

WEB APPLICATION PENTESTING

GROUP – 2.6

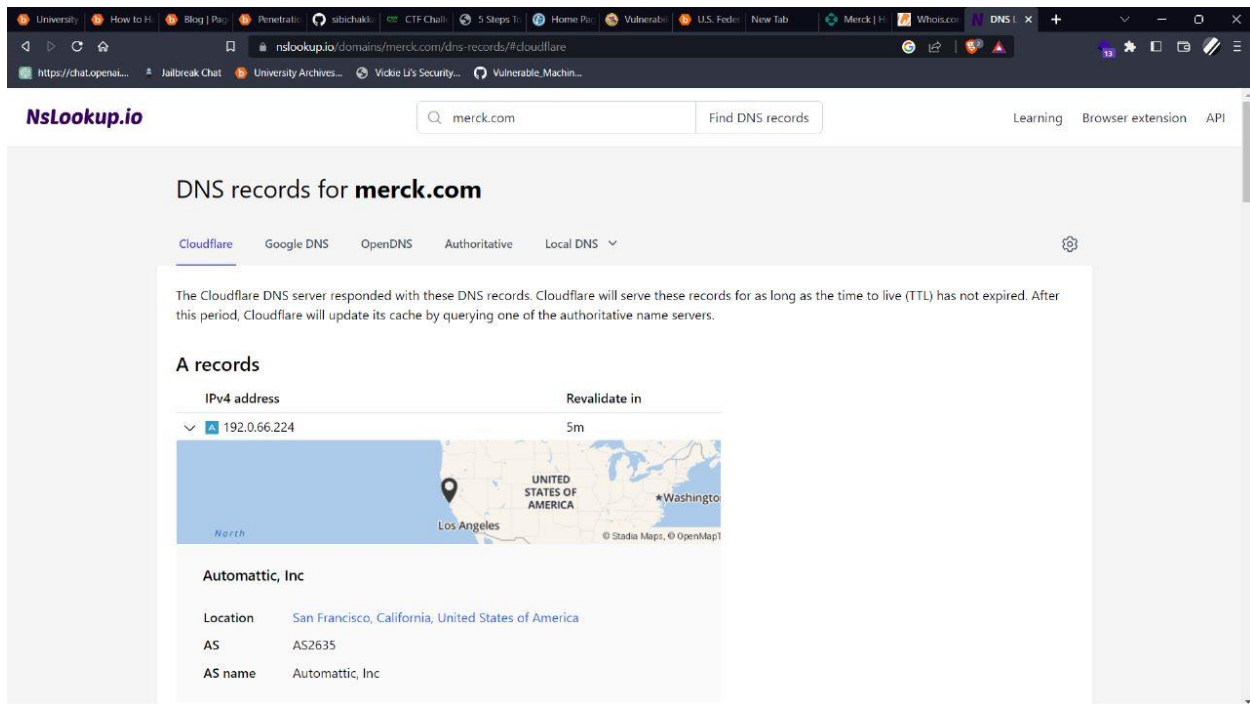
G. PUSHKAR – 20BCN7119

M.SURYATEJA-20BCN7021

G. KARTHIK – 20BCN7008

TARGET: merck.com

DNS – LOOKUP:



The screenshot shows the Nslookup.io website interface. The browser's address bar displays the URL `nslookup.io/domains/merck.com/dns-records/#cloudflare`. The website header includes the Nslookup.io logo, a search bar with `merck.com`, and a "Find DNS records" button. Below the header, the page title is "DNS records for merck.com". A navigation bar shows tabs for "Cloudflare", "Google DNS", "OpenDNS", "Authoritative", and "Local DNS". A message states: "The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers." Under the "A records" section, the IPv4 address `192.0.66.224` is listed with a "Revalidate in 5m" timer. A map shows the location of the IP address in Los Angeles, California. Below the map, the organization "Automattic, Inc" is listed with its location in San Francisco, California, and its AS number AS2635.

IPv4 address	Revalidate in
192.0.66.224	5m

Automattic, Inc

Location	San Francisco, California, United States of America
AS	AS2635
AS name	Automattic, Inc

Cloudflare		
Google DNS		
OpenDNS		
Authoritative		
Local DNS		
NS records		
Name server	Revalidate in	
ns6.customer.level3.net.	1h	
cmtu.mt.ns.els-gms.att.net.	1h	
dbur.br.ns.els-gms.att.net.	1h	
ns9.customer.level3.net.	1h	
cbru.br.ns.els-gms.att.net.	1h	
dmtu.mt.ns.els-gms.att.net.	1h	
MX records		
Mail server	Priority	Revalidate in
msdcloud.mail.protection.outlook.com.	0 Primary	1h
Other records		
SOA		
SOA data		
Start of authority	dbur.br.ns.els-gms.att.net.	Revalidate in
Email	rm-hostmaster@ems.att.com	
Serial	1682	
Refresh	1h	
Retry	20m	

Nmap scan:

Zenmap

Scan

Tools

Profile

Help

Target:

192.0.66.224

Profile:

Intense scan, all TCP ports

Scan

Cancel

Command:

nmap -p 1-65535 -T4 -A -v 192.0.66.224

Hosts

Services

Nmap Output

Ports/Hosts

Topology

Host Details

Scans

OS

Host

192.0.66.224

Nmap -p 1-65535 -T4 -A -v 192.0.66.224

Starting Nmap 7.93 (<https://nmap.org>) at 2023-06-19 15:43 India Standard Time

NSOCK ERROR [0.3600s] ssl_init_helper(): OpenSSL legacy provider failed to load.

NSE: Loaded 155 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 15:43

Completed NSE at 15:43, 0.00s elapsed

Initiating NSE at 15:43

Completed NSE at 15:43, 0.00s elapsed

Initiating NSE at 15:43

Completed NSE at 15:43, 0.00s elapsed

Initiating Ping Scan at 15:43

Completed Ping Scan at 15:43, 0.23s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 15:43

Completed Parallel DNS resolution of 1 host. at 15:43, 0.07s elapsed

Initiating SYN Stealth Scan at 15:43

Scanning 192.0.66.224 [65535 ports]

Discovered open port 80/tcp on 192.0.66.224

Discovered open port 443/tcp on 192.0.66.224

SYN Stealth Scan Timing: About 6.68% done; ETC: 15:50 (0:07:13 remaining)

SYN Stealth Scan Timing: About 14.14% done; ETC: 15:51 (0:06:47 remaining)

SYN Stealth Scan Timing: About 25.80% done; ETC: 15:49 (0:04:39 remaining)

SYN Stealth Scan Timing: About 39.45% done; ETC: 15:48 (0:03:15 remaining)

SYN Stealth Scan Timing: About 53.99% done; ETC: 15:47 (0:02:14 remaining)

SYN Stealth Scan Timing: About 71.84% done; ETC: 15:47 (0:01:13 remaining)

Completed SYN Stealth Scan at 15:47, 235.98s elapsed (65535 total ports)

Initiating Service scan at 15:47

Scanning 2 services on 192.0.66.224

Completed Service scan at 15:47, 18.82s elapsed (2 services on 1 host)

Initiating OS detection (try #1) against 192.0.66.224

Initiating Traceroute at 15:47

Completed Traceroute at 15:47, 3.03s elapsed

Initiating Parallel DNS resolution of 7 hosts. at 15:47

Completed Parallel DNS resolution of 7 hosts. at 15:47, 11.17s elapsed

NSE: Script scanning 192.0.66.224.

Initiating NSE at 15:47

Completed NSE at 15:47, 5.28s elapsed

Initiating NSE at 15:47

Completed NSE at 15:47, 1.89s elapsed

Initiating NSE at 15:47

Completed NSE at 15:47, 0.00s elapsed

Nmap scan report for 192.0.66.224

Host is up (0.11s latency).

Not shown: 65533 filtered tcp ports (no-response)

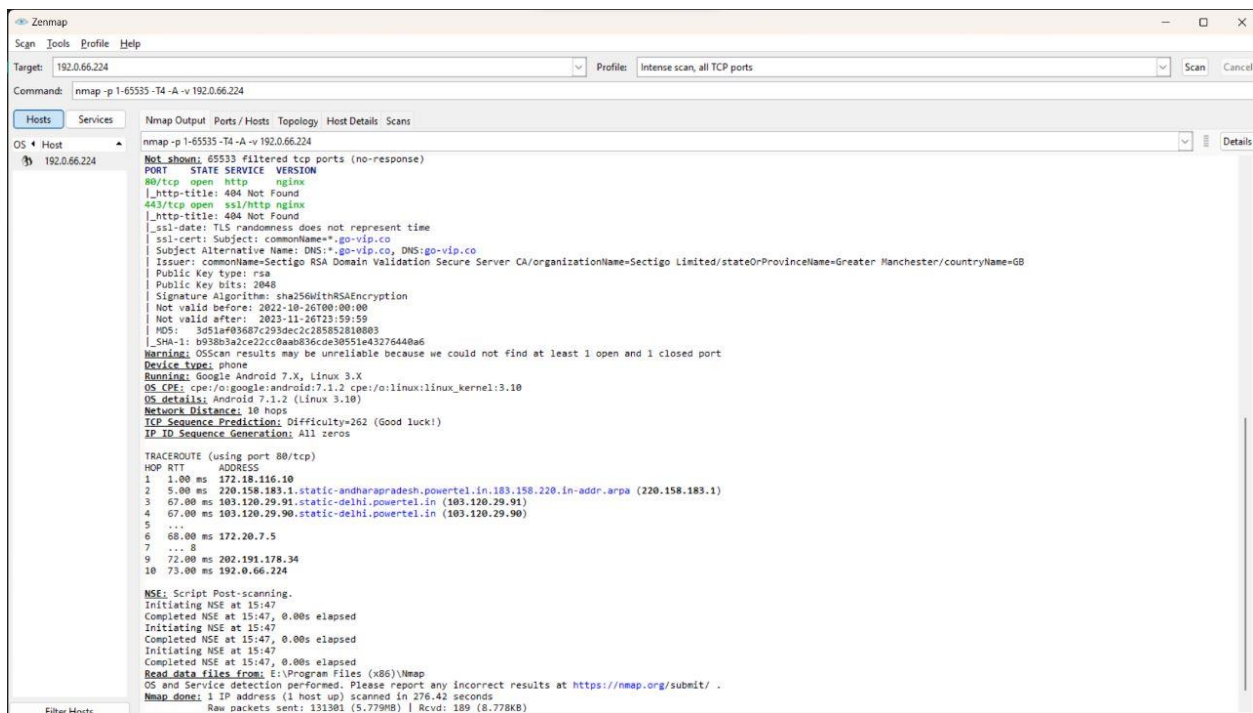
PORT STATE SERVICE VERSION

80/tcp open http nginx

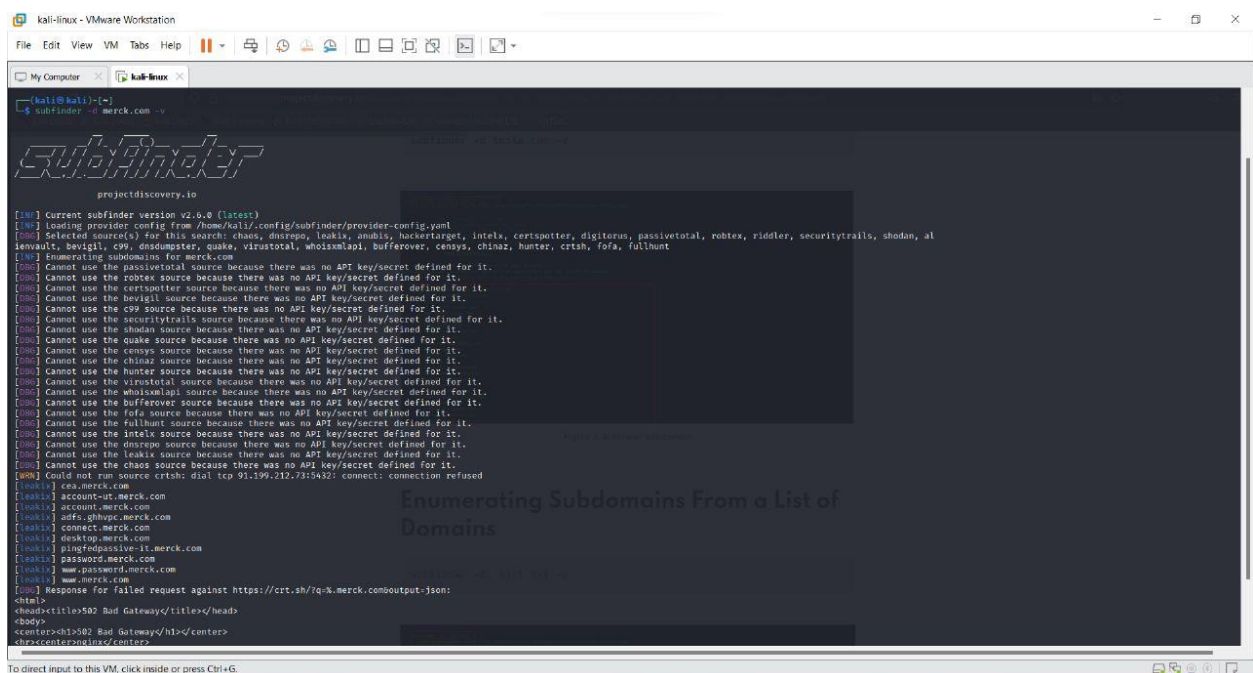
|_http-title: 404 Not Found

443/tcp open ssl/https nginx

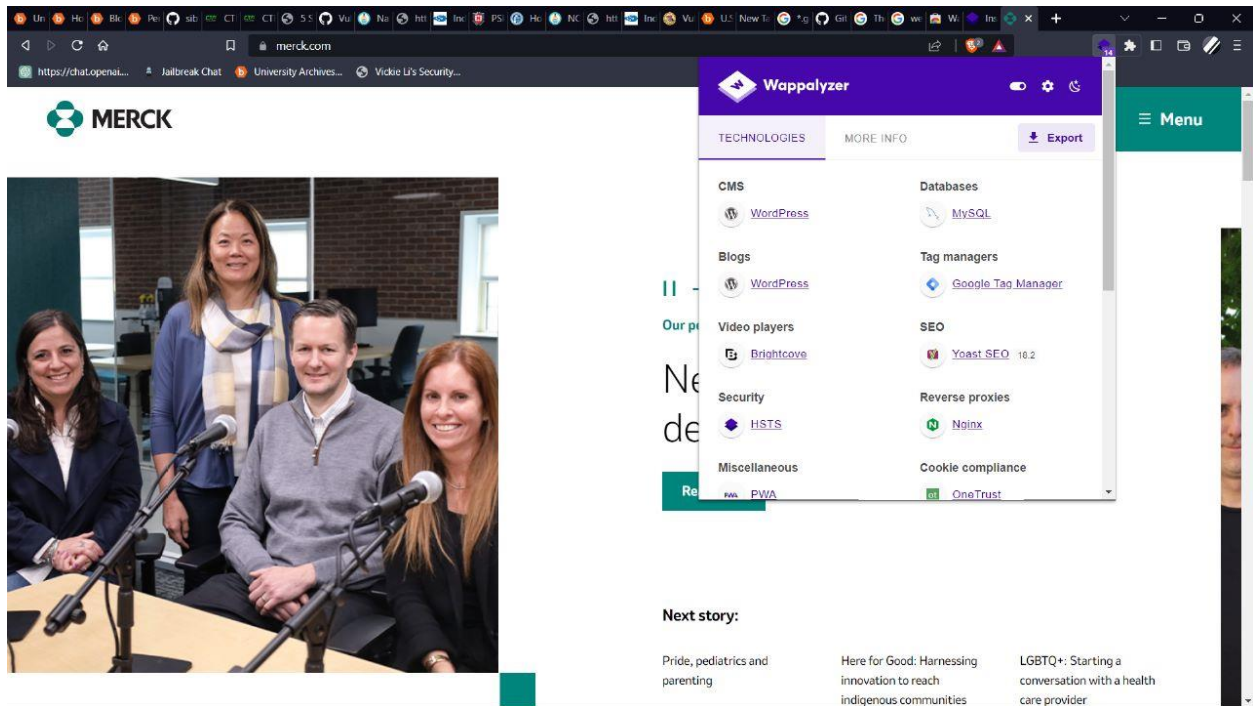
Filter Hosts



Subdomains:



Wappalyzer:



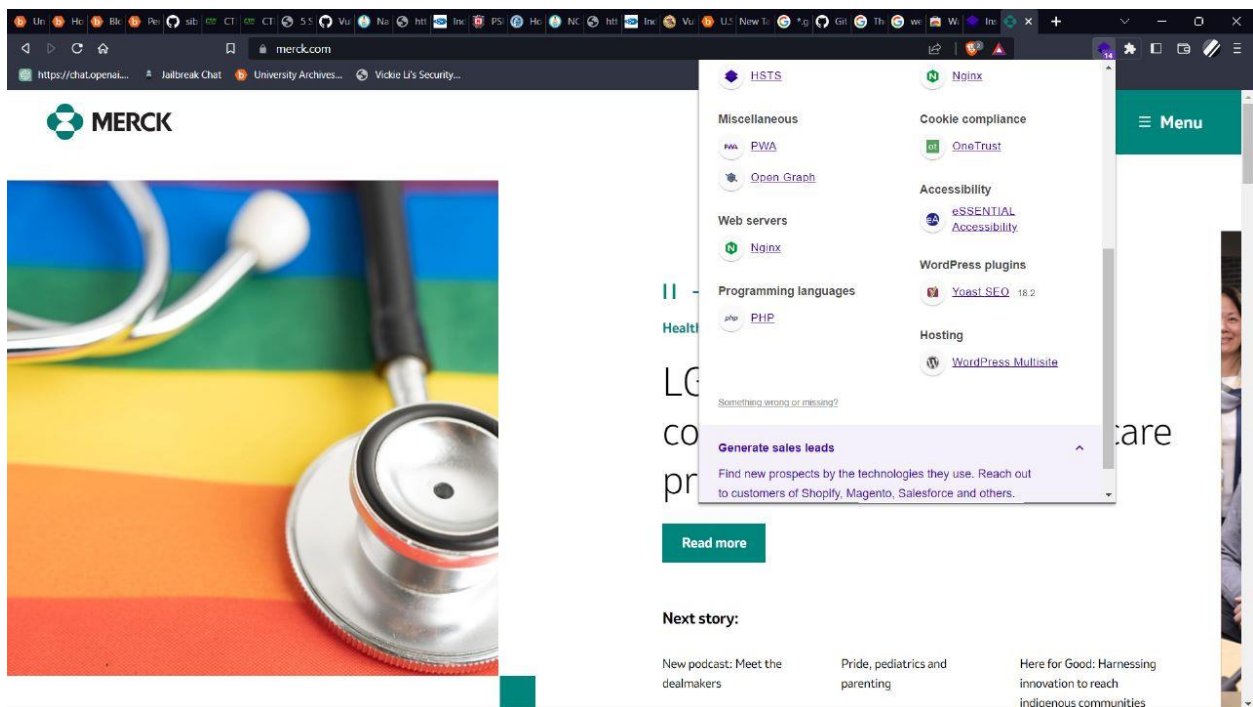
Wappalyzer

TECHNOLOGIES MORE INFO Export

- CMS: WordPress
- Blogs: WordPress
- Video players: Brightcove
- Security: HSTS
- Miscellaneous: PWA
- Databases: MySQL
- Tag managers: Google Tag Manager
- SEO: Yoast SEO 18.2
- Reverse proxies: Nginx
- Cookie compliance: OneTrust

Next story:

- Pride, pediatrics and parenting
- Here for Good: Harnessing innovation to reach indigenous communities
- LGBTQ+: Starting a conversation with a health care provider



Wappalyzer

Miscellaneous: PWA, Open Graph

Web servers: Nginx

Programming languages: PHP

Cookie compliance: OneTrust

Accessibility: eSSENTIAL Accessibility

WordPress plugins: Yoast SEO 18.2

Hosting: WordPress Multisite

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Next story:

- New podcast: Meet the dealmakers
- Pride, pediatrics and parenting
- Here for Good: Harnessing innovation to reach indigenous communities