

A02:2021 - Cryptographic Failures

Deskripsi

Cryptographic Failures, atau kegagalan kriptografi terjadi ketika mekanisme kriptografi yang digunakan untuk melindungi data tidak berfungsi dengan baik. Kegagalan kriptografi disebabkan antara lain:

- Tidak menerapkan enkripsi / pemilihan algoritma yang tidak tepat.
- Kesalahan dalam implementasi
- Manajemen kunci kriptografi yang kurang memadai.
- Pengguna tidak memverifikasi sertifikat elektronik dari server

Dampak

Kegagalan kriptografi dapat menimbulkan risiko keamanan siber yang serius, seperti kebocoran data sensitif, manipulasi data, kerugian finansial, dan kerusakan reputasi bisnis

Mitigasi

- Mengklasifikasikan data yang diproses, disimpan, atau dikirim oleh aplikasi sesuai dengan ketentuan perundang-undangan, persyaratan peraturan, atau kebutuhan bisnis.
- Menetapkan kontrol sesuai klasifikasi.
- Jangan menyimpan data sensitif yang tidak perlu.
- Mengenkripsi semua data sensitif pada *database*
- Menggunakan standar algoritma, protokol yang mutakhir dan kuat, serta menerapkan manajemen kunci yang tepat.
- Mengenkripsi semua data saat transmisi dengan protokol aman seperti TLS dengan *cipher perfect forward secrecy* (PFS), prioritas cipher oleh server, dan parameter yang aman. Menerapkan enkripsi seperti HTTP *Strict Transport Security* (HSTS).
- Menonaktifkan *caching* untuk respons yang berisi data sensitif.
- Menyimpan kata sandi (*password*) menggunakan fungsi *hashing* adaptif dan salted yang kuat.
- Verifikasi secara independen efektivitas konfigurasi dan pengaturan.

- Melakukan audit dan pemantauan keamanan.
-

Revision #2

Created 2025-10-04 01:28:23 UTC by Tim Persandian

Updated 2025-10-04 04:42:07 UTC by Tim Persandian