PRACTICAL: 3

AIM:

Footprinting is the process of accumulating data regarding a specific network environment, usually to find ways to intrude into it. It can reveal system vulnerabilities and improve the ease with which they can be exploited. Footprinting is also known as reconnaissance. Study a practical approach to implementing Footprinting: Gathering Target Information using the OSINT Framework.

THEORY:

OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources. Some of the sites included might require registration or offer more data for $$$, but you should be able to get at least a portion of the available information for no cost.

The five tools we will use in this exercise are:

1. WhatsMyName
2. Web Archive (Wayback Machine)
3. URLScan.io
4. DNSDumpster
5. OpenCorporates

1. WhatsMyName: Gathering DNS and Subdomain Information

Overview: WhatsMyName is an OSINT tool designed to perform DNS lookups and provide information about domain names. It helps identify various domain records associated with a target, including subdomains, IP addresses, and mail servers.

Steps:

- Go to the **WhatsMyName** website.
- Enter the domain name (e.g., "example.com") of the target you wish to investigate.
- The tool will return DNS records, which may include:
    - **A Records**: IP addresses associated with the domain.
    - **MX Records**: Mail servers linked to the domain.
    - **Subdomains**: Any additional domains or subdomains tied to the target.
    - **Nameservers**: Information about the authoritative nameservers for the domain.

This information helps us build a map of the target's domain infrastructure. It can reveal other systems or services the target might be running or any exposed services like mail servers or web applications.

2. Web Archive (Wayback Machine): Exploring Historical Web Data

Overview: The Wayback Machine, part of the Internet Archive, allows you to access historical versions of websites. It provides snapshots of websites taken at various points in time, enabling you to uncover potentially exposed information that has since been removed or changed.

Steps:

- Visit the **Wayback Machine** at archive.org/web.
- Enter the target's URL (e.g., "example.com") and press "Browse History."
- You will be shown a calendar of snapshots taken by the Wayback Machine, which you can explore by clicking on different dates.

Reviewing past versions of the target's website might reveal old content that could have been inadvertently exposed, such as outdated documents, forms, or login pages.

This can help you identify misconfigurations or legacy systems that have since been updated or removed from the live site.

3. URLScan.io: Scanning and Analyzing Web Pages

Overview: URLScan.io is a security analysis tool that scans websites and provides detailed reports about how a site behaves. It highlights external domains, embedded JavaScript, network activities, and potential security issues that might not be immediately visible from a standard web visit.

Steps:

- Go to **URLScan.io**.
- Enter the target URL (e.g., "example.com") in the search bar.
- URLScan.io will scan the website and return a report detailing:
    - External domains the site is connected to (e.g., third-party services, trackers).
    - Embedded JavaScript files and other resources.
    - Security headers and potential vulnerabilities.

This tool helps identify connections to external servers or suspicious domains that the target website might be communicating with.

The scan results can reveal potential security risks, such as unprotected scripts or malicious activity linked to the domain.

4. DNSDumpster: Comprehensive DNS and Network Mapping

Overview: DNSDumpster is a free tool that maps out DNS records for a given domain. It can provide insights into a target's DNS infrastructure, uncovering subdomains, associated IP addresses, and DNS record details that might help in understanding the target's network architecture.

Steps:

- Visit **DNSDumpster.com**.
- Enter the target domain name (e.g., "example.com") in the search bar and click "Search."
- The tool will display:
    - **Subdomains**: A list of subdomains linked to the target domain.
    - **DNS Records**: Information such as A, MX, and CNAME records.
    - **IP Addresses**: The range of IP addresses associated with the target's services.
    - **Geolocation Information**: The physical locations of the associated servers.

Use the subdomain and IP information to uncover additional services or infrastructure related to the target.

Mapping out DNS records helps you identify vulnerable or exposed systems, such as mail servers, that could be potential entry points.

5. OpenCorporates: Investigating Corporate Data

Overview: OpenCorporates is a database that aggregates public company registration data from jurisdictions around the world. It provides insights into the legal and business structure of organizations, which can be invaluable for foot printing a target company.

Steps:

- Go to **OpenCorporates** at opencorporates.com.
- Enter the target company name (e.g., "Example Corp.") or its business registration number.
- OpenCorporates will return:
    - **Corporate Registration Information**: Data about the company's registration, including jurisdiction and date of incorporation.
    - **Corporate Structure**: Information about subsidiaries, parent companies, and related entities.

- **Directors and Key Personnel**: Publicly available data about the company's executives and board members.

This tool helps us to understand the organizational structure of the target, revealing potential subsidiaries, associated businesses, or directors who may have connections to other vulnerable assets.

The company's legal records could also provide insights into its history, legal standing, and potential financial issues, all of which can be valuable when assessing security risks.

CODE:

N/A

OUTPUT:

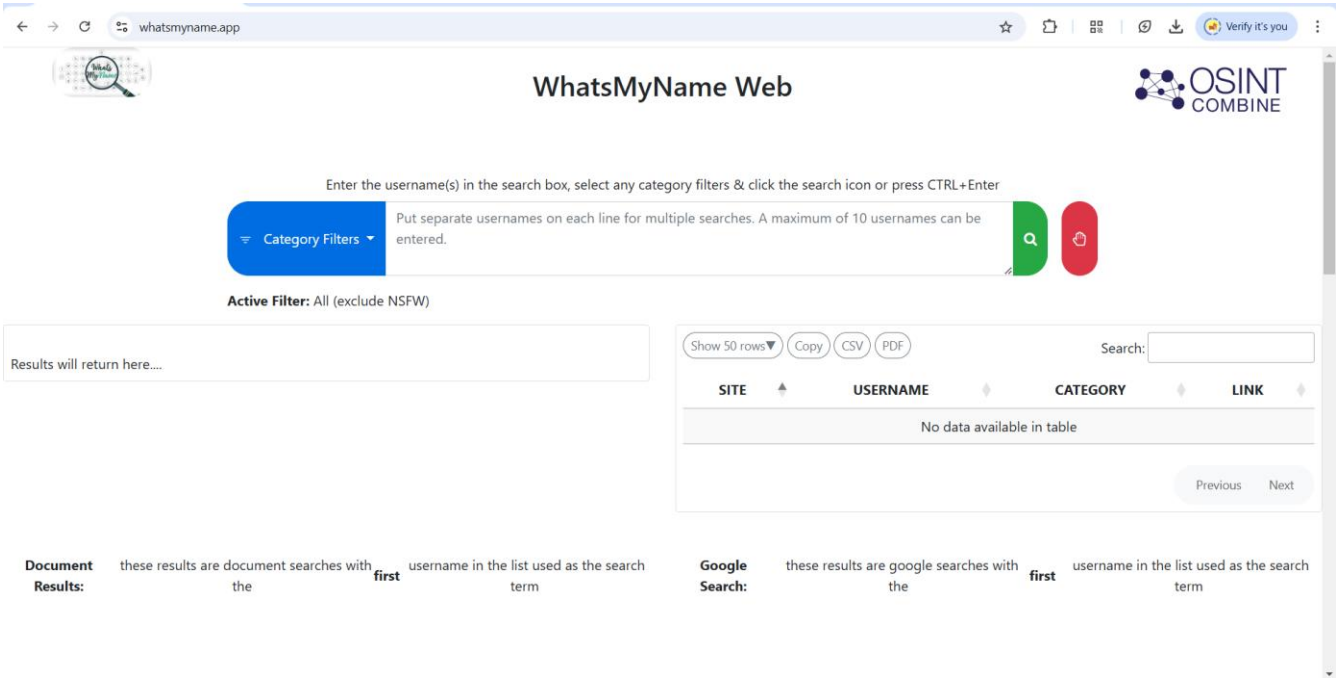


Figure 1:OSINT whatsMyName Web tool

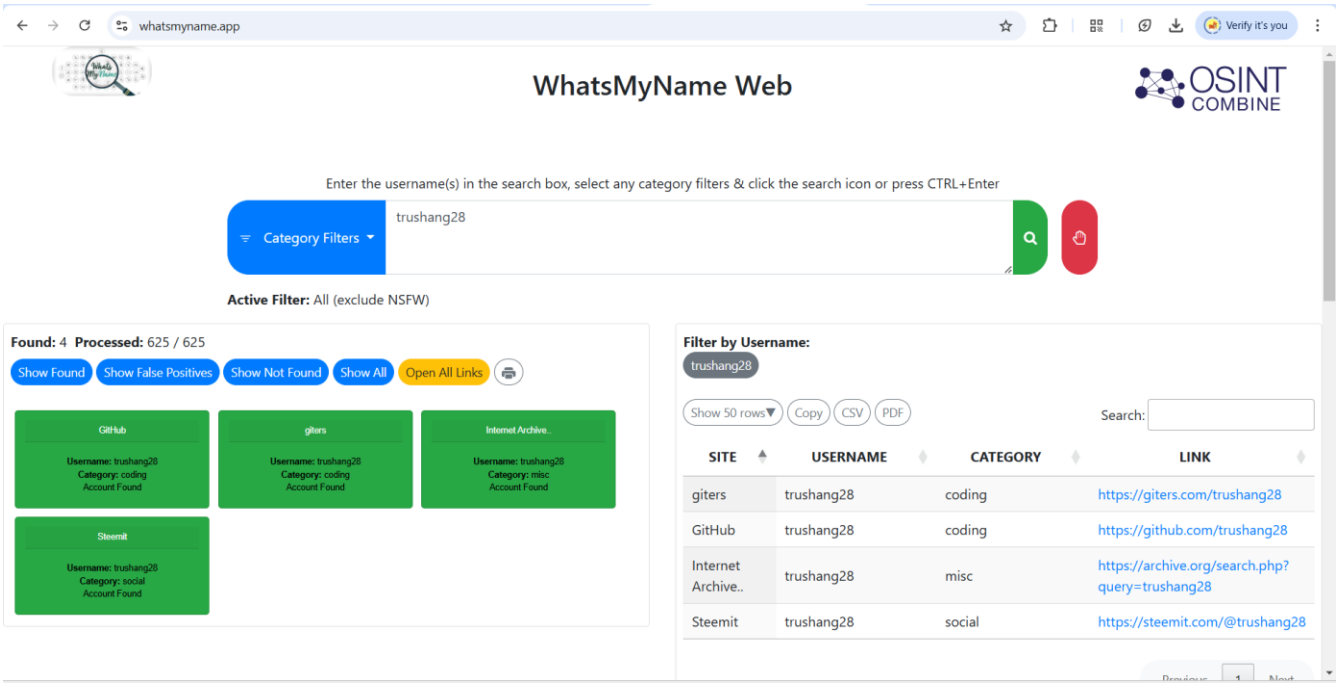


Figure 2:We provide our username it will check 625 site and found 4 as this username

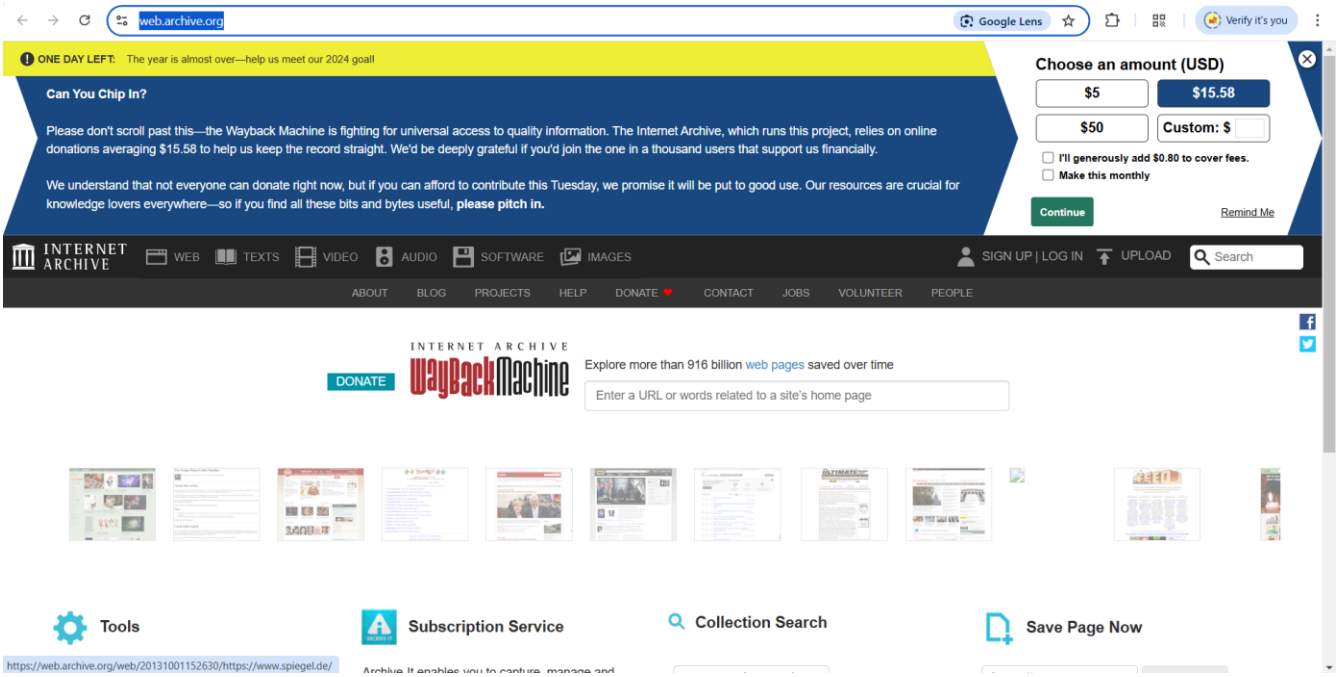


Figure 3:Second tools are web archive

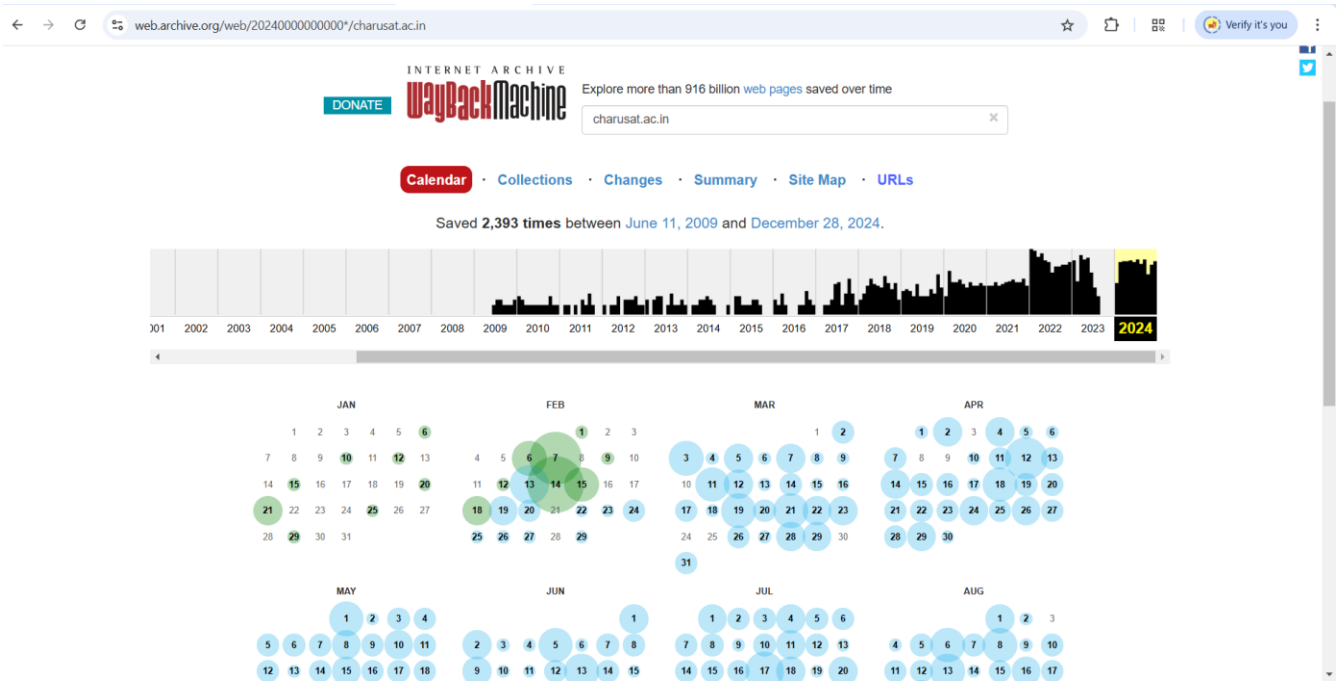


Figure 4:This is change in website month wise

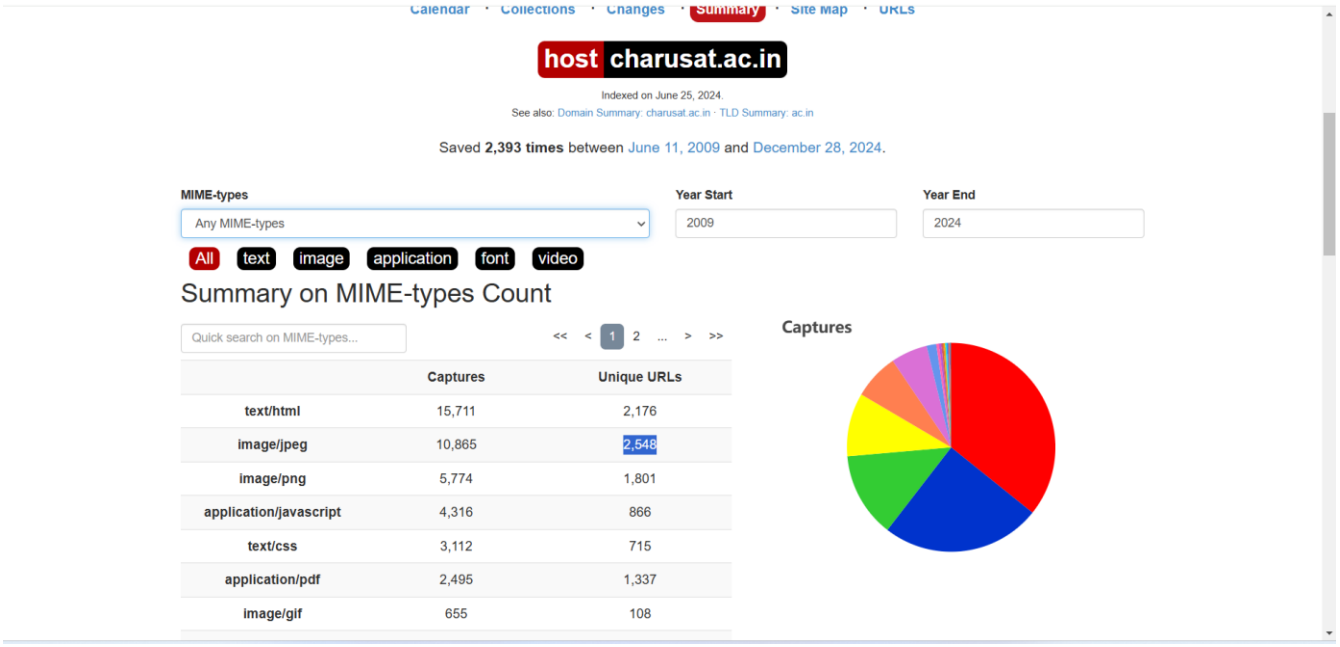
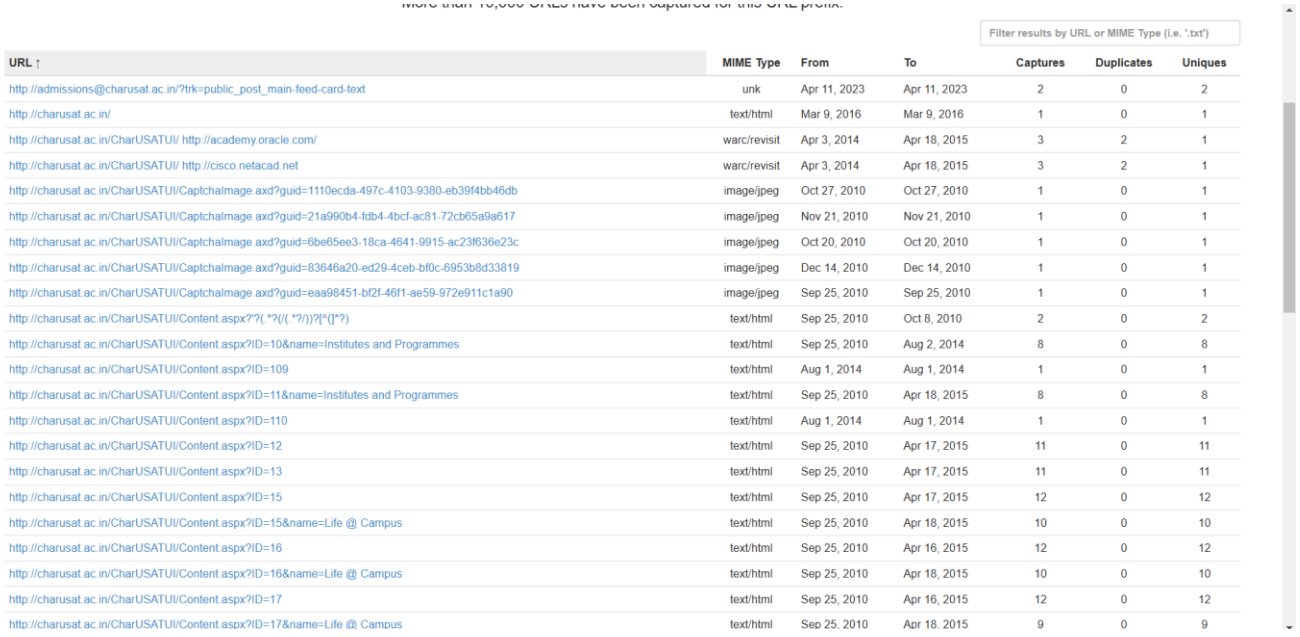


Figure 5:This is summary of charusat.ac.in

Figure 6:This is site map for charusat.ac.in of year 2024



Filter results by URL or MIME Type (i.e. '.txt')

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://admissions@charusat.ac.in/?trk=public_post_main-feed-card-text	unk	Apr 11, 2023	Apr 11, 2023	2	0	2
http://charusat.ac.in/	text/html	Mar 9, 2016	Mar 9, 2016	1	0	1
http://charusat.ac.in/CharUSATUI/ http://academy.oracle.com/	warc/revisit	Apr 3, 2014	Apr 18, 2015	3	2	1
http://charusat.ac.in/CharUSATUI/ http://cisco.netacad.net	warc/revisit	Apr 3, 2014	Apr 18, 2015	3	2	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=1110ecda-497c-4103-9380-eb39f4bb46db	image/jpeg	Oct 27, 2010	Oct 27, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=21a990b4-fdb4-4bcf-ac81-72cb65a9a617	image/jpeg	Nov 21, 2010	Nov 21, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=6be65ee3-18ca-4641-9915-ac23f636e23c	image/jpeg	Oct 20, 2010	Oct 20, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=83646a20-ed29-4ceb-bf0c-6953b8d33819	image/jpeg	Dec 14, 2010	Dec 14, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/CaptchaImage.axd?guid=eaa98451-bf2f-46f1-ae59-972e911c1a90	image/jpeg	Sep 25, 2010	Sep 25, 2010	1	0	1
http://charusat.ac.in/CharUSATUI/Content.aspx?'?(.*?(/(.*?/))?[^(]*?)	text/html	Sep 25, 2010	Oct 8, 2010	2	0	2
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=10&name=Institutes and Programmes	text/html	Sep 25, 2010	Aug 2, 2014	8	0	8
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=109	text/html	Aug 1, 2014	Aug 1, 2014	1	0	1
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=11&name=Institutes and Programmes	text/html	Sep 25, 2010	Apr 18, 2015	8	0	8
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=110	text/html	Aug 1, 2014	Aug 1, 2014	1	0	1
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=12	text/html	Sep 25, 2010	Apr 17, 2015	11	0	11
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=13	text/html	Sep 25, 2010	Apr 17, 2015	11	0	11
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=15	text/html	Sep 25, 2010	Apr 17, 2015	12	0	12
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=15&name=Life @ Campus	text/html	Sep 25, 2010	Apr 18, 2015	10	0	10
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=16	text/html	Sep 25, 2010	Apr 16, 2015	12	0	12
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=16&name=Life @ Campus	text/html	Sep 25, 2010	Apr 18, 2015	10	0	10
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=17	text/html	Sep 25, 2010	Apr 16, 2015	12	0	12
http://charusat.ac.in/CharUSATUI/Content.aspx?ID=17&name=Life @ Campus	text/html	Sep 25, 2010	Apr 18, 2015	9	0	9

Figure 7:This are URL where charusat.ac.in is used as prefix

Figure 8:Third tool are urlscan.io

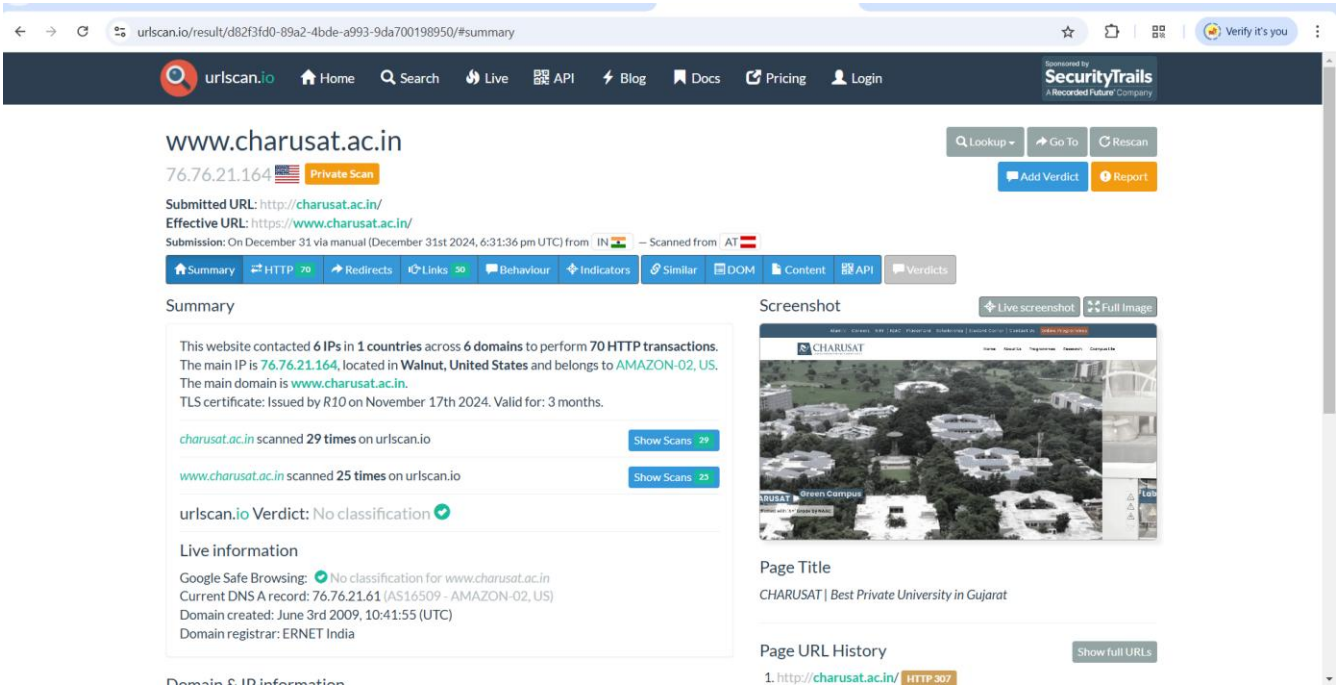


Figure 9:We scan charusat.ac.in privately and we scan charusat.ac.in 25 times

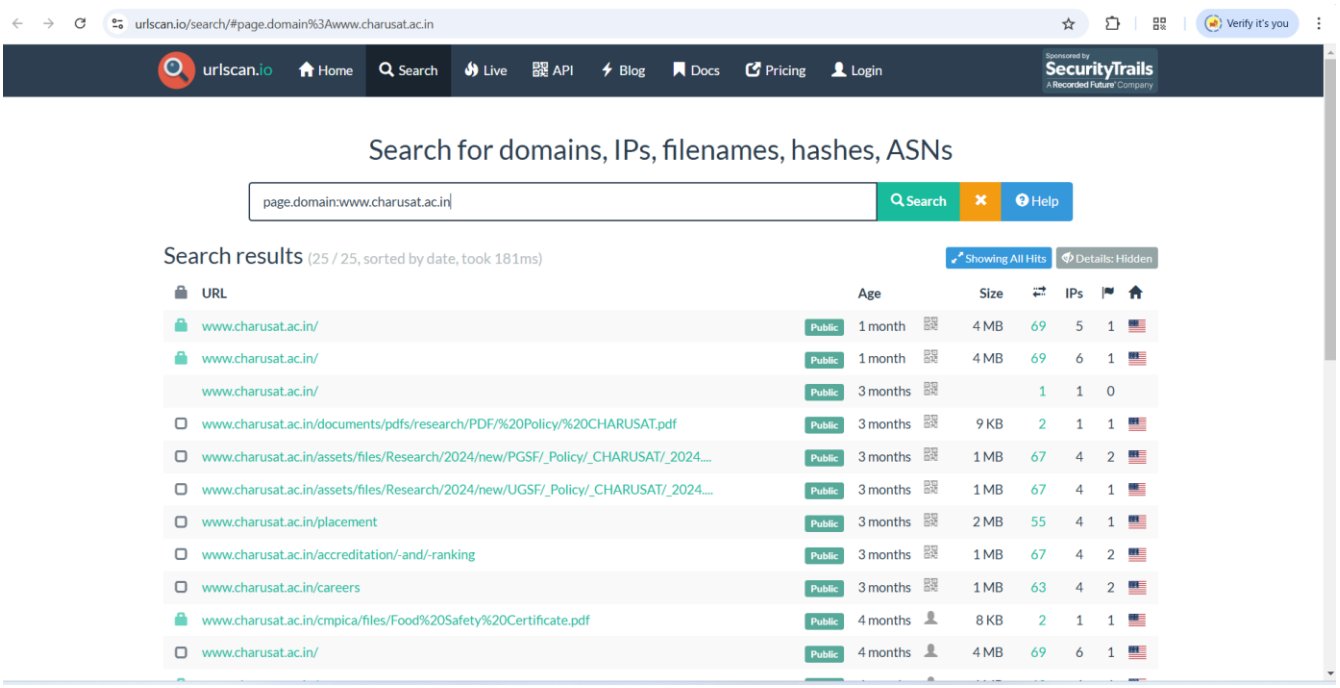


Figure 10:We can see which sub domain URL scan happened

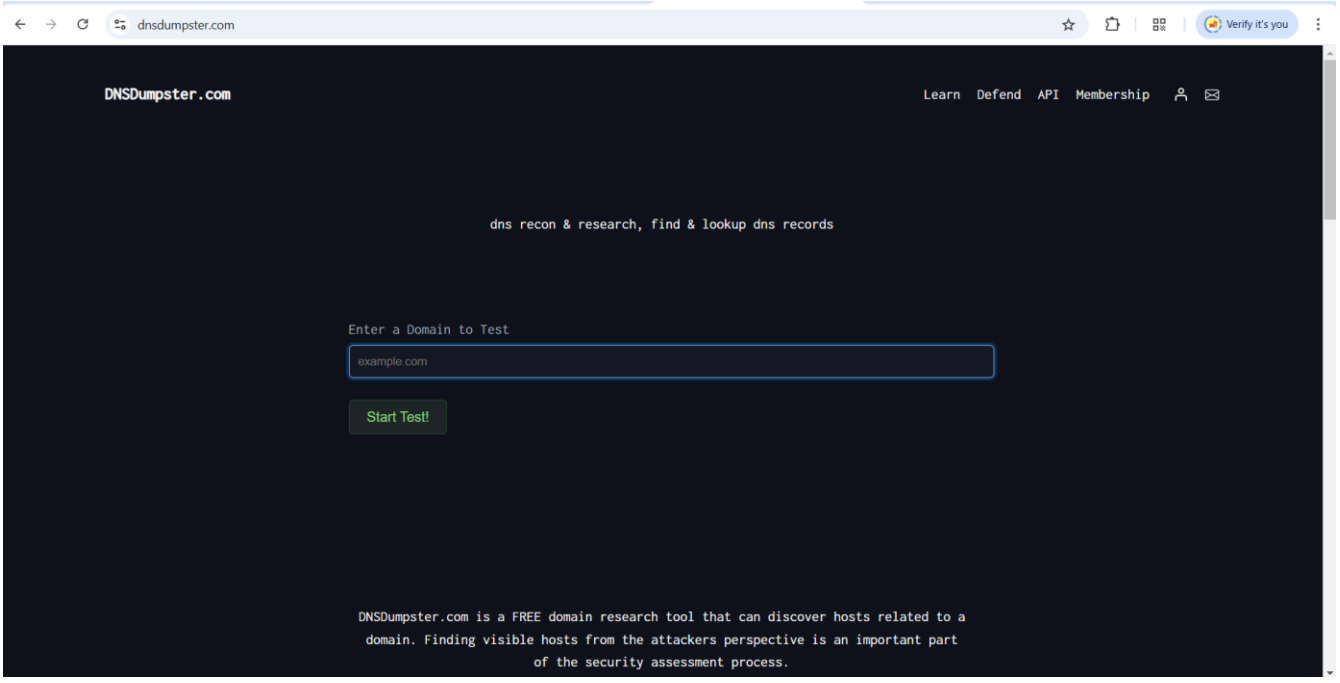


Figure 11:4th tool is DNSDumpster.com

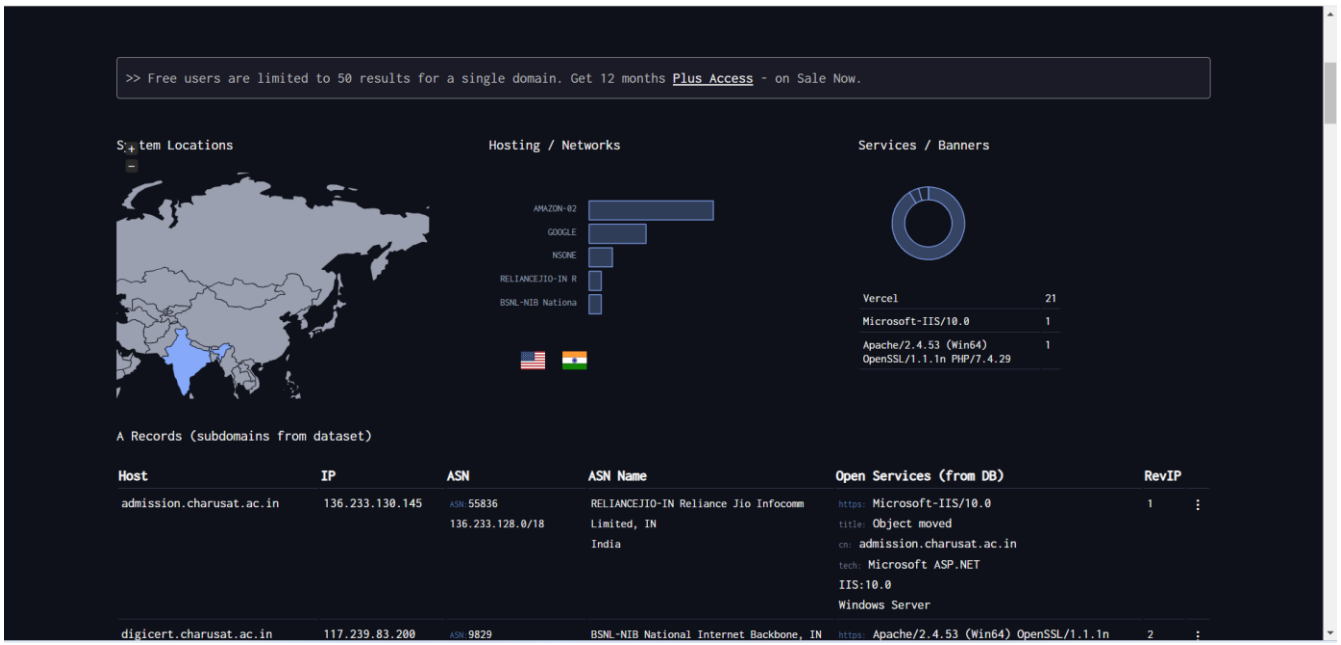


Figure 12:This is a result of dnsdumpster.com

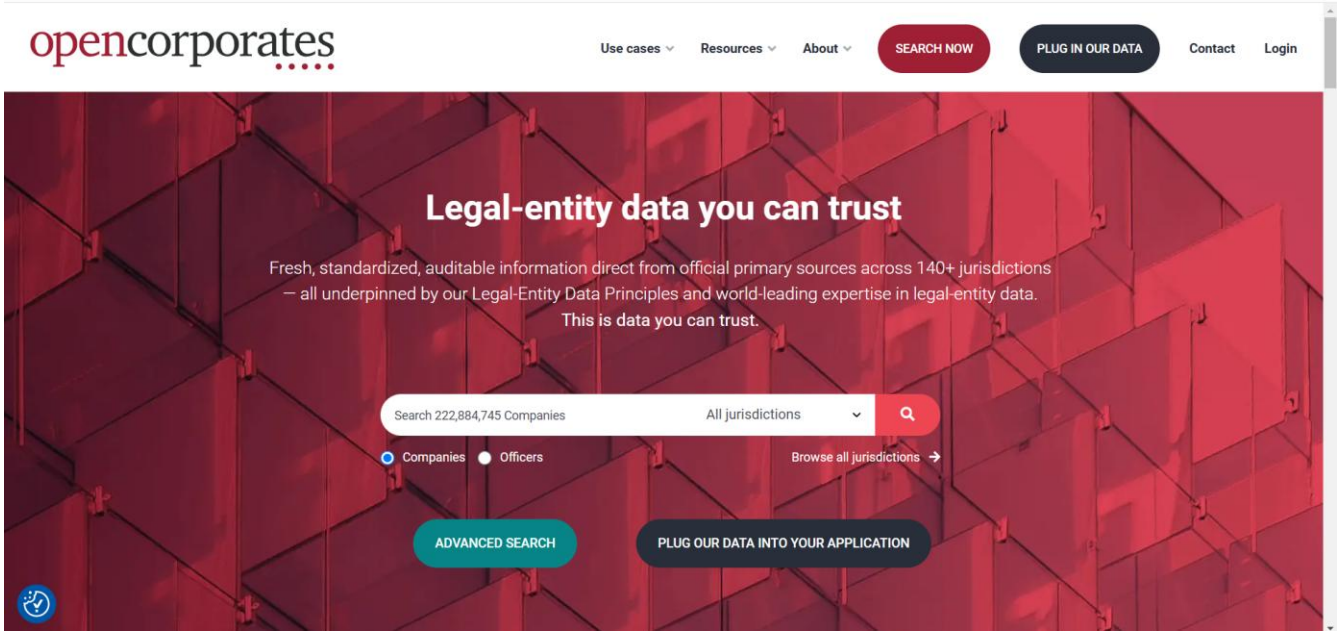


Figure 13:5th tool are opencorporates

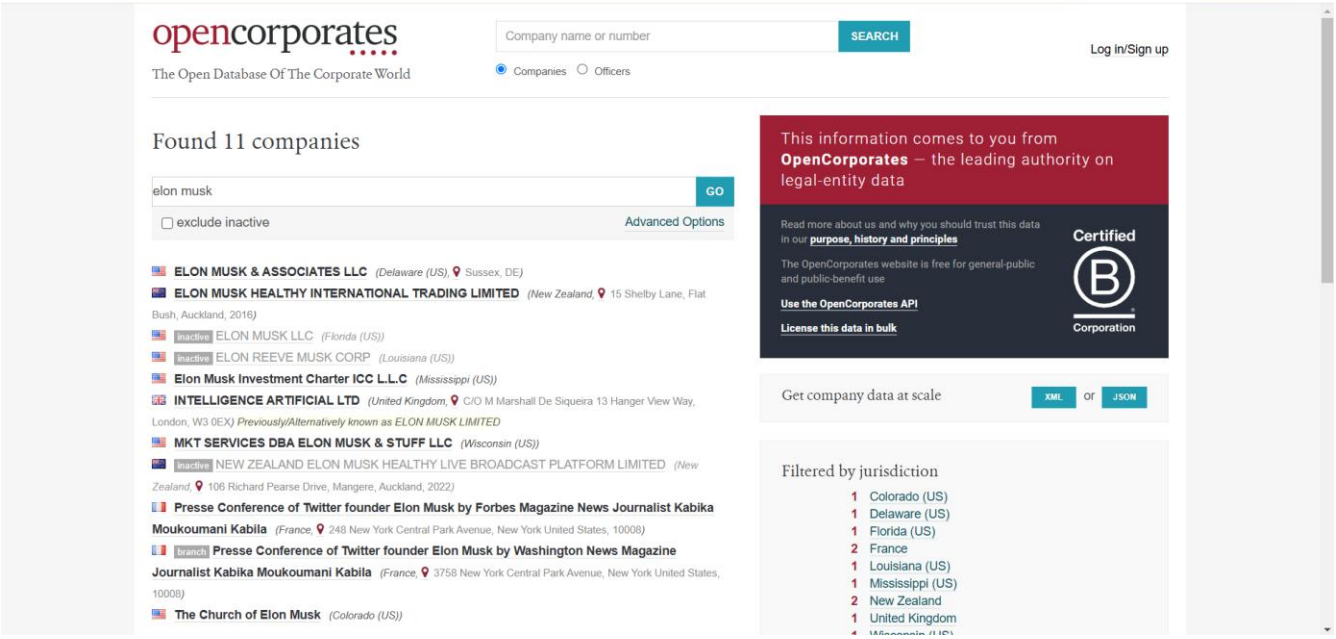


Figure 14:It will find 11 companies for Elon musk

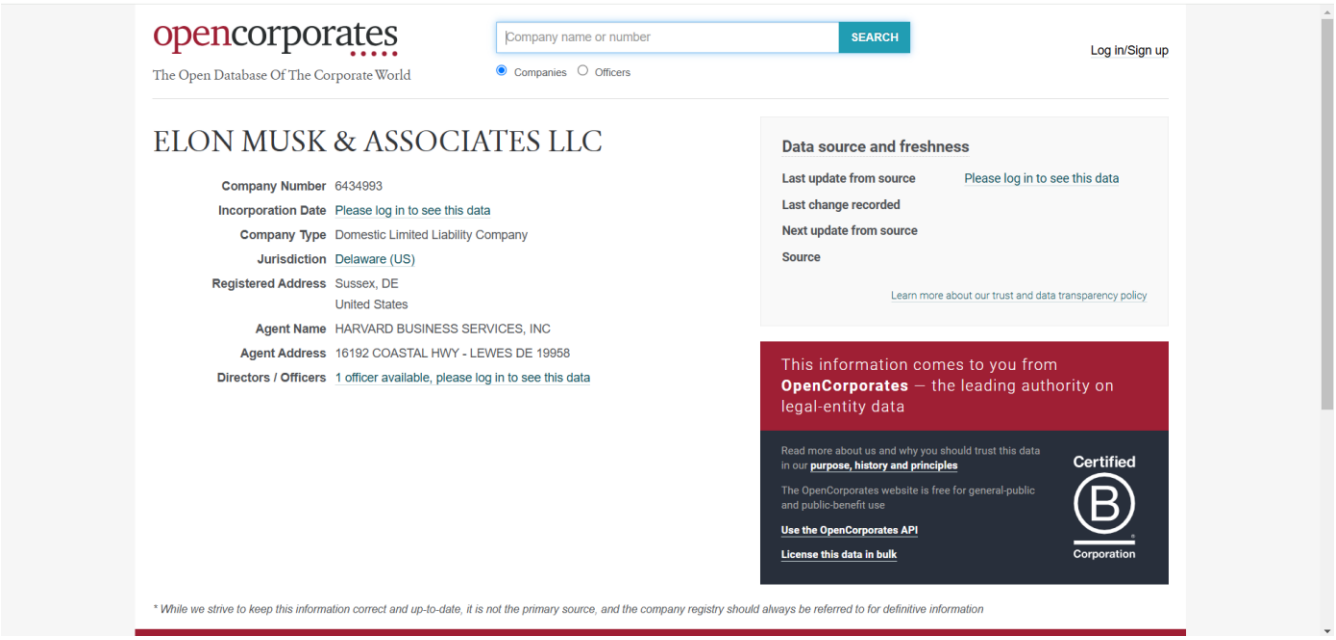


Figure 15:This is a details of Elon musk company

LATEST APPLICATIONS:

- Reconnaissance for Phishing Campaigns
- Cyber Threat Intelligence (CTI) Analysis
- Digital Forensics and Incident Response (DFIR)
- Website Threat Intelligence
- Vulnerability Discovery in Cloud Infrastructure
- Corporate Governance and Insider Threat Analysis
- Mergers and Acquisitions (M&A) Risk Assessment

LEARNING OUTCOME:

In this practical we learn about foot printing and reconnaissance using various OSINT frameworks tool

REFERENCES:

1. OSINT Framework: https://osintframework.com/
2. WhatsMyName: https://whatsmyname.app/
3. Urlscan.io: https://urlscan.io/
4. Wayback Machine: https://web.archive.org/
5. DNSDumpster: https://dnsdumpster.com/
6. opencorporates: https://opencorporates.com/