LAPORAN RESMI KERENTANAN KEAMANAN (SQL INJECTION)

1. Ringkasan Eksekutif

Laporan ini mendokumentasikan temuan kerentanan SQL Injection (SQLi) pada salah satu endpoint milik Kampus. Kerentanan ini memungkinkan penyerang memodifikasi query database, mengakses data sensitif, atau melakukan tindakan tidak sah lainnya. Temuan dikategorikan High Severity karena berdampak pada confidentiality, integrity, dan availability.

2. Informasi Temuan

Jenis: SQL Injection

Kategori: OWASP Top 10 – A03 Injection

Severity: High

Tanggal Temuan: 1 Desember 2025

Reporter: Andi Fitra Furqan,S.T; CEH,ECIH / AFIF

3. Lokasi Kerentanan

Endpoint:

https://ujimaterial.polman-bandung.ac.id/

Parameter Rentan: id

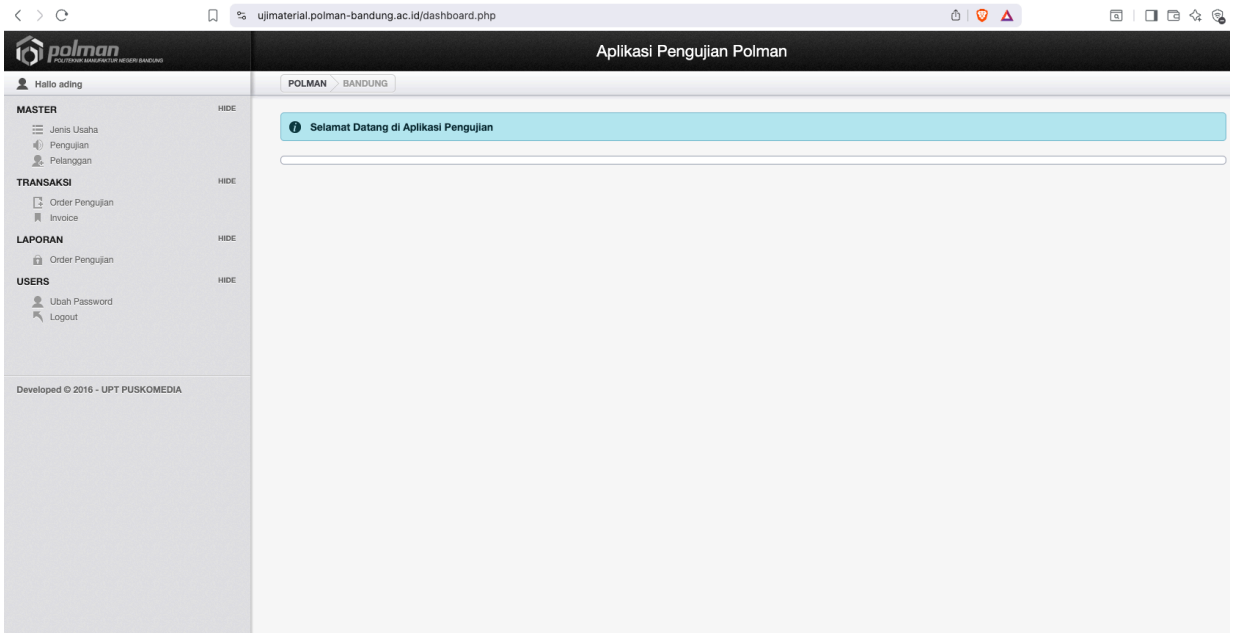
4. Langkah Reproduksi (Proof of Concept)

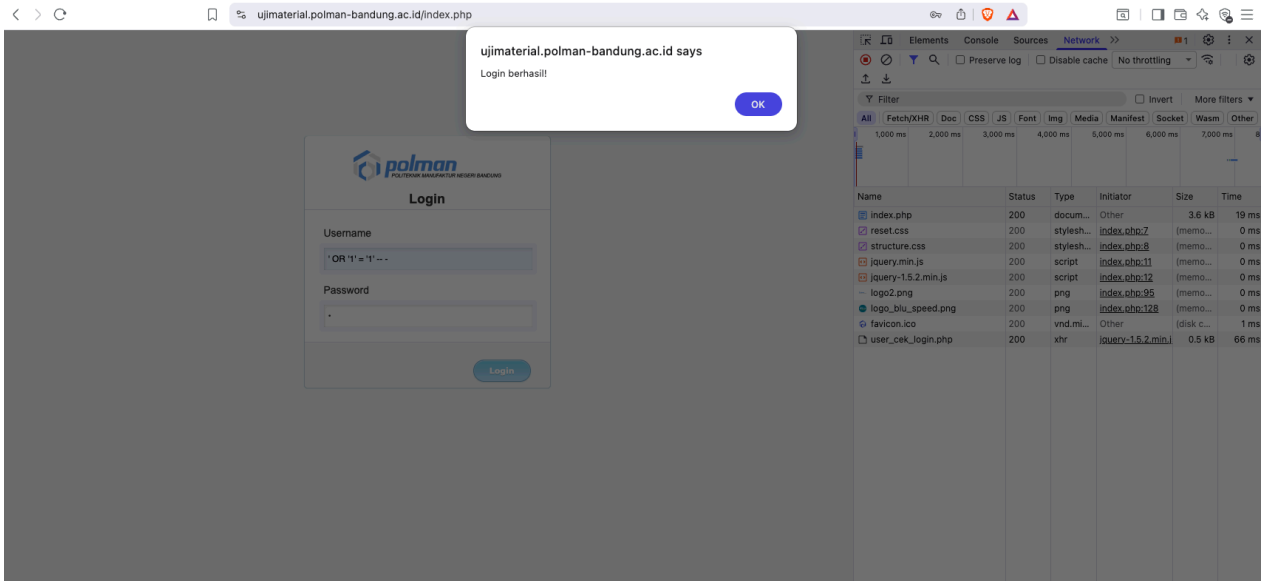
4.1 Error-Based Test

Payload: ‘ OR ‘1’ = ‘1’

Respon: True (Berhasil Login)

5. Bukti Pendukung





6. Analisis Dampak

– Potensi bocornya data sensitif (PII, data pelanggan, Mahasiswa)

– Potensi bypass authentication

– Potensi modifikasi atau penghapusan data

– Potensi RCE pada konfigurasi tertentu

– Potensi gangguan layanan

7. Root Cause

– Input tidak divalidasi

– Query menggunakan dynamic SQL (concatenation)

– Tidak ada prepared statements

– Error database terlihat secara publik

8. Rekomendasi Mitigasi

Teknis:

1. Gunakan prepared statements/parameterized queries.

2. Terapkan input validation dengan allowlist.

3. Sembunyikan error database dari publik.

4. Aktifkan WAF rule untuk SQLi.

Operasional:

1. Lakukan secure code review.

2. Implementasi DevSecOps.

3. Lakukan penetration testing berkala.

4. Monitoring SIEM untuk pola SQL Injection.

9. Penutup

Kerentanan ini perlu segera ditangani karena berdampak signifikan pada keamanan data dan operasional. Laporan ini disampaikan dalam semangat Responsible Disclosure untuk peningkatan keamanan sistem.