Laporan Proyek Impact\_ctf\_blue\_labs

1. Tujuan proyek:

Tujuan dari proyek impact\_ctf\_blue\_labs adalah untuk membangun, menguji, dan mendokumentasikan sebuah mini-lab Cyber Security berbasis pendekatan Blue Team yang berfokus pada kegiatan monitoring sistem, deteksi aktivitas mencurigakan, serta penerapan hardening pada aplikasi web. Proyek ini dirancang untuk memberikan pemahaman praktis mengenai bagaimana seorang Incident Response atau Blue Team Analyst bekerja dalam mengamati perilaku sistem, mengidentifikasi potensi ancaman, dan mengambil tindakan defensif yang sesuai.

Melalui proyek ini, dilakukan observasi terhadap perilaku normal aplikasi (baseline) sebagai acuan awal, kemudian dilakukan analisis terhadap log untuk mendeteksi penyimpangan atau indikator aktivitas mencurigakan. Selanjutnya, diterapkan kontrol keamanan tambahan seperti pembatasan akses dan penguatan lapisan proteksi untuk mengurangi risiko serangan. Seluruh proses dilaksanakan di lingkungan lokal berbasis Windows dan Docker Desktop, sehingga aman, terkontrol, dan ditujukan murni untuk keperluan pembelajaran serta simulasi keamanan non-produktif.

1. Website yang digunakan dalam project:

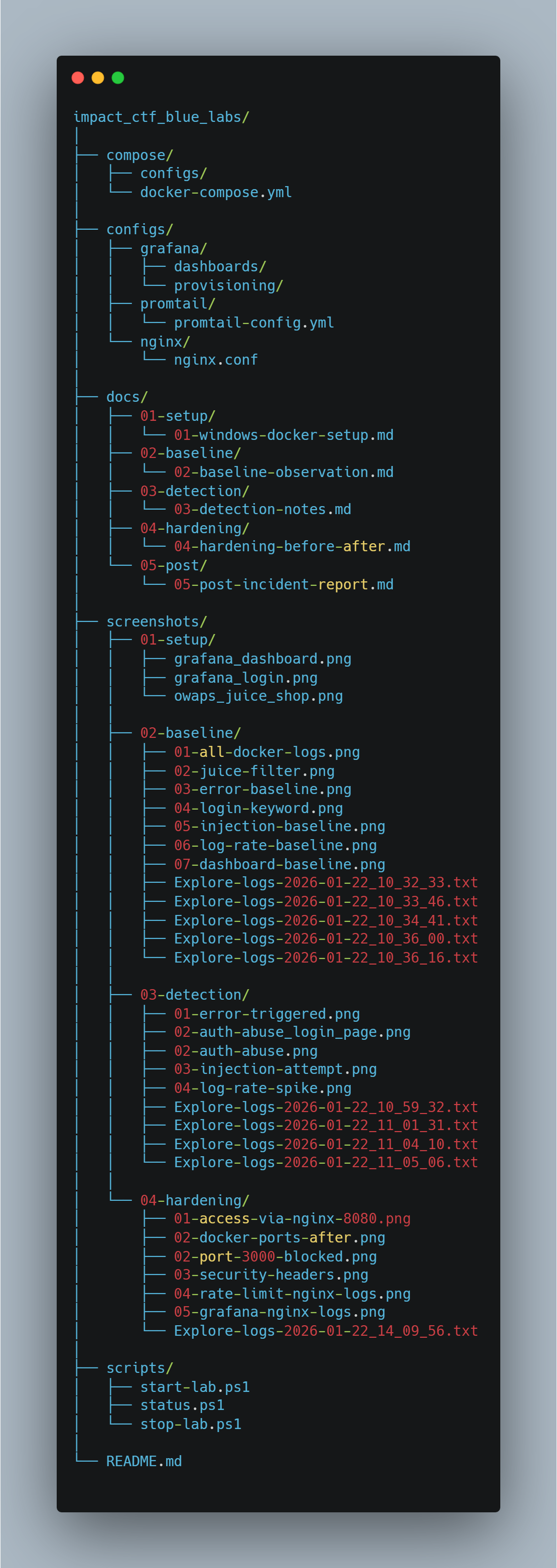
Website yang digunakan dalam proyek ini adalah:

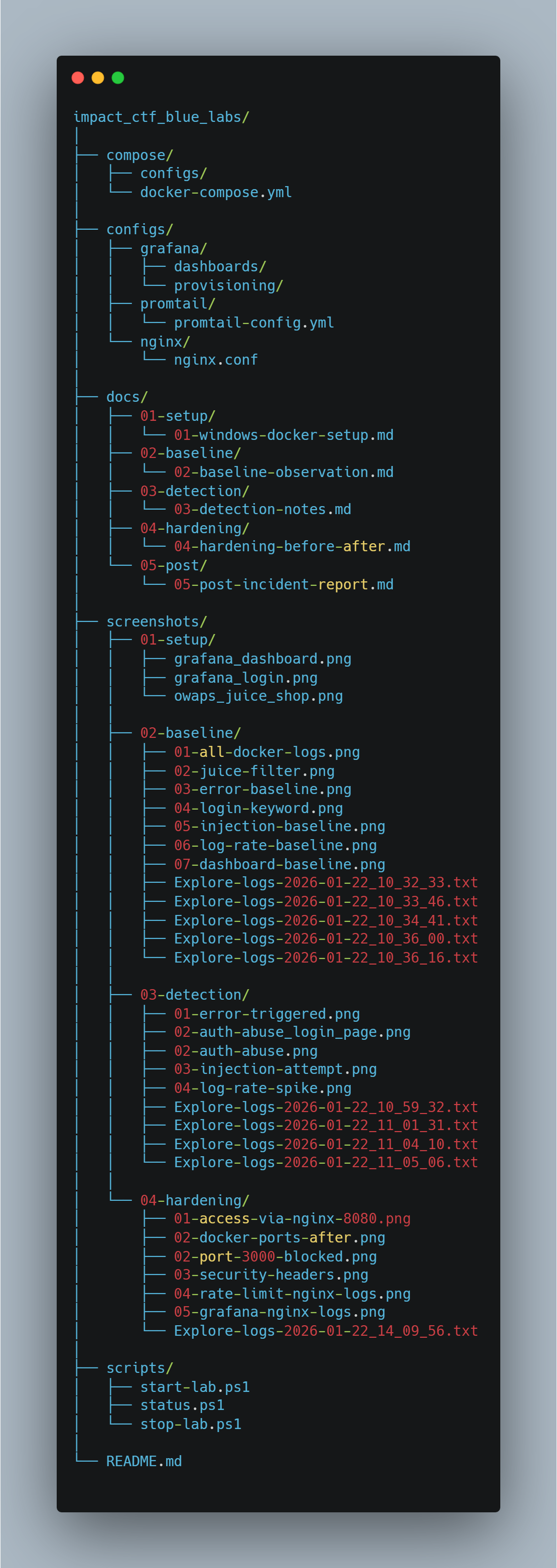
* OWASP Juice Shop – diambil dari web OWASP yang dimana web ini dibuat sangat rentang dengan serangan.

1. Penjelasan singkat:

Proyek impact\_ctf\_blue\_labs merupakan simulasi pengamanan aplikasi web yang menitikberatkan pada sudut pandang defensif (Blue Team). Aplikasi web dijalankan di dalam container dan dipantau menggunakan sistem logging serta monitoring terpusat untuk memahami pola aktivitas normal pengguna dan sistem. Dengan adanya baseline tersebut, aktivitas yang menyimpang atau tidak wajar dapat diidentifikasi melalui analisis log secara sistematis.

Setelah indikator aktivitas mencurigakan ditemukan, dilakukan langkah hardening untuk memperkuat keamanan aplikasi, terutama pada sisi akses dan pengendalian trafik. Perubahan yang dilakukan kemudian dianalisis dengan membandingkan kondisi sistem sebelum dan sesudah hardening. Seluruh hasil pengamatan, analisis, dan tindakan defensif tersebut didokumentasikan dalam bentuk laporan keamanan sebagai simulasi proses penanganan insiden yang umum dilakukan dalam lingkungan kerja Cyber Security.

1. Struktur folder:



1. Privasi dan otorisasi:

Seluruh aktivitas yang dilakukan dalam proyek impact\_ctf\_blue\_labs dilaksanakan pada lingkungan lokal dan non-produktif yang sepenuhnya berada di bawah kendali penulis. Aplikasi web yang digunakan dijalankan secara lokal menggunakan Docker Desktop dan tidak terhubung ke sistem produksi, jaringan publik, maupun data pengguna nyata.

Website yang digunakan dalam proyek ini merupakan aplikasi yang memang dirancang untuk tujuan pembelajaran dan simulasi keamanan. Tidak ada upaya eksploitasi terhadap sistem milik pihak ketiga, serta tidak ada data sensitif atau informasi pribadi yang digunakan selama pengujian. Dengan demikian, seluruh aktivitas dalam proyek ini dilakukan dengan izin penuh, sesuai dengan prinsip etika dan praktik yang berlaku dalam bidang Cyber Security.

1. Prasyarat, persiapan dan action plan yang diperlukan:
   1. Prasyarat Perangkat & Sistem

Agar proyek dapat dijalankan dengan stabil, diperlukan prasyarat berikut:

1. Perangkat

* Laptop/PC dengan resource memadai (disarankan RAM minimal 8 GB agar Docker dan Grafana berjalan lancar).
* Ruang penyimpanan cukup (image Docker + log + screenshot).

1. Sistem Operasi

* Windows 10/11 (lingkungan proyek dijalankan 100% di Windows).

1. Aplikasi/Tools

* Docker Desktop (wajib dalam kondisi berjalan/Running).
* Visual Studio Code (untuk editing file konfigurasi dan dokumentasi).
* Browser (Chrome/Edge/Firefox untuk mengakses Juice Shop & Grafana).
* PowerShell (untuk menjalankan skrip otomasi lab).

1. Koneksi Internet

* Dibutuhkan saat awal untuk menarik (pull) image Docker yang diperlukan.
  1. Prasyarat Konsep (Agar Proses Analisis Valid)

Sebelum memulai, penulis memastikan pemahaman dasar berikut agar analisis log dan hardening memiliki arah yang jelas:

* Memahami konsep baseline (pola normal sebelum ada insiden).
* Memahami konsep indicator of suspicious activity (kata kunci/pola yang menandakan potensi serangan).
* Memahami tujuan Blue Team: detect → analyze → respond → harden → verify.
* Memastikan proyek dilakukan pada lingkungan lokal, non-produktif, dan authorized.
  1. Persiapan Project Workspace

Tahap persiapan workspace dilakukan agar seluruh aktivitas terdokumentasi rapi dan mudah diaudit ulang.

1. Membuat folder proyek

* Folder utama impact\_ctf\_blue\_labs dibuat sebagai root workspace.

1. Membuat struktur folder standar proyek

* compose/ untuk file docker compose.
* configs/ untuk konfigurasi Grafana/Loki/Promtail/Nginx.
* docs/ untuk dokumentasi setiap tahap.
* scripts/ untuk otomasi PowerShell.
* screenshots/ untuk bukti visual.
* README.md untuk ringkasan proyek.

1. Menyiapkan dokumentasi per tahap

* Setiap tahap proyek memiliki file markdown:
  + setup
  + baseline
  + detection
  + hardening
  + post-incident report

Tujuan: setiap tindakan yang dilakukan dapat ditelusuri kembali secara step-by-step.

* 1. Persiapan Infrastruktur Lab (Docker)

Agar mini-lab berjalan, disiapkan beberapa komponen container utama:

1. Target Aplikasi

* OWASP Juice Shop sebagai aplikasi target.

1. Monitoring & Logging

* Grafana sebagai dashboard.
* Loki sebagai log storage/query engine.
* Promtail sebagai log shipper dari Docker logs menuju Loki.

1. Hardening Layer

* Nginx reverse proxy sebagai “edge layer” untuk:
  + memusatkan akses ke aplikasi
  + menerapkan security headers
  + rate limiting (pengendalian traffic)
  1. Persiapan Evidence & Bukti

Agar laporan proyek bersifat profesional dan dapat diverifikasi, disiapkan standar bukti:

1. Screenshot

* Setiap tahap wajib memiliki folder screenshot:
  + 01-setup
  + 02-baseline
  + 03-detection
  + 04-hardening
  + 05-post (opsional)
* Screenshot dipilih yang paling relevan (dashboard, query log, bukti port, bukti header, bukti rate limit).

1. Log Ekspor (opsional sebagai lampiran)

* Ekspor log dari Grafana Explore disimpan dalam file .txt sebagai bukti pendukung bila dibutuhkan audit, namun tidak wajib dimasukkan seluruhnya ke laporan utama.
  1. Action Plan yang Digunakan (Tahapan Proyek)

Rencana aksi proyek disusun agar pelaksanaan sistematis dan dapat dievaluasi:

Tahap 1 – Setup Lab

* Menjalankan container Juice Shop + monitoring stack.
* Validasi akses aplikasi dan dashboard Grafana.

Tahap 2 – Baseline Observation

* Menghasilkan traffic normal.
* Mencatat pola log normal dan log-rate normal.

Tahap 3 – Detection / Suspicious Activity Simulation

* Mensimulasikan aktivitas mencurigakan yang terkendali (error trigger, auth abuse, injection keyword, traffic spike).
* Mengambil bukti deteksi melalui query log dan screenshot.

Tahap 4 – Hardening

* Menambah Nginx reverse proxy.
* Menghapus expose langsung port aplikasi.
* Menerapkan security headers dan rate limiting.
* Membuktikan perubahan sebelum/sesudah.

Tahap 5 – Post-Incident Report

* Merangkum indikator, tindakan, dan hasil perbandingan before/after.
* Menyusun rekomendasi lanjutan.

1. Langkah-langkah:

Tahap 1 — Setup Mini-Lab (Windows + Docker Desktop)

1. Menyalakan Docker Desktop hingga status Running.
2. Membuat struktur folder proyek dan file dokumentasi awal.
3. Menyiapkan file docker-compose.yml untuk menjalankan:
   * OWASP Juice Shop
   * Grafana
   * Loki
   * Promtail
4. Menjalankan lab melalui PowerShell script:
   * start-lab.ps1 untuk menjalankan container.
   * status.ps1 untuk memastikan container berjalan.
5. Validasi akses:
   * Juice Shop dapat diakses melalui browser.
   * Grafana dapat diakses melalui browser.
6. Mengambil screenshot bukti tahap setup:
   * halaman Juice Shop
   * halaman login Grafana
   * dashboard Grafana

Tahap 2 — Baseline Observation

1. Membuat folder bukti baseline:
   * screenshots/02-baseline/
2. Menghasilkan traffic normal dengan aktivitas wajar:
   * membuka halaman utama
   * melakukan pencarian produk
   * membuka detail produk
   * navigasi menu umum
3. Membuka Grafana → Explore → Loki untuk mengamati log normal.
4. Menjalankan query baseline untuk memastikan data log masuk (contoh konsep):
   * query semua log docker
   * filter log relevan Juice Shop
   * filter error baseline
   * pemantauan log rate baseline (time series)
5. Mencatat karakteristik baseline:
   * apakah log stabil
   * apakah error ada/tidak
   * intensitas log rate normal
6. Mengambil screenshot baseline yang penting:
   * all logs
   * filter juice shop
   * error baseline
   * log rate baseline
   * dashboard baseline

Tahap 3 — Detection (Simulasi Aktivitas Mencurigakan)

1. Membuat folder bukti detection:
   * screenshots/03-detection/
2. Mensimulasikan aktivitas mencurigakan secara terkendali:
   * Error triggering: input aneh pada search/login untuk memicu error log.
   * Authentication abuse: percobaan login salah berulang (indikator brute force).
   * Injection attempt: memasukkan payload keyword seperti SQL/XSS ke input field.
   * Traffic spike: request berulang (browser refresh cepat atau loop PowerShell).
3. Mengamati dan membuktikan indikator di Grafana:
   * query error keyword
   * query login/auth keyword
   * query injection keyword
   * log rate spike (time series)
4. Mengambil screenshot bukti detection:
   * error triggered
   * auth abuse evidence
   * injection attempt evidence
   * log rate spike evidence
5. Mencatat temuan utama:
   * perbedaan pola dibanding baseline
   * indikator yang muncul di log
   * bentuk spike yang terdeteksi

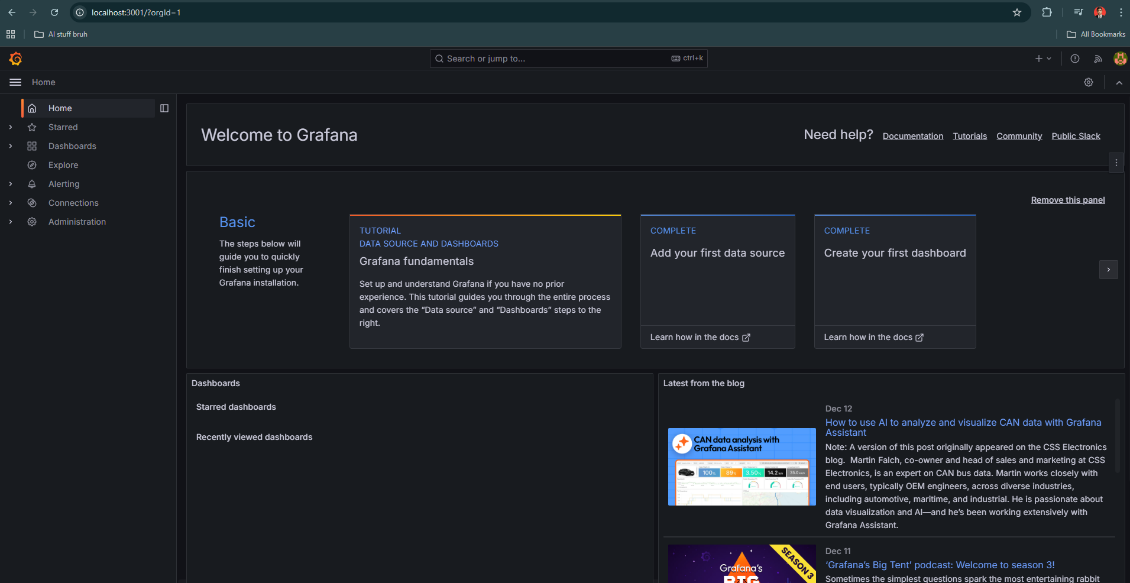
Tahap 4 — Hardening (Reverse Proxy + Rate Limit + Security Headers)

1. Membuat folder bukti hardening:
   * screenshots/04-hardening/
2. Menambahkan komponen Nginx reverse proxy:
   * Nginx menjadi pintu masuk akses user.
   * Aplikasi target tidak diakses langsung dari host.
3. Mengubah konfigurasi Docker Compose:
   * menghapus mapping port langsung dari Juice Shop
   * membuka port host untuk Nginx (contoh: 8080)
4. Menyiapkan konfigurasi Nginx:
   * security headers (nosniff, deny frame, referrer policy)
   * rate limiting (pengendalian request per IP)
5. Restart container agar konfigurasi terbaru diterapkan.
6. Verifikasi after-hardening:
   * akses aplikasi melalui Nginx (berhasil)
   * cek port mapping docker memastikan port aplikasi tidak diekspos
   * cek security headers via PowerShell (response headers)
   * uji request berulang untuk melihat efek rate limiting
   * validasi log Nginx muncul di Grafana/Loki
7. Mengambil screenshot bukti hardening:
   * akses via nginx
   * bukti port mapping setelah hardening
   * bukti security headers
   * bukti rate limit (log nginx / perubahan perilaku)
   * bukti log nginx di Grafana

Tahap 5 — Post-Incident Analysis

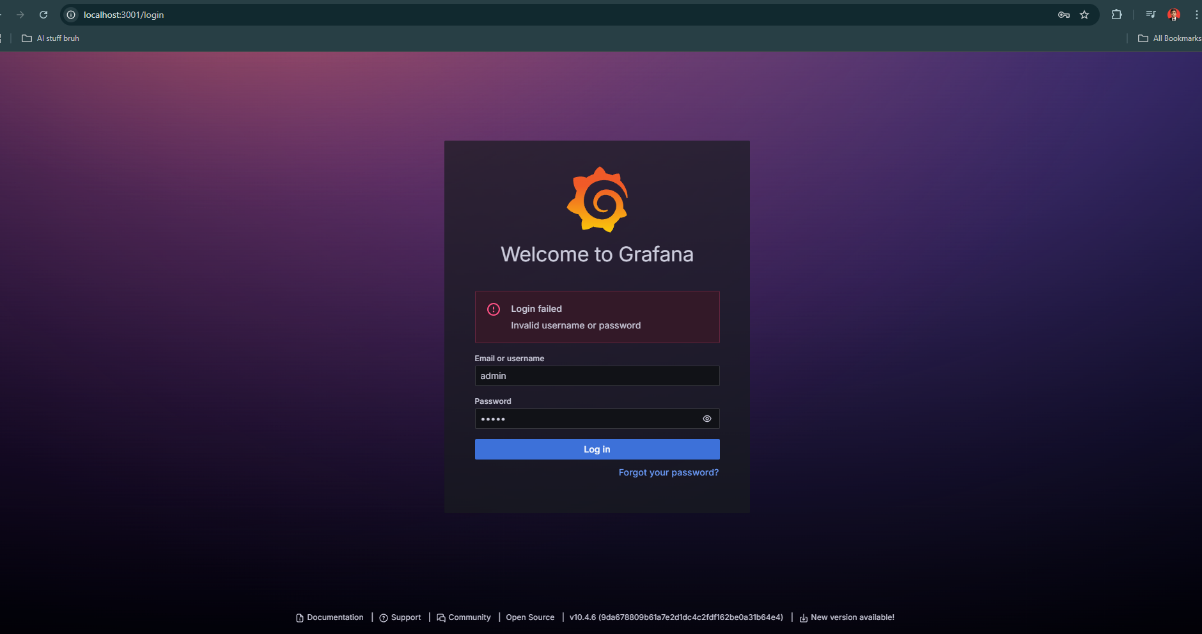
1. Mengumpulkan ringkasan bukti dari baseline, detection, dan hardening.
2. Menyusun laporan akhir:
   * indikator yang ditemukan
   * timeline tahapan
   * tindakan hardening yang diterapkan
   * analisis before vs after
3. Menuliskan rekomendasi lanjutan untuk peningkatan keamanan:
   * alerting berbasis log spike dan login failure
   * integrasi SIEM
   * kontrol tambahan seperti WAF
4. Hasil dan pembahasan:
   1. Setup

Pada tahap setup, fokus utama adalah memastikan bahwa seluruh lingkungan kerja dan komponen pendukung proyek impact\_ctf\_blue\_labs dapat berjalan dengan baik sebelum dilakukan analisis keamanan. Tahap ini juga menjadi bukti awal bahwa sistem telah siap digunakan untuk kegiatan monitoring dan pengamanan aplikasi web.



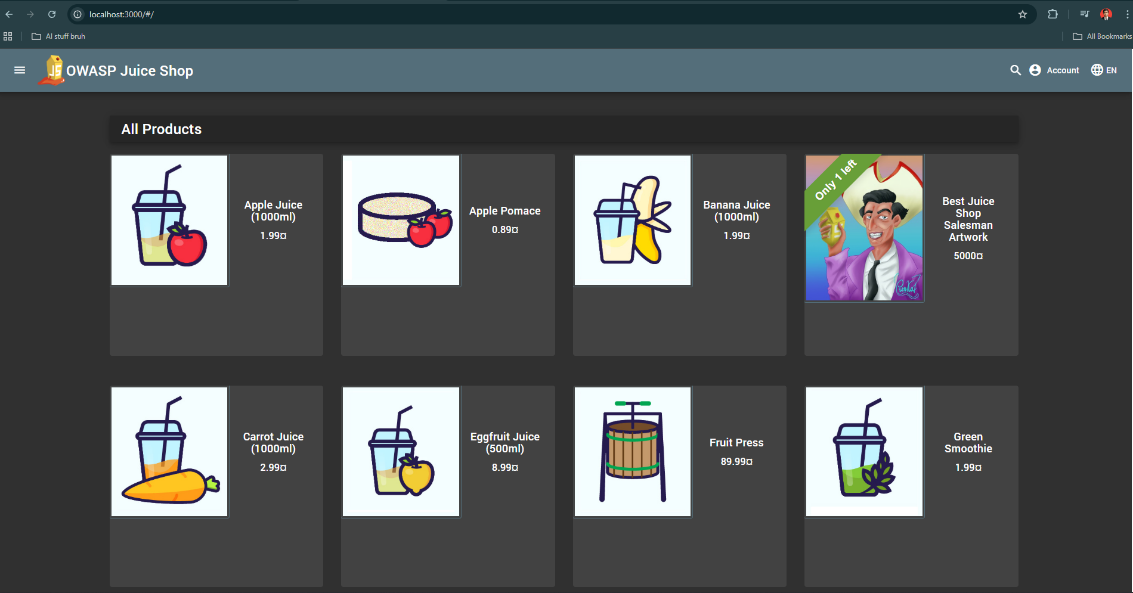
Gambar pertama menunjukkan tampilan dashboard utama Grafana setelah berhasil diakses. Halaman ini menandakan bahwa layanan Grafana telah berjalan dengan normal di dalam container Docker dan dapat diakses melalui browser. Keberhasilan menampilkan halaman dashboard ini menjadi indikator awal bahwa sistem monitoring siap digunakan sebagai pusat observasi log dan aktivitas sistem.

Dashboard Grafana berfungsi sebagai antarmuka utama untuk memvisualisasikan data log dan metrik yang dikumpulkan dari container Docker. Pada tahap setup, tampilan ini digunakan untuk memastikan bahwa Grafana dapat dimuat tanpa kendala dan siap menerima data dari sumber log.



Gambar kedua memperlihatkan halaman login Grafana. Halaman ini menunjukkan bahwa mekanisme autentikasi Grafana aktif dan berfungsi dengan baik. Proses login menggunakan akun administrator berhasil dilakukan, yang menandakan bahwa sistem telah dikonfigurasi dengan benar dan tidak mengalami error pada tahap inisialisasi.

Keberadaan halaman login ini juga menunjukkan bahwa akses ke dashboard monitoring tidak bersifat terbuka, sehingga hanya pengguna yang memiliki kredensial yang dapat mengakses data monitoring. Hal ini penting sebagai langkah awal pengendalian akses pada sistem monitoring.



Gambar ketiga menampilkan halaman utama aplikasi OWASP Juice Shop yang diakses melalui browser. Tampilan daftar produk yang muncul menunjukkan bahwa aplikasi web target telah berjalan dengan normal di dalam container Docker. Hal ini menandakan bahwa layanan frontend dan backend aplikasi dapat diakses dan digunakan sebagaimana mestinya.

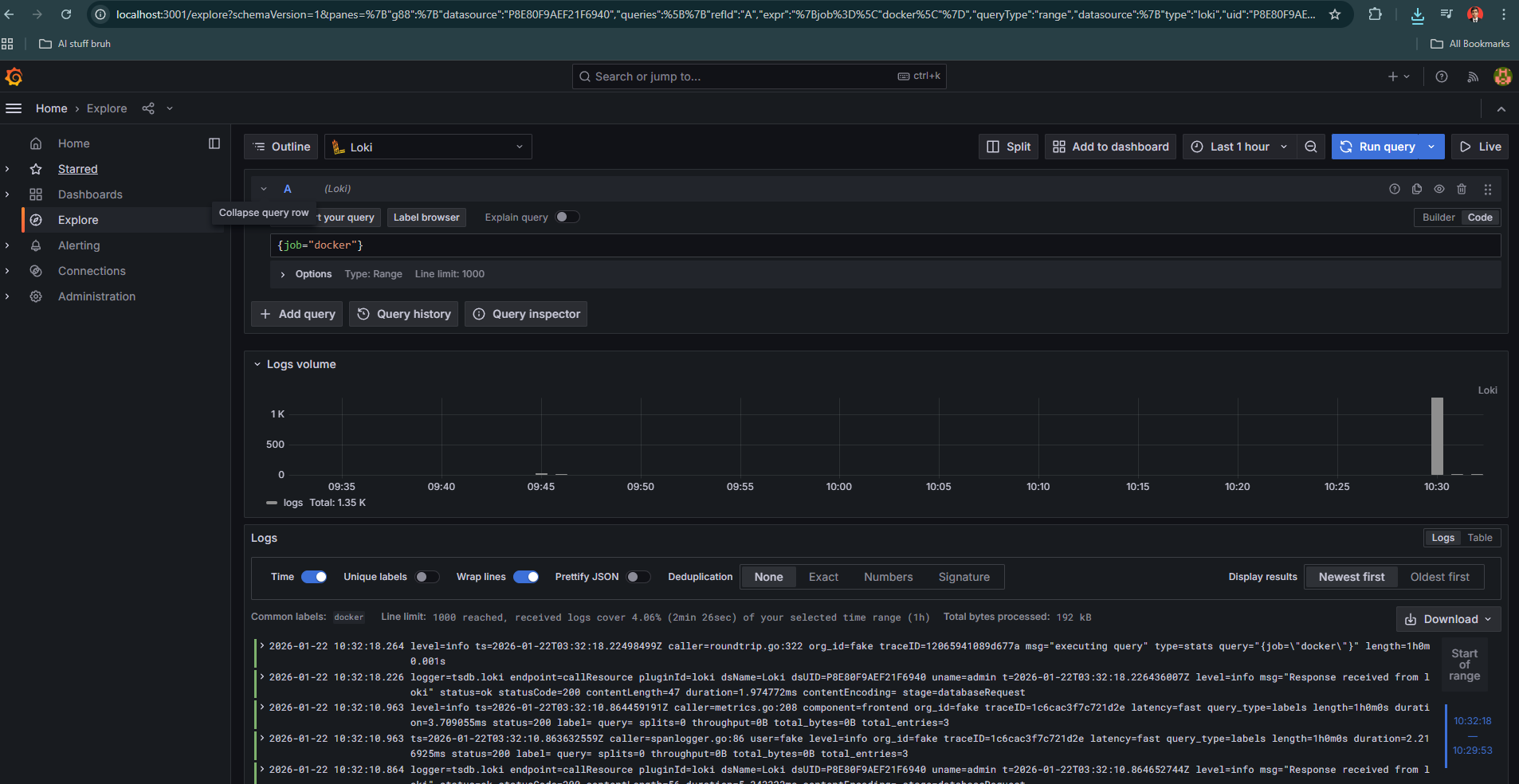
Keberhasilan mengakses OWASP Juice Shop menjadi indikator bahwa aplikasi target siap untuk dipantau aktivitasnya. Pada tahap selanjutnya, aplikasi ini akan menjadi sumber utama log yang dianalisis untuk mendeteksi aktivitas mencurigakan.

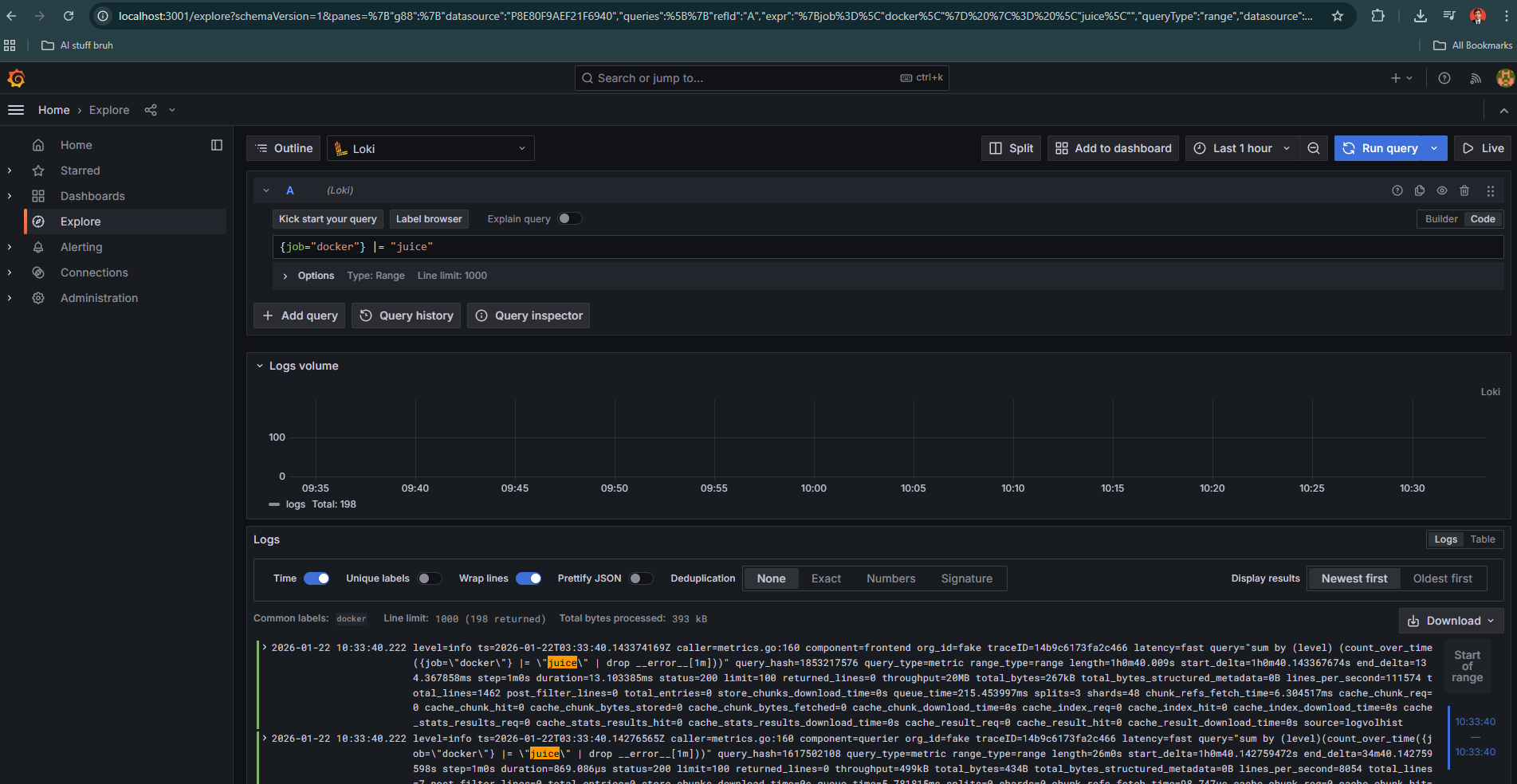
Berdasarkan ketiga gambar tersebut, dapat disimpulkan bahwa tahap setup berhasil dilakukan dengan baik. Seluruh komponen utama dalam mini-lab, yaitu aplikasi web target dan sistem monitoring, telah berjalan secara normal dan saling terintegrasi. Docker Desktop berhasil digunakan sebagai platform untuk menjalankan seluruh layanan secara terisolasi dan terkontrol di lingkungan Windows.

Keberhasilan setup ini menjadi fondasi penting bagi tahapan selanjutnya, karena tanpa lingkungan yang stabil dan monitoring yang aktif, proses observasi baseline, deteksi insiden, dan hardening tidak dapat dilakukan secara optimal. Dengan selesainya tahap setup, proyek impact\_ctf\_blue\_labs siap dilanjutkan ke tahap baseline observation untuk memahami perilaku normal sistem sebelum dilakukan simulasi aktivitas mencurigakan.

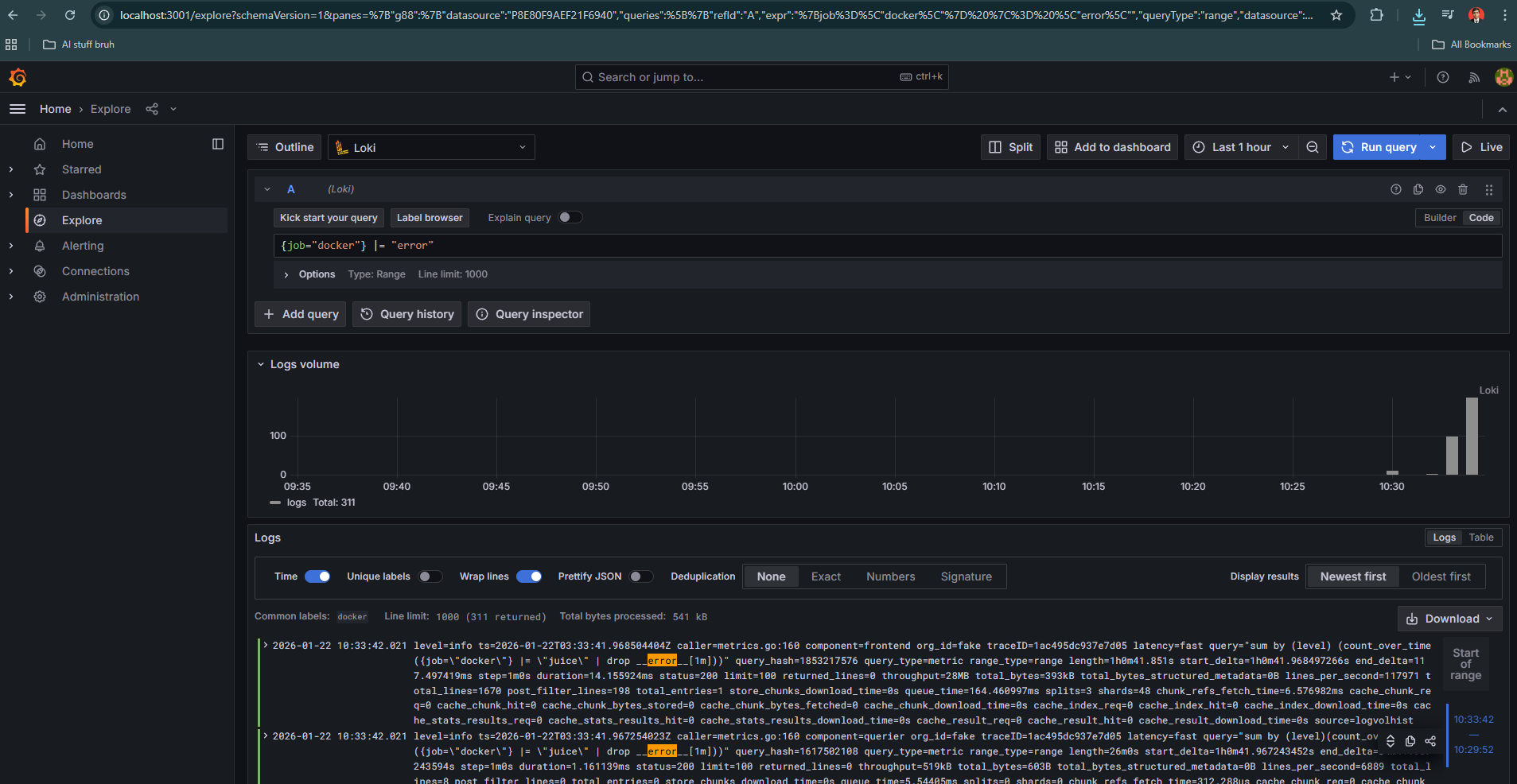
* 1. Baseline

Tahap baseline dilakukan untuk memahami kondisi normal sistem sebelum adanya simulasi serangan atau penerapan hardening. Pada tahap ini, aplikasi OWASP Juice Shop dijalankan dan digunakan secara wajar, sementara seluruh aktivitasnya dipantau menggunakan sistem logging dan monitoring terpusat berbasis Grafana dan Loki. Baseline ini berfungsi sebagai acuan awal untuk membedakan antara aktivitas normal dan aktivitas mencurigakan pada tahap berikutnya.

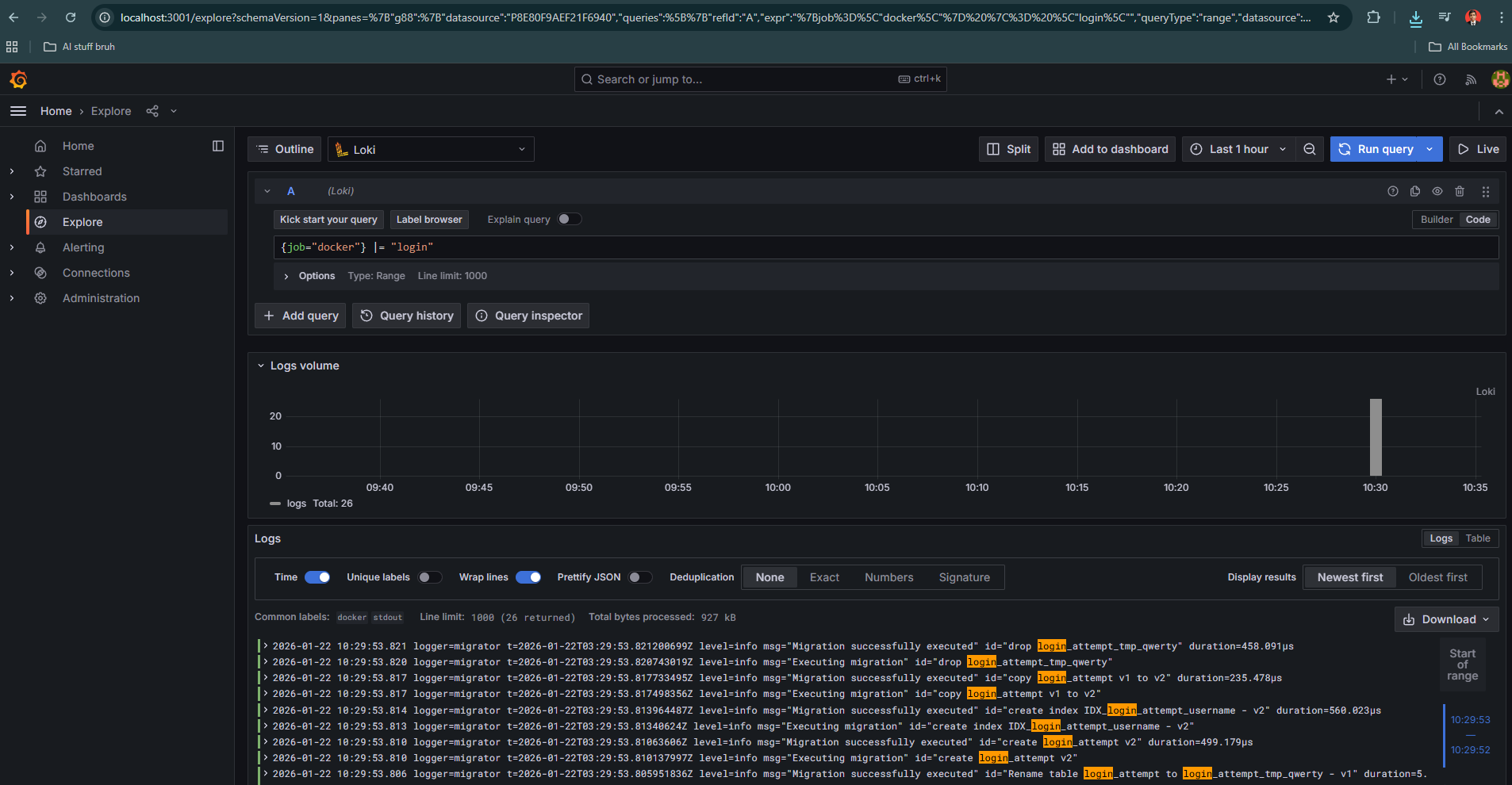


Pada tahap awal baseline, dilakukan observasi terhadap seluruh log yang dihasilkan oleh container Docker. Melalui fitur Explore di Grafana, semua log dengan label docker ditampilkan tanpa filter khusus. Dari hasil observasi, terlihat bahwa log dihasilkan secara kontinu seiring dengan aktivitas sistem dan interaksi pengguna normal. Tidak terdapat lonjakan log secara tiba-tiba maupun pesan error kritis yang muncul secara berulang. Hal ini menunjukkan bahwa seluruh container berjalan stabil dan sesuai dengan fungsi normalnya. 

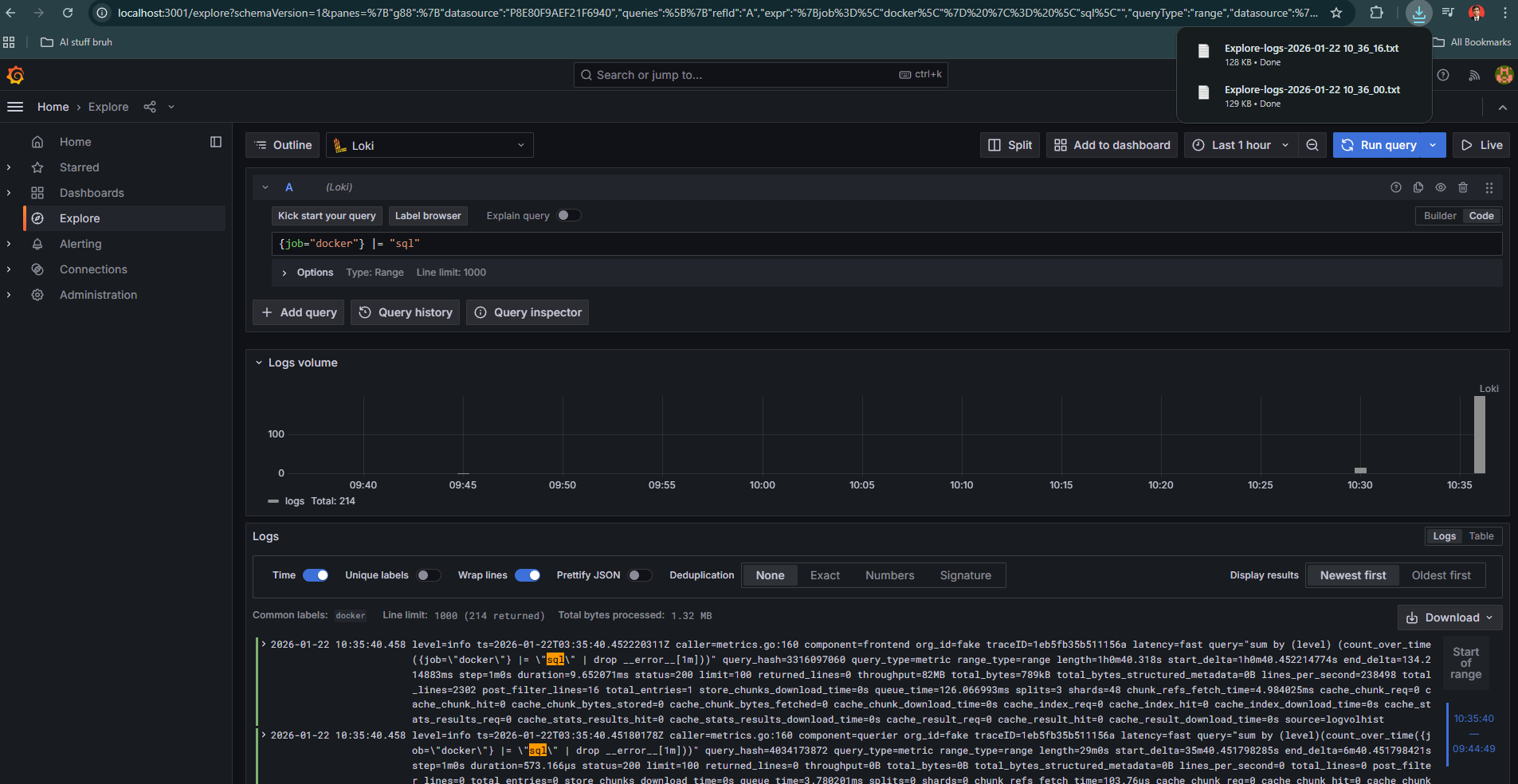
Selanjutnya dilakukan pemfilteran log yang secara spesifik berkaitan dengan aplikasi OWASP Juice Shop. Log yang muncul berasal dari aktivitas normal seperti pemuatan halaman, penampilan daftar produk, dan navigasi antarmuka pengguna. Pola log bersifat konsisten dan tidak menunjukkan anomali, yang mengindikasikan bahwa aplikasi berada dalam kondisi operasional normal tanpa adanya gangguan atau eksploitasi.



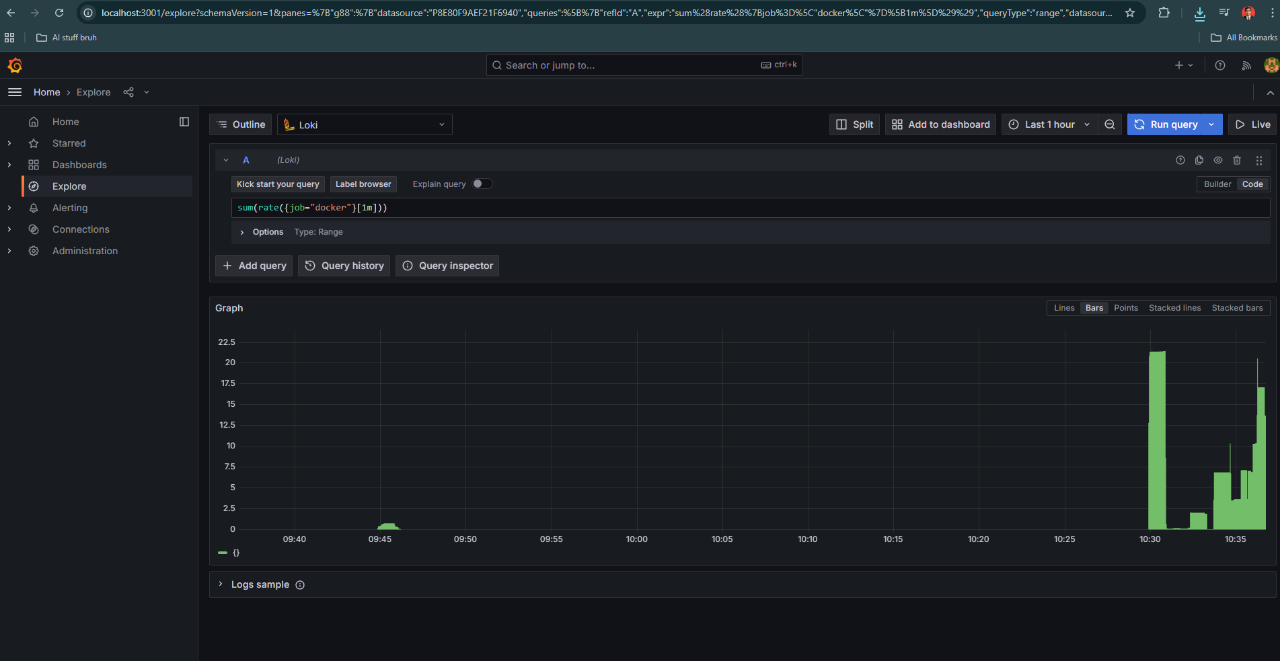
Pada tahap ini dilakukan pencarian log menggunakan kata kunci error untuk mengidentifikasi kemungkinan kegagalan sistem atau indikasi awal serangan. Hasil pencarian menunjukkan bahwa error yang muncul bersifat minor dan berasal dari proses internal sistem atau komponen monitoring. Tidak ditemukan error kritis yang berdampak pada ketersediaan aplikasi maupun error berulang yang dapat mengindikasikan serangan atau misconfiguration.



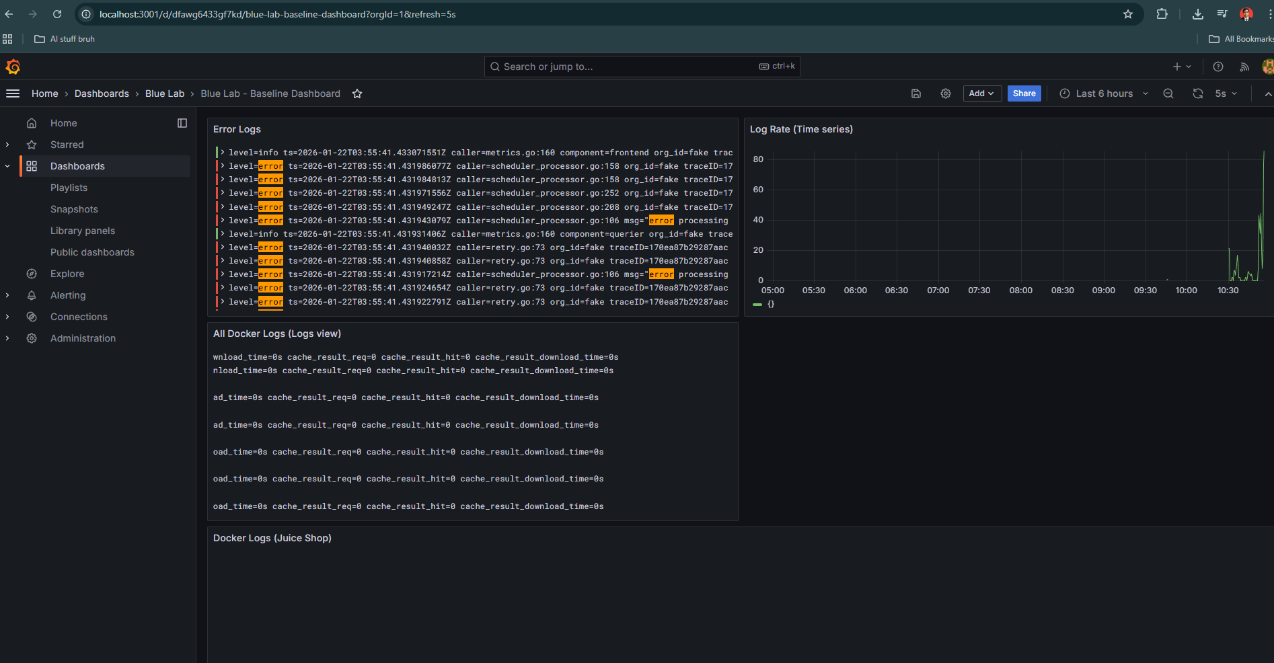
Log dengan kata kunci login dianalisis untuk memahami pola autentikasi pengguna pada kondisi normal. Dari hasil observasi, aktivitas login yang terekam bersifat terbatas dan tidak menunjukkan adanya percobaan login gagal secara berulang. Tidak terdapat indikasi brute force, credential stuffing, atau penyalahgunaan mekanisme autentikasi. Aktivitas login pada tahap baseline ini dapat dikategorikan sebagai aktivitas normal.



Untuk mendeteksi kemungkinan eksploitasi awal, dilakukan pencarian log menggunakan kata kunci sql. Pada tahap baseline, log yang muncul tidak berasal dari input pengguna yang mencurigakan, melainkan dari proses internal aplikasi dan sistem monitoring. Tidak ditemukan payload injection, error database, maupun query abnormal yang biasanya menjadi ciri serangan SQL injection. Hal ini menunjukkan bahwa pada fase baseline belum terjadi upaya eksploitasi terhadap layer database aplikasi.



Grafik laju log dianalisis untuk melihat stabilitas aktivitas sistem dalam rentang waktu tertentu. Hasil pengamatan menunjukkan bahwa laju log relatif stabil dan meningkat secara wajar sesuai dengan interaksi pengguna normal. Tidak terdapat lonjakan tajam yang biasanya menjadi indikator serangan, scanning agresif, atau kesalahan sistem dalam skala besar.

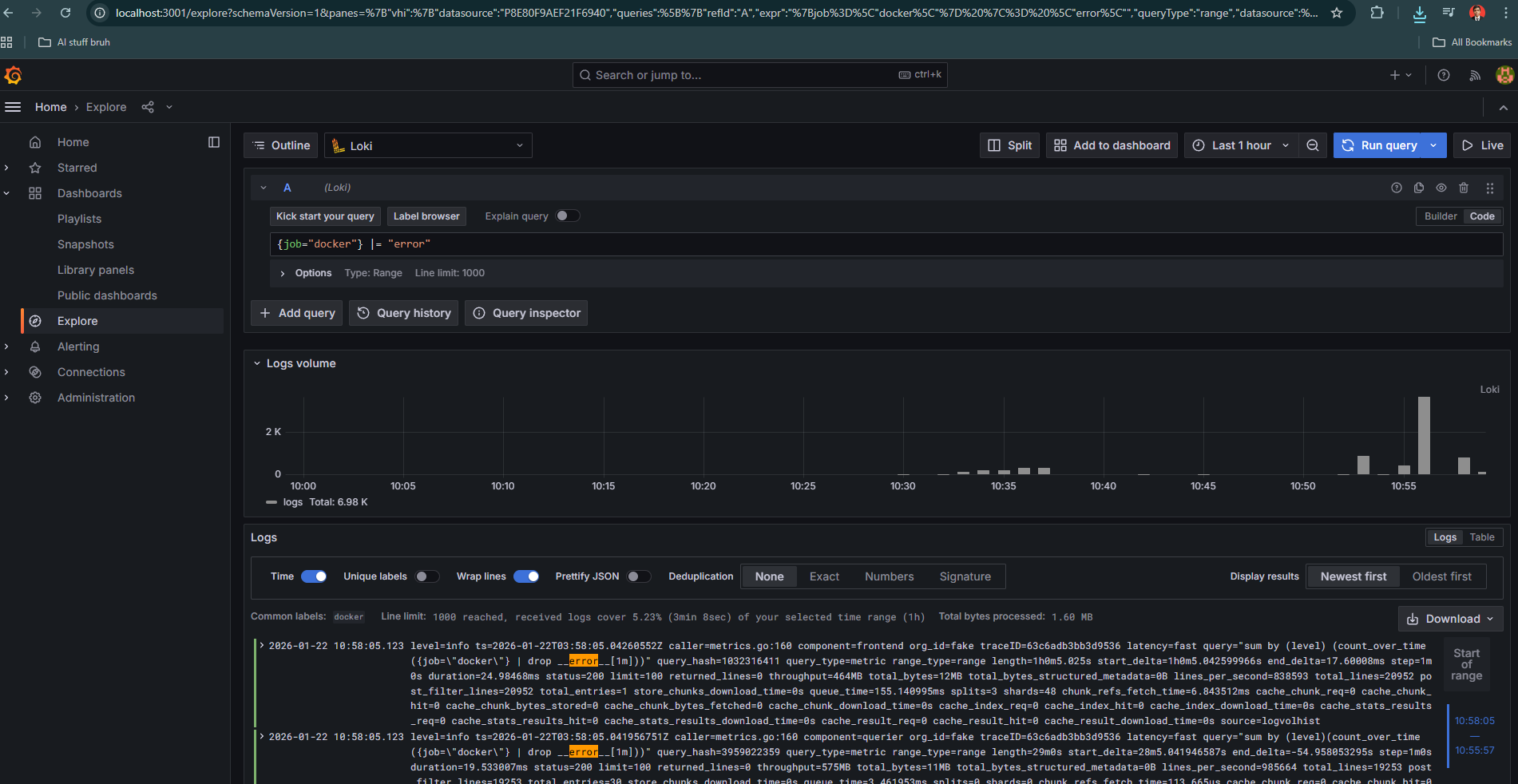


Dashboard baseline disusun untuk menyajikan ringkasan kondisi normal sistem secara visual. Dashboard ini menampilkan error log, laju log, serta ringkasan log aplikasi. Dashboard baseline berfungsi sebagai referensi utama yang akan dibandingkan dengan kondisi sistem pada tahap detection dan hardening. Dengan adanya dashboard ini, perubahan perilaku sistem dapat dengan mudah diidentifikasi secara visual.

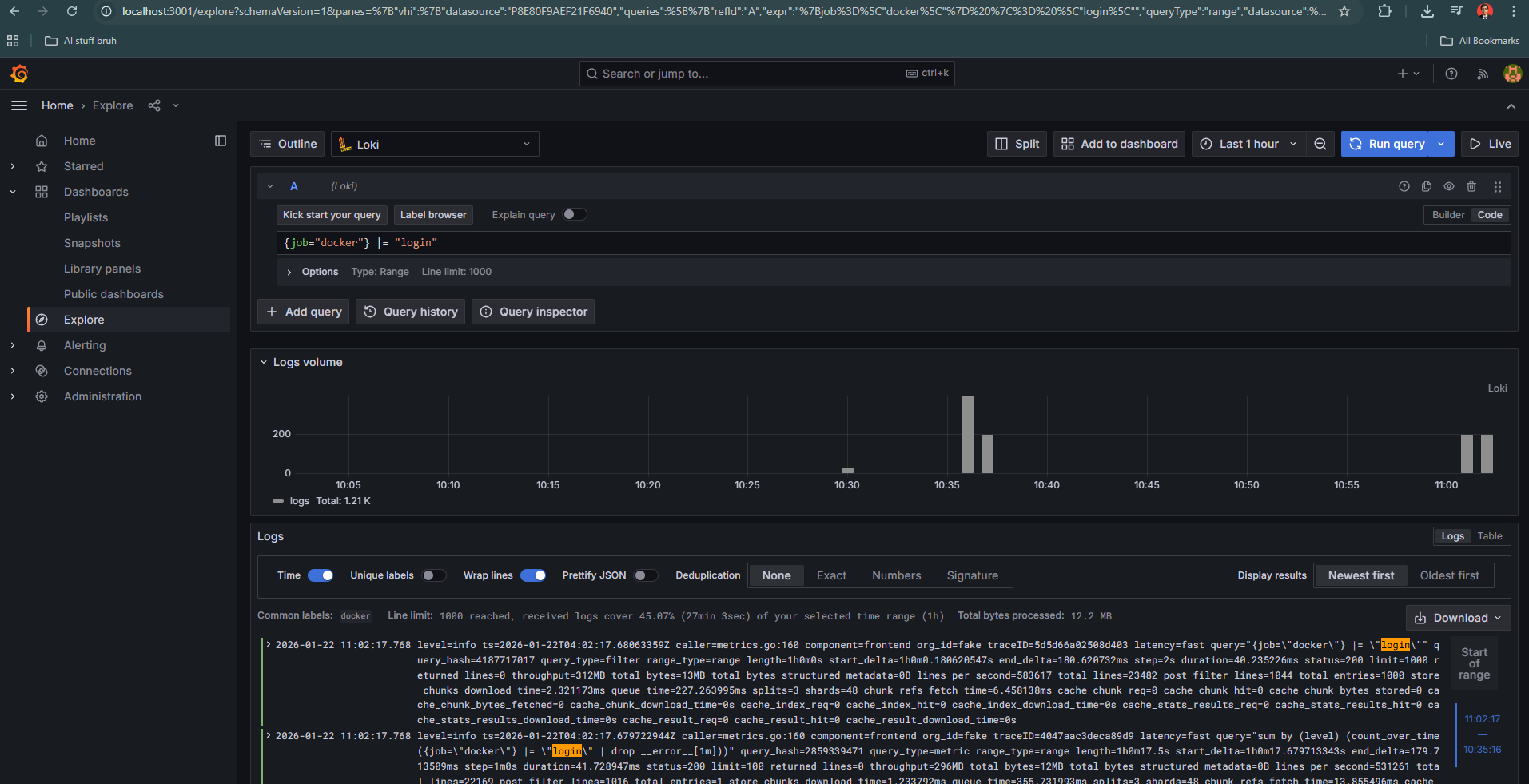
Selain observasi melalui dashboard, dilakukan pula analisis terhadap file log hasil ekspor dari Grafana Explore. File log ini berisi detail hasil query terhadap berbagai kata kunci penting seperti login dan sql. Dari hasil analisis, jumlah log yang terekam berada dalam batas normal dan tersebar secara merata dalam rentang waktu pengamatan. Tidak ditemukan pola login gagal berulang, lonjakan autentikasi, maupun indikasi eksploitasi injection. Metadata query dan status eksekusi menunjukkan bahwa sistem logging berjalan dengan baik dan mampu merekam aktivitas secara konsisten.

* 1. Detection

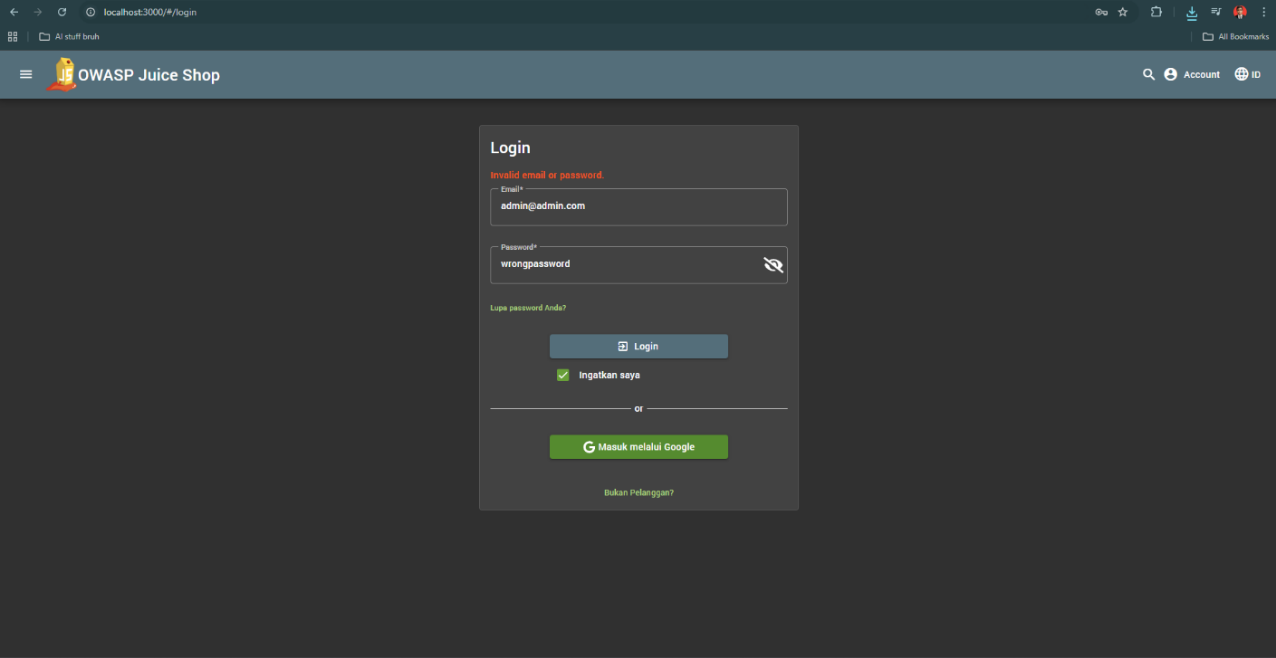
Tahap detection bertujuan untuk mengidentifikasi dan menganalisis aktivitas yang menyimpang dari baseline normal sistem. Pada tahap ini dilakukan simulasi aktivitas mencurigakan terhadap aplikasi OWASP Juice Shop untuk melihat bagaimana sistem logging dan monitoring mendeteksi indikasi insiden keamanan melalui log Docker yang dianalisis menggunakan Grafana dan Loki.



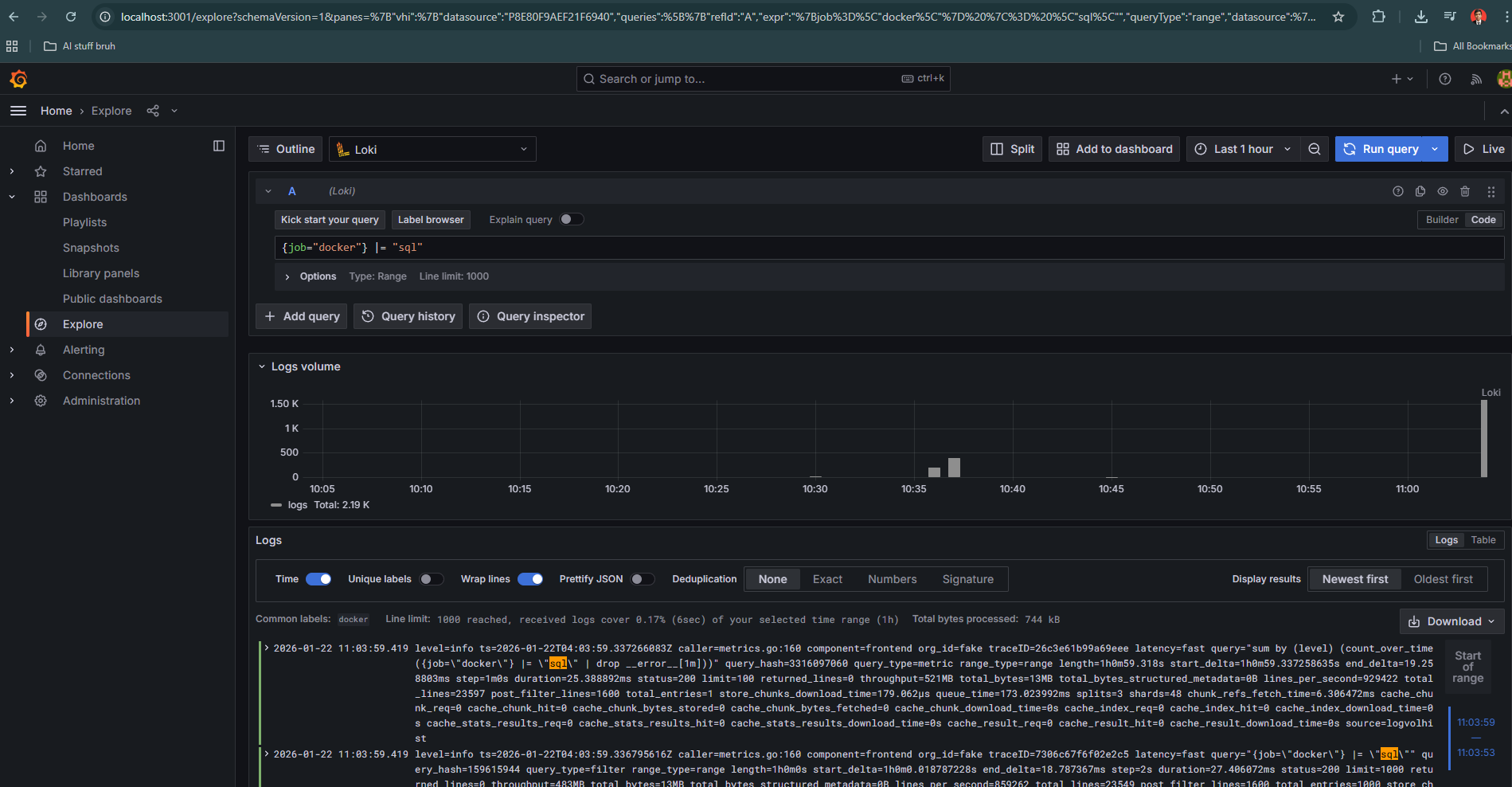
Pada gambar pertama terlihat hasil query log dengan kata kunci error. Aktivitas ini dipicu dengan memberikan input yang tidak valid atau tidak sesuai format pada aplikasi. Hasilnya, sistem menghasilkan sejumlah log error dalam waktu yang relatif berdekatan. Pola ini berbeda dengan baseline, di mana error hanya muncul secara sporadis. Munculnya error yang meningkat dalam waktu singkat menjadi indikator awal adanya aktivitas yang tidak normal.



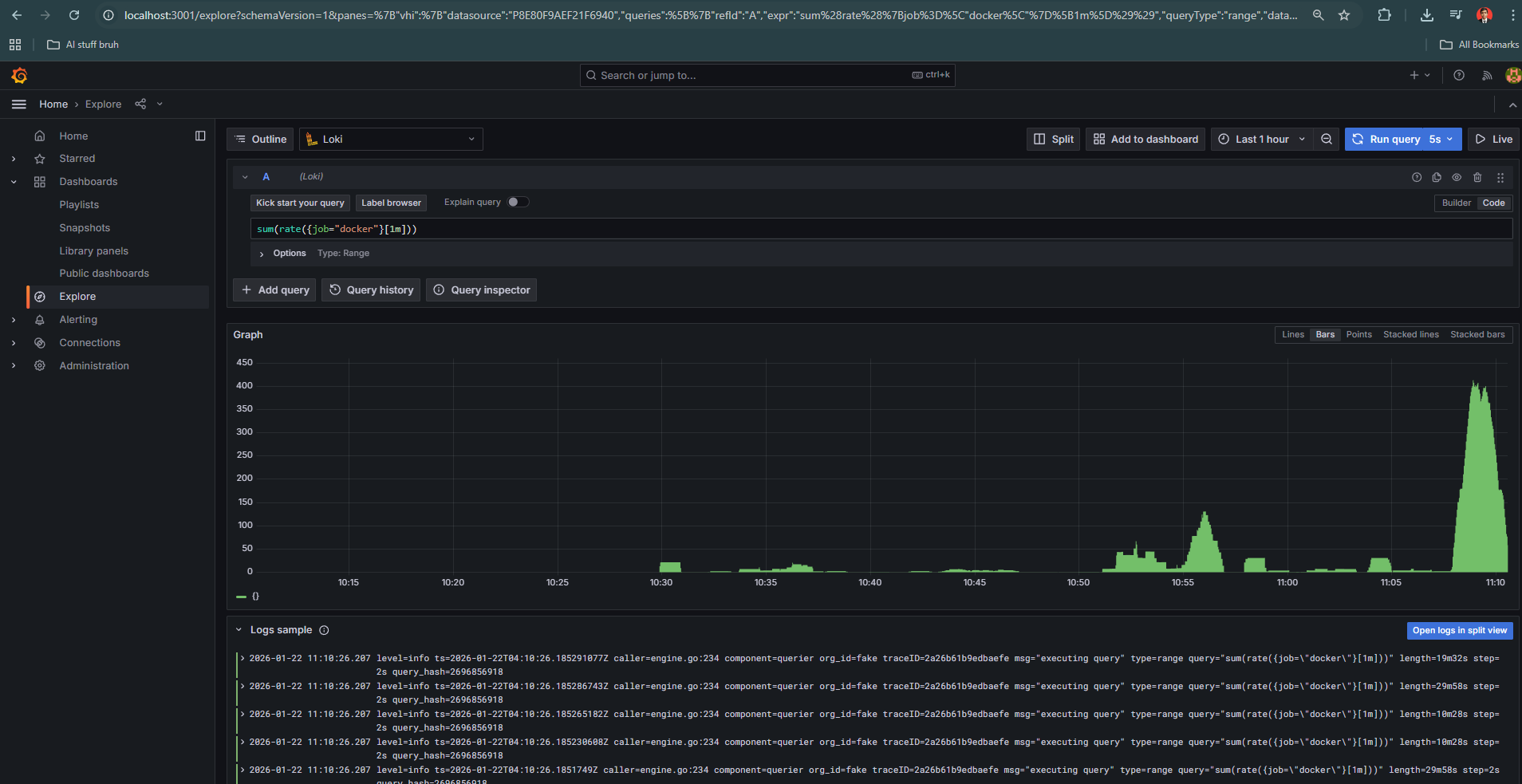
Gambar kedua dan ketiga menunjukkan aktivitas login gagal secara berulang pada halaman login OWASP Juice Shop. Pada sisi aplikasi, terlihat pesan kesalahan akibat kredensial yang salah. Sementara itu, pada sisi Grafana Explore, log dengan kata kunci login meningkat secara signifikan dalam rentang waktu yang singkat. Pola ini mengindikasikan adanya percobaan login berulang yang menyerupai brute force atau credential guessing, yang tidak ditemukan pada tahap baseline.



Gambar selanjutnya memperlihatkan hasil query log dengan kata kunci sql. Aktivitas ini disimulasikan dengan memasukkan payload yang menyerupai SQL injection pada input aplikasi. Log yang terekam menunjukkan adanya kata kunci terkait query database yang sebelumnya tidak muncul pada baseline. Walaupun aplikasi tidak berhasil dieksploitasi, keberadaan pola ini di dalam log menjadi indikator penting adanya upaya eksploitasi terhadap layer aplikasi atau database.



Pada gambar grafik laju log, terlihat lonjakan tajam jumlah log dalam waktu singkat. Lonjakan ini muncul bersamaan dengan aktivitas error, login gagal berulang, dan percobaan injection. Jika dibandingkan dengan grafik baseline yang stabil, spike ini merupakan deviasi signifikan yang menandakan adanya aktivitas tidak wajar. Analisis laju log menjadi metode efektif untuk mendeteksi insiden secara cepat tanpa harus membaca log satu per satu.

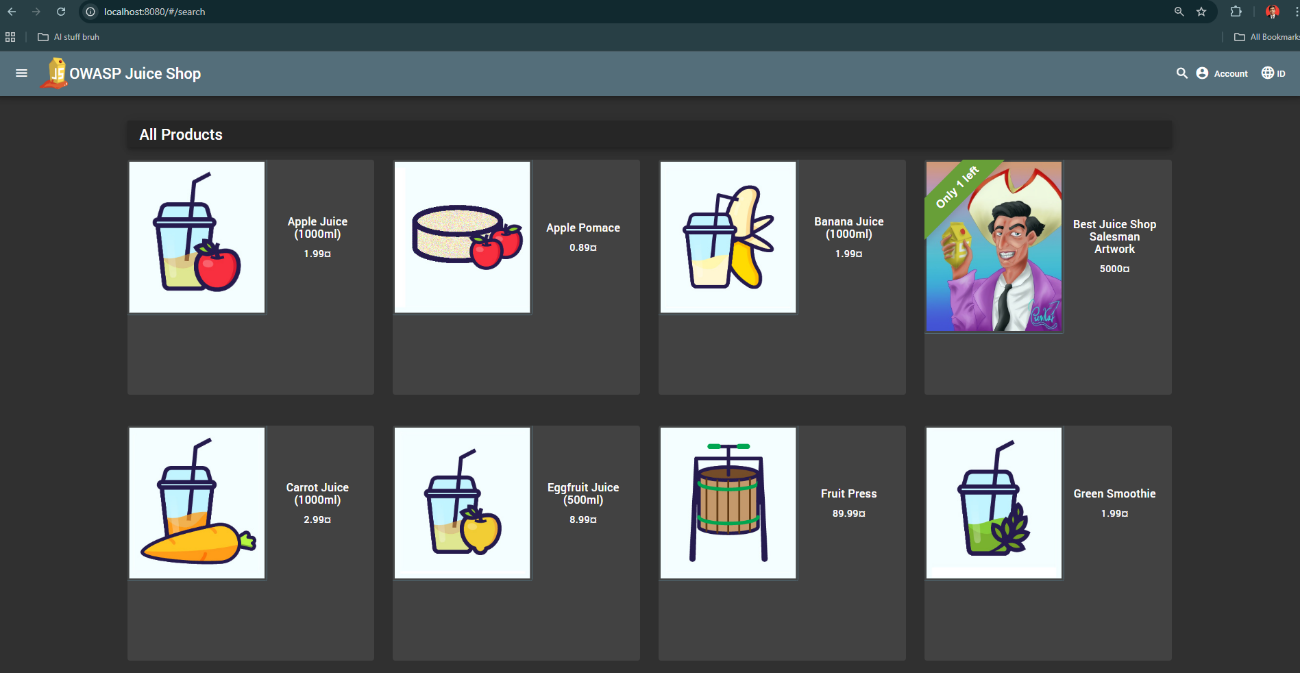


Selain observasi visual, dilakukan analisis terhadap file log hasil ekspor dari Grafana Explore. File log menunjukkan peningkatan jumlah entri dengan kata kunci error, login, dan sql dalam periode waktu yang berdekatan. Metadata log memperlihatkan bahwa volume log, throughput, dan jumlah baris per detik meningkat drastis dibandingkan baseline. Pola ini menguatkan indikasi bahwa sistem sedang mengalami aktivitas mencurigakan yang terkoordinasi, bukan sekadar penggunaan normal.

Tahap detection ini membuktikan bahwa sistem logging dan monitoring yang dibangun mampu berfungsi sebagai alat deteksi awal insiden. Informasi yang dihasilkan pada tahap ini menjadi dasar penting untuk melakukan tindakan lanjutan berupa hardening dan mitigasi guna menurunkan risiko serta mencegah kejadian serupa di masa mendatang.

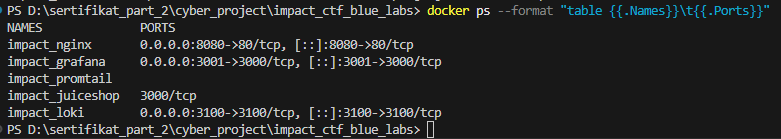
* 1. Hardening

Tahap hardening dilakukan sebagai respons langsung terhadap temuan pada tahap detection. Berdasarkan hasil analisis log, sistem menunjukkan indikasi aktivitas mencurigakan berupa lonjakan error, percobaan login berulang, pola injection, serta peningkatan laju request dalam waktu singkat. Oleh karena itu, diterapkan serangkaian kontrol keamanan defensif untuk memperkuat aplikasi web dan membatasi permukaan serangan (attack surface).



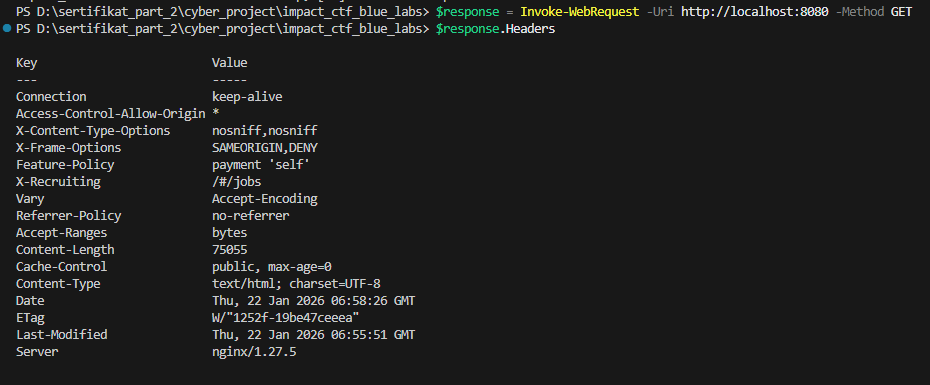
Gambar pertama menunjukkan bahwa aplikasi OWASP Juice Shop berhasil diakses melalui Nginx reverse proxy pada port 8080. Hal ini menandakan bahwa Nginx telah berfungsi sebagai lapisan depan (edge layer) yang menangani seluruh permintaan dari pengguna sebelum diteruskan ke aplikasi backend.

Dengan penerapan reverse proxy, akses pengguna tidak lagi langsung menuju aplikasi, melainkan melalui satu titik kontrol terpusat. Pendekatan ini umum digunakan dalam lingkungan produksi untuk meningkatkan kontrol keamanan, mempermudah penerapan kebijakan proteksi, serta meningkatkan visibilitas trafik masuk.



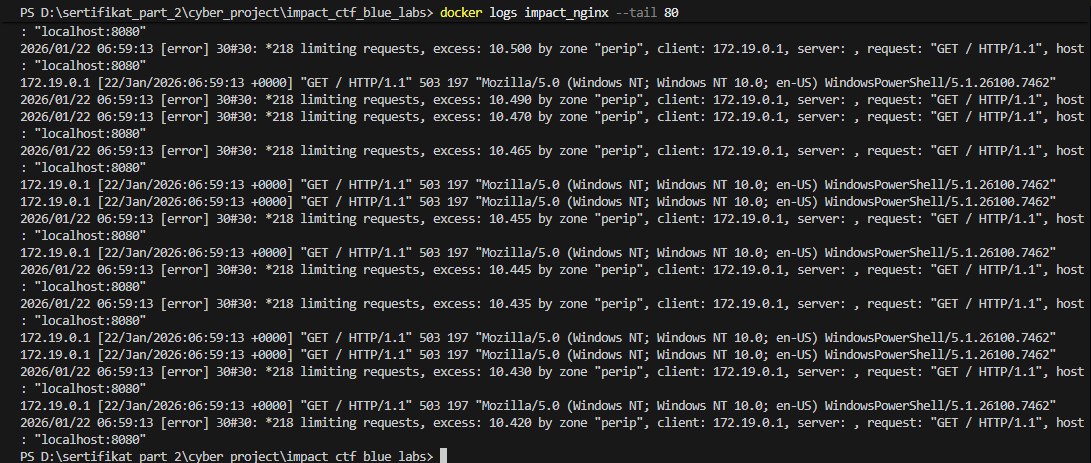
Gambar kedua memperlihatkan kondisi port mapping container setelah hardening diterapkan. Pada kondisi ini, port aplikasi OWASP Juice Shop tidak lagi diekspos langsung ke host. Hanya port Nginx yang dibuka untuk akses dari luar, sementara container aplikasi berada di jaringan internal Docker. Perubahan ini bertujuan untuk mengurangi risiko akses langsung ke aplikasi backend.

Dengan menutup port aplikasi dari host, potensi serangan langsung terhadap service backend dapat diminimalkan, dan seluruh trafik dipaksa melewati lapisan proteksi Nginx. Akses langsung ke port aplikasi lama (contoh: port 3000) tidak lagi dapat dilakukan. Upaya mengakses port tersebut gagal, yang menandakan bahwa hardening pada level jaringan dan port exposure telah berhasil diterapkan. Langkah ini merupakan bagian penting dari prinsip defense in depth, di mana lapisan keamanan tidak hanya diterapkan pada aplikasi, tetapi juga pada konfigurasi infrastruktur.



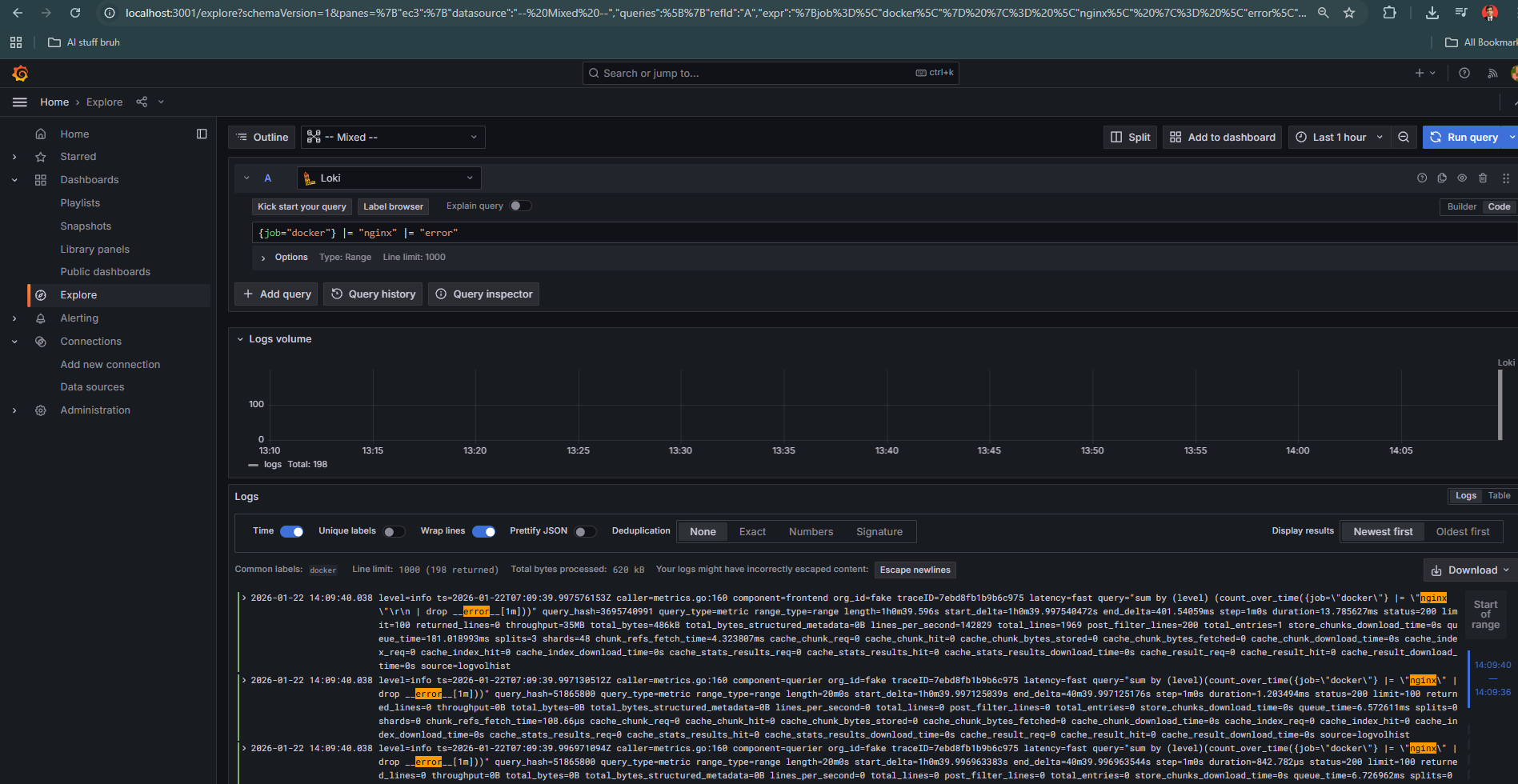
Gambar selanjutnya memperlihatkan hasil pemeriksaan HTTP response headers menggunakan PowerShell. Terlihat bahwa beberapa security headers telah aktif, seperti pengaturan untuk mencegah MIME sniffing, pembatasan framing, kebijakan referrer, serta kontrol fitur tertentu pada browser.

Penerapan security headers ini bertujuan untuk mengurangi risiko serangan berbasis browser, seperti clickjacking, content sniffing, dan penyalahgunaan konteks halaman. Meskipun tidak terlihat langsung oleh pengguna, konfigurasi ini berperan penting dalam meningkatkan keamanan sisi klien.



Pada gambar berikutnya ditampilkan log Nginx yang menunjukkan pesan pembatasan request (rate limiting). Log memperlihatkan bahwa permintaan berulang dalam jumlah tinggi dari satu sumber dibatasi dan ditolak oleh sistem. Hal ini membuktikan bahwa mekanisme rate limiting berjalan sesuai konfigurasi.

Rate limiting diterapkan untuk mengurangi dampak serangan seperti brute force login, request flooding, atau scanning agresif. Dengan adanya pembatasan ini, sistem menjadi lebih tahan terhadap lonjakan trafik tidak wajar yang sebelumnya terdeteksi pada tahap detection.



Gambar terakhir menunjukkan bahwa log Nginx berhasil masuk dan divisualisasikan di Grafana melalui Loki. Hal ini menandakan bahwa hardening tidak hanya menambah kontrol keamanan, tetapi juga meningkatkan visibilitas monitoring pada lapisan edge.

Dengan masuknya log Nginx ke sistem monitoring terpusat, aktivitas yang diblokir, dibatasi, maupun diteruskan dapat dianalisis secara real time. Ini memungkinkan Blue Team untuk melakukan korelasi antara log aplikasi dan log proxy, sehingga investigasi insiden menjadi lebih komprehensif.

* 1. Post

Tahap post merupakan tahap evaluasi akhir setelah proses detection dan hardening diterapkan pada lingkungan impact\_ctf\_blue\_labs. Pada tahap ini dilakukan peninjauan ulang terhadap kondisi sistem untuk memastikan bahwa kontrol keamanan yang telah diterapkan berjalan efektif dan mampu mengurangi risiko yang sebelumnya teridentifikasi. Fokus utama pada tahap ini adalah menilai perubahan perilaku sistem, stabilitas layanan, serta konsistensi mekanisme monitoring setelah hardening dilakukan.

Hasil evaluasi menunjukkan bahwa sistem berada dalam kondisi yang lebih terkendali dibandingkan sebelum hardening. Akses ke aplikasi telah terpusat melalui reverse proxy, lonjakan request dapat dibatasi dengan mekanisme rate limiting, dan aktivitas mencurigakan tidak lagi berdampak langsung ke aplikasi backend. Dari sisi monitoring, sistem logging mampu merekam dan menampilkan aktivitas penting secara konsisten, sehingga memudahkan proses observasi lanjutan dan analisis insiden.

Secara keseluruhan, tahap post menegaskan bahwa pendekatan Blue Team yang diterapkan berhasil meningkatkan posture keamanan sistem. Lingkungan menjadi lebih aman, terkontrol, dan siap untuk dilakukan pemantauan berkelanjutan. Tahap ini juga memastikan bahwa sistem tidak hanya aman secara konfigurasi, tetapi juga siap dari sisi operasional untuk mendukung proses incident response di masa mendatang.

1. Kesimpulan dan rekomendasi:
2. Pendapat penulis:
3. Verifikasi pelaksana:

* Pelaksana: Abiel Nathanael Georgius Pasaribu
* Tanggal: 22 Januari 2026
* Email: abielpasaribu@gmail.com
* Peran: Pemilik, Pengembang dan Security Tester
* Tanggal eksekusi: 22-23 Januari 2026
* Nomor telepon: 081338987883