

# PRACTICAL: INFORMATION GATHERING



SUBMITTED BY: RAVEEHA NASEEM  
LAIBA REHMAN  
AYESHA MUSTAFA  
SUMMITTED TO: SIR BILAL

**CORVIT EDUCATION SYSTEM MULTAN**

**TARGET: TATA CONSULTANCY SERVICES (TCS)**

**URL: <https://www.tcs.com/>**

## PASSIVE INFORMATION GATHERING

**By using Subdomain Finder**

Subdomain	IP	CloudFlare
agileSPACE.tcs.com	219.64.33.94	FALSE
alm4jal.mastercraft.tcs.com	14.140.248.159	FALSE
apg-asia2.tcs.com	20.204.69.161	FALSE
apg-eastus2.tcs.com	20.127.135.8	FALSE
apg-europe2.tcs.com	23.100.48.199	FALSE
apgasia-assets.tcs.com	52.172.249.100	FALSE
apgasia-preprod2.tcs.com	52.172.218.148	FALSE
apgeus-assets.tcs.com	20.62.217.113	FALSE
apphonics.tcs.com	125.17.73.221	FALSE
appmart.tcs.com	203.199.19.237	FALSE
assets.tcs.com	23.55.225.139	FALSE
autodiscover.tcs.com	45.249.218.30	FALSE
bancssupport.tcs.com	121.241.193.21	FALSE
bap.workspace.tcs.com	115.111.203.40	FALSE
bbsbbt.workspace.tcs.com	14.141.110.80	FALSE
blranc.workspace.tcs.com	121.241.130.114	FALSE
blrbhu.workspace.tcs.com	14.143.34.117	FALSE
blrbhuwfh.workspace.tcs.com	14.143.34.126	FALSE
blrexp.workspace.tcs.com	115.112.63.246	FALSE
blrgla.workspace.tcs.com	219.65.96.41	FALSE
blrlce.workspace.tcs.com	121.241.193.189	FALSE
blrpio.workspace.tcs.com	122.15.43.11	FALSE
blrtkc.workspace.tcs.com	121.242.29.16	FALSE
blrvic.workspace.tcs.com	14.143.178.220	FALSE
bodapp.tcs.com	203.199.20.249	FALSE
bodstore.tcs.com	121.240.8.182	FALSE
brazilbsi.tcs.com	200.212.144.8	FALSE

brtamm02.tcs.com	208.44.114.52	FALSE
brtamm102.tcs.com	65.51.161.134	FALSE
careers.tcs.com	4.247.162.6	FALSE
cdc.workspace.tcs.com	45.249.218.26	FALSE
cdcn.workspace.tcs.com	45.249.218.46	FALSE
cep.bpo.tcs.com	115.112.77.102	FALSE
chncho.workspace.tcs.com	121.242.62.162	FALSE
chnexo.tcs.com	122.184.60.102	FALSE
chnicc.workspace.tcs.com	125.17.102.210	FALSE
chnmgm.workspace.tcs.com	125.21.186.16	FALSE
chnsir.workspace.tcs.com	121.241.146.221	FALSE
chnsnr.workspace.tcs.com	203.199.254.134	FALSE
chntdl.workspace.tcs.com	203.199.209.99	FALSE
chntrl.workspace.tcs.com	14.141.100.174	FALSE
chnvel.workspace.tcs.com	202.54.180.188	FALSE
conference1.tcs.com	172.21.161.172	FALSE
delgg5.workspace.tcs.com	121.242.45.149	FALSE
delgg6.workspace.tcs.com	115.111.246.85	FALSE
delgg7.workspace.tcs.com	121.241.127.34	FALSE
delnd5.workspace.tcs.com	14.143.181.86	FALSE
delnd6.workspace.tcs.com	121.241.103.58	FALSE
delndo.workspace.tcs.com	14.140.71.126	FALSE
digitalsoftware.tcs.com	14.141.110.181	FALSE
dominoconnect.tcs.com	219.64.34.32	FALSE
ebcssl1.tcs.com	122.15.107.26	FALSE
ebcssl2.tcs.com	14.141.164.242	FALSE
emeaswzprovpn01.tcs.com	51.107.86.224	FALSE
emeaswzprovpn02.tcs.com	51.107.86.138	FALSE
filesync.tcs.com	219.64.33.248	FALSE
ftc.tcs.com	59.163.27.22	FALSE
gbams.tcs.com	203.199.19.93	FALSE
gnrgc.workspace.tcs.com	14.142.138.115	FALSE
gnrgp.workspace.tcs.com	14.142.16.6	FALSE
grs.tcs.com	219.64.34.57	FALSE
guestwifi.tcs.com	219.64.33.183	FALSE
hungaryvpn.tcs.com	91.120.250.11	FALSE
hydadi.workspace.tcs.com	182.19.66.181	FALSE
hyddep.workspace.tcs.com	203.200.212.60	FALSE
hydsp4.workspace.tcs.com	115.111.228.95	FALSE
hydssp.workspace.tcs.com	121.241.164.50	FALSE
ibegin.tcs.com	121.240.8.35	FALSE
inblrg01.tcs.com	121.242.48.3	FALSE
inblrg02.tcs.com	121.242.48.116	FALSE

inblrg03.tcs.com	121.242.48.29	FALSE
inchng01.tcs.com	122.184.60.13	FALSE
inchng02.tcs.com	122.184.60.14	FALSE
inchng03.tcs.com	122.184.60.32	FALSE
inchng04.tcs.com	122.184.60.109	FALSE
inchngs01.tcs.com	14.143.141.144	FALSE
inchngs02.tcs.com	14.143.141.145	FALSE
inchnprojectvpn.tcs.com	121.242.63.49	FALSE
inchntelstravpn.tcs.com	52.172.49.196	FALSE
inchnvpn.tcs.com	122.184.60.22	FALSE
indelg01.tcs.com	203.200.109.55	FALSE
indelg02.tcs.com	203.200.109.58	FALSE
indruk02.tcs.com	219.64.33.204	FALSE
indruk03.tcs.com	219.64.33.177	FALSE
indruktv01.tcs.com	219.64.33.34	FALSE
indsez.workspace.tcs.com	14.143.129.4	FALSE
info.tcs.com	104.17.71.206	TRUE
inggnloandepotvpn.tcs.com	52.163.249.74	FALSE
inhyverizonvpn.tcs.com	52.172.30.223	FALSE
inmumg01.tcs.com	219.64.33.12	FALSE
inmumg02.tcs.com	219.64.33.222	FALSE
inmumg03.tcs.com	219.64.33.120	FALSE
inmumg04.tcs.com	45.249.218.97	FALSE
inmumgs01.tcs.com	219.64.33.40	FALSE
inmumgs02.tcs.com	219.64.34.164	FALSE
inmumitv09.tcs.com	10.52.160.108	FALSE
inmummig01.tcs.com	219.64.33.249	FALSE
inmummig02.tcs.com	219.64.33.250	FALSE
inmumprojectvpn.tcs.com	219.64.33.95	FALSE
inmumtcshosvpn.tcs.com	115.113.106.159	FALSE
inmumtelstravpn.tcs.com	52.172.188.47	FALSE
inmumuatvpn.tcs.com	219.64.33.195	FALSE
inmumvpn.tcs.com	219.64.33.210	FALSE
inmumvpn1.tcs.com	45.249.218.250	FALSE
inmumvpn2.tcs.com	45.249.218.251	FALSE
inmumvpnaz.tcs.com	13.71.68.18	FALSE
inpundutelecomvpn.tcs.com	52.172.12.91	FALSE
inpunspdigitatevpn.tcs.com	14.142.130.36	FALSE
inpunspvpn.tcs.com	14.140.45.250	FALSE
inpunspvpn2.tcs.com	14.140.45.251	FALSE
investors.tcs.com	184.30.132.46	FALSE
isometrix.tcs.com	121.241.146.81	FALSE
isometrixr.tcs.com	121.241.146.198	FALSE

koccen.workspace.tcs.com	14.140.177.165	FALSE
koleco01.workspace.tcs.com	115.112.160.130	FALSE
kolgpr.workspace.tcs.com	118.185.75.76	FALSE
kolinf.workspace.tcs.com	125.16.11.212	FALSE
kolsal.workspace.tcs.com	59.163.128.128	FALSE
login.workspace.tcs.com	45.249.218.68	FALSE
mail.tcs.com	122.184.60.102	FALSE
mailsync.tcs.com	45.249.218.30	FALSE
moss1.tcs.com	219.64.33.178	FALSE
mumbaiconnect.tcs.com	219.64.33.92	FALSE
mumexo.tcs.com	45.249.218.30	FALSE
mumken.workspace.tcs.com	121.242.10.90	FALSE
mumolym.workspace.tcs.com	59.145.67.186	FALSE
mumspz.workspace.tcs.com	115.113.136.165	FALSE
mumyap.workspace.tcs.com	121.241.6.209	FALSE
mumyapn.workspace.tcs.com	121.241.6.232	FALSE
myapp.tcs.com	121.240.8.152	FALSE
nextstep.tcs.com	203.199.20.21	FALSE
ngpmih.workspace.tcs.com	122.252.236.53	FALSE
ngpmih2.workspace.tcs.com	14.142.236.53	FALSE
nikochiwhf.tcs.com	14.142.53.38	FALSE
noamconnect.tcs.com	208.44.114.100	FALSE
on.tcs.com	67.199.248.12	FALSE
optumera-retail.tcs.com	45.114.77.234	FALSE
patved.workspace.tcs.com	115.112.74.202	FALSE
perspectives.tcs.com	40.114.36.22	FALSE
peruclaro.tcs.com	104.41.49.56	FALSE
pilot-qa.tcs.com	255.255.255.255	FALSE
pilot-qa2.tcs.com	52.172.218.148	FALSE
puncyp.workspace.tcs.com	14.143.46.214	FALSE
punsp.workspace.tcs.com	59.160.73.119	FALSE
safetyfirst.tcs.com	219.64.33.126	FALSE
sam.ey.tcs.com	14.142.107.34	FALSE
secureaccess.tcs.com	14.143.141.164	FALSE
secureaccessjuniper.tcs.com	121.242.30.84	FALSE
slides.tcs.com	219.64.33.170	FALSE
smetrics.tcs.com	63.140.62.17	FALSE
sustainisprod.mastercraft.tcs.com	121.241.146.185	FALSE
tcsapcgtlsbc01.tcs.com	103.120.19.201	FALSE
tcsemeagtlsbc01.tcs.com	31.171.245.100	FALSE
tcsfsvpn.tcs.com	210.9.102.198	FALSE
tcsnoamgtlsbc01.tcs.com	162.213.36.177	FALSE
tvmpp.workspace.tcs.com	122.15.83.70	FALSE

tvmsez.workspace.tcs.com	14.141.182.222	FALSE
uklong01.tcs.com	80.82.129.165	FALSE
uklong02.tcs.com	80.82.129.166	FALSE
ukprivpn.tcs.com	80.82.129.188	FALSE
uksecvpn.tcs.com	195.219.173.134	FALSE
usbankvpn.tcs.com	23.99.196.169	FALSE
uscinsapvpn.tcs.com	12.36.190.162	FALSE
usnjyg01.tcs.com	208.44.114.64	FALSE
usprivpn.tcs.com	208.44.114.226	FALSE
ussecvpn.tcs.com	65.51.161.148	FALSE
ustv03.tcs.com	10.101.136.169	FALSE
vc.tcs.com	219.64.33.59	FALSE
vcse.tcs.com	8.20.250.15	FALSE
vcseindia.tcs.com	115.111.249.140	FALSE
vcseus.tcs.com	8.20.250.15	FALSE
video.tcs.com	172.17.253.140	FALSE
vmsprocurement.tcs.com	219.64.33.174	FALSE
webmail.tcs.com	219.64.34.213	FALSE
workspace.tcs.com	45.249.218.47	FALSE
www.alumniportal.tcs.com	20.193.149.15	FALSE
www.careers.tcs.com	4.247.162.6	FALSE
www.investors.tcs.com	23.55.225.139	FALSE
www.mastercraft.tcs.com	115.112.72.174	FALSE
www.pilot-qa.tcs.com	255.255.255.255	FALSE
www.pilotqa-business4.tcs.com	255.255.255.255	FALSE
www.secureaccess.tcs.com	14.143.141.164	FALSE
www.tcs-ca.tcs.com	13.71.18.13	FALSE
www.tcs.com	23.45.111.234	FALSE
zcinwfhtelstrapunefw01.tcs.com	52.172.184.169	FALSE
zcinwflbgpunefw01.tcs.com	52.172.207.153	FALSE

## By using IpInfo

**Ip:** "4.247.162.6"  
**City:** "Pune"  
**Region:** "Maharashtra"  
**Country:** "IN"  
**Loc:** "18.5196, 73.8554"  
**Org:** "AS8075 Microsoft Corporation"  
**Postal:** "411001"  
**Time zone:** "Asia/Kolkata"  
**Asn:** "AS8075"  
**Name:** "Microsoft Corporation"  
**Domain:** "microsoft.com"  
**Route:** "4.240.0.0/12"  
**Type:** "Hosting"  
**Company Name:** "Microsoft Corporation"  
**Domain:** "microsoft.com"  
**Type:** "Hosting"  
**Privacy:** Object  
**Vpn:** False  
**Proxy:** false  
**Tor:** false  
**Relay:** false  
**Hosting:** true  
**Address:** "US, WA, Redmond, One Microsoft Way, 98052"  
**Country:** "US"  
**Email:** "abuse@microsoft.com"  
**Name:** "Microsoft Abuse Contact"  
**Network:** "4.240.0.0/12"  
**Phone:** "+1-425-882-8080"

## By using ClearBit & LinkedIn

### Overview:

Tata Consultancy Services is an **IT services**, consulting and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over **56** years. Our consulting-led, cognitive powered, portfolio of business, technology and engineering services and solutions is delivered through our unique Location Independent Agile™ delivery model, recognized as a benchmark of excellence in software development.

A part of the Tata group, India's largest multinational business group, TCS has over **601,000** of the world's best-trained consultants in **55** countries.

### Website

<https://www.tcs.com/>

### Verified page

August 16, 2023

### Industry

IT Services and IT Consulting

### Company size

10,001+ employees

[599,270 associated members](#)

### Headquarters

Mumbai, Maharashtra

### Specialties

IT Services, Business Solutions, and Consulting



LinkedIn profile page for Tata Consultancy Services (TCS) showing 599,270 associated members. The page displays a search bar, navigation tabs (Home, My Network, Jobs, Messaging, Notifications), and a list of products people also use (Quartz, Ethereum, Ripple). A sidebar on the right shows a list of companies to follow (TCS Insurance, This Run). A Windows taskbar is visible at the bottom.

599,270 associated members

Search employees by title, keyword or school

Where they live + Add

- 450,165 | India
- 105,952 | Maharashtra, India
- 86,376 | Tamil Nadu, India
- 74,656 | Karnataka, India
- 69,694 | Greater Bengaluru Area
- 68,751 | Telangana, India
- 66,693 | Bengaluru
- 66,607 | Greater Chennai Area
- 65,973 | Greater Hyderabad Area

Where they studied + Add

- 7,343 | Anna University Chennai
- 7,208 | University of Mumbai
- 7,086 | Savitribai Phule Pune University
- 4,655 | Kendriya Vidyalaya
- 4,424 | Visvesvaraya Technological University
- 4,218 | University of Madras
- 3,953 | Jawaharlal Nehru Technological Univers...
- 2,767 | Rajiv Gandhi Prodyogiki Vishwavidyalaya
- 2,007 | University of Calcutta

Products people also use

- Quartz™ Blockchain Platforms
- Ethereum Blockchain Platforms
- Ripple Blockchain Platforms

Activate Windows  
Go to Settings to activate Windows.

nslookup.io domains/tcs.com/dns-records/#cloudflare

DNS for Developers — Learn DNS once and for all

Nslookup.io

Find DNS records

DNS records for **tcs.com**

Cloudflare Google DNS Authoritative Control D Local DNS

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

**A records**

IPv4 address	Revalidate in
> 4.247.162.6	30s

**AAAA records**


No AAAA records found.

**CNAME record**

Activate Windows  
Go to Settings to activate Windows.

**Full name:** Rajesh Gopinathan  
**Given name:** Rajesh  
**Email:** r.gopinathan@tcs.com  
**Employment:** CEO  
**Role:** Seniority  
**Country:** United States  
**LinkedIn Profile:** [in/rajeshgopinathan](https://www.linkedin.com/in/rajeshgopinathan)





Rajesh Gopinathan  
Mumbai, India

← Skills

All

Industry Knowledge

Interpersonal Skills


Leadership

Business Strategy

Corporate Finance


Growth Strategies

Digital Transformation




Rajesh Gopinathan  
Mumbai, India


Experience



Professor of Practice, Head Translational Research & Entrepreneurship  
Indian Institute of Technology, Bombay  
Dec 2023 - Present · 9 mos



Career transition  
Career Break  
Sep 2023 - Dec 2023 · 4 mos  
Mumbai, Maharashtra




Tata Consultancy Services  
22 yrs 6 mos

● Chief Executive Officer  
Feb 2017 - Jun 2023 · 6 yrs 5 mos  
Mumbai Area, India


● Chief Financial Officer  
2013 - 2017 · 4 yrs  
Mumbai Area, India

● Multiple Roles  
Jan 2001 - Feb 2013 · 12 yrs 2 mos  
Worked across operations, sales and corporate functions.


## Some other people related to tcs.com & Rajesh Gopinathan

**Ravi Yadav**  
Global Head, Cybersecurity Business Unit at Tata Consultancy Services


**Experience**

**Tata Consultancy Services**  
17 yrs 5 mos


- Global Head, Cybersecurity Business Unit at Tata Consultancy Services**  
Full-time  
May 2022 - Present · 2 yrs 4 mos  
USA
- Global Head - Cloud Security & Cyber Security Professional Services**  
Full-time  
Oct 2017 - Apr 2022 · 4 yrs 7 mos  
Atlanta, Georgia, United States  
  
Heads TCS Cloud Security and Cyber Security professional services. In this role, I drive cloud security professional services practice and I am responsible for developing, designing and implementing security strategy. . ...see more
- Practice Director - Cloud & Cyber Security**  
Full-time  
Jan 2014 - Sep 2017 · 3 yrs 9 mos  
Atlanta, Georgia  
  
Established Cloud Security Center of Excellence Team to develop, execute, and sustain comprehensive strategic plans to continuously strengthen the Cloud security program and offerings for TCS customers. Cloud . ...see more

**Karthick Govindarajan**  
Information Security Analyst at Tata Consultancy Services

**Experience**

**Information Security Analyst**  
Tata Consultancy Services · Full-time  
Aug 2012 - Present · 12 yrs 1 mo  
Smyrna, Georgia, United States

**Education**


**University of Madras**  
Bachelor's , Mathematics and Computer Science  
2005 - 2008

**Skills**

**Information Security**


**Security Information and Event Management (SIEM)**

## By using Wappalyzer


 **Wappalyzer** 🔍 ⚙️ 🔄

TECHNOLOGIES MORE INFO [📄 Export](#)



### CMS

 [Adobe Experience Manager](#)


### Widgets

 [StorifyMe](#)


### Analytics

 [Adobe Analytics](#)  
 [LinkedIn Insight Tag](#)



### Video players

 [VideoJS](#)


### Programming languages

 [Java](#)


### CDN

 [Unpkg](#)  
 [Akamai](#)




### Advertising

 [LinkedIn Ads](#)




### Tag managers

 [Adobe Experience Platform Launch](#)


### Security

 [Akamai Bot Manager](#)  
 [reCAPTCHA](#)  
 [HSTS](#)



### Miscellaneous

 [PWA](#)  
 [Open Graph](#)  
 [PDF.js](#) 2.14.305


### Web servers

 [Apache HTTP Server](#)


### JavaScript libraries

 [Swiper](#)  
 [jQuery](#) 3.6.0


### UI frameworks

 [Bootstrap](#) 4.6.1


### Cookie compliance

 [OneTrust](#)

### Digital asset management

 [Adobe Dynamic Media Classic](#)

### Customer data platform


 [Adobe Experience Platform Identity Service](#)

[Something wrong or missing?](#)

## By using Shodan

// TAGS: **cdn**

---

 **General Information**

Hostnames

a23-42-205-106.deploy.static.akamaitechnologies.com  
**tcs.com**  
assets.**tcs.com**  
investors.**tcs.com**  
www.investors.**tcs.com**  
www.**tcs.com**

---

Domains

AKAMAITECHNOLOGIES.COM

TCS.COM

---

Country **United States**

---

City **Los Angeles**

---


Organization **Akamai International, BV**

---

ISP **Akamai Technologies, Inc.**

---

ASN **AS16625**

 **Open Ports**

80

443

## DomainRecords:

	A	4.247.162.6
	MX	Inmumg04.tcs.com
	MX	inblrg01.tcs.com
	MX	inblrg03.tcs.com
	MX	inchng01.tcs.com
	MX	inchng02.tcs.com
	MX	inchng04.tcs.com
	MX	indelg02.tcs.com
	MX	inmumg01.tcs.com
	MX	inmumg02.tcs.com
	MX	uklong01.tcs.com
	MX	usnjyg01.tcs.com
	NS	ns3.tcs.com
	NS	ns4.tcs.com
	NS	ns5.tcs.com
	NS	ns6.tcs.com
	NS	ns7.tcs.com
	SOA	ns4.tcs.com
agilespace	A	219.64.33.94
alm4jal.mastercraftA		14.140.248.159
apg-eastus2	CNAME	tcscomprod2appgw01.eastus.cloudapp.azure.com
apgasia-assets	A	52.172.249.100443 cloud
apgasia-preprod2	A	52.172.218.148
apgeus-assets	A	20.62.217.113
apphonics	A	125.17.73.221
appmart	A	203.199.19.237443
assets	CNAME	assets.tcs.com.edgekey.net
autodiscover	A	45.249.218.30
bodapp	CNAME	tata.bodapp.trafficmanager.net
bodstore	A	121.240.8.182443
brazilbfsi	A	200.212.144.8443

brtamm02	A	208.44.114.52
careers	A	4.247.162.6
cdc.workspace	A	45.249.218.26
cdcn.workspace	A	45.249.218.46443
cep.bpo	A	115.112.77.102
chncho.workspace	A	121.242.62.162
chnexo	A	122.184.60.102
chnicc.workspace	A	125.17.102.210
chnmgm.workspace	A	125.21.186.16
chnsir.workspace	A	121.241.146.221
chnsir.workspace	A	121.242.63.20
chnsnr.workspace	A	203.199.254.134
chntdl.workspace	A	203.199.209.99
chntrl.workspace	A	14.141.100.174
chnvel.workspace	A	118.185.115.167
chnvel.workspace	A	202.54.180.188
conference1	A	10.102.114.172
conference1	A	10.18.220.61
conference1	A	10.25.100.89
conference1	A	172.16.246.235
conference1	A	172.16.246.236
conference1	A	172.16.246.237
conference1	A	172.17.12.55
conference1	A	172.17.9.56
conference1	A	172.17.9.62
conference1	A	203.200.71.44443
conference1	A	219.64.33.157
delgg5.workspace	A	121.242.45.149
delgg6.workspace	A	115.111.246.85
delgg7.workspace	A	121.241.127.34
delnd5.workspace	A	14.143.181.86
digitalsoftware	A	14.141.110.181
dominoconnect	A	219.64.34.32

ebcssl1	A	122.15.107.26	
emeaswzprovpn01A		51.107.86.224443	cloud
emeaswzprovpn02A		51.107.86.138443	cloud
feeds	CNAME	feeds.feedburner.com	
gnrgc.workspace	A	14.142.138.115	
gnrgp.workspace	A	14.142.16.6	
grs	CNAME	tcs.grs.trafficmanager.net	
hob-sit	A	121.242.62.41	
hydadi.workspace	A	182.19.66.181	
hyddp.workspace	A	203.200.212.60	
hydsp4.workspace	A	115.111.228.95	
hydsyp.workspace	A	121.241.164.50	
hydsyp.workspace	A	14.140.185.148	
ibegin	CNAME	tcs.ibegin.trafficmanager.net	
ignite	A	125.17.102.12	
ilpcms	A	14.140.178.150	
inblra01	A	125.16.95.26	
inblrg01	A	121.242.48.325	
inblrg02	A	121.242.48.116	
indruk03	A	219.64.33.177	
indsez.workspace	A	14.143.129.44438443	
info	CNAME	tcsmktgprod.mktoweb.com	
inggnloandepotvpnA		52.163.249.74443	cloud
inhydlbgvpn	A	13.71.115.68443	cloud
inhyverizonvpn	A	52.172.30.223443	cloud
pilot-qa	CNAME	a7f924c4-922d-4177-b96f9e28c98f41c8.cloudapp.net	
pilot-qa2	CNAME	46298282-693d-490d-a4e8-76870c3259be.cloudapp.net	
puncyp.workspace	A	14.143.46.214	
punsp.workspace	A	59.160.73.119	
research-innovationA		104.211.92.25280443	cloud
safetyfirst	A	219.64.33.126	
sam.ey	A	14.142.107.34	
secureaccess	A	14.143.141.164	



secureaccess	A	219.64.33.225	
secureaccessjuniper	A	121.242.30.84	
securitycommunity	CNAME	securitycommunity.tcs.com.indusguard.com	
slides	A	219.64.33.170	
smetrics	CNAME	tcs.com.ssl.sc.omtrdc.net	
sms	A	203.200.212.163	
sslwebmail	A	219.64.34.6	
tcsapcgtlsbc01	A	103.120.19.20122	
tcsemeagtlsbc01	A	31.171.245.10080443	
tvmsez.workspace	A	14.141.182.222443	
uklong01	A	80.82.129.16525	
uklong02	A	80.82.129.166	
ukprivpn	A	80.82.129.188443	
uksecvpn	A	195.219.173.134443	
uscinsapvpn	A	12.36.190.162	
vcseindia	A	115.111.249.140443	
vcseus	A	8.20.250.15443	
vmsprocurement	CNAME	tcs.vmsprocurement.trafficmanager.net	
webmail	A	219.64.34.213	
workspace	A	45.249.218.47443	
worldwide	A	104.211.88.5280443	cloud
www	CNAME	www.tcs.com.edgekey.net	
<a href="#">www.alumniportal</a>	CNAME	tcs.alumniportal.trafficmanager.net	
<a href="#">www.careers</a>	CNAME	careers.tcs.com	
<a href="#">www.investors</a>	CNAME	www.investors.tcs.com.edgekey.net	
<a href="#">www.mastercraft</a>	A	115.112.72.174	
<a href="#">www.tcs-ca</a>	A	13.71.18.1380443	cloud
zcinwfhtelstrapunefw01	A	52.172.184.169443	cloud
zcinwflbgnagpurfw01	A	52.172.214.183443	cloud
zcinwflbgpunefw01	A	52.172.207.153443	cloud

---

# ACTIVE INFORMATION GATHERING

---

By using Kali Linux

```
(kali㉿kali)-[~]
└─$ nslookup tcs.com
Server:           192.168.35.2
Address: 192.168.35.2#53:
Non-authoritative answer: /meta_config
Name: rcetcs.com / .set/meta_config
Address: 4.247.162.6 payload generator
Resource record (/root/.set/meta_config)
```

```
(kali㉿kali)-[~]
└─$ nmap --script vuln tcs.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 07:52 EDT
Nmap scan report for tcs.com (4.247.162.6)
Host is up (0.082s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
443/tcp   open  https
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
[*] Exploit completed, but no session was created.
Nmap done: 1 IP address (1 host up) scanned in 65.79 seconds
```

## VULNERABILITY:

We did not find any vulnerabilities on **tcs.com**, so we conducted a test on **chatgpt** to assess our knowledge:

### chat.openai.com

IP Address	104.18.6.87
------------	-------------

Hostname(s)	p2gold.com
-------------	------------

Tags	cdn
------	-----

Vulnerabilities	CVE-2019-9637, CVE-2015-9253, CVE-2020-11022, CVE-2022-31628, CVE-2019-9020, CVE-2017-9120, CVE-2020-11579, CVE-2019-11358, CVE-2019-9675, CVE-2019-9638, CVE-2019-6977, CVE-2019-9021, CVE-2013-2220, CVE-2018-19395, CVE-2019-9022, CVE-2017-7272, CVE-2020-11023, CVE-2017-7963, CVE-2019-9639, CVE-2022-31629, CVE-2019-9024, CVE-2024-4577, CVE-2019-9023, CVE-2007-3205, CVE-2019-9641, CVE-2017-8923, CVE-2018-19396
-----------------	---

THE END  
THE END