Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 21/08/2023

Assignment Details

Assigned Date: 18/08/2023

Due Date: 21/08/2023

Topic: Passive Information Gathering

Introduction

Passive information gathering through browser extensions like Netcraft and Wappalyzer, combined with online tools such as CentralOps.net, has become an indispensable part of the modern digital reconnaissance toolkit. These tools allow security professionals, researchers, and web enthusiasts to collect valuable data about websites and their underlying technologies without directly engaging with the target. This passive approach is particularly useful for information gathering, competitive analysis, and threat intelligence.

Netcraft is a renowned browser extension that provides insights into a website's infrastructure, such as its hosting provider, SSL certificate details, and historical data about the site's uptime and changes. By simply visiting a website, Netcraft can reveal a wealth of information about its backend, helping users understand the technology stack employed and any potential vulnerabilities or attack vectors. This passive approach enables security teams to proactively assess and mitigate risks.

Wappalyzer, another powerful browser extension, specializes in identifying the software stack and technologies used by a website. It can detect content management systems, web frameworks, e-commerce platforms, and more. This information is invaluable for competitive analysis, as it allows businesses to gain insights into their competitors' tech stacks and potentially discover new tools or trends they can leverage to gain a competitive edge.

CentralOps.net serves as a centralized platform that complements these browser extensions. It offers various online tools and services, including domain name lookups, email verification, and network diagnostics. Users can obtain valuable passive information, such as the domain's WHOIS records, DNS information, and IP address details, all of which can aid in understanding a target's online footprint and infrastructure. This platform enhances the capabilities of browser extensions by providing a more comprehensive view of a target's digital presence.

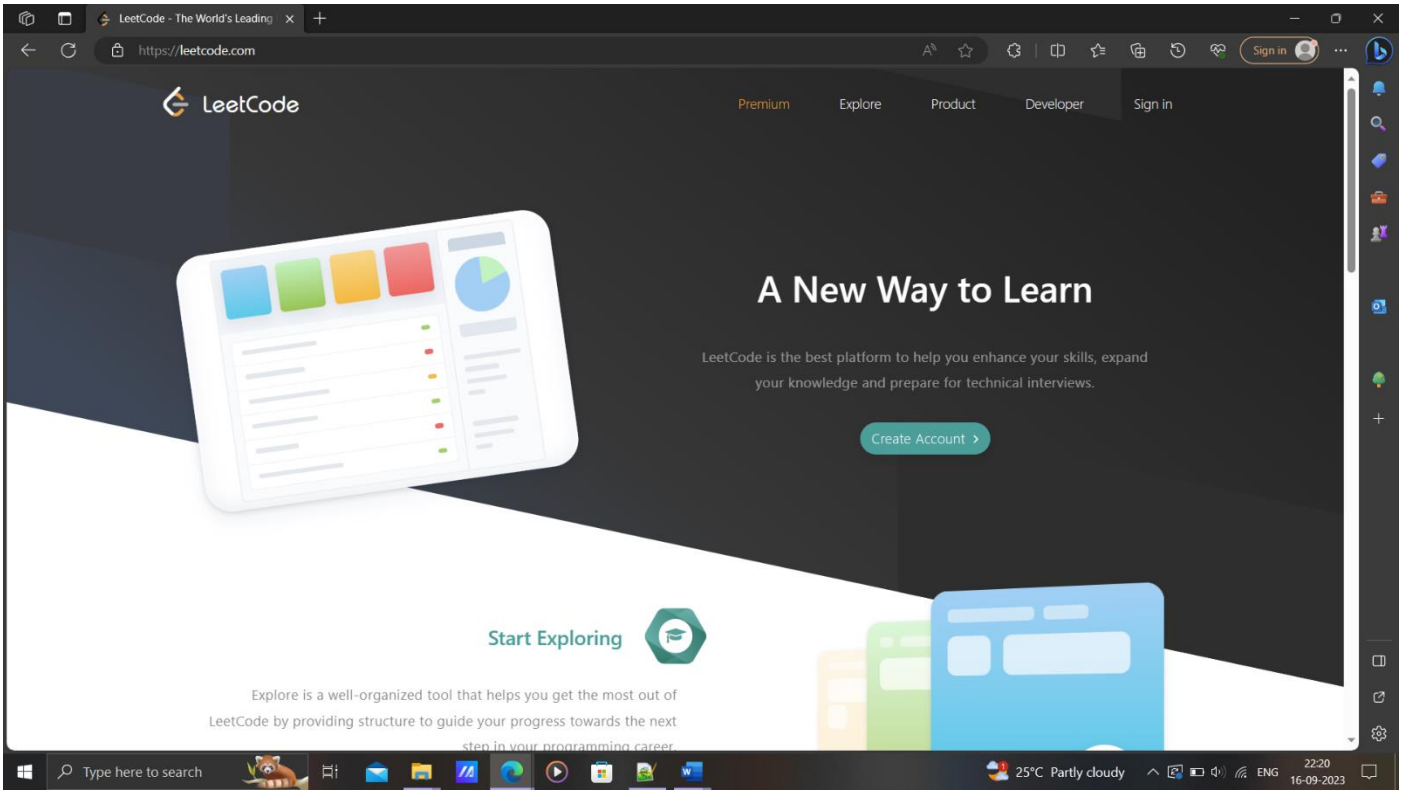
Content

Target 1:

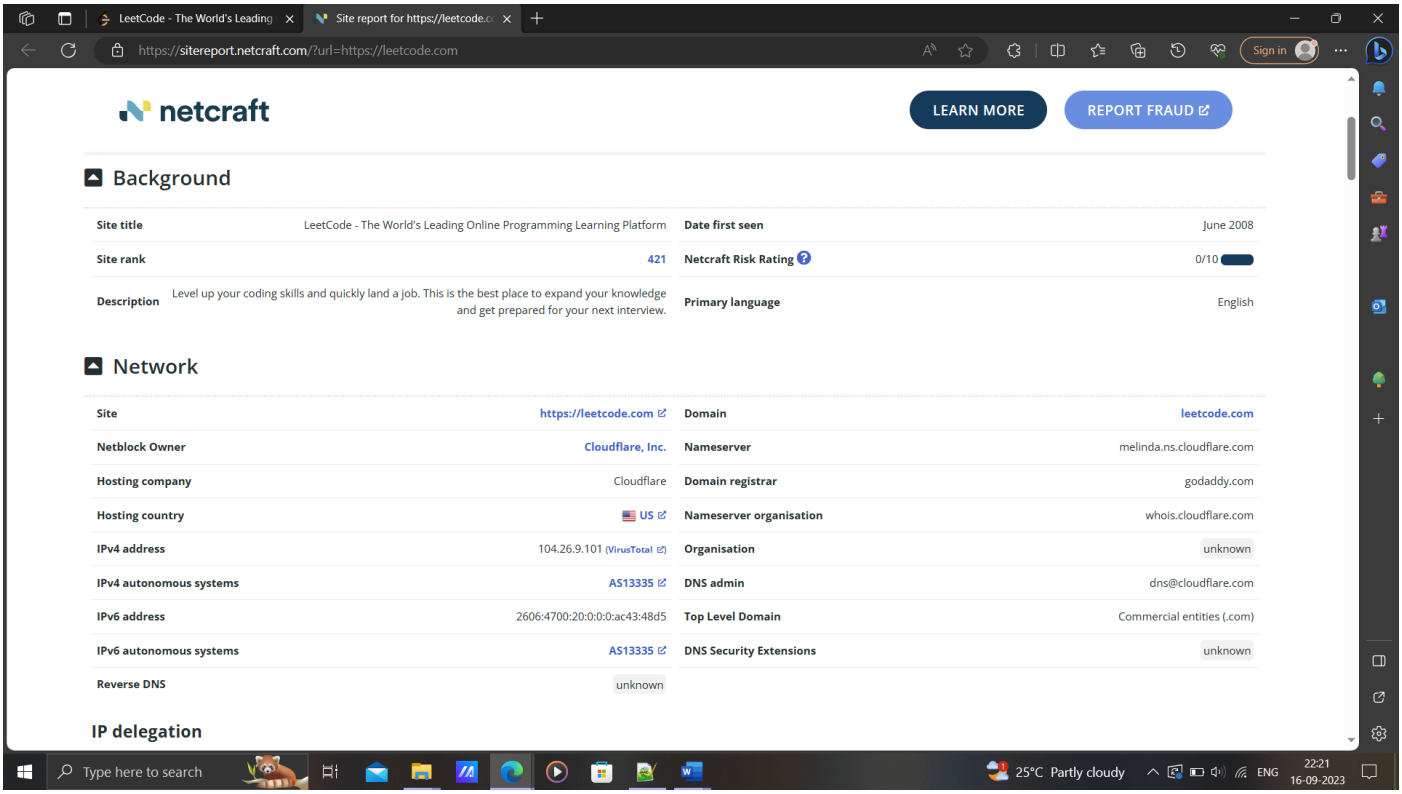
Leetcode

Domain: leetcode.com

Alias: www.leetcode.com



Passive IG (Information Gathering)



IP addresses:

IPv4 address (104.26.8.101)

IPv6 address (2606:4700:20:0:0:0:ac43:48d5)

Subdomains:

interview.leetcode.com: IPv4 address (104.26.8.101)

IPv6 address (2606:4700:20:0:0:0:681a:865)

support.leetcode.com: IPv4 address (104.16.53.111)

IPv6 address (N/A)

assets.leetcode.com : IPv4 address (104.26.9.101)

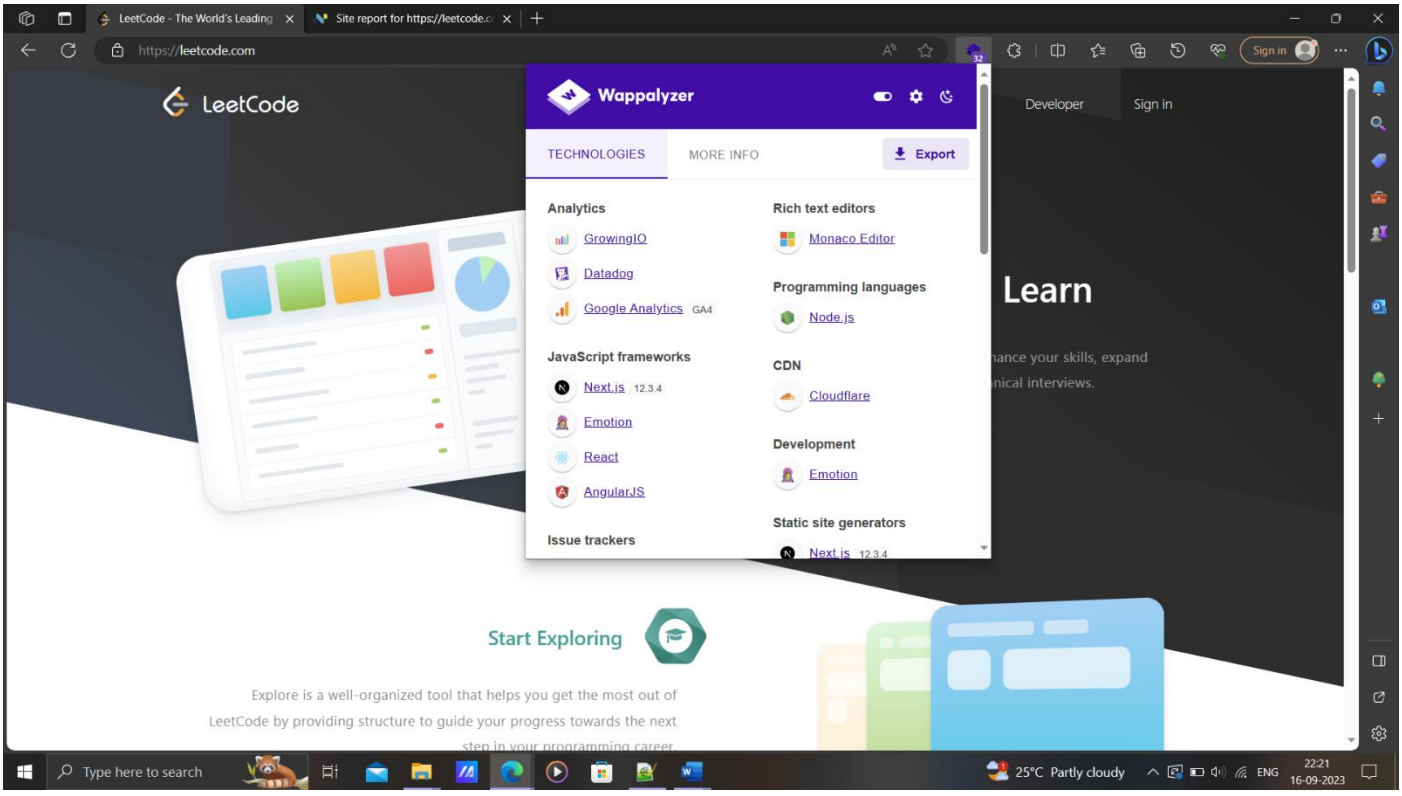
IPv6 address (2606:4700:20:0:0:0:681a:865)

DNS details / NameServer:

MELINDA.NS.CLOUDFLARE.COM

ROB.NS.CLOUDFLARE.COM

Technologies Used:



"URL": "https://leetcode.com"

"Miscellaneous": "Open Graph ; Webpack ; Babel ; Module Federation"

"Widgets": ""

"Analytics": "Datadog ; GrowingIO ; Google Analytics"

"Comment systems": ""

"Security": "reCAPTCHA ; HSTS"

"Font scripts": "Font Awesome"

"CDN": "Cloudflare"

"Marketing automation": ""

"Advertising": ""

"Webcams": ""

"Tag managers": ""

"Live chat": ""

"JavaScript libraries": "Select2 ; Lodash ; core-js ; SweetAlert2 ; jQuery UI ; jQuery ; Clipboard.js ; Bootstrap Table"

"Cookie compliance": ""

"Accessibility": ""

"SSL/TLS certificate authorities": ""

"Affiliate programs": ""

"Appointment scheduling": ""

"Surveys": ""

"A/B testing": ""

"Email": ""

"Personalisation": ""

"Retargeting": ""

"RUM": "New Relic ; Datadog"

"Geolocation": ""

"Browser fingerprinting": ""

"Loyalty & rewards": ""

"Feature management": ""

"Segmentation": ""

"Hosting": ""

"Translation": ""

"Reviews": ""

"Buy now pay later": ""

"Performance": ""

"Reservations & delivery": ""

"Referral marketing": ""

"Digital asset management": ""

"Content curation": ""

"Customer data platform": ""

"Cart abandonment": ""

"Shipping carriers": ""

"Recruitment & staffing": ""

"Returns": ""

"Livestreaming": ""

"Ticket booking": ""

"Augmented reality": ""

"Domain parking": ""

"Fundraising & donations": ""

"JavaScript frameworks": "Emotion ; React ; AngularJS"

"Web servers": ""

"Mobile frameworks": ""

"Payment processors": ""

"SEO": ""

"User onboarding": ""

"Containers": ""

"PaaS": ""

"IaaS": ""

"WordPress plugins": ""

"Shopify apps": ""

"Form builders": ""

"Video players": "Vimeo"

"Web frameworks": ""

"Caching": ""

"Web server extensions": ""

"Reverse proxies": ""

"Load balancers": ""

"UI frameworks": "Bootstrap"

"WordPress themes": ""

"Shopify themes": ""

"Drupal themes": ""

"JavaScript graphics": ""

"Operating systems": ""

"Authentication": ""

"Cross border ecommerce": ""

"Fulfilment": ""

"Ecommerce frontends": ""

"Rich text editors": ""

"Programming languages": ""

"Databases": ""

"CRM": ""

"Cryptominers": ""

"Editor": ""

"Search engines": ""

"CI": ""

"Database managers": ""

"Documentation tools": ""

"Hosting panels": ""

"Issue trackers": "Sentry"

"Webmail": ""

"Network services": ""

"Development": "Emotion"

"Network storage": ""

"CMS": ""

"Message boards": ""

"Ecommerce": ""

"Photo galleries": ""

"Wikis": ""

"LMS": ""

"Media servers": ""

"Remote Access": ""

"Feed readers": ""

"DMS": ""

"Page builder": ""

"Accounting": ""

"Static site generators": ""

"Phone number": ""

"Skype": ""

"WhatsApp": ""

"Email address": ""

"Email address (verified)": ""

"Email address (safe)": ""

"Twitter": ""

"Facebook": ""

"Instagram": ""

"GitHub": ""

"YouTube": ""

"Pinterest": ""

"LinkedIn": ""

"Owler": ""

"Title": ""

"Description": ""

"Copyright": ""

"Copyright year": ""

"Responsive": ""

"schema.org types": ""

"Cert organisation": ""

"Cert country": ""

"Cert state": ""

"Cert locality": ""

"Cert issuer": ""

"Cert protocol": ""

"Cert expiry": ""

"SPF record": ""

"DMARC record": ""

"SSL/TLS enabled": ""

"Google Analytics": ""

"Google AdSense": ""

"Medianet": ""

"Optimizely": ""

"Company name": ""

"Inferred company name": ""

"Industry": ""

"About": ""

"Locations": ""

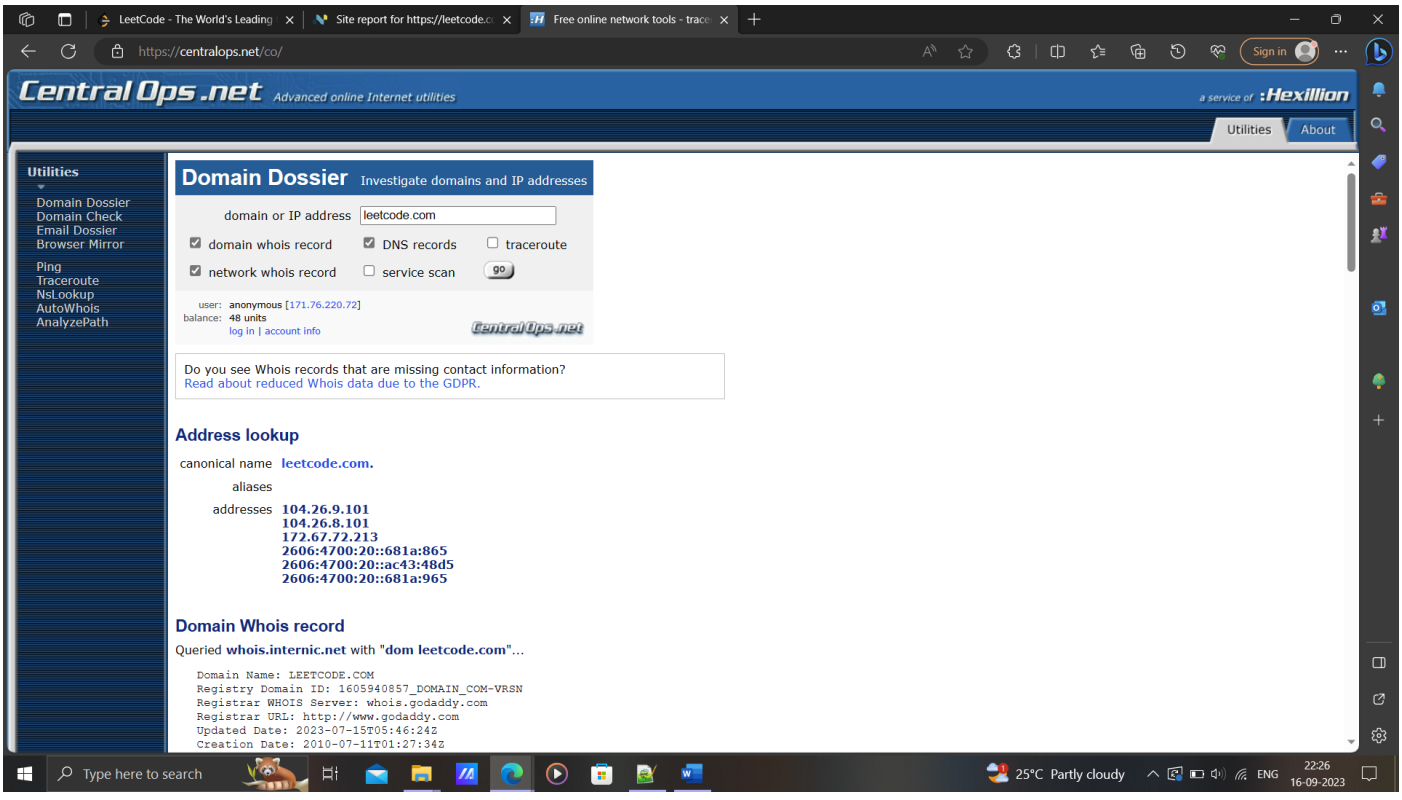
"Company size": ""

"Company type": ""

"Company founded": ""

"People": ""

centralOps.net:



Name Server: MELINDA.NS.CLOUDFLARE.COM

Name Server: ROB.NS.CLOUDFLARE.COM

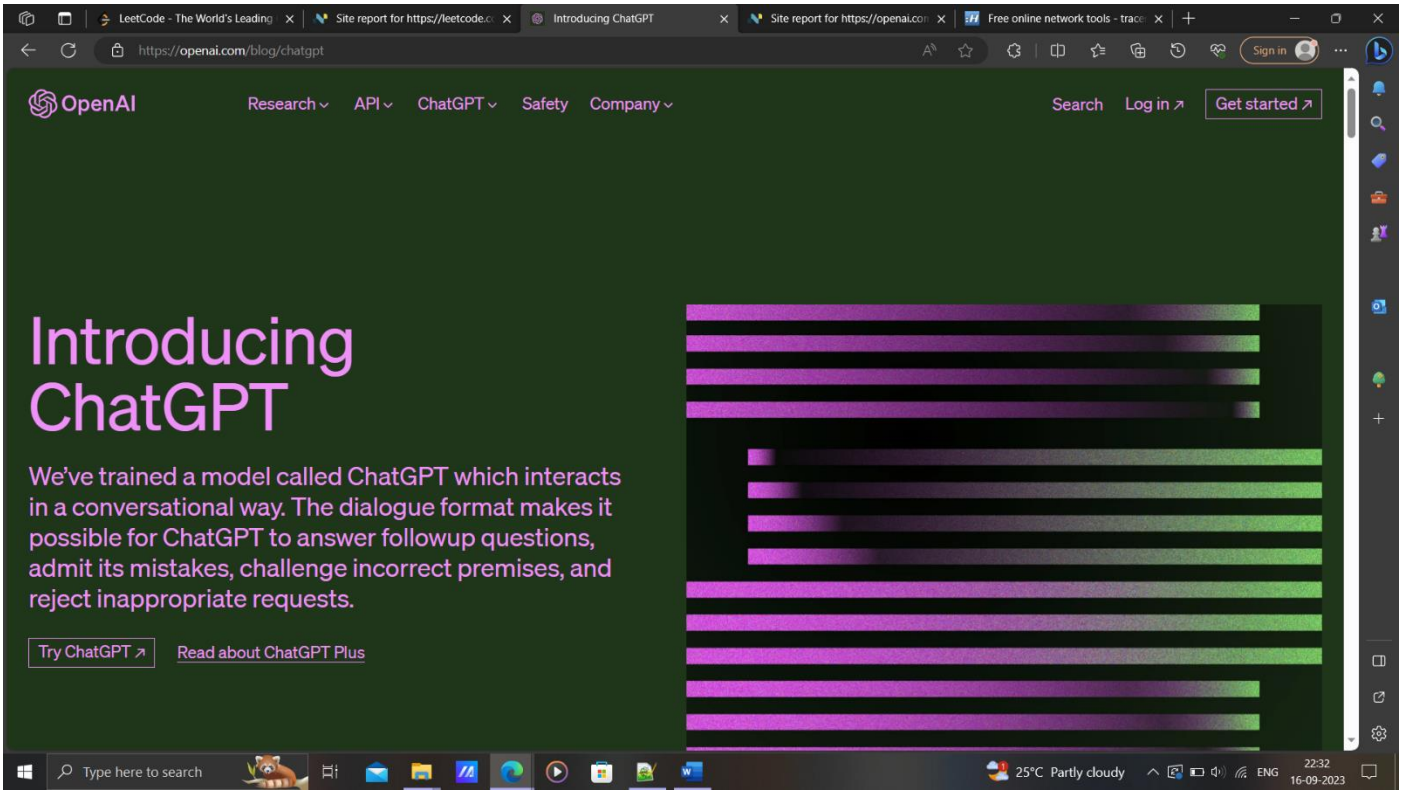
Target 2:

ChatGPT

Domain: openai.com

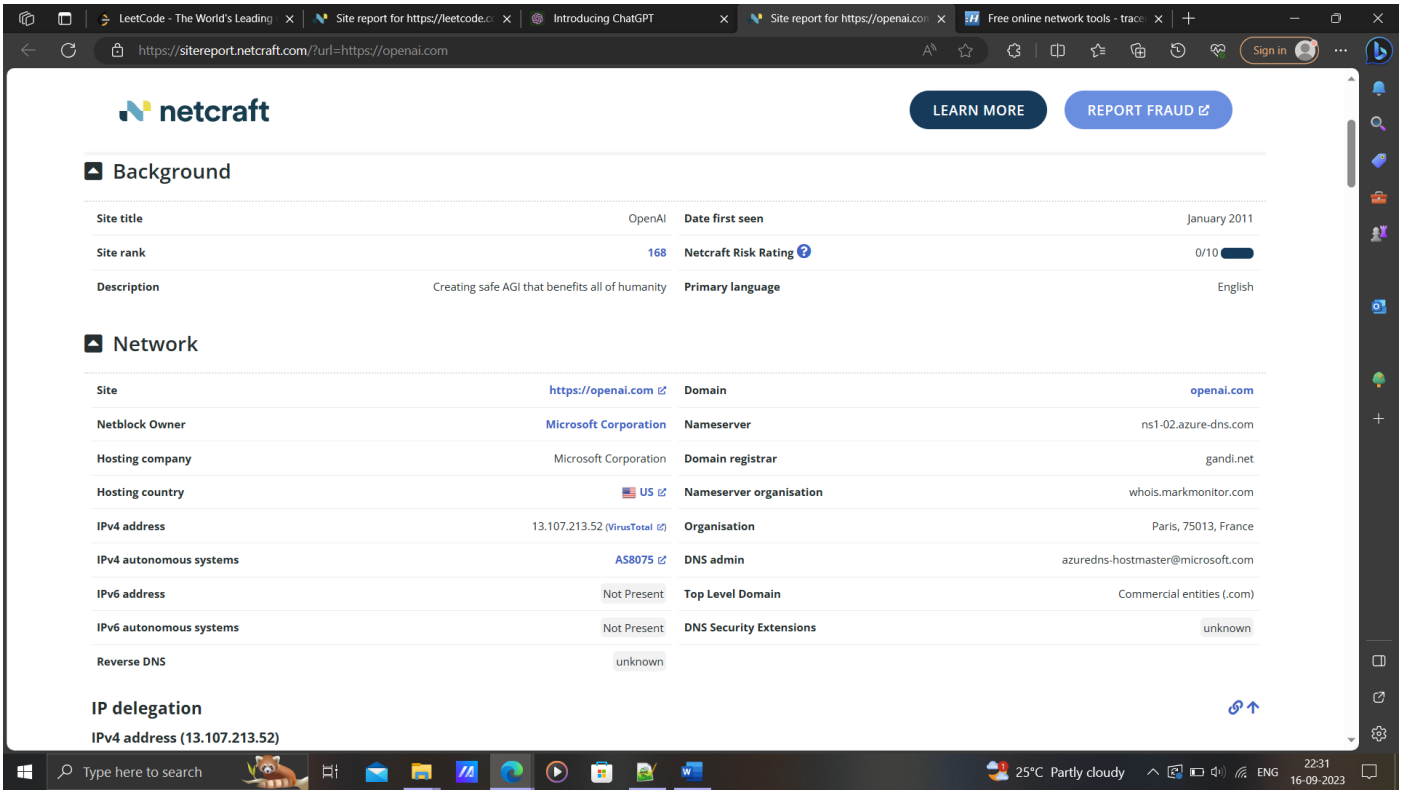
Site: https://chat.openai.com

Alias: chat.openai.com



Passive IG (Information Gathering)

IP addresses:



IPv4 address (104.18.2.161)

IPv6 address (2606:4700:0:0:0:0:6812:2a1)

Subdomains:

auth0.openai.com

beta.openai.com

platform.openai.com

labs.openai.com

help.openai.com

pay.openai.com

community.openai.com

feather.openai.com

chat.apps.openai.com

status.openai.com

cdn.openai.com

api.openai.com

spinningup.openai.com

www.openai.com

url3243.email.openai.com

microscope.openai.com

jukebox.openai.com

gym.openai.com

challenge.openai.com

home.apps.openai.com

DNS details / NameServer:

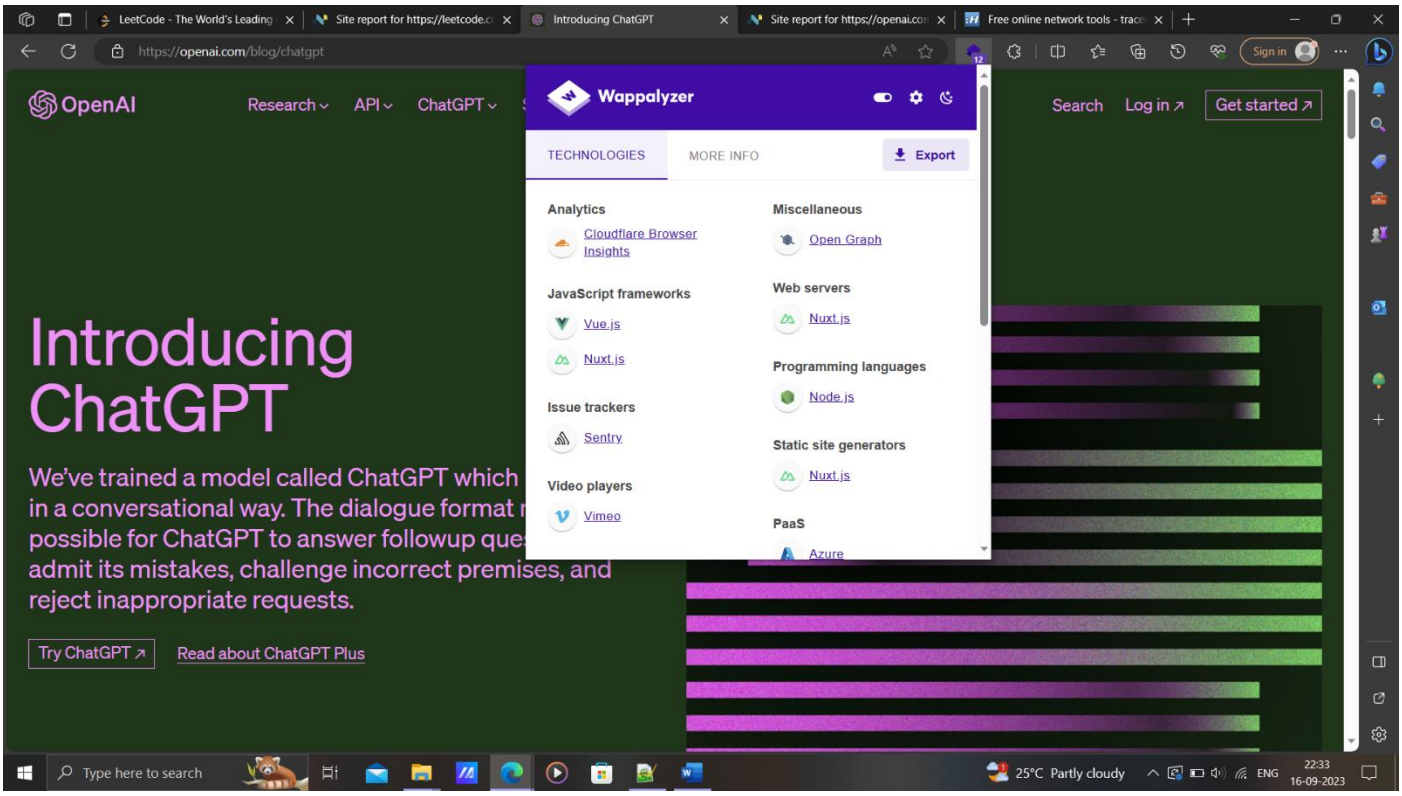
NS1-02.AZURE-DNS.COM

NS2-02.AZURE-DNS.NET

NS3-02.AZURE-DNS.ORG

NS4-02.AZURE-DNS.INFO

Technologies Used:



"URL": "https://chat.openai.com"

"Miscellaneous": "Webpack ; Open Graph ; Module Federation ; HTTP/3"

"Widgets": ""

"Analytics": "Datadog"

"Comment systems": ""

"Security": "Cloudflare Bot Management ; HSTS"

"Font scripts": ""

"CDN": "Cloudflare"

"Marketing automation": ""

"Advertising": ""

"Webcams": ""

"Tag managers": ""

"Live chat": "Intercom"

"JavaScript libraries": "PubSubJS ; Lodash ; core-js"

"Cookie compliance": ""

"Accessibility": ""

"SSL/TLS certificate authorities": ""

"Affiliate programs": ""

"Appointment scheduling": ""

"Surveys": ""

"A/B testing": ""

"Email": ""

"Personalisation": ""

"Retargeting": ""

"RUM": "Datadog"

"Geolocation": ""

"Browser fingerprinting": ""

"Loyalty & rewards": ""

"Feature management": ""

"Segmentation": ""

"Hosting": ""

"Translation": ""

"Reviews": ""

"Buy now pay later": ""

"Performance": ""

"Reservations & delivery": ""

"Referral marketing": ""

"Digital asset management": ""

"Content curation": ""

"Customer data platform": ""

"Cart abandonment": ""

"Shipping carriers": ""

"Recruitment & staffing": ""

"Returns": ""

"Livestreaming": ""

"Ticket booking": ""

"Augmented reality": ""

"Domain parking": ""

"Fundraising & donations": ""

"JavaScript frameworks": "React ; Emotion ; Next.js"

"Web servers": "Next.js"

"Mobile frameworks": ""

"Payment processors": ""

"SEO": ""

"User onboarding": ""

"Containers": ""

"PaaS": ""

"IaaS": ""

"WordPress plugins": ""

"Shopify apps": ""

"Form builders": ""

"Video players": ""

"Web frameworks": "Next.js"

"Caching": ""

"Web server extensions": ""

"Reverse proxies": ""

"Load balancers": ""

"UI frameworks": "Headless UI ; Tailwind CSS"

"WordPress themes": ""

"Shopify themes": ""

"Drupal themes": ""

"JavaScript graphics": ""

"Operating systems": ""

"Maps": ""

"Authentication": "NextAuth.js"

"Cross border ecommerce": ""

"Fulfilment": ""

"Ecommerce frontends": ""

"Rich text editors": ""

"Programming languages": "Node.js"

"Databases": ""

"CRM": "Intercom"

"Cryptominers": ""

"Editor": ""

"Search engines": ""

"CI": ""

"Database managers": ""

"Documentation tools": ""

"Hosting panels": ""

"Issue trackers": "Sentry"

"Webmail": ""

"Network services": ""

"": ""

"Development": "Emotion"

"Network storage": ""

"CMS": ""

"Message boards": ""

"Ecommerce": ""

"Photo galleries": ""

"Wikis": ""

"Blogs": ""

"LMS": ""

"Media servers": ""

"Remote Access": ""

"Feed readers": ""

"DMS": ""

"Page builder": ""

"Accounting": ""

"Static site generators": "Next.js"

"Phone number": ""

"Skype": ""

"WhatsApp": ""

"Email address": ""

"Email address (verified)": ""

"Email address (safe)": ""

"Twitter": ""

"Facebook": ""

"Instagram": ""

"GitHub": ""

"TikTok": ""

"YouTube": ""

"Pinterest": ""

"LinkedIn": ""

"Owler": ""

"Title": ""

"Description": ""

"Copyright": ""

"Copyright year": ""

"Responsive": ""

"schema.org types": ""

"Cert organisation": ""

"Cert country": ""

"Cert state": ""

"Cert locality": ""

"Cert issuer": ""

"Cert protocol": ""

"Cert expiry": ""

"SPF record": ""

"DMARC record": ""

"SSL/TLS enabled": ""

"Google Analytics": ""

"Google AdSense": ""

"Medianet": ""

"Optimizely": ""

"Company name": ""

"Inferred company name": ""

"Industry": ""

"About": ""

"Locations": ""

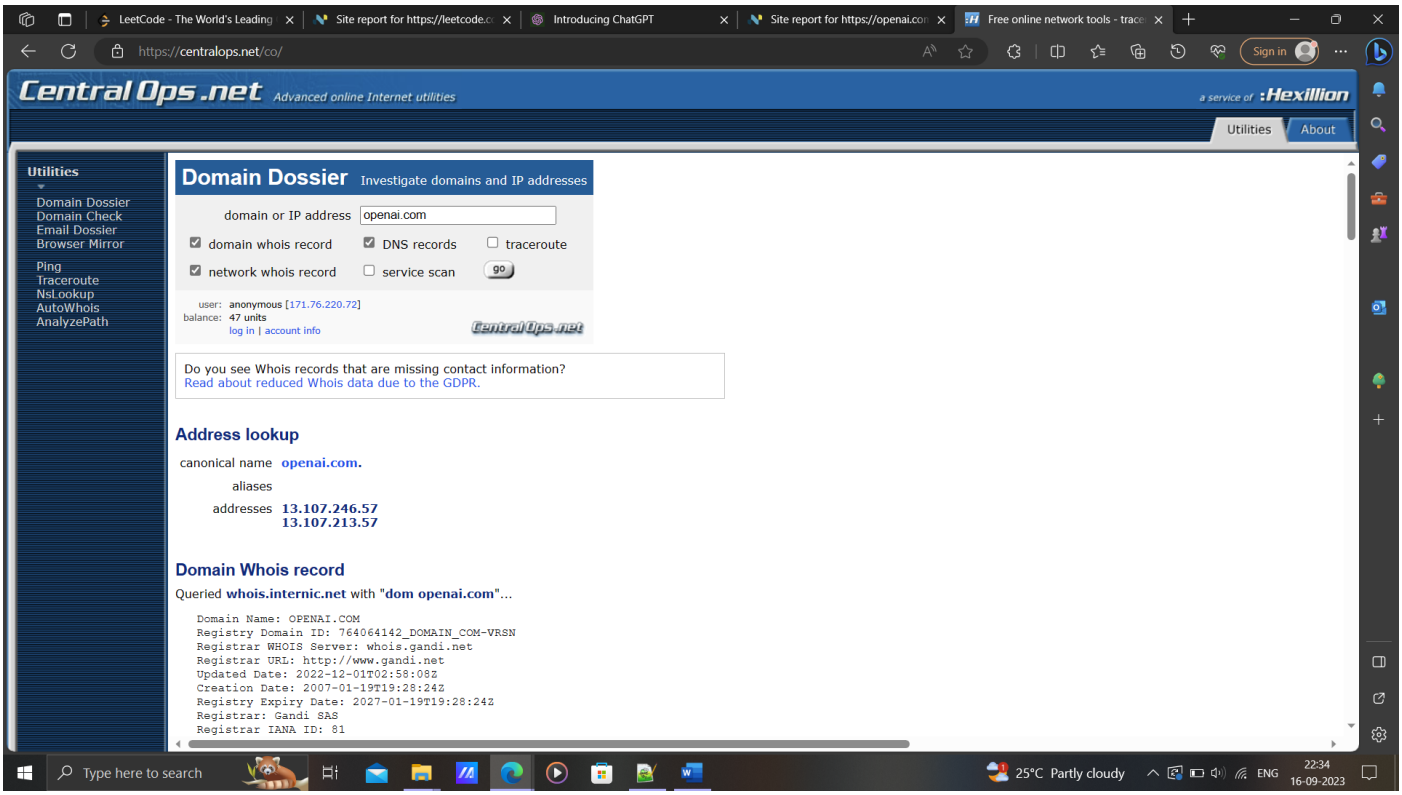
"Company size": ""

"Company type": ""

"Company founded": ""

"People": ""

centralOps.net:



Name Server: NS1-02.AZURE-DNS.COM

Name Server: NS2-02.AZURE-DNS.NET

Name Server: NS3-02.AZURE-DNS.ORG

Name Server: NS4-02.AZURE-DNS.INFO

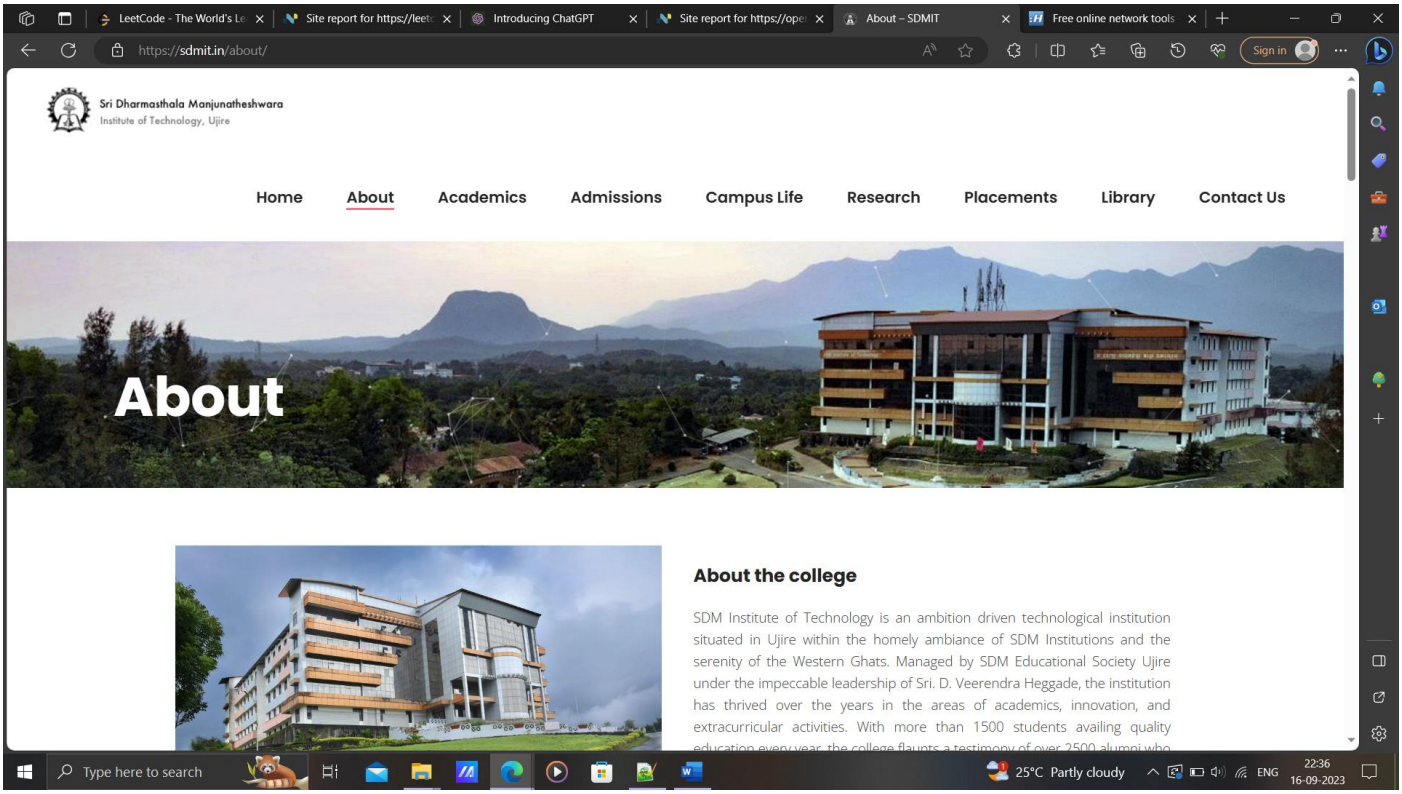
Target 3:

SDMIT – Ujire

Domain: sdmit.in

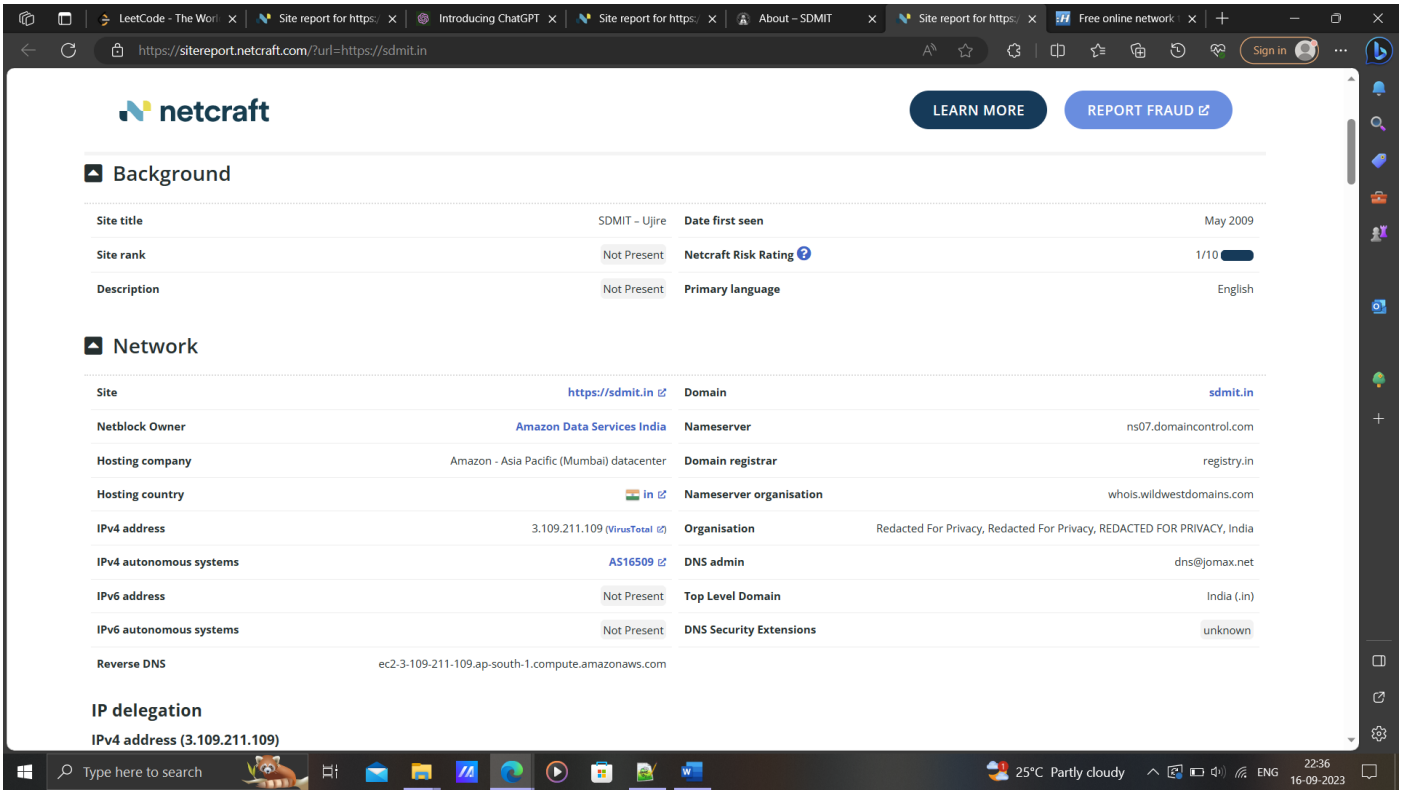
Site: https://sdmit.in

Alias: N/A



Passive IG(Information Gathering)

IP addresses:



IPv4 address (3.109.211.109)

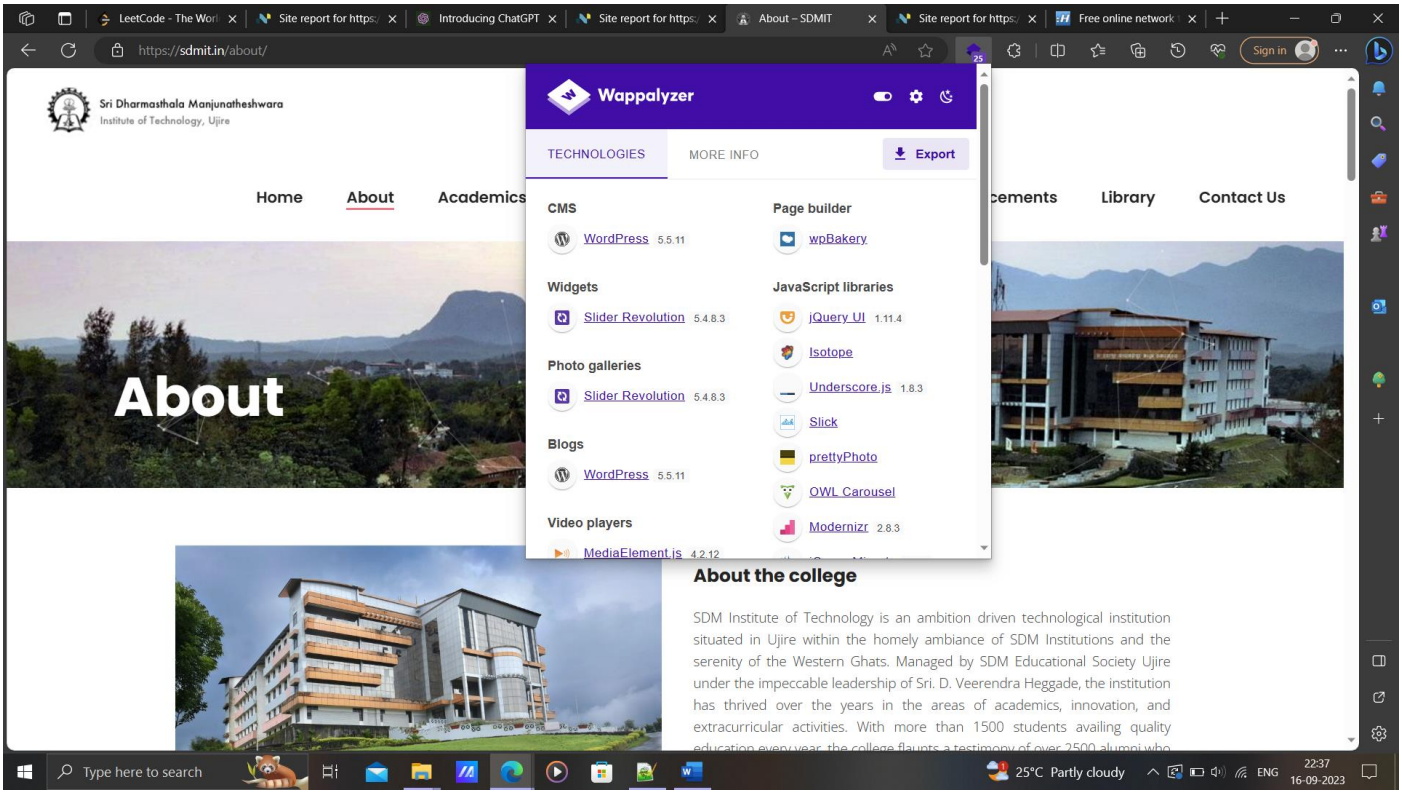
Subdomains: N/A

DNS details / NameServer:

ns08.domaincontrol.com

ns07.domaincontrol.com

Technologies Used:



"URL": "https://sdmit.in"

"Miscellaneous": "RSS"

"Widgets": "Slider Revolution"

"Analytics": ""

"Comment systems": ""

"Security": ""

"Font scripts": "Google Font API ; Twitter Emoji (Twemoji) ; Ionicons"

"CDN": ""

"Marketing automation": ""

"Advertising": ""

"Webcams": ""

"Tag managers": ""

"Live chat": ""

"JavaScript libraries": "jQuery UI ; Isotope ; Underscore.js ; Slick ; prettyPhoto ; OWL Carousel ; Modernizr ; jQuery Migrate ; jQuery"

"Cookie compliance": ""

"Accessibility": ""

"SSL/TLS certificate authorities": ""

"Affiliate programs": ""

"Appointment scheduling": ""

"Surveys": ""

"A/B testing": ""

"Email": ""

"Personalisation": ""

"Retargeting": ""

"RUM": ""

"Geolocation": ""

"Browser fingerprinting": ""

"Loyalty & rewards": ""

"Feature management": ""

"Segmentation": ""

"Hosting": ""

"Translation": ""

"Reviews": ""

"Buy now pay later": ""

"Performance": ""

"Reservations & delivery": ""

"Referral marketing": ""

"Digital asset management": ""

"Content curation": ""

"Customer data platform": ""

"Cart abandonment": ""

"Shipping carriers": ""

"Recruitment & staffing": ""

"Returns": ""

"Livestreaming": ""

"Ticket booking": ""

"Augmented reality": ""

"Domain parking": ""

"Fundraising & donations": ""

"JavaScript frameworks": ""

"Web servers": "Nginx"

"Mobile frameworks": ""

"Payment processors": ""

"SEO": ""

"User onboarding": ""

"Containers": ""

"PaaS": ""

"IaaS": ""

"WordPress plugins": "wpBakery ; WPForms ; The Events Calendar ; Contact Form 7"

"Shopify apps": ""

"Form builders": "WPForms ; Contact Form 7"

"Video players": "MediaElement.js"

"Web frameworks": ""

"Caching": ""

"Web server extensions": ""

"Reverse proxies": "Nginx"

"Load balancers": ""

"UI frameworks": ""

"WordPress themes": ""

"Shopify themes": ""

"Drupal themes": ""

"JavaScript graphics": ""

"Operating systems": "Ubuntu"

"Maps": ""

"Authentication": "Facebook Login"

"Cross border ecommerce": ""

"Fulfilment": ""

"Ecommerce frontends": ""

"Rich text editors": ""

"Programming languages": "PHP"

"Databases": "MySQL"

"CRM": ""

"Cryptominers": ""

"Editor": ""

"Search engines": ""

"CI": ""

"Database managers": ""

"Documentation tools": ""

"Hosting panels": ""

"Issue trackers": ""

"Webmail": ""

"Network services": ""

"": ""

"Development": ""

"Network storage": ""

"CMS": "WordPress"

"Message boards": ""

"Ecommerce": ""

"Photo galleries": "Slider Revolution"

"Wikis": ""

"Blogs": "WordPress"

"LMS": ""

"Media servers": ""

"Remote Access": ""

"Feed readers": ""

"DMS": ""

"Page builder": "wpBakery"

"Accounting": ""

"Static site generators": ""

"Phone number": ""

"Skype": ""

"WhatsApp": ""

"Email address": ""

"Email address (verified)": ""

"Email address (safe)": ""

"Twitter": ""

"Facebook": ""

"Instagram": ""

"GitHub": ""

"TikTok": ""

"YouTube": ""

"Pinterest": ""

"LinkedIn": ""

"Owler": ""

"Title": ""

"Description": ""

"Copyright": ""

"Copyright year": ""

"Responsive": ""

"schema.org types": ""

"Cert organisation": ""

"Cert country": ""

"Cert state": ""

"Cert locality": ""

"Cert issuer": ""

"Cert protocol": ""

"Cert expiry": ""

"SPF record": ""

"DMARC record": ""

"SSL/TLS enabled": ""

"Google Analytics": ""

"Google AdSense": ""

"Medianet": ""

"Optimizely": ""

"Company name": ""

"Inferred company name": ""

"Industry": ""

"About": ""

"Locations": ""

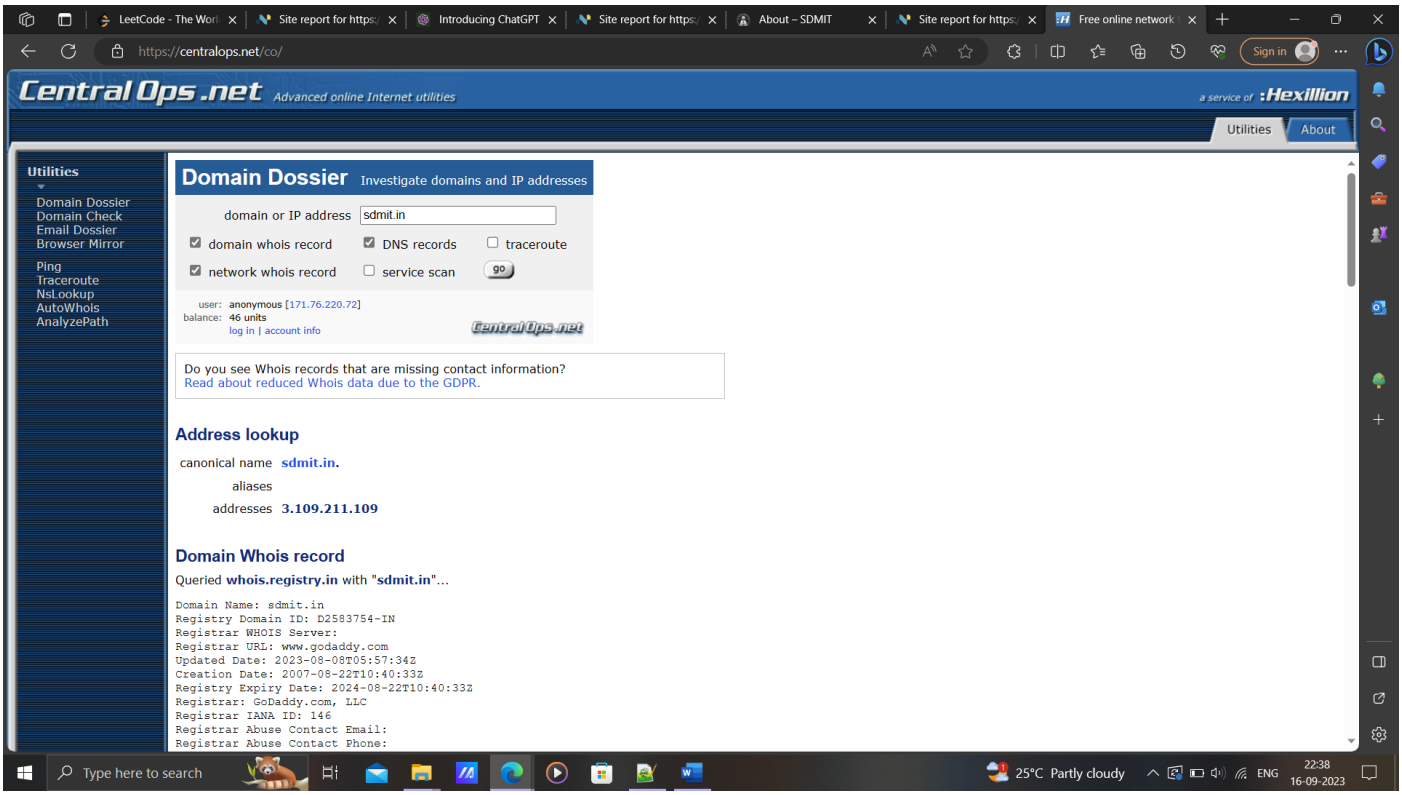
"Company size": ""

"Company type": ""

"Company founded": ""

"People": ""

centralOps.net:



Name Server: ns08.domaincontrol.com

Name Server: ns07.domaincontrol.com

Analysis

The project focused on the practice of passive information gathering, examining its implications across three distinct targets. By employing a range of ethical techniques, the analysis revealed comprehensive insights into each target's digital footprint, potential vulnerabilities, and security posture. Through thorough examination of publicly available sources, including websites, social media, and public records, the study shed light on the significance of passive reconnaissance in understanding and assessing the information landscape surrounding the selected targets. The project underscored the importance of responsible and legal approaches to information gathering while emphasizing the need for organizations to proactively manage their online presence.

Conclusion

In conclusion, the project demonstrated the significance of passive information gathering as a valuable method for acquiring insights without direct engagement. Through the examination of three diverse targets, it became evident that publicly available information can provide a substantial understanding of their digital identities and potential security vulnerabilities. However, ethical considerations and legal boundaries must be rigorously upheld to ensure responsible information collection practices. As the digital landscape continues to evolve, embracing passive information gathering as a complementary tool within the realm of cybersecurity and intelligence remains paramount.