A03:2021 - Injection

Deskripsi

Kerentanan muncul ketika data yang tidak terpercaya dikirimkan ke interpreter, yang dapat menyebabkan eksekusi perintah yang tidak diinginkan. Kerentanan disebabkan antara lain:

- Kurangnya validasi input
- Sanitasi data yang tidak cukup
- Penggunaan metode pengolahan data yang tidak aman
- Kueri secara dinamis atau permintaan yang tidak diberikan parameter tanpa konteks-peringatan pengalihan

Dampak

- Penyerang bisa menyisipkan kode berbahaya yang akan dijalankan oleh sistem secara ilegal.
- Kebocoran data sensitif.
- Kerusakan sistem dan data
- Kerugian Finansial
- Kerusakan reputasi
- Konsekuensi hukum dan kepatuhan

Mitigasi

- Penyimpanan data terpisah dari perintah dan *query.*
- Menggunakan API yang aman yang mencegah penggunaan mesin penerjemah secara keseluruhan, menyediakan sebuah tatap muka berparameter, atau migrasi ke perangkat pemetaan relasi objek.
- Menggunakan daftar (*whitelist*) pada validasi input di sisi server.
- Menerapkan validasi dan sanitasi terhadap input pengguna.
- Menggunakan LIMIT dan kontrol SQL lainnya di antara *query* untuk mencegah terungkapnya data jika terjadi injection.
- Melakukan pengujian keamanan

Revision #2
Created 4 September 2024 01:53:42 by Tim Persandian
Updated 4 September 2024 04:44:34 by Tim Persandian