Streamlit Hash Cracker - Detailed Documentation

This document provides a detailed explanation and user guide for the Streamlit-based Hash Cracker tool. The tool provides a web-based interface for cracking password hashes using techniques such as dictionary attacks, rule-based mutations, brute-force, mask-based generation, and combinator attacks. It supports MD5, SHA1, and SHA256 algorithms and stores cracked results in a log file.

Requirements: - Python 3.7+ - Libraries: streamlit, hashlib, itertools, multiprocessing, datetime

Installation:
1. Save the provided Python script as *streamlit_hash_cracker.py*.
2. Install dependencies using pip:
pip install streamlit
3. Run the application with:
streamlit run streamlit_hash_cracker.py
4. The application will open in your web browser (default: http://localhost:8501).

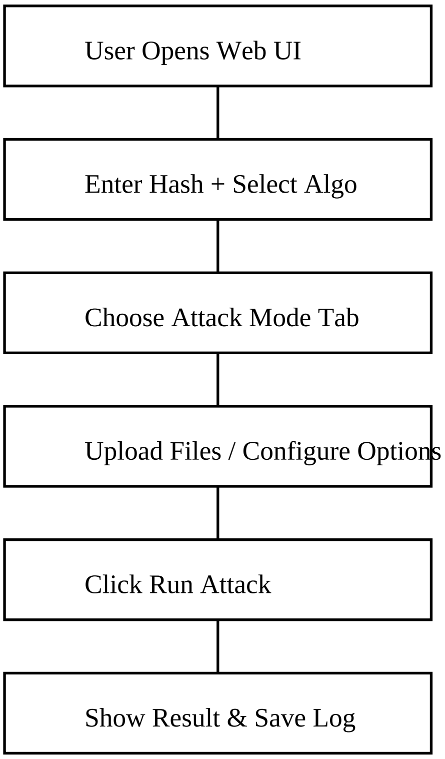
Available Modes

- **Dictionary Attack:** Upload a wordlist (.txt). The tool checks each word against the target hash.
- **Rule-based Attack:** Applies simple mutations (123, !, capitalization, reverse, leetspeak) on uploaded words.
- **Brute-force Attack:** Tries all combinations from a given character set up to a chosen maximum length.
- **Mask Attack:** Generates candidates from a pattern (e.g., ?l?l?d = lowercase+lowercase+digit).
- **Combinator Attack:** Uploads two wordlists and tests concatenated combinations (word1+word2, word2+word1).

User Interface Flow:
1. Enter the hash value in the input box.
2. Select the hashing algorithm (MD5, SHA1, SHA256).
3. Choose one of the five modes from the tabs:
- Dictionary
- Rule-based
- Brute-force
- Mask
- Combinator
4. Upload files or configure options depending on the mode.
5. Click the corresponding button (e.g., "Run Dictionary Attack").
6. If a match is found, it will be displayed as a success message.

Logs & Output:
- Success results are displayed on the Streamlit interface with a green success box.
- If no match is found, a red error box appears.
- All cracked results are stored in *cracked_log.txt* with timestamp, algorithm, hash, and password.

Workflow Diagram


User Opens Web UI
Enter Hash + Select Algo
Choose Attack Mode Tab
Upload Files / Configure Options
Click Run Attack
Show Result & Save Log