**Cyber Threat Intelligence Dashboard**

**1. Introduction**

The *Cyber Threat Intelligence Dashboard* is a simple Flask-based web application designed to help cybersecurity analysts and learners perform threat intelligence analysis. It accepts an IP address or domain as input, queries open-source threat intelligence APIs—**VirusTotal** and AbuseIPDB—and presents the results in a readable format.

**2. Objective**

The main goal of the project is to provide a lightweight and easy-to-use tool to:

* Analyze IOCs (Indicators of Compromise).
* Retrieve threat statistics like malicious, suspicious, and harmless verdicts.
* View abuse confidence scores for IPs.
* Store and search IOC records locally.

**3. Tools & Technologies**

* **Language**: Python
* **Framework**: Flask
* **Frontend**: HTML (Jinja2 Templates)
* **APIs**:
  + VirusTotal
  + AbuseIPDB
* **Storage**: CSV file (threat\_data.csv)

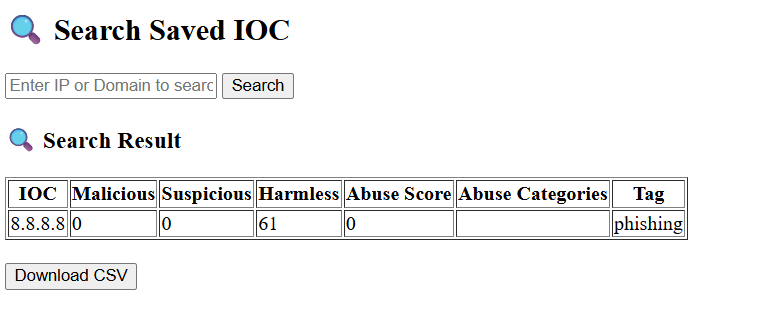
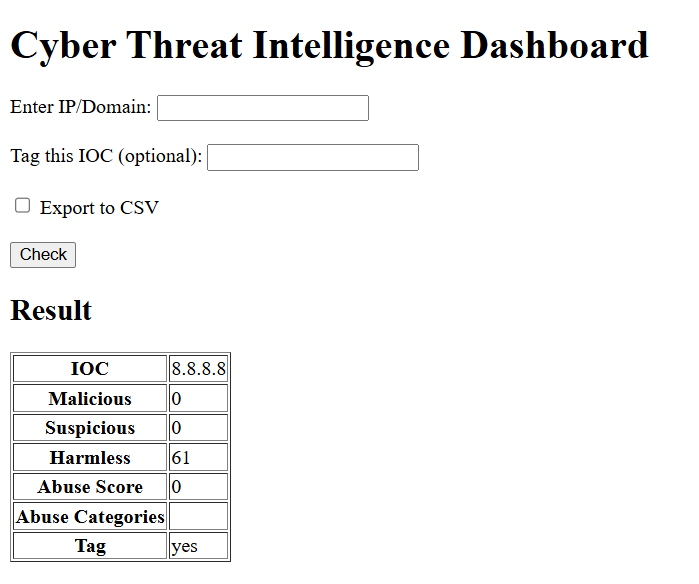
**4. Functionalities**

* IOC input field (IP or domain).
* Optional IOC tagging.
* Fetch and display:
  + Malicious / Suspicious / Harmless status (from VirusTotal).
  + Abuse Confidence Score and Categories (from AbuseIPDB).
* Export results to CSV.
* Search previously saved IOCs.

**How it Works (Backend)**

1. **User Input:** IOC entered via the web form.
2. **VirusTotal API:** Checks reputation & statistics of the IP/domain.
3. **AbuseIPDB API:** Provides abuse score for IPs only.
4. **Display:** Results shown on the same page.
5. **Export:** User can save the results with optional tagging.
6. **Search:** A stored IOC can be retrieved from the CSV file.

**Screenshot Suggestions (Include These in Your Report)**

S**creenshot 1** – Full Dashboard UI,**Screenshot 2** – Search Feature:  
  


Submitted By : Suhaila P.S