OWASP Top 10 | Improper Credential Usage (Beginner)

1. Apa yang dimaksud dengan “improper Credential Usage”?
    A. Penggunaan kredensial yang kuat dan unik
    B. Penggunaan kredensial default atau mudah ditebak
    C. Penggunaan authentication multifactor
    D. Penggunaan enkripsi untuk menyimpan data

    Jawaban: B

2. Mengapa penggunaan kata sandi seperti “123456” berisiko?
    A. Sulit diingat
    B. Mudah ditebak oleh penyerang
    C. Terlalu panjang
    D. Tidak dapat digunakan di semua situs

    Jawaban: B

3. Apa itu “credential stuffing”?
    A. Mengisi formulir pendaftaran dengan data palsu
    B. Menggunakan kredensial yang sama di banyak situs
    C. Menguji kombinasi nama pengguna dan kata sandi yang dicuri
    D. Menyimpan kredensial di tempat yang aman

    Jawaban: C

4. Bagaimana cara melindungi akun dari serangan brute force?
    A. Menggunakan kata sandi yang sama di semua akun
    B. Menonaktifkan autentikasi dua faktor
    C. Menggunakan autentikasi dua faktor (2FA)
    D. Menghindari penggunaan kata sandi

    Jawaban: C

5. Apa risiko menggunakan kredensial default pada perangkat atau aplikasi?
    A. Meningkatkan keamanan
    B. Memudahkan akses oleh penyerang
    C. Mengurangi kebutuhan pelatihan
    D. Tidak ada risiko

    Jawaban: B

6. Mengapa penting untuk mengganti kata sandi secara berkala?
    A. Untuk mempersulit penyerang menebak kata sandi
    B. Untuk mengikuti tren teknologi
    C. Untuk menghindari lupa kata sandi
    D. Tidak penting

    Jawaban: A

7. Apa itu manajer kata sandi (password manager)?
    A. Alat untuk membuat dan menyimpan kata sandi yang kuat
    B. Program untuk meretas kata sandi
    C. Layanan untuk membagikan kata sandi
    D. Sistem untuk menghapus kata sandi

    Jawaban: A

8. Apa yang harus dilakukan jika mencurigai akun telah diretas?
    A. Mengabaikannya
    B. Mengganti kata sandi dan mengaktifkan 2FA
    C. Menonaktifkan akun
    D. Membuat akun baru

    Jawaban: B

9. Apa itu Two Factor Authentication (2FA)?
    A. Menggunakan dua kata sandi yang berbeda
    B. Menggabungkan nama pengguna dan kata sandi
    C. Menggunakan dua metode verifikasi untuk masuk
    D. Menggunakan kata sandi yang panjang

    Jawaban: C

10. Mengapa tidak disarankan menggunakan kata sandi yang sama di beberapa akun?
    A. Memudahkan pengelolaan akun
    B. Mengurangi risiko keamanan
    C. Jika satu akun diretas, akun lain juga berisiko
    D. Tidak ada alasan khusus

    Jawaban: C

ISO/IEC 27001 | Organizational Controls (Beginner)

1. Apa tujuan utama dari kontrol organisasi dalam ISO/IEC 27001?
    A. Mengatur struktur organisasi
    B. Menetapkan kebijakan dan prosedur keamanan informasi
    C. Mengelola keuangan perusahaan
    D. Meningkatkan penjualan

    Jawaban: B

2. Siapa yang bertanggung jawab atas keamanan informasi dalam organisasi?
    A. Semua anggota organisasi
    B. Hanya manajer TI
    C. Hanya tim keamanan
    D. Hanya karyawan baru

    Jawaban: A

3. Mengapa penting memiliki kebijakan keamanan informasi tertulis?
    A. Untuk memenuhi persyaratan hukum
    B. Untuk memberikan panduan persyaratan kepada karyawan
    C. Untuk menunjukkan komitmen manajemen
    D. Semua jawaban benar

    Jawaban: D

4. Apa itu pelatihan kesadaran keamanan informasi?
    A. Pelatihan tentang penggunaan perangkat lunak
    B. Pelatihan tentang pentingnya menjaga keamanan informasi
    C. Pelatihan tentang pemasaran digital
    D. Pelatihan tentang manajemen proyek

    Jawaban: B

5. Apa langkah pertama dalam menerapkan kontrol organisasi?
    A. Menyusun kebijakan keamanan informasi
    B. Membeli perangkat lunak keamanan
    C. Mengganti semua kata sandi
    D. Memecat karyawan yang tidak patuh

    Jawaban: A

6. Mengapa penting melakukan penilaian risiko secara berkala?
    A. Untuk mengidentifikasi ancaman baru

B. Untuk memenuhi persyaratan ISO
C. Untuk mengurangi biaya operasional
D. Tidak penting

Jawaban: A

7. Apa itu peran dan tanggung jawab dalam konteks keamanan informasi?
   A. Tugas yang diberikan kepada karyawan
   B. Deskripsi pekerjaan umum
   C. Penugasan spesifik terkait keamanan informasi
   D. Tidak ada hubungannya

   Jawaban: C

8. Mengapa penting memiliki proses manajemen insiden keamanan informasi?
   A. Untuk mendokumentasikan semua aktivitas
   B. Untuk merespons dan memulihkan dari insiden dengan cepat
   C. Untuk melatih karyawan baru
   D. Untuk meningkatkan penjualan

   Jawaban: B

9. Apa itu kontrol akses dalam keamanan informasi?
   A. Proses mengatur siapa yang dapat mengakses informasi tertentu
   B. Proses membuat informasi tersedia untuk semua
   C. Proses menyimpan informasi di cloud
   D. Proses mencetak dokumen

   Jawaban: A

10. Mengapa penting melakukan audit internal terhadap sistem manajemen keamanan informasi?
    A. Untuk menemukan kesalahan dalam laporan keuangan
    B. Untuk memastikan kepatuhan terhadap kebijakan dan prosedur
    C. Untuk meningkatkan penjualan
    D. Tidak Penting

    Jawaban: B

Referensi:
OWASP Top 10 Vulnerabilities MCQ [Free PDF] - Objective Question Answer for OWASP Top 10 Vulnerabilities Quiz - Download Now!

OWASP Top 10 Quiz With Answers | Attempts: 47126 - Trivia & Questions

ISO 27001 Clauses Review questions Professional Development Quiz | Quizizz

Learning | Improper Credential Usage (OWASP Top 10)

Bayangkan kamu punya kunci rumah yang kamu simpan di bawah keset, gampang banget ditemukan orang, kan? Nah, Improper Credential Usage adalah kesalahan serupa, tapi di dunia digital. Ini terjadi saat aplikasi menyimpan atau kredensial (seperti username, password, token API, atau kunci enkripsi) dengan cara yang tidak aman.

Contoh yang sering Terjadi:

- Hardcoded Credentials
  Kredensial disimpan langsung di kode aplikasi. Kalau kodenya diretas atau di dekompilasi, siapapun bisa melihatnya.

- Password Default
  masih pakai password “admin” atau “123456”? Itu undangan terbuka bagi hacker.

- File Konfigurasi Tanpa Enkripsi
  Kredensial disimpan di file biasa, tanpa perlindungan. Bahaya kalau file ini jatuh ke tangan yang salah.

Risiko Nyata

- Akses ilegal ke sistem dan data sensitif.
- Pencurian data atau kerusakan sistem.
- Nama baik perusahaan bisa tercoreng.

Cara Aman Mengelola Kredensial

- Gunakan Credential Manager seperti Keystore, Keychain, atau Vault.
- Aktifkan MFA (Multi Factor Authentication) biar nggak cukup cuma tahu password.
- Jangan simpan kredensial di dalam kode.
- Selalu enkripsi data penting, termasuk saat dikirim.

Learning | Organizational Controls

Organizational Controls adalah semacam “aturan main” dan “pembagian peran” dalam organisasi untuk menjaga keamanan informasi. Tujuannya biar semua orang tahu tanggung jawabnya, dan sistem tetap aman.

Komponen Utama:

1. Kebijakan keamanan Informasi

Setiap orang tahu tugasnya. Misalnya siapa yang bertugas mengatur akses, siapa yang menangani insiden, dst.

2. Peran dan Tanggung Jawab
   Setiap orang tahu tugasnya. Misal, siapa yang bertugas mengatur akses, siapa yang menangani insiden, dst.

3. Manajemen Risiko
   Kenali risiko > Nilai dampaknya > Cari solusinya.

4. Pelatihan dan Kesadaran
   Karyawan diajak paham soal keamanan, bukan cuma IT nya saja.

5. Audit dan Review
   Cek berkala: Apakah kebijakan masih efektif? Sudah dijalankan belum?

Manfaat untuk Organisasi

- Patuh regulasi dan standar.
- Data lebih aman.
- Client dan mitra makin percaya.

Cara Implementasi

- Buat dan sebarkan kebijakan keamanan.
- Latih semua staf secara berkala.
- Audit dan evaluasi: jangan hanya sekali, tapi rutin.

referensi:
ICT Institute | ISO27002:2022 explained – Organizational controls
ISO 27001:2022 Annex A Controls - A Complete Guide
OWASP Mobile Top 10 | OWASP Foundation

OWASP Mobile Top 10

1. Improper Credential Usage
2. Inadequate Supply Chain Security
3. Insecure Authentication/Authorization
4. Insufficient Input/Output Validation
5. Insecure Communication
6. Inadequate Privacy Controls
7. Insufficient Binary Protections
8. Security Misconfiguration
9. Insecure Data Storage
10. Insufficient Cryptography

ISO/IEC 27001

1. Organizational Controls
2. People Controls
3. Physical Controls
4. Technological Controls

Achievement

1. **First Step Secured** : Menyelesaikan materi pertama.
2. **Quiz Novice**: Mencapai skor 100% pada quiz pertama.
3. **Streak Starter**: Menyelesaikan materi atau quiz selama 3 hari berturut-turut.
4. **Module Master**: Menyelesaikan semua materi dalam satu module.
5. **Quiz Champion**: Mencapai skor 100% pada semua quiz dalam satu modul.
6. **Consistency King**: Menyelesaikan aktivitas pembelajaran selama 7 hari berturut-turut
7. **Security Explorer**: Menyelesaikan materi dari kedua module.
8. **Perfectionist**: Mencapai skor 100% pada semua quiz di Hack n Go.
9. **Cybersecurity Guru**: Menyelesaikan semua materi dan kuis di aplikasi.