Madhur Nagrath(19CSU169)
DS-IV-C
Cyber Security

Reconnaissance Tools

Final Report on Flipkart.com

Background

Domain:	flipkartcom
Registry Domain ID:	21242797_DOMAIN_COM-VRSN
Site Title:	Flipkart.com: Buy shopping goods 429
Site rank:	
Description:	Flipkart is an e-commerce company headquartered in Bangalore, Karnataka, India, and registered in Singapore. The company initially focused on online book sales before expanding into other product categories such as consumer electronics, fashion, home essentials, groceries, and lifestyle products.
Created:	
Updated:	2000-03-03 12:13:23 UTC
Registry Expiration:	2022-03-03 12:13:23 UTC
Primary language:	English

Registrar Information

Domain registrar:	markmonitor.com
IANA ID:	292
Abuse contact email:	abusecomplaints@markmonitor.com
Abuse contact phone:	+1.2083895770

Network

Netblock Owner:	Automattic, Inc
Hosting company:	Automattic
Hosting country:	US
IPv4 address:	192.0.78.17
IPv4 autonomous systems:	AS2635

Madhur19csu169

Madhur
Nagrath(19CSU169) DS-IV-
C
Cyber Security

Nameserver:	ns1.flipkart.com (has 1,602,757 domains) ns2.flipkart.com (has 1,602,757 domains) ns3.flipkart.com (has 1,602,757 domains) ns4.flipkart.com (has 1,602,757 domains)
Nameserver organization:	whois.markmonitor.com
Organisation:	Automattic, Inc., United States
DNS admin:	mmmmmm@gmail.com
Top Level Domain:	Commercial entities (.com)

IP Delegation

IPv4 Address:	192.0.78.17 - 3,885 other sites hosted on this server
IP Location:	California - San Francisco - Automattic Inc
ASN:	AS2635 AUTOMATTIC, US (registered Oct 01, 2012)
IP History:	47 changes on 47 unique IP addresses over 17 years
Registrar History:	4 registrars
Hosting History:	9 changes on 6 unique name servers over 16 years

IP Range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
192.0.0.0-192.255.255.255	United States	NET192	Various Registries (Maintained by ARIN)
192.0.64.0-192.0.127.255	United States	AUTOMATTIC	Automattic, Inc
192.0.78.17	United States	AUTOMATTIC	Automattic, Inc

Authoritative Servers

Registry Server URL: https://rdap.verisign.com/com/v1/domain/flipkart.com

Last updated from Registry RDAP DB: 2021-02-22 17:14:41 UTC

Registrar Server URL:
https://rdap.markmonitor.com/rdap/domain/Flipkart.com

Last updated from Registrar RDAP DB: 2021-02-22 13:29:31 UTC

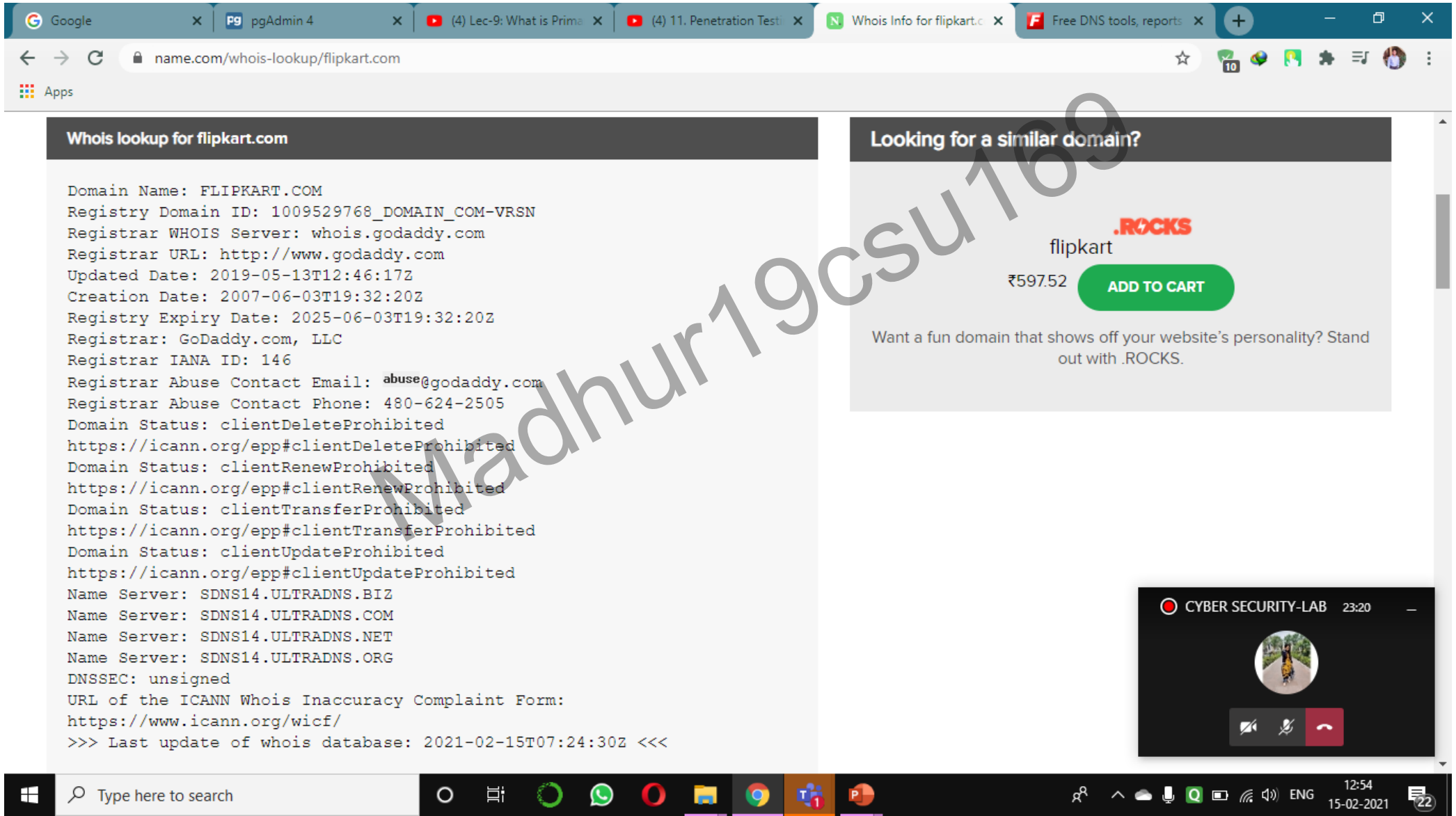
Madhur19csu169

Information Gathering Tools

Website: https://www.flipkart.com/

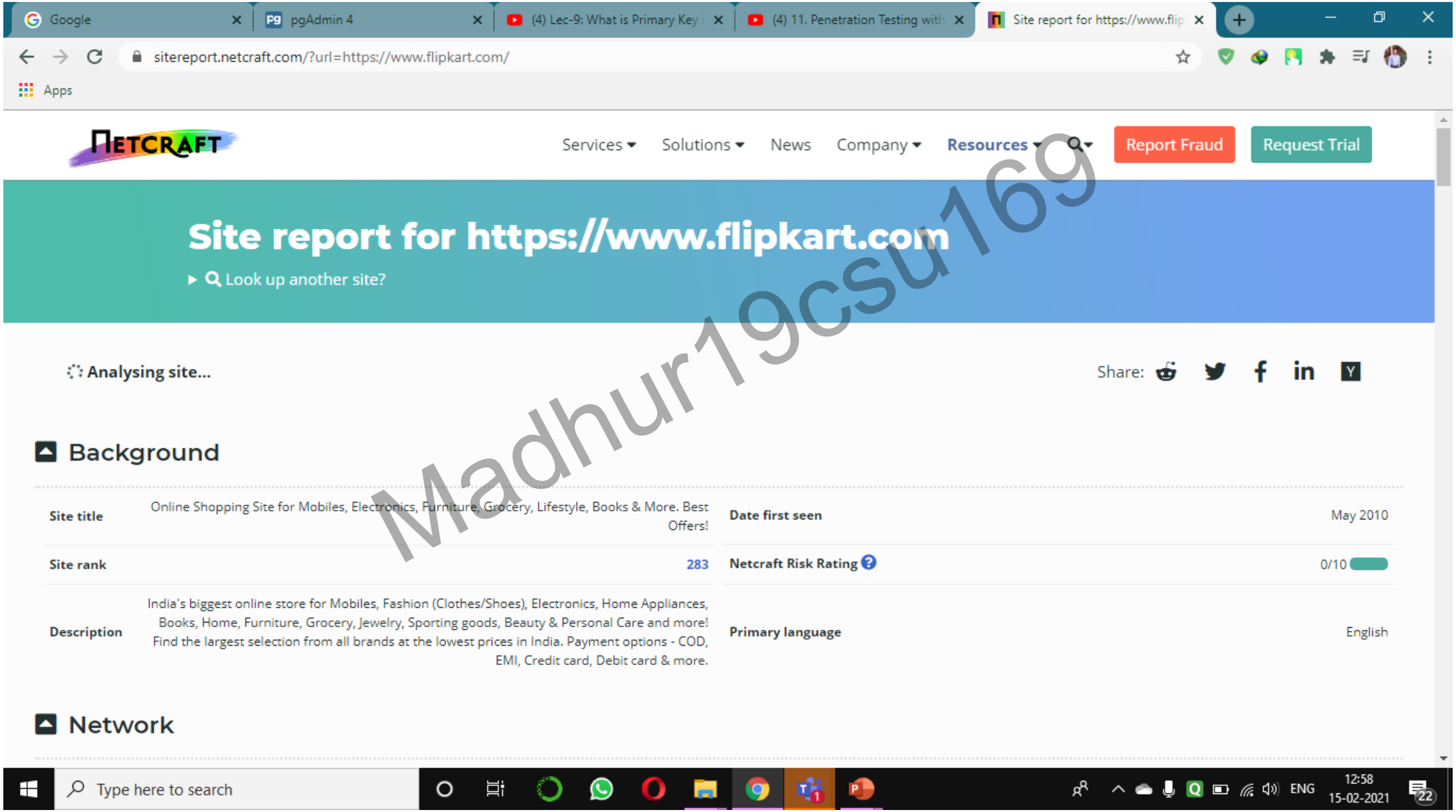
Madhur19csu169

Tool 1 : whois info.com

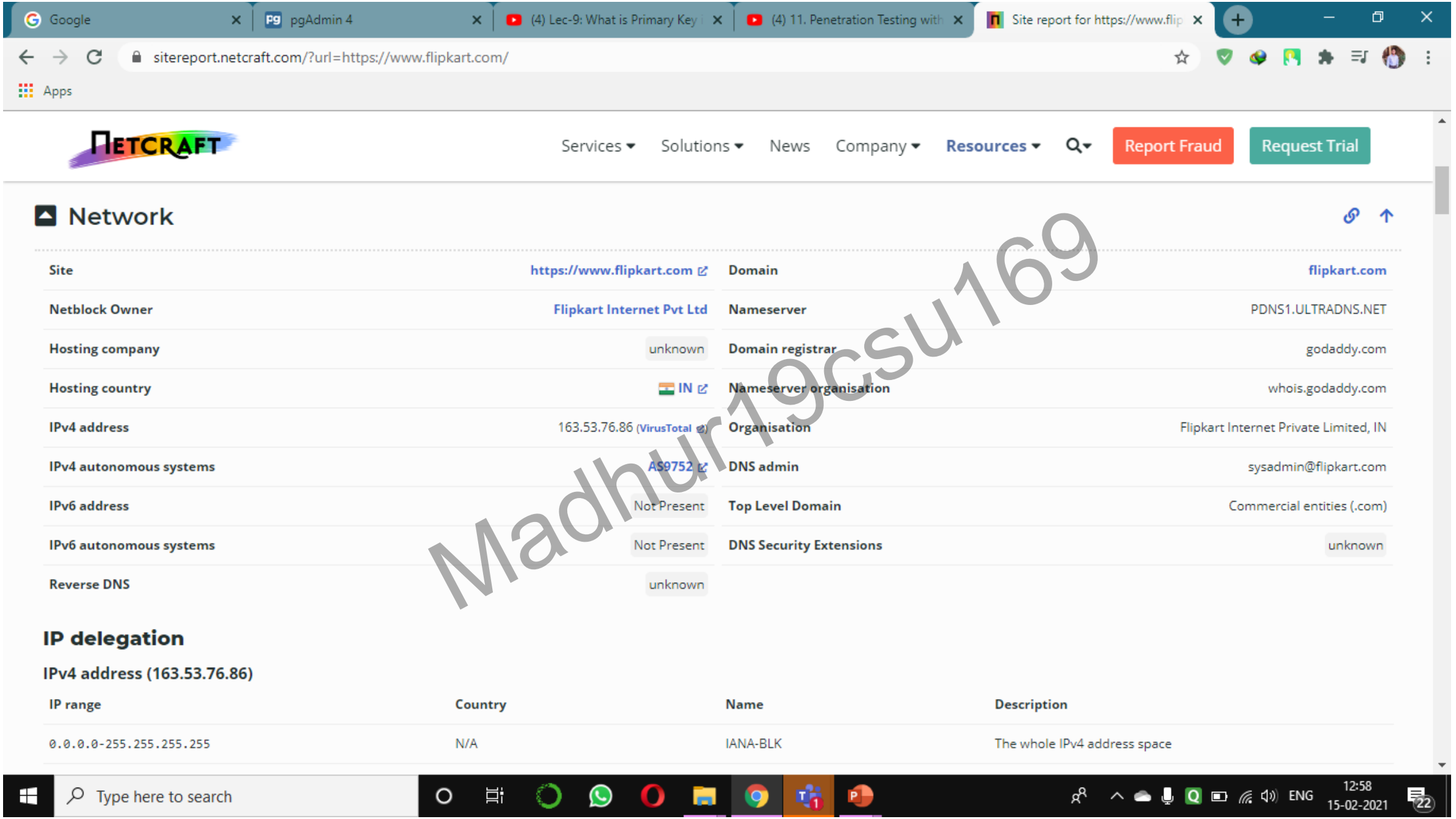


Madhur19csu169

Tool 2 : Netcraft.com



Madhur19csu169



Madhur19csu169

IP delegation

IPv4 address (163.53.76.86)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 163.0.0.0-163.255.255.255	Australia	APNIC-ERX-163	Asia Pacific Network Information Centre
↳ 163.53.76.0-163.53.79.255	India	FK-NET-IN	Flipkart Internet Pvt Ltd
↳ 163.53.76.86	India	FK-NET-IN	Flipkart Internet Pvt Ltd

Last Reboot (89 days ago)

SSL/TLS

Assurance	Domain validation	**Perfect Forward Secrecy**	Yes
Common name	www.flipkart.com	**Supported TLS Extensions**	RFC4366 server name, RFC5746 renegotiation info, RFC4492 EC point formats, RFC5077 session ticket
Organisation	Not Present	**Application-Layer Protocol Negotiation**	Not Present

Madhur19csu169

SSL/TLS

Assurance	Domain validation	**Perfect Forward Secrecy**	Yes
Common name	www.flipkart.com	**Supported TLS Extensions**	RFC4366 server name, RFC5746 renegotiation info, RFC4492 EC point formats, RFC5077 session ticket
Organisation	Not Present	**Application-Layer Protocol Negotiation**	Not Present
State	Not Present	**Next Protocol Negotiation**	Not Present
Country	Not Present	**Issuing organisation**	GoDaddy.com, Inc.
Organisational unit	Domain Control Validated	**Issuer common name**	Go Daddy Secure Certificate Authority - G2
Subject Alternative Name	▶ www.flipkart.com, flipkart.com, indusind.store.flipkart.com, offers.store.flipkart.com, bhaskar.store.flipkart.com, accounts.flipkart.com, itzcash.store.flipkart.com, m.flipkart.com, axis.store.flipkart.com, airtel.store.flipkart.com, yono.store.flipkart.com and 4 more	**Issuer unit**	http://certs.godaddy.com/repository/
Validity period	From Jul 23 2020 to Jul 23 2022 (24 months)	**Issuer location**	Scottsdale
Matches hostname	Yes	**Issuer country**	US
Server	nginx	**Issuer state**	Arizona
Public key		**Certificate Revocation Lists**	http://crl.godaddy.com/gdig2s1-2149.crl

Madhur19csu169

Version number	0x02

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Argon 2022 KXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4Q=	2020-07-23 07:55:02	Success
Certificate	DigiCert Yeti 2022 IkVFB1lVJFaWP6Ev8fdthuAjJmOtwEt/XcaDXG7iDwI=	2020-07-23 07:55:02	Success
Certificate	Let's Encrypt Oak 2022 36Veq2iCTx9sre64X04+WurNohKkal6OOxLAIERcKnM=	2020-07-23 07:55:02	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

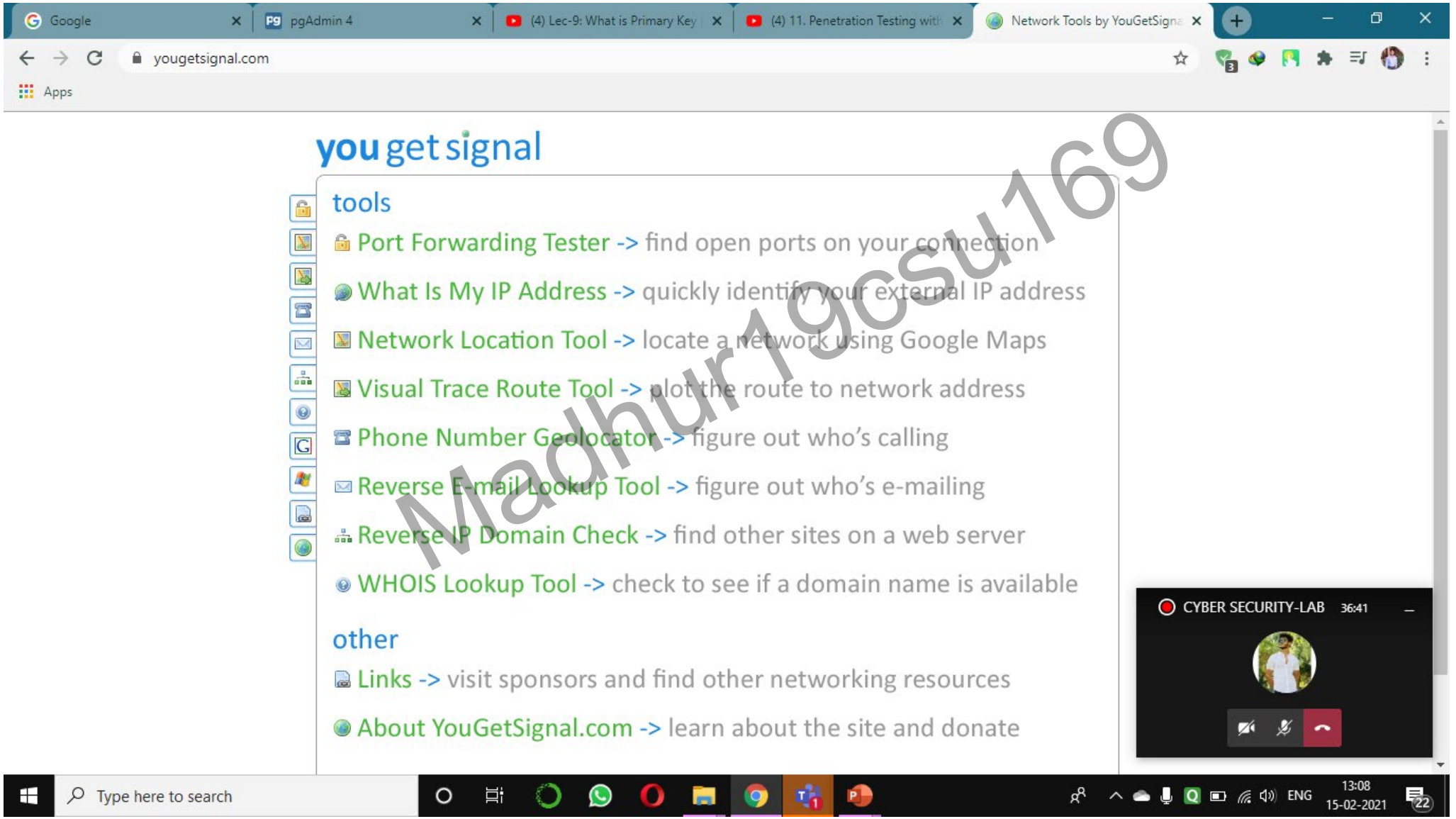
Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.

Madhur19csu169

Tool 3 : youget signal.com



Madhur19csu169

Google | pgAdmin 4 | (4) Lec-9: What is Primary Key | (4) 11. Penetration Testing with | Open Port Check Tool - Test Po

yougetsignal.com/tools/open-ports/

Apps

you get signal

Port Forwarding Tester

your external address

171.50.165.26

open port finder

Remote Address 171.50.165.26 Port Number 80 Check

Use Current IP

Check a port's status by entering an address and port number above.

about

The open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is setup correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. It is important to note that some ports, such as port 25, are often blocked at the ISP level in an attempt to prevent malicious activity.

For more a comprehensive list of TCP and UDP ports, check out this Wikipedia article.

If you are looking for a software solution to help you configure port forwarding on your network, try using this powerful Port Forwarding Wizard.

If my tool has been helpful to you, check out my desktop wallpaper site or follow me on Twitter @kirkouimet. Also, if your router is causing you massive grief try picking up a cheap Netgear N600 on Amazon.

common ports

21 FTP
22 SSH
23 TELNET
25 SMTP
53 DNS
80 HTTP
110 POP3
115 SFTP
135 RPC
139 NetBIOS
143 IMAP
194 IRC
443 SSL
445 SMB
1433 MSSQL
3306 MySQL
3389 Remote Desktop
5632 PCAnywhere
5900 VNC
25565 Minecraft
Scan All Common Ports

Mayhur1965u169

©2009 Kirk Ouimet Design. All rights reserved. Privacy Policy. Hosted by VPSServer.com.

CYBER SECURITY-LAB 36:50

Type here to search

ENG 13:08 15-02-2021

Google | pgAdmin 4 | (4) Lec-9: What is Primary Key | (4) 11. Penetration Testing with | IP Location Tool - Locate a Net

yougetsignal.com/tools/network-location/

Apps

you get signal

Network Location Tool

approximate geophysical location

network information

IP Address
193.34.232.23
Base Domain
193.34.232.23
Country
United Kingdom
Region
C5
City
Speke
Latitude
53.3333
Longitude
-2.85
Area Code
Unknown
Postal Code
Unknown
Distance from Last (as the crow flies)
0 miles
Source
MaxMind

locate a network

Remote Address 193.34.232.23 Locate
Use Current IP
Source ◉ MaxMind ○ Hostip.info

about

Madhur19csu169

CYBER SECURITY-LAB 37:02

Type here to search

ENG 13:08 15-02-2021

Google | pgAdmin 4 | (4) Lec-9: What is Primary Key | (4) 11. Penetration Testing with | What is My IP Address?

yougetsignal.com/what-is-my-ip-address/

Apps

you get signal

Your IP address is:

2.58.194.138

Madhur19csu169

©2009 Kirk Ouimet Design. All rights reserved. Privacy Policy. Hosted by VPSServer.com.

CYBER SECURITY-LAB 38:06

Type here to search

ENG 13:09 15-02-2021

Google | pgAdmin 4 | (4) Lec-9: What is Primary Key | (4) 11. Penetration Testing with | Spokeo | People Search

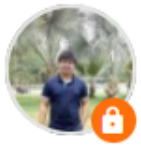
spokeo.com/purchase?escape=false&q=sw-ewUQ7zFpmZoWbTE8_Oh7u_xxPxPXeEAaTXFkPttYcTgTd-2bvVZPZw&sc=U%7Cg%3Dgeneral_text_1_A...

Apps

SPOKEO

Get Instant Information on madhurnagrath@gmail.com

Your Purchase is confidential. The Social Owner of **madhurnagrath@gmail.com** will **NOT** be notified of your purchase.



RESULTS ARE READY!

madhur nagrath

Latest report as of 02/14/2021

Report Includes Available Information On:

OWNER'S NAME:	Madhur Nagrath
SOCIAL PROFILES:	1 Social Profile Found
PROFILE PHOTOS:	See Available Results
DATING PROFILES:	See Available Results
CONTACT DETAILS:	See Available Results
ADDRESS HISTORY:	See Available Results

PICK YOUR OPTION

FULL SOCIAL REPORT

$0.95 51% OFF

SPECIAL PRICE

CONTINUE >

Special Offer with FREE Trial Membership gives you:

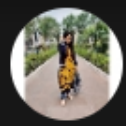
- **Full Access to Social Search**
  Find people in the U.S. by social to quickly see their social profiles, photos, and more.
- **Instant Access to Name, Phone & Address Search**

Social Report Only

$1.95 regular price

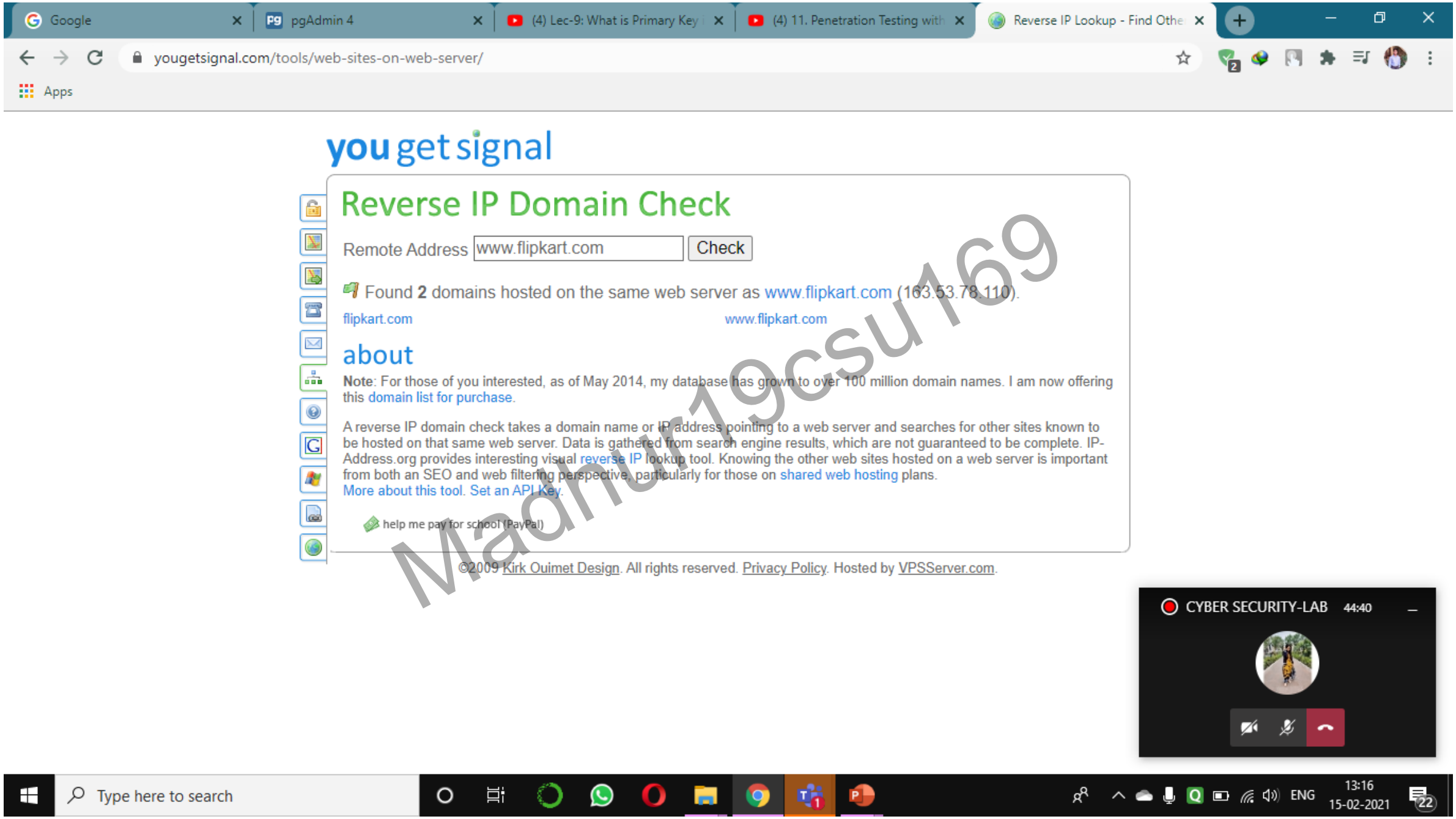
Madhur19csu169

CYBER SECURITY-LAB 40:29

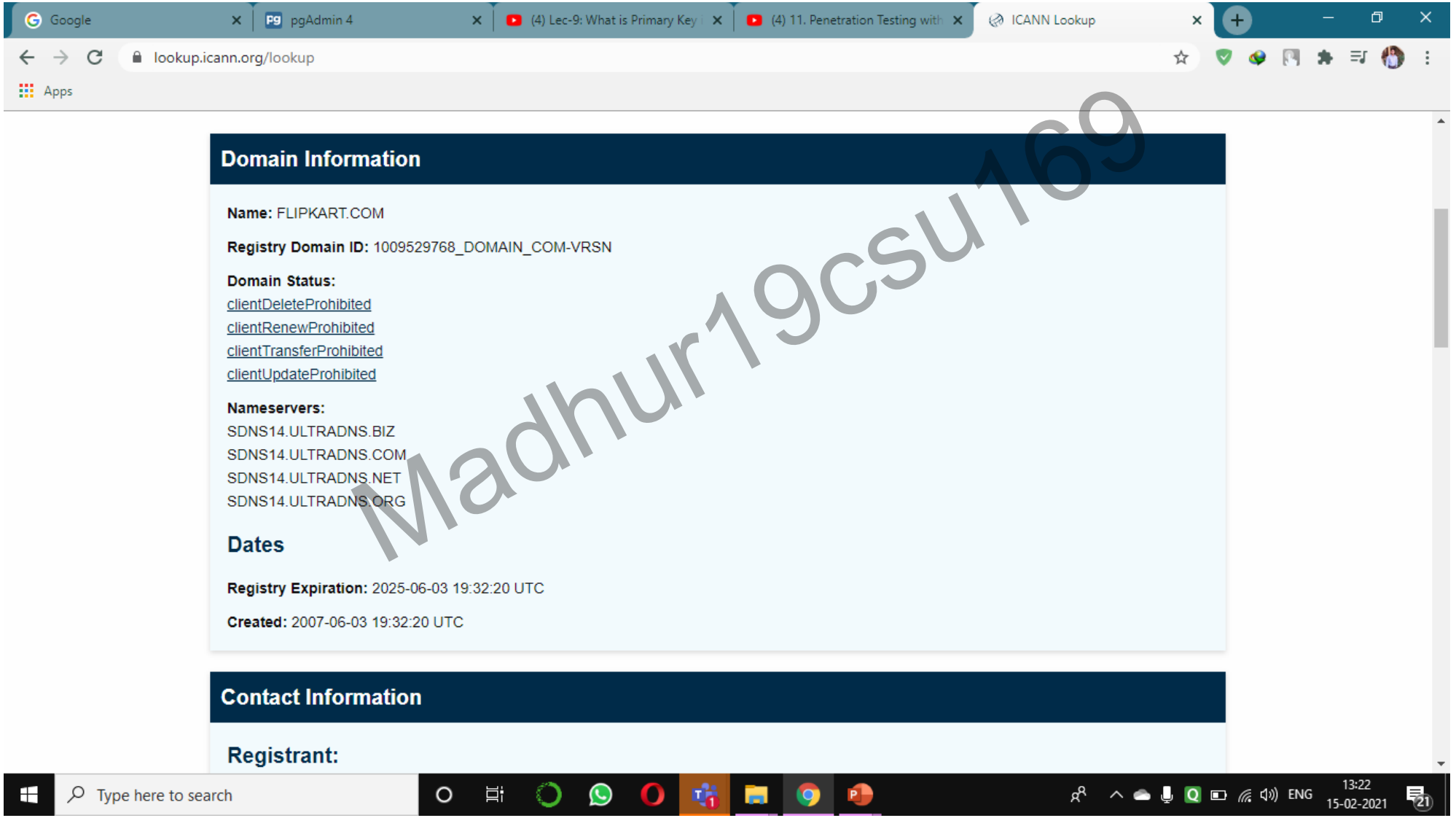


Type here to search

ENG 13:11 15-02-2021


Google
pgAdmin 4
(4) Lec-9: What is Primary Key
(4) 11. Penetration Testing with
Reverse IP Lookup - Find Othe
yougetsignal.com/tools/web-sites-on-web-server/
Apps
you get signal
Reverse IP Domain Check
Remote Address www.flipkart.com Check
Found 2 domains hosted on the same web server as www.flipkart.com (163.53.78.110).
flipkart.com
www.flipkart.com
about
Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this domain list for purchase.
A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides interesting visual reverse IP lookup tool. Knowing the other web sites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on shared web hosting plans.
More about this tool. Set an API Key.
help me pay for school (PayPal)
©2009 Kirk Ouimet Design. All rights reserved. Privacy Policy. Hosted by VPSServer.com.
Madhur19csu169
CYBER SECURITY-LAB 44:40
Type here to search
ENG
13:16
15-02-2021

Tool 5: lookup.icann.org



Madhur19csu169

Google | pgAdmin 4 | (4) Lec-9: What is Primary Key | (4) 11. Penetration Testing with | ICANN Lookup
lookup.icann.org/lookup
Apps

Contact Information

Registrant:

Organization: Flipkart Internet Private Limited

Mailing Address: Karnataka, India

Technical:

Organization: Flipkart Internet Pvt Ltd

Mailing Address: Karnataka, India

Administrative:

Organization: Flipkart Internet Pvt Ltd

Mailing Address: Karnataka, India

Billing:

Organization: Flipkart Internet Pvt Ltd

Mailing Address: Karnataka, India

Redacted for privacy: some of the data in this object has been removed.

Madhur19csu169

Registrar Information

Type here to search
ENG 13:22 15-02-2021

Google | pgAdmin 4 | (4) Lec-9: What is Primary Key | (4) 11. Penetration Testing with | ICANN Lookup
lookup.icann.org/lookup
Apps

Registrar Information

Name: GoDaddy.com, LLC

IANA ID: 146

Abuse contact email: abuse@godaddy.com

Abuse contact phone: tel:480-624-2505

DNSSEC Information

Delegation Signed: Unsigned

Authoritative Servers

Registry Server URL: https://rdap.verisign.com/com/v1/domain/flipkart.com

Last updated from Registry RDAP DB: 2021-02-15 17:06:32 UTC

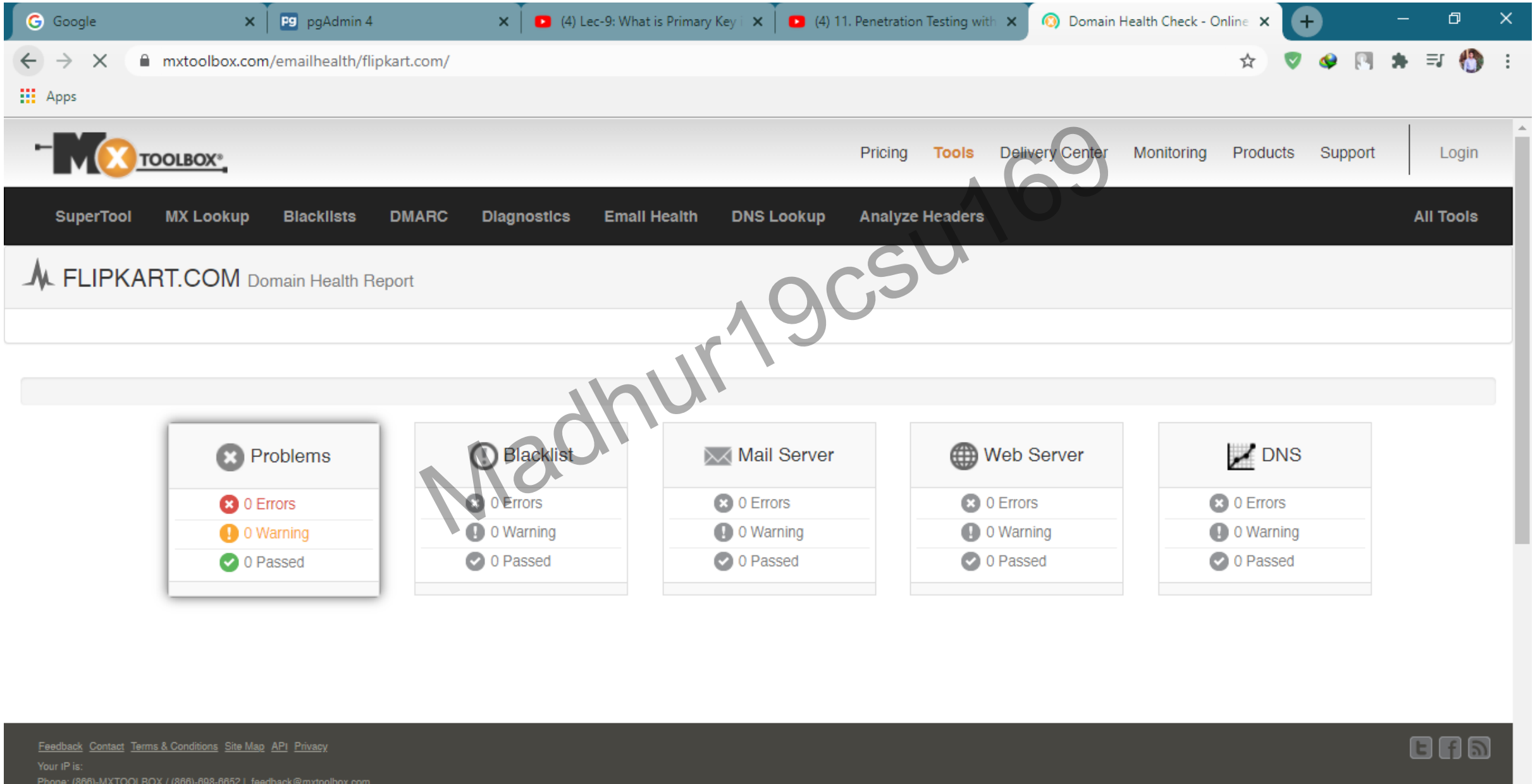
Registrar Server URL: https://rdap.godaddy.com/v1/domain/FLIPKART.COM

Last updated from Registrar RDAP DB: 2021-02-15 13:21:09 UTC

Madhur19csu169

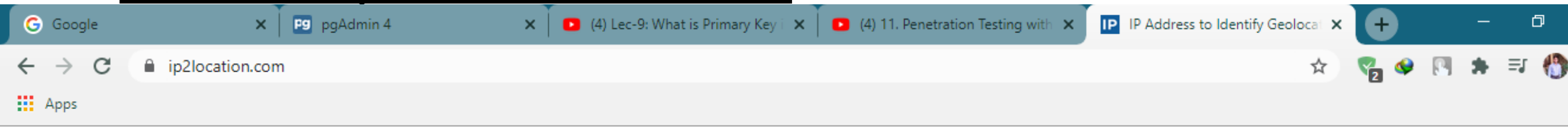
Type here to search
ENG 13:22 15-02-2021

Tool 6 :Mxtoolbox.com



Madhur19csu169

Tool 7 : ip2location.com



Learn more about your Internet traffics

Madhur19csu169

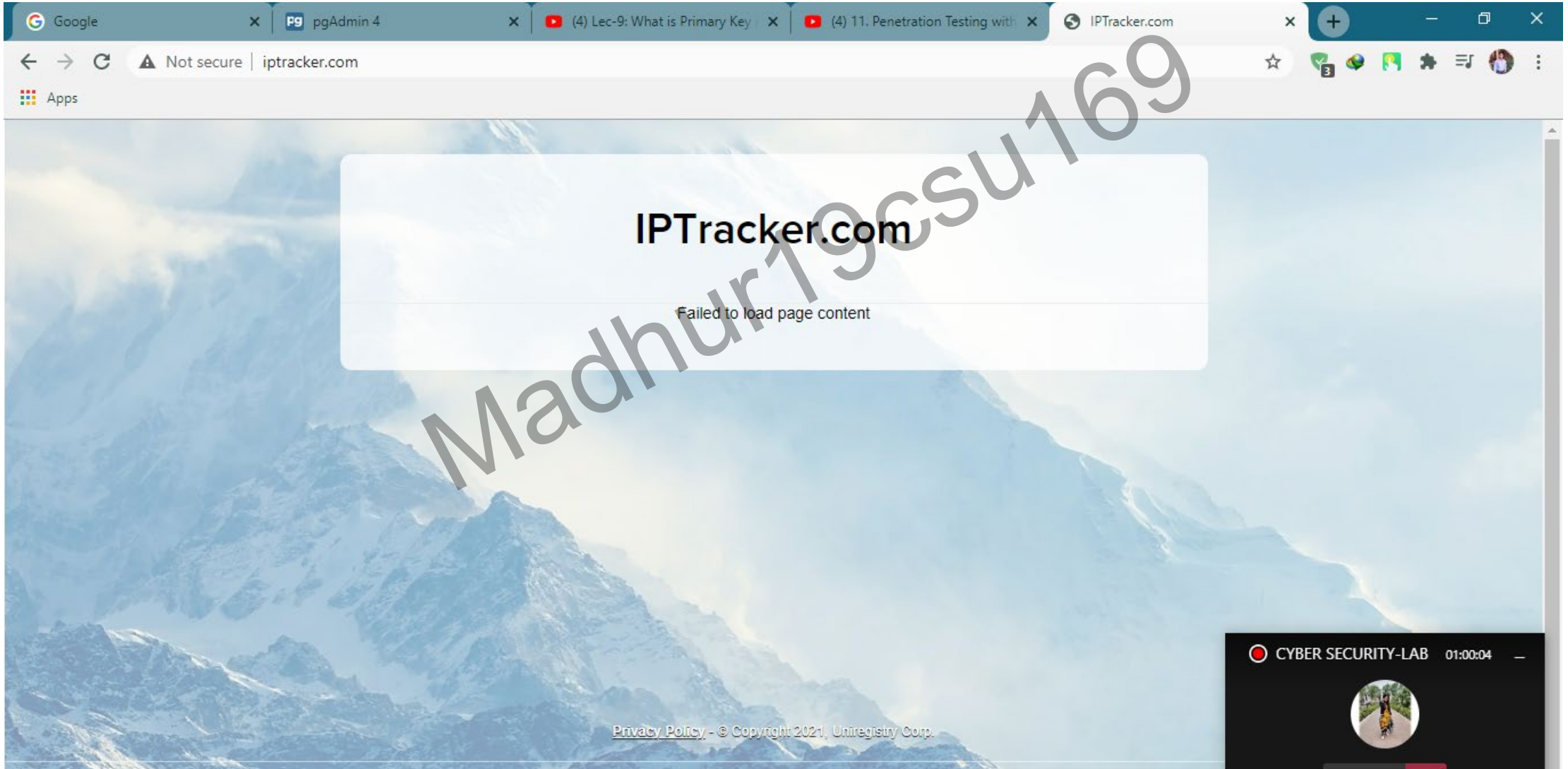
Your IP Address 171.50.165.26	**Domain** airtel.in	**Is Proxy** No
Country India	**Net Speed** DSL	**Proxy Type** -
Region Haryana	**IDD & Area Code** +(91) 0124	**ASN** -
City Gurgaon	**ZIP Code** 122101	**Security Threat** -
Coordinates 28.46667, 77.03333	**Weather Station** New Delhi/Safdarjung (INXX0142)	**Proxy Last Seen** -
ISP Bharti Airtel Ltd.	**Elevation** 224 m	
Time Zone +05:30	**Usage Type** ISP/MOB	

Try IP2Location Demo

171.50.165.26 LOOK UP

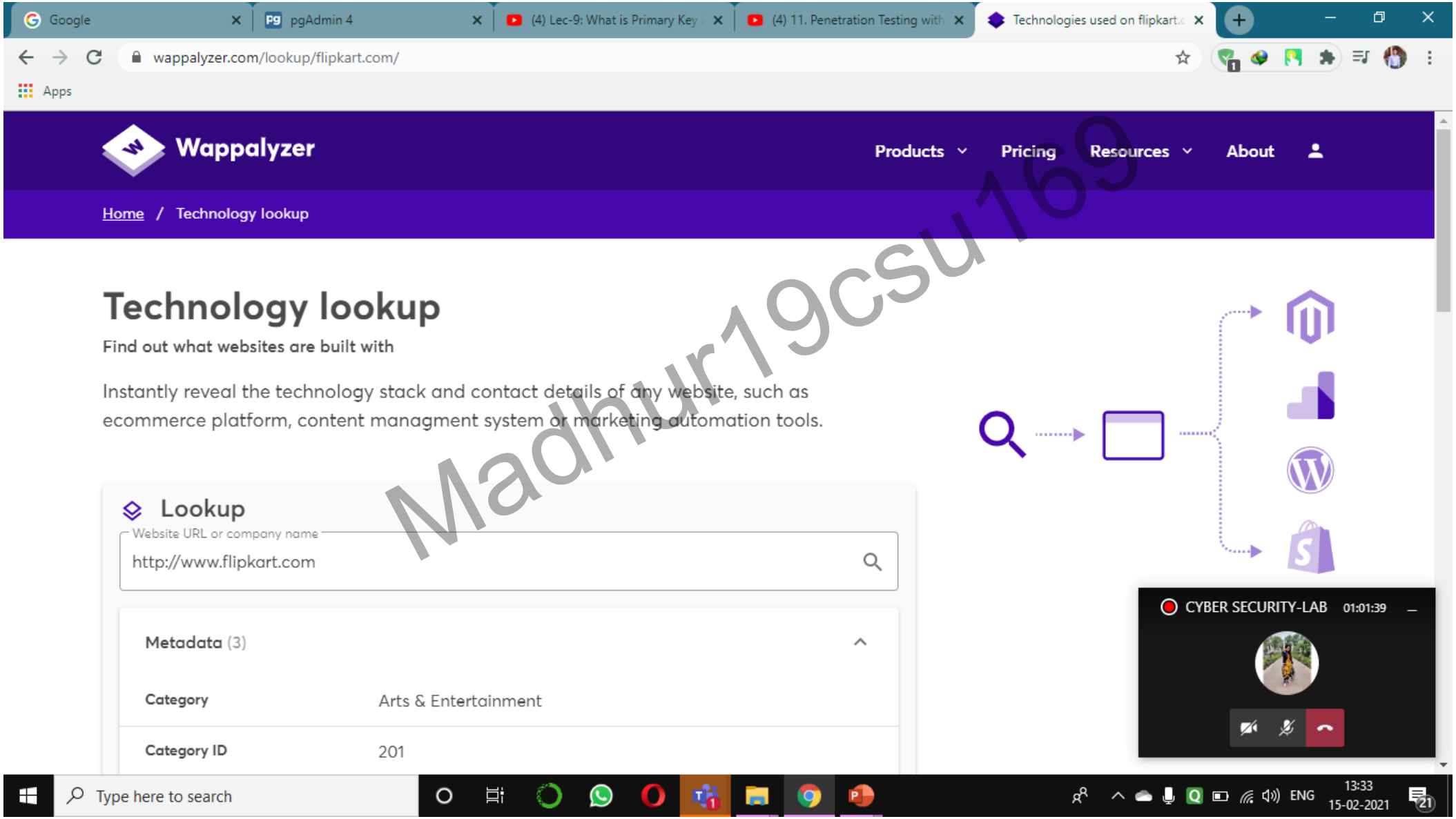
Try out the demo to get the comprehensive geolocation data of an IP address. Supports both IPv4 and IPv6 address lookup.

Tool 8 : iptracker.com



Madhur19csu169

Tool 9 : Wappalyzer.com



Madhur19csu169

Category ID	201
Title	Online Shopping Site for Mobiles, Electronics, Furniture, Grocery, Lifestyle, Books & More. Best Offers!

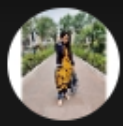
Locale (2)

Technologies (9)

React	JavaScript frameworks
Nginx	Web servers
Nginx	Reverse proxies
webpack	Miscellaneous
Adobe Experience Platform Identity Service	Analytics
Adobe Analytics	
Cart Functionality	Ecommerce
Sentry	Issue trackers

Madhur19csu169

CYBER SECURITY-LAB 01:01:43



Nginx	Web servers
Nginx	Reverse proxies
webpack	Miscellaneous
Adobe Experience Platform Identity Service Adobe Analytics	Analytics
Cart Functionality	Ecommerce
Sentry	Issue trackers
Google Workspace	Webmail
Google Workspace MailChimp	Email
MailChimp	Marketing automation

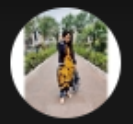
Madhur19csu169

Look up 5,000 websites at once with Bulk lookup.

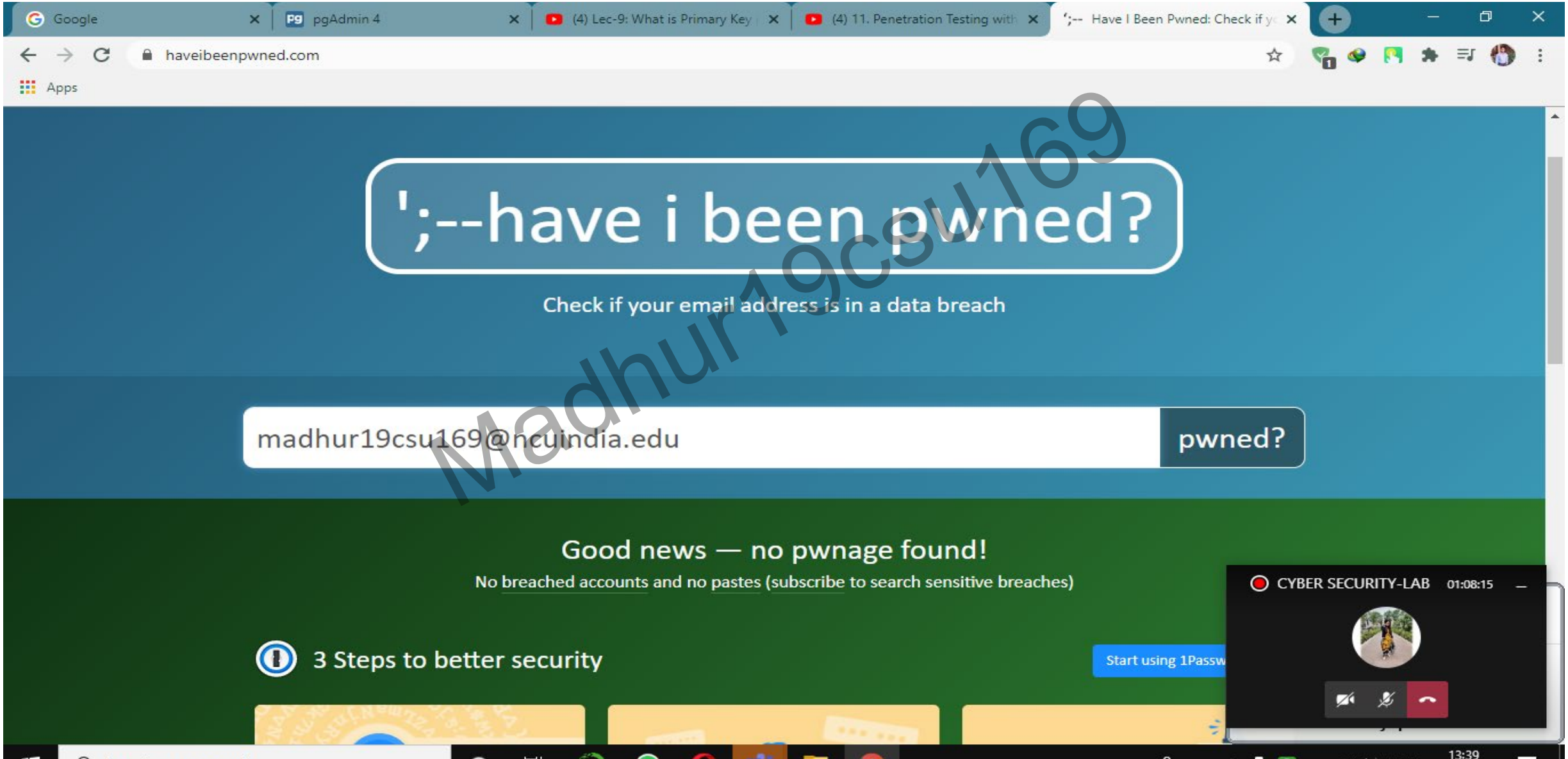
Automate lookups with the Lookup API or CRM integration.

Get the free browser extension.

CYBER SECURITY-LAB 01:01:47



Tool 10 : haveibeenpawned.com



Madhur19csu169

Google | pgAdmin 4 | (4) Lec-9: What is Primary Key | (4) 11. Penetration Testing with | ';-- Have I Been Pwned: Check if y

haveibeenpwned.com

Apps

';--have i been pwned?

Check if your email address is in a data breach

madhurnagrath@gmail.com pwned?

Madhur19csu169

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Passw

CYBER SECURITY-LAB 01:09:01

Type here to search

ENG 13:40 15-02-2021

Tool 11 : Pipl.com

Madhur19csu169