**MALICIOUS IP DETECTION**

Name: Vemuri Sai Soumya

Date: 01-09-2025

Github Repository: <https://github.com/Soumyaa2005/CyberSecurity-Project>

**MALICIOUS IP DETECTION - REPORT**

**ABSTRACT**

Malicious IPs are a significant threat to cybersecurity as they are often linked with spam, phishing, botnets, and other abusive activities. This project aims to detect and classify IP addresses as Safe or Malicious using the AbuseIPDB threat intelligence API. A Colab-based solution was developed to query IPs individually or in bulk through CSV uploads, evaluate their abuse confidence scores, and provide results in a user-friendly, color-coded output. The system also supports exporting results to CSV for audit purposes. This project demonstrates how cybersecurity APIs can be integrated with Python to provide a practical, lightweight, and accessible IP reputation monitoring tool.

# APPROACH

1. **Problem Definition:** Detect whether an IP address is Safe or Malicious using AbuseIPDB.
2. **Data Source:** AbuseIPDB API, providing real-time abuseConfidenceScore for queried IP addresses.
3. **Implementation:**

* **Single IP Check:** Users can input one IP and receive a status report.
* **Bulk IP Check:** Users can upload a CSV file with an 'IP' column or paste multiple Ips.
* **Threat Scoring:** IPs with abuseConfidenceScore > 50 are labeled 'Malicious'; otherwise, 'Safe'.
* **Output:** Results displayed in a color-coded table in Colab and stored in a history DataFrame.
* **Export:** History exported as CSV for further review or reporting.

# RESULTS

The system successfully classified both Safe and Malicious IPs using AbuseIPDB API results.

**Sample test results:**

8.8.8.8 → Safe

185.62.189.27 → Malicious

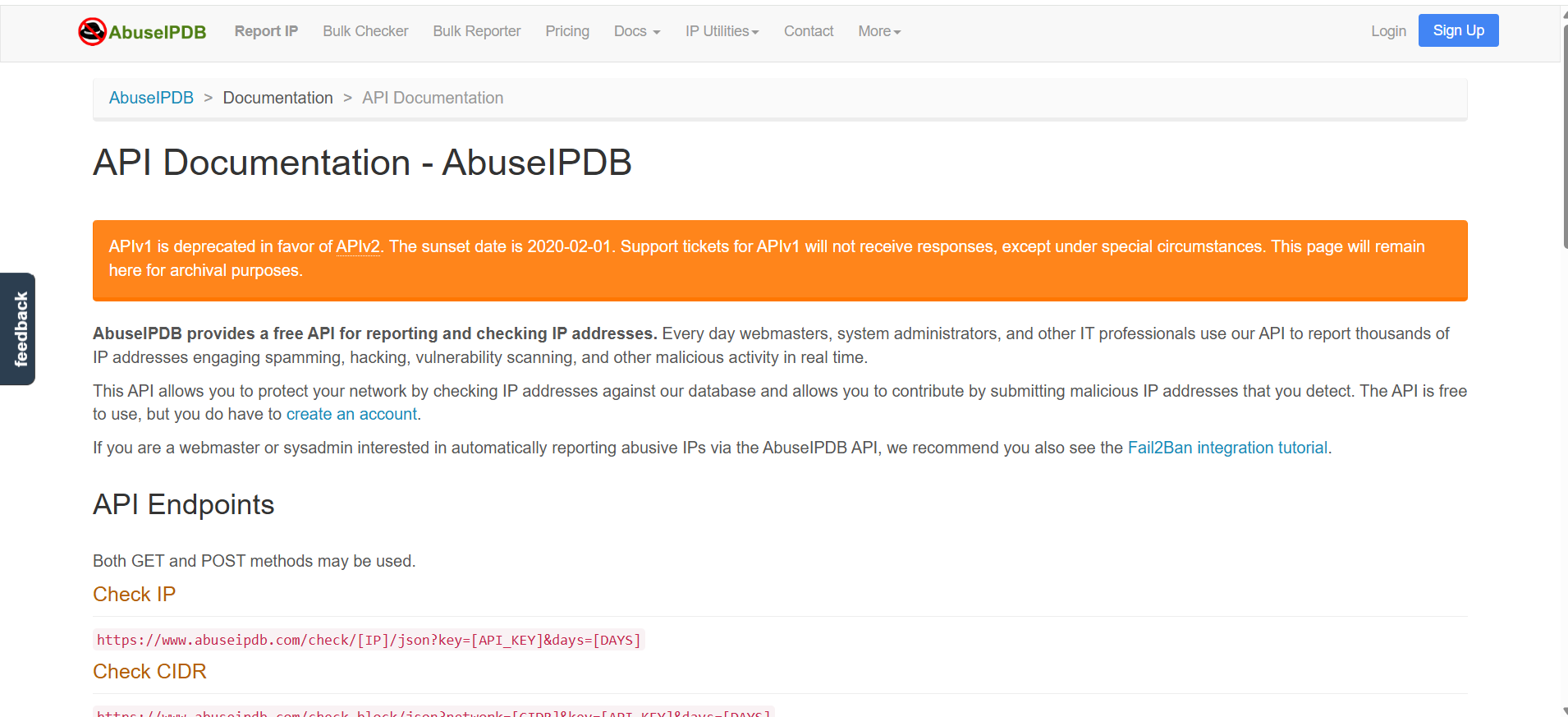
**Features:**

- Real-time API-based detection.  
- Color-coded table output (green = Safe, red = Malicious).  
- Support for interactive input and CSV batch uploads.  
- Exportable history for documentation.

**CASE 1:**  
Shows 'Malicious' because the IP has high abuse confidence score in AbuseIPDB.

**CASE 2:**  
Shows 'Safe' because the IP has not been flagged or has a low abuse confidence score.

**The Cybersecurity tool explored:** AbuseIPDB



The data source was the AbuseIPDB official API, providing abuse reports and scores.

# CONCLUSION

This project demonstrated the practical use of AbuseIPDB in detecting and monitoring malicious IP addresses. By combining Python automation in Colab with AbuseIPDB’s API, the solution achieved effective results in evaluating IP reputation. The system provides quick, reliable classification, supports CSV batch processing, and generates exportable history logs. This makes it a valuable cybersecurity utility for analysts, students, and professionals seeking lightweight tools for network monitoring and threat detection.