

IMPLEMENTASI DAN ANALISIS KEAMANAN PASSWORD STRENGTH VALIDATION PADA SISTEM MONITORING PESANAN PRODUK CETAK BERBASIS WEB

Wahyu Danuarta, Rezki Kurniati

Teknik Informatika, Politeknik Negeri Bengkalis
Jalan Bathin Alam Desa Sungai Alam, Kab. Bengkalis, Indonesia
wahyudanuarta001@gmail.com

ABSTRAK

Perkembangan teknologi informasi telah mendorong perusahaan percetakan untuk beralih ke sistem digital demi meningkatkan efisiensi dan kualitas layanan mereka. Meski demikian, penerapan sistem berbasis web juga menimbulkan risiko terhadap keamanan, terutama dalam hal identifikasi pengguna. Penelitian ini berfokus pada penerapan dan analisis keamanan Password Strength Validation (PSV) dalam sistem pemantauan pesanan produk cetak berbasis web di Pemuda Grafika Bengkalis. Metode yang dipakai untuk pengembangan sistem adalah Prototype, sementara analisis keamanan dilakukan dengan menggunakan pendekatan validasi berdasarkan aturan dan entropi. Sistem ini juga dilengkapi dengan batasan maksimum login sebanyak tiga kali percobaan untuk mencegah serangan brutal. Pengujian dilakukan menggunakan metode Black Box Testing untuk mengevaluasi fungsi-fungsi sistem serta fitur-fitur keamanan yang diterapkan. Temuan penelitian mengindikasikan bahwa penerapan Password Strength Validation (PSV) dapat menurunkan penggunaan kata sandi yang lemah dan meningkatkan kesadaran pengguna terkait masalah keamanan, serta batasan login yang efektif dalam menghalangi akses yang tidak sah. Dengan demikian, sistem pemantauan pesanan yang dikembangkan tidak hanya meningkatkan efisiensi dalam manajemen pesanan tetapi juga memberikan perlindungan yang lebih baik terhadap data pengguna.

Kata kunci : Keamanan Sistem, Password Strength Validation, Produk Cetak, Sistem Monitoring, Web

1. PENDAHULUAN

Perkembangan teknologi informasi mendorong berbagai sektor usaha, termasuk usaha percetakan, untuk mengadopsi sistem digital dalam meningkatkan efisiensi operasional dan kualitas layanan. Pemanfaatan sistem berbasis web memungkinkan proses pemesanan, pengelolaan data, dan pemantauan status pesanan dilakukan secara lebih cepat dan terintegrasi. Digitalisasi ini menjadi penting terutama bagi usaha mikro, kecil, dan menengah agar mampu bersaing dan memenuhi kebutuhan pelanggan yang menuntut layanan yang praktis dan transparan [1].

Dalam konteks usaha percetakan, sistem monitoring pesanan berbasis web memberikan kemudahan bagi pelanggan untuk memantau status pesanan tanpa harus datang langsung ke lokasi usaha. Selain meningkatkan kenyamanan pelanggan, sistem ini juga membantu pemilik usaha dan kasir dalam mengelola pesanan secara terstruktur dan terdokumentasi dengan baik. Namun, penerapan sistem berbasis web tidak hanya membawa manfaat, tetapi juga menimbulkan tantangan baru, khususnya pada aspek keamanan sistem informasi [2].

Salah satu aspek keamanan yang sering diabaikan dalam sistem berbasis web adalah mekanisme autentikasi pengguna. Penggunaan kata sandi yang lemah masih menjadi celah utama terjadinya kebocoran data dan akses tidak sah. Berbagai serangan seperti brute force attack memanfaatkan kelemahan kata sandi untuk memperoleh akses ke dalam sistem [3]. Laporan keamanan menunjukkan bahwa penyalahgunaan

kredensial masih menjadi salah satu penyebab utama insiden pelanggaran data pada aplikasi berbasis web [4]. Kondisi ini menunjukkan bahwa sistem monitoring pesanan berbasis web masih rentan terhadap akses tidak sah apabila tidak dilengkapi dengan mekanisme autentikasi yang kuat.

PSV merupakan salah satu pendekatan yang dapat digunakan untuk meningkatkan keamanan autentikasi pengguna. PSV bekerja dengan memvalidasi kata sandi berdasarkan aturan tertentu, seperti panjang karakter dan variasi penggunaan huruf besar, huruf kecil, angka, dan simbol, serta dapat dikombinasikan dengan perhitungan entropi untuk mengukur tingkat kekuatan kata sandi secara matematis. Selain itu, penerapan pembatasan jumlah percobaan login juga terbukti efektif dalam mengurangi risiko serangan brute force dengan membatasi upaya login berulang yang tidak sah [5]. Mekanisme keamanan tersebut diterapkan pada sistem monitoring pesanan produk cetak berbasis web yang dikembangkan dalam penelitian ini.

Beberapa penelitian sebelumnya telah mengembangkan sistem pemesanan produk cetak berbasis web dengan fokus pada peningkatan efisiensi layanan dan manajemen pesanan [2], [6]. Penelitian lain juga membahas validasi kekuatan kata sandi dan analisis entropi sebagai upaya meningkatkan keamanan sistem autentikasi [7], [5]. Namun, sebagian besar penelitian tersebut masih membahas aspek fungsional sistem pemesanan dan keamanan secara terpisah, serta belum secara khusus mengintegrasikan analisis keamanan Password Strength Validation

(PSV) ke dalam sistem monitoring pesanan produk cetak berbasis web.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk implementasikan dan menganalisis mekanisme PSV pada sistem monitoring pesanan produk cetak berbasis web di Pemuda Grafika Bengkalis. Sistem dikembangkan menggunakan metode Prototype dan dilengkapi dengan mekanisme pembatasan login untuk meningkatkan perlindungan terhadap akses tidak sah. Pengujian sistem dilakukan menggunakan metode Black Box Testing. Penelitian ini diharapkan tidak hanya mampu meningkatkan efisiensi pengelolaan dan monitoring pesanan, tetapi juga memberikan kontribusi dalam peningkatan keamanan autentikasi pengguna pada sistem informasi berbasis web, khususnya pada skala UMKM.

2. TINJAUAN PUSTAKA

Tinjauan Pustaka mencakup pembahasan terdahulu dan landasan teori yang relevan sebagai dasar dalam penelitian ini. Pembahasan difokuskan pada sistem monitoring pesanan berbasis web, aspek keamanan sistem informasi, serta penerapan PSV dan batasan login untuk meningkatkan keamanan otentikasi pengguna. Tinjauan ini bertujuan untuk memperkuat kerangka konseptual dan menegaskan kontribusi penelitian.

2.1. Penelitian Terdahulu

Beberapa penelitian sebelumnya telah membahas mengenai pengembangan sistem pemesanan dan pemantauan produk cetak berbasis web dengan tujuan untuk meningkatkan efisiensi layanan dan pengelolaan data pesanan. Sistem ini mampu mempercepat proses pemesanan dan mengurangi kesalahan dalam penginputan data, namun keamanan autentikasi pengguna belum menjadi perhatian utama dalam pengembangannya [2], [6].

Dalam penelitian lainnya, sistem pemesanan berbasis web juga terbukti memberikan kejelasan informasi kepada pelanggan serta memudahkan pengelolaan status pesanan oleh para administrator. Namun, sebagian besar studi ini masih lebih mengutamakan aspek fungsional dari sistem dan belum sepenuhnya menyelidiki cara-cara untuk melindungi akses pengguna ke dalam sistem [1], [8].

Penelitian mengenai keamanan autentikasi pengguna menunjukkan bahwa kata sandi yang lemah tetap menjadi kelemahan utama untuk akses yang tidak sah. Beberapa penelitian menyarankan langkah-langkah kekuatan kata sandi dengan pendekatan entropi untuk mengklasifikasikan keamanan kata sandi pengguna, sementara yang lain menggunakan metode berbasis aturan untuk membatasi upaya login yang berulang sebagai cara untuk mencegah serangan brute-force [5], [7].

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa kajian tentang sistem pemesanan dan kajian mengenai mekanisme keamanan autentikasi sebagian besar masih dilakukan secara terpisah. Oleh

karena itu, penelitian ini menggabungkan mekanisme PSV berbasis aturan dan entropi serta pembatasan login ke dalam sistem pemantauan pesanan produk cetak berbasis web, sehingga memperkuat keamanan autentikasi pengguna dalam satu sistem yang terintegrasi.

2.2. Sistem Monitoring Pesanan Berbasis Web

Sistem monitoring pesanan berbasis web telah banyak diterapkan di perusahaan percetakan untuk meningkatkan efisiensi layanan dan pengelolaan data pesanan. Sistem ini memungkinkan pemesanan, pencatatan transaksi, dan pemantauan status pesanan secara terintegrasi dan real-time. Beberapa penelitian telah menunjukkan bahwa sistem pemesanan layanan percetakan berbasis web dapat mempercepat proses layanan dan mengurangi kesalahan dalam pencatatan data pesanan [1], [2].

Selain mendukung efisiensi operasional, sistem monitoring pesanan berbasis web juga memberikan transparansi informasi kepada pelanggan. Sistem ini memudahkan pelanggan untuk melihat status pesanan tanpa perlu berkomunikasi secara langsung, serta mempermudah administrator dalam mengelola data transaksi secara teratur [8]. Penelitian lain juga menunjukkan bahwa sistem pemesanan produk cetak berbasis web dapat meningkatkan kualitas layanan serta ketepatan pengelolaan data di bisnis percetakan [6]. Namun, sebagian besar penelitian ini masih lebih menekankan pada aspek fungsional dari sistem dan belum membahas keamanan autentikasi pengguna secara mendalam.

2.3. Keamanan Sistem Informasi Berbasis Web

Keamanan sistem informasi berbasis web telah menjadi hal yang sangat penting seiring dengan meningkatnya pemakaian sistem digital di berbagai sektor bisnis. Salah satu elemen penting dari keamanan sistem berbasis web adalah mekanisme otentikasi pengguna, terutama penggunaan kata sandi sebagai kontrol akses utama. Kata sandi yang lemah masih menjadi faktor utama dalam kebocoran data dan akses tidak sah ke sistem informasi [3].

Laporan keamanan terbaru mengungkapkan bahwa penyalahgunaan kredensial merupakan salah satu penyebab utama terjadinya kebocoran data pada aplikasi berbasis web [4]. Kondisi ini menegaskan bahwa memperkuat mekanisme autentikasi pengguna merupakan kebutuhan penting dalam pengembangan sistem informasi berbasis web agar risiko akses tanpa izin dapat dikurangi.

2.4. Password Strength Validation

PSV adalah metode yang digunakan untuk meningkatkan keamanan autentikasi pengguna dengan memeriksa kekuatan kata sandi berdasarkan aturan dan kompleksitas karakter tertentu. Validasi ini biasanya mencakup pemeriksaan panjang karakter, penggunaan huruf besar dan kecil, angka, serta simbol sebagai syarat dasar untuk membuat kata sandi yang aman.

Pendekatan yang didasarkan pada entropi digunakan untuk secara matematis menilai seberapa acak suatu kata sandi. Dengan cara ini, kata sandi yang memiliki kombinasi karakter yang lebih bervariasi memiliki tingkat keamanan yang lebih tinggi dan lebih sulit ditebak oleh penyerang [7]. Dengan demikian, penerapan PSV dapat mendorong pengguna untuk memilih kata sandi yang lebih kuat dan lebih aman.

2.5. Pembatasan Login dan Brute Force Attack

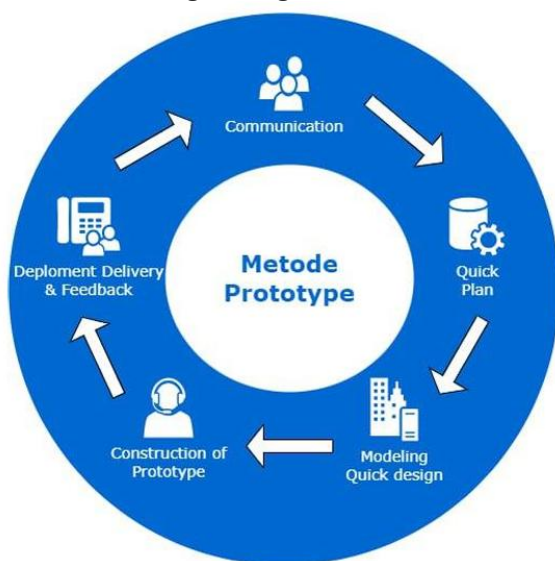
Selain memvalidasi kekuatan kata sandi, membatasi jumlah percobaan login merupakan mekanisme keamanan yang penting untuk mencegah serangan brute-force. Serangan brute-force melibatkan upaya berulang untuk mencoba berbagai kombinasi kata sandi hingga akses diperoleh. Penelitian menunjukkan bahwa penerapan metode berbasis aturan yang dipadukan dengan pembatasan jumlah percobaan login efektif dalam mendeteksi dan mengurangi risiko serangan brute-force di sistem berbasis web [5].

Mekanisme pengaturan login membatasi upaya masuk yang tidak sah dan memberikan perlindungan tambahan terhadap akses yang tidak diizinkan. Gabungan antara PSV dan pembatasan login diharapkan dapat secara signifikan meningkatkan keamanan autentikasi pengguna dalam sistem pemantauan pesanan berbasis web.

3. METODE PENELITIAN

Metode penelitian ini menguraikan tahapan dalam pengembangan sistem monitoring pemesanan produk cetak berbasis web serta metode analisis keamanan PSV yang diterapkan untuk meningkatkan keamanan autentikasi pengguna.

3.1. Metode Pengembangan Sistem



Gambar 1. Konsep Metode Prototype [9]

Metode pengembangan sistem yang diterapkan dalam penelitian ini adalah metode Prototype. Metode Prototype dipilih karena memungkinkan proses

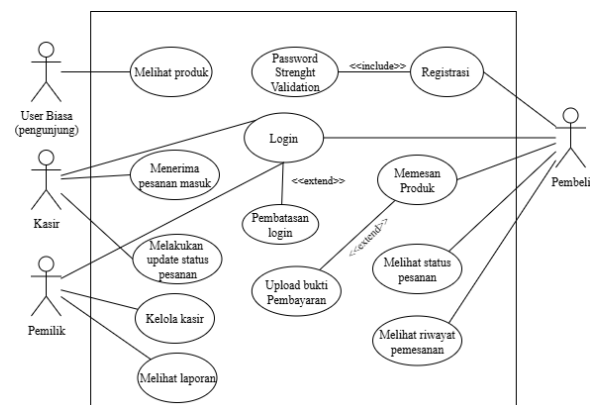
pengembangan sistem yang bersifat iteratif dengan partisipasi langsung dari pengguna di setiap tahap evaluasi. Metode ini memungkinkan sistem dikembangkan secara bertahap dan disesuaikan dengan kebutuhan pengguna berdasarkan umpan balik yang diberikan.

Berdasarkan Gambar 1, metode prototype terdiri dari beberapa tahap utama: mengenali kebutuhan pengguna, membuat prototype awal, menilai prototype, memperbaiki sistem, dan menerapkan sistem akhir. Tahapan ini dilakukan secara berulang untuk memastikan bahwa sistem yang dikembangkan sesuai dengan kebutuhan pengguna dan tujuan penelitian [9].

3.2. Perancangan Sistem Monitoring Pesanan

Sistem monitoring pesanan produk cetak dirancang untuk mengelola proses pemesanan, mencatat transaksi, dan memantau status pesanan secara terintegrasi. Sistem ini menawarkan otentikasi pengguna, pengelolaan data pesanan, dan informasi status pesanan yang dapat diakses sesuai dengan hak akses masing-masing pengguna.

Desain sistem ini mengutamakan kemudahan penggunaan, kejernihan alur proses, dan keamanan data pengguna. Sistem ini dirancang untuk mendukung proses bisnis percetakan dengan cara yang efektif dan efisien.



Gambar 2. Use case diagram sistem monitoring pesanan produk cetak

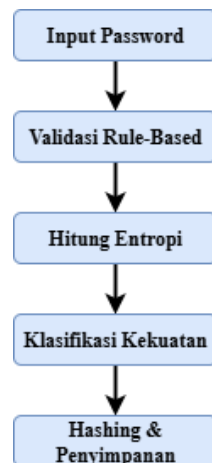
Berdasarkan Gambar 2, sistem pemantauan pesanan produk cetak melibatkan beberapa pihak: pengguna biasa, pembeli, kasir, dan pemilik. Pengguna biasa dapat melihat produk yang tersedia. Pembeli bisa mendaftar, masuk, memesan produk, mengunggah bukti pembayaran, serta memantau status dan riwayat pesanan. Selama proses pendaftaran, sistem menerapkan mekanisme PSV untuk memastikan bahwa kata sandi yang digunakan memenuhi kriteria keamanan.

Kasir bertugas untuk menerima pesan yang masuk dan memperbarui statusnya sesuai dengan proses produksi. Pemilik memiliki hak untuk mengelola data kasir dan melihat laporan pesanan. Seluruh proses otentikasi pengguna dimulai dengan

login, yang dilengkapi dengan mekanisme pembatasan masuk untuk mencegah akses yang tidak sah. Diagram ini menggambarkan hubungan antara aktor dan fungsi sistem secara terstruktur, sejalan dengan alur proses bisnis di sebuah usaha percetakan

3.3. Metode Analisis Keamanan Password

Analisis keamanan otentikasi pengguna dilakukan dengan menggunakan metode PSV. Tujuan dari metode ini adalah untuk memastikan kata sandi pengguna memenuhi standar keamanan minimum dan memiliki tingkat kompleksitas yang cukup.



Gambar 3. Diagram alur proses analisis password strength validation

Berdasarkan Gambar 3, proses analisis keamanan kata sandi dimulai ketika pengguna memasukkan kata sandi. Selanjutnya, sistem melakukan validasi berbasis aturan untuk memastikan bahwa kata sandi memenuhi kriteria minimum yang telah ditetapkan. Kata sandi yang lolos validasi kemudian dianalisis dengan menghitung entropi untuk mengukur kekuatannya secara matematis. Nilai entropi yang didapat digunakan untuk mengklasifikasikan kekuatan kata sandi menjadi kategori tertentu sebelum kata sandi tersebut diproses menggunakan mekanisme hashing dan disimpan dalam basis data.

3.4. Validasi Berbasis Aturan (Rule-Based Validation)

Validasi berbasis aturan diterapkan dengan cara menetapkan kriteria minimum untuk kata sandi, yang meliputi:

- Panjang karakter minimum
- Kombinasi huruf besar dan huruf kecil
- Penggunaan angka
- Penggunaan simbol

Kata sandi yang tidak memenuhi syarat panjang karakter minimum akan ditolak oleh sistem, dan pengguna akan diminta untuk membuat kata sandi baru yang sesuai dengan aturan yang telah ditentukan.

3.5. Validasi Berbasis Entropi (Entropy-Based Validation)

Validasi yang berdasarkan entropi digunakan untuk mengukur kekuatan kata sandi secara kuantitatif. Ukuran ini bergantung pada panjang kata sandi dan ukuran himpunan karakter yang digunakan, sehingga kata sandi dengan lebih banyak kombinasi karakter yang beragam memiliki nilai entropi yang lebih tinggi.

Rumus entropi yang digunakan ditampilkan dalam Persamaan (1).

$$H = L \times \log_2 (C) \quad (1)$$

Keterangan:

H = nilai entropi (bit)

L = panjang kata sandi

C = jumlah kemungkinan karakter (character set)

Dalam penelitian ini, penentuan jumlah karakter yang mungkin (C) didasarkan pada jenis karakter yang digunakan dalam kata sandi. Huruf kecil (a–z) terdiri dari 26 karakter, huruf kapital (A–Z) juga memiliki 26 karakter, angka (0–9) memiliki 10 karakter, dan simbol umum memiliki 32 karakter. Oleh karena itu, sebuah kata sandi yang memanfaatkan semua jenis karakter ini memiliki total 94 karakter yang mungkin.

Tabel 1. Kategori kekuatan password berdasarkan nilai entropi

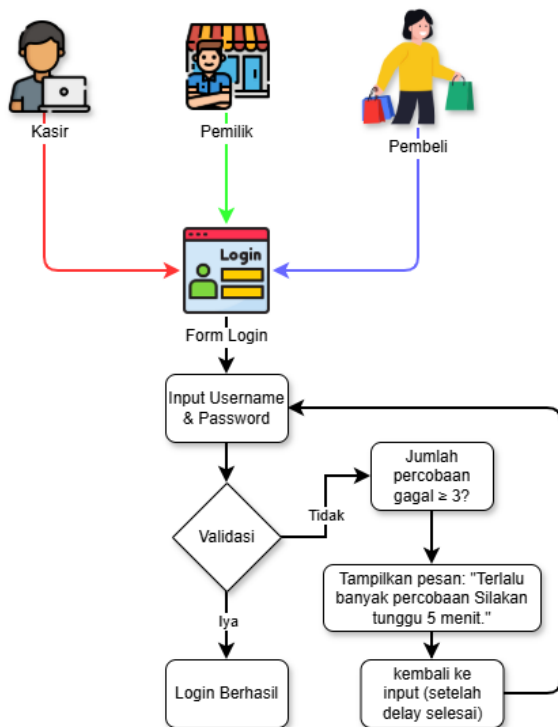
Nilai Entropi (bit)	Kategori Kekuatan
< 30	Sangat Lemah
30 – 50	Lemah
50 – 60	Sedang
≥ 60	Kuat

Klasifikasi kekuatan kata sandi berdasarkan nilai entropi dalam Tabel 1, mengacu pada penelitian sebelumnya yang membahas pengukuran kekuatan kata sandi dengan pendekatan entropi [10].

3.6. Mekanisme Pembatasan Login

Untuk menghindari serangan brute-force, sistem dilengkapi dengan fitur yang membatasi jumlah usaha masuk. Pengguna diizinkan untuk mencoba login maksimal hingga tiga kali. Jika batas ini terlampaui, sistem akan sementara menolak akses pengguna sebagai langkah perlindungan dari upaya login yang tidak sah.

Mekanisme pembatasan masuk ini berfungsi sebagai lapisan tambahan untuk menjaga keamanan agar sistem tidak terpapar pada upaya akses berulang yang dapat mengancam data pengguna.



Gambar 4. Alur Proses login dan pembatasan percobaan login

Berdasarkan Gambar 4, proses login dimulai dengan pengguna memasukkan nama pengguna dan kata sandi melalui formulir login. Sistem kemudian memeriksa apakah kredensial yang diberikan valid. Jika validasi berhasil, pengguna dapat mengakses sistem. Namun, jika validasi tidak berhasil, sistem akan menghitung jumlah upaya login yang gagal. Ketika jumlah upaya gagal melebihi batas yang telah ditentukan, sistem akan menampilkan pesan peringatan dan menerapkan jeda waktu sebelum pengguna dapat mencoba masuk kembali. Mekanisme ini bertujuan untuk mencegah serangan brute-force dan meningkatkan keamanan autentikasi pengguna.

3.7. Metode Pengujian Sistem

Pengujian sistem dilakukan dengan menggunakan metode Black Box Testing. Metode ini digunakan untuk menguji fungsionalitas sistem berdasarkan masukan dan keluaran tanpa memperhatikan susunan kode program. Fokus pengujian diarahkan pada fungsi inti sistem, termasuk otentikasi pengguna, penerapan Validasi Kekuatan Kata Sandi, mekanisme pembatasan login, dan fungsi pemantauan pesan.

4. HASIL DAN PEMBAHASAN

Bagian ini menunjukkan hasil uji coba serta pembahasan mengenai penerapan mekanisme keamanan dalam sistem pemantauan pemesanan produk cetak berbasis web serta penyajian tampilan aplikasi sebagai bentuk implementasi sistem. Pengujian difokuskan pada PSV dan pembatasan login guna memastikan sistem dapat meningkatkan

keamanan autentikasi pengguna tanpa mengganggu fungsi sistem.

4.1. Hasil Pengujian Password Strength Validation

Pengujian PSV dilakukan untuk menilai kemampuan sistem dalam memverifikasi dan mengklasifikasikan kekuatan kata sandi selama proses pendaftaran akun. Uji coba diterapkan pada akun pembeli dan kasir untuk memastikan bahwa mekanisme keamanan berfungsi secara konsisten di seluruh peran pengguna.

Hasil uji menunjukkan bahwa sistem dapat mengklasifikasikan kekuatan kata sandi berdasarkan kombinasi karakter yang digunakan. Kata sandi yang terdiri dari karakter sederhana dikategorikan sebagai sangat lemah atau lemah, sedangkan kata sandi yang memiliki kombinasi huruf kapital, huruf kecil, angka, dan simbol dikategorikan sebagai sedang hingga kuat. Ringkasan hasil uji Validasi Kekuatan Kata Sandi ditampilkan dalam Tabel 2.

Tabel 2. Hasil pengujian password strength validation

Input Kata Sandi	Hasil Validasi Sistem	Kategori	Status
123456	Tidak memenuhi kriteria	Sangat lemah	Sesuai
123456789	Memenuhi sebagian kriteria	Lemah	Sesuai
Pemuda123	Memenuhi sebagian besar kriteria	Sedang	Sesuai
Admin!@1234	Memenuhi seluruh kriteria	Kuat	Sesuai

Sebagai contoh, berdasar pada hasil pengujian sistem, kata sandi Admin!@1234 yang memiliki panjang $L = 10$ dan menggunakan kombinasi huruf kapital, huruf kecil, angka, dan simbol (sehingga $C = 94$) menghasilkan nilai entropi yang dihitung dengan menggunakan rumus (2).

$$H = 10 \times \log_2(94) \approx 65,5 \text{ bit.} \quad (2)$$

Berdasarkan kategori kekuatan kata sandi yang digunakan, nilai ini termasuk dalam kategori kuat. Hasil ini menunjukkan bahwa mekanisme PSV dapat menghitung dan mengklasifikasikan kekuatan kata sandi secara kuantitatif berdasarkan kompleksitas karakter yang digunakan.

4.2. Hasil Pengujian Pembatasan Login

Pengujian pembatasan login dilakukan untuk mengevaluasi seberapa efektif sistem dalam mencegah upaya login yang tidak sah. Pengujian ini dilakukan pada akun pelanggan dan kasir, dengan situasi yang melibatkan pengisian kredensial yang salah secara berturut-turut.

Hasil uji menunjukkan bahwa sistem membatasi jumlah percobaan login yang gagal hingga maksimum

tiga kali. Apabila batas ini terlampaui, sistem secara otomatis menolak akses dan menerapkan jeda waktu sebelum pengguna dapat mencoba untuk login lagi. Ringkasan dari hasil uji pembatasan login ditampilkan dalam Tabel 3.

Tabel 3. Hasil pengujian pembatasan login

No	Skenario Pengujian	Percobaan Login	Respons Sistem	Status
1	Login salah berulang	> 3 kali	Akses diblokir sementara	Sesuai
2	Login benar saat masa blokir	—	Akses ditolak	Sesuai

Berdasarkan Tabel 3, sistem pembatasan login berfungsi sesuai dengan skenario uji yang telah ditetapkan. Ketika seorang pengguna mencoba untuk masuk dengan informasi yang salah lebih dari tiga kali, sistem secara otomatis menanggguhkan akses pengguna untuk sementara waktu. Selain itu, jika pengguna mencoba masuk kembali dengan informasi yang benar selama periode penangguhan, sistem tetap akan menolak akses sampai waktu yang ditentukan berakhir. Temuan ini menunjukkan bahwa sistem pembatasan login efektif dalam mencegah upaya akses tidak sah yang berulang dan berfungsi sebagai langkah keamanan tambahan dalam proses autentikasi pengguna.

4.3. Pembahasan Keamanan Sistem

Berdasarkan hasil pengujian, penerapan PSV dan pembatasan login memberikan dampak positif dalam meningkatkan keamanan autentikasi pada sistem pemantauan pemesanan produk cetak berbasis web. PSV berfungsi untuk meningkatkan kesadaran pengguna, baik pembeli maupun kasir, tentang pentingnya menggunakan kata sandi yang kuat melalui mekanisme validasi dan umpan balik yang informatif.

Pembatasan login berfungsi sebagai lapisan tambahan keamanan untuk mencegah akses yang tidak sah melalui upaya login yang berulang. Pengujian pada akun kasir merupakan nilai tambah dalam penelitian ini, mengingat peran penting kasir dalam pengelolaan pesanan dan transaksi. Oleh karena itu, sistem yang dikembangkan tidak hanya mendukung pemantauan pesanan yang efektif tetapi juga menyediakan perlindungan keamanan autentikasi yang lebih baik dan cocok untuk diterapkan di skala usaha mikro, kecil, dan menengah (UMKM).

4.4. Tampilan Aplikasi

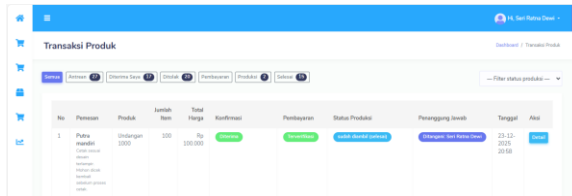
Bagian ini menyajikan berbagai antarmuka untuk aplikasi pemantauan pesanan produk cetak berbasis web yang telah dikembangkan. Antarmuka aplikasi ini dirancang untuk menunjukkan penerapan fitur-fitur utama sistem, khususnya mengenai aspek keamanan autentikasi pengguna dan fungsi pemantauan pesanan.

Gambar 5. Tampilan halaman registrasi pengguna

Berdasarkan Gambar 5, menampilkan halaman pendaftaran pengguna dalam aplikasi pemantauan pesanan. Halaman ini menerapkan mekanisme PSV, yang menilai kekuatan kata sandi berdasarkan kombinasi karakter yang digunakan. Sistem memberikan umpan balik langsung kepada pengguna terkait dengan kekuatan kata sandi yang telah dimasukkan.

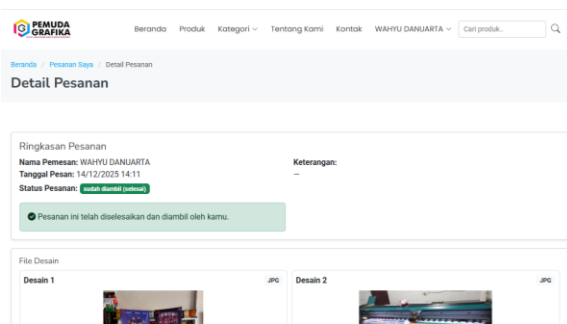
Gambar 6. Tampilan Halaman Login

Berdasarkan Gambar 6, memperlihatkan halaman login, yang mencakup batasan pada percobaan login. Aplikasi ini membatasi jumlah percobaan login yang gagal hingga tiga kali. Jika batas ini terlampaui, sistem akan secara sementara menolak akses selama lima menit sebagai langkah pencegahan terhadap serangan brute-force.



Gambar 7. Tampilan transaksi produk kasir

Berdasarkan Gambar 7, menunjukkan halaman transaksi produk kasir yang digunakan untuk memantau data pesanan produk cetak pengguna. Informasi status pesanan ditampilkan dengan cara yang teratur, sehingga memudahkan kasir bisnis untuk memantau serta mengelola pesanan dengan efisien.



Gambar 8. Tampilan detail status pesanan pengguna

Berdasarkan Gambar 8, memperlihatkan halaman rincian pesanan yang dapat diakses oleh pengguna. Halaman ini menampilkan informasi status pesanan dengan jelas, sehingga pengguna dapat melihat tahap-tahap terkini dari proses pesanan tanpa harus datang langsung ke lokasi pencetakan.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil uji dan diskusi yang telah dilakukan, dapat disimpulkan bahwa penerapan PSV dalam sistem pemantauan pesanan produk cetak berbasis web dapat dengan baik mengklasifikasikan kekuatan kata sandi berdasarkan kombinasi karakter dan nilai entropi, serta memberikan umpan balik yang mendorong penggunaan kata sandi yang lebih aman pada akun pembeli dan kasir. Selain itu, mekanisme pembatasan login terbukti efektif dalam mengurangi upaya login berulang yang tidak sah, sehingga meningkatkan perlindungan terhadap serangan brute force yang mungkin terjadi. Dengan demikian, sistem yang dikembangkan tidak hanya mendukung efisiensi pemantauan pesanan tetapi juga meningkatkan keamanan otentikasi pengguna dan cocok untuk diterapkan pada skala usaha mikro, kecil, dan menengah. Untuk pengembangan selanjutnya,

penelitian dapat mempertimbangkan penerapan mekanisme keamanan tambahan seperti otentikasi multi-faktor atau analisis pola login untuk meningkatkan ketahanan sistem terhadap ancaman keamanan yang lebih kompleks.

DAFTAR PUSTAKA

- [1] K. S. F. A. Sania Yuni, "Rancang Bangun Sistem Pemesanan Produk Jasa Percetakan Berbasis Web Di CV. Fajar Advertising," *Jurnal Media Infotama*, vol. 20, 2024, Accessed: Jun. 01, 2025. [Online]. Available: <https://jurnal.unived.ac.id/index.php/jmi/article/view/6374/4847>
- [2] Hasbillah, Muhammad rifqi aji pratama, Niken Tri Desnawati, Dwi Vernanda, and Rian Piarna, "Sistem Informasi Pemesanan Digital Printing Berbasis Web untuk Optimalisasi Layanan dan Manajemen Pemesanan," *Inventor: Jurnal Inovasi dan Tren Pendidikan Teknologi Informasi*, vol. 3, no. 1, pp. 25–35, Feb. 2025, doi: 10.37630/inventor.v3i1.2215.
- [3] Yamin.M, Malethi Tifani Thresia, Monica, Jodhika, and Natali Silvina, "EVALUASI RISIKO PADA PENGGUNAAN PASSWORD YANG LEMAH: ANALISIS KASUS PENGGUNAAN PASSWORD UMUM," *Jurnal Ilmiah Multidisiplin Ilmu Komputer*, vol. 1, pp. 41–48, Aug. 2023, Accessed: Jul. 01, 2025. [Online]. Available: <https://geloraciptanusantara.org/jurnal/index.php/jimik/article/view/112/50>
- [4] Verizon, "2025 Data Breach Investigations Report," 2025. Accessed: Jul. 24, 2025. [Online]. Available: <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>
- [5] K. Mubarak and Moh. A. Romli, "Implementasi Metode Rule Based dalam Mendeteksi Serangan Brute Force pada Owncloud," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 1, pp. 159–167, Dec. 2024, doi: 10.57152/malcom.v5i1.1701.
- [6] Jamaluddin, R. Hajriyanti, and Bahrani, "Sistem Informasi Pemesanan Produk Percetakan Berbasis Web pada CV. Page Grafika Banda Aceh," *Computer Journal*, vol. 1, no. 1, pp. 23–32, Feb. 2023, doi: 10.58477/cj.v1i1.32.
- [7] B. A. Suburdjati, F. Nindita Iswari, and W. K. Jonathan, "Aplikasi Pengukuran Kekuatan dan Rekomendasi Password Berdasarkan Input Pengguna dengan Metode Entropi," *JURNAL INFORMATIKA*, vol. 3, no. 2, Sep. 2024, [Online]. Available: <https://jurnal.uniraya.ac.id/index.php/JI>
- [8] A. E. Febrianisa, I. Oktaviani, and W. Wijianto, "Sistem Informasi Monitoring Data Pesanan Customer Berbasis Website Pada JeeDee Advertising," *Journal Computer Science and*

- Information Systems : J-Cosys*, vol. 4, no. 2, Aug. 2024, doi: 10.53514/jco.v4i2.521.
- [9] F. Putri, A. Koko, and A. Yayuri, "Rancang Bangun Sistem Informasi Inventaris menggunakan Metode Prototype pada SMK Muhammadiyah 3 Pekanbaru," *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI V*, vol. 7, no. 1, pp. 143–153, 2024, Accessed: Jul. 03, 2025. [Online]. Available: <https://ejournal.sisfokomtek.org/index.php/jikom/article/view/2852/1850>
- [10] N. A. Chowdhury, "Analyzing Password Strength: A Combinatorial Entropy Approach," 2024. doi: 10.5281/zenodo.10487696