A04:2021 - Insecure Design Vulnerabilities

Deskripsi

Insecure design vulnerabilities adalah celah keamanan yang muncul akibat kurangnya perhatian atau perencanaan yang memadai pada aspek keamanan selama fase desain aplikasi atau sistem. Kerentanan ini terjadi ketika arsitektur dan perencanaan sistem tidak memperhitungkan ancaman potensial atau tidak mengikuti praktik keamanan yang terbaik.

Terdapat perbedaan antara desain tidak aman dan implementasi tidak aman. Sebuah desain aman masih bisa memiliki kerusakan implementasi yang mengarah ke kerentanan yang dapat dieksploitasi. **Suatu desain tidak aman tidak dapat diperbaiki oleh sebuah implementasi yang sempurna** . Satu dari faktor yang berkontribusi terhadap desain tidak aman adalah ketiadaan pembuatan profil risiko bisnis yang inheren dalam perangkat lunak atau sistem yang sedang dikembangkan, maka menjadi kegagagalan untuk menentukan desain keamanan level yang diperlukan.

Dampak

Sistem menjadi rentan terhadap eksploitasi bahkan sebelum proses implementasi dan pengujian dimulai.

Mitigasi

- Membuat dan menggunakan prosedur pengembangan secara aman untuk mengevaluasi dan mendesain kontrol keamanan.
- Menggunakan permodelan ancaman untuk autentikasi darurat, kontrol akses, *business logic*, dan *key flows.*
- Mengintegrasikan kendali dan bahasa keamanan ke dalam *use case.*
- Mengintegrasikan pengujian untuk *frontend* dan *backend*.
- Mensegregasikan lapisan tier pada sistem dan lapisan jaringan berdasarkan kebutuhan eksposur dan proteksi
- Mensegregasikan tenant secara robust dengan desain pada seluruh tier
- Membatasi konsumsi sumber daya oleh pengguna atau layanan

Revision #1
Created 2025-10-04 02:00:33 UTC by Tim Persandian
Updated 2025-10-04 02:10:53 UTC by Tim Persandian