# LAPORAN PENANGANAN INSIDEN KEAMANAN

# (INCIDENT HANDLING REPORT)

### KASUS: BRUTE FORCE LOGIN PADA APLIKASI JUICE SHOP


Disusun Oleh:

Zico Nakano Morientes

88032023006


## PROGRAM STUDI REKAYASA KEAMANAN SIBER

## POLITEKNIK BHAKTI SEMESTA

## 2025

# DAFTAR ISI

# 1. INFORMASI UMUM INSIDEN

- Jenis Insiden: Brute Force Login Attack
- Target Aplikasi: OWASP Juice Shop
- Lingkungan: Docker (Localhost – http://127.0.0.1:3000)
- Kategori Insiden: Authentication Attack
- Tingkat Dampak: Medium – High
- Downtime Layana: Tidak ada

Insiden yang terjadi pada aplikasi OWASP Juice Shop diklasifikasikan sebagai Brute Force Login Attack, yaitu upaya penyerang untuk memperoleh akses tidak sah dengan cara melakukan percobaan login berulang menggunakan kombinasi kredensial yang berbeda. Serangan ini secara khusus menargetkan mekanisme autentikasi, yang merupakan salah satu komponen kritis dalam keamanan aplikasi web.

Aplikasi OWASP Juice Shop dijalankan pada lingkungan Docker lokal dan diakses melalui alamat http://127.0.0.1:3000. Meskipun lingkungan pengujian bersifat non-produksi, skenario ini merepresentasikan kondisi nyata yang sering terjadi pada aplikasi web modern. Oleh karena itu, simulasi insiden ini tetap memiliki relevansi tinggi dalam konteks penerapan DevSecOps dan incident handling.

Berdasarkan hasil monitoring dan analisis dampak, insiden ini dikategorikan memiliki tingkat dampak Medium hingga High. Hal ini disebabkan oleh potensi risiko pengambilalihan akun pengguna serta peningkatan beban sistem akibat tingginya jumlah permintaan autentikasi. Namun demikian, selama insiden berlangsung tidak ditemukan gangguan terhadap ketersediaan layanan (no downtime), sehingga aplikasi tetap dapat diakses oleh pengguna secara normal.

Tidak adanya downtime menunjukkan bahwa aplikasi masih mampu menangani lonjakan permintaan autentikasi tanpa mengalami kegagalan layanan. Meskipun demikian, insiden ini tetap menjadi indikator penting adanya kelemahan pada kontrol pencegahan brute force yang perlu dievaluasi dan ditingkatkan sebagai bagian dari upaya pengamanan berkelanjutan dalam pendekatan DevSecOps.

# 2. INCIDENT IDENTIFICATION

Insiden brute force login diidentifikasi melalui adanya percobaan login gagal yang terjadi secara berulang dalam waktu singkat pada halaman autentikasi aplikasi OWASP Juice Shop. Aktivitas tersebut menimbulkan peningkatan jumlah request secara signifikan ke endpoint login, yang berbeda dari pola akses pengguna normal. Kondisi ini menjadi indikator awal adanya aktivitas tidak wajar yang mengarah pada upaya eksploitasi mekanisme autentikasi.

Selama periode kejadian, sistem monitoring menunjukkan adanya lonjakan penggunaan resource pada container aplikasi. Meskipun OWASP Juice Shop tidak menyediakan audit log autentikasi yang terintegrasi ke sistem logging terpusat, indikasi insiden tetap dapat terdeteksi melalui observabilitas berbasis metrics dan log HTTP. Indikator yang diamati antara lain:

- Peningkatan response time pada dashboard Grafana, yang menunjukkan bertambahnya beban permintaan terhadap aplikasi
- Lonjakan CPU usage dan memory usage pada Node Exporter, yang menandakan meningkatnya proses autentikasi yang dijalankan secara berulang
- Munculnya status HTTP 401 (Unauthorized) secara berulang pada Elastic Discover, yang mengindikasikan kegagalan autentikasi akibat kredensial tidak valid

Kombinasi dari indikator tersebut membentuk pola aktivitas yang konsisten dengan karakteristik brute force login attack, di mana penyerang berusaha menebak kredensial pengguna melalui otomatisasi percobaan login. Meskipun tidak terdapat bukti keberhasilan login tidak sah, pola anomali ini cukup kuat untuk menetapkan kejadian tersebut sebagai insiden keamanan pada tahap identifikasi.

# 3. INCIDENT CONTAINMENT

Setelah insiden brute force login berhasil diidentifikasi, langkah incident containment dilakukan untuk membatasi dampak serangan serta mencegah eskalasi yang dapat mengganggu ketersediaan layanan aplikasi. Tahap containment difokuskan pada pengendalian aktivitas autentikasi dan peningkatan pengawasan terhadap komponen sistem yang menjadi target serangan, khususnya endpoint login.

Containment dilakukan dengan memastikan bahwa aktivitas login berulang tidak berkembang menjadi beban berlebih yang berpotensi menyebabkan penurunan performa atau denial of service. Pada tahap ini, sistem tidak dihentikan karena aplikasi masih berada dalam kondisi operasional dan tidak menunjukkan kegagalan layanan. Sebaliknya, pendekatan containment dilakukan melalui monitoring intensif untuk mengendalikan dampak serangan secara real-time. Monitoring selama tahap containment difokuskan pada beberapa indikator utama, yaitu:

- Request rate ke endpoint login, untuk mengamati pola akses dan mendeteksi percobaan autentikasi yang berulang dan tidak normal
- Penggunaan resource sistem, meliputi CPU usage, memory usage, dan load average, guna memastikan bahwa beban sistem tetap berada dalam batas aman
- Status ketersediaan aplikasi (availability), untuk memastikan layanan tetap dapat diakses oleh pengguna yang sah

Tujuan utama dari tahap containment ini adalah menjaga stabilitas dan ketersediaan layanan selama insiden berlangsung, sekaligus mencegah serangan brute force berkembang menjadi gangguan layanan yang lebih serius. Pendekatan ini sejalan dengan prinsip DevSecOps, di mana keamanan ditangani secara berkelanjutan tanpa mengorbankan aspek operasional aplikasi.

# 4. INCIDENT ERADICATION

Pada tahap incident eradication, dilakukan evaluasi terhadap mekanisme autentikasi aplikasi OWASP Juice Shop untuk memastikan bahwa tidak terdapat akun pengguna yang berhasil dikompromikan selama simulasi serangan brute force berlangsung. Berdasarkan hasil observasi dan monitoring, tidak ditemukan indikasi keberhasilan login tidak sah maupun perubahan status akun yang mencurigakan selama periode insiden.

Selain verifikasi kondisi akun, tahap eradication juga mencakup peninjauan terhadap kontrol keamanan autentikasi guna mengidentifikasi potensi kelemahan yang dapat dimanfaatkan oleh serangan serupa di masa mendatang. Evaluasi ini dilakukan dengan mempertimbangkan karakteristik serangan brute force yang terdeteksi pada tahap sebelumnya, khususnya pola percobaan login berulang dan peningkatan beban sistem.

Beberapa kontrol keamanan yang direkomendasikan sebagai bagian dari upaya eradication meliputi:

- Penerapan rate limiting pada endpoint login, untuk membatasi jumlah percobaan autentikasi dalam periode waktu tertentu
- Penambahan mekanisme CAPTCHA, guna membedakan aktivitas pengguna manusia dengan otomatisasi serangan
- Penguatan kebijakan autentikasi dan monitoring login, termasuk peningkatan visibilitas terhadap aktivitas login gagal dan pola akses tidak normal

Tahap eradication ini bertujuan untuk menghilangkan atau meminimalkan vektor serangan brute force yang telah teridentifikasi, sehingga risiko terulangnya insiden serupa dapat dikurangi. Pendekatan ini juga mendukung prinsip perbaikan berkelanjutan dalam DevSecOps, di mana hasil insiden digunakan sebagai dasar peningkatan kontrol keamanan aplikasi.

# 5. INCIDENT RECOVERY

Tahap recovery dilakukan dengan memastikan aplikasi kembali beroperasi dalam kondisi normal setelah aktivitas login berulang dihentikan. Monitoring lanjutan menunjukkan bahwa:

- CPU usage dan memory usage kembali ke kondisi baseline
- Response time aplikasi kembali stabil
- Tidak terdapat lonjakan request mencurigakan lanjutan

Aplikasi OWASP Juice Shop tetap dapat diakses oleh pengguna tanpa gangguan selama dan setelah insiden.

Tahap incident recovery dilakukan setelah aktivitas login berulang yang terindikasi sebagai brute force attack dihentikan dan tidak lagi terdeteksi melalui sistem monitoring. Fokus utama pada tahap ini adalah memastikan bahwa aplikasi OWASP Juice Shop kembali beroperasi dalam kondisi normal serta tidak mengalami dampak lanjutan akibat insiden yang telah terjadi.

Monitoring lanjutan dilakukan secara berkelanjutan untuk mengamati stabilitas sistem dan memastikan bahwa seluruh komponen aplikasi berfungsi sebagaimana mestinya. Hasil monitoring menunjukkan bahwa:

- CPU usage dan memory usage kembali ke kondisi baseline, yang menandakan beban sistem telah kembali normal
- Response time aplikasi kembali stabil dan berada dalam rentang operasional yang wajar
- Tidak terdapat lonjakan request mencurigakan lanjutan, khususnya pada endpoint autentikasi

Selain pemantauan resource, status ketersediaan aplikasi juga diperiksa untuk memastikan bahwa layanan tetap dapat diakses oleh pengguna yang sah. Selama dan setelah tahap recovery, aplikasi OWASP Juice Shop tetap berada dalam kondisi available (UP) dan tidak mengalami gangguan layanan maupun downtime.

Tahap recovery ini menegaskan bahwa insiden brute force login tidak meninggalkan dampak residu terhadap stabilitas dan ketersediaan aplikasi. Proses recovery yang didukung oleh monitoring berbasis metrics memungkinkan verifikasi kondisi sistem secara objektif sebelum dinyatakan kembali ke status operasional normal.

# 6. LESSONS LEARNED

Berdasarkan insiden brute force login yang telah disimulasikan, dapat disimpulkan bahwa monitoring berbasis metrics memiliki peran yang sangat penting dalam mendeteksi anomali keamanan, khususnya pada aplikasi yang memiliki keterbatasan mekanisme audit log autentikasi. Meskipun tidak tersedia log autentikasi secara detail, indikator seperti lonjakan request, peningkatan response time, serta penggunaan resource sistem terbukti efektif dalam mengidentifikasi aktivitas mencurigakan.

Insiden ini juga menunjukkan bahwa penerapan incident handling yang terstruktur memungkinkan proses penanganan insiden dilakukan secara sistematis, mulai dari tahap identifikasi hingga recovery, tanpa harus menghentikan layanan aplikasi. Pendekatan ini sejalan dengan prinsip DevSecOps yang menekankan keseimbangan antara keamanan dan ketersediaan layanan dalam lingkungan operasional.

Sebagai upaya peningkatan keamanan di masa mendatang, beberapa rekomendasi yang dapat diterapkan antara lain:

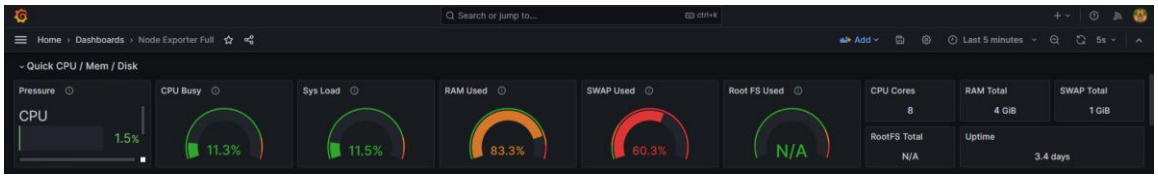
- Implementasi audit log autentikasi yang lebih detail, sehingga aktivitas login gagal dan berhasil dapat dianalisis secara lebih akurat
- Penerapan alert otomatis berbasis metrics, untuk mempercepat proses deteksi dan respons terhadap anomali keamanan
- Penambahan kontrol pencegahan brute force, seperti rate limiting dan CAPTCHA, sebagai bagian dari praktik keamanan berkelanjutan dalam DevSecOps

Secara keseluruhan, insiden ini memberikan pembelajaran bahwa keamanan aplikasi tidak hanya bergantung pada kemampuan pencegahan, tetapi juga pada kemampuan deteksi, respons, dan pemulihan yang didukung oleh monitoring dan observabilitas yang baik. Integrasi aspek tersebut menjadi kunci dalam membangun aplikasi yang aman dan andal.

# 7. BUKTI PENDUKUNG (EVIDENCE)

Bukti pendukung pada insiden brute force login ini diperoleh dari sistem monitoring dan logging yang digunakan untuk mengamati kondisi aplikasi OWASP Juice Shop selama dan setelah insiden berlangsung. Evidence ini berfungsi untuk memperkuat hasil analisis pada tahap identification, containment, eradication, dan recovery, serta memberikan dasar objektif dalam penilaian dampak insiden.

## 1. Dashboard Grafana




Gambar 7.1 – Dashboard Grafana sebelum insiden

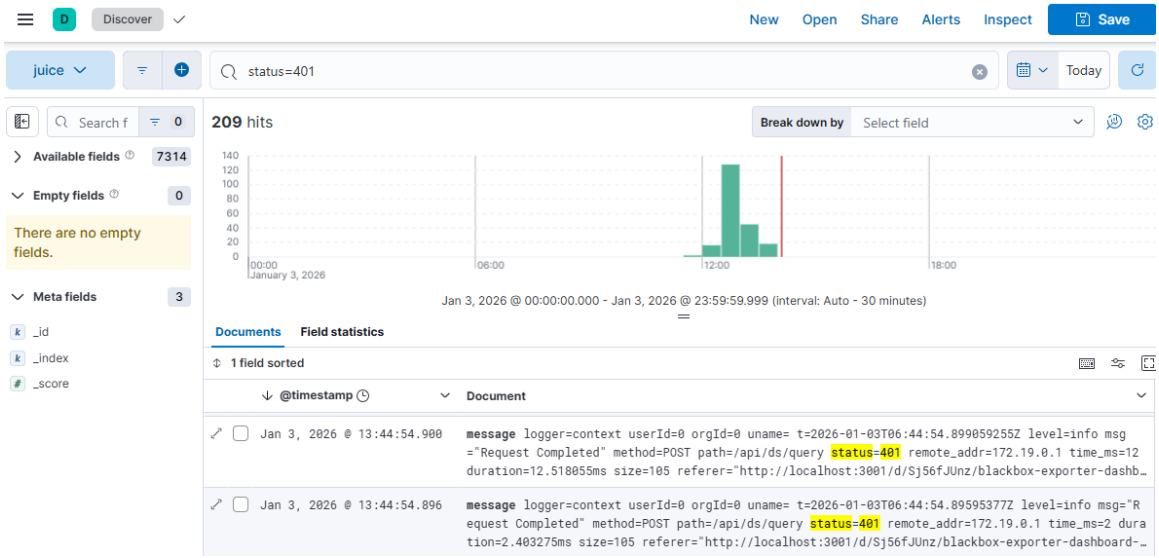

Gambar 7.2 – Dashboard Grafana saat insiden

Dashboard Grafana digunakan sebagai alat utama untuk memantau performa dan ketersediaan aplikasi secara real-time. Selama insiden berlangsung, panel yang diamati menunjukkan adanya anomali dibandingkan kondisi operasional normal, antara lain:

- CPU Usage, yang mengalami peningkatan seiring bertambahnya jumlah percobaan login
- Memory Usage, yang ikut meningkat akibat pemrosesan request autentikasi secara berulang
- Response Time, yang menunjukkan kenaikan latency akibat lonjakan request ke endpoint login

Perubahan metrik ini menjadi indikator utama terjadinya aktivitas tidak normal pada sistem.

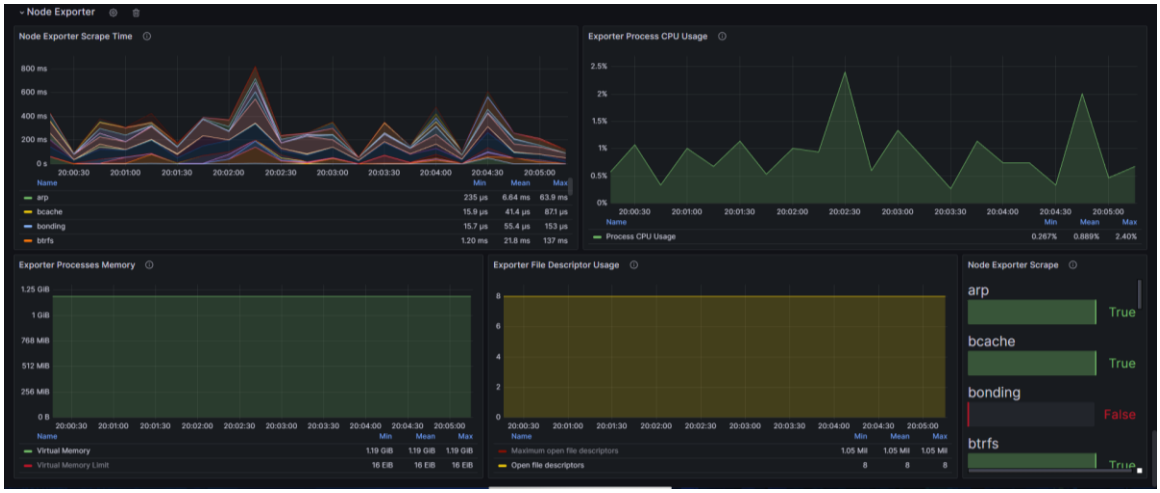
## 2. Elastic Discover




Gambar 7.3 – Log HTTP 401 pada Elastic Discover

Elastic Discover digunakan untuk menganalisis log HTTP yang dihasilkan oleh aplikasi. Selama periode insiden, ditemukan status HTTP 401 (Unauthorized) yang muncul secara berulang, yang menunjukkan kegagalan autentikasi akibat kredensial tidak valid. Pola kemunculan status 401 dalam jumlah besar dan waktu singkat memperkuat indikasi adanya serangan brute force login.

## Node Exporter Metrics




Gambar 7.4 – Load Average & Resource Utilization

Node Exporter menyediakan metrik tingkat sistem yang digunakan untuk mengevaluasi dampak insiden terhadap resource host. Metrik yang diamati meliputi:

- Load Average, yang meningkat seiring bertambahnya jumlah proses yang dijalankan
- Resource Utilization, yang mencerminkan tekanan sistem akibat aktivitas login berulang

Kombinasi data dari Grafana, Elastic Discover, dan Node Exporter memberikan gambaran menyeluruh mengenai perilaku sistem selama insiden berlangsung. Evidence ini mendukung kesimpulan bahwa aktivitas yang terdeteksi merupakan brute force login attack, serta menunjukkan bahwa meskipun terjadi peningkatan beban sistem, aplikasi tetap berada dalam kondisi tersedia dan dapat dipulihkan dengan baik.

# 8. KESIMPULAN

Penerapan pendekatan DevSecOps pada aplikasi OWASP Juice Shop berhasil menunjukkan pentingnya integrasi keamanan ke dalam seluruh siklus pengembangan aplikasi. Melalui penerapan Secure SDLC dan threat modeling, aset penting dan potensi ancaman dapat diidentifikasi sejak awal sehingga pengamanan dilakukan secara lebih terarah.

Implementasi CI/CD pipeline dengan pengujian keamanan otomatis (SAST, SCA, container scanning, dan DAST) membuktikan bahwa automasi mampu meningkatkan efektivitas deteksi kerentanan tanpa menghambat proses pengembangan. Meskipun masih ditemukan kerentanan pada dependensi aplikasi, penerapan Docker hardening berhasil mengurangi attack surface dan meningkatkan keamanan lingkungan runtime.

Monitoring dan observabilitas berperan penting dalam mendeteksi anomali serta mendukung proses incident handling, khususnya pada simulasi brute force login attack. Walaupun terdapat keterbatasan audit log autentikasi, indikator berbasis metrics terbukti efektif dalam mendeteksi, membatasi, dan memulihkan insiden tanpa menyebabkan downtime layanan.

Secara keseluruhan, proyek ini menegaskan bahwa keamanan aplikasi merupakan tanggung jawab bersama antara developer, operator, dan security engineer. Pendekatan DevSecOps memungkinkan keamanan diterapkan secara berkelanjutan, sistematis, dan terintegrasi dalam pengembangan aplikasi modern.

# 9. REFERENSI


1. Amazon Web Services. What is DevSecOps? https://aws.amazon.com/id/what-is/devsecops/
2. OWASP Foundation. OWASP DevSecOps Guideline https://owasp.org/www-project-devsecops-guideline/
3. OWASP Foundation. OWASP Juice Shop Project https://owasp.org/www-project-juice-shop/
4. Wikipedia. Static Application Security Testing https://en.wikipedia.org/wiki/Static_application_security_testing
5. Wikipedia. Dynamic Application Security Testing https://en.wikipedia.org/wiki/Dynamic_application_security_testing