KEAMANAN JARINGAN

SECURITY LOGGING AND MONITORING FAILURES

Disusun Oleh :
Choirun Annas 3122640032
Muhammad Dzaky Mahfuzh 3122640050
D4 LJ B Teknik Informatika

Politeknik Elektronika Negeri Surabaya Kampus ITS Keputih Sukolilo
Surabaya 60111 Telp. 031-5947280, 031-5946114, Fax:031-594611

Laporan Praktikum

Security Logging and Monitoring Failures
Membantu dalam mendeteksi, mengeskalasi, dan menanggapi pelanggaran aktif. Tanpa pencatatan (logging) dan pemantauan (monitoring), pelanggaran tidak dapat dideteksi. Pencatatan deteksi harusnya dapat terjadi saat :
- Login berulang kali yang gagal
- Peringatan dan kesalahan akan menghasilkan pesan log yang tidak memadai
- Peringatan dan respons yang tidak ada Berikut merupakan daftar klasifikasi CWE pada kategori A9 ini :
- CWE-117 Improper Output Neutralization for Logs Memungkinkan penyerang memalsukan entri log atau konten berbahaya ke dalam log. Terjadi ketika :

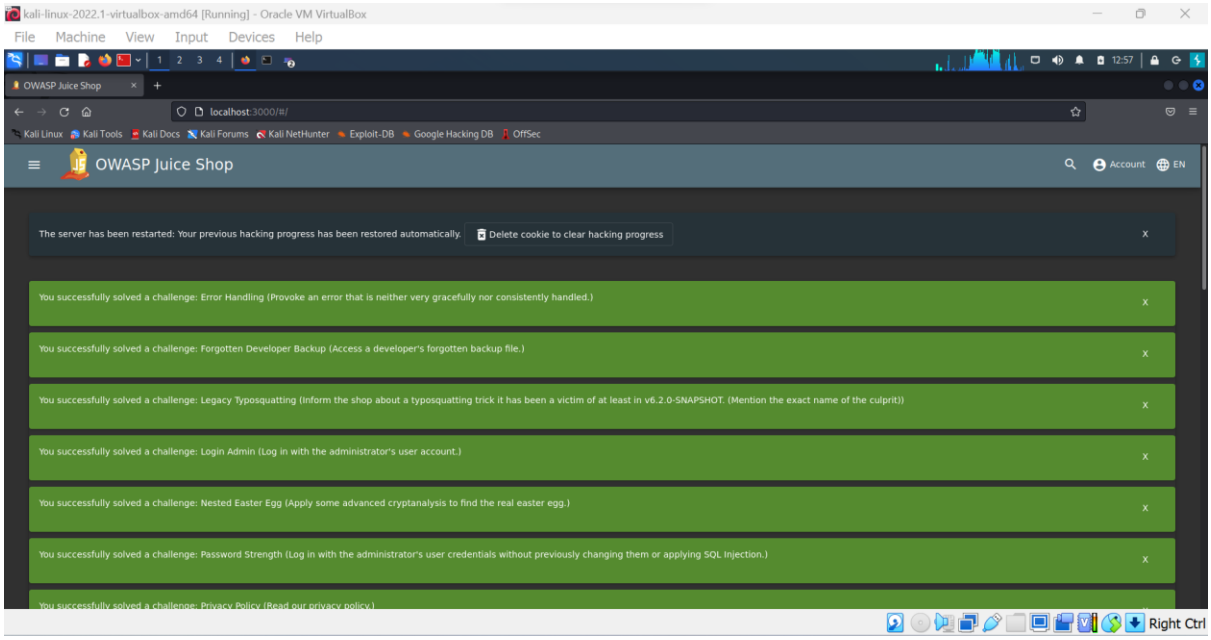
a. Data memasuki aplikasi dari sumber yang tidak terpercaya
b. Data ditulis ke file log aplikasi atau sistem
- CWE-223 Omission of Security-relevant Information Aplikasi tidak merekam atau menampilkan informasi yang penting untuk mengidentifikasi sumber atau sifat serangan atau menentukan apakah suatu Tindakan tidak aman.
- CWE-532 Insertion of Sensitive Information into Log File

a. Informasi yang ditulis ke file log dapat bersifat sensitive dan memberikan panduan berharga bagi penyerang atau mengekspos informasi pengguna yang sensitive
b. Meskipun mencatat semua informasi mungkin berguna selama tahap pengembangan, penting agar tingkat pencatatan diatur dengan tepat sebelum produk dikirimkan sehingga data pengguna yang sensitive dan informasi sistem tidak terpapar ke penyerang.

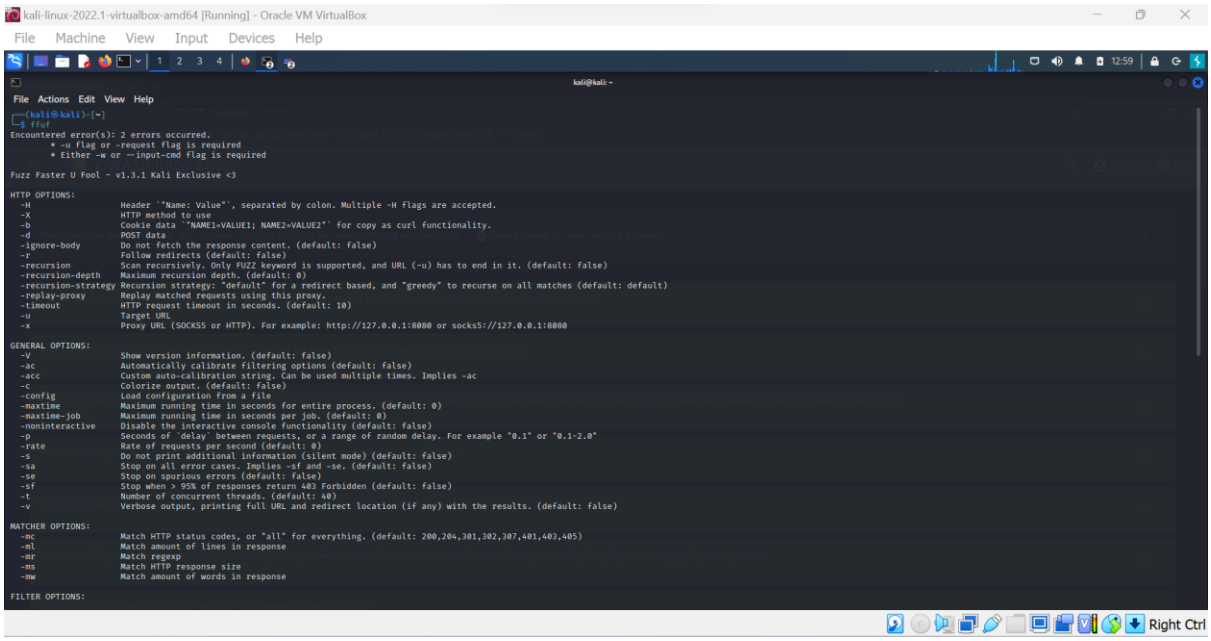
- CWE-778 Insufficient Logging
a. Perangkat tidak merekam peristiwa tersebut atau menghilangkan detail penting tentang peristiwa tersebut saat mencatatnya
b. Peristiwa penting keamanan tidak dicatat dengan benar, seperti Upaya login yang gagal berkali-kali.

Percobaan

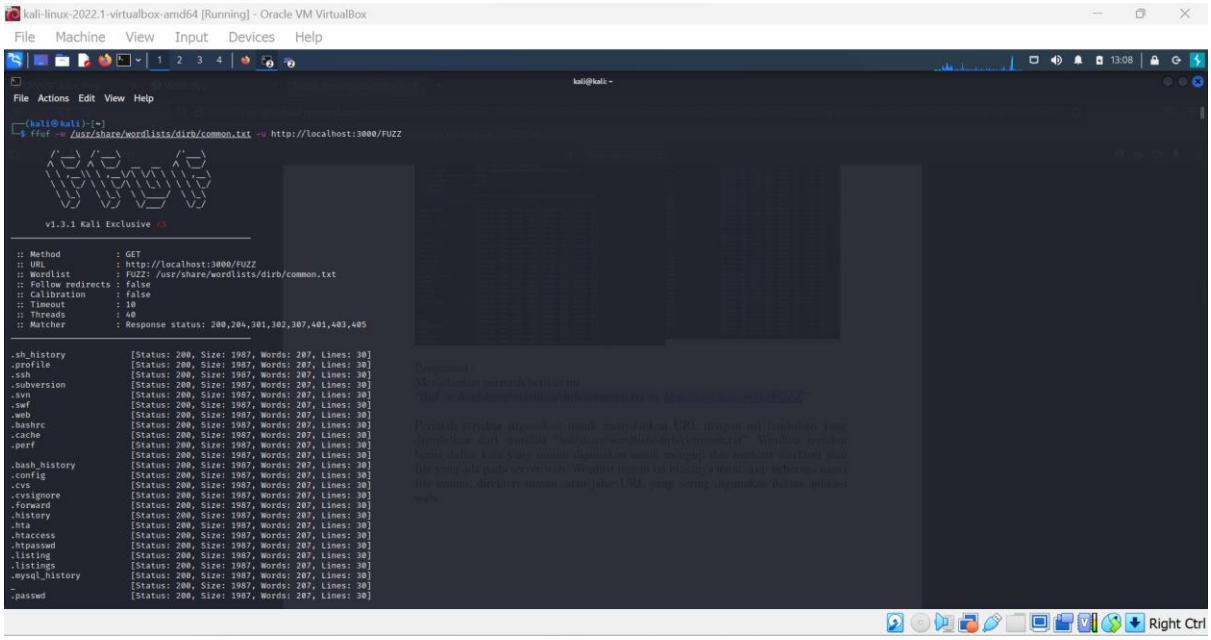
1. Start website juiceshop dengan menggunakan npm start



2. Menggunakan FFUF untuk melakukan fuzzing pada aplikasi web



3. Menjalankan perintah berikut ini : “ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/FUZZ” 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 nama file umum, direktori umum, atau jalur URL yang sering digunakan dalam aplikasi web.



4. Menambahkan perintah ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/support/FUZZ -fs 1987

5. Mendapatkan file acces log yang bersifat rahasia dari website