



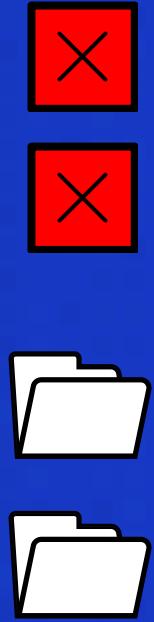


Password Strength Analyzer with AI, ML, HIBP and Hashcat

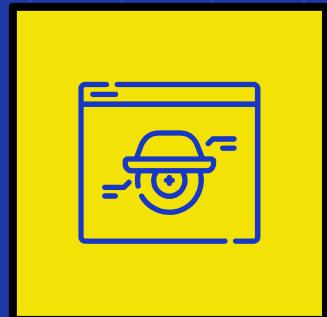
Intelligent Tool for Password Strength Analysis using GenAI, Machine Learning and Hashcat



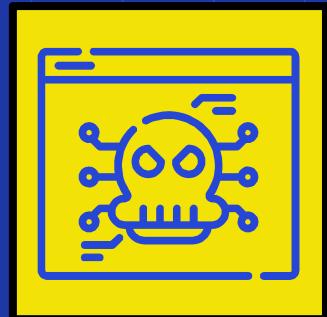
HACK-O-HIRE-2025



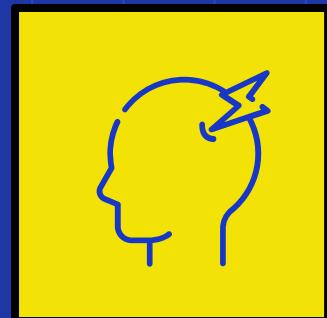
TEAM - Back to Lays



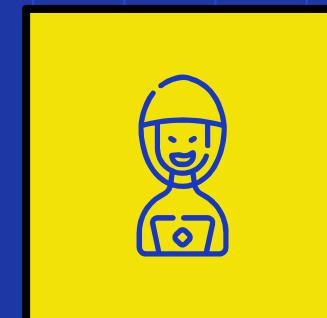
Aditi Roy



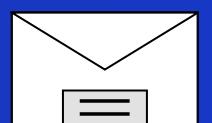
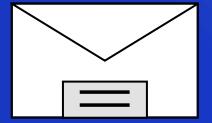
Aditya Verma



Sahil Adhikari



Ayush Mukherjee





UNDERSTANDING THE PROBLEM STATEMENT

Problem Statement:

- Weak passwords are a major vulnerability, leading to frequent security breaches.
- Existing strength meters often lack in-depth analysis and actionable insights.
- There is a need for an intelligent tool that not only evaluates password strength but also explains weaknesses and suggests improvements smartly—all while keeping user data private (local processing & hashing).

Objective:

- Develop an intelligent web based AI tool to analyze password strength using ML for analysis (RockYou 2009&2024), realtime HIBP Lookup and pre-trained GEN-AI models
- Estimate time-to-crack using bcrypt and hashcat, check against breach databases, and provide interpretable feedback with strong alternative suggestions.



OUR SOLUTION

With over 80% of breaches linked to weak passwords, securing this vulnerability is critical. Our tool addresses this head-on..



Phase 1 - Requirement Analysis

Objective:

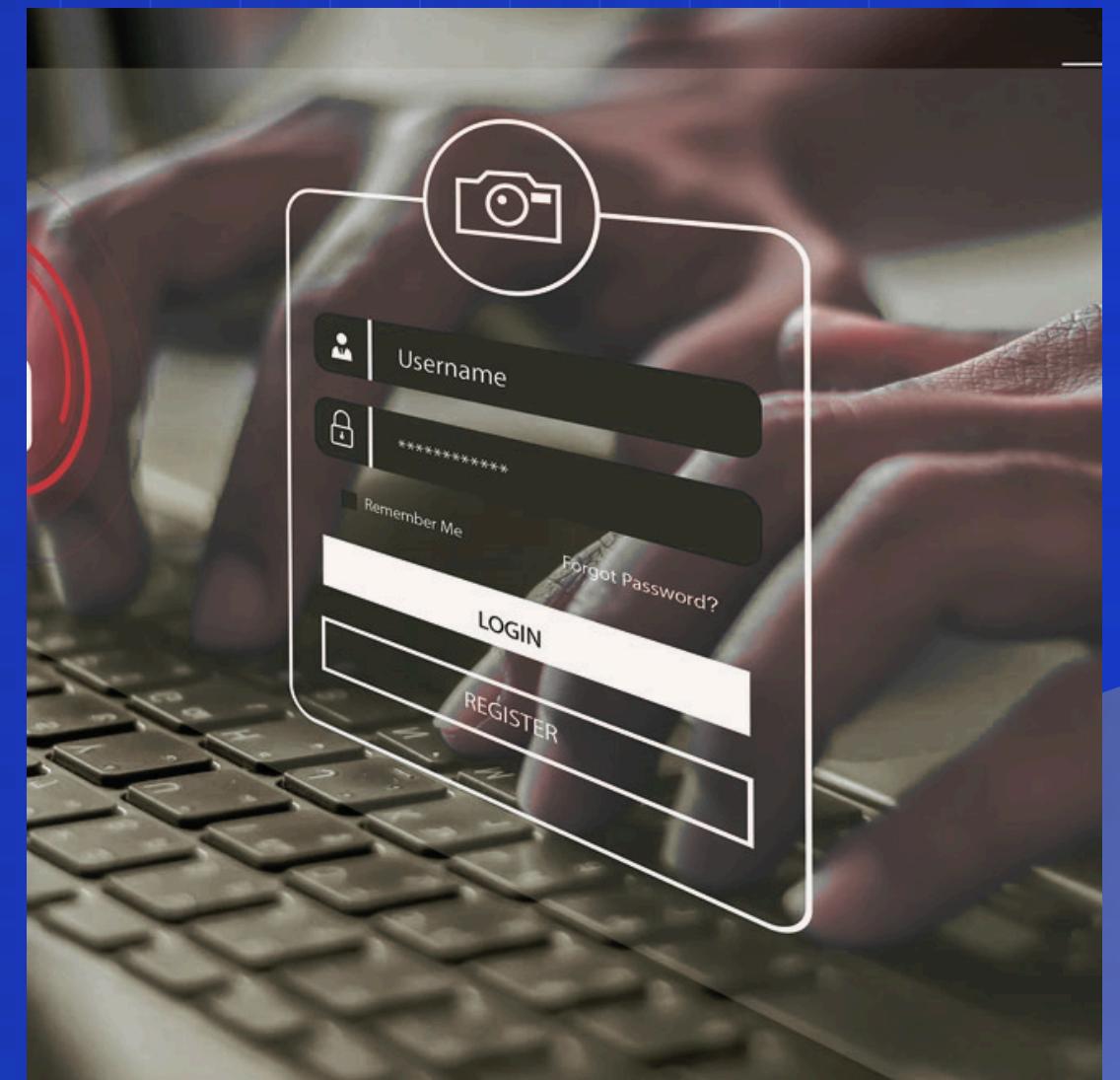
- Identify security gaps in current password strength evaluations.
- Analyze the RockYou and HIBP dataset and leaked password trends.

Define key features:

- GenAI-based password suggestions.
- Machine Learning Pattern Analysis
- Time-to-crack estimation.
- Vulnerability feedback.

Stakeholders:

- Barclays / Enterprise Cybersecurity Team
- End Users (Employees, Customers)
- Regulatory Bodies



Phase 2 - System Design



Architectural Considerations:

- Frontend: Vite/React for a responsive modular user interface.
- Backend: Efficient FastAPI framework for low-latency, high-performance password analysis and security evaluation.

- ML & AI:

- GenAI (OLLAMA LLM) for generating human-readable explanations and suggestions.
 - Trained on RockYou LightGBM Classifier – A gradient boosting model

- Security Analysis:

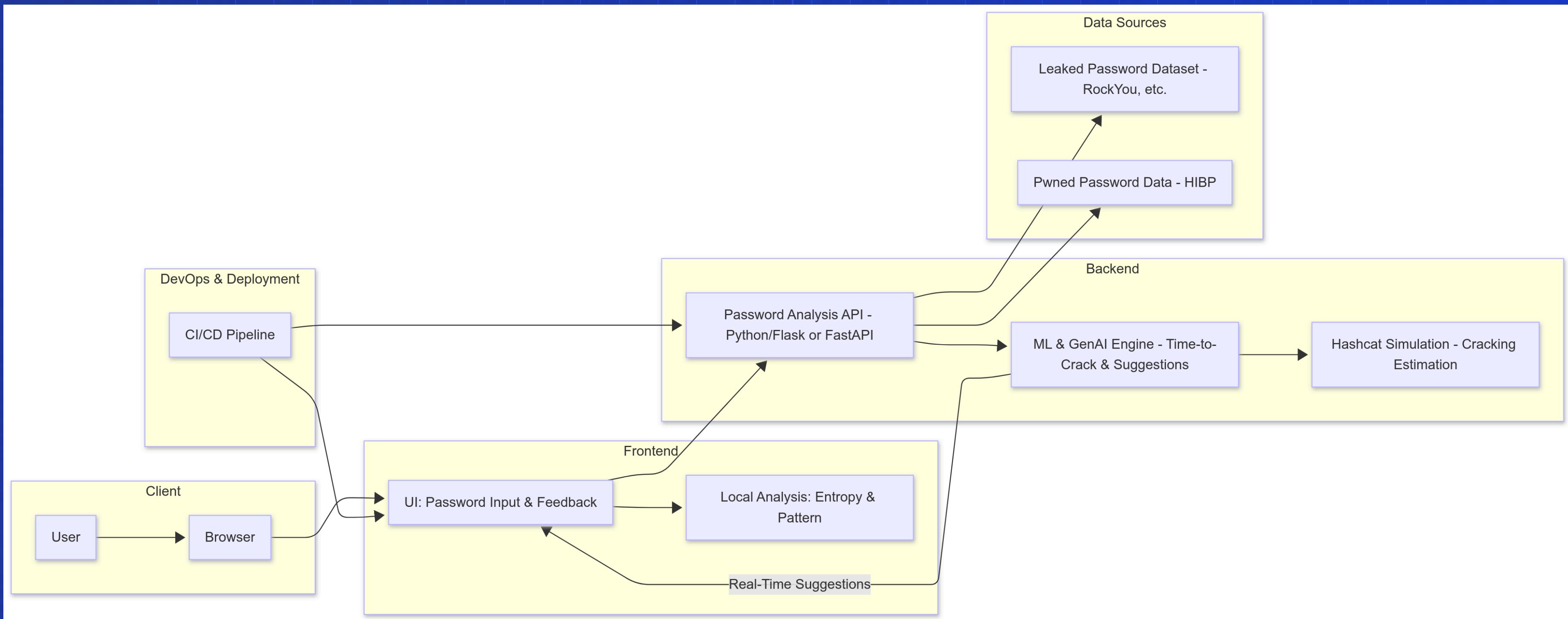
- Hashcat for password cracking simulation.
 - Entropy-based evaluation for detailed strength metrics.
 - For security and user data safety model will be processing locally(user device)
 - Live lookup on HIBP Database



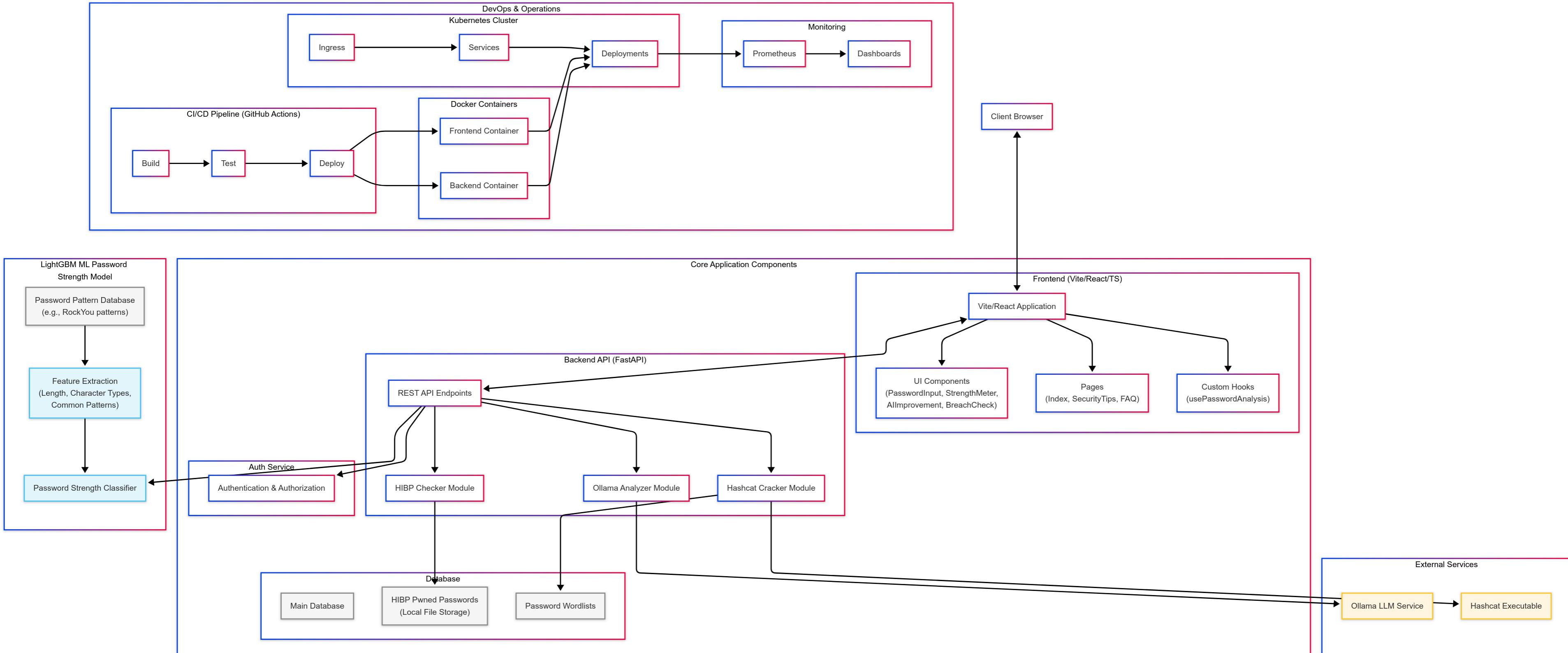
High-Level System Architecture (Diagram):

UI ➔ Backend API ➔ ML Model ➔ HIBP lookup and Hashcat result ➔ GenAI model ➔ Feedback to User.

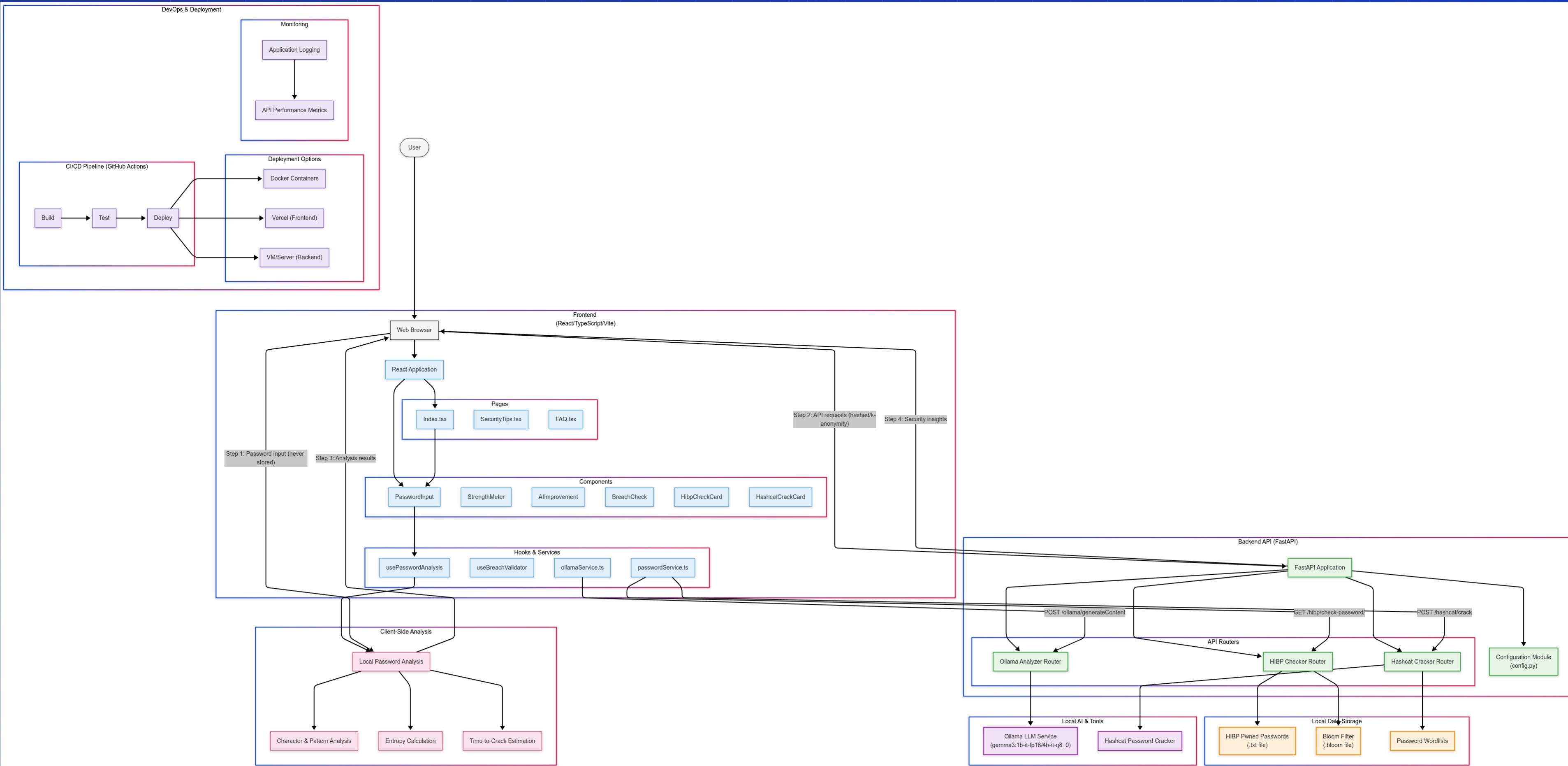
HIGH LEVEL WORKFLOW DIAGRAM



WORKFLOW DIAGRAM



DETAILED WORKFLOW DIAGRAM



Phase 3 - Implementation

Sprint-Based Development Approach:

Sprint 1

Data Collection & Preprocessing

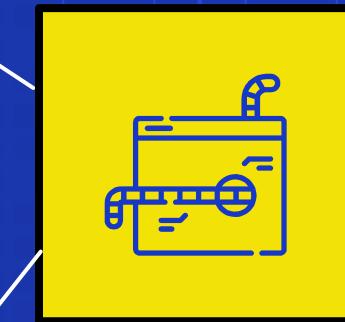
Gather RockYou dataset and analyze password patterns.



Sprint 2

Model Development

Train ML models on password vulnerabilities, HIBP lookup and hashcat program



Sprint 5

Security Enhancements & Optimization

Implement additional safeguards, optimize performance, and refine calculations.

Sprint 3

GenAI Integration

Integrate GenAI to generate explanations and suggest enhancements.

Sprint 4

Web UI & API Development

Build a clean, interactive frontend that calls the /analyze endpoint.



Phase 4 - Testing

Types of Testing Used:

1

Unit Testing

Validate password strength evaluation and hashing algorithm efficiency.

2

Integration Testing:

Ensure smooth communication between the ML model, GenAI LLM, Hashcat and HIBP service API, and UI.

3

Security Testing:

Simulate attacks (brute-force, dictionary-based) using Hashcat. [MD5 & SHA256]

4

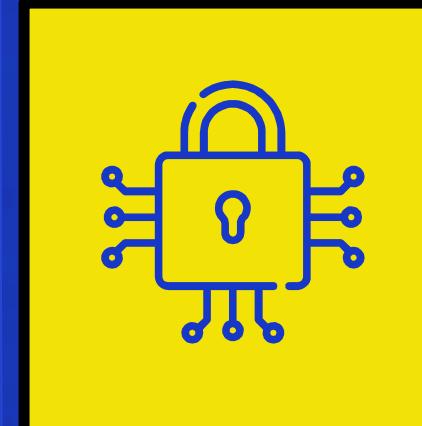
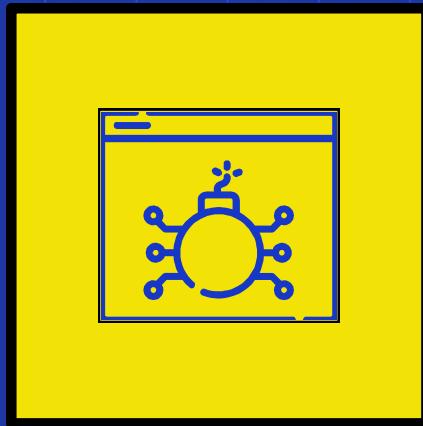
User Testing

Gather feedback on usability and clarity of explanations.





Phase 5 - Deployment & Maintenance

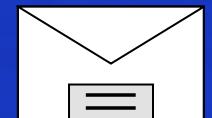


Deployment Strategy

- CI/CD Pipeline: Automate deployments using GitHub Actions or Jenkins.
- Cloud Deployment: Host on AWS/GCP for scalability.
- Prometheus and Grafana for API monitoring
- Docker and Kubernetes

Maintenance Approach

- Regular Updates: Continuously update ML models and HIBP with new versions.
- Logging & Monitoring: Detect anomalies such as frequent weak passwords.
- User Feedback Loop: Refine UI and AI suggestions based on user interactions.



Output UI Design Result



Intelligent Password Strength Analyzer

Check how secure your password is with our advanced AI analysis tool. Get real-time feedback to create stronger, safer passwords.

Enter a password to analyze

Copy Reset

Weak 85.4

Character Composition
13 characters total

Category	Count	Percentage
Uppercase	1	(8%)
Lowercase	7	(54%)
Numbers	4	(31%)
Symbols	1	(8%)

Brute Force:
+300 years
4 weeks

Hardware-specific estimates (bcrypt):
Standard CPU: 3 days
Normal GPU: 1 hour
High-End GPU: 7 minutes

⚠️ 59% of real passwords are cracked within an hour using smart algorithms

Feedback & Suggestions

- Avoid common words like 'password' or 'admin'
- This pattern appears in the RockYou (Common Wordlist) breach dataset
- Avoid sequential patterns like '123' or 'abc'
- 59% of real passwords are cracked within an hour
- Entropy: 85.4 bits (higher is better)

AI-Powered Suggestions

Smart password analysis and enhancement based on your input

Analysis Password Gen

⚠️ Vulnerability analysis:

- The password's low entropy (85.4 bits) and reliance on a common pattern ('Password') make it highly vulnerable to dictionary and brute-force attacks, particularly when combined with the limited character set.
- Despite the relatively high entropy, the password's length is only 13 characters, which is insufficient to withstand prolonged attacks, especially with the availability of powerful hardware.

ⓘ Improvement suggestions:

- Increase password length to 16+ characters to improve resistance against brute-force attacks. Example: 'SecurePassw0rd!@#\$'
- Incorporate more diverse symbols beyond the current set to enhance entropy and complexity. Example: 'SecurePassw0rd!@#\$7'
- Avoid using common or easily guessable patterns like 'Password' followed by a simple numeric sequence. Example: 'SecurePassw0rd1234567890'

AI-generated strong alternative: Customize

Not found in known breach databases
.....

Copy Regenerate

Strength Score: 4/4

Output UI Design Result

Password Found in HIBP Database
This exact password was found in the Have I Been Pwned database, indicating it has been exposed in a data breach. You should not use it.

Password potentially compromised
This password pattern appears similar to known compromised passwords (confidence: 100%).

Similar passwords found in these breach databases:

- Have I Been Pwned

Vulnerable to these attack methods:

- Known Breach Exposure

Our password security system uses patterns from known breaches to evaluate your password.

Hashcat: Password Cracked (Insecure)
Hash successfully cracked.
 Password Found: Password@1234
Original Hash (MD5): 0f1ba603c1a843a3d02d6c5038d8e959
 Wordlist Used: rockyou.txt
 Hash Mode: 0 (MD5)
 Time Elapsed: 11.30 seconds

Your password is never stored or sent to any third-party services

AI-Powered Suggestions
Smart password analysis and enhancement based on your input

[Analysis](#) [Password Gen](#)

Customize your password:

Length: 16

Uppercase (A-Z) Lowercase (a-z)
 Numbers (0-9) Symbols (!@#\$)

Strength Score: 4/4

Estimated crack times:
CPU (bcrypt): 7047 thousand years
Normal GPU: 167 thousand years
High-End GPU: 13 thousand years

)G&]318\$22eBt;Wj

Generate

Not found in known breach databases

Copy to Clipboard





Benefits

■ Enhanced Security:

Significantly reduces the risk of password-related breaches by not only on character composition but also realtime lookup with GenAI

■ Real-time Feedback

Provides immediate, actionable insights for stronger passwords.

■ Compliance & Risk Mitigation

Helps meet cybersecurity policies and regulatory standards.





Future Scope

■ Multilingual Support

Enable analysis of passwords in various languages, accommodating diverse character sets and linguistic patterns. Research indicates that multilingual passphrases can significantly increase password strength by expanding the character set and disrupting predictable patterns.

■ Enterprise Integration

Facilitate seamless integration with enterprise systems, such as Single Sign-On (SSO) and Identity and Access Management (IAM) solutions. This will allow organizations to enforce password policies consistently across their infrastructure, enhancing security and compliance.

■ Enhanced User Interaction & Personalized Guidance

- GenAI to act as an adaptive coach, offering specific, context-aware transformations tailored to identified weaknesses. We also plan to introduce novel structural visualizations that intuitively highlighting the weakest links for better user understanding and exploring privacy-aware gamification elements and feedback on common weak patterns making the tool a proactive partner in improving long-term security hygiene.



Conclusion



- **SDLC-driven approach incorporating ML and GenAI to enhance password security**
- **Iterative phases from requirement analysis to deployment, with a strong emphasis on privacy and robust testing**

