LAPORAN PENANGANAN INSIDEN KEAMANAN

(Incident Handling Report)

Kasus: *Brute Force Login Attack* pada Aplikasi Web

Disusun Oleh:

Surya Aditia Febriyan | 88032023007

POLITEKNIK BHAKTI SEMESTA

REKAYASA KEAMANAN SIBER

2025

PERNYATAAN KERAHASIAAN

Dokumen ini berisi informasi terkait insiden keamanan sistem dan hanya digunakan untuk kepentingan analisis internal, pembelajaran, dan peningkatan keamanan. Dilarang mendistribusikan dokumen ini tanpa izin pihak terkait.

DAFTAR ISI

RINGKASAN EKSEKUTIF

Keamanan aplikasi dan infrastruktur digital merupakan aspek krusial yang harus dijaga secara berkelanjutan oleh setiap organisasi. Seiring meningkatnya ketergantungan terhadap sistem berbasis aplikasi, risiko terjadinya insiden keamanan seperti akses tidak sah, penyalahgunaan sistem, dan gangguan layanan juga semakin tinggi. Berdasarkan praktik terbaik penanganan insiden keamanan yang mengacu pada standar *NIST SP 800-61 (Computer Security Incident Handling Guide)*, setiap organisasi diwajibkan memiliki kemampuan untuk mendeteksi, merespons, dan memulihkan sistem dari insiden keamanan secara cepat dan terstruktur.

Laporan ini disusun untuk mendokumentasikan temuan insiden keamanan berupa serangan brute force pada mekanisme login aplikasi web, yang terdeteksi melalui sistem *logging* dan *monitoring* dalam lingkungan DevSecOps. Insiden ini ditandai dengan adanya percobaan login gagal secara berulang dalam waktu singkat dari alamat IP yang sama, yang berpotensi mengancam kerahasiaan dan integritas sistem apabila tidak segera ditangani.

Tujuan utama dari penyusunan laporan insiden ini adalah untuk memberikan gambaran menyeluruh mengenai kronologi kejadian, dampak insiden, akar penyebab, serta langkah-langkah penanganan yang telah dilakukan. Melalui proses identifikasi dan analisis log aplikasi serta metrik sistem, insiden berhasil dideteksi pada tahap awal sehingga tidak berkembang menjadi pelanggaran keamanan yang lebih serius, seperti pengambilalihan akun atau kebocoran data.

Sebagai bagian dari proses penanganan insiden, dilakukan serangkaian tindakan yang mencakup identifikasi insiden melalui analisis log terpusat, isolasi sumber serangan dengan mekanisme pemblokiran sementara, pembersihan akar penyebab insiden, serta pemulihan layanan agar kembali beroperasi secara normal. Seluruh tindakan ini dilaksanakan dengan tujuan untuk meminimalkan dampak operasional dan memastikan keberlangsungan layanan aplikasi.

Hasil dari penanganan insiden ini disajikan dalam bentuk laporan yang terstruktur dan mudah dipahami, mencakup analisis risiko serta rekomendasi perbaikan yang bersifat teknis dan prosedural. Diharapkan laporan ini dapat menjadi dasar bagi organisasi dalam meningkatkan kesiapan *incident handling*, memperkuat kontrol keamanan aplikasi, serta

mengintegrasikan keamanan secara lebih efektif ke dalam proses DevSecOps, guna mencegah terulangnya insiden serupa di masa mendatang.

LATAR BELAKANG INSIDEN

Aplikasi web dan infrastruktur digital merupakan aset penting yang mendukung operasional bisnis. Seiring meningkatnya penggunaan sistem berbasis aplikasi, risiko terjadinya insiden keamanan juga semakin tinggi, khususnya pada komponen kritis seperti mekanisme login. Endpoint autentikasi sering menjadi target serangan karena berfungsi sebagai pintu masuk utama ke dalam sistem.

Salah satu ancaman yang umum terjadi adalah serangan brute force login, yaitu upaya akses tidak sah dengan mencoba berbagai kombinasi kredensial secara berulang. Apabila tidak didukung dengan kontrol keamanan yang memadai, serangan ini berpotensi mengganggu operasional layanan dan membuka peluang penyalahgunaan akses.

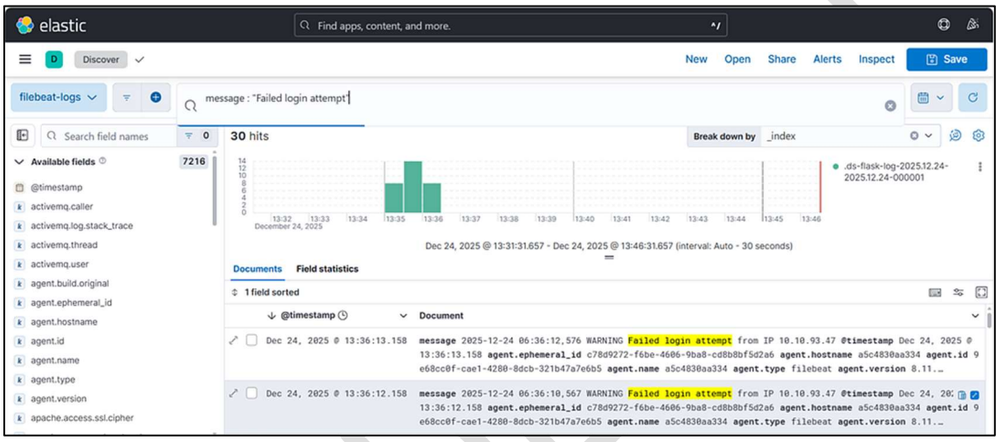
Dalam lingkungan DevSecOps, deteksi dini dan respons cepat terhadap insiden menjadi faktor kunci untuk meminimalkan dampak terhadap sistem dan bisnis. Oleh karena itu, logging dan monitoring yang terintegrasi digunakan untuk mengidentifikasi aktivitas mencurigakan secara real-time. Insiden yang dibahas dalam laporan ini menunjukkan pentingnya kesiapan sistem dalam mendeteksi dan menangani ancaman keamanan sejak tahap awal sebelum berkembang menjadi insiden yang lebih serius.

RINGKASAN INSIDEN

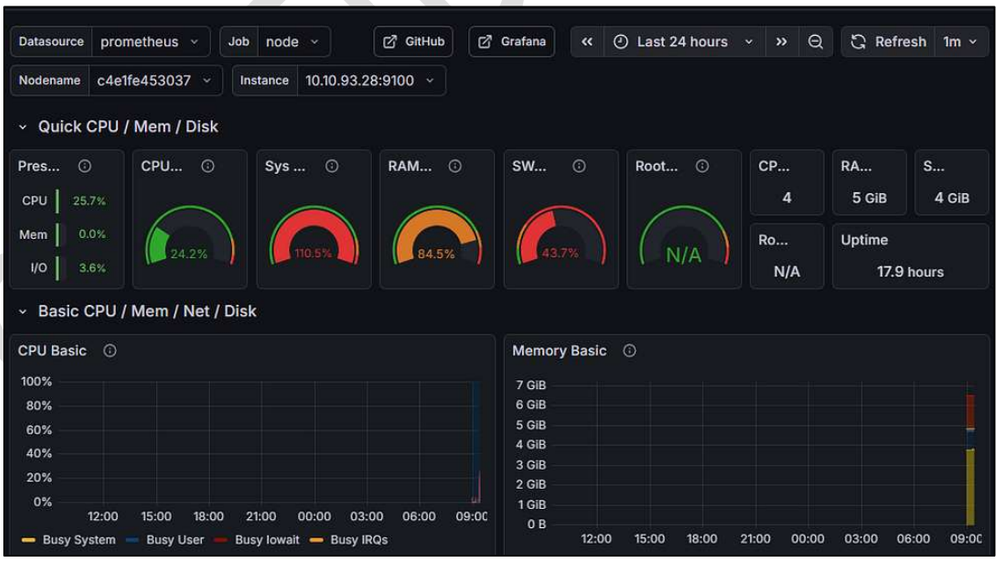
Insiden yang terjadi adalah percobaan login tidak sah secara berulang (*brute force attack*) terhadap endpoint login aplikasi berbasis Flask. Serangan dilakukan dengan mengirimkan permintaan login secara otomatis menggunakan kredensial yang salah dalam jumlah besar dan waktu singkat.

Sistem mendeteksi insiden melalui:

1. Peningkatan signifikan log failed login attempt:



2. Lonjakan trafik dan penggunaan sumber daya sistem



Insiden ini dikategorikan sebagai:

Jenis Insiden : Unauthorized Access Attempt

Tingkat Keparahan : Medium

Status : Terkendali dan Ditangani

WAKTU DAN KRONOLOGI KEJADIAN

Insiden keamanan teridentifikasi selama periode operasional sistem melalui mekanisme monitoring dan logging yang telah diterapkan. Waktu kejadian dicatat berdasarkan hasil observasi log aplikasi dan metrik sistem, dengan fokus pada urutan peristiwa utama yang relevan terhadap penanganan insiden.

Waktu Kejadian:

Tanggal : 24 Desember 2025

Rentang Waktu : 13:30 – 15:00

Status : Insiden berhasil dideteksi dan ditangani pada hari yang sama

Kronologi Kejadian:

1. Awal Aktivitas Mencurigakan

   Sistem menerima sejumlah permintaan login yang tidak valid ke endpoint autentikasi aplikasi. Permintaan tersebut terjadi secara berulang dengan interval waktu yang singkat.

2. Pencatatan oleh Sistem Logging

   Aplikasi secara otomatis mencatat setiap percobaan login gagal ke dalam log aplikasi. Dalam periode singkat, jumlah log *failed login attempt* meningkat secara signifikan dan menunjukkan pola yang konsisten dari sumber alamat IP yang sama.

3. Deteksi Anomali oleh Monitoring Sistem monitoring menampilkan peningkatan jumlah request dan aktivitas sistem yang tidak sesuai dengan pola penggunaan normal, khususnya pada komponen yang menangani proses login.

4. Konfirmasi Insiden

   Berdasarkan korelasi antara data log dan metrik sistem, aktivitas tersebut dikonfirmasi sebagai insiden keamanan berupa percobaan akses tidak sah (*brute force login*), bukan kesalahan konfigurasi atau gangguan teknis biasa.

5. Inisiasi Respons Insiden

   Setelah insiden dikonfirmasi, proses penanganan insiden segera diaktifkan sesuai prosedur *incident handling*, dengan tujuan menghentikan aktivitas mencurigakan dan mencegah potensi eskalasi.

DAMPAK INSIDEN

Insiden keamanan yang teridentifikasi memberikan dampak pada beberapa aspek sistem dan operasional. Meskipun tidak menyebabkan gangguan layanan secara langsung, insiden ini tetap memiliki implikasi yang perlu menjadi perhatian dari sisi keamanan, operasional, dan bisnis.

Dampak terhadap Keamanan Sistem

Percobaan brute force login menunjukkan adanya upaya akses tidak sah terhadap mekanisme autentikasi aplikasi. Jika aktivitas tersebut tidak terdeteksi dan dihentikan, terdapat risiko terjadinya pengambilalihan akun pengguna yang dapat berujung pada penyalahgunaan hak akses. Kondisi ini berpotensi mengancam kerahasiaan data serta integritas sistem secara keseluruhan.

Dampak terhadap Ketersediaan Layanan

Lonjakan permintaan login yang tidak valid menyebabkan peningkatan beban pada komponen aplikasi yang menangani autentikasi. Dalam skala yang lebih besar atau durasi yang lebih lama, aktivitas serupa berpotensi menurunkan performa layanan dan dapat berkembang menjadi gangguan ketersediaan layanan (service degradation).

Dampak terhadap Operasional

Insiden ini memerlukan intervensi tim untuk melakukan analisis log, pemantauan sistem, serta penerapan langkah mitigasi. Walaupun tidak berdampak pada downtime, insiden tersebut tetap menambah beban operasional dan menunjukkan perlunya mekanisme pencegahan yang lebih proaktif.

Dampak terhadap Risiko Bisnis

Dari sudut pandang bisnis, insiden brute force login yang tidak tertangani dapat berdampak pada kepercayaan pengguna dan reputasi layanan. Insiden ini juga menyoroti potensi risiko kepatuhan terhadap kebijakan keamanan internal apabila kontrol pengamanan dasar tidak diterapkan secara konsisten.

ANALISIS AKAR PENYEBAB *(ROOT CAUSE)*

Berdasarkan hasil analisis log aplikasi, observasi metrik sistem, serta evaluasi terhadap konfigurasi keamanan yang diterapkan, insiden *brute force login* terjadi akibat kelemahan pada mekanisme pengamanan endpoint autentikasi. Akar penyebab utama insiden diidentifikasi sebagai tidak adanya kontrol pembatasan percobaan login secara efektif.

Secara lebih rinci, faktor-faktor yang berkontribusi terhadap terjadinya insiden meliputi:

1. Tidak Diterapkannya Rate Limiting pada Endpoint Login

   Endpoint login menerima permintaan autentikasi tanpa pembatasan jumlah percobaan dalam periode waktu tertentu. Kondisi ini memungkinkan pihak tidak sah melakukan percobaan login secara berulang dalam waktu singkat tanpa hambatan berarti.

2. Tidak Adanya Mekanisme Penguncian Akun (Account Lockout)

   Sistem tidak melakukan penguncian sementara terhadap akun setelah sejumlah percobaan login gagal. Hal ini meningkatkan peluang keberhasilan brute force, terutama jika kredensial lemah digunakan.

3. Proteksi Jaringan yang Masih Bersifat Reaktif

   Pemblokiran alamat IP dilakukan setelah insiden terdeteksi, bukan sebagai mekanisme pencegahan otomatis. Tidak adanya aturan proteksi proaktif seperti Web Application Firewall atau aturan firewall berbasis perilaku menjadi faktor pendukung terjadinya insiden.

4. Kontrol Keamanan Aplikasi Belum Terintegrasi Secara Penuh

   Fokus pengembangan aplikasi masih lebih menitikberatkan pada fungsi utama, sementara kontrol keamanan dasar pada fitur kritis belum diimplementasikan secara menyeluruh sejak awal.

Analisis ini menunjukkan bahwa insiden tidak disebabkan oleh eksploitasi kerentanan kompleks, melainkan oleh ketiadaan kontrol keamanan dasar yang seharusnya diterapkan pada mekanisme autentikasi. Kondisi ini menegaskan pentingnya penerapan prinsip *secure by default* dan integrasi keamanan secara konsisten dalam proses pengembangan dan operasional sistem.

TINDAKAN PENANGANAN INSIDEN

Penanganan insiden dilakukan secara terstruktur dengan mengacu pada tahapan Incident Response Lifecycle sebagaimana direkomendasikan dalam NIST SP 800-61. Tujuan utama dari tindakan ini adalah menghentikan aktivitas mencurigakan, menghilangkan penyebab insiden, serta memastikan sistem kembali beroperasi secara normal tanpa dampak lanjutan terhadap operasional.

1. **Identifikasi Insiden (Identification)**

   Langkah awal dilakukan dengan mengidentifikasi dan mengonfirmasi bahwa aktivitas yang terdeteksi merupakan insiden keamanan. Proses ini mencakup:

   - Analisis log aplikasi melalui sistem logging terpusat untuk mengidentifikasi pola login gagal berulang.
   - Korelasi data log dengan metrik sistem pada dashboard monitoring untuk memastikan adanya anomali trafik.
   - Validasi bahwa aktivitas tersebut bukan disebabkan oleh kesalahan konfigurasi atau penggunaan normal aplikasi.

   Hasil identifikasi memastikan bahwa kejadian tersebut merupakan percobaan akses tidak sah *(brute force login)* yang memerlukan respons segera.

2. **Isolasi Insiden (Containment)**

   Setelah insiden terkonfirmasi, langkah isolasi dilakukan untuk mencegah eskalasi dan membatasi dampak terhadap sistem. Tindakan yang diambil meliputi:

   - Pemblokiran sementara alamat IP sumber serangan melalui mekanisme firewall.
   - Pengawasan lanjutan terhadap endpoint login untuk memastikan tidak ada aktivitas mencurigakan lainnya.

   Langkah ini bersifat sementara dan difokuskan untuk menghentikan serangan tanpa mengganggu layanan yang sah.

3. **Pembersihan Insiden (Eradication)**

   Pada tahap ini, dilakukan tindakan untuk menghilangkan penyebab utama insiden, bukan hanya menghentikan gejalanya. Tahap eradication bertujuan untuk mencegah terulangnya insiden dengan pola serupa. Tindakan yang dilakukan antara lain:

   - Penyesuaian konfigurasi aplikasi untuk memperlambat atau membatasi percobaan login gagal.

- Evaluasi ulang mekanisme autentikasi untuk memastikan tidak terdapat celah keamanan tambahan.
- Pembersihan log dan validasi bahwa tidak ada akun atau data yang terdampak selama insiden berlangsung.

4. **Pemulihan Sistem (Recovery)**

   Setelah tindakan pembersihan selesai, sistem dikembalikan ke kondisi operasional normal. Proses pemulihan meliputi:

   - Penghapusan aturan pemblokiran sementara setelah sistem dinyatakan aman.
   - Pengujian fungsi login dan layanan terkait untuk memastikan operasional berjalan normal.
   - Monitoring intensif pasca-insiden guna mendeteksi potensi aktivitas mencurigakan lanjutan.

REKOMENDASI DAN TINDAK LANJUT

Berdasarkan hasil analisis insiden, penanganan yang telah dilakukan, serta evaluasi terhadap kontrol keamanan yang ada, berikut adalah rekomendasi dan rencana tindak lanjut yang bertujuan untuk meningkatkan ketahanan sistem dan mencegah terulangnya insiden serupa di masa mendatang.

1. Rekomendasi Teknis

a. Penerapan Rate Limiting pada Endpoint Login

Disarankan untuk menerapkan pembatasan jumlah percobaan login dalam periode waktu tertentu secara otomatis guna mengurangi efektivitas serangan brute force.

b. Mekanisme Penguncian Akun Sementara (Account Lockout)

Sistem perlu dikonfigurasi untuk melakukan penguncian akun sementara setelah sejumlah percobaan login gagal, sehingga mencegah percobaan berulang dari akun yang sama.

c. Penerapan Web Application Firewall (WAF)

Penggunaan WAF dengan aturan proteksi terhadap serangan brute force dan anomali trafik akan membantu mendeteksi dan memblokir serangan lebih awal sebelum mencapai aplikasi.

d. Penguatan Mekanisme Autentikasi

Implementasi autentikasi multi-faktor (MFA) direkomendasikan untuk menambah lapisan keamanan pada proses login, terutama untuk akun dengan hak akses tinggi.

2. Rekomendasi Operasional

a. Peningkatan Monitoring dan Alert Otomatis

Sistem monitoring perlu dilengkapi dengan alert otomatis berbasis ambang batas (threshold) dan pola anomali, sehingga insiden dapat terdeteksi lebih cepat tanpa bergantung pada pemantauan manual.

b. Standarisasi Prosedur Incident Handling

Disarankan untuk menyusun dan menerapkan prosedur baku penanganan insiden yang mencakup eskalasi, dokumentasi, dan penutupan insiden secara konsisten.

c. Simulasi Insiden Secara Berkala

Melakukan latihan simulasi insiden (incident drill) secara berkala untuk memastikan kesiapan tim dan efektivitas prosedur yang diterapkan.

3. Tindak Lanjut

Sebagai tindak lanjut dari insiden ini, akan dilakukan:

a. Implementasi bertahap rekomendasi teknis sesuai prioritas risiko.
b. Evaluasi ulang kontrol keamanan pada fitur kritis aplikasi.
c. Pemantauan berkelanjutan terhadap efektivitas perbaikan yang diterapkan.

Dengan dilaksanakannya rekomendasi dan tindak lanjut tersebut, diharapkan tingkat risiko keamanan dapat ditekan dan kesiapan organisasi dalam menghadapi insiden keamanan dapat ditingkatkan secara berkelanjutan.

KESIMPULAN

Insiden keamanan berupa percobaan brute force pada mekanisme login aplikasi web berhasil terdeteksi dan ditangani secara efektif melalui penerapan sistem logging dan monitoring yang terintegrasi. Insiden ini tidak menimbulkan kebocoran data maupun gangguan layanan yang signifikan, namun menunjukkan adanya kelemahan pada kontrol keamanan dasar yang perlu segera diperbaiki.

Proses penanganan insiden yang dilakukan, mulai dari identifikasi, isolasi, pembersihan, hingga pemulihan sistem, berjalan sesuai dengan tahapan Incident Response Lifecycle dan mampu mencegah eskalasi risiko ke tingkat yang lebih tinggi. Hal ini membuktikan bahwa kesiapan incident handling memiliki peran penting dalam menjaga stabilitas operasional dan keamanan sistem.

Temuan dari insiden ini menegaskan bahwa ancaman keamanan tidak selalu berasal dari eksploitasi yang kompleks, melainkan sering kali disebabkan oleh kurangnya penerapan kontrol pengamanan dasar pada komponen kritis aplikasi. Oleh karena itu, integrasi keamanan ke dalam proses pengembangan dan operasional sistem harus dilakukan secara konsisten sebagai bagian dari praktik DevSecOps.

Dengan menerapkan rekomendasi dan tindak lanjut yang telah diusulkan, organisasi diharapkan dapat meningkatkan ketahanan sistem, menurunkan risiko insiden serupa di masa depan, serta memastikan keberlangsungan layanan dan kepercayaan pengguna tetap terjaga.

REFERENSI

1. OWASP Foundation – Blocking Brute Force Attacks
   https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
2. OWASP Top 10:2021 – Identification and Authentication Failures
   https://owasp.org/Top10/2021/id/A07_2021-Identification_and_Authentication_Failures/
3. OWASP Authentication Cheat Sheet
   https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
4. NIST SP 800-63B – Authentication and Lifecycle Management
   https://pages.nist.gov/800-63-4/sp800-63b.html
5. Pedoman Keamanan Microservice dan API (CSIRT BPS)
   https://csirt.bps.go.id/assets/panduan/Pedoman-Keamanan-Microservice-dan-API_compressed.pdf
6. Fortinet – Preventing Authentication Failures with WAF
   https://docs.fortinet.com/document/fortiweb/8.0.0/waf-solutions-against-owasp-top-10-risks/384483/preventing-identification-and-authentication-failures-with-fortiweb
7. Contoh Laporan Penetration Testing – No Rate Limit Login
   https://new-dev-isk.air.id/storage/product/20240313_100231-product-28-Laporan%20Penetration%20Testing%20iOffice%20BAg%20v1.1.pdf