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*

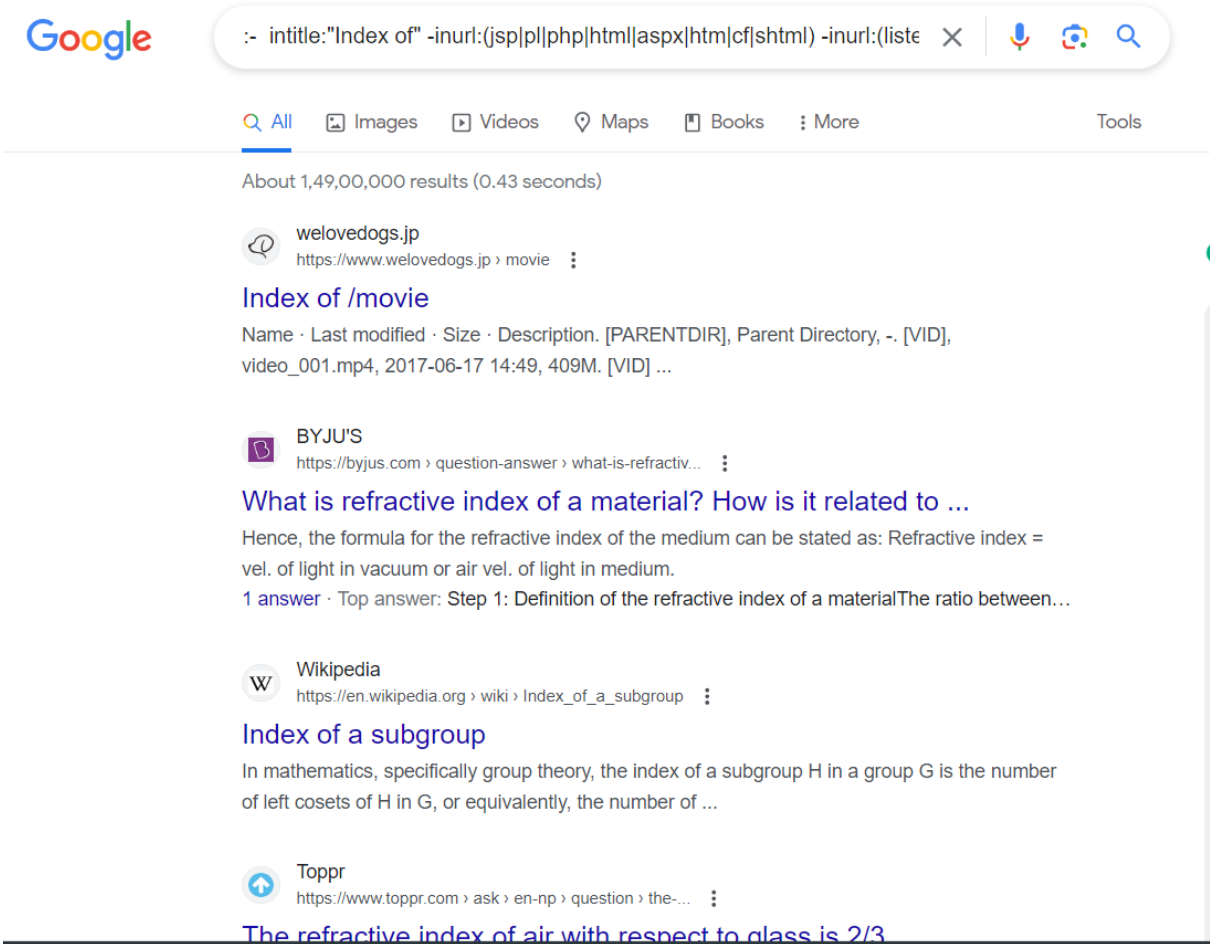
Google dorking, also known as Google hacking, is a technique where specific search queries are used to find sensitive information or vulnerabilities on websites by exploiting search engine operators and filters. It's often used by security professionals and hackers for reconnaissance and information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

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)

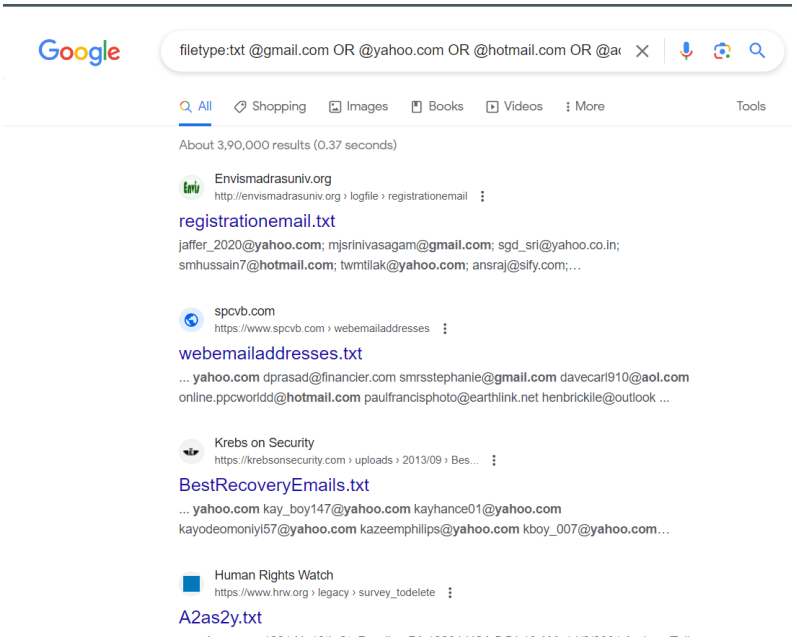
Description:- The above Google dork searches for web directories with the title "Index of" while excluding common web page extensions (jsp, pl, php, etc.) and known music-related directories (listen77, mp3raid, etc.). It helps find open directories containing various files for potential download.



2. Finding Email lists:

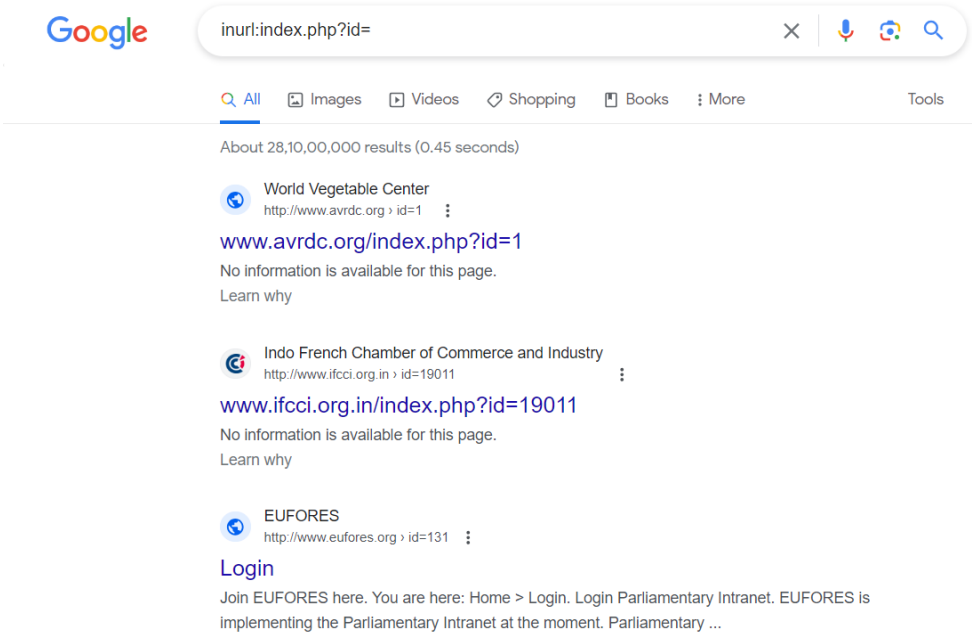
Dork:- filetype:txt @gmail.com OR @yahoo.com OR @hotmail.com OR @aol.com

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

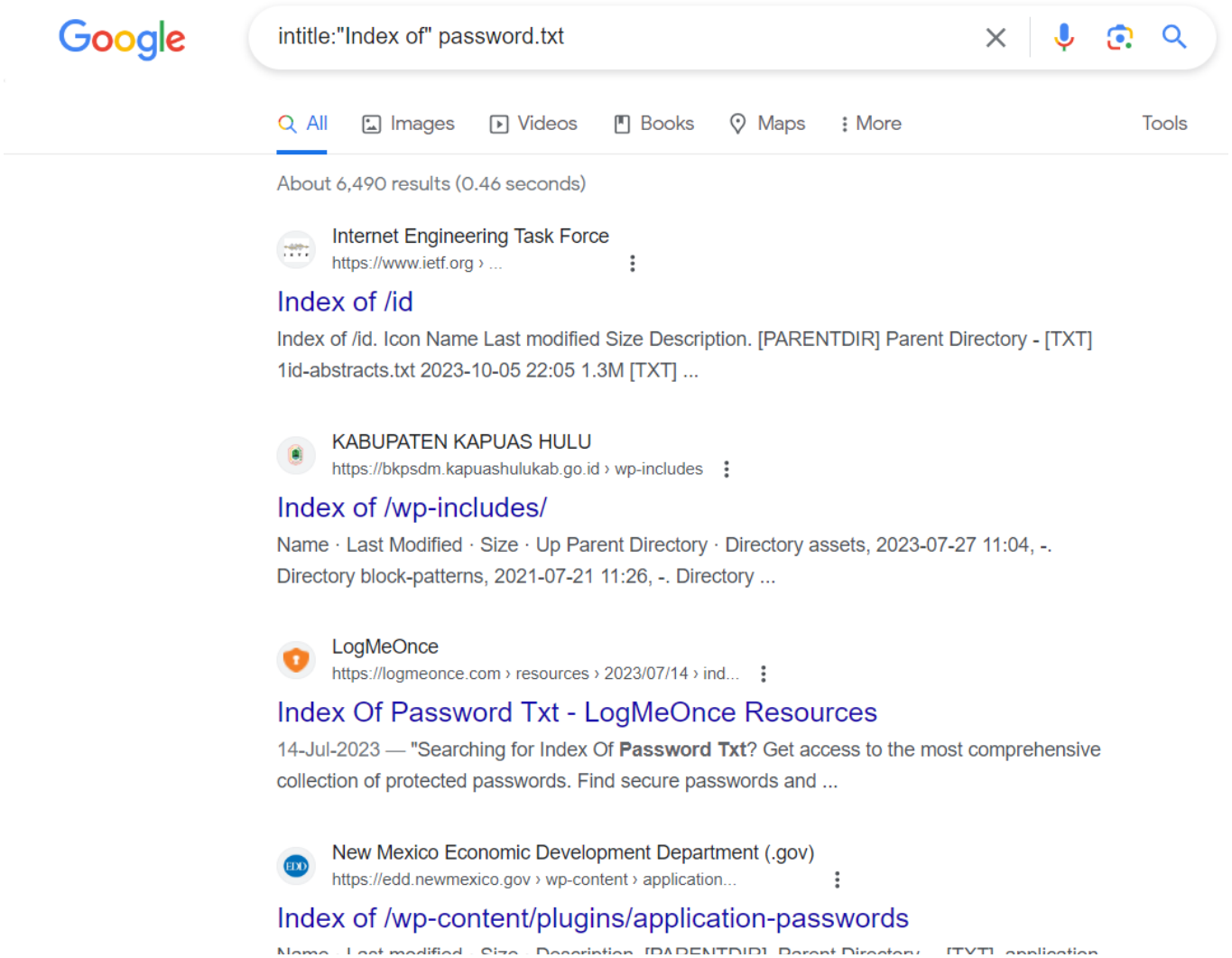
Dork:- inurl:index.php?id=
Description:- Google dorking using "inurl:index.php?id=" is a technique to search for websites with URLs containing "index.php?id=" in their address, often revealing potential vulnerabilities.



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.



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.