A07:2021 - Identification and Authentication Failures

Deskripsi

Identification and authentication failures merupakan kelemahan atau kegagalan dalam sistem identifikasi dan autentikasi yang dapat menyebabkan akses tidak sah atau kebocoran informasi sensitif. Hal ini dapat terjadi ketika aplikasi tidak berhasil memverifikasi identitas pengguna atau tidak mengelola akses dengan efektif. Kerentanan ini disebabkan antara lain karena:

- Mengijinkan bruteforce / serangan otomatis seperti isian kredensial, di mana penyerang memiliki daftar nama pengguna dan kata sandi yang valid.
- Mengijinkan penggunaan kata sandi bawaan atau lemah.
- Menggunakan pemulihan (*restore*) kredensial yang lemah atau tidak efektif dan proses lupa kata sandi yang tidak aman.
- Menggunakan password dengan teks biasa, terenkripsi, atau dengan hash yang lemah
- Memiliki otentikasi multi-faktor yang hilang atau tidak efektif.
- Mengekspos ID Sesi di URL
- Tidak membatalkan ID Sesi dengan benar. Sesi pengguna atau token autentikasi (terutama token single sign-on (SSO)) tidak divalidasi dengan benar selama logout atau periode tidak aktif.

Dampak

Kegagalan dalam aspek ini dapat menciptakan celah bagi penyerang untuk mendapatkan akses yang tidak sah, menyusup ke dalam sistem, atau mengeksploitasi data pribadi.

Mitigasi

- Mnerapkan otentikasi multi-faktor untuk mencegah pengisian kredensial otomatis, brute force, dan serangan penggunaan kembali kredensial yang hilang / dicuri.

- Tidak menggunakan kredensial bawaan apa pun, terutama untuk pengguna admin.
- Menerapkan pemeriksaan kata sandi (password)yang lemah, seperti menguji kata sandi baru.
- Menerapkan kata sandi (password) dengan mengatur panjang sandi, kompleksitas, dan kebijakan rotasi sesuai pedoman yang berlaku (misal NIST 800-63b)
- Pastikan pendaftaran, pemulihan (*restore*) kredensial, dan jalur API diperkuat terhadap serangan enumerasi akun dengan menggunakan pesan yang sama untuk semua hasil.
- Mencatata dan membatasi upaya login yang gagal.
- Menggunakan pengelola sesi built-in sisi server yang aman, menghasilkan ID sesi acak baru dengan entropi tinggi setelah login.
- ID sesi tidak boleh ada di URL, disimpan dengan aman, dan tidak valid setelah keluar, *idle*, dan waktu tunggu absolut.

Revision #1
Created 2025-10-04 03:49:27 UTC by Tim Persandian
Updated 2025-10-04 04:07:15 UTC by Tim Persandian