LAPORAN KEAMANAN JARINGAN
SECURITY LOGGING AND MONITORING FAILURE

OLEH :

VEHA RAMADHAN DESENDAYA

3122640047

D4 LJ TEKNIK INFORMATIKA

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

Kegagalan logging dan monitoring keamanan merujuk pada situasi di mana mekanisme logging dan monitoring dalam suatu sistem atau aplikasi gagal secara efektif untuk menangkap dan menganalisis peristiwa atau insiden terkait keamanan. Kegagalan ini dapat menyebabkan kurangnya visibilitas terhadap ancaman atau pelanggaran keamanan potensial, sehingga sulit untuk mendeteksi, menyelidiki, dan menanggapi insiden keamanan dengan tepat waktu.

Beberapa penyebab umum kegagalan logging dan monitoring keamanan meliputi:

1. Konfigurasi logging yang tidak memadai: Jika mekanisme logging tidak dikonfigurasi dengan benar untuk menangkap peristiwa keamanan yang relevan atau jika tingkat logging yang digunakan tidak memadai, informasi penting terkait keamanan mungkin terlewatkan.

2. Gagal memonitor log: Bahkan jika logging dikonfigurasi dengan benar, jika tidak ada pemantauan dan analisis reguler terhadap log, insiden keamanan mungkin tidak terdeteksi. Penting untuk memiliki personel yang ditugaskan atau sistem otomatis yang secara aktif memantau log untuk aktivitas yang mencurigakan.

3. Kurangnya pemberitahuan dan notifikasi: Jika tidak ada pengaturan pemberitahuan dan notifikasi untuk peristiwa keamanan penting, pelanggaran atau anomali potensial mungkin tidak segera teridentifikasi dan ditindaklanjuti.

4. Data log yang tidak lengkap atau tidak akurat: Jika informasi yang tercatat tidak lengkap, inkonsisten, atau tidak memiliki detail yang relevan, hal ini dapat menghambat analisis dan penyelidikan insiden keamanan yang efektif.

5. Kekurangan kemampuan respons insiden: Jika tidak ada proses respons insiden yang ditetapkan atau sumber daya yang cukup untuk menangani insiden keamanan dengan efektif, dapat menyebabkan penanggapan yang terlambat atau tidak memadai.

Untuk mengatasi kegagalan logging dan monitoring keamanan, penting untuk menerapkan langkah-langkah berikut:

- Tentukan dan terapkan kebijakan dan konfigurasi logging yang komprehensif yang menangkap peristiwa keamanan yang relevan.

- Secara berkala tinjau dan analisis log untuk mengidentifikasi aktivitas yang mencurigakan atau anomali.

- Atur pemberitahuan otomatis untuk peristiwa keamanan yang kritis untuk memastikan respons yang tepat waktu.

- Pastikan integritas dan akurasi data log dengan menerapkan praktik manajemen log yang baik.

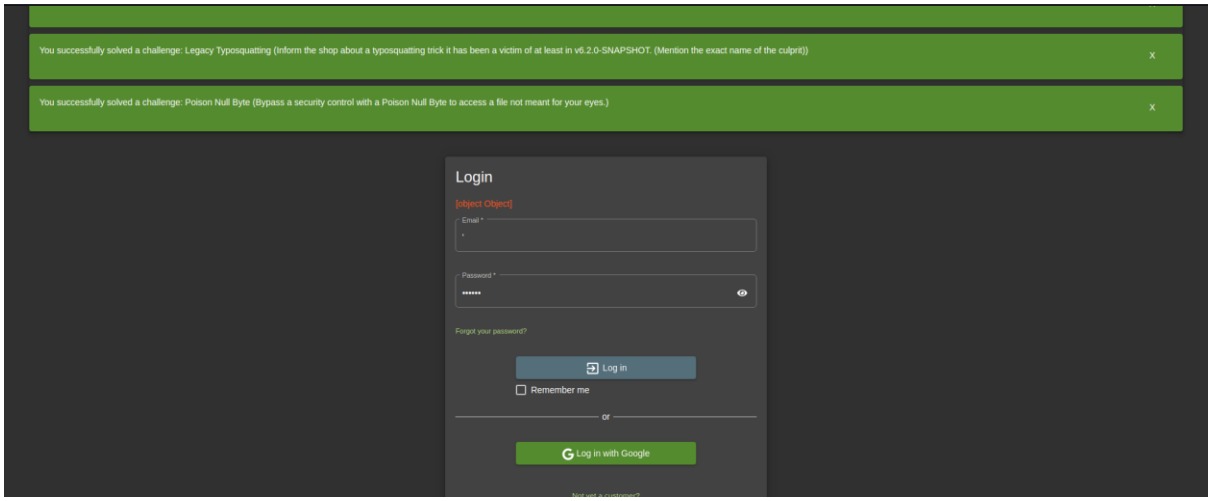
- Tetapkan rencana respons insiden yang efektif yang menjelaskan peran, tanggung jawab, dan tindakan yang harus dilakukan dalam kasus insiden keamanan.

- Secara rutin uji dan evaluasi mekanisme logging dan monitoring untuk memastikan efektivitasnya.

Dengan mengatasi masalah ini, organisasi dapat meningkatkan kemampuan mereka untuk mendeteksi dan menanggapi insiden keamanan, meningkatkan keamanan sistem secara keseluruhan, dan mengurangi dampak

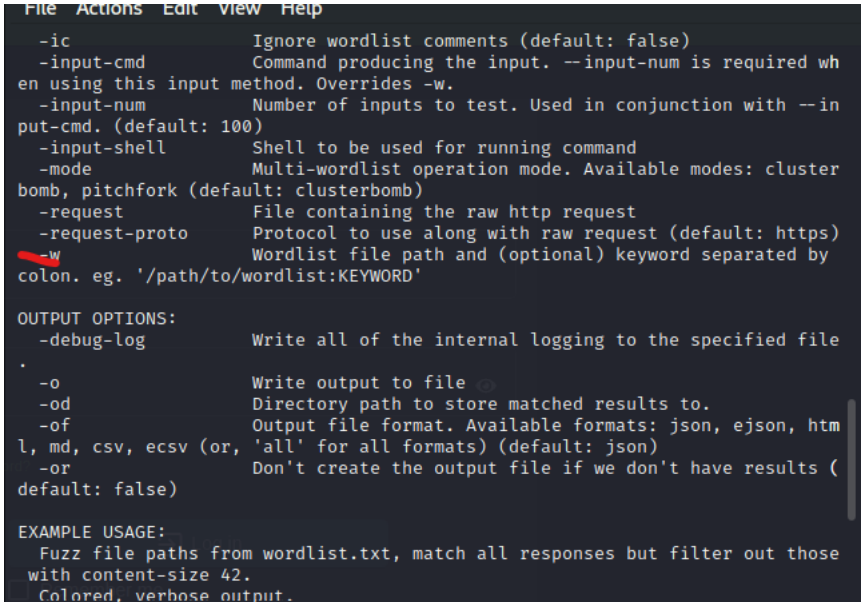
Percobaan 1

Buka aplikasi juice shop

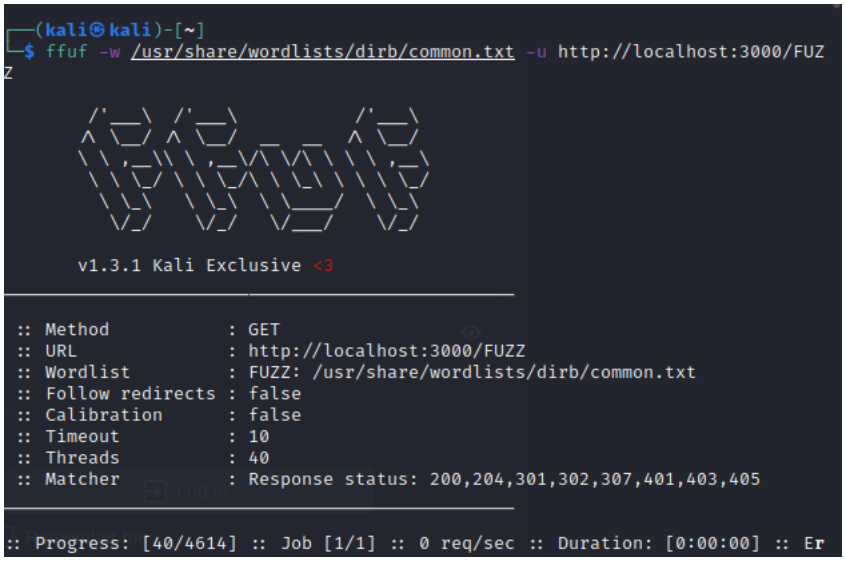


Gunakan FFUF

Pada kali ini kita akan gunakan ffuf -w untuk melakukan fuzzing terhadap aplikasi web



Jalankan perintah berikut ini



Perintah tersebut digunakan untuk menjalankan URL dengan url tambahan yang diambilkan dari wordlist “usr/share/wordlists/dirb/common.txt”

Wordlist tersebut berisi daftar kata yang umum digunakan untuk menguji dan mencari direktori atau file yang ada pada server web. Wordlist umum ini biasanya mencakup beberapa namafile umum, direktori umum, atau jalur URL yang sering digunakan dalam aplikasi web.