Password Strength Checker – Comprehensive Documentation

1. Purpose & Scope

Goals

- Provide an intuitive tool to evaluate password strength based on standard security practices.
- Educate users on creating secure passwords through real-time, actionable feedback.
- Offer a clean and interactive interface for quick and easy password strength assessment.

Target Audience

- **General Users**: Individuals looking to test their personal passwords.
- **Developers**: Those interested in implementing similar logic into apps or systems.
- **Security Professionals**: Teams validating internal password strength policies.

Inclusions

- Password evaluation and scoring logic
- Gradio-based user interface
- Suggestions for improvement and example strong passwords

Exclusions

- No database or breach-detection functionality
- No multilingual support or user authentication

2. Structure & Organization

Documentation Hierarchy

- Overview
- Features
- Requirements
- Installation & Setup
- How It Works
- Evaluation Logic
- UI Components
- Code Walkthrough
- Example Outputs
- Customization Options
- Known Limitations
- License & Legal
- Feedback Mechanism
- FAQ’s

Formatting Conventions

- Markdown with consistent headers (##, ###)
- Lists and bullet points for readability
- Code blocks for technical examples
- Tables and diagrams where applicable

3. Content Quality & Clarity

Language Style

- Clear, simple, and active voice
- Minimal jargon to enhance accessibility

Visuals (Optional)

- UI screenshot of the Gradio interface
- Flowchart showing password evaluation steps

Example

```
# Password evaluation logic
if len(password) >= 8:
   score += 1
```

Use Case Example:
Input: Pass123! → Output: Strong Password (100%)

4. Version Control & Updates

Version Tracking

- Managed on GitHub with commit history

Changelog Example:

```
## v1.0.0 (2024-07-20)

- Initial release with full Gradio-based UI.
```

Maintenance

- Update documentation upon changes to:
  - Scoring logic
  - UI/UX components
  - Suggestions or criteria

5. Accessibility & Searchability

Navigation

- Sectioned headers allow quick searching via browser (CTRL+F)
- Internal links (on platforms like GitHub) for jumping between topics

Mobile Compatibility

- Gradio's interface is responsive by default and works well on mobile devices

6. Collaboration & Review Process

Roles

- **Writer**: Creates and maintains documentation
- **Reviewer**: Ensures technical accuracy and clarity
- **Maintainer**: Syncs updates with codebase changes

Tools

- GitHub Wiki for collaborative editing
- Google Docs or Notion for drafting and peer reviews

7. Tools & Platforms

Documentation

- Written in Markdown
- Hosted on GitHub (Project Documentation/README.md)

Deployment

- Hosted on Hugging Face Spaces.

8. Legal & Compliance

Disclaimer

This tool performs local evaluations only and does **not store or transmit passwords**. Use it at your own discretion.

License

Released under the **MIT License** – free for personal and commercial reuse with attribution.

9. User Feedback & Improvement

Feedback Channels

- GitHub Issues for reporting bugs or feature requests
- (Optional) Google Forms or feedback link for usability reviews

Iteration Cycle

- Documentation and logic reviewed quarterly
- Examples and UI suggestions updated based on user feedback

10. FAQ's

- **Q: Does this check password breaches?**
  A: No, this only evaluates complexity, not exposure.
- **Q: Can I use this in my own app?**
  A: Yes, it's open-source and MIT-licensed.

Glossary

Term	Definition
Password Strength	A measure of how resistant a password is to guessing or brute-force attacks, based on length, complexity, and unpredictability.
Uppercase Letter	A capital letter (A-Z). Required for stronger passwords.
Lowercase Letter	A small letter (a-z). Required for stronger passwords.
Digit	A numerical character (0-9). Enhances password complexity.
Special Character	A symbol like !@#$%^&*() that increases security.
Brute-Force Attack	A hacking method where attackers try all possible password combinations.
Gradio	A Python library used to create web interfaces for machine learning and data science apps.
Verdict	The final assessment of password strength (Weak/Medium/Strong).
Score (%)	A numerical rating (0-100%) reflecting password strength.

Term	Definition
Open Source	Software with publicly available code, free to modify and distribute (e.g., MIT License).