

GOOGLE DORKING



GOOGLE DORK

Google Dorking is also known as Google Hacking. Basically, it is an advance technique to search information's on search engines. It is widely used by pentesters and hackers to discover the vulnerability in the websites.

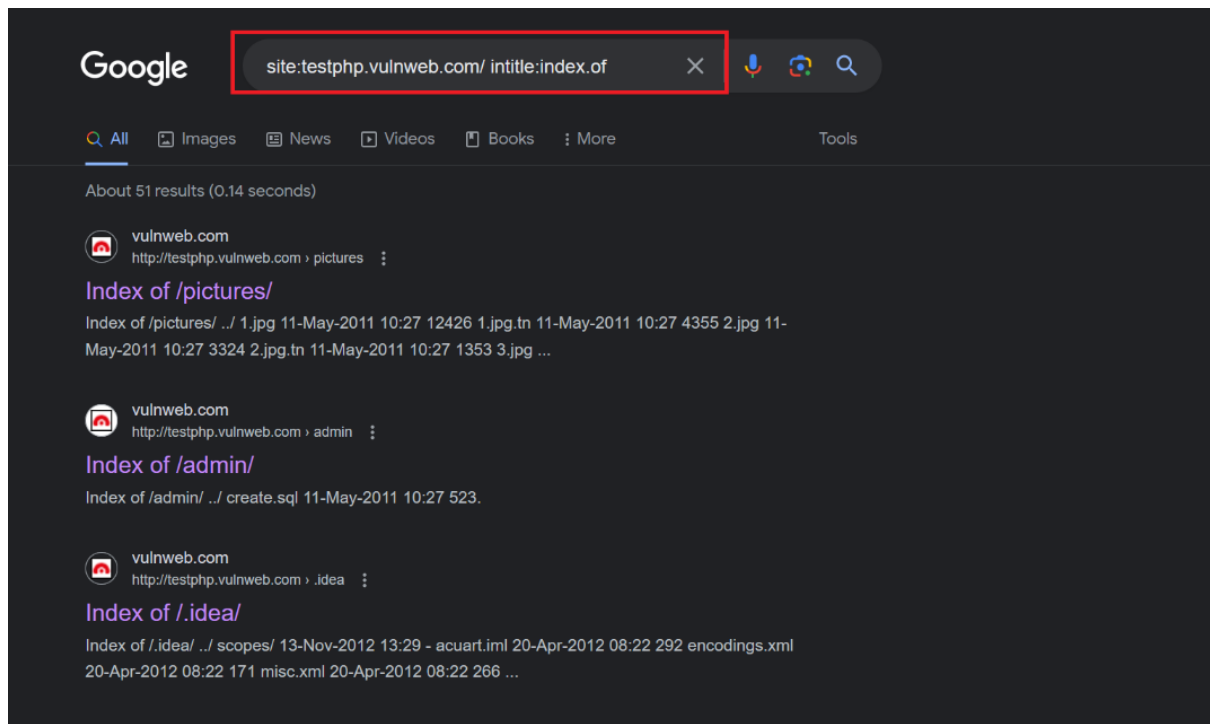
Using different queries narrow down the searches and uncover the hidden data which does not comes in regular search.

Basically user puts some operators and ask search engine algorithm to extract results for a particular target according to the keyword or strings.

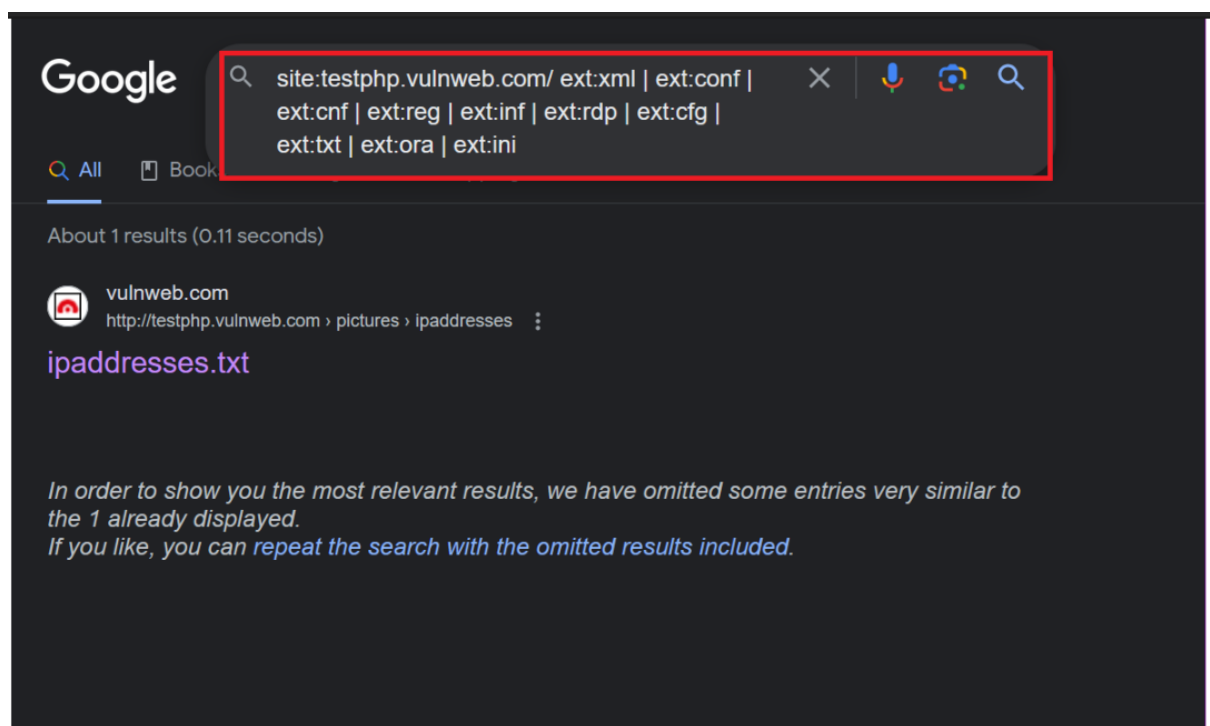
LIST OF COMMON TECHNIQUES FOR GOOGLE DORKS

1. **FileType**: This operator search for specific FileType. For Example: 'Filetpye:pdf' would return PDF files.
2. **Inrul**: This operator can be used to find specific word within the URL of the page. For Example: 'Inrul:login' would return with page login in the URL.
3. **Php?id=1**: This operator can be used for those websites which contains Php?id=1.
4. **Intext**: This operator can be used to search for specific text content within the webpage. For example: Intext:'password', this will return back the results with webpage that contain the word 'password'.
5. **Link**: This operator can be used to search for the pages that contains link to the specific URL. For example: link:domain.com and this will return the pages that is similar to this domain.com.
6. **Site**: This operator uses to search the for the specific website.
7. **Cache**: This operator returns the cache version of website for example: cache:domain.com.

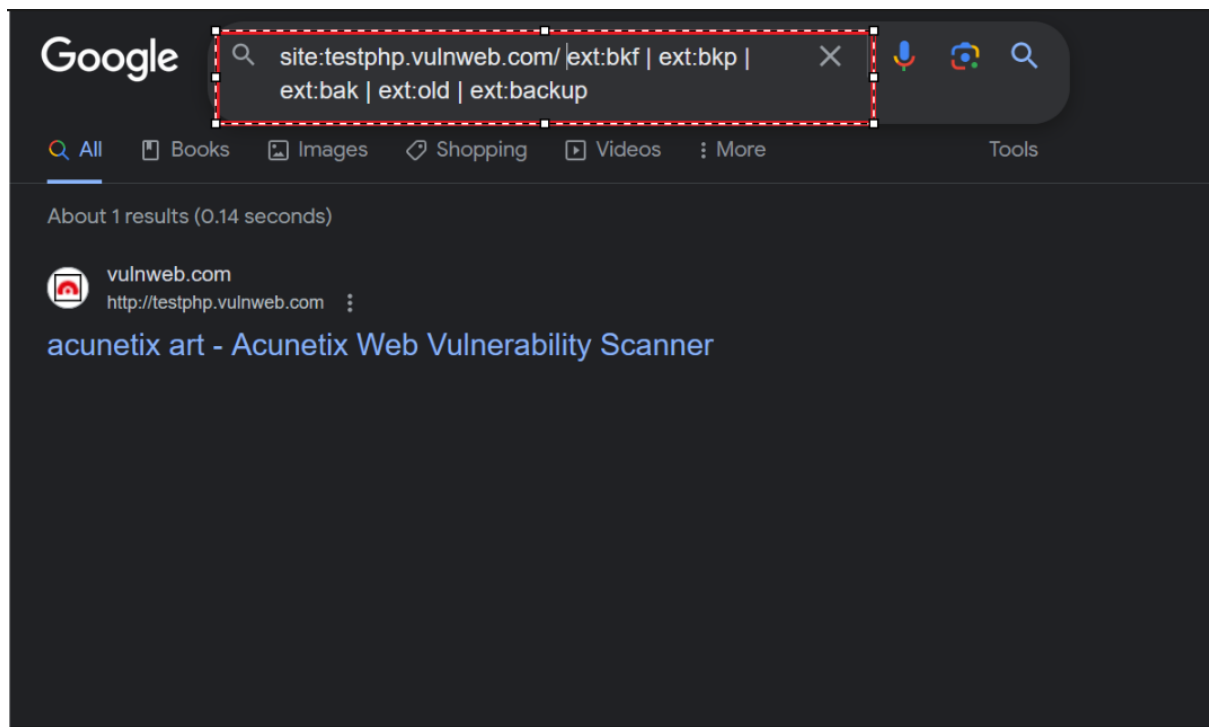
SCREENSHOT OF LIVE USECASE ON TESTPHP.VULNWEB.COM USING OPERATORS



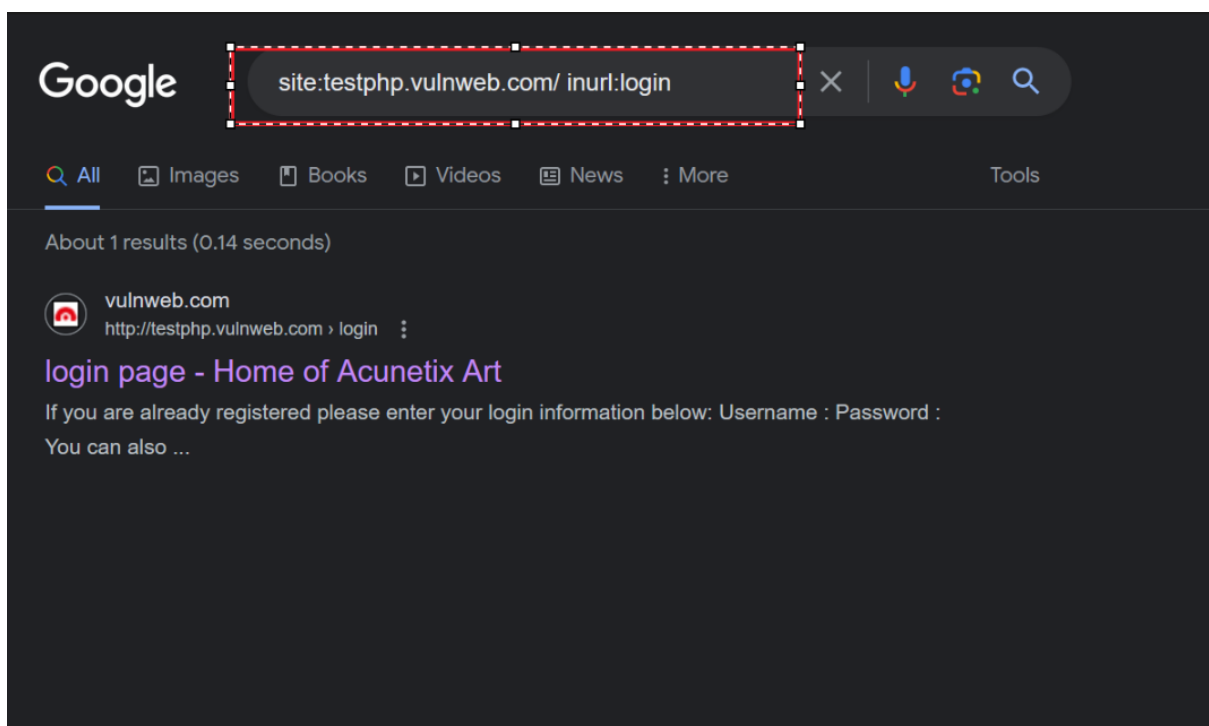
SITE:TESTPHP.VULNWEB.COM/ INTITLE:INDEX.OF



SITE:TESTPHP.VULNWEB.COM/ EXT:XML | EXT:CONF | EXT:CNF | EXT:REG | EXT:INF | EXT:RDP | EXT:CFG | EXT:TXT | EXT:ORA | EXT:INI



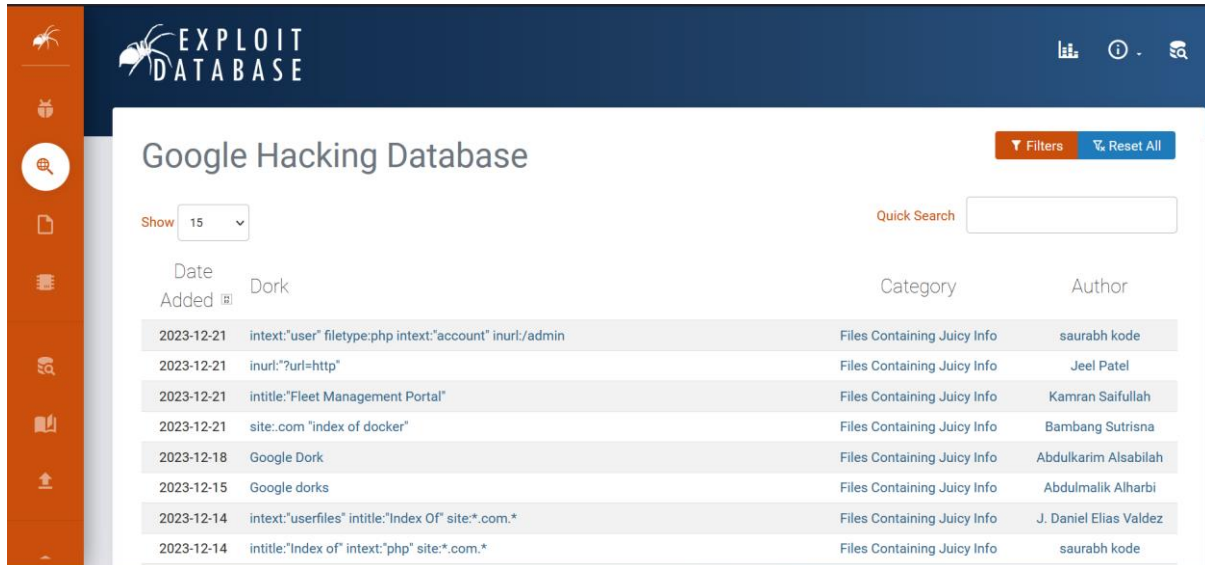
SITE:TESTPHP.VULNWEB.COM/ EXT:BKF | EXT:BKP | EXT:BAK | EXT:OLD | EXT:BACKUP



SITE:TESTPHP.VULNWEB.COM/ INURL:LOGIN

GOOGLE HACKING DATABASE

Google hacking database gives a wide range of queries which can be used to identify security vulnerabilities in the web application which is publicly available. It is useful to gather information, disclosing sensitive information and the file containing credentials as well as other sensitive data by using queries. User can use this queries on their target website to gather sensitive information.



Date Added	Dork	Category	Author
2023-12-21	intext:"user" filetype:php intext:"account" inurl:/admin	Files Containing Juicy Info	saurabh kode
2023-12-21	inurl:"?url=http"	Files Containing Juicy Info	Jeel Patel
2023-12-21	intitle:"Fleet Management Portal"	Files Containing Juicy Info	Kamran Saifullah
2023-12-21	site:.com "index of docker"	Files Containing Juicy Info	Bambang Sutrisna
2023-12-18	Google Dork	Files Containing Juicy Info	Abdulkarim Alsabilah
2023-12-15	Google dorks	Files Containing Juicy Info	Abdulmalik Alharbi
2023-12-14	intext:"userfiles" intitle:"Index Of" site:*.com.*	Files Containing Juicy Info	J. Daniel Elias Valdez
2023-12-14	intitle:"Index of" intext:"php" site:*.com.*	Files Containing Juicy Info	saurabh kode

GOOGLE HACKING DATABASE

REFERENCE

https://www.tutorialspoint.com/google_hacking_tests.htm

<https://chat.openai.com/>

https://www.youtube.com/watch?v=3RvCoo6u_EQ