

Token Restricted Dapat Mengakses Credential Tingkat Akun

Format universal CyberSecAudit untuk temuan authorization yang memerlukan bukti kriptografi dan verifikasi state.

KATEGORI	RISIKO	BUKTI	DATA
Broken Access Control	Medium · rekomendasi	Reproduced	Owned only
00	Pemberitahuan Publikasi Rekonstruksi teredaksi dari pengujian terotorisasi. Nama target, domain, endpoint, akun, token, secret, identifier, dan bukti mentah tidak dipublikasikan.		
01	Ringkasan Eksekutif Token yang dibatasi ke satu akun bisnis tetap dapat membaca credential autentikasi tingkat akun dan mencabut satu credential disposable. Enforcement scope terbukti aktif pada resource pembanding.		
02	Security Invariant Token Restricted tidak boleh mengakses credential management global tanpa izin eksplisit yang terpisah dari scope bisnis.		
03	Prasyarat dan Ruang Lingkup Aktor memiliki token Restricted yang sah. Seluruh akun dan credential disposable dimiliki peneliti.		
04	Langkah Reproduksi • Konfirmasi scope A diterima dan scope B ditolak. • Gunakan token yang sama pada credential management tingkat akun. • Validasi exact secret pada operasi read-only. • Ubah satu karakter sebagai negative control. • Cabut credential disposable dan baca ulang inventory owner.		
05	Bukti Teknis restricted_scope_A → 200 comparison_scope_B → 403 credential_read → 200 [REDACTED] exact_secret → 200 one_character_mutation → 403 owner_inventory → credential removed		
06	Expected vs Actual Expected: token ditolak pada operasi credential global. Actual: read, reveal, dan revoke berhasil.		

07	Dampak Terverifikasi • Credential autentikasi terpisah berhasil diperoleh dan divalidasi. • Satu credential disposable milik owner berhasil dicabut.
08	Negative Controls • Tanpa token dan token salah ditolak. • Scope pembanding ditolak. • Secret termutasi satu karakter gagal.
09	Batas Klaim Tidak diklaim akses lintas tenant, downtime, penghapusan massal, atau kerugian finansial.
10	Remediasi Pisahkan permission metadata, reveal, create, rotate, revoke, dan delete. Tolak token Restricted pada operasi global secara default.
11	Cleanup dan Retest Credential sementara dinonaktifkan dan inventory dikembalikan ke baseline.

Konsultasi audit keamanan

<https://cybersecaudit.site/konsultasi> · securityteam@cybersecaudit.site