LAPORAN PENDAHULUAN

REKAYASA PERANGKAT LUNAK 2

ANALISIS DATASET rockyou.txt DAN KALKULATOR KEMANAN PASSWORD

Nama Anggota :

1. **FARRAS DZAKY FAISA (50422533)**
2. **MUHAMMAD BUKHORI (51422002)**
3. **MUHAMMAD BINTANG ALIFIANSYAH (514422001)**
4. **MUHAMMAD VIRGAWAN (51422167)**

KELAS 4IA12

PROGRAM STUDI INFORMATIKA

UNIVERSITAS GUNADARMA

DEPOK

2025

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa, karena atas limpahan rahmat dan karunia-Nya penulis dapat menyelesaikan **laporan pendahuluan** ini dengan baik dan tepat waktu. Laporan pendahuluan ini disusun sebagai salah satu bentuk pemenuhan tugas perkuliahan serta sebagai sarana untuk menambah wawasan dan pemahaman penulis terhadap materi yang dibahas.

Ucapan terima kasih penulis sampaikan kepada Ibu **Linda Handayani** selaku dosen pengampu mata kuliah **Rekayasa Perangkat Lunak 2** yang telah memberikan bimbingan, arahan, dan ilmu pengetahuan selama proses penyusunan laporan pendahuluan ini. Penulis juga mengucapkan terima kasih kepada semua pihak yang telah membantu, baik secara langsung maupun tidak langsung, sehingga laporan pendahuluan ini dapat diselesaikan dengan baik.

Kami menyadari bahwa dalam penyusunan ini masih banyak kekurangan karena keterbatasan kami. Maka dari itu penyusun sangat mengharapkan kritik dan saran untuk menyempurnakan. Semoga apa yang ditulis dapat bermanfaat bagi semua pihak yang membutuhkan.

Depok, 29 Desember 2025

Kelompok 9

DAFTAR ISI

BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan informasi merupakan aspek fundamental dalam sistem informasi modern, khususnya dalam menjaga kerahasiaan data dan identitas pengguna. Salah satu mekanisme pengamanan yang paling umum digunakan adalah password. Password berfungsi sebagai kunci autentikasi utama untuk mengakses berbagai layanan digital, mulai dari sistem akademik, perbankan, hingga media sosial. Namun, dalam praktiknya masih banyak pengguna yang menggunakan password sederhana dan mudah ditebak, seperti tanggal lahir, nama pribadi, atau kombinasi angka berurutan. Pola penggunaan password yang lemah ini secara signifikan meningkatkan risiko terjadinya kebocoran data dan penyalahgunaan akun.

Berbagai insiden kebocoran data menunjukkan bahwa kelemahan password masih menjadi celah utama dalam keamanan siber. Salah satu dataset yang sering digunakan untuk mengkaji fenomena tersebut adalah rockyou.txt, yaitu kumpulan password hasil kebocoran data yang berisi lebih dari 14 juta entri password asli dari pengguna. Dataset ini mencerminkan pola nyata perilaku pengguna dalam membuat password dan menjadi sumber yang relevan untuk menganalisis tingkat keamanan password secara empiris.

Berdasarkan permasalahan tersebut, diperlukan suatu pendekatan kuantitatif yang mampu mengukur kekuatan password secara objektif. Salah satu metode yang dapat digunakan adalah Shannon Entropy, yaitu ukuran matematis yang menggambarkan tingkat ketidakpastian atau keacakan suatu informasi. Dengan pendekatan ini, kekuatan password dapat dinilai berdasarkan panjang karakter dan variasi karakter yang digunakan. Oleh karena itu, proyek ini dirancang untuk menganalisis kekuatan password berbasis entropy serta menyajikan hasil analisis tersebut dalam bentuk aplikasi web yang bersifat edukatif dan interaktif.

1.2. Rumusan Masalah

- Bagaimana tingkat kekuatan password pada dataset rockyou.txt jika dianalisis menggunakan metode Shannon Entropy?
- Bagaimana perancangan sistem yang dapat mengklasifikasikan kekuatan password berdasarkan nilai entropy?
- Bagaimana menyajikan hasil analisis kekuatan password dalam bentuk aplikasi berbasis web yang interaktif dan edukatif?

1.3. Tujuan Penulisan

Tujuan penyusunan laporan pendahuluan ini adalah untuk memberikan gambaran awal mengenai proyek analisis kekuatan password berbasis entropy. Secara khusus, tujuan yang ingin dicapai adalah menganalisis tingkat kekuatan password menggunakan metode Shannon Entropy, merancang sistem klasifikasi kekuatan password berdasarkan nilai entropy, serta merencanakan pengembangan aplikasi berbasis web yang dapat digunakan sebagai media edukasi keamanan password bagi pengguna.

BAB II
PEMBAHASAN

2.1. Deskripsi Sistem

Klasifikasi kekuatan password dibagi ke dalam empat kategori, yaitu sangat lemah, lemah, sedang, dan kuat, berdasarkan rentang nilai entropy yang telah ditentukan. Implementasi sistem direncanakan dalam bentuk aplikasi berbasis web menggunakan bahasa pemrograman Python dengan framework Streamlit. Analisis data berskala besar dilakukan menggunakan Google Colaboratory. Proyek ini tidak membahas aspek kriptografi lanjutan maupun penerapan sistem autentikasi pada lingkungan produksi.

2.2. Rencana Arsitektur Sistem

Secara umum, sistem yang direncanakan akan menerima input berupa string password dari pengguna. Password tersebut dianalisis untuk menentukan panjang karakter dan jenis karakter yang digunakan, meliputi huruf kecil, huruf besar, angka, dan simbol. Berdasarkan kombinasi karakter tersebut, sistem akan menentukan ukuran charset yang digunakan.

Selanjutnya, sistem menghitung nilai entropy menggunakan rumus Shannon Entropy, yaitu $H = L \times log_2 N$ di mana H merupakan nilai entropy, L adalah panjang password, dan N adalah ukuran charset. Nilai entropy yang diperoleh digunakan untuk menentukan kategori kekuatan password. Hasil analisis ditampilkan kepada pengguna dalam bentuk informasi tingkat kekuatan password beserta penjelasan singkat yang bersifat edukatif.

2.3. Analisis Kekuatan Password

Analisis kekuatan password dilakukan dengan menerapkan metode Shannon Entropy terhadap dataset rockyou.txt yang berisi lebih dari 14 juta password hasil kebocoran data. Tahapan analisis dimulai dengan menghitung nilai entropy untuk setiap password berdasarkan panjang karakter dan variasi jenis karakter yang digunakan, meliputi huruf kecil, huruf besar, angka, dan simbol.

Nilai entropy yang dihasilkan kemudian digunakan untuk mengklasifikasikan password ke dalam empat kategori kekuatan, yaitu sangat lemah, lemah, sedang, dan kuat. Hasil analisis menunjukkan bahwa sebagian besar password dalam dataset berada pada kategori sangat lemah

hingga sedang, yang mengindikasikan rendahnya tingkat keamanan password yang digunakan oleh pengguna secara umum.

Distribusi nilai entropy dianalisis secara kuantitatif untuk mengetahui pola umum pembentukan password. Password dengan panjang pendek dan variasi karakter terbatas cenderung memiliki nilai entropy rendah, sedangkan password dengan panjang lebih besar serta kombinasi karakter yang beragam menunjukkan nilai entropy yang lebih tinggi dan tingkat keamanan yang lebih baik.

2.4. Analisis Kekuatan Password

Sebelum dilakukan analisis lebih lanjut, dataset rockyou.txt melalui tahap filterisasi untuk memastikan kualitas dan relevansi data. Proses filterisasi ini bertujuan untuk menghilangkan password yang tidak memenuhi kriteria analisis keamanan.

Tahap pertama filterisasi dilakukan dengan menghapus data duplikat agar setiap password yang dianalisis bersifat unik. Selanjutnya, dilakukan penyaringan berdasarkan panjang karakter, di mana password yang terlalu pendek dikeluarkan dari dataset karena memiliki tingkat keamanan yang sangat rendah dan tidak representatif untuk analisis kekuatan.

BAB III
PENUTUP

3.1. Kesimpulan

Hasil analisis terhadap dataset rockyou.txt menunjukkan bahwa sebagian besar password yang digunakan oleh pengguna masih berada pada kategori sangat lemah hingga sedang. Temuan ini mengindikasikan bahwa kesadaran pengguna terhadap pentingnya penggunaan password yang kuat masih tergolong rendah, sehingga berpotensi meningkatkan risiko kebocoran data dan penyalahgunaan akun. Kondisi tersebut menegaskan bahwa password sederhana dan mudah ditebak masih menjadi permasalahan utama dalam keamanan informasi.

Selain itu, proses filterisasi password yang dilakukan sebelum tahap analisis memiliki peranan penting dalam meningkatkan kualitas dan validitas data. Dengan menghapus data duplikat, menyaring password yang terlalu pendek, serta memvalidasi karakter yang digunakan, dataset yang dianalisis menjadi lebih representatif. Hal ini berdampak langsung pada keakuratan hasil pengukuran entropy dan klasifikasi kekuatan password yang dihasilkan. Secara keseluruhan, laporan pendahuluan ini memberikan landasan konseptual dan metodologis yang kuat bagi pengembangan sistem analisis kekuatan password berbasis web pada tahap selanjutnya.

3.2. Saran

Penelitian berikutnya disarankan untuk mengombinasikan metode Shannon Entropy dengan pendekatan lain, seperti analisis pola password atau penerapan teknik machine learning, guna memperoleh hasil penilaian kekuatan password yang lebih komprehensif dan adaptif terhadap pola serangan modern.

Selain itu, sistem analisis kekuatan password yang dikembangkan dapat ditingkatkan dengan menambahkan fitur rekomendasi perbaikan password secara otomatis. Dengan adanya fitur tersebut, pengguna tidak hanya mengetahui tingkat kekuatan password yang digunakan, tetapi juga memperoleh panduan konkret dalam menyusun password yang lebih aman dan sesuai dengan standar keamanan informasi.

Dari sisi implementasi, disarankan agar aplikasi berbasis web yang dirancang dilengkapi dengan antarmuka yang lebih interaktif serta visualisasi data yang informatif. Pengembangan tersebut diharapkan dapat meningkatkan pemahaman dan kesadaran pengguna terhadap pentingnya keamanan password, sehingga sistem yang dibangun tidak hanya berfungsi sebagai alat analisis, tetapi juga sebagai media edukasi keamanan informasi di lingkungan digital.