

****

**School of Computer Science**

**University of Petroleum & Energy Studies  
Bidholi, Via Prem Nagar, Dehradun, Uttarakhand  
November– 2024**

***Project Report***

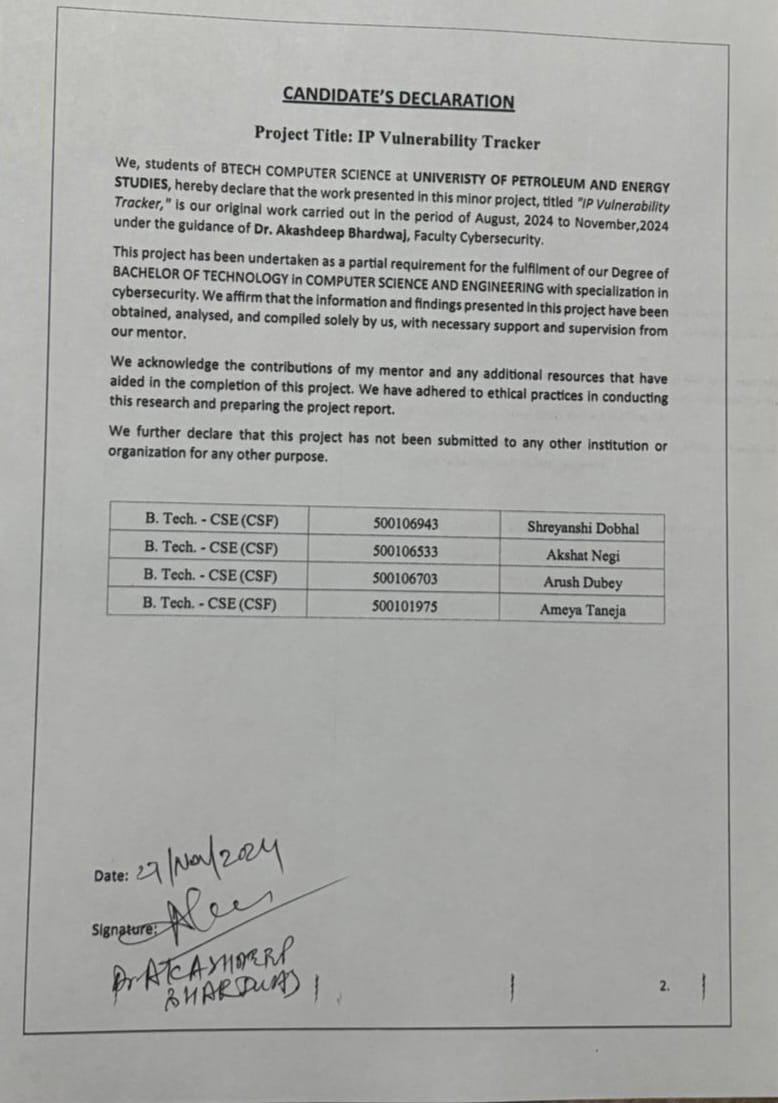
*submitted in fulfillment of the   
requirements for the award of the degree of*

**IP VULNERABILITY TRACKER**

***under the guidance of  
Dr. Akashdeep Bhardwaj***

|  |  |  |
| --- | --- | --- |
| **Specialization** | **SAP ID** | **Name** |
| B.Tech-CSE (CSF) | 500106943 | Shreyanshi Dobhal |
| B.Tech-CSE (CSF) | 500106533 | Akshat Negi |
| B.Tech-CSE(CSF) | 500106703 | Arush Dubey |
| B.Tech-CSE(CSF) | 500101975 | Ameya Taneja |

|  |  |  |
| --- | --- | --- |
| **TABLE OF CONTENTS** | | |
| Table of Contents | | 1. |
| Candidate Declaration | | 2. |
| Acknowledgment | | 3. |
| Abstract of the project | | 4. |
| Problem statement | | 4. |
| 1. | **Introduction** | 4. |
|  | 1.1 Purpose of the Project | 4. |
|  | 1.2 Target Beneficiary | 5. |
|  | 1.3 Project Scope | 5. |
|  | 1.4 References | 6. |
| 2. | **Project Description** | **7.** |
|  | 2.1 Problem statement | 7. |
|  | 2.2 SWOT Analysis | 7. |
|  | 2.3 Project Features | 8. |
| 3. | **System Design** | 8. |
|  | 3.1 Project Architecture | 8-11 |
|  | 3.2 Frontend Description | 11-18 |
|  | 3.3 Database Description | 18-19 |
| 4. | **Area of Application** | 20. |
| 5. | **Conclusion** | 21. |



### 

### ABSTRACT OF THE PROJECT

This report presents a comprehensive analysis of Internet Protocol (IP) data, focusing on detecting and mitigating security threats within a network. The project leverages advanced algorithms to identify and classify IP traffic anomalies, with the aim of enhancing network security. By analyzing sample IP data and employing a reference algorithm, the project aims to highlight vulnerabilities, mitigate risks, and improve overall network efficiency.

### PROBLEM STATEMENT

With the increasing reliance on IP networks, organizations are more vulnerable to cyberattacks targeting IP addresses, which can lead to data breaches and system compromises. Existing security tools often lack real-time monitoring or automated detection of IP vulnerabilities, leaving networks exposed.

The IP Vulnerability Tracker aims to address this gap by automating the detection of IP vulnerabilities, providing real-time alerts, and offering actionable remediation recommendations. This tool will help organizations identify and mitigate security risks in their IP infrastructure, enhancing overall network security.

### Introduction

With our growing hyper-connected world, our dependence on the Internet has increasingly grown, with innovation like e-commerce, fast communication. Each day, huge amounts of data travels through the globe. However, with this massive flow of personal and public data daily, there comes a very significant need to safeguard Data and Networks, from various Cyber Threats.

The growing dependence on the Internet and innovation have led to a significant need to safeguard data and networks from cyber threats. This project aims to analyse IP traffic data using advanced algorithms to identify potential security breaches. By combining real-time data analysis with automated threat response capabilities, the system provides a dependable defence against cyber-attacks. The project focuses on reliable and fast information about IP, enabling the scalability of large-scale networks. The goal is to deliver a comprehensive cybersecurity tool that provides comprehensive protection against cyber threats.

### Purpose of the Project

1. **Proactive Risk Management**: Identifying vulnerabilities in network devices, servers, or endpoints before attackers can exploit them.
2. **Compliance and Regulation**: Ensuring adherence to cybersecurity standards like GDPR, HIPAA, or PCI DSS by maintaining secure infrastructure.
3. **Real-time Monitoring**: Continuously scanning for new vulnerabilities or changes in the network that could introduce risks.
4. **Incident Response**: Assisting in the detection and mitigation of security incidents by pinpointing vulnerable IPs that may be exploited during attacks.
5. **System Hardening**: Providing actionable insights to improve the security posture by patching software, updating configurations, or removing outdated systems.
6. **Threat Intelligence Integration**: Leveraging vulnerability data to prioritize responses based on current threat landscapes.

### Target Beneficiary

* **Organizations:**
* Small, Medium, and **large** enterprises for network security.
* IT companies managing complex infrastructures.
* Financial institutions protecting sensitive customer data.
* **Cybersecurity Professionals:**
* Security analysts for vulnerability assessment.
* Penetration testers for identifying exploitable weaknesses.
* Incident response teams for mitigating risks quickly.
* **Government and Public Sector:**
* Agencies ensuring critical infrastructure security.
* Regulatory bodies monitoring compliance with security standards.

### Project scope

* **Objective:**
* To identify, monitor, and address vulnerabilities associated with devices, systems, and services linked to specific IP addresses.
* **Features:**
* Automated IP scanning for vulnerabilities.
* Detection of open ports, DNS, geographical location, SSL certificate check.
* Generation of detailed vulnerability reports.
* **Functional Scope:**
* Input: Single IP for scanning.
* Output: Risk assessments and detailed vulnerability reports.
* **Target Audience:**
* Network administrators, IT security teams, small and medium businesses, and cybersecurity enthusiasts.
* **Boundaries:**
* Focused only on IP-based vulnerabilities (no deep application-level analysis).
* Excludes exploit testing or advanced penetration testing.
* **Technical Scope:**
* Web-based dashboard or command-line interface for results visualization.
* Potential integration with APIs for extensibility.

### References

* 1. Lissy93 (2023). *GitHub - Lissy93/web-check: 🕵️‍♂️ All-in-one OSINT tool for analysing any website*. [online] GitHub. Available at: https://github.com/Lissy93/web-check [Accessed 27 Nov. 2024].
  2. ‌Kaushik, S., Bhutto, A. and Pandey, B. (2019). Efficient Information Gathering using NMAP and NBTSCAN: Case study on 172.19.19.0 IP Address. *Indian Journal of Science and Technology*, 12(28), pp.1–13. doi:https://doi.org/10.17485/ijst/2019/v12i28/147004.
  3. Barman, F., Alkaabi, N., Almenhali, H., Alshedi, M., & Ikuesan, R. (2023). A Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle. European Conference on Cyber Warfare and Security, 22(1), 54–64https:/doi.org/10.34190/eccws.22.1.1438
  4. Vugrin, E. D, et al. (2020). Cyber threat modeling and validation: Port Scanning and Detection https://doi.org/10.1145/3384217.3385626
  5. Sivasangari, A., B, P., M, K., Ajitha, P., Gomathi, R., & Vignesh, N. (2023). Dart | Data Analysis For Red Teamers. https://doi.org/10.1109/ictbig59752.2023.10456020

### PROJECT DESCRIPTION

* 1. **Problem statement**

Traditional IP analysis tools are severely limited in their capacity to identify and mitigate security threats in real time due to the complexity and size of modern networks. Due to these flaws, networks may be compromised and breaches may occur. Cybercriminals may take advantage of these vulnerabilities. This project is focused on creating a sophisticated IP vulnerability tracker framework in order to address this important problem. In order to provide a dependable and scalable defense against the ever-changing landscape of cyber risks, the system is built to provide accurate, real-time detection and response to security threats.

* 1. **SWOT Analysis**
* **Strengths**
* Real-Time Threat Detection: The system's ability to analyse IP traffic as it happens provides a powerful defence mechanism, allowing immediate identification and response to potential security threats. This real-time capability ensures that malicious activities, such as DDoS attacks or unauthorized access attempts, are detected and mitigated before they can cause significant damage.
* Scalability: Designed to handle vast amounts of data, vulnerability tracker system is highly scalable, making it suitable for large, complex networks with millions of IP connections. This adaptability ensures that the system remains effective as network demands grow, from small businesses to global enterprises.
* **Weaknesses**
* Resource-Intensive Processing: The computational demands of real-time IP traffic analysis, especially in large-scale networks, can be significant. This may require substantial investment in hardware and computational resources, potentially limiting its accessibility to organizations with smaller IT budgets.
* **Opportunities**
* Integration with Existing Security Infrastructures: The Vulnerability tracker system can be seamlessly integrated with other security tools like Geolocation. This integration offers a holistic approach to threat management, combining real-time detection with broader incident response capabilities.
* Customization for Industry-Specific Needs: The system can be tailored to meet the unique security requirements of different industries, such as finance, healthcare, and government. By customizing detection algorithms and thresholds, the system can provide targeted protection against industry-specific threats, increasing its value and relevance.
* **Threats**
* Evolving Cyber Threat Landscape: The constantly changing nature of cyber threats poses a challenge to the effectiveness of this vulnerability tracker system. New attack techniques and vulnerabilities may emerge that the current algorithms and data models are not equipped to handle, necessitating continuous updates and adaptations.
* Data Privacy and Regulatory Compliance: Handling and analysing IP data, especially in regions with strict data protection laws, introduces potential privacy concerns. Ensuring compliance with regulations and other privacy frameworks is crucial to avoid legal repercussions and maintain user trust.
  1. **Project Features**

Key features include:

* IP Scanning and discovery
* Vulnerability detection
* Real time detection

### SYSTEM DESIGN

The system is designed to be both robust and adaptable, using a combination of APIs and a central database to gather and analyse detailed information about websites. This approach enables us to provide insights into various aspects, such as IP details, SSL chains, DNS records, and server configurations.

One of the key components of the system is its comprehensive dashboard, which serves as the main interface for users. The dashboard is structured to present the analysed data clearly and accessibly, giving a thorough overview of a website’s security status. Users can track a variety of important metrics, including IP information, SSL chain integrity, DNS records, and open port status. Additionally, it offers insights into site performance, security settings, and potential vulnerabilities, making it a practical tool for both technical teams and decision-makers.

* 1. **Project Architecture**

The Vulnerability Tracker project architecture is designed to deliver comprehensive insights into website security and performance by integrating multiple scanning tools and APIs. The system is built with a modular approach, ensuring scalability, reliability, and ease of integration with various external services.

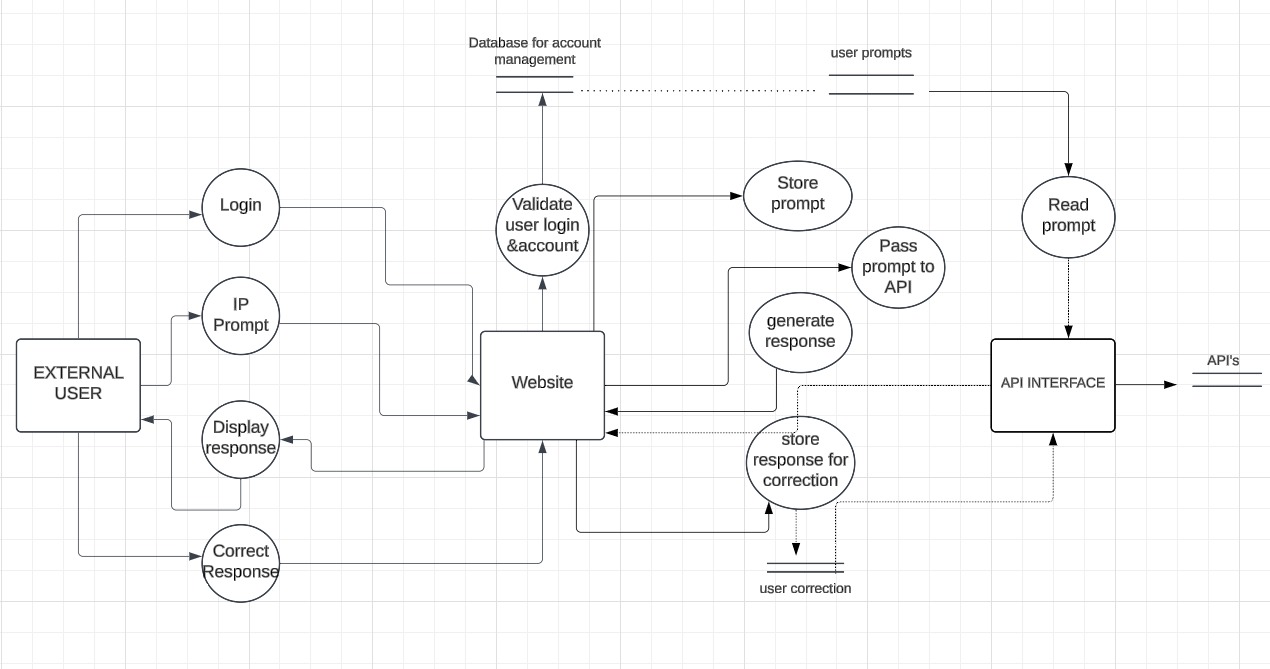
### System Overview

The system architecture consists of several key components:

* + **Frontend (ReactJS):** The user interface is built with React, providing an interactive dashboard where users can view detailed insights about a website. This includes sections for IP information, SSL chain, DNS records, server location, open ports, and more.
  + **Backend (Node.js/Express):** The backend serves API requests from the frontend, processes data, and interacts with the database. It also handles communication with external APIs for additional data retrieval and analysis.
  + **Database (MongoDB):** All collected data is stored in a MongoDB database. This includes historical data on IPs, DNS records, SSL certificates, and more, enabling the system to perform trend analysis and provide historical insights.
  + **External APIs:**
    - Shodan API: This API provides information on associated Ports and Vulnerabilities for a given domain, which is crucial for identifying potential security risks.
    - WhoAPI: Offers comprehensive Whois records, providing detailed domain information that supports the identification of potential vulnerabilities.
    - Rapid API: This API provides information on associated hostnames, DNS Information for a given domain, which is crucial for identifying potential security risks.
  + **Scanning Modules:** The system includes various scanning modules that perform specific checks and analyses:
    - IP Information: Retrieves and analyses the IP address data of a given website.
    - SSL Chain: Examines SSL certificates to ensure they are valid and properly configured.
    - DNS Records: Collects and analyses DNS records, including TXT and A records, to ensure proper configuration and security.
    - Open Ports: Scans for open ports on the server, which could be potential entry points for attackers.
    - HTTP Security Features: Analyses HTTP headers and other configurations to assess the website’s security posture.
    - Site Performance and Carbon Footprint: Measures the website's performance metrics and evaluates its environmental impact based on energy consumption.

### Data Flow

* + **Data Collection:** The frontend sends a request to the backend to analyse a specific website. The backend orchestrates the scanning process by invoking the relevant scanning modules and external APIs.
  + **Data Processing:** The results from the scanning modules and external APIs are processed and stored in the database. The backend also performs additional analysis, such as identifying trends or anomalies in the data.
  + **Data Presentation:** The processed data is sent back to the frontend, where it is displayed on the dashboard. Users can view detailed information about the website’s security, performance, and environmental impact.



### API Configuration

To enhance the system’s capabilities, the following environmental variables can be configured:

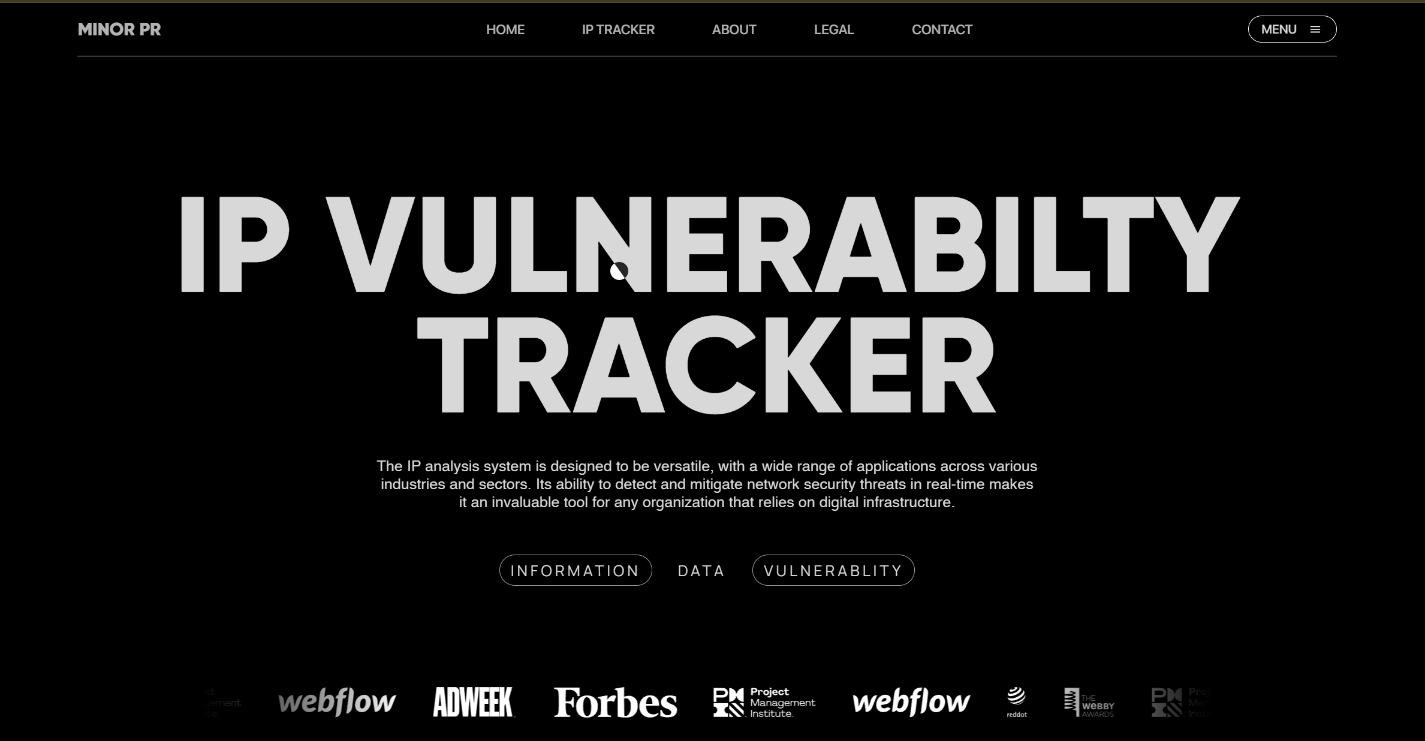
* + **Rapid\_API\_KEY:** For accessing website’s DNS metrics.
  + **SHODAN\_API\_KEY:** To retrieve associated hostnames via Shodan.
  + **WHO\_API\_KEY:** For obtaining comprehensive Whois records.

Additional configuration settings include port assignments, API rate-limiting, CORS policies, and timeout limits, which ensure the system operates smoothly and securely in various environments.

* 1. **Frontend description**
* Developed the frontend page.
* Used modern frontend framework i.e. React to handle dynamic routing.
* Below are the typical routes and their purposes:

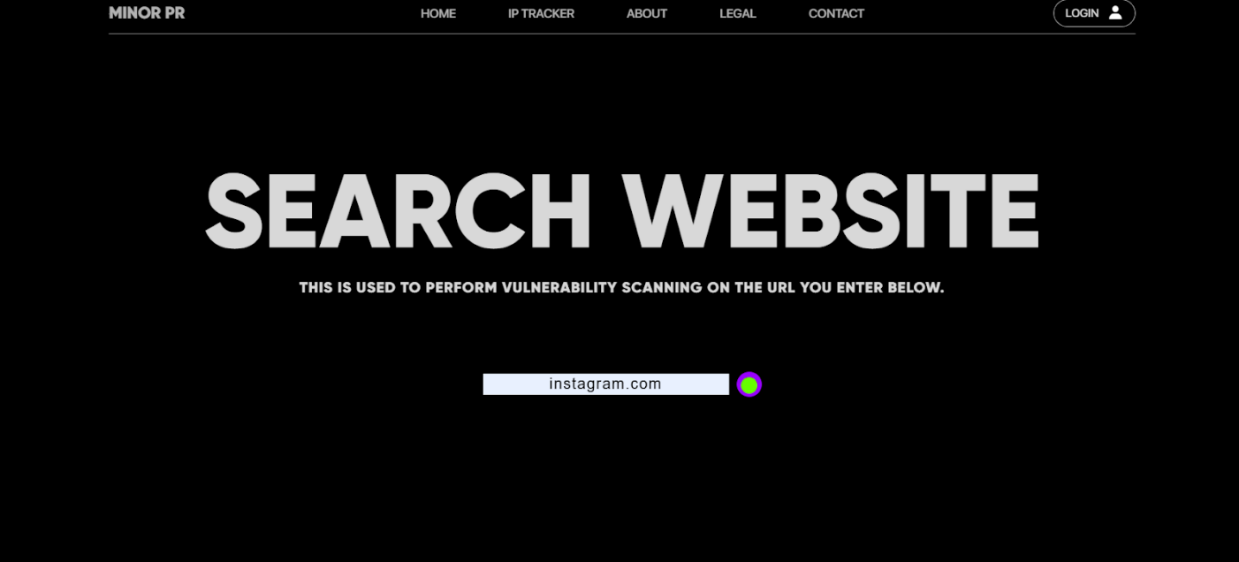
1. Home

* Purpose: Provides an introduction to your tool, highlights its features, and explains how it works.
* Requirements:
* Short description of the tool and its purpose.

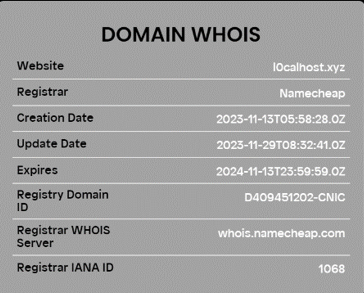


1. IP Tracker

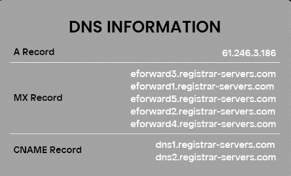
* Purpose: The core functionality page for checking vulnerabilities.
* Requirements:
  + Input field(s) for IP address or domain.
  + Results display section for identified vulnerabilities.
  + Integrated multiple APIs to track the vulnerability.



* APIs used:
  + **Domain WHOIS:** used to retrieve information such as the domain's registrar, registration date, expiration date, domain owner (if not private), contact information, and more.

****

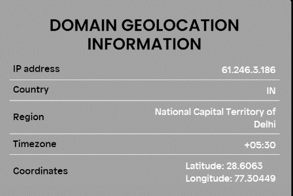
* + **DNS information:** refers to details about how a domain is set up and resolved across the internet. Key DNS records include:
    - A Record: Maps a domain to an IPv4 address.
    - CNAME Record: Aliases one domain name to another
    - MX Record: Specifies mail servers responsible for email delivery.



* + **SSL Certificate:** SSL certificate information provides details about a domain's connection.
    - Certificate Issuer: The authority (e.g., Let's Encrypt, DigiCert) that issued the SSL certificate.
    - Domain Name: The domain for which the SSL certificate was issued.
    - Public Key: Used for encrypting data sent to the server.
    - Validity Period: The start and end dates of the certificate's validity.
    - Encryption Algorithm: The encryption standard used (e.g., RSA, ECC).

****

* + **Domain geolocation information:** refers to the geographical location of the IP address associated with a domain. It includes:
    - Country: The country where the domain's server is hosted.
    - City: The city of the server’s location.
    - Region: The broader region or state where the server is located.
    - Latitude and Longitude: The coordinates pinpointing the server's physical location.
    - ISP (Internet Service Provider): The company providing internet services for the domain’s server.
    - Time-zone: The local time zone of the server.

****

* + **Port information:** refers to the communication endpoints used by network protocols to route data between devices. Key details include:
    - Port Number: A numerical identifier (0-65535) that specifies the type of service or protocol.

****

* + **Website vulnerabilities:** This card provide you weaknesses or flaws in the design, implementation, or configuration of a website that could be exploited by attackers to compromise the site’s security, functionality, or data.

****

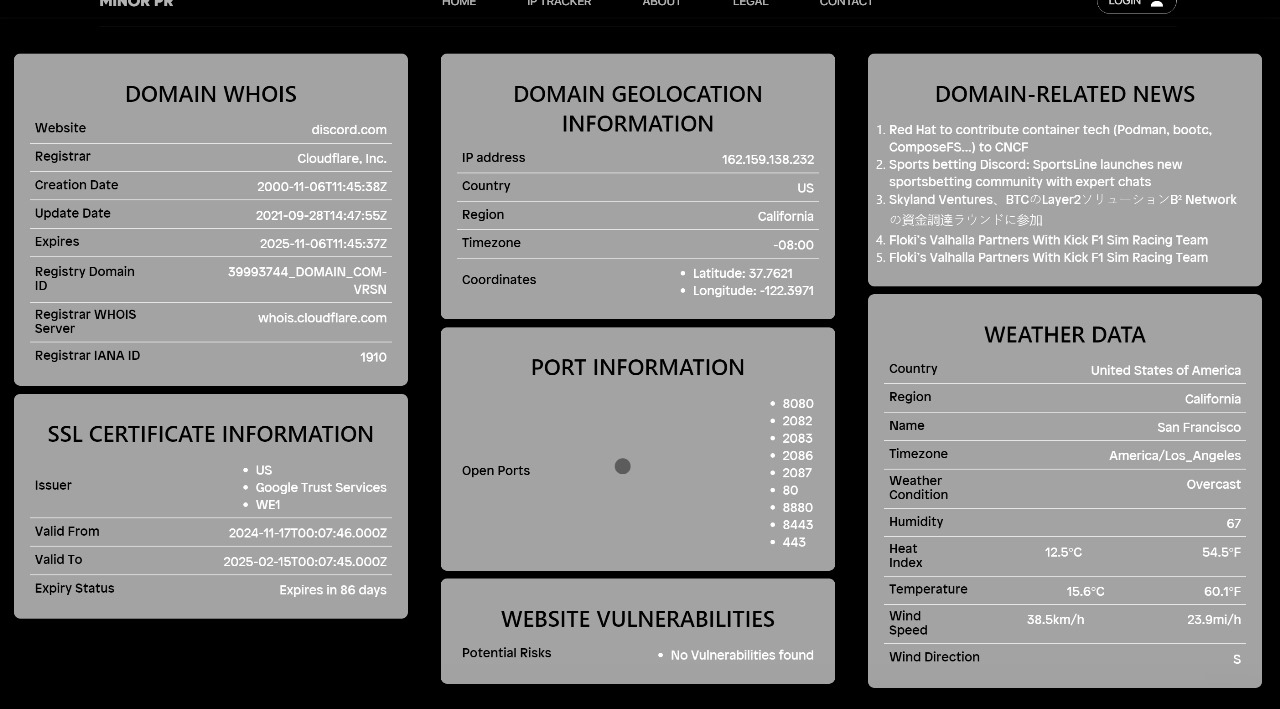
* + **Domain related news:** This card provide you weaknesses or flaws in the design, implementation, or configuration of a website that could be exploited by attackers to compromise the site’s security.



* + **Weather Information:** refers to data and forecasts related to atmospheric conditions at a specific location and time of the specific place.

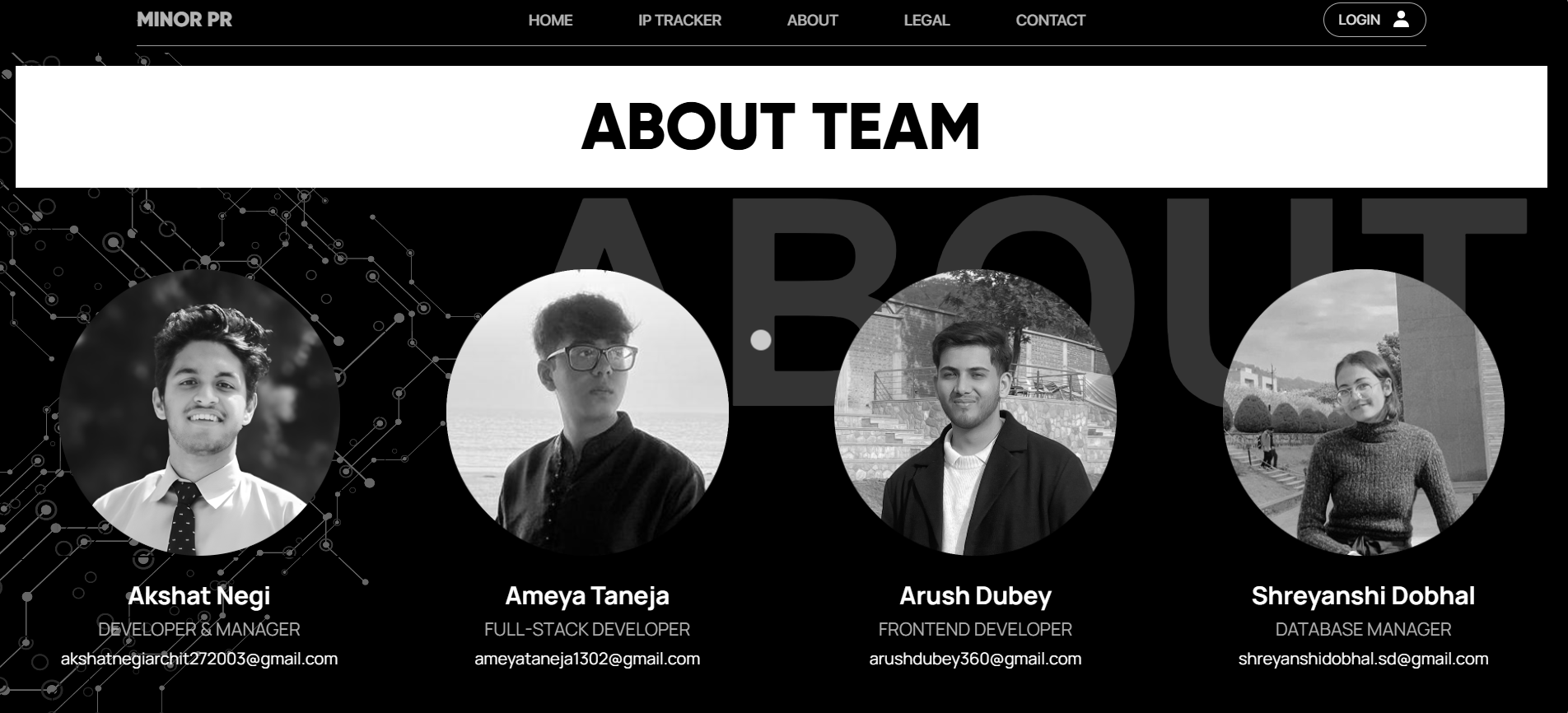


* + **Combined APIs are:**Following are the cards that are visible in combined if any url is scanned.



1. About

* Purpose: Provide information about our team.
* Requirements:
  + Content about team members and their work.
  + Option to contact or connect via LinkedIn.



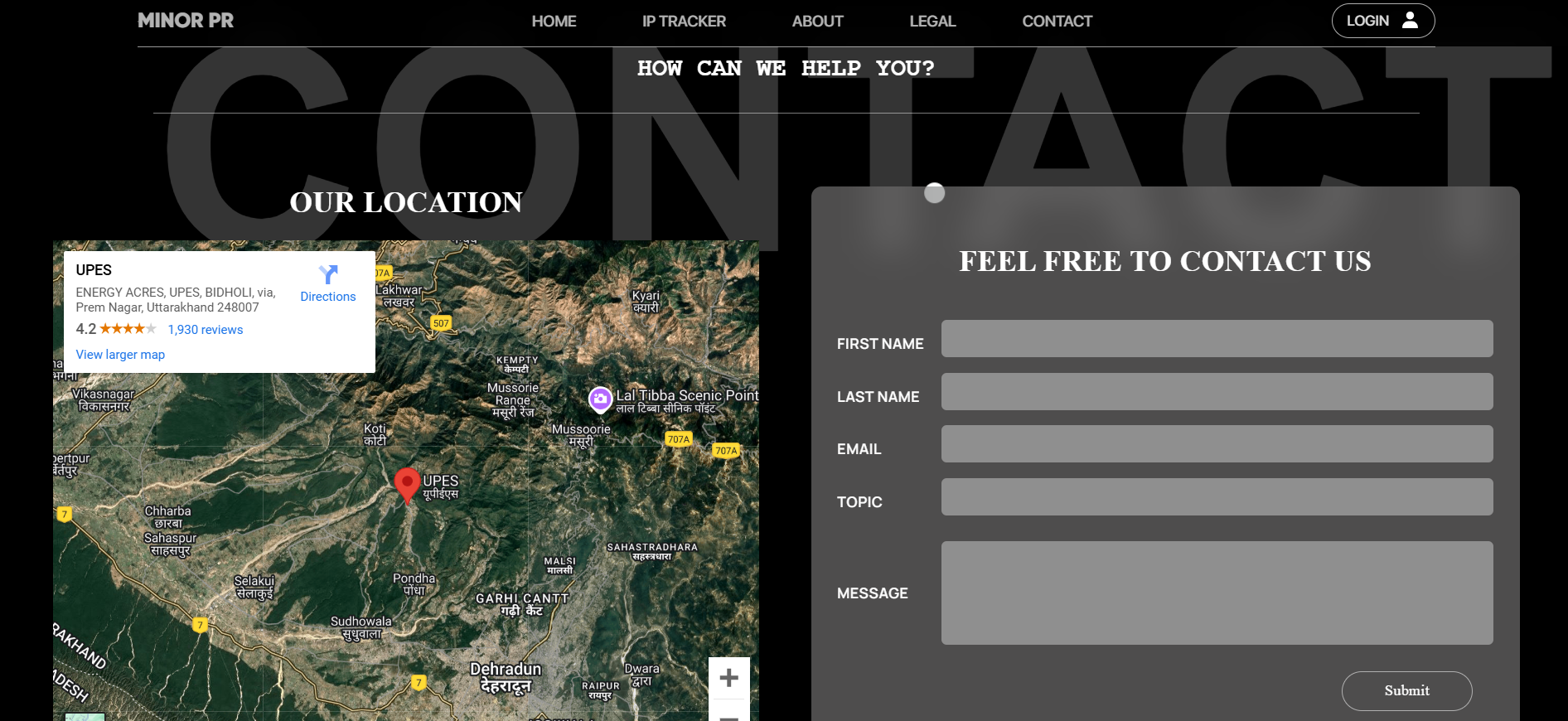
1. Legal

* Purpose: Display legal information about the service.
  + Privacy Policy
  + Interpretation and Definitions
  + Collecting and using your personal data.
  + Child privacy
  + Changes to privacy policy.
* Requirements:
  + Ensure proper formatting with collapsible sections for ease of reading.
  + Include links to these pages in the footer.



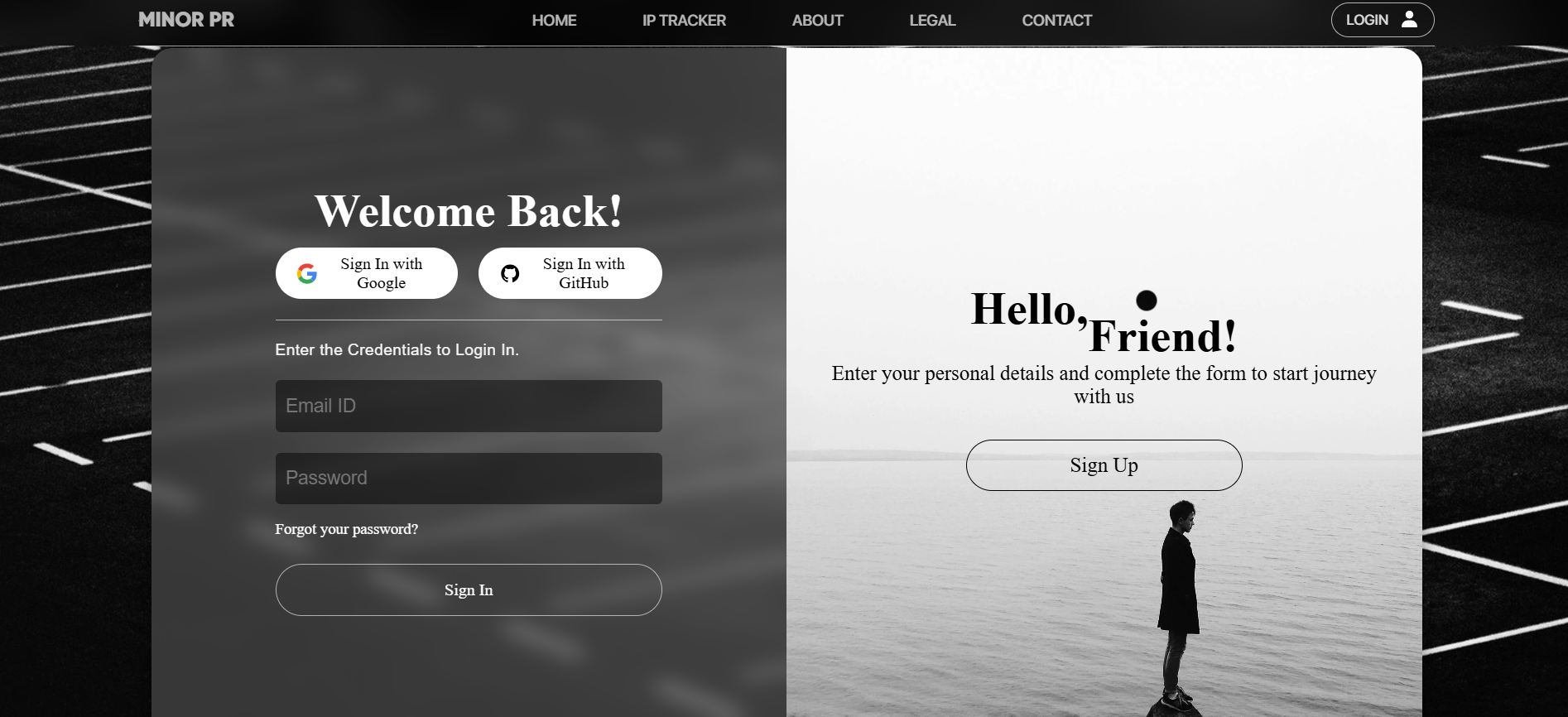
1. Contact

* Purpose: Allow users to reach out for support, feedback, or inquiries.
* Requirements:
  + Page layout that ensures responsiveness for different devices.
  + Contact form which includes name, email address, topic and message the user want to send.
  + After Form submission, the data is sent to our team member.
  + Embed a map for the official physical address of the team.



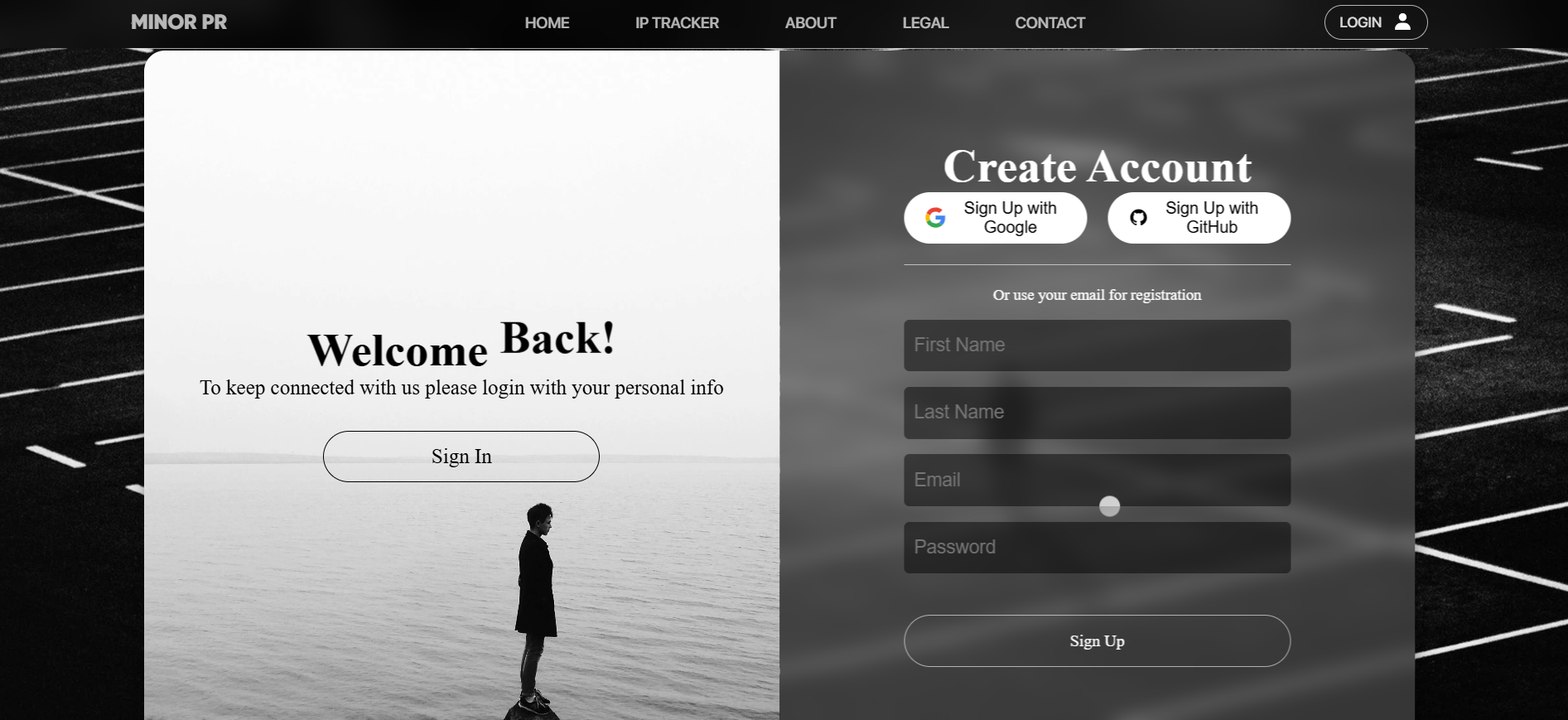
1. Login

* Purpose: Allow users to authenticate and access protected features of the application.
* Requirements:
  + Login form which includes email (text input) and password (password input).
  + Hide the toggle password.
  + Provide a link to the registration page.



1. Sign up

* Purpose: Allow new users to create a new account and access protected features of the application.
* Requirements:
  + Signup form which includes username (text input), email (text input) and password (password input).
  + Hide the toggle password.
  + Provide a link to the login page for the existing users.



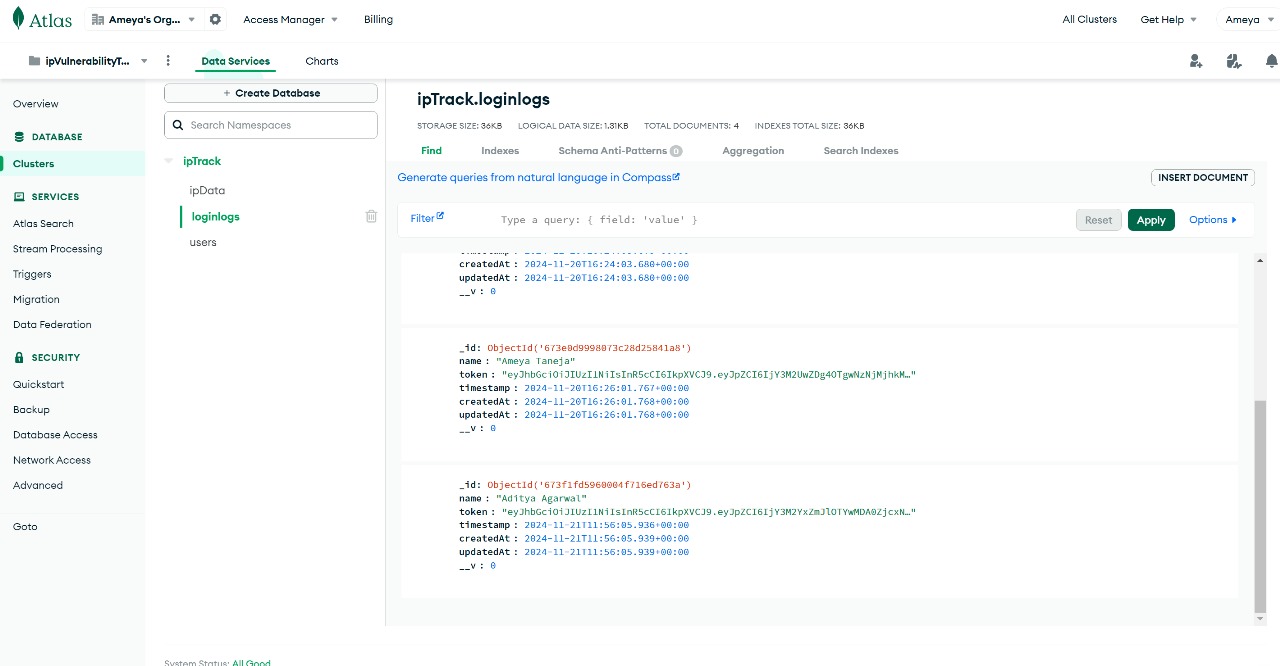
* 1. **Database description**

The database is a critical component of an IP Vulnerability Tracker, used to store and manage all relevant data securely and efficiently. Here's a detailed description:

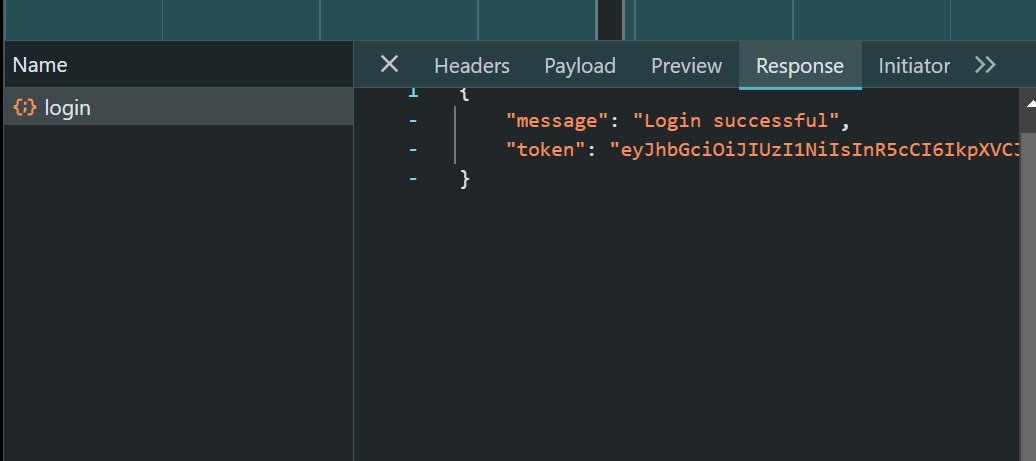
* **Purpose**
* The database serves to:
* Store scan results, vulnerability details, and metadata.
* Maintain user accounts, roles, and preferences.
* Provide historical data for trends, reporting, and audits.
* **Database Used**
* MongoDB Database
* Suitable for unstructured or semi-structured data, like raw scan outputs or logs.
* **Login logs**

Login logs are used for many purposes that are:

* Audit and Compliance
* User behaviour analysis
* Incident response
* Performance metrices.
* Security Monitoring



Respective response that is generated is:



* **Sign in logs**

Sign in logs record every instance a user attempts to access their account, providing critical insights into system usage, security, and user behavior.

The key purpose for sign in logs is:

* Security and Threat detection
* System performance
* Incident investigation



### AREA OF APPLICATION

The area of application refers to the scope or domain where a particular tool, technology, concept, or methodology is used to address specific challenges, provide solutions, or achieve desired outcomes. Here are some examples of the areas of application in various fields:

* Digital Forensics
  + - Cybersecurity: Investigating cyberattacks, malware, and unauthorized access incidents.
    - Law Enforcement: Analysing digital evidence for criminal investigations.
    - Corporate Security: Detecting and preventing insider threats or intellectual property theft.
    - Litigation Support: Providing evidence in legal disputes and e-discovery.
* Web Application Development
  + - E-Commerce: Building online stores and payment platforms.
    - Social Networking: Creating interactive platforms for user engagement.
    - IP Vulnerability Tracking: Monitoring network vulnerabilities to enhance security (your project).
    - Healthcare: Developing patient management or telemedicine solutions.
* Machine Learning and AI
  + - Healthcare: Diagnostics, treatment predictions, and drug discovery.
    - Finance: Fraud detection and risk analysis.
    - Retail: Personalized recommendations and demand forecasting.
    - Transportation: Autonomous vehicles and traffic management.

### CONCLUSION

The IP Vulnerability Tracker effectively integrates advanced scanning modules and APIs to deliver detailed insights into network security. By identifying vulnerabilities such as open ports, DNS misconfigurations, and SSL certificate issues, the system empowers organizations to address potential threats proactively. The inclusion of real-time monitoring and actionable reporting ensures a robust defence against evolving cyber risks. This project serves as a comprehensive tool for enhancing network security, paving the way for future advancements in automated vulnerability detection and mitigation.

* INPUT FORMAT
* To utilize the application’s scanning features effectively, users must define the domain name as the primary input. This domain name serves as the focal point for the tool’s analysis, enabling a comprehensive evaluation of its associated digital elements.