Laporan Analisis Kerentanan Backend Flask

Deskripsi Umum

Dokumen ini berisi hasil analisis kerentanan dari backend web berbasis Flask yang diberikan oleh pengguna. Analisis ini dilakukan secara statis terhadap file views.py, models.py, dan urls.py, serta konfigurasi yang terdeteksi.

1. Arsitektur Tidak Konsisten (Django + Flask Campur)

File views.py dan urls.py menggunakan pola Django, sedangkan models.py dan konfigurasi lainnya menggunakan Flask. Hal ini menyebabkan inkonsistensi besar dalam framework dan dapat menimbulkan error atau masalah keamanan.

2. Tidak Ada Proteksi CSRF

Semua form POST tidak dilengkapi token CSRF. Ini membuat aplikasi rentan terhadap serangan CSRF (Cross-Site Request Forgery).

3. Stripe Token Tidak Terverifikasi

Stripe token diambil dari POST tanpa validasi lebih lanjut. Penyerang dapat memalsukan token untuk membuat transaksi palsu.

4. Input Review Tidak Divalidasi

Rating dan review disimpan tanpa validasi format atau sanitasi, membuat sistem rentan terhadap XSS (Cross-Site Scripting).

5. Session Tidak Memiliki Batas Waktu Jelas

Opsi remember login disimpan tanpa batas waktu eksplisit, berisiko menyebabkan session hijacking.

6. IDOR (Insecure Direct Object Reference)

Beberapa objek seperti Order atau Review diakses tanpa pengecekan apakah user memiliki hak akses

terhadap objek tersebut.

Rekomendasi Umum

- Gunakan hanya satu framework: Flask atau Django.
- Tambahkan Flask-WTF untuk CSRF protection.
- Validasi semua input dari user dan sanitasi output ke browser.
- Gunakan session timeout.
- Validasi semua akses terhadap objek berdasarkan user_id.
- Simpan secret key dan token dalam variabel environment, bukan hardcoded.