

A01:2021-Broken Access Control

Deskripsi

Broken Access Control adalah salah satu ancaman keamanan aplikasi/web yang paling serius dan menduduki peringkat pertama dalam OWASP Top 10. Kontrol akses adalah proses yang menentukan siapa yang memiliki hak untuk melihat atau menggunakan sumber daya dalam sistem. Kerentanan ini umumnya terjadi ketika sistem gagal menerapkan mekanisme kontrol akses yang memadai diantaranya:

- Tidak terdapat pengecekan akses kontrol dengan memodifikasi URL, *internal application state*, atau *HTML page*, atau menggunakan *custom API attack tool*.
- Mengizinkan *primary key* untuk dapat diganti ke record user lain, yang memungkinkan untuk melihat atau melakukan perubahan pada akun lain.
- Peningkatan sebuah privilege (*Elevation Privilege*), pengguna memiliki akses sebagai admin menggunakan akun *user standard*.
- Manipulasi metadata
- Konfigurasi yang salah pada CORS sehingga menyebabkan API mengakses sistem yang tidak diizinkan

Dampak

- Pengguna yang tidak berwenang dapat mengakses atau mengubah data yang seharusnya dilindungi.
- Pengambilalihan sistem
- Kerugian finansial dan kerusakan reputasi
- Konsekuensi hukum dan regulasi

Mitigasi

- Menolak semua akses kecuali ke direktori yang dapat diakses publik
- Melakukan implementasi mekanisme one time password (OTP) pada seluruh aplikasi sehingga meminimalisir penggunaan CORS.
- Menerapkan kontrol akses minimal pada pengguna (*least user privilege*)
- Menonaktifkan *directory listing web server* dan memastikan file metadata (contohnya *.git*) dan *file backup* tidak ada di dalam web roots.

- Mencatat kegagalan akses kontrol dan alert admin jika diperlukan (seperti adanya kegagalan yang terjadi berulang - ulang).
 - Membatasi ukuran API dan akses ke kontroler untuk meminimalisir kerusakan dari *automated attack tooling*.
 - *JWT tokens* harus langsung di hilangkan validasinya pada server setelah logout.
 - Melakukan pengujian kerentanan keamanan
-

Revision #2

Created 2025-10-04 01:07:40 UTC by Tim Persandian

Updated 2025-10-04 04:40:44 UTC by Tim Persandian