--- I will tell Yahoo to take USPS still shipping
--- bbb_078
--- My Yahoo Message: ben winger
--- E-Mail: ben_jenny@yahoo.com
--- WWW: bwiner.com
--- Credit Cards-Pastebin.txt
--- 36

Some More Working Samples...

Credit Cards-Pastebin.txt
The first query produced 3000+ results!

Let's click on one of the SERPS

You can control the camera

Pan, scan, tilt & zoom

Many more queries possible for CCTV

inurl:LvAppl intitle:liveapplet

inurl:"viewerframe?mode=motion"

intitle:"Live View / - AXIS"

intitle:"snc-rz30 home"

inurl:indexFrame.shtml "Axis Video Server"

So where is the database?

http://www.exploit-db.com/google-dorks/
OK, I’M CONVINCED

So, how do I secure myself?

Securing ourselves from Google Hackers

Keep your sensitive data off the web!

- Even if you think you’re only putting your data on a website temporarily, there’s a good chance that you’ll either forget about it, or that a web crawler might find it. Consider more secure ways of sharing sensitive data, such as SSH/SCP or encrypted email.
- A proper robots.txt file to instruct Google to skip sensitive directories.
- Captcha for forms helps ensure Google doesn’t index those forms and reports.
SOME ADDITIONAL INFO

To Inspire You To Be A Security Tester

BHDB

BHDB – Bing Hacking Database and how is it different from GHDB
How Vulnerability Scanners work

Scanner Limitations

- If the DB doesn’t have it, it won’t detect it – purely signature based
- Authentication by scanner is not trust-worthy
- Lacks IDS detection bypass
- No realistic fuzzing possible
- Can’t replace manual SQL Injection
- No intelligence in detecting attack vectors and surfaces
- Working with custom apps is a limitation
- Can identify points of weakness but can’t anticipate complex attack schemes
- Can’t handle asynchronous & offline attack vectors
- Limitations should be clearly understood
- Can’t detect logic flaws, weak cryptographic functions, information leakage etc
WHERE DO ACTUAL HACKS COME FROM

So, who are these hackers?

Real-life hacker categories

Career Hackers
- Hack websites
  - Steal Credit Cards
  - Financial Gain
- Anonymous, LulzSec
- Greater Good & Political drive
  - Want to have fun, mainly kids/young adults

Hacktivists
- Government-sponsored
  - 21st Century Warfare
- Hackers hired in underground forums

Nation states
THE TAKE-AWAY

Top Simple Security Searches that Work!

Queries

Combine searches with “site:” operator

Intitle:index.of → Leads to a direct hack

intitle:intranet | help.desk

Filetype:xls username OR password

Inurl:admin inurl:userlist
More Queries...

Inurl:admin OR inurl:password filetype:xls (csv)

Inurl:lvappl Live Applet site:*.*

inurl:intranet intitle:intranet +intext:"human resources"

Filetype:log username putty

So where is the GH “database”?

Top Ten Searches PDF (http://tinyurl.com/starwestghdb2013)
Search API OS Script

Google Web Search API Wsdl deprecated

Now Custom Search APIs used

Google controls the use: https://developers.google.com/web-search/terms

Open source script: http://pastebin.com/uE5wJWMy

1. Download the script 2. Rename as JS 3. Create data file 4. Call in any HTML

http://www.exploit-db.com/google-dorks/

Tools within OS Systems

Open Source penetration testing platforms such as Backtrack and Kali support tools for Google hacking. They are:

- Exploit-DB
- Searchsploit
- Goodork
- Websploit
- Social Engineering Toolkit
- Burp Suite (decoder)
So...

Can You We Hack

Before the Hacker Does?

MIMOS PORE

About the Presenter

Kiran or Kk
Handle – WTH4CK
Certifications:
Certified Ethical Hacker (CEH)
Security Tube Metasploit Framework (SMFE)
OSSTMM Professional Security Tester Accredited Certification (OPST)
http://www.isoc.my/profile/WTHack/