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?

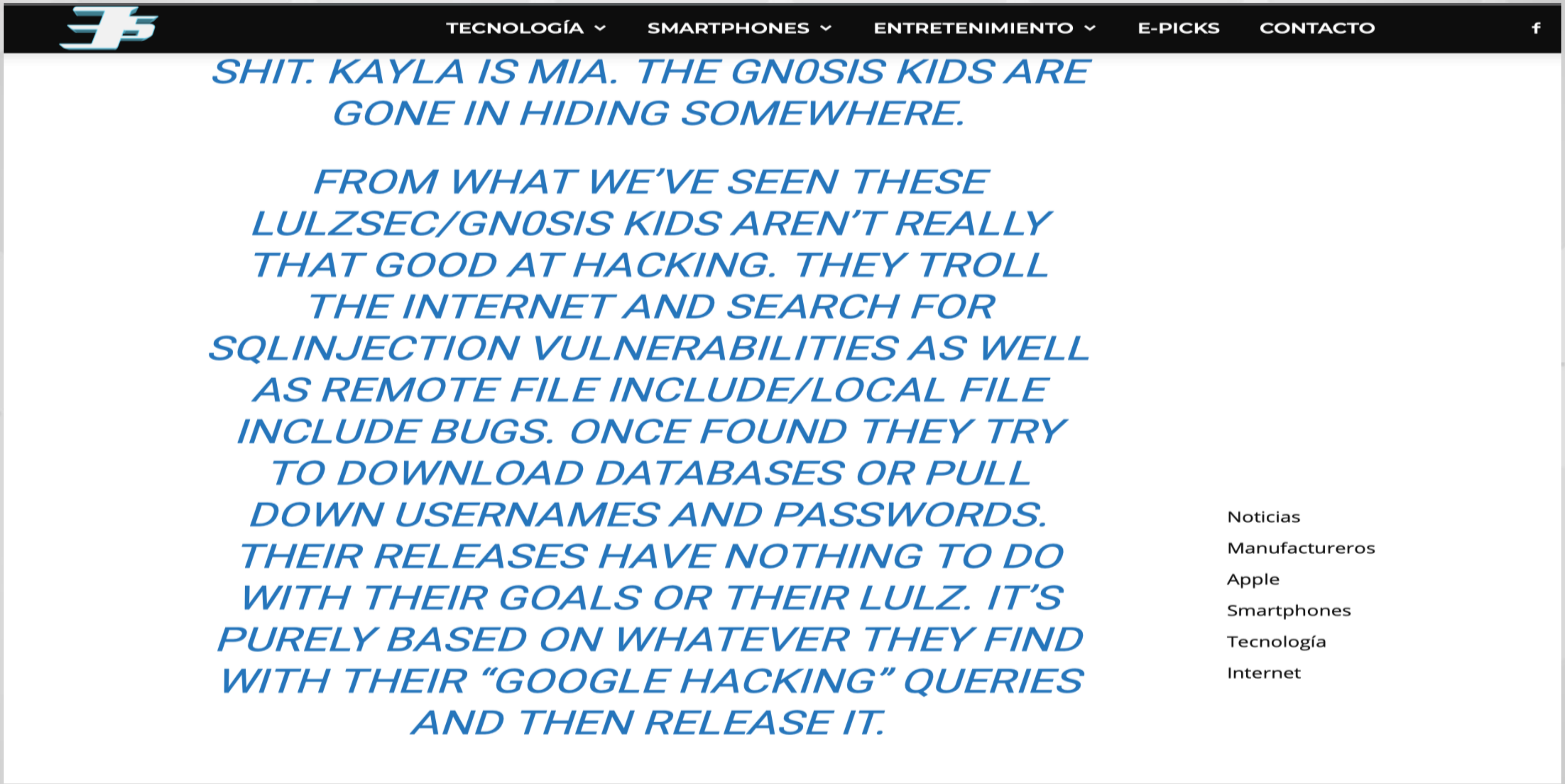
- OFFICIAL NAME GOOGLE DORKING / GOOGLE HACKING

- 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?

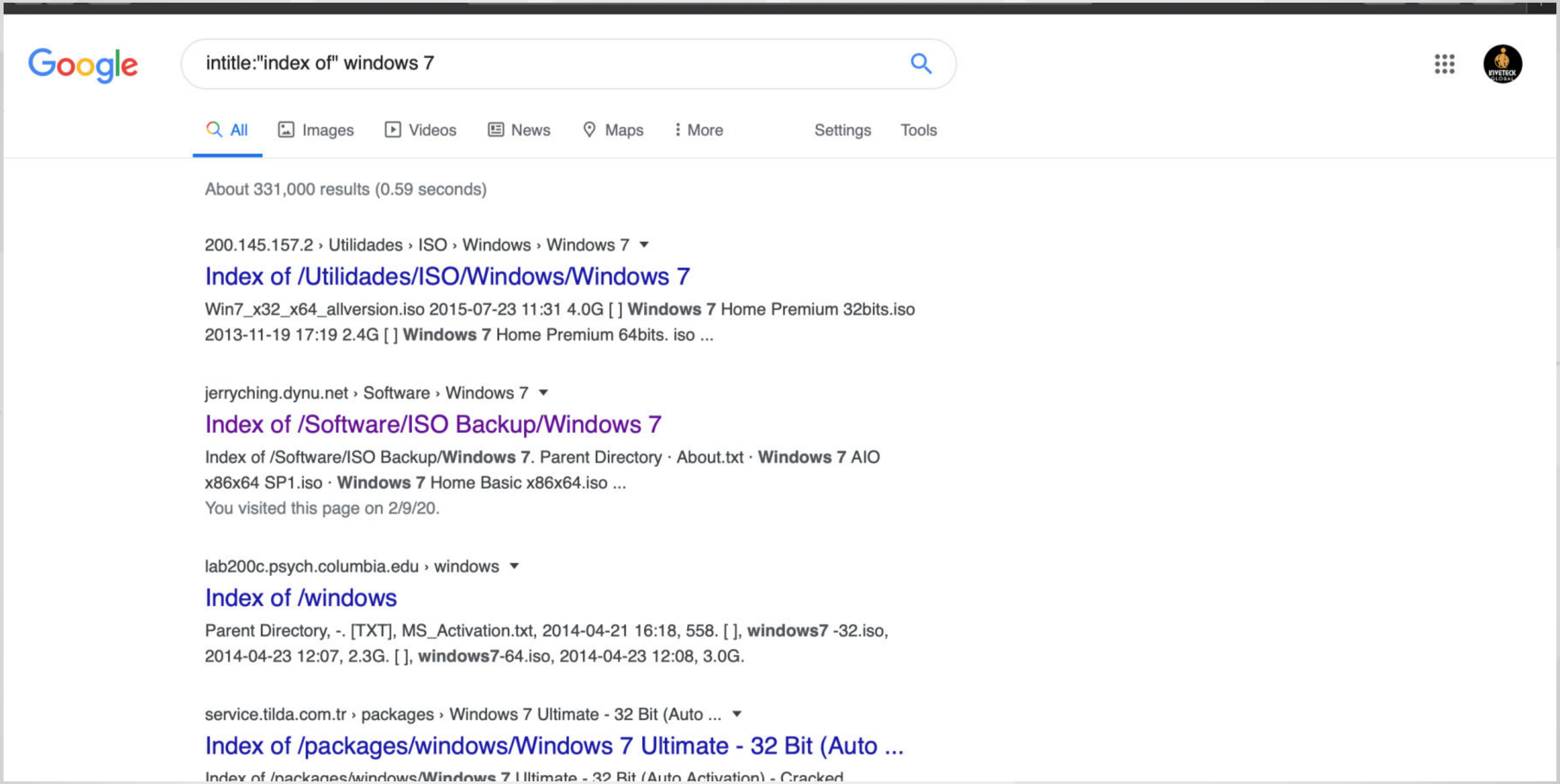


SHIT. KAYLA IS MIA. THE GN0SIS KIDS ARE GONE IN HIDING SOMEWHERE.

FROM WHAT WE'VE SEEN THESE LULZSEC/GN0SIS 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.

HACKER HACKING WITH GOOGLE DORKS

USING OFFENSIVE GOOGLING FOR NON-MALICIOUS ACTIVITIES



intitle:"index of" windows 7

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

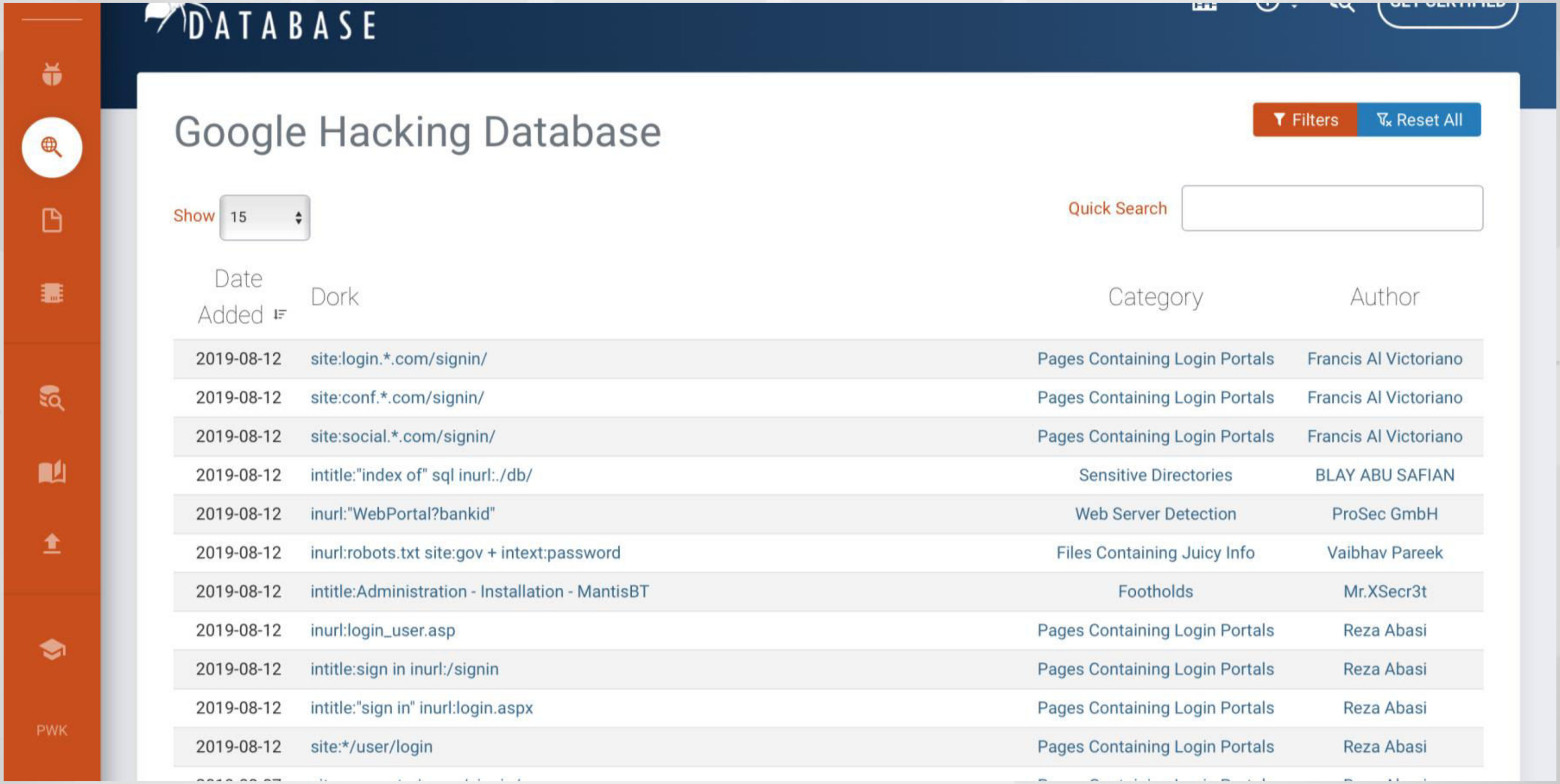
WHERE TO FIND OFFENSIVE GOOGLING QUERIES?

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?

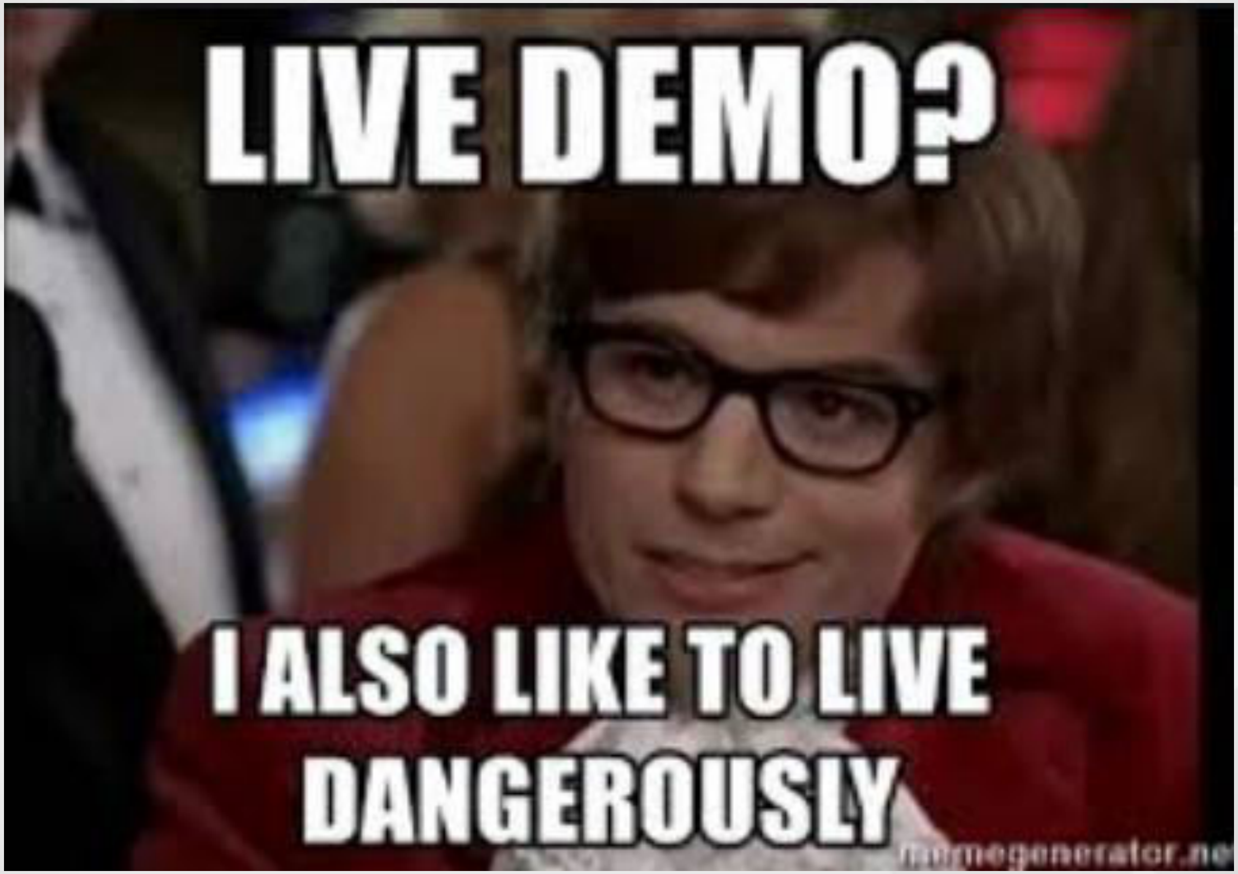


Google Hacking Database

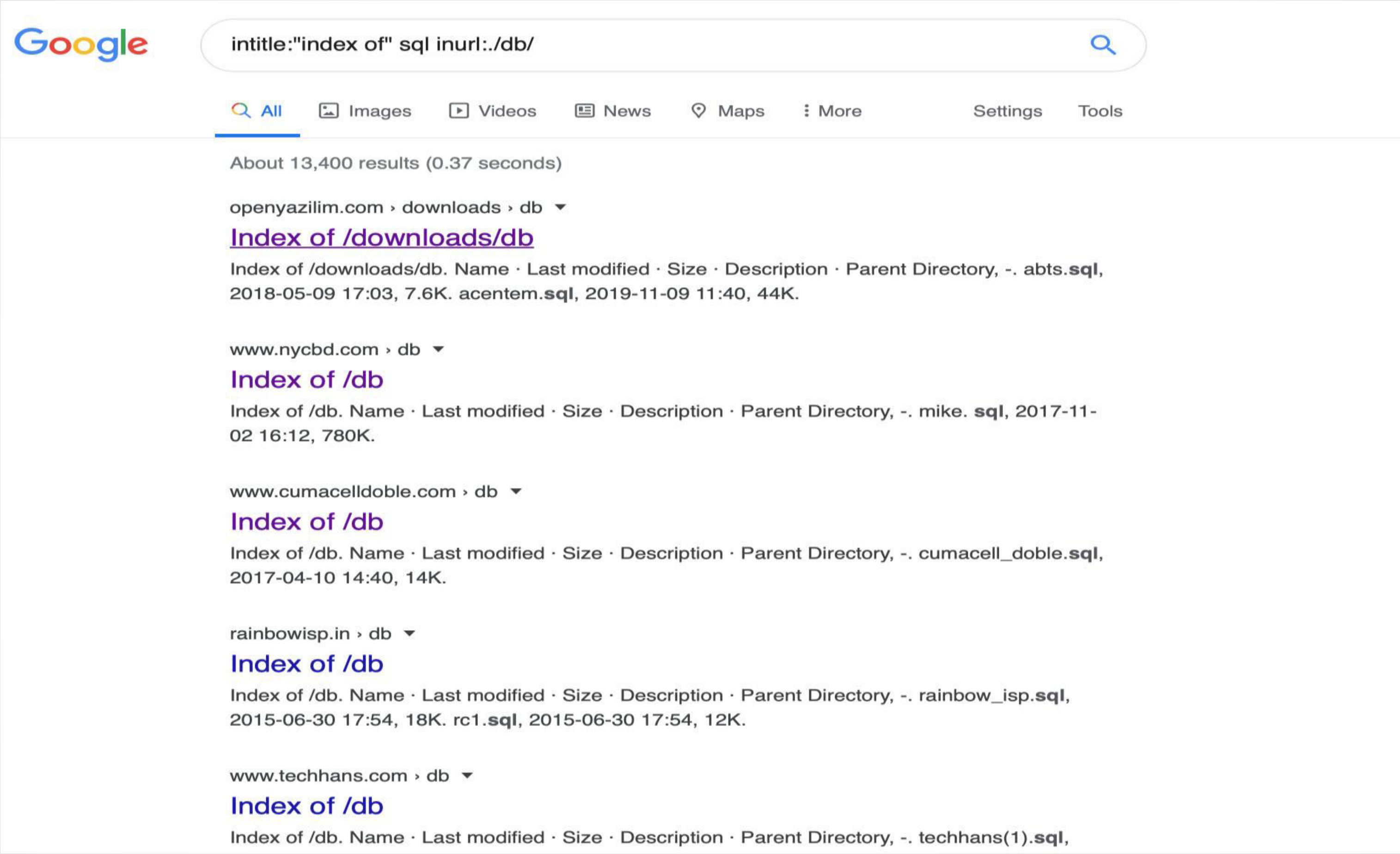
Date Added	Dork	Category	Author
2019-08-12	site:login.*.com/signin/	Pages Containing Login Portals	Francis Al Victoriano
2019-08-12	site:conf.*.com/signin/	Pages Containing Login Portals	Francis Al Victoriano
2019-08-12	site:social.*.com/signin/	Pages Containing Login Portals	Francis Al Victoriano
2019-08-12	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


LIVE DEMO?
I ALSO LIKE TO LIVE DANGEROUSLY
memegenerator.net

OFFENSIVE GOOGLING



intitle:"index of" sql inurl:./db/

About 13,400 results (0.37 seconds)

openyazilim.com › downloads › db

Index of /downloads/db

Index of /downloads/db. Name · Last modified · Size · Description · Parent Directory, -. abts.**sql**, 2018-05-09 17:03, 7.6K. acentem.**sql**, 2019-11-09 11:40, 44K.

www.nycbd.com › db

Index of /db

Index of /db. Name · Last modified · Size · Description · Parent Directory, -. mike. **sql**, 2017-11-02 16:12, 780K.

www.cumacelldoble.com › db

Index of /db

Index of /db. Name · Last modified · Size · Description · Parent Directory, -. cumacell_doble.**sql**, 2017-04-10 14:40, 14K.

rainbowisp.in › db

Index of /db

Index of /db. Name · Last modified · Size · Description · Parent Directory, -. rainbow_isp.**sql**, 2015-06-30 17:54, 18K. rc1.**sql**, 2015-06-30 17:54, 12K.

www.techhans.com › db

Index of /db

Index of /db. Name · Last modified · Size · Description · Parent Directory, -. techhans(1).**sql**,

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/

ANY QUESTION