



T23

Concurrent Class

10/3/2013 3:00:00 PM

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

Presented by:

**Kiran Karnad
Mimos Berhad**

Brought to you by:



340 Corporate Way, Suite 300, Orange Park, FL 32073
888-268-8770 · 904-278-0524 · sqinfo@sqe.com · www.sqe.com

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.



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

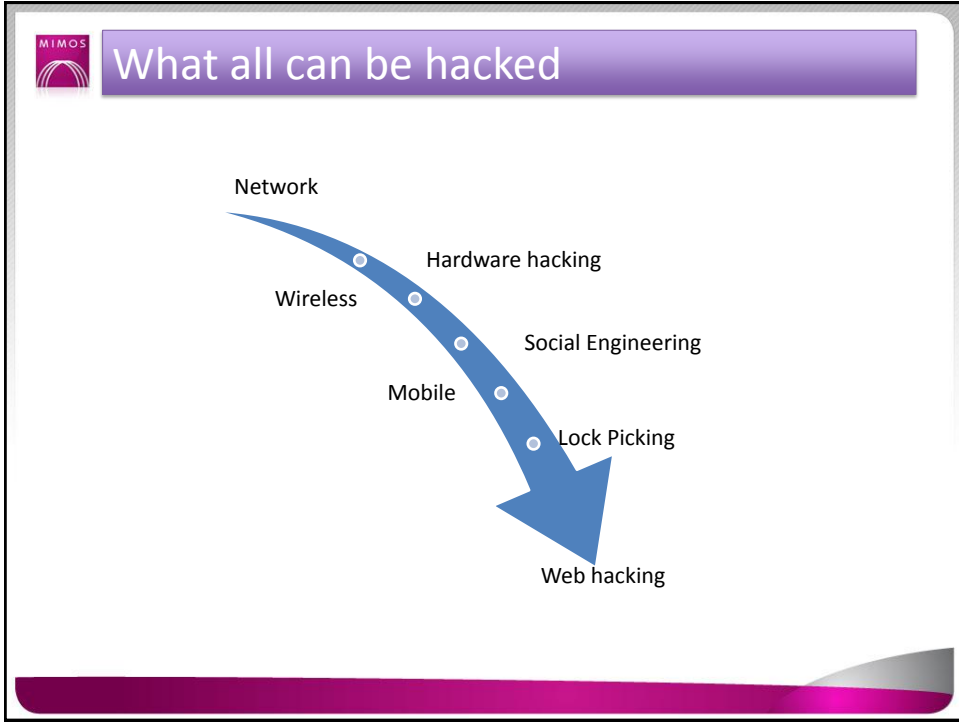


In the Recent Past



If you are not hacked, you are not important!

It you are not hacked, you are not important!



MIMOS

OS INT

What you don't know might hurt...

Innovation for Life™

MIMOS OSINT – Let's define

Intelligence collected from public sources

OSINT Communities

- Google
- Social Engines
- Details on next slide

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

MIMOS OSINT – Some methods

```

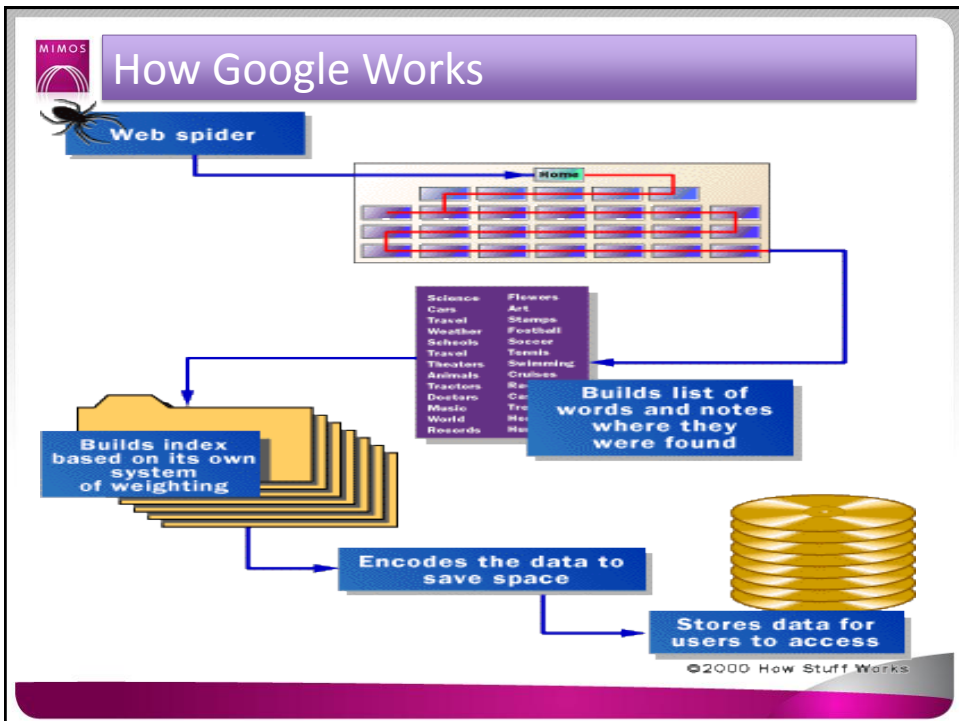
    graph TD
      Facebook[Facebook] --- Mobistealth[Mobistealth]
      JobsDB[Jobs DB] --- Spokeo[Spokeo]
      Spokeo --- ReconNg[Recon-ng]
      ReconNg --- GHDB[GHDB]
      Mobistealth --- SocialEng[Social Engineering]
      SocialEng --- StackOverflow[StackOverflow]
      Shodan[Shodan] --- StackOverflow
      StackOverflow --- GHDB
  
```

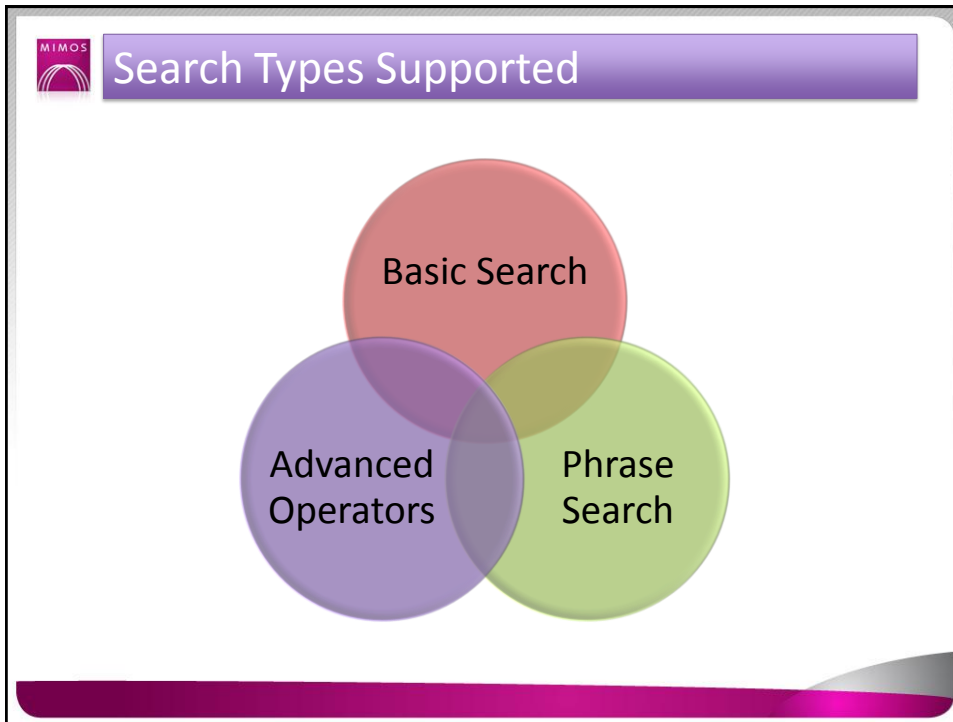


GOOGLE HACKING

It's what you expose

Innovation for Life™





MIMOS

BASIC SEARCH

The most used type of search

Innovation for Life™

A slide with a white background and a large purple and grey wave graphic at the bottom. The MIMOS logo is in the top left. The text 'BASIC SEARCH' is in large, bold, white letters. Below it, the text 'The most used type of search' is in a smaller white font. The 'Innovation for Life™' logo is in the bottom right corner.

MIMOS So InSenSitiVe

Starwest 2013

Web Images Maps Shopping More Search tools

About 1,590,000 results (0.38 seconds)

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

stARwEST 2013

Web Images Maps Shopping More Search tools

About 1,590,000 results (0.38 seconds)

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

MIMOS 5W 1H – Google doesn't mind

when did the monkey cross the road

Web Images Maps Shopping Videos More Search tools

About 205,000,000 results (0.48 seconds)

where did the monkey cross the road

Web Images Maps Shopping Videos More Search tools

About 205,000,000 results (0.62 seconds)

what did the monkey cross the road

Web Images Maps Shopping Videos More Search tools

About 205,000,000 results (0.61 seconds)

how did the monkey cross the road

Web Images Maps Shopping Videos More Search tools

About 205,000,000 results (0.54 seconds)

MIMOS Mark my Ten Words, that's it

can I use nmap to find out if a network has any vulnerabilities which can be exposed?

can I use nmap to find out if a network has any vulnerabilities which can be

Web Images Maps Shopping More Search tools

About 1,060,000 results (0.57 seconds)

41.2 Vulnerability Assessment - CentOS
www.centos.org/docs/5/html/Deployment_Guide.../ch-sec-access.html

using nmap for network vulnerabilities

Web Images Maps Shopping Videos More Search tools

About 38,900 results (0.32 seconds)

Ad related to using nmap for network vulnerabilities

15 words in this query

Using 5 words

MIMOS 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 *

we the people of the united states in order to form a more perfect union est

Web Images Maps Shopping Videos More Search tools

About 2,170,000 results (0.45 seconds)

More than 15 words

we * people * * united states * order * form * more perfect *

Web Images Maps Shopping Videos More Search tools

About 1,980,000,000 results (2.68 seconds)

Using * to accommodate more

And I'm Always There

play squash

Web Images Maps Shopping News More Search tools

About 45,500,000 results (0.36 seconds)

play and squash

Web Images Maps Shopping News More Search tools

About 45,000,000 results (0.28 seconds)

and play and squash

Web Images Maps Shopping News More Search tools

About 45,000,000 results (0.37 seconds)

play squash and

Web Images Maps Shopping News More Search tools

About 45,000,000 results (0.34 seconds)

MIMOS

Now, try this... +the * *

+the * *

Web Images Maps Shopping News More Search tools

About 11,860,000,000 results (0.36 seconds)

[The Sun | The Best for News, Sport, Showbiz, Celebrities | The Sun](#)
www.thesun.co.uk/

Get the latest news and features at The Sun - Showbiz, babes, celebrities, sport and racing, national and international news. Check out the best pictures, videos, ...

[The Weather Network: Current Weather - Canadian, US, and ...](#)
www.theweathernetwork.com/

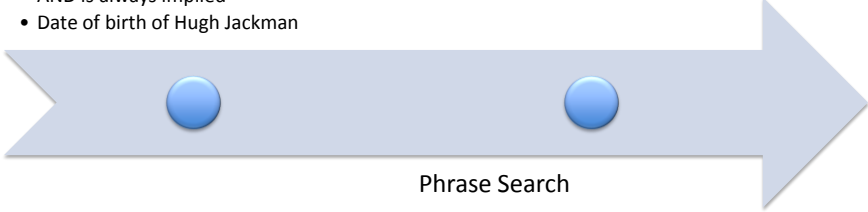
Provides current observations and forecasts for hundreds of cities in Canada, weather warnings, and seasonal reports.

MIMOS

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”

Innovation for Life™



“Is there a difference?”

travel spots in Malaysia

Web Images Maps Shopping Videos More Search tools

About 8,870,000 results (0.31 seconds)

8.8 Million Results!

Ad related to travel spots in Malaysia ⓘ

[LEGOLAND® Malaysia - Malaysia's 1st International Theme Park](#)
www.legoland.com/
Book Your Tickets Online Now!

“travel spots in Malaysia”

Web Images Maps Shopping More Search tools

About 2,060 results (0.33 seconds)

[travel - Where are good photography spots in Malaysia...](#)
photo.stackexchange.com/.../where-are-good-photography-spots-in-mala...
Nov 1, 2012 - Awespot 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.

MIMOS Force The Plus, Exclude The Minus

Kiran Karnad

Web Images Maps Shopping More Search tools

About 195,000 results (0.30 seconds)

Kiran +Karnad

Web Images Maps Shopping More Search tools

About 21 results (0.18 seconds)

Kiran -Karnad

Web Images Maps Shopping Blogs More Search tools

About 94,000,000 results (0.26 seconds)

"Kiran Karnad"

Web Images Maps Shopping More Search tools

About 1,830 results (0.15 seconds)

MIMOS OR vs. AND

hot and spicy

Web Images Maps Shopping News More Search tools

About 51,200,000 results (0.26 seconds)

hot OR spicy

Web Images Maps Shopping News More Search tools

About 5,050,000,000 results (0.31 seconds)

hot spicy

Web Images Maps Shopping News More Search tools

About 39,800,000 results (0.44 seconds)

MIMOS

OR | or

ferrari **or** lamborghini

Web Images Maps Shopping More Search tools

About 137,000,000 results (0.37 seconds)

[Ferrari vs Lamborghini - Difference and Comparison | Diffen](#)
www.diffen.com/difference/Ferrari_vs_Lamborghini

Ferrari vs Lamborghini comparison. This is a comparison of the styles (including pictures), performance, power, popularity and cost of Ferrari and Lamborghini

ferrari **OR** lamborghini

Web Images Maps Shopping News More Search tools

About 548,000,000 results (0.32 seconds)

[Automobili Lamborghini S.p.A.](#)
www.lamborghini.com/

Official website of Automobili Lamborghini S.p.A. Since 1963, Italian luxury and super sports cars maker. Sant'Agata Bolognese, Bologna, Italy.

MIMOS


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:

 **intitle:**


 

[Web](#) [Images](#) [Maps](#) [Shopping](#) [More ▾](#) [Search tools](#)

About 39,200 results (0.21 seconds)

[STARWest | starwest.techwell.com/ ▾](#)
 STARWEST is the premier event for software testers and quality assurance professionals—covering all your testing needs with 100+ learning and networking ...

inurl:




[Web](#) [Images](#) [Maps](#) [Shopping](#) [More ▾](#) [Search tools](#)

About 32,100 results (0.28 seconds)

[STARWest | starwest.techwell.com/ ▾](#)
 STARWEST is the premier event for software testers and quality assurance professionals—covering all your testing needs with 100+ learning and networking ...

intext:

 **intext:**

[Web](#) [Images](#) [Maps](#) [Shopping](#) [More ▾](#) [Search tools](#)

About 148,000,000 results (0.37 seconds)

[STARWest | starwest.techwell.com/ ▾](#)
 STARWEST is the premier event for software testers and quality assurance professionals—covering all your testing needs with 100+ learning and networking ...

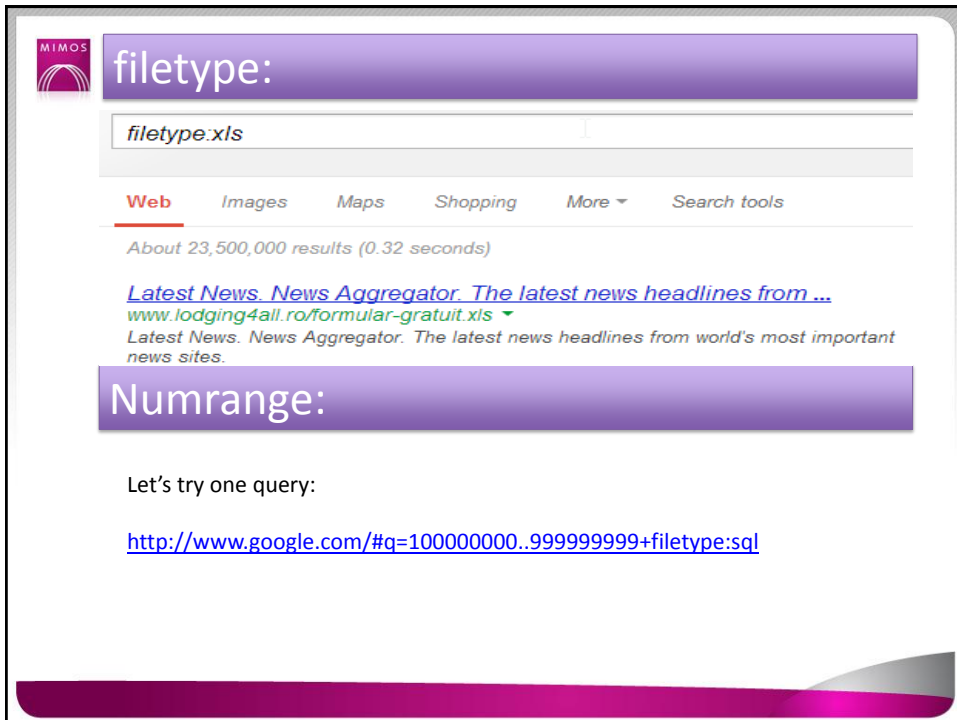
[Bulk Herbs, Organic Herbs, Spices, Loose Tea & Essential Oils ...](#)

Inanchor:

[Web](#) [Images](#) [Maps](#) [Shopping](#) [More ▾](#) [Search tools](#)

About 504,000 results (0.22 seconds)

[STARWest | starwest.techwell.com/ ▾](#)
 STARWEST is the premier event for software testers and quality assurance professionals—covering all your testing needs with 100+ learning and networking ...



MIMOS

filetype:

`filetype:xls`

[Web](#) [Images](#) [Maps](#) [Shopping](#) [More ▾](#) [Search tools](#)

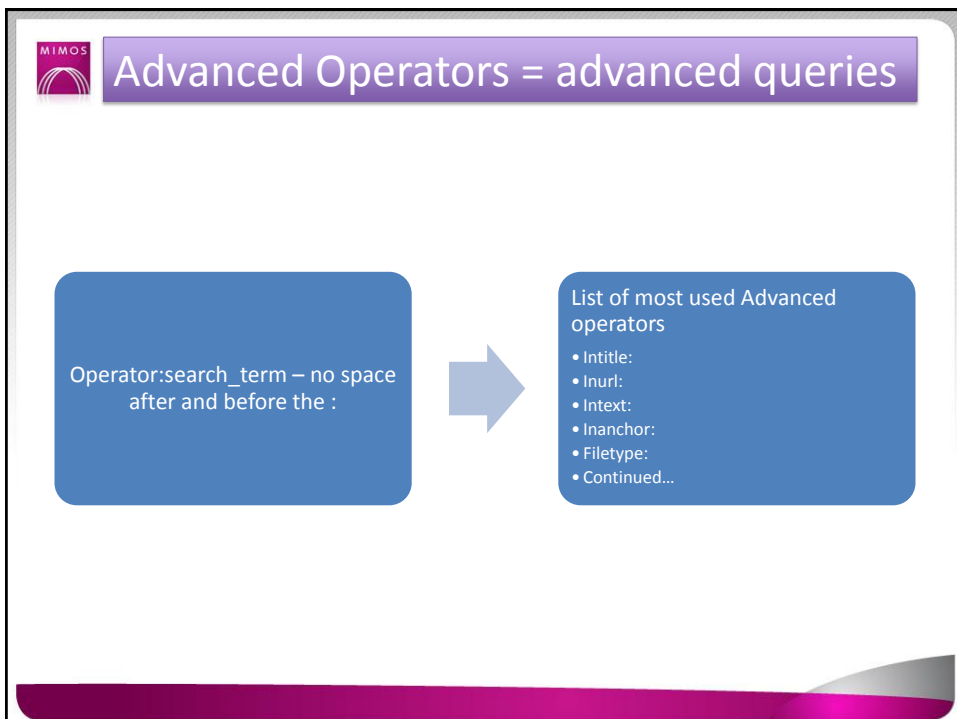
About 23,500,000 results (0.32 seconds)

[Latest News. News Aggregator. The latest news headlines from ...
www.lodging4all.ro/formular-gratuit.xls ▾](#)
Latest News. News Aggregator. The latest news headlines from world's most important news sites.

Numrange:

Let's try one query:

<http://www.google.com/#q=100000000..999999999+filetype:sql>



MIMOS

Advanced Operators = advanced queries

Operator:search_term – no space after and before the :

→

List of most used Advanced operators

- Intitle:
- Inurl:
- Intext:
- Inanchor:
- Filetype:
- Continued...

MIMOS **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:

MIMOS **T1ll n0w, w3 534Rch3d...**

B451c
Phr453
Op3r4t0r5

↓

Fr0m n0w, w3 H4ck

MIMOS Intitle:index.of server.at

Index of /

Name	Last modified	Size	Description
1.2/	13-Oct-2008 22:47	-	
1.4/	24-Jun-2013 02:00	-	
1.5/	09-Sep-2009 13:47	-	
1.6/	24-Jun-2013 02:02	-	
1.7/	29-Mar-2010 01:00	-	
1.8/	16-Jul-2013 09:00	-	
1.9/	16-Jul-2013 09:01	-	
1.10/	16-Jul-2013 09:01	-	
1.11/	16-Jul-2013 09:01	-	
trunk/	16-Jul-2013 09:02	-	

Apache/2.2.16 (Debian) Server at addons.wesnoth.org Port 80

Directory Listings

Web Server details obtained.

MIMOS So What?

- What can a hacker do with this info?
 - Go to <http://www.cvedetails.com>
 - Check [vulnerabilities for Apache 2.2.16](#)
 - Trigger Metasploit

Apache • Http Server • 2.2.16: Security Vulnerabilities

Can Name CVE ID First Exploit Vulnerability Type(s) Public Date Update Date Score Gained Access Level Access Complexity Authentication Conf. Integ Avail.

#	CVE ID	CVE ID	First Exploit	Vulnerability Type(s)	Public Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ	Avail.
1	CVE-2013-0169	CVE-2013-0169	DoS	DoS	2013-07-10	2013-07-11	4.3	None	Remote	Medium	Not required	None	None	Partial
2	CVE-2013-0168	CVE-2013-0168	DoS	DoS	2013-06-05	2013-06-05	5.0	None	Remote	High	Not required	Partial	Partial	Partial
3	CVE-2013-0168	CVE-2013-0168	DoS	DoS	2013-06-05	2013-06-05	5.0	None	Remote	High	Not required	Partial	Partial	Partial
4	CVE-2013-0167	CVE-2013-0167	DoS	DoS	2013-01-30	2013-01-30	5.0	None	Remote	Low	Not required	None	None	Partial
5	CVE-2012-2489	CVE-2012-2489	DoS	DoS	2012-10-26	2012-10-26	4.3	None	Remote	Medium	Not required	None	None	Partial

```
meterpreter > shell
[*] 172.16.30.229:49262 PROPFIND /documents/cmd.exe
[*] 172.16.30.229:49262 PROPFIND => 404 (/documents/cmd.exe)
Process 3448 created.
Channel 1 created.
\\172.16.30.16\documents\
CMD.EXE was started with the above path as the current director
UNC paths are not supported. Defaulting to Windows directory.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

MIMOS Intitle:index.of server.at site:aol.com

- Linux server installer files are obtained

ubuntu-mtc-a.evip.aol.com/pool/universe/g/gimp-resynthesizer/

Getting Started CVE security vulnera... Talks - gta2011 MSM Self Service - L... Kisamak Adr

Index of /pool/universe/g/gimp-resynthesizer

Name	Last modified	Size	Description
Parent Directory	-	-	-
gimp-resynthesizer_0.15-2build2.diff.gz	08-Sep-2007 09:03	2.9K	
gimp-resynthesizer_0.15-2build2.dsc	08-Sep-2007 09:03	653	
gimp-resynthesizer_0.15-2build2_amd64.deb	08-Sep-2007 10:03	22K	

Files on AOL server.

www.ai.mit.edu/projects/

Getting Started CVE security vulnera... Talks - gta2011 MSM Self Service - L...

Index of /projects

Name	Last modified	Size	Description
Parent Directory	-	-	-
BEAM	18-Jan-2005 15:50	-	-
HIE	30-Sep-2004 11:19	-	-
IV	03-Mar-2000 23:30	-	-
ImmersiveVideo	03-Mar-2000 23:30	-	-
NTTCollaboration	08-Dec-1999 18:31	-	-

Files on MIT server.

MIMOS Hyped Music

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

hypem.com/download/M/Maal/Nobody%27s_Sayin%27/

Getting Started CVE security vulnera... Talks - gta2011 MSM Self Service - L... Kisamak Admin Imported From Firf...

Index of /download/M/Maal/Nobody%27s_Sayin%27/

Name	Last modified	Size	Description
Parent Directory	-	-	-
01-maal-nobodvs_savin_floft_17a_1an_club_mxl...>	16-Jul-2013 02:29	4.4M	
02-maal-nobodvs_savin_floft_17a_1an_dubl.mp3	16-Jul-2013 02:35	3.6M	
03-maal-nobodvs_savin_floft_17_vs_srefano_maal...>	16-Jul-2013 02:41	2.2M	
04-maal-nobodvs_savin_floft_17_vs_srefano_maal...>	16-Jul-2013 02:47	3.2M	

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

hypem.com/popular

Getting Started CVE security vulnera... Talks - gta2011 MSM Self Service - L... Kisamak Admin Imported From Firf... Security


HYPE MACHINE Latest Popular Premieres Genres Blogs Spy ...

Dan Croit - In/Out Head Four...

HYPE MACHINE TEES AR

Every day, thousands of people around the world write about music they love — and it all e
Join us and find new music worth listening to. Also available on the iPhone and Andrc

Their business is selling music online!



Our Learning Till Now...

Directory Listings


Show server version information

Useful for an attacker `intitle:index.of server.at`

`intitle:index.of server.at site:aol.com`

Finding Directory Listings `intitle:index.of "parent directory"`

`intitle:index.of name size`



Piracy – MP3s

- `intitle:index.of mp3 jackson AND iso kaspersky`
- Remember, Google stems!

Index of /music/Michael Jackson

[Enable Image Thumbnails](#)

Name	Last modified	Size
Parent Directory	2012-JAN-03 16:38:31	0
01 - Michael Jackson - Hold My hand (i...)	2012-JAN-03 16:45:58	4984K
02 Nobody (1).mp3	2010-MAY-01 21:42:15	2625K
04 - Heaven Knows I Love You.mp3	2011-NOV-24 20:54:11	7M
06 - Michael Jackson - Beat of lov (p...)	2012-JAN-03 16:45:16	4234K
08 I Can't Help It.mp3	2011-NOV-24 20:41:05	6M
08 Speechless.mp3	2010-NOV-29 22:16:12	4658K
09 - Michael Jackson - Behind the Mas...)	2012-JAN-03 16:47:00	7M
09 Who Ya It.mp3	2011-NOV-24 20:53:07	6M
10 - Billie Jean.mp3	2011-NOV-24 21:04:24	6M
10 - Michael Jackson - Much too soon...)	2012-JAN-03 16:47:45	3487K
104-michael_jackson-on_the_line-music...)	2010-MAY-03 17:15:05	7M
Ruth Song-Michael Jackson.mp3	2010-NOV-30 06:07:30	6M
Human Nature-Michael Jackson.mp3	2011-NOV-24 20:44:25	4107K
Instrumental Liberty Girl-Michael Jac...)	2010-APR-27 06:32:56	2164K
Instrumental-Stranger in Moscow-Micha...)	2010-APR-27 06:32:56	2423K
Jackson 5 - I Want You Back (Instrume...)	2010-JUN-13 06:22:24	4239K
Just Can't Stop Loving You-Michael Ja...)	2011-NOV-24 20:57:27	4144K
Michael Jackson - 80s Disco Mega mix.mp3	2009-JUN-26 12:43:49	8M

Index of /Soft_all

- [Parent Directory](#)
- [ABBYY FineReader 9.0/](#)
- [Adobe/](#)
- [Arhivatori/](#)
- [Browser/](#)
- [CleanMem 2.3.0 \(dimitech.net\).exe](#)
- [CorelDraw Portable/](#)
- [DU Meter/](#)
- [Dicton/](#)
- [Diskeeper_2011_Enterprise_Server_15.0.951.0_Final_632.rar](#)
- [DjVu Soft/](#)
- [Download menajer/](#)
- [File Format Converters.exe](#)
- [FlexType XP + kg/](#)
- [GENUINE ADVANTAGE VALIDATION/](#)
- [IrfanView/](#)
- [Kaspersky Anti-Virus/](#)
- [Nero/](#)
- [Nero... 00000 ...](#)



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!

Index of /microsoft/

Name	Last Modified	Size
Parent Directory/		-
6.0.6001.18000.387--KRM5DK_EN.iso	2010-Apr-20 11:46:33	1.3G
6001.18000.080118-1840-kb3a1k1_en.iso	2009-Jan-19 02:07:02	1.3G
7601.17514.101118-1850_Update_Sp_Wavel-GRMSP1.1_DVD.iso	2010-Nov-23 13:49:56	1.9G
OSDKK_Feb10.exe	2010-Feb-05 13:30:06	584.6M
DotNETFrameWorkx2.OSDK_Setup.exe	2005-Sep-24 06:59:12	354.0M
InstallDVD.iso	2010-Nov-10 22:14:26	4.0G
KB3AKK_EN.iso	2010-Mar-30 19:50:17	1.6G
NetFX64.exe	2005-Sep-24 01:15:25	45.2M
Office2003SP3-KB923618-Fullfile-ENU.exe	2008-Oct-15 10:56:15	117.6M
ProfessionalPlus.exe	2010-Apr-28 04:04:33	650.2M
VS2008ExpressENUX1397568.iso	2009-Nov-24 00:37:12	894.6M
VS2008ExpressWithSP1ENUX1504728.iso	2008-Jul-31 13:16:47	748.5M
VS2008ProfessionalTodayTrialENUX1438222.iso	2010-Jul-15 10:17:35	197.7M
VS2008SP1ENUX1512962.iso	2008-Aug-01 06:28:41	831.3M
VS2010Beta1ENU_VTS.iso	2009-May-11 23:40:13	2.2G
VS2010Beta1ENU_VSTS.iso	2009-May-09 06:31:44	1.2G
VS2010ProTrial_4PartTotal.part1.exe	2010-Mar-31 05:44:35	700.0M
VS2010ProTrial_4PartTotal.part2.rar	2010-Mar-24 16:36:22	700.0M
VS2010ProTrial_4PartTotal.part3.rar	2010-Mar-24 17:04:16	700.0M
VS2010ProTrial_4PartTotal.part4.rar	2010-Mar-24 17:08:55	92.6M
VS2010UltimTrial_4PartTotal.part1.exe	2010-Mar-31 05:44:33	700.0M
VS2010UltimTrial_4PartTotal.part2.rar	2010-Mar-25 03:55:27	700.0M
VS2010UltimTrial_4PartTotal.part3.rar	2010-Mar-25 04:25:44	700.0M
VS2010UltimTrial_4PartTotal.part4.rar	2010-Mar-25 04:33:11	183.0M
W2KSP4_EN.EXE	2009-May-28 23:50:05	129.2M
WS05_RTM_x86_EnterpriseVHD.exe	2008-Nov-05 11:37:38	1.4G
Windows6.0-KB936330-x64-wave0.exe	2008-Oct-15 11:44:17	726.5M
Windows6.0-KB936330-X86-wave0.exe	2008-Oct-15 10:54:46	434.5M
Windows6.0-KB948465-X64.exe	2010-Jan-17 11:19:35	577.3M
Windows6.0-KB948465-X86.exe	2009-Jul-12 14:41:06	348.3M
Windows8-ConsumerPreview-32bit-English.iso	2012-Feb-25 12:57:52	2.5G
Windows8-ConsumerPreview-64bit-English.iso	2012-Feb-25 11:22:59	3.3G
WindowsDeveloperPreview-32bit-English.iso	2011-Sep-10 12:03:28	1.8G
WindowsDeveloperPreview-64bit-English.iso	2011-Sep-10 12:45:09	3.6G
WindowsXP-KB936929-SP3-x86-ENU.exe	2008-Oct-15 10:51:38	316.4M
WindowsXP-KB937159-x86-ENU.exe	2008-Nov-14 01:53:42	803.8K
	2010-Jul-20 11:00:40	840.3K

MIMOS **Johnny's Disclaimer**

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

MIMOS **Listing all the index pages...**

intitle:index of inurl:admin

Web Images Maps Shopping More Search tools

About 967,000 results (0.30 seconds)

[Index of /admin - MIT](#)
web.mit.edu/admin/

Index of /admin. Name Last modified Size Description. [DIR] Parent Directory 20-Jun-2009 23:36 - [DIR] lggy/ 14-Sep-1997 20:04 - [DIR] assignments/ ...
You've visited this page 5 times. Last visit: 6/14/13

services/	07-Jun-2001 16:19	-
systems/	14-May-2004 01:13	-
windows/	25-Jun-2007 13:14	-
www/	23-Feb-2010 12:44	-

Apache/1.3.41 Server at web.mit.edu Port 80

xlt.php.jpg	01-Jun-2013 19:27	156k
xlt4.php.jpg	01-Jun-2013 20:01	156k
yes.php.jpeg	01-Jun-2013 20:18	260k

Proudly Served by LiteSpeed Web Server at www.bensaidgroup.com Port 80

MIMOS Listing all the subdomains

site.sqe.com -site:www.sqe.com unique

Web Images Maps Shopping More Search tools

8 results (0.12 seconds)

[PDF] Sample test plans - Brown & Donaldson
 bdonline.sqe.com/documents/testplans.pdf
 Dec 9, 2000 - will be analyzed to determine how many clients are using the Web site (target was for at 10,000 **unique** visitors per day) and how many of these ...

What's New Gram - Your weekly update about what's new on ...
 pub.sqe.com/content/WNG
 Jun 8, 2010 - @StickyMinds.com on Twitter Want to get a daily dose of what's new and popular on StickyMinds.com and in Better Software magazine? And ...

Game Testing - SQE.com
 forms.sqe.com/forms/12CPL136
unique game testing challenges—this white paper is for you. As with all customer-facing software, poorly tested games cause the user experience to suffer.

[PDF] Requirements - Brown & Donaldson
 bdonline.sqe.com/documents/requirements.pdf
 Dec 15, 2000 - Note, each page component on the "floorplan" will be assigned a **unique** # (typically ordered top- left to bottom-right), the supporting description ...

What's New Gram - Your weekly update about what's new on ...
 pub.sqe.com/content/WNG
 Jun 8, 2010 - @StickyMinds.com on Twitter Want to get a daily dose of what's new and popular on StickyMinds.com and in Better Software magazine? And ...

MIMOS HR Intranet with details on...

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

Web Images Maps Shopping More Search tools

About 19,300 results (0.26 seconds)

Human Resources | Staff Intranet
 intranet.mdhs.unimelb.edu.au/hr
 MDHS is a large and complex Faculty, geographically dispersed and with close relationships with a number of institutes and hospitals. The Faculty Human ...

MCAD Intranet Human Resources
 intranet.mcad.edu / Departments & Services
 Staff Lee Brucker Human Resources Assistant (612) 674-3770 lbrucker@mcad.edu.
 Rm M16. Staff Patty Heilm Human Resources Assistant (612) 674-3504

Human Resources - CLA Intranet - University of Minnesota
 cla.umn.edu/intranet/hr
 Jul 17, 2013 - Human Resources: Who Do I Contact in CLA HR? 2013/14 Deadlines in Faculty & Human Resources - OHR Manager's Toolkit - CLA NOW ...

Human Resources Intranet
 hr.intranet.unchealthcare.org/
 This section of the Human Resources website is for UNC Health Care employees only. Employees must enter their system user and password to continue.

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

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

SQL Injectable Websites

Filetype:php inurl:id=

Web Images Maps Shopping More Search tools

About 38,700 results (0.34 seconds)

[موقع مرور منطقة الرياض - filetype:php inurl:id= intitle:buy](#)
[www.rt.gov.sa/default_with_eid3banner.php?id=41439.shtml](#)
 Jul 18, 2013 - replica filetype:php inurl:id= intitle:buy - christian louboutin white satin wedding shoe online store, best christian louboutin rantus orlato star ...

[inurl:shop.php?id' - best PDFs Search engine. Free unlimited pdf...](#)
[www.gopdfs.com/inurl-shop.php?id'](#)

The first query brought 38K results

inurl.id= filetype:php

Web Images Maps Shopping More Search tools

About 3,300,000,000 results (0.21 seconds)

[Identification Cards - DMV.org](#)
[www.dmv.org/id-cards.php](#)
 Information for applying for a new state ID card - Steps for obtaining a new state ID car listed by state.

[ID Requirements - Peace Bridge](#)
[www.peacebridge.com/index.php?Itemid=743&id=57&option=...](#)
 Cross-Border Travel Identification Requirements: What is the Western Hemisphere

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

mysql_connect filetype:phps

Web Images Maps Shopping More Search tools

About 2,340 results (0.21 seconds)

[Twixel/includes/mysql_connect.php at master · GZanmiller · GitHub](#)
https://github.com/GZanmiller/Twixel/blob/master/.../mysql_connect.php...
[Twixel - The Repo for the DIG 4530 E-Commerce class assignment.](#)

[download the code - Adam Young](#)
adamyoung.net/files/dbdiff.php

```

... $src_tables = getTables($src); @CreateStatements($src, $src_tables); $dst =
mysql_connect($dst_host, $dst_user, $dst_pass); if (!$mysql_select_db($dst_db, ...

<?php
//for gmm-student
//$con = mysql_connect("gmm-student.fakem.utm.my", "YOUR-LOGIN-
$con = mysql_connect("localhost", "root", "");
if (!$con)
{
die("Could not connect: " . mysql_error());
}
mysql_select_db("wbt", $con);
$result = mysql_query("SELECT * FROM student");
?>
<!DOCTYPE html PUBLIC "-//W3C/DTD XHTML 1.0 Transitional//EN"
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-
<title>Untitled Document</title>
</head>
<body>
<table border="1">
<tr>
<th scope="col">Index</th>
<th scope="col">Fname</th>
<th scope="col">Matrlike</th>
<th scope="col">Name</th>

```

Query to get MySQL connection details

This also enumerates all the tables via the SQL

So you know the connection details, IP and the tables!

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>

Team Login ID/Username:TX4_22_22307,	Password: [REDACTED]5148	Allredge, Kimberly S
Team Login ID/Username:TX4_22_22308,	Password:RRIF1 [REDACTED]	Canastuj Tiu, Felipe Antonio
Team Login ID/Username:TX4_22_22309,	Password:[REDACTED]7011	Cross, Matthew C
Team Login ID/Username:TX4_22_22310,	Password:LGC [REDACTED]9	EFRAIM, LAIS
Team Login ID/Username:TX4_22_22300,	Password:[REDACTED]65	Eldridge, Darwin Laquahn
Team Login ID/Username:TX4_22_22301,	Password:QNA [REDACTED]24	Hanft, Lawrence Wolfaana
Team Login ID/Username:TX4_22_22302,	Password:[REDACTED]YA893	Hill
Team Login ID/Username:TX4_22_22303,	Password:MKV [REDACTED]29	Jor
Team Login ID/Username:TX4_22_22304,	Password:BR [REDACTED]207	Jue
Team Login ID/Username:TX4_22_22305,	Password:FGP [REDACTED]	Kir
Team Login ID/Username:TX4_22_22306,	Password:C [REDACTED]27312	Lar
Team Login ID/Username:TX4_22_22311,	Password:PDR [REDACTED]	Mo

Number of results: 46500


MIMOS 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>

Team Login ID/Username:TX4_22_ZZ307,	Password: [REDACTED]5148	Allredge, Kimberly S
Team Login ID/Username:TX4_22_ZZ308,	Password:RRIF1 [REDACTED]	Canastuj Tiu, Felipe Antonio
Team Login ID/Username:TX4_22_ZZ309,	Password:[REDACTED]7011	Cross, Matthew C
Team Login ID/Username:TX4_22_ZZ310,	Password:LGC [REDACTED]9	EFRAIM, LAIS
Team Login ID/Username:TX4_22_ZZ300,	Password:[REDACTED]65	Eldridge, Darwin Laquahn
Team Login ID/Username:TX4_22_ZZ301,	Password:QNG [REDACTED]324	Hanft, Lawrence Wolfaana
Team Login ID/Username:TX4_22_ZZ302,	Password:[REDACTED]YA893	Hill
Team Login ID/Username:TX4_22_ZZ303,	Password:MKV [REDACTED]29	Jordan
Team Login ID/Username:TX4_22_ZZ304,	Password:BR [REDACTED]107	Jules
Team Login ID/Username:TX4_22_ZZ305,	Password:FGP [REDACTED]	Kirby
Team Login ID/Username:TX4_22_ZZ306,	Password:C [REDACTED]27312	Larson
Team Login ID/Username:TX4_22_ZZ311,	Password:PDR [REDACTED]4	Moore

Number of results: 46500



MIMOS 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™

MIMOS Which sites have been hacked?

All hacked sites have a r00t.php

inurl:"r00t.php"







MIMOS The Logs might help

Checking hacked website logs for more info

allintext:"fs-admin.php"

allintext:"fs-admin.php"

Web Images Maps Shopping More Search tools

About 389,000 results (0.13 seconds)

[Index of /wp-content/plugins/forum-server/fs-admin](#)
[www.thecanyonsmusic.com/wp-content/plugins/forum_.../fs-admin/](#)
 Parent Directory: fs-admin.php fs-admin_pro.php wpf-addforum.php wpf-addgroup.php wpf-add-usergroup.php wpf-addusers.php wpf-edit-forum-group

[31-May-2010 05:03:55] PHP Fatal error: Call to a member function ...
[www.ceeds.us/wp-content/plugins/forum-server/fs-admin/error_log](#)
 ... show_errors() on a non-object in /home2/ceedsua/public_html/wp-content/...

```

plugins/forum-server/fs-admin/error_log
.0 05:03:55] PHP Fatal error: Call to a member function get_moderators() on a non-object in /home2/c
oderator.php on line 5
.0 05:04:12] PHP Fatal error: Call to a member function get_usergroup_name() on a non-object in /hom
admin/vpf-usergroup-edit.php on line 22
.0 05:04:28] PHP Fatal error: Call to undefined function __() in /home2/ceedsua/public_html/wp-conte
.0 05:04:53] PHP Fatal error: Call to undefined function __() in /home2/ceedsua/public_html/wp-conte
.0 05:05:18] PHP Fatal error: Call to a member function show_errors() on a non-object in /home2/ceed
bin.php on line 14
.0 05:12:32] PHP Fatal error: Call to a member function get_usergroups() on a non-object in /home2/c
ddusers.php on line 2
.0 05:01:21] PHP Fatal error: Call to a member function get_moderators() on a non-object in /home2/c
oderator.php on line 5
.0 05:16:07] PHP Fatal error: Call to a member function show_errors() on a non-object in /home2/ceed
bin.php on line 14
.0 11:22:47] PHP Fatal error: Call to a member function get_usergroup_name() on a non-object in /hom
admin/vpf-usergroup-edit.php on line 22
.0 03:11:32] PHP Fatal error: Call to undefined function __() in /home2/ceedsua/public_html/wp-conte
    
```




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 two 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:

This is a query to get inline passwords from search engines (not just Google), you must type in the query followed with the domain name without the .com or .net


Another way is by just typing

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

"http://*:*@www" domainname

"http://*:*@www" gamespy or http://*:*@www"gamespy

"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.

Not all of these pages are administrator's access databases containing usernames, passwords and other sensitive information, but many are!

allinurl: admin mdb




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

Numbers	Amex: (15 digits)	3000000000000000..399999999999999
	MC: (16 digits)	5178000000000000..5178999999999999
	Visa : (16 digits)	4356000000000000..4356999999999999

MIMOS Working Samples!

pastebin.com/raw.php?i=NMIkFgRn

Getting Started CVE security vulnera... Talks - gtac2011 MSM Self Service - L... Kisam

Please View : http://www.youtube.com/watch?v=ZSNF5gLV-mg

```

====> Welcome to all of you in my service.
====> I have my side CVV + cc + + discharge any track on the world
====> And I have unlocked many software makes good money
+ Example:
- Software for the bug and MITM slot in the Western Union.
* Version: 2.0.1.3 (new update)
- Software to open the balance in PayPal and Bank Connection
* I do not sell well for my client, and my familiarity
- I update more than 200 cc daily + CVV.
* There are all kinds of CC + CVV:
(Visa, MasterCard, AMEX, Discover, dob, ssn, full details)
Fresh + good + + + With valid high balance best price
- And I have all kinds of shock right track + 1 / 2 fresh
====> If you are a serious buyer, please add my yahoo ID and contact me
====> I just use yahoo to talk and sell stuff: ==== ben_cvv <====
====> My Yahoo Messenger: ben_cvv
====>E-Mail: ben_cvv@yahoo.com
====>> TON :659493049
  
```

1. download more http://q.gs/1276166/cc

2.

3. Credit card , visa card AND master cards

4.

5.

6.

7. card NUMBER : 371383100830806

8. card NUMBER : Oskar Brecher

9. Expiration DATE : 06/13

10. CV : 6491

11.

12.

13.

14. card NUMBER : 580776180417341

15. card NUMBER : eric peters

16. Expiration DATE : 03/14

17. CV : 627

18.

19.

20. card NUMBER : 4271783040283647

21. card NUMBER : Robert W. Stock

22. Expiration DATE : 02/14

23. CV : 044

24.

25.

26. card NUMBER : 5401 6830 9265 6443

27. card NUMBER : wilson h. shunkiller

Credit-Cards-Pastebin.txt

MIMOS Some More Working Samples...

pastebin.com/XiHniBDH

CVE security vulnera... Talks - gtac2011 MSN

```

5. Number: 4468 [redacted] 5311
6. EXP: 1113
7. CVV: 739
8. Name: Justin miller
9. Country: United States
10. State: Iowa
11. ZIP: 50702
12. City: Waterloo
13. Street: 935 oregon st
14. [redacted]
15. Bank: WELLS FARGO BANK, NATIONAL ASSOCIATION PLATINUM
16. Email: Justmiller26 [redacted] il.com
17.
18. MM--> Credit card With Mastercard Secure Code.....(MSCS)
19.
20. Card: 5460 [redacted] 506
21. Exp Date: 08|2014
22. Cvv2:768
23. Name On Card: B [redacted] well
24. Address :1401 Apple Ln East Meadow
New York
25. Zip Code: 11554
26. Countr: United St [redacted]
27. Phone: 516-318-5965
28. => Info Bank: |CAPITAL ONE, N.A.|
29. Type: DEBIT GOLD
30. UNITED_STATES
31. 18888104013 OR 18775478003 OR 18774423764
  
```

```

17. Card Number :426 [redacted] 142177003
18. Expiry Date:07/13
19. CVV :228
20. State :California
21. Country :United States
22. City:Nevada City
23. Zip Code :95959
24. Address :P.O. Box 1208
25. Phone :530-677-7941
26. Email ID :jd [redacted] rd48@gmail.com
27. SSN :N/A
28. DOB :N/A
29. Card Type :CREDIT GOLD/PREMIUM
30. Bank : Chase Bank
31.
32. Status : Live
33.
34. 41208 [redacted] 230537
35. CVV: 172
36. EXP: 11/15 First Name: Ann H
37. Last Name: M [redacted] n
38. DoB: N/A
39. email: N/A
40. Phone: N/A Country: USA
41. State: CT
42. City: Torrington
43. ZIP: 06790
44. Address: 122 Calhoun St
  
```

MIMOS CC TV Control

inurl:LvAppl intitle:liveapplet

Web Images Maps Shopping More Search tools

About 3,380 results (0.35 seconds)

LiveApplet - Network Camera Server VB101
203.95.34.11/sampleLvApplLvAppl.htm
You've visited this page many times. Last visit: 6/28/13

LiveApplet - Network Camera Server VB-C10/VB-C10R
62.44.223.185/sampleLvApplLvAppl.htm
You've visited this page many times. Last visit: 6/14/13

Camera: Camera1

WebView - Livascopa

Pan, scan, tilt & zoom

You can control the camera

Start Control

MIMOS 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?

Innovation for Life™



Securing ourselves from Google Hackers

Keep your sensitive data off the web!

Even if you think you're only putting your data on a web site 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

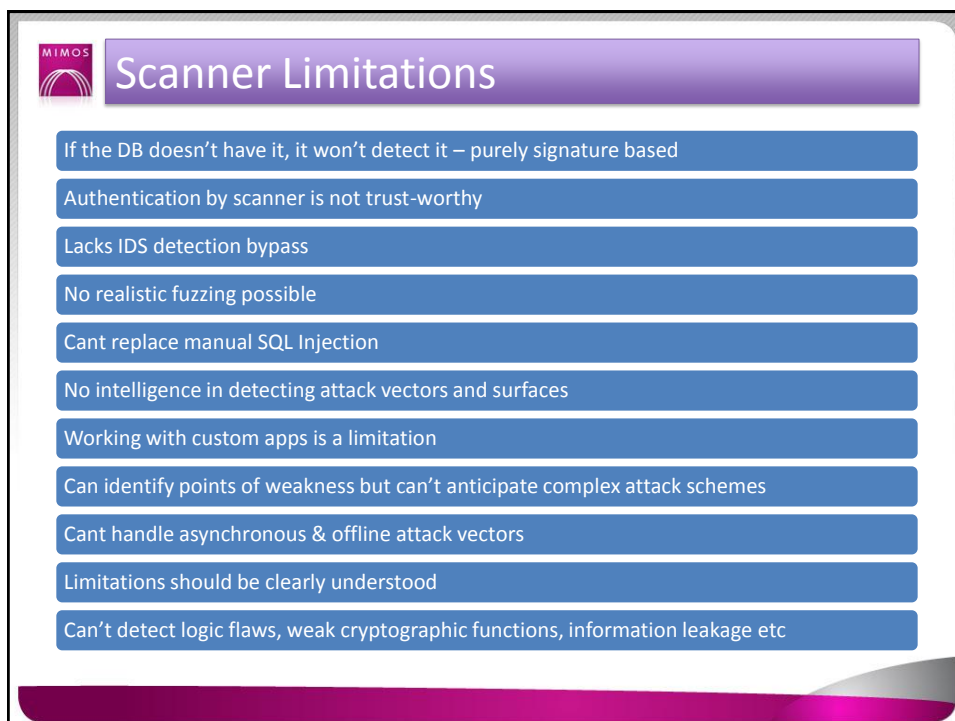
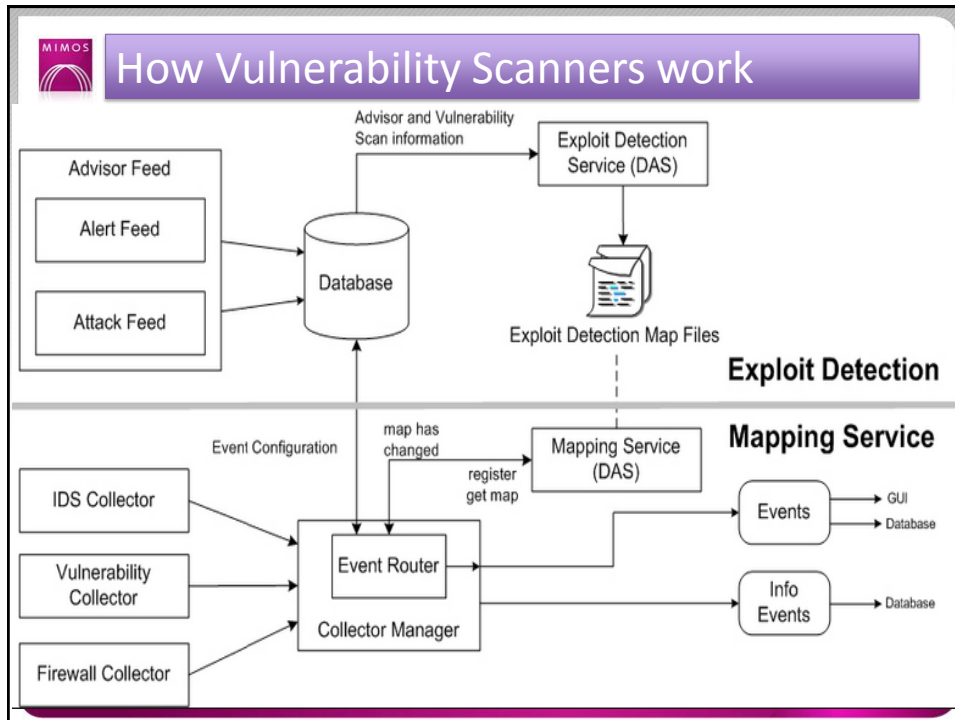
To Inspire You To Be A Security Tester

Innovation for Life™



BHDB

BHDB – Bing Hacking Database and how is it different from GHDB





WHERE DO ACTUAL HACKS COME FROM

So, who are these hackers?

Innovation for Life™



Real-life hacker categories


Category	Characteristics
Career Hackers	Hack websites Steal Credit Cards Financial Gain
Hacktivist	Anonymous, LulzSec Greater Good & Political drive Want to have fun, mainly kids/ young adults
Nation states	Government-sponsored 21 st Century Warfare Hackers hired in underground forums



THE TAKE-AWAY

Top Simple Security Searches that Work!

Innovation for Life™



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 \(http://tinyurl.com/starwestghdb2013\)](http://tinyurl.com/starwestghdb2013)



AUTOMATION

Automating the Google Searches

Innovation for Life™



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 We Hack YOU

Before the Hacker Does?
MIMOS PORE

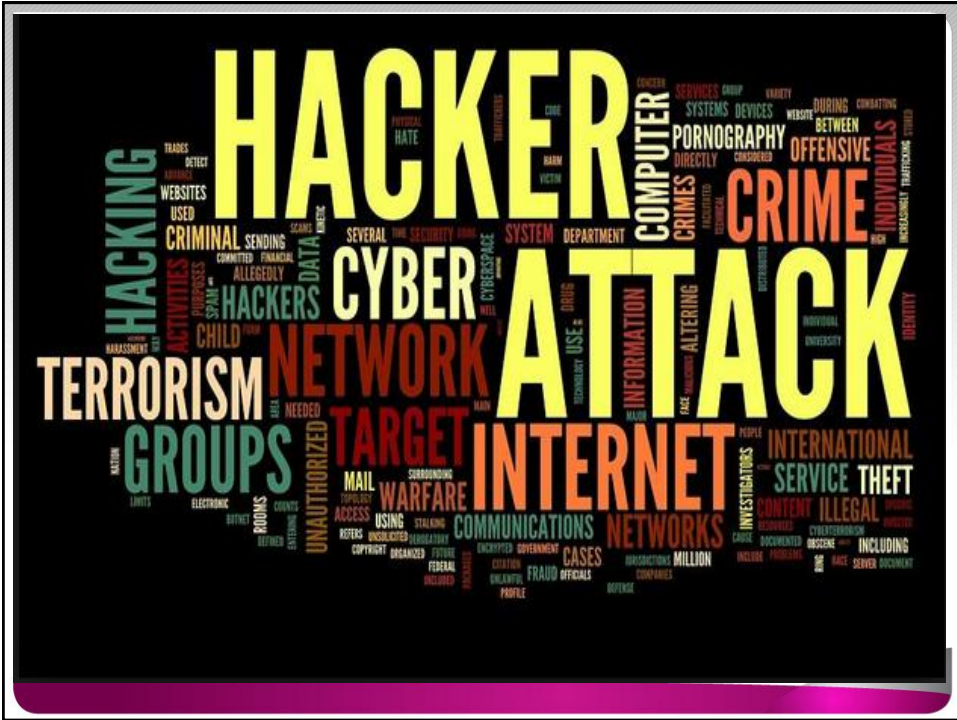
The slide features a purple header bar with the MIMOS logo and the text 'So...'. The main content is a large graphic with a yellow-to-white gradient background. The words 'Can We Hack' are in white, and 'YOU' is in large, yellow, 3D block letters. A purple sphere is positioned behind the 'YOU' text. Below the main text, the phrase 'Before the Hacker Does?' is written in red, and 'MIMOS PORE' is in purple. A purple decorative bar is at the bottom.



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/>

The slide features a purple header bar with the MIMOS logo and the text 'About the Presenter'. The main content is a dark blue rounded rectangle containing the presenter's name, handle, certifications, and website. A purple decorative bar is at the bottom.





MIMOS

TERIMA KASIH
THANK YOU

www.mimos.my

Innovation for Life™

© 2012 MIMOS Berhad. All Rights Reserved.