DEVSKILLS MINOR PROJECT

Name : SHAIK UMAR FAROOQ

Internship period : 11,jun,2024 to 11,sep,2024

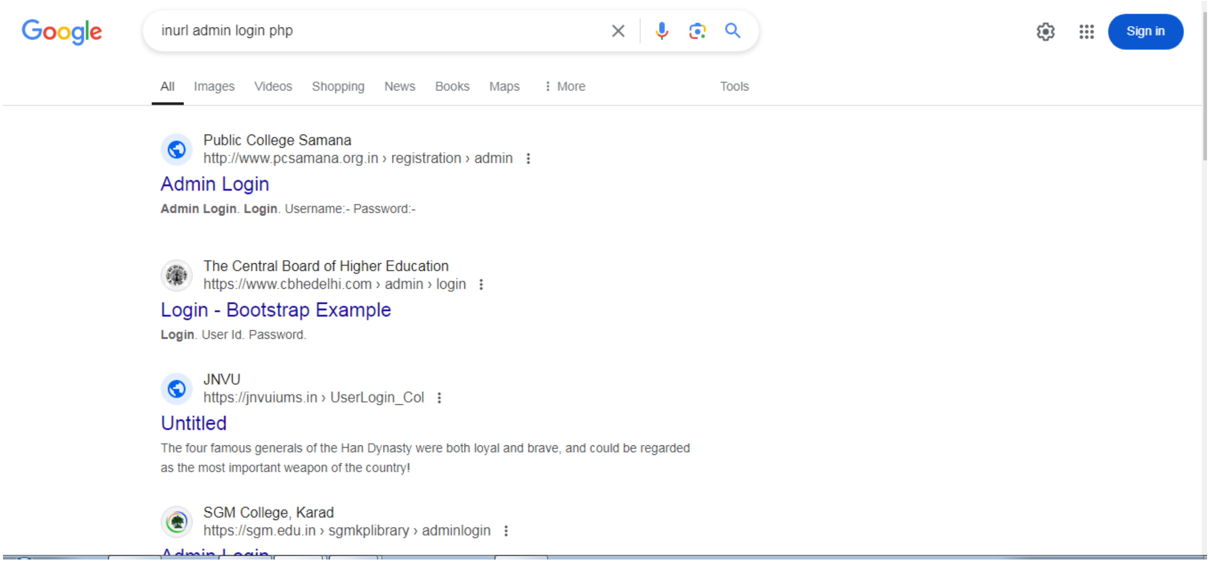
Email id : umarfarooqshiak7863@gmail.com

MINOR *PROJECT-1*

1.a)Find application which are vulnerable for sql injection

STEP-1:

Get the syntax for the vulnerability sql injections form the google hacking data base and paste it in the google browser.



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

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

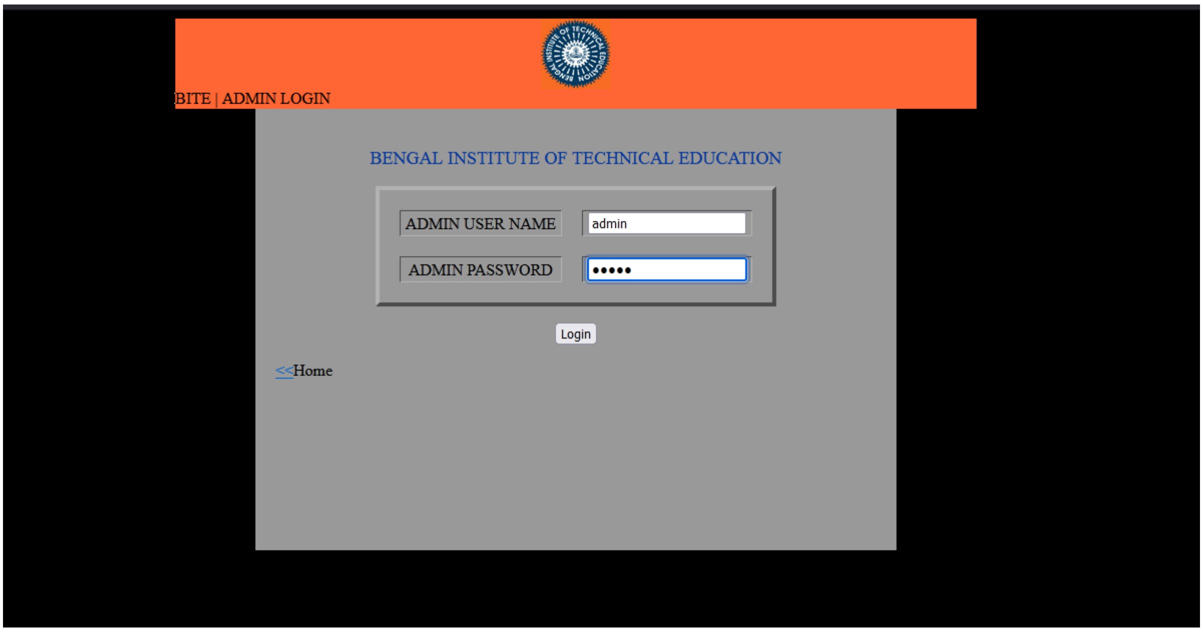
JNVU
https://jnvuiums.in › UserLogin_Col
Untitled
The four famous generals of the Han Dynasty were both loyal and brave, and could be regarded as the most important weapon of the country!

SGM College, Karad
https://sgm.edu.in › sgmkplibrary › adminlogin
Admin Login

STEP-2:

Now open as many websites as you can and perform SQL Injection by using the payload 1’ or ‘1’=’1.

DEVSKILLS MINOR *PROJECT*

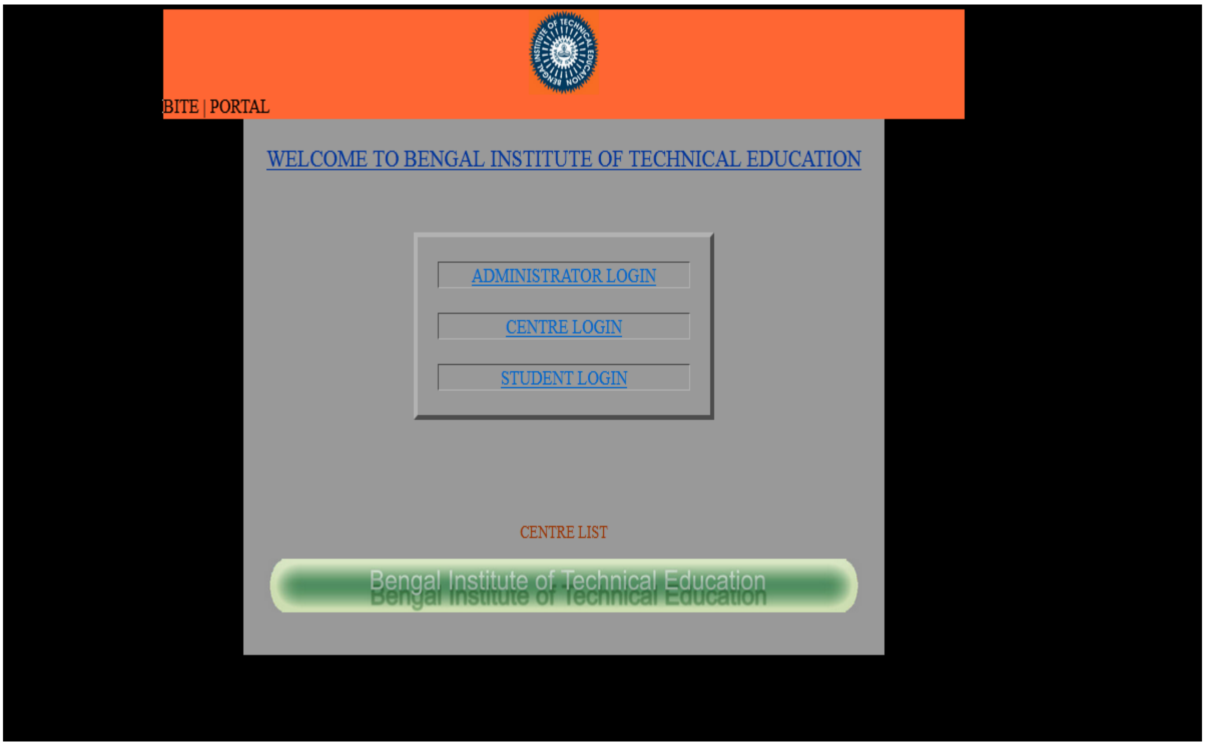


BITE | ADMIN LOGIN

BENGAL INSTITUTE OF TECHNICAL EDUCATION

ADMIN USER NAME: admin

ADMIN PASSWORD: •••••

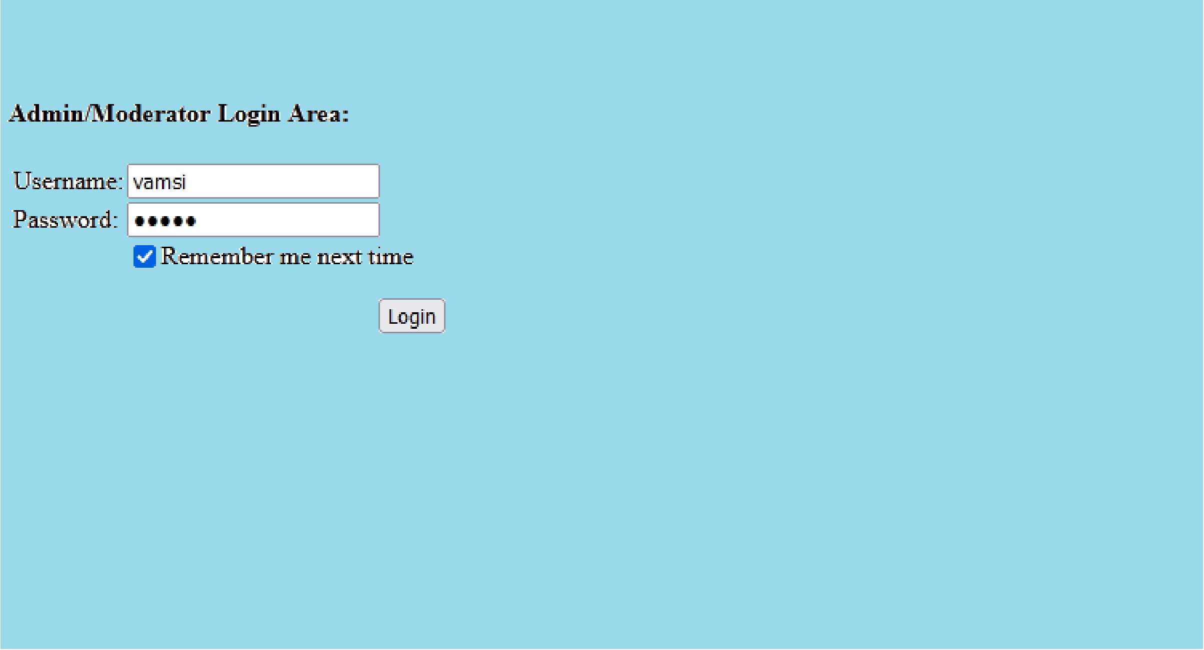


BITE | PORTAL

WELCOME TO BENGAL INSTITUTE OF TECHNICAL EDUCATION

Website 1 admin login successful.

DEVSKILLS MINOR *PROJECT*

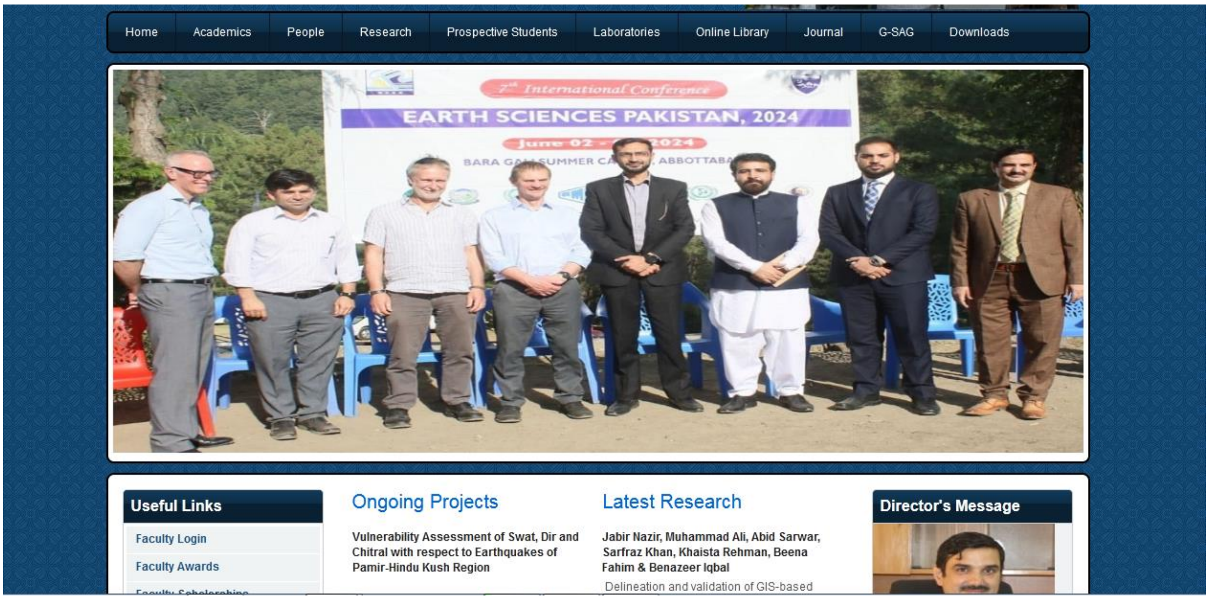


Admin/Moderator Login Area:

Username: vamsi

Password: ●●●●●

☑ Remember me next time



Ongoing Projects

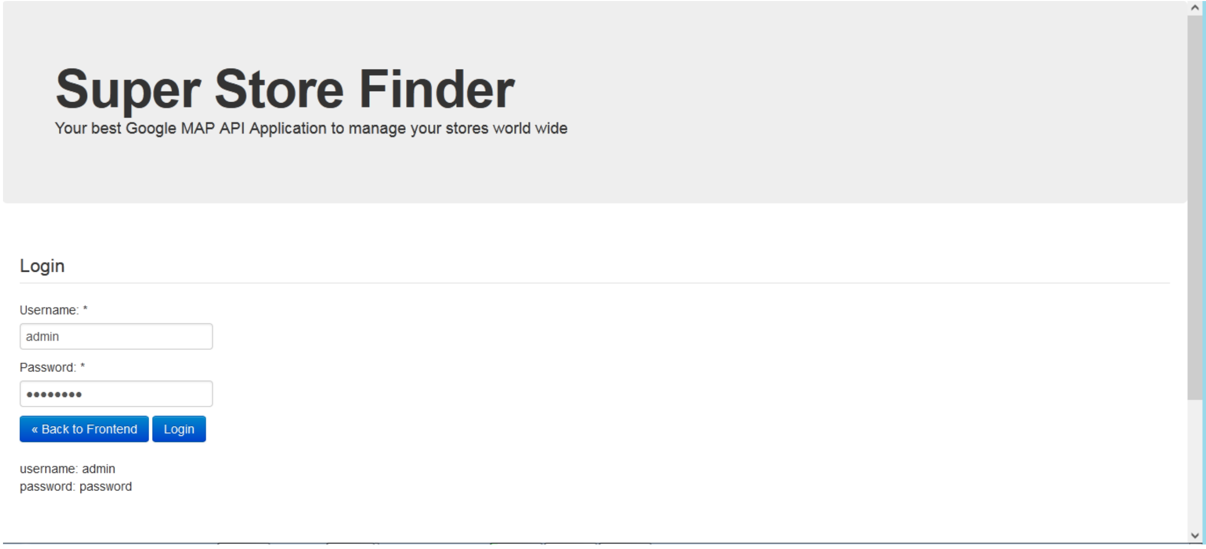
Vulnerability Assessment of Swat, Dir and Chitral with respect to Earthquakes of Pamir-Hindu Kush Region

Latest Research

Jabir Nazir, Muhammad Ali, Abid Sarwar, Sarfraz Khan, Khaista Rehman, Beena Fahim & Benazeer Iqbal

Delineation and validation of GIS-based

Website 2 admin login successful.



Super Store Finder

Your best Google MAP API Application to manage your stores world wide

Login

Username: *

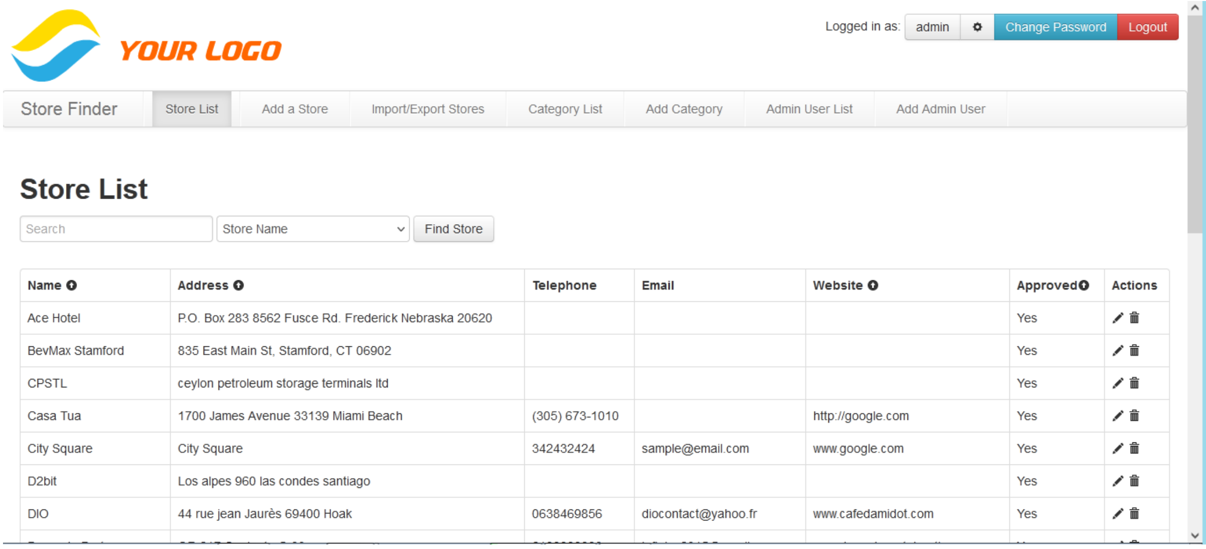
admin

Password: *

••••••••

« Back to Frontend | Login

username: admin
password: password



Store List

Search | Store Name | Find Store

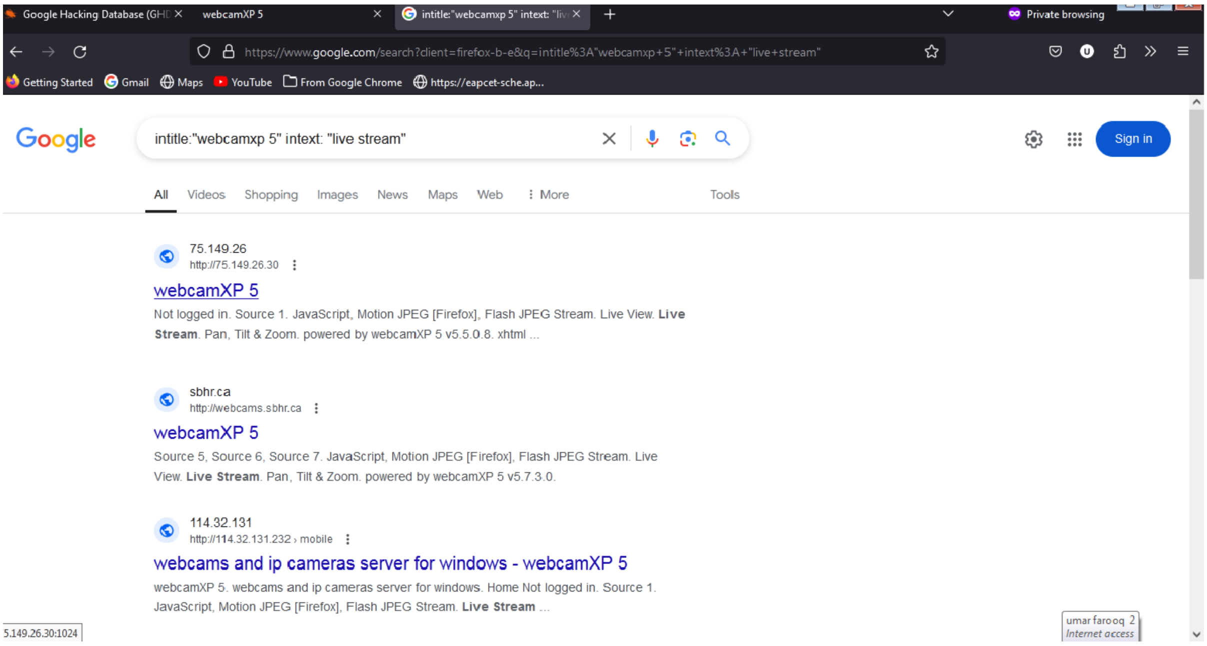
Name	Address	Telephone	Email	Website	Approved	Actions
Ace Hotel	P.O. Box 283 8562 Fusce Rd. Frederick Nebraska 20620				Yes	✎ 🗑
BevMax Stamford	835 East Main St, Stamford, CT 06902				Yes	✎ 🗑
CPSTL	ceylon petroleum storage terminals ltd				Yes	✎ 🗑
Casa Tua	1700 James Avenue 33139 Miami Beach	(305) 673-1010		http://google.com	Yes	✎ 🗑
City Square	City Square	342432424	sample@email.com	www.google.com	Yes	✎ 🗑
D2bit	Los alpes 960 las condes santiago				Yes	✎ 🗑
DIO	44 rue jean Jaurès 69400 Hoak	0638469856	diocontact@yahoo.fr	www.cafedamidot.com	Yes	✎ 🗑

Website 3 admin login successful.

b. Find vulnerable live cameras,

STEP 1:

Get the syntax for the vulnerability SQL injections from the google hacking data base and paste it in the google browser.



https://www.google.com/search?client=firefox-b-e&q=intitle%3A"webcamxp+5"+intext%3A+"live+stream"

intitle:"webcamxp 5" intext: "live stream"

75.149.26
http://75.149.26.30

webcamXP 5

Not logged in. Source 1. JavaScript, Motion JPEG [Firefox], Flash JPEG Stream. Live View. **Live Stream**. Pan, Tilt & Zoom. powered by webcamXP 5 v5.5.0.8. xhtml ...

sbhr.ca
http://webcams.sbhr.ca

webcamXP 5

Source 5, Source 6, Source 7. JavaScript, Motion JPEG [Firefox], Flash JPEG Stream. Live View. **Live Stream**. Pan, Tilt & Zoom. powered by webcamXP 5 v5.7.3.0.

114.32.131
http://114.32.131.232 › mobile

webcams and ip cameras server for windows - webcamXP 5

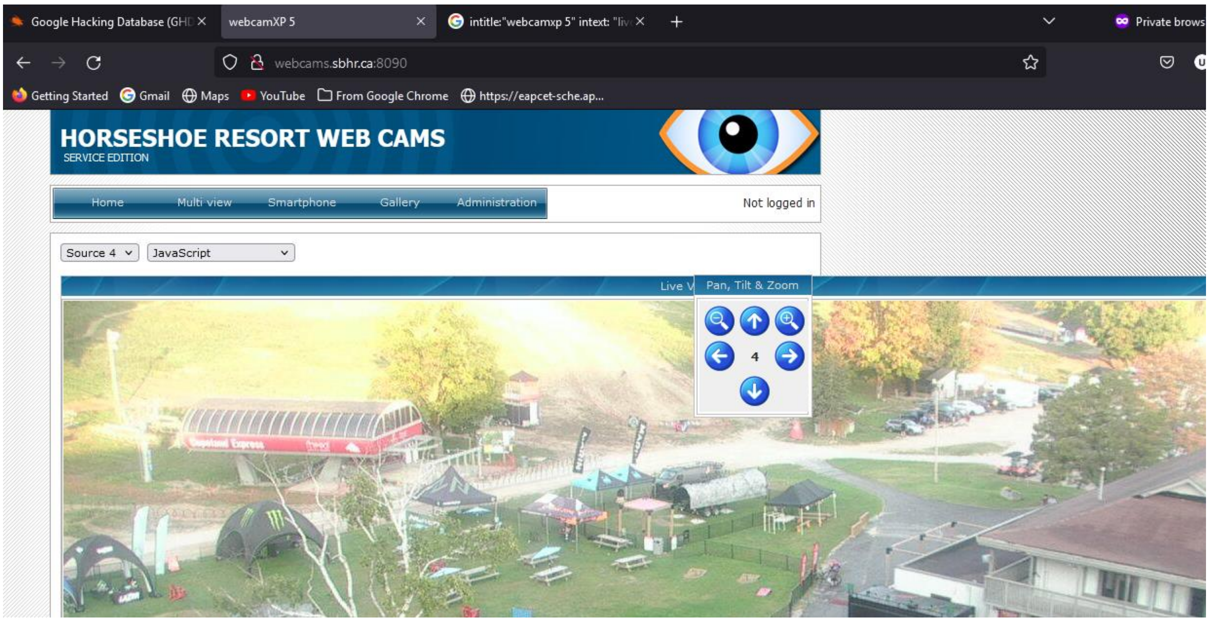
webcamXP 5. webcams and ip cameras server for windows. Home Not logged in. Source 1. JavaScript, Motion JPEG [Firefox], Flash JPEG Stream. **Live Stream** ...

5.149.26.30:1024

umar farooq 2
Internet access

STEP 2:

Now open as many websites as you can and search live cams. These cams may be house hold cams or public cams.



Acces to the webcam is successful.

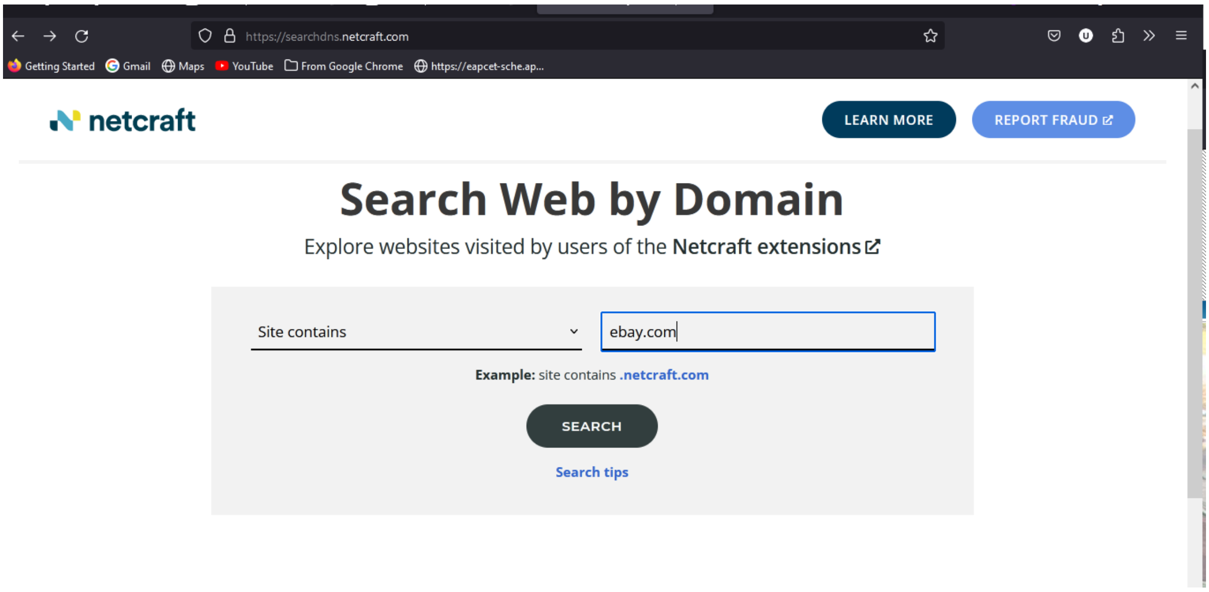
2. Find sub-domain details of the target (choose any).

STEP 1:

Select any of the domain you wish. I have chosen https://www.ebay.com/

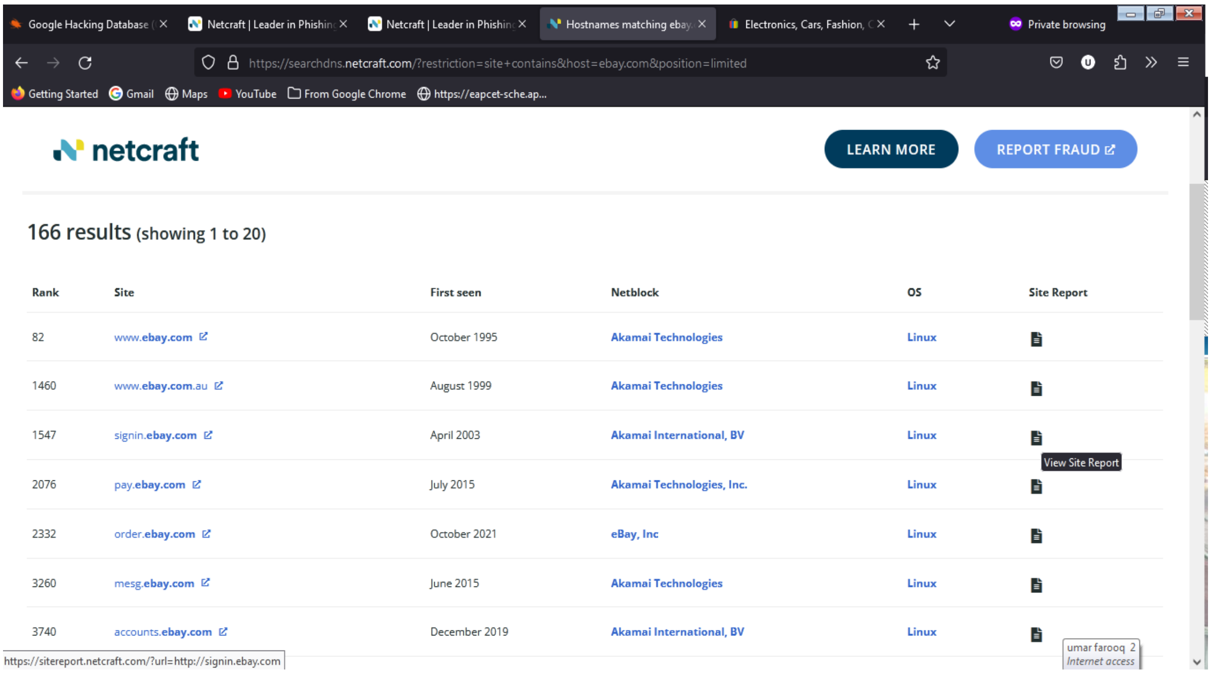
STEP 2:

Now there are websites such as netcraft, search DNS to search the sub domines of the target website. Now go into each of the website and paste or search the domain vivo to get its subdomain details.


https://searchdns.netcraft.com
Getting Started
Gmail
Maps
YouTube
From Google Chrome
https://eapcet-sche.ap...
netcraft
LEARN MORE
REPORT FRAUD
Search Web by Domain
Explore websites visited by users of the Netcraft extensions
Example: site contains .netcraft.com
SEARCH
Search tips

Site contains ebay.com

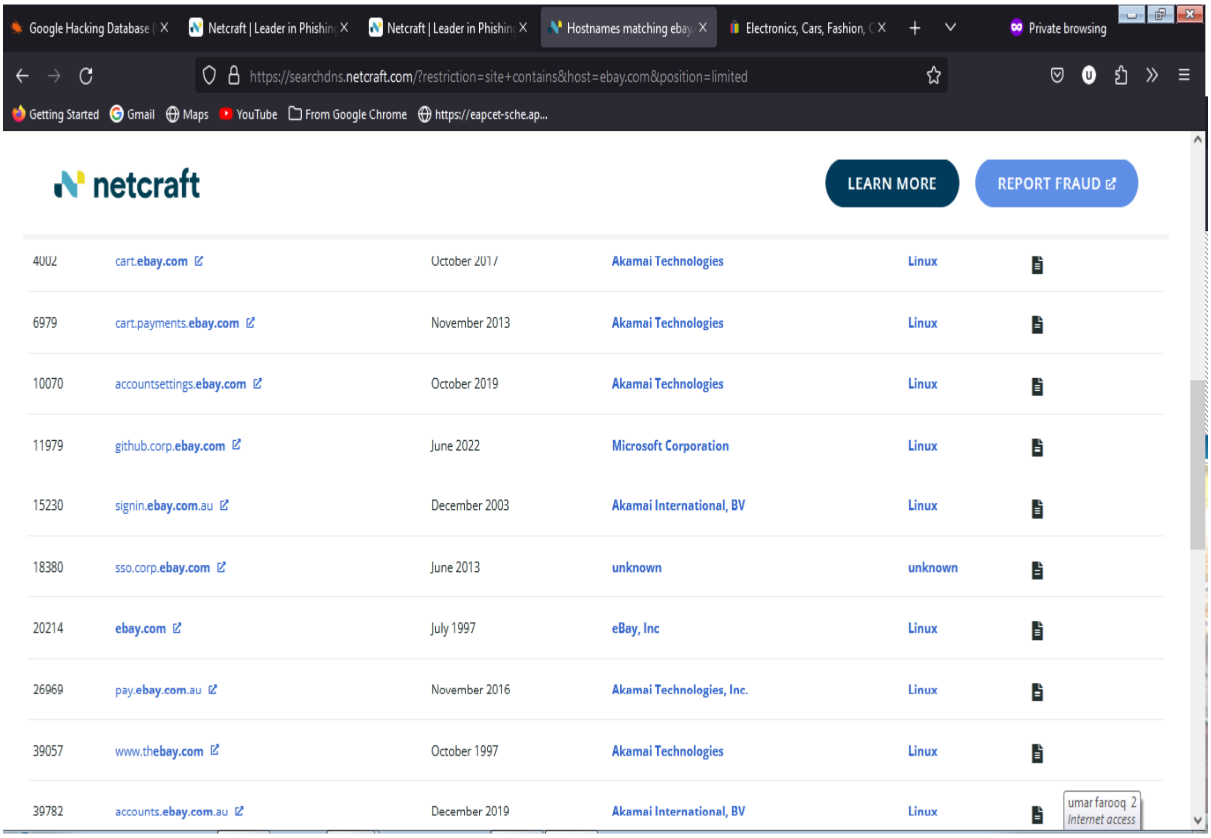
DEVSKILLS MINOR *PROJECT*


Google Hacking Database (
Netcraft | Leader in Phishin
Netcraft | Leader in Phishin
Hostnames matching ebay
Electronics, Cars, Fashion, C
Private browsing
https://searchdns.netcraft.com/?restriction=site+contains&host=ebay.com&position=limited
Getting Started
Gmail
Maps
YouTube
From Google Chrome
https://eapcet-sche.ap...
netcraft
LEARN MORE
REPORT FRAUD
View Site Report
umar farooq 2
Internet access

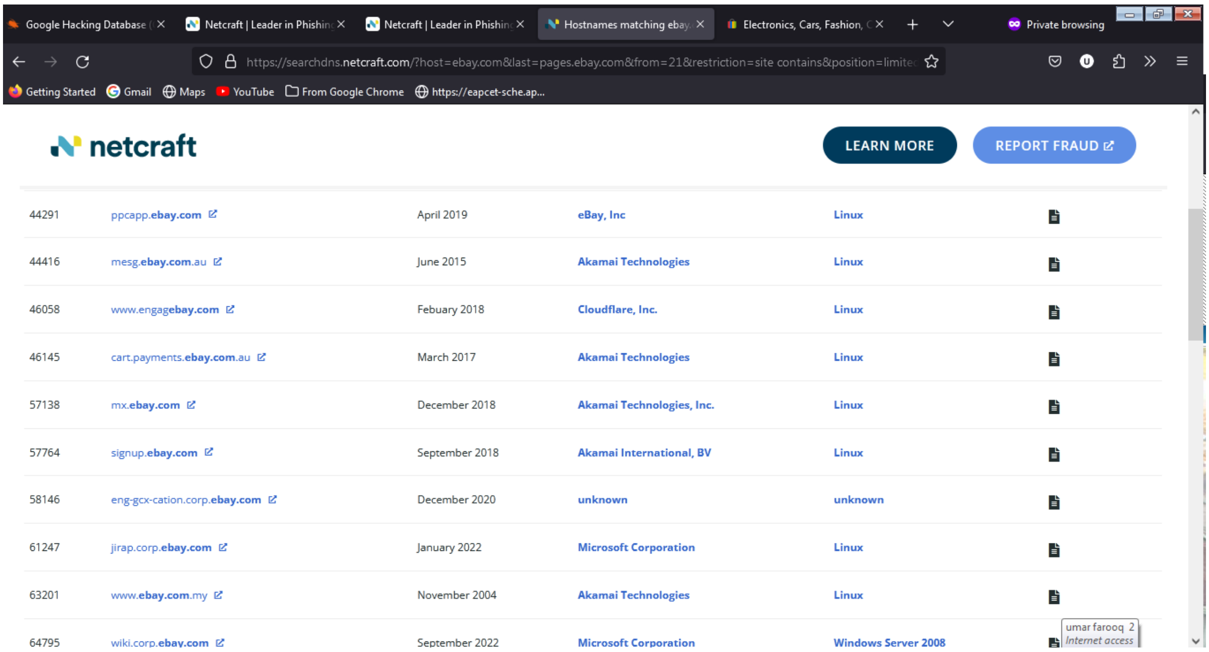
166 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS	Site Report
82	www.ebay.com	October 1995	Akamai Technologies	Linux	
1460	www.ebay.com.au	August 1999	Akamai Technologies	Linux	
1547	signin.ebay.com	April 2003	Akamai International, BV	Linux	
2076	pay.ebay.com	July 2015	Akamai Technologies, Inc.	Linux	
2332	order.ebay.com	October 2021	eBay, Inc	Linux	
3260	mesg.ebay.com	June 2015	Akamai Technologies	Linux	
3740	accounts.ebay.com	December 2019	Akamai International, BV	Linux	

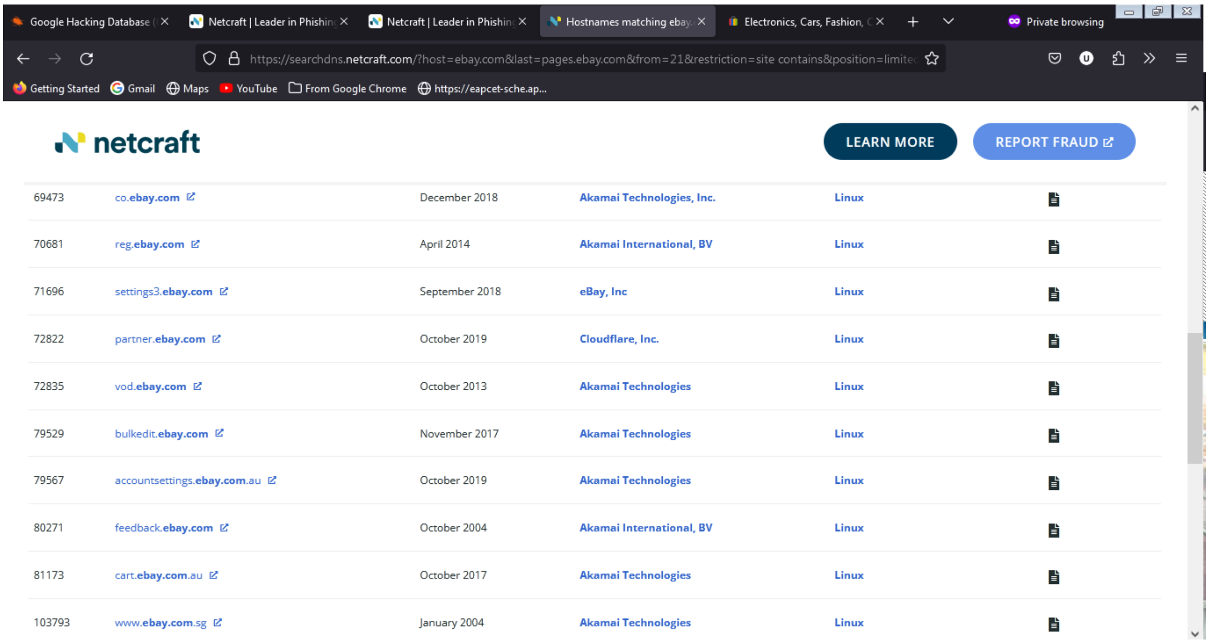
https://sitereport.netcraft.com/?url=http://signin.ebay.com


Google Hacking Database (
Netcraft | Leader in Phishin
Netcraft | Leader in Phishin
Hostnames matching ebay
Electronics, Cars, Fashion, C
Private browsing
https://searchdns.netcraft.com/?restriction=site+contains&host=ebay.com&position=limited
Getting Started
Gmail
Maps
YouTube
From Google Chrome
https://eapcet-sche.ap...
netcraft
LEARN MORE
REPORT FRAUD
umar farooq 2
Internet access

4002	cart.ebay.com	October 2017	Akamai Technologies	Linux	
6979	cart.payments.ebay.com	November 2013	Akamai Technologies	Linux	
10070	accountsettings.ebay.com	October 2019	Akamai Technologies	Linux	
11979	github.corp.ebay.com	June 2022	Microsoft Corporation	Linux	
15230	signin.ebay.com.au	December 2003	Akamai International, BV	Linux	
18380	sso.corp.ebay.com	June 2013	unknown	unknown	
20214	ebay.com	July 1997	eBay, Inc	Linux	
26969	pay.ebay.com.au	November 2016	Akamai Technologies, Inc.	Linux	
39057	www.thebay.com	October 1997	Akamai Technologies	Linux	
39782	accounts.ebay.com.au	December 2019	Akamai International, BV	Linux	


Google Hacking Database
Netcraft | Leader in Phishin
Netcraft | Leader in Phishin
Hostnames matching ebay
Electronics, Cars, Fashion,
Private browsing
https://searchdns.netcraft.com/?host=ebay.com&last=pages.ebay.com&from=21&restriction=site contains&position=limite
Getting Started
Gmail
Maps
YouTube
From Google Chrome
https://eapcet-sche.ap...
netcraft
LEARN MORE
REPORT FRAUD
umar farooq 2
Internet access

44291	ppcapp.ebay.com	April 2019	eBay, Inc	Linux	
44416	mesg.ebay.com.au	June 2015	Akamai Technologies	Linux	
46058	www.engagebay.com	Febuary 2018	Cloudflare, Inc.	Linux	
46145	cart.payments.ebay.com.au	March 2017	Akamai Technologies	Linux	
57138	mx.ebay.com	December 2018	Akamai Technologies, Inc.	Linux	
57764	signup.ebay.com	September 2018	Akamai International, BV	Linux	
58146	eng-gcx-cation.corp.ebay.com	December 2020	unknown	unknown	
61247	jirap.corp.ebay.com	January 2022	Microsoft Corporation	Linux	
63201	www.ebay.com.my	November 2004	Akamai Technologies	Linux	
64795	wiki.corp.ebay.com	September 2022	Microsoft Corporation	Windows Server 2008	


Google Hacking Database
Netcraft | Leader in Phishin
Netcraft | Leader in Phishin
Hostnames matching ebay
Electronics, Cars, Fashion,
Private browsing
https://searchdns.netcraft.com/?host=ebay.com&last=pages.ebay.com&from=21&restriction=site contains&position=limite
Getting Started
Gmail
Maps
YouTube
From Google Chrome
https://eapcet-sche.ap...
netcraft
LEARN MORE
REPORT FRAUD

69473	co.ebay.com	December 2018	Akamai Technologies, Inc.	Linux	
70681	reg.ebay.com	April 2014	Akamai International, BV	Linux	
71696	settings3.ebay.com	September 2018	eBay, Inc	Linux	
72822	partner.ebay.com	October 2019	Cloudflare, Inc.	Linux	
72835	vod.ebay.com	October 2013	Akamai Technologies	Linux	
79529	bulkedit.ebay.com	November 2017	Akamai Technologies	Linux	
79567	accountsettings.ebay.com.au	October 2019	Akamai Technologies	Linux	
80271	feedback.ebay.com	October 2004	Akamai International, BV	Linux	
81173	cart.ebay.com.au	October 2017	Akamai Technologies	Linux	
103793	www.ebay.com.sg	January 2004	Akamai Technologies	Linux	

There are 166 subdomains for the domain or host ebay.com So subdomain details are gathered successfully for the targeted website ebay.

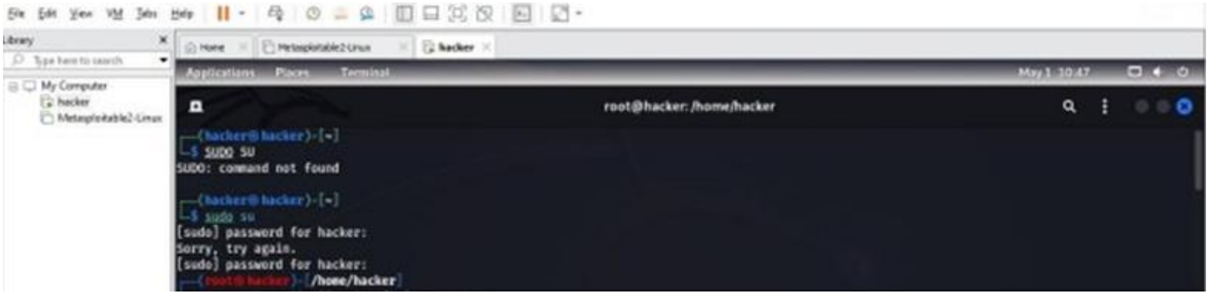
3. Take a Target and Scan using NMAP and getnd get open port information as well as Version Details.

STEP 1:

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

STEP 2:

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



```
┌──(hacker㉿hacker)-[~]
└─$ SUDO SU
SUDO: command not found

┌──(hacker㉿hacker)-[~]
└─$ sudo su
[sudo] password for hacker:
Sorry, try again.
[sudo] password for hacker:
┌──(root㉿hacker)-[/home/hacker]
```

STEP 3:

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

```
PORT   STATE  SERVICE VERSION

10/tcp open tcpwrapped
11/tcp open tcpwrapped
12/tcp open tcpwrapped
13/tcp open tcpwrapped
14/tcp open tcpwrapped
15/tcp open tcpwrapped
16/tcp open tcpwrapped
17/tcp open tcpwrapped
18/tcp open tcpwrapped
19/tcp open tcpwrapped
20/tcp open tcpwrapped
21/tcp open ftp Pure-FTPd
23/tcp open tcpwrapped
24/tcp open tcpwrapped
25/tcp open tcpwrapped
26/tcp open tcpwrapped
27/tcp open tcpwrapped
28/tcp open tcpwrapped
```

```
29/tcp open tcpwrapped

30/tcp open tcpwrapped

31/tcp open tcpwrapped

32/tcp open tcpwrapped

33/tcp open tcpwrapped

34/tcp open tcpwrapped

35/tcp open tcpwrapped

36/tcp open tcpwrapped

37/tcp open tcpwrapped

38/tcp open tcpwrapped

39/tcp open topwrapped

40/tcp open topwrapped

41/tcp open tcpwrapped

42/tcp open topwrapped

 44/tcp open tcpwrapped

43/tcp open  tcpwrapped

45/tcp open tcpwrapped

46/tcp open tcpwrapped

47/tcp open tcpwrapped

48/tcp open tcpwrapped
```

```
49/tcp open tcpwrapped

50/tcp open tcpwrapped

51/tcp open tcpwrapped

52/tcp open tcpwrapped

53/tcp open domain PowerDNS Authoritative Server 4.7.2

54/tcp open tcpwrapped

55/tcp open tcpwrapped

56/tcp open tcpwrapped

57/tcp open tcpwrapped

58/tcp open tcpwrapped

59/tcp open tcpwrapped

60/tcp open tcpwrapped

61/tcp open tcpwrapped

62/tcp open tcpwrapped

63/tcp open tcpwrapped

64/tcp open tcpwrapped

65/tcp open tcpwrapped

66/tcp open tcpwrapped

67/tcp open tcpwrapped

68/tcp open tcpwrapped
```

```
69/tcp open tcpwrapped

70/tcp open tcpwrapped

71/tcp open tcpwrapped

72/tcp open tcpwrapped

73/tcp open tcpwrapped

74/tcp open tcpwrapped

75/tcp open tcpwrapped

76/tcp open tcpwrapped

77/tcp open tcpwrapped

78/tcp open tcpwrapped

79/tcp open tcpwrapped

80/tcp open http LiteSpeed

81/tcp open tcpwrapped

82/tcp open tcpwrapped

83/tcp open tcpwrapped

84/tcp open tcpwrapped

85/tcp open tcpwrapped

86/tcp open tcpwrapped

87/tcp open tcpwrapped

88/tcp open tcpwrapped
```

```
89/tcp open tcpwrapped

90/tcp open tcpwrapped

91/tcp open tcpwrapped

92/tcp open tcpwrapped

93/tcp open tcpwrapped

94/tcp open tcpwrapped

95/tcp open tcpwrapped

96/tcp open tcpwrapped

97/tcp open tcpwrapped

98/tcp open tcpwrapped

99/tcp open tcpwrapped

100/tcp open tcpwrapped

1 service unrecognized despite returning data. If you know
the service/version, please submit the following fingerprint
at https://nmap.org/cgi-bin/submit.cgi?new-service:


Service detection performed. Please report any incorrect
results at https://nmap.org/submit/.


Nmap done: 1 IP address (1 host up) scanned in 89.08
seconds
```

HENCE NMAP SCAN WITH VERSION DETALIS IS SUCCSCEFUL.

________________********_______________