



OWASP

Open Web Application
Security Project

OFFENSIVE GOOGLING

ABOUT ME

- BLAY ABU SAFIAN
- FOUNDER/CEO of INVETECK GLOBAL
- Engineer / Security Researcher / Penetration Tester / Part-Time Bug Hunter
- www.inveteckglobal.com
- INSTAGRAM: inveteck_global
- TWITTER: Inveteck



WHAT IS GOOGLE?

AMERICAN MULTINATIONAL TECHNOLOGY COMPANY THAT SPECIALIZE IN INTERNET RELATED SERVICES AND PRODUCTS INCLUDING SOFTWARE, HARDWARE, CLOUD COMPUTING ETC.

WHY USE GOOGLE ?

- PROVIDES RELEVANT RESULTS QUICKLY.
- FOR AD DISPLAYS.
- CAN BE USED TO TRANSLATE LANGUAGES.
- HIDDEN VERTICAL SEARCH ENGINES FOR FINDING SECRETFILES, VIDEOS, PICTURES

GOOGLE WEBPAGE

WHAT IS OFFENSIVE GOOGLING?

- OFFICIAL NAME GOOGLE DORKING / GOOGLE HACKING
- ADVANCE GOOGLE SEARCH TO FIND SECURITY VULNERABILTIES IN THE CONFIGURATION THAT A WEBSITE USES.

WHY OFFENSIVE GOOGLING

- FIND WEBSITE SERVER MISCONFIGURATION.
- FIND LEAKED/SENSITIVE CREDENTIALS.
- FOR ADVANCE SEARCH

WHO HAS USED OFFENSIVE GOOGLING IN THE PAST?



TECNOLOGÍA ▾

SMARTPHONES ▾

ENTRETENIMIENTO ▾

E-PICKS

CONTACTO



SHIT. KAYLA IS MIA. THE GNOSIS KIDS ARE GONE IN HIDING SOMEWHERE.

FROM WHAT WE'VE SEEN THESE LULZSEC/GNOSIS KIDS AREN'T REALLY THAT GOOD AT HACKING. THEY TROLL THE INTERNET AND SEARCH FOR SQLINJECTION VULNERABILITIES AS WELL AS REMOTE FILE INCLUDE/LOCAL FILE INCLUDE BUGS. ONCE FOUND THEY TRY TO DOWNLOAD DATABASES OR PULL DOWN USERNAMES AND PASSWORDS. 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.

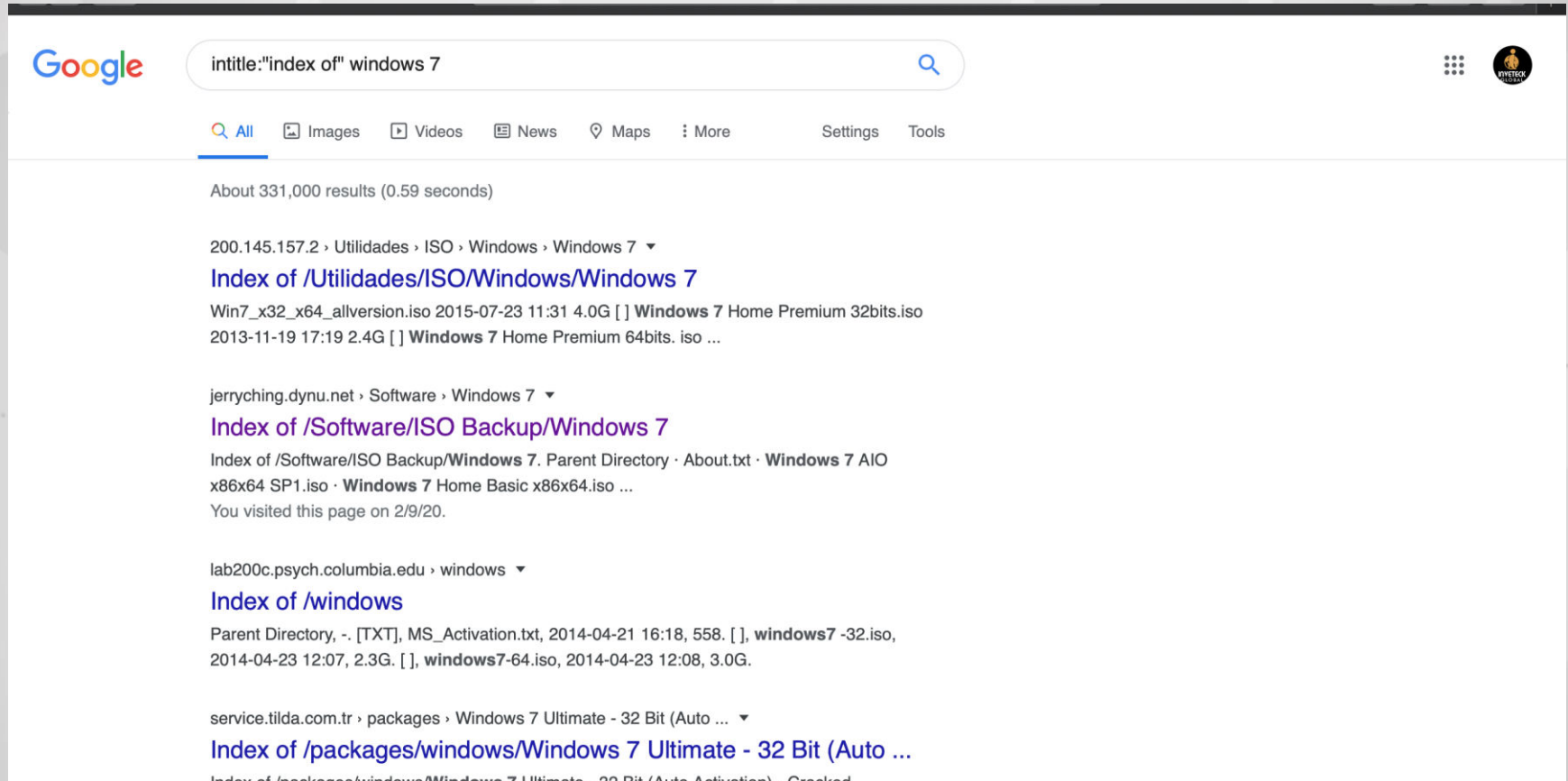
Noticias
Manufactureros
Apple
Smartphones
Tecnología
Internet

HACKER HACKING WITH GOOGLE DORKS



OWASP
Open Web Application
Security Project

USING OFFENSIVE GOOGLING FOR NON-MALICIOUS ACTIVITIES



The screenshot shows a Google search interface with the query "intitle:\"index of\" windows 7" entered in the search bar. The search results are displayed below the search bar, showing several entries with titles and snippets of text. The first entry is "Index of /Utilidades/ISO/Windows/Windows 7" with a snippet mentioning "Win7_x32_x64_allversion.iso" and "Windows 7 Home Premium 32bits.iso". The second entry is "Index of /Software/ISO Backup/Windows 7" with a snippet mentioning "Parent Directory" and "Windows 7 AIO x86x64 SP1.iso". The third entry is "Index of /windows" with a snippet mentioning "Parent Directory" and "windows7 -32.iso". The fourth entry is "Index of /packages/windows/Windows 7 Ultimate - 32 Bit (Auto ..." with a snippet mentioning "Index of /packages/windows/Windows 7 Ultimate - 32 Bit (Auto Activation) - Cracked".

Google

intitle:"index of" windows 7

All Images Videos News Maps More Settings Tools

About 331,000 results (0.59 seconds)

200.145.157.2 › Utilidades › ISO › Windows › Windows 7 ▼
Index of /Utilidades/ISO/Windows/Windows 7
Win7_x32_x64_allversion.iso 2015-07-23 11:31 4.0G [] Windows 7 Home Premium 32bits.iso
2013-11-19 17:19 2.4G [] Windows 7 Home Premium 64bits. iso ...

jerryching.dynu.net › Software › Windows 7 ▼
Index of /Software/ISO Backup/Windows 7
Index of /Software/ISO Backup/Windows 7. Parent Directory · About.txt · Windows 7 AIO
x86x64 SP1.iso · Windows 7 Home Basic x86x64.iso ...
You visited this page on 2/9/20.

lab200c.psych.columbia.edu › windows ▼
Index of /windows
Parent Directory, -, [TXT], MS_Activation.txt, 2014-04-21 16:18, 558. [], windows7 -32.iso,
2014-04-23 12:07, 2.3G. [], windows7-64.iso, 2014-04-23 12:08, 3.0G.

service.tilda.com.tr › packages › Windows 7 Ultimate - 32 Bit (Auto ... ▼
Index of /packages/windows/Windows 7 Ultimate - 32 Bit (Auto ...
Index of /packages/windows/Windows 7 Ultimate - 32 Bit (Auto Activation) - Cracked

GOOGLE DORKS FOR SEARCHING WINDOWS 7 OS

WHERE TO FIND OFFENSIVE GOOGLING QUERIES?

CONNECT.

LEARN.

GROW.

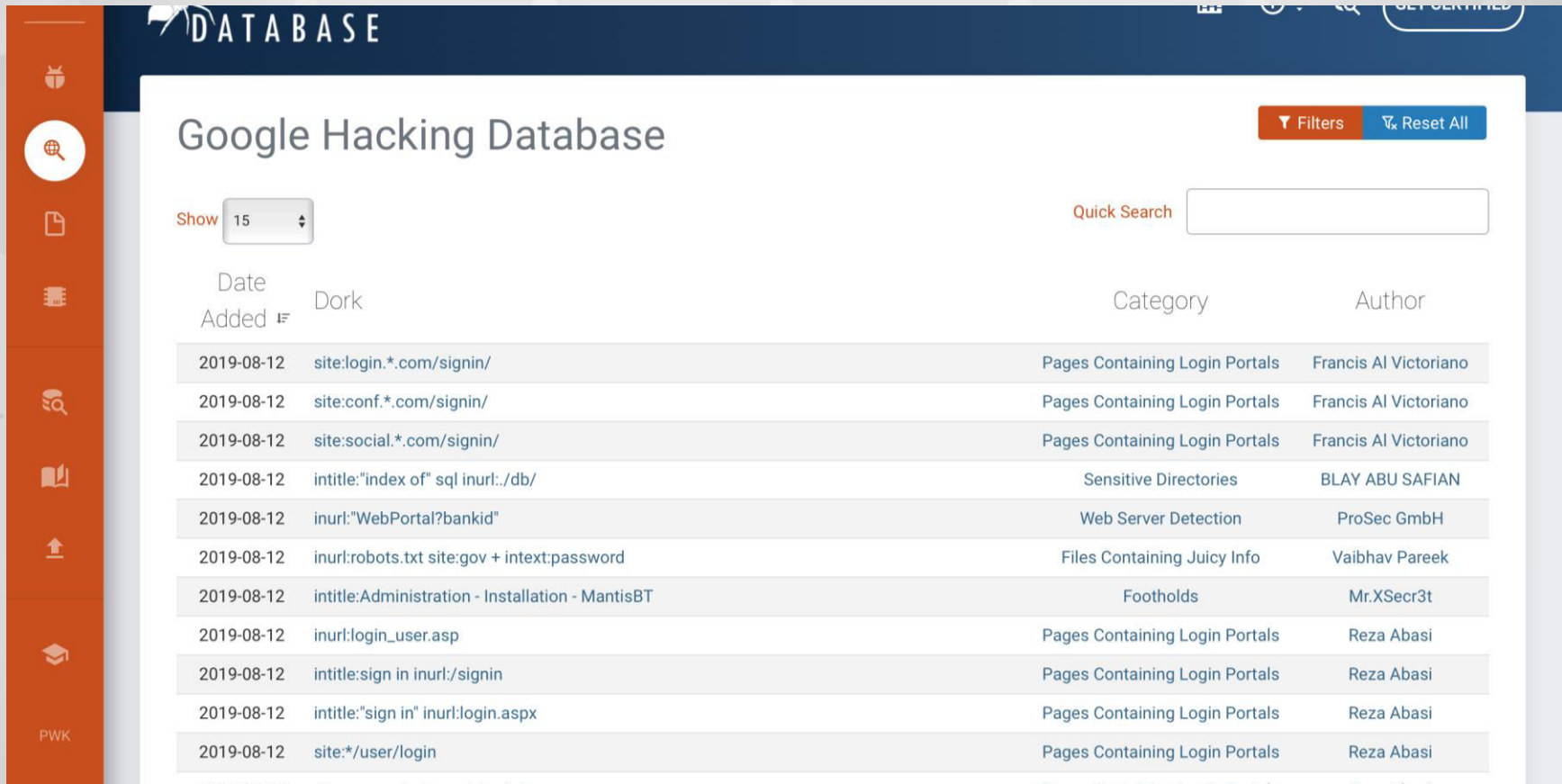
<https://www.exploit-db.com>



EXAMPLE OF OFFENSIVE GOOGLING QUERIES?

- GOOGLE DORK DESCRIPTION: intitle:"index of" sql inurl:./db/
- GOOGLE DORK DESCRIPTION: intitle:"index of" "sms.log"

EXAMPLE OF OFFENSIVE GOOGLING PAYLOADS?

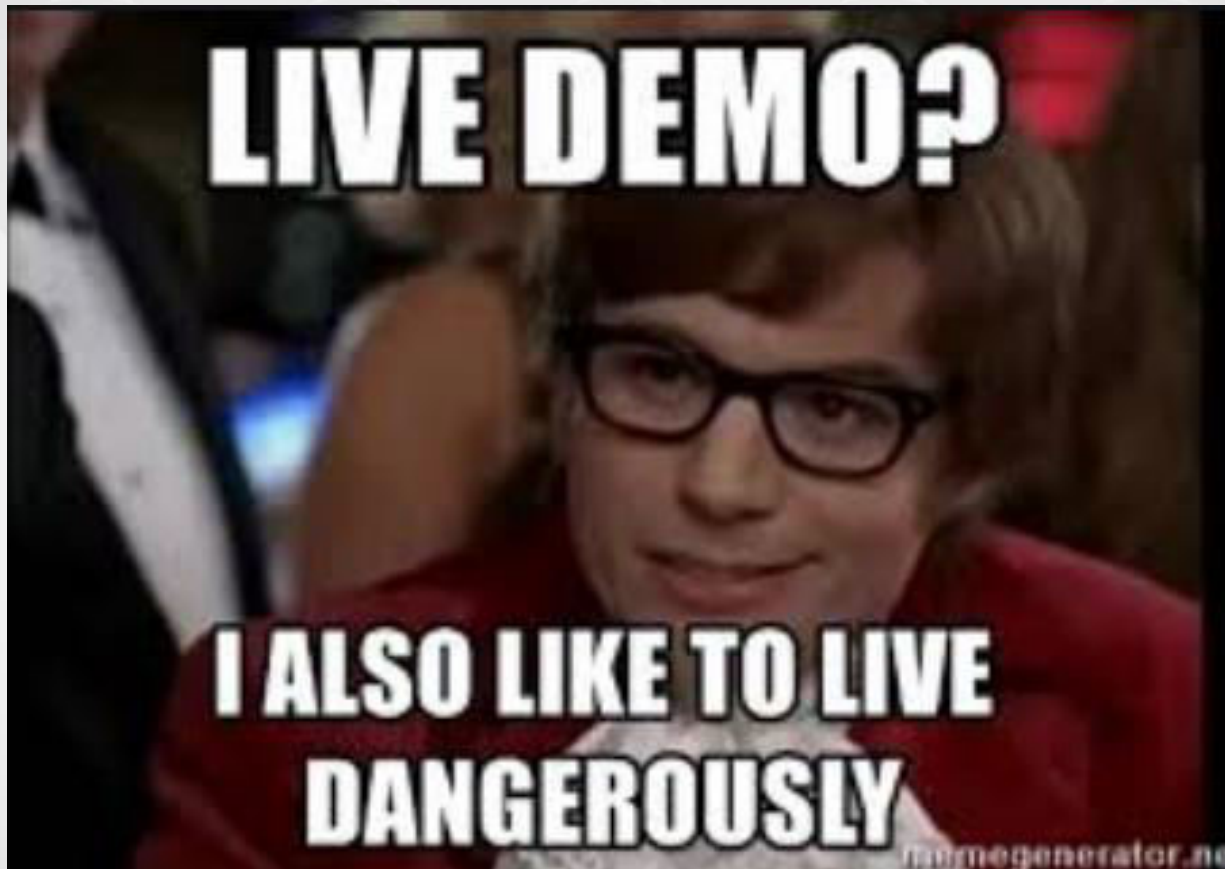


The screenshot displays the Google Hacking Database (GHD) interface. At the top, there is a navigation bar with 'DATABASE' and 'SETUP' options. The main header reads 'Google Hacking Database' with 'Filters' and 'Reset All' buttons. A search bar is labeled 'Quick Search'. Below the search bar, there is a 'Show' dropdown set to '15'. The results are presented in a table with columns for 'Date Added', 'Dork', 'Category', and 'Author'. The table lists several search results, all dated 2019-08-12, with various dork strings and categories.

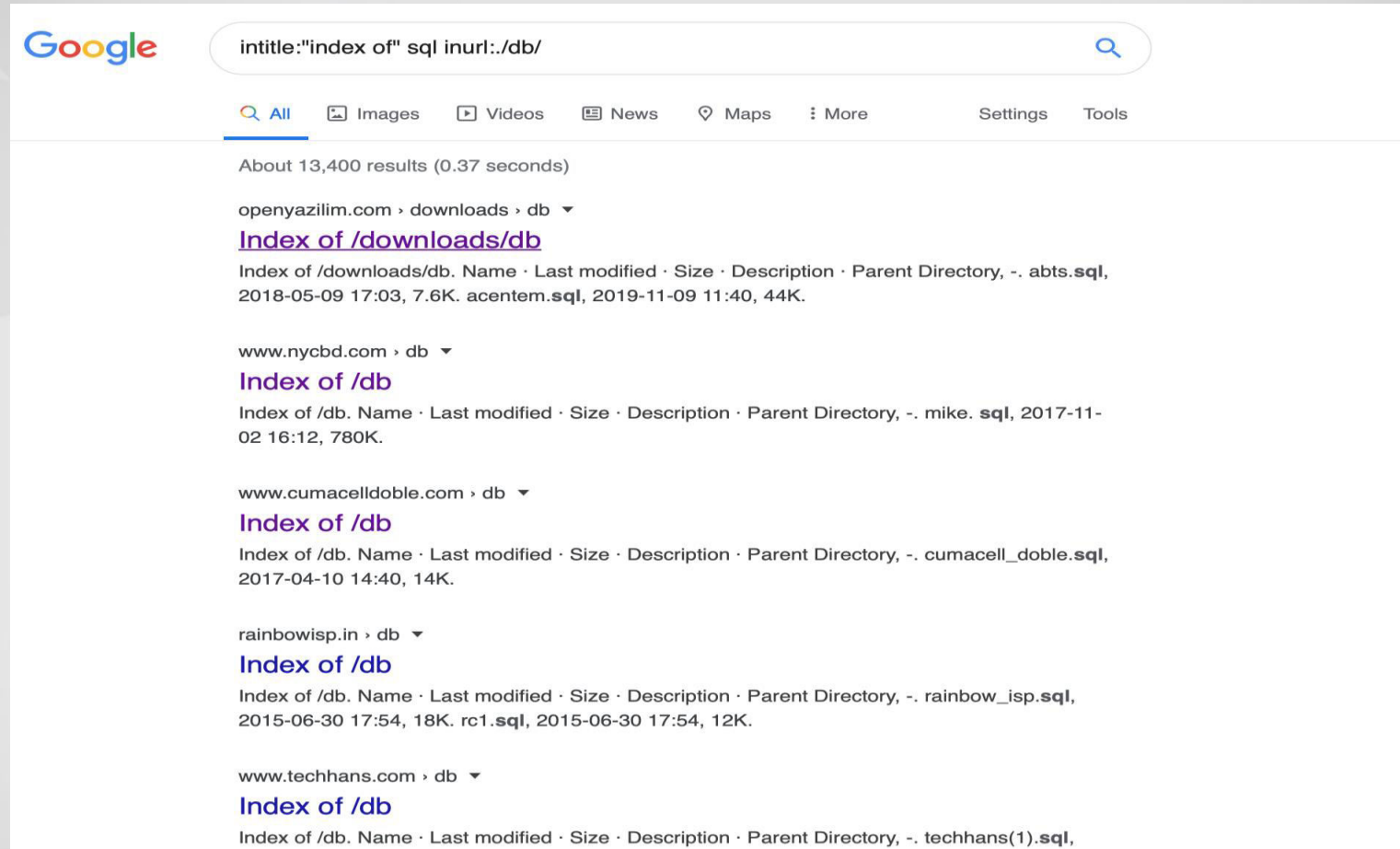
Date Added	Dork	Category	Author
2019-08-12	site:login.*.com/signin/	Pages Containing Login Portals	Francis Al Victoriano
2019-08-12	site:conf.*.com/signin/	Pages Containing Login Portals	Francis Al Victoriano
2019-08-12	site:social.*.com/signin/	Pages Containing Login Portals	Francis Al Victoriano
2019-08-12	intitle:"index of" sql inurl:./db/	Sensitive Directories	BLAY ABU SAFIAN
2019-08-12	inurl:"WebPortal?bankid"	Web Server Detection	ProSec GmbH
2019-08-12	inurl:robots.txt site:gov + intext:password	Files Containing Juicy Info	Vaibhav Pareek
2019-08-12	intitle:Administration - Installation - MantisBT	Footholds	Mr.XSecr3t
2019-08-12	inurl:login_user.asp	Pages Containing Login Portals	Reza Abasi
2019-08-12	intitle:sign in inurl:/signin	Pages Containing Login Portals	Reza Abasi
2019-08-12	intitle:"sign in" inurl:login.aspx	Pages Containing Login Portals	Reza Abasi
2019-08-12	site:*/user/login	Pages Containing Login Portals	Reza Abasi

GOOGLE EXPLOIT- DB

Demo



OFFENSIVE GOOGLING



The screenshot shows a Google search interface with the following elements:

- Search Bar:** Contains the query `intitle:"index of" sql inurl:./db/`.
- Navigation:** Includes links for All, Images, Videos, News, Maps, More, Settings, and Tools.
- Results:** Shows approximately 13,400 results in 0.37 seconds. The top results are:

Domain	Path	Index of /db	File Name	Size	Last Modified
openyazilim.com	downloads	db	abts.sql	7.6K	2018-05-09 17:03
www.nycbd.com		/db	mike.sql	780K	2017-11-02 16:12
www.cumacelldoble.com		/db	cumacell_doble.sql	14K	2017-04-10 14:40
rainbowisp.in		/db	rainbow_isp.sql	18K	2015-06-30 17:54
www.techhans.com		/db	techhans(1).sql	12K	2015-06-30 17:54



CONCLUSION

- OFFENSIVE GOOGLING CAN BE USED FOR BOTH MALICIOUS AND NON MALICIOUS ACTIVITIES

REFERENCES

- <https://www.jabari-holder.com/blog/a-team-hacker-group-exposes-lulzsec/>

CONNECT. **ANY QUESTION**