An Advanced Security Framework for Active and Passive Reconnaissance - Setup & Run Guide

System Requirements

- - Operating System: Linux, macOS, or Windows
- - Python Version: Python 3.7 or higher
- - RAM: At least 2 GB
- - Internet Access: Required for external enumeration & scanning

Install Python & pip

- On Linux/macOS:
  sudo apt update
  sudo apt install python3 python3-pip -y
- On Windows:
  Download Python from https://www.python.org/downloads/
  Ensure 'Add Python to PATH' is checked during install

Project Directory Structure

- project/
  ├── app.py
  ├── wordlists/
  │ └── common.txt
  ├── templates/
  │ ├── index.html
  │ ├── sql_attack.html
  │ ├── xss_attack.html
  │ ├── subdomain.html
  │ ├── url_grabber.html
  │ ├── testing.html
  │ ├── directory_traversal.html
  │ └── all_type_attack.html
  └── static/

Install Required Python Packages

- pip install flask aiohttp aiofiles beautifulsoup4 dnspython validators requests
- Optional (to disable SSL warnings):
  pip install urllib3
- Add to app.py:
  import urllib3
  urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

Run the Flask Application

- In the project folder:
  python app.py

Access the Web Interface

- Open browser and go to: http://127.0.0.1:5000/

Available Features & Routes

- / – Home
- /sql_attack – SQL Injection Scanner
- /xss_attack – XSS Scanner
- /directory_traversal – Directory Traversal
- /subdomain – Subdomain Enumerator
- /url_grabber – URL Grabber
- /all_type_attack – All-in-One Attack Panel

Functionality Overview

- SQL Injection:
  - Upload payload file
  - Input target URL
  - Real-time scan logs
- XSS Testing:
  - GET/POST modes
  - Optional blind mode
- Directory Traversal:
  - Tests common OS paths
  - Highlights leakage indicators
- Subdomain Enumeration:
  - Passive (crt.sh, AlienVault, RapidDNS)
  - Active brute-force
- URL Extraction:
  - Paste or upload text
  - Extracts and scrapes URLs

Saved Data Files

- - subdomains_<domain>.txt
- - extracted_urls.txt

Stopping the App

- Use CTRL+C to stop the server
- Clean files manually:
  rm subdomains_*.txt
  rm extracted_urls.txt

Optional: requirements.txt

- Contents:
  flask
  aiohttp
  aiofiles
  beautifulsoup4
  dnspython
  validators
  requests
  urllib3
- Install with:
  pip install -r requirements.txt