LAPORAN PENANGANAN INSIDEN KEAMANAN
(INCIDENT HANDLING REPORT)
KASUS BRUTE FORCE LOGIN ATTACK PADA APLIKASI WEB

PROGRAM REKAYASA KEAMANAN SIBER

POLITEKNIK BHAKTI SEMESTA

2025

RINGKASAN EKSEKUTIF

Laporan ini menyajikan hasil simulasi penanganan insiden keamanan (incident handling) terhadap kasus brute force login attack pada sebuah aplikasi web sederhana berbasis Flask. Insiden terjadi akibat adanya percobaan login tidak sah secara berulang dalam waktu singkat pada endpoint autentikasi, yang terdeteksi melalui peningkatan signifikan log failed login attempt serta lonjakan trafik dan penggunaan sumber daya sistem.

Deteksi insiden dilakukan dengan mengorelasikan data log aplikasi yang dianalisis menggunakan sistem logging terpusat berbasis ELK Stack dengan metrik performa sistem yang dipantau melalui Prometheus dan Grafana. Hasil analisis menunjukkan bahwa aktivitas tersebut merupakan upaya akses tidak sah (Unauthorized Access Attempt) dengan tingkat keparahan menengah dan tidak mengakibatkan keberhasilan login maupun kebocoran data.

Penanganan insiden dilakukan secara bertahap sesuai prinsip incident handling, meliputi isolasi sumber serangan melalui pemblokiran alamat IP dan penerapan rate limiting, pembersihan akar permasalahan dengan penambahan kontrol keamanan pada endpoint login, serta pemulihan layanan hingga kembali ke kondisi operasional normal. Seluruh proses penanganan berhasil diselesaikan pada hari yang sama tanpa menimbulkan gangguan layanan berkepanjangan.

Hasil simulasi ini menegaskan pentingnya penerapan kontrol keamanan dasar, monitoring terpusat, serta mekanisme peringatan dini dalam menjaga keamanan aplikasi web. Dokumentasi dan evaluasi pasca-insiden juga menjadi faktor penting untuk meningkatkan kesiapan sistem dalam menghadapi ancaman keamanan di masa mendatang dan mendukung peningkatan keamanan secara berkelanjutan.

LATAR BELAKANG

Seiring berkembangnya teknologi informasi, semakin banyak layanan yang diakses melalui aplikasi berbasis web. Aplikasi-aplikasi tersebut umumnya menyediakan fitur autentikasi sebagai gerbang utama bagi pengguna. Namun, mekanisme autentikasi juga menjadi target utama serangan siber, khususnya brute force login attack, yang dilakukan secara otomatis dan masif dalam waktu singkat.

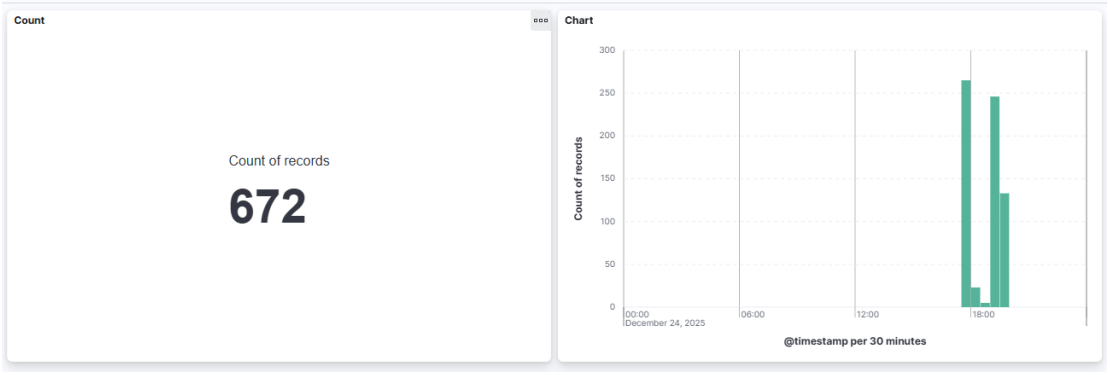
Pada banyak kasus, aplikasi web sederhana masih dikembangkan tanpa penerapan kontrol keamanan yang memadai, seperti pembatasan percobaan login, pencatatan aktivitas yang detail, serta pemantauan performa sistem secara real-time. Kondisi ini menyebabkan serangan dapat berlangsung cukup lama sebelum terdeteksi, sehingga berpotensi menimbulkan dampak berupa penurunan kinerja sistem, gangguan layanan, hingga risiko kebocoran data. Kurangnya kesiapan dalam menangani insiden turut memperbesar potensi kerugian yang ditimbulkan.

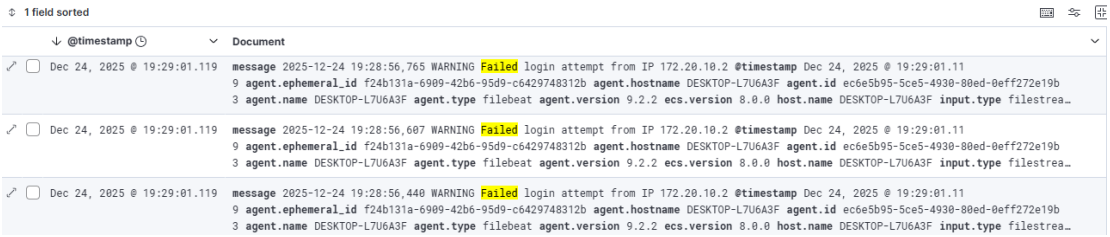
Oleh karena itu, diperlukan penerapan proses penanganan insiden keamanan yang terstruktur dan terdokumentasi dengan baik. Dengan memanfaatkan sistem logging terpusat dan monitoring performa, aktivitas mencurigakan dapat diidentifikasi lebih cepat dan dianalisis secara akurat. Simulasi ini dilakukan untuk memberikan gambaran nyata mengenai pentingnya monitoring, respons insiden, dan evaluasi berkelanjutan dalam menjaga keamanan serta stabilitas sistem aplikasi.

RINGKASAN INSIDEN

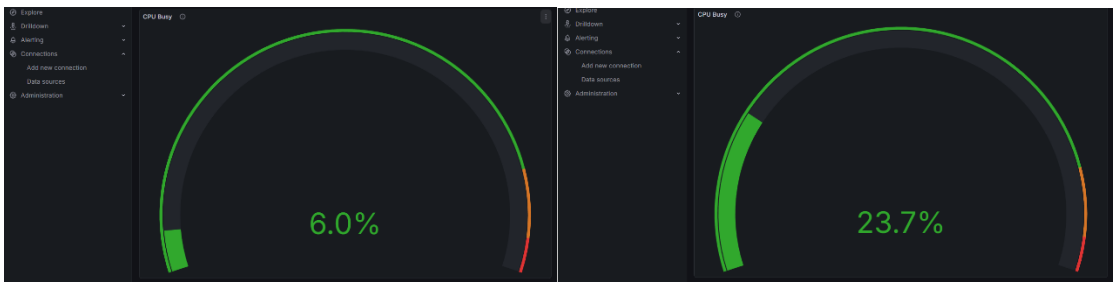
Insiden keamanan yang terjadi berupa brute force login attack yang teridentifikasi melalui peningkatan signifikan jumlah percobaan login gagal dalam waktu singkat dari satu alamat IP yang sama. Pola ini menunjukkan adanya upaya sistematis untuk menebak kredensial pengguna secara berulang. Sistem mendeteksi insiden melalui:

1. Peningkatan signifikan log failed login attempt:





2. Lonjakan trafik dan penggunaan sumber daya system



Sebelum Lonjakan Ketika Lonjakan

Deteksi insiden dilakukan melalui dua indikator utama, yaitu meningkatnya log failed login attempt pada aplikasi serta lonjakan trafik dan penggunaan sumber daya sistem pada komponen autentikasi. Berdasarkan hasil analisis, insiden diklasifikasikan sebagai upaya akses tidak sah (Unauthorized Access Attempt) dengan tingkat keparahan menengah (Medium). Insiden berhasil dikendalikan dan ditangani tanpa menimbulkan kebocoran data.

WAKTU DAN KRONOLOGI KEJADIAN

Waktu Kejadian

- Tanggal : 25 Desember 2025
- Rentang Waktu : 09:00 – 12:00
- Status : Insiden berhasil dideteksi dan ditangani pada hari yang sama

Kronologi Kejadian

Insiden diawali dengan diterimanya sejumlah permintaan login tidak valid pada endpoint autentikasi aplikasi yang terjadi secara berulang dalam interval waktu singkat dan melebihi pola penggunaan normal. Setiap percobaan login gagal dicatat oleh sistem logging aplikasi, sehingga dalam waktu singkat jumlah log failed login attempt meningkat secara signifikan dan menunjukkan pola yang konsisten dari alamat IP yang sama.

Secara bersamaan, sistem monitoring menunjukkan adanya peningkatan jumlah request dan aktivitas sistem yang tidak wajar, khususnya pada komponen yang menangani proses login. Korelasi antara data log aplikasi dan metrik sistem mengonfirmasi bahwa aktivitas tersebut merupakan percobaan akses tidak sah berupa brute force login attack. Setelah insiden dipastikan, proses respons insiden segera diinisiasi sesuai prosedur incident handling untuk menghentikan serangan dan membatasi dampak lebih lanjut.

DAMPAK TERHADAP SISTEM

Insiden brute force login memberikan dampak terhadap aspek operasional dan keamanan sistem, meskipun tidak menyebabkan kompromi data secara langsung. Dampak utama yang teridentifikasi adalah meningkatnya beban pada komponen autentikasi akibat tingginya jumlah permintaan login yang tidak valid dalam waktu singkat.

Selain itu, insiden ini menimbulkan potensi gangguan terhadap ketersediaan layanan. Apabila serangan dibiarkan berlangsung lebih lama, sistem berisiko mengalami penurunan performa atau ketidakstabilan layanan yang dapat memengaruhi pengguna sah. Dari sisi keamanan, insiden ini mengindikasikan lemahnya kontrol proteksi pada endpoint login yang berpotensi dimanfaatkan untuk memperoleh akses tidak sah.

ROOT CAUSE (AKAR PENYEBAB)

Berdasarkan hasil analisis, akar penyebab insiden berasal dari tidak diterapkannya kontrol keamanan dasar pada endpoint autentikasi. Endpoint login dapat diakses tanpa pembatasan jumlah percobaan login, sehingga memungkinkan terjadinya percobaan autentikasi berulang dari sumber yang sama.

Selain itu, sistem monitoring belum dilengkapi dengan mekanisme peringatan otomatis (alerting) untuk mendeteksi pola anomali sejak tahap awal. Akibatnya, deteksi insiden masih bergantung pada analisis manual setelah aktivitas mencurigakan terjadi. Konfigurasi aplikasi yang masih bersifat default tanpa hardening tambahan juga turut berkontribusi terhadap terjadinya insiden ini.

TINDAKAN YANG DIAMBIL

Tindakan penanganan insiden dilakukan secara bertahap sesuai dengan prinsip incident handling untuk memastikan dampak insiden dapat dikendalikan dan sistem dapat dipulihkan dengan aman.

1. Containment (Isolasi Insiden)

   Langkah isolasi dilakukan dengan membatasi sumber serangan agar aktivitas mencurigakan tidak berlanjut. Pemblokiran sementara terhadap alamat IP yang teridentifikasi sebagai sumber serangan diterapkan melalui mekanisme firewall sistem operasi. Selain itu, diterapkan pembatasan jumlah percobaan login pada level aplikasi melalui mekanisme rate limiting untuk mencegah terjadinya brute force berulang.
2. Eradication (Pembersihan Akar Masalah)

   Setelah serangan berhasil dihentikan, dilakukan pembersihan terhadap akar permasalahan dengan menutup celah keamanan pada endpoint login. Aplikasi diperbarui dengan menambahkan kontrol akses yang lebih ketat dan memperbarui dependency ke versi terbaru untuk mengurangi risiko eksploitasi kerentanan yang telah diketahui. Karena tidak terdapat sistem manajemen akun pengguna yang sesungguhnya, proses penghapusan akun attacker dan reset kredensial dilakukan secara konseptual sebagai bagian dari simulasi praktik terbaik.
3. Recovery (Pemulihan Sistem)

   Pada tahap pemulihan, layanan aplikasi dikembalikan ke kondisi operasional normal setelah memastikan tidak ada konfigurasi darurat yang tertinggal. Performa sistem dipantau kembali melalui dashboard monitoring untuk memastikan penggunaan sumber daya telah kembali stabil. Monitoring log aplikasi juga dilakukan secara intensif untuk memastikan tidak terdapat aktivitas mencurigakan lanjutan.

REKOMENDASI PENCEGAHAN

Berdasarkan hasil analisis dan penanganan insiden keamanan yang terjadi, beberapa rekomendasi disusun sebagai langkah pencegahan dan peningkatan keamanan sistem di masa mendatang. Rekomendasi ini bertujuan untuk meminimalkan risiko terulangnya insiden serupa serta meningkatkan kesiapan sistem dalam menghadapi potensi ancaman keamanan.

Pertama, perlu diterapkan kontrol keamanan yang lebih ketat pada endpoint sensitif, khususnya pada mekanisme autentikasi. Penerapan pembatasan percobaan login (rate limiting), validasi akses berbasis alamat IP, serta mekanisme penguncian sementara setelah sejumlah percobaan gagal dapat secara signifikan mengurangi risiko brute force login.

Kedua, sistem monitoring perlu ditingkatkan dari pendekatan reaktif menjadi proaktif. Hal ini dapat dilakukan dengan mengaktifkan fitur peringatan otomatis (alerting) berbasis log dan metrik, sehingga anomali seperti lonjakan login gagal atau peningkatan penggunaan sumber daya dapat terdeteksi dan ditangani lebih cepat tanpa menunggu analisis manual.

Ketiga, diperlukan proses pemeliharaan sistem yang berkelanjutan melalui pembaruan dependency aplikasi dan hardening konfigurasi secara berkala. Pembaruan ini bertujuan untuk menutup celah keamanan yang berasal dari kerentanan versi lama serta memastikan sistem tetap selaras dengan praktik keamanan terkini.

Keempat, dokumentasi prosedur penanganan insiden perlu diperbarui dan disosialisasikan secara rutin. Dokumentasi yang jelas akan membantu memastikan bahwa setiap insiden dapat ditangani secara konsisten, terstruktur, dan efisien oleh pihak yang bertanggung jawab.

KESIMPULAN

Berdasarkan keseluruhan proses yang telah dilakukan, insiden keamanan berupa percobaan brute force login pada aplikasi web dapat dideteksi, ditangani, dan dipulihkan dengan baik melalui penerapan mekanisme monitoring dan respons insiden yang terstruktur. Insiden ini teridentifikasi melalui korelasi antara log aplikasi yang mencatat percobaan login gagal berulang dan metrik sistem yang menunjukkan peningkatan aktivitas tidak normal.

Penanganan insiden dilakukan secara bertahap, dimulai dari isolasi sumber serangan, pembersihan akar permasalahan, hingga pemulihan layanan ke kondisi operasional normal. Meskipun tidak ditemukan indikasi kebocoran data atau keberhasilan akses tidak sah, insiden ini mengungkap pentingnya penerapan kontrol keamanan dasar sejak tahap awal pengembangan aplikasi.

Secara keseluruhan, penerapan monitoring terpusat, analisis log, serta pemantauan metrik sistem terbukti efektif dalam mendukung proses incident handling. Pengalaman dari insiden ini menjadi pembelajaran penting bahwa kesiapan sistem, deteksi dini, dan respons yang cepat merupakan faktor kunci dalam menjaga keamanan dan stabilitas layanan aplikasi.