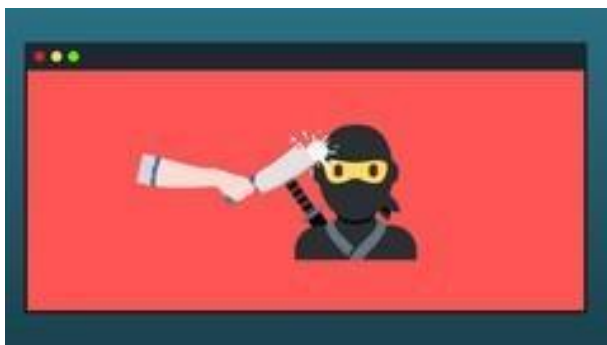


COURSE: Recon for Ethical Hacking / Penetration Testing & Bug Bounty

Navigating the Art of Reconnaissance in Ethical Hacking, Penetration Testing & Bug Bounty Hunting



□ Introduction:

In the ever-evolving landscape of cybersecurity, one truth remains constant: knowledge is power. Ethical hackers, penetration testers, and bug bounty hunters are driven by an insatiable curiosity to uncover vulnerabilities, safeguard systems, and contribute to a safer digital realm. Welcome to the enlightening Udemy course "Recon for Ethical Hacking / Penetration Testing & Bug Bounty." In this article, we invite you to embark on a journey of discovery through the intricacies of reconnaissance—the foundation upon which effective cybersecurity strategies are built.

□ What is Google Dorking

Google dorking, also known as Google hacking, is a technique where specific search queries are used to find sensitive information or vulnerabilities on websites by exploiting search engine operators and filters. It's often used by security professionals and hackers for reconnaissance and information gathering.

Google Dork

Top 5 Google Dorking in 2023

1. Finding exposed directories:

Dork:- `intitle:"Index of" -inurl:(jsp|pl|php|html|aspx|htm|cf|shtml)
-inurl:(listen77|mp3raid|mp3toss|mp3drug|index_of|wallywashis)`

Description:- The above Google dork searches for web directories with the title "Index of" while excluding common web page extensions (jsp, pl, php, etc.) and known music-related directories (listen77, mp3raid, etc.). It helps find open directories containing various files for potential download.

Google

`:- intitle:"Index of" -inurl:(jsp|pl|php|html|aspx|htm|cf|shtml) -inurl:(listen77|mp3raid|mp3toss|mp3drug|index_of|wallywashis)`

All Images Videos Maps Books More Tools

About 1,49,00,000 results (0.43 seconds)

welovedogs.jp
https://www.welovedogs.jp › movie

Index of /movie

Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [VID], video_001.mp4, 2017-06-17 14:49, 409M. [VID] ...

BYJU'S
https://byjus.com › question-answer › what-is-refractiv...

What is refractive index of a material? How is it related to ...

Hence, the formula for the refractive index of the medium can be stated as: Refractive index = vel. of light in vacuum or air vel. of light in medium.

1 answer · Top answer: Step 1: Definition of the refractive index of a materialThe ratio between...

Wikipedia
https://en.wikipedia.org › wiki › Index_of_a_subgroup

Index of a subgroup

In mathematics, specifically group theory, the index of a subgroup H in a group G is the number of left cosets of H in G, or equivalently, the number of ...

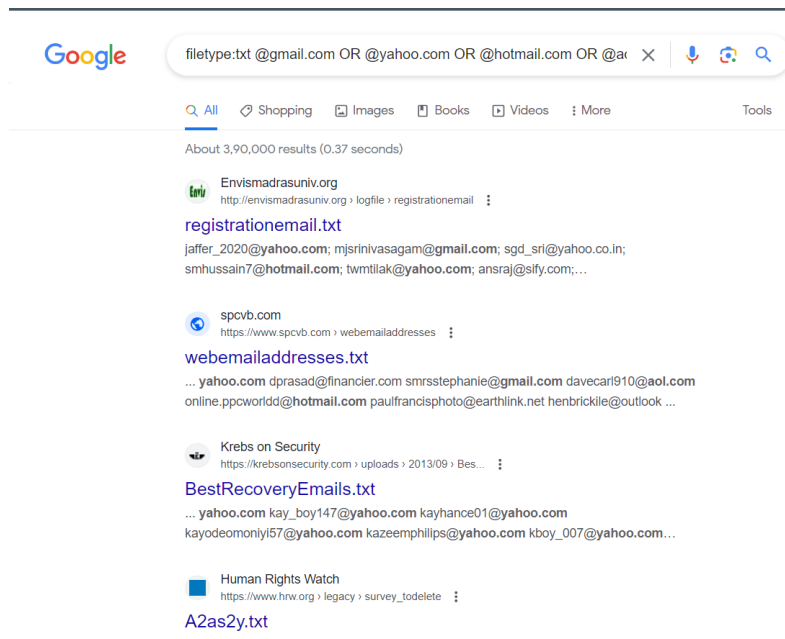
Toppr
https://www.toppr.com › ask › en-np › question › the-...

The refractive index of air with respect to glass is 2/3

2. Finding Email lists:

Dork:- filetype:txt @gmail.com OR @yahoo.com OR @hotmail.com OR @aol.com

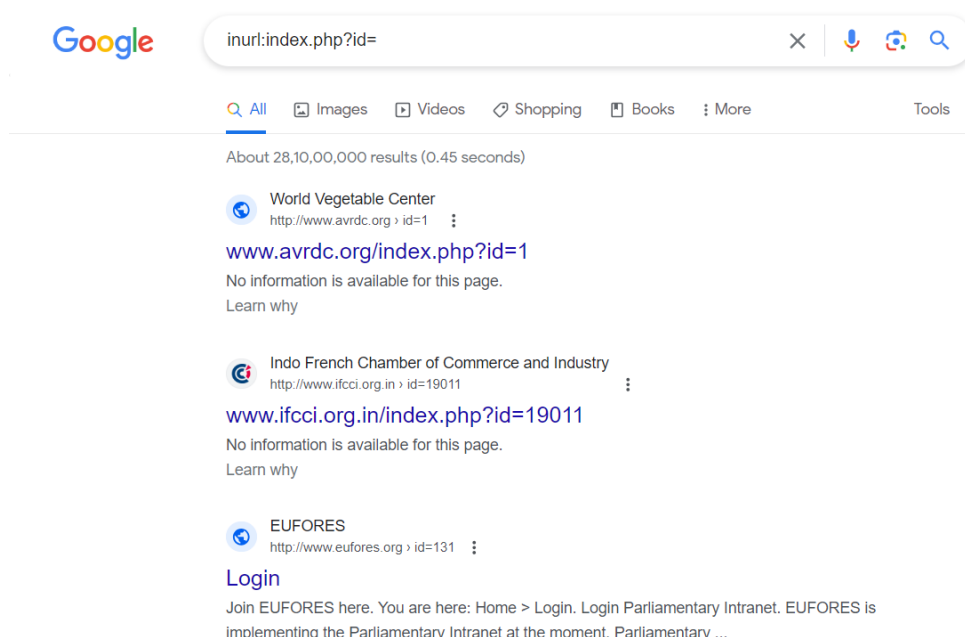
Description:- This Google dork searches for text files containing email addresses with the domains @gmail.com, @yahoo.com, @hotmail.com, or @aol.com.



3. Finding SQL injection vulnerabilities

Dork:- inurl:index.php?id=

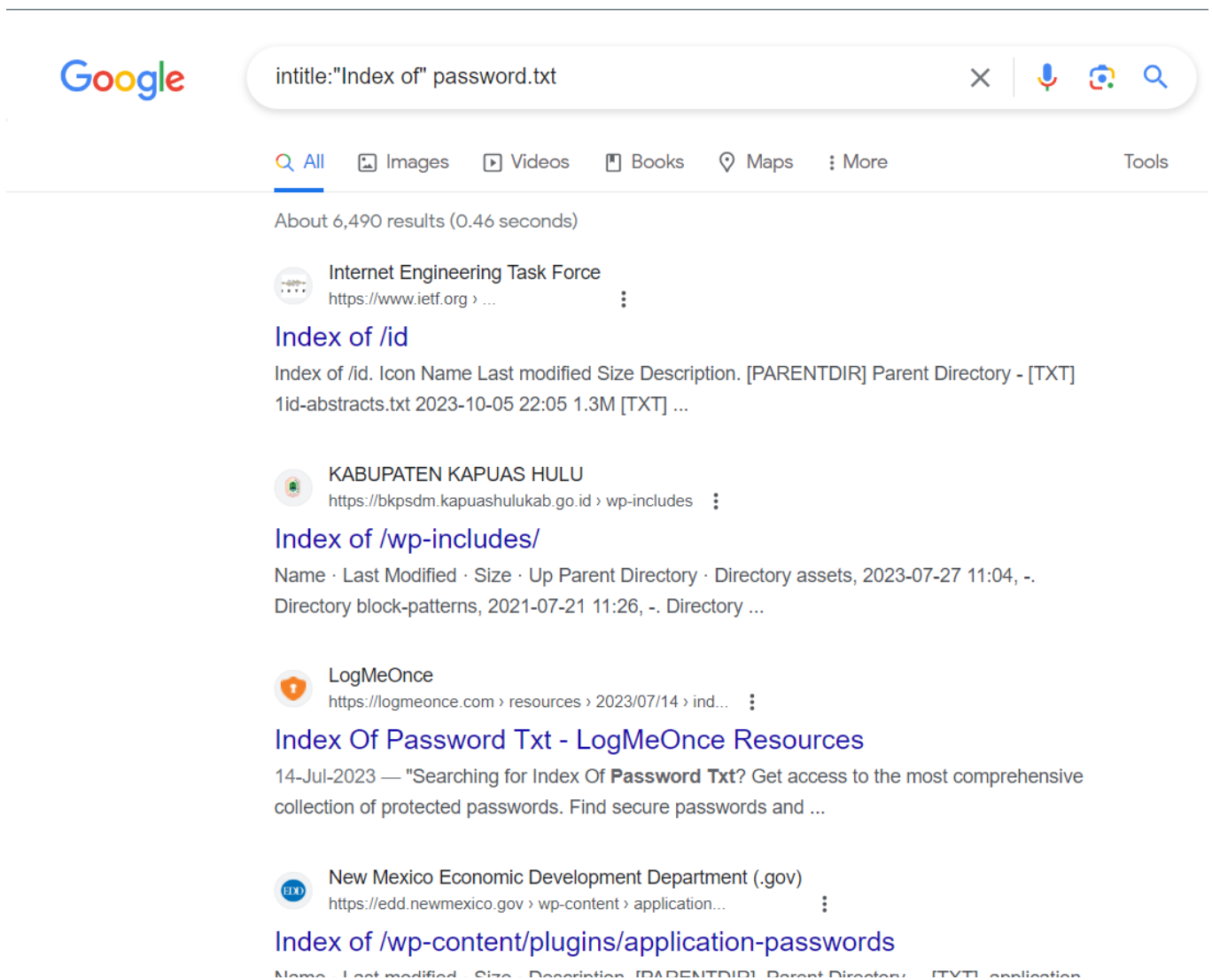
Description:- Google dorking using "inurl:index.php?id=" is a technique to search for websites with URLs containing "index.php?id=" in their address, often revealing potential vulnerabilities.



4. Uncovering sensitive information in files:

Dork:- intitle:"Index of" password.txt

Description:- "intitle:"Index of" password.txt" searches for web directories or listings with a title containing "Index of" and a file named "password.txt," potentially revealing insecure password files.

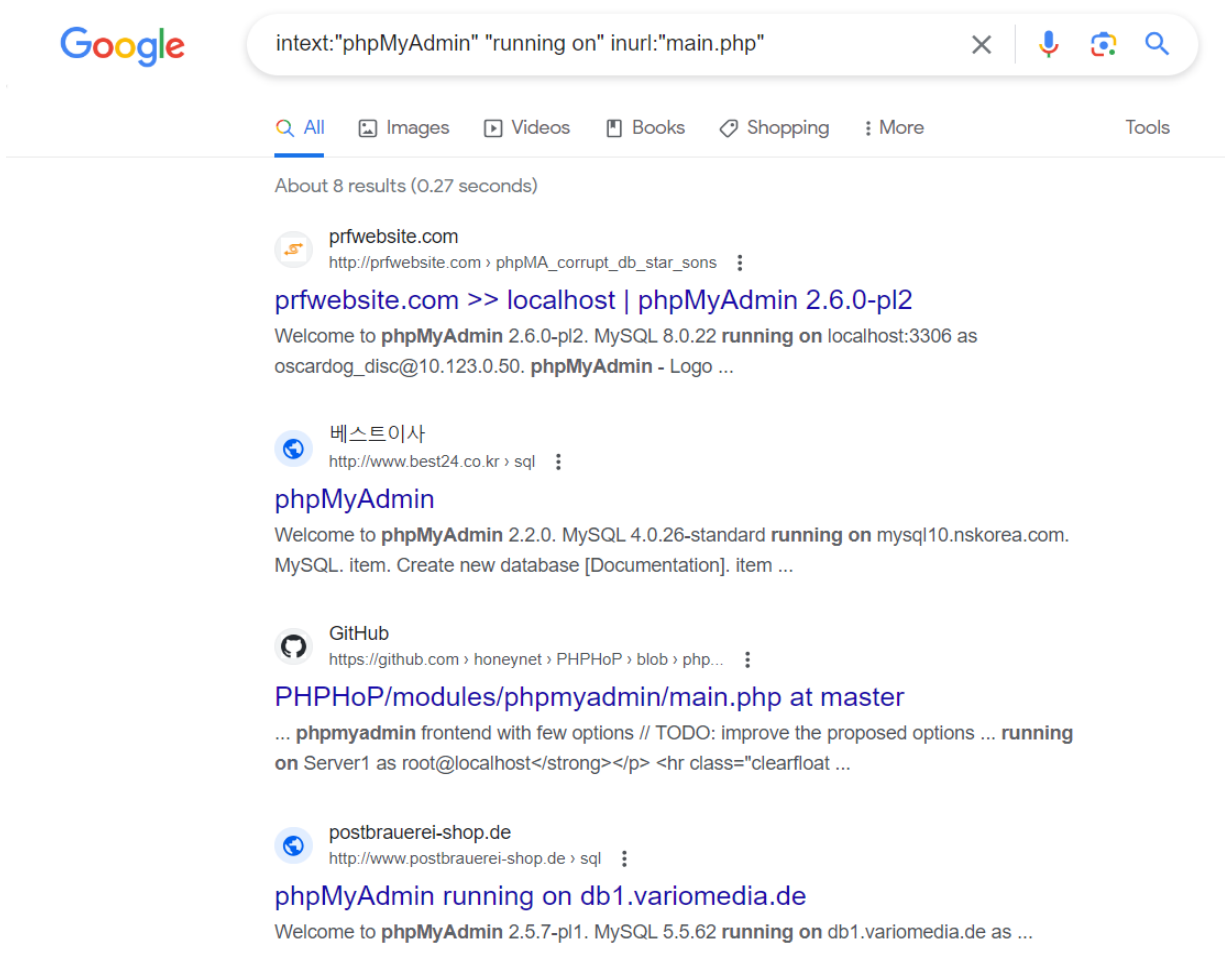


The screenshot shows a Google search interface with the query "intitle:Index of password.txt" entered in the search bar. The search results are displayed below the search bar, showing four results. Each result includes a site icon, the site name, the URL, and a snippet of the search results. The first result is from "Internet Engineering Task Force" (https://www.ietf.org) with the title "Index of /id" and a snippet mentioning "1id-abstracts.txt 2023-10-05 22:05 1.3M [TXT] ...". The second result is from "KABUPATEN KAPUAS HULU" (https://bkpsdm.kapuashulukab.go.id) with the title "Index of /wp-includes/" and a snippet mentioning "Name · Last Modified · Size · Up Parent Directory · Directory assets, 2023-07-27 11:04, -, Directory block-patterns, 2021-07-21 11:26, -, Directory ...". The third result is from "LogMeOnce" (https://logmeonce.com) with the title "Index Of Password Txt - LogMeOnce Resources" and a snippet mentioning "14-Jul-2023 — "Searching for Index Of Password Txt? Get access to the most comprehensive collection of protected passwords. Find secure passwords and ...". The fourth result is from "New Mexico Economic Development Department (.gov)" (https://edd.newmexico.gov) with the title "Index of /wp-content/plugins/application-passwords" and a snippet mentioning "Name · Last modified · Size · Description · [PARENTDIR] Parent Directory · [TXT] application...".

5. Finding exposed databases:

Dork:- `intext:"phpMyAdmin" "running on" inurl:"main.php"`

Description:- This Google dork is a search query used to find web pages that have the text "phpMyAdmin" and "running on" in their content and also contain the URL "main.php." It's often used by security professionals and hackers to identify websites that might have a vulnerable or misconfigured phpMyAdmin installation, which could potentially be exploited for unauthorized access or other security issues.



Google

intext:"phpMyAdmin" "running on" inurl:"main.php"

All Images Videos Books Shopping More Tools

About 8 results (0.27 seconds)

prfwebsite.com
http://prfwebsite.com › phpMA_corrupt_db_star_sons
prfwebsite.com >> localhost | phpMyAdmin 2.6.0-pl2
Welcome to **phpMyAdmin** 2.6.0-pl2. MySQL 8.0.22 **running on** localhost:3306 as oscarDOG_disc@10.123.0.50. **phpMyAdmin** - Logo ...

베스트이사
http://www.best24.co.kr › sql
phpMyAdmin
Welcome to **phpMyAdmin** 2.2.0. MySQL 4.0.26-standard **running on** mysql10.nskorea.com. MySQL. item. Create new database [Documentation]. item ...

GitHub
https://github.com › honeynet › PHPHoP › blob › php...
PHPHoP/modules/phpmyadmin/main.php at master
... **phpmyadmin** frontend with few options // TODO: improve the proposed options ... **running on** Server1 as root@localhost

postbrauerei-shop.de
http://www.postbrauerei-shop.de › sql
phpMyAdmin running on db1.variomediam.de
Welcome to **phpMyAdmin** 2.5.7-pl1. MySQL 5.5.62 **running on** db1.variomediam.de as ...