

Nama : Naufal Mussyafa Arrada
NIM : 20230801306
Mata Kuliah : Keamanan Informasi

1.Keamanan informasi adalah praktik untuk melindungi informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau kerusakan yang tidak sah. Tujuannya adalah untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi.

2. Confidentiality

(Kerahasiaan): Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang.

Integrity

(Integritas): Menjaga keakuratan dan keutuhan informasi agar tidak diubah oleh pihak yang tidak berwenang.

Availability

(Ketersediaan): Memastikan bahwa informasi dapat diakses saat dibutuhkan oleh pihak yang berwenang.

3. Phishing

Malware (virus, trojan, ransomware)

SQL Injection

Cross-Site Scripting (XSS)

Denial of Service (DoS)

Man-in-the-Middle (MitM)

Weak passwords

Software dengan celah keamanan (vulnerable software)

4 Hash:

Proses mengubah data menjadi string tetap menggunakan algoritma seperti SHA-256.

Hash tidak bisa dikembalikan ke bentuk asalnya. Umumnya digunakan untuk verifikasi data seperti password.

Encryption:

Proses mengubah data menjadi bentuk yang tidak bisa dibaca tanpa kunci dekripsi. Berfungsi untuk melindungi kerahasiaan data saat disimpan atau dikirim.

5. Session:

Proses penyimpanan informasi pengguna sementara setelah proses login, agar pengguna tidak perlu login ulang setiap kali berpindah halaman.

Authentication:

Proses untuk memastikan identitas pengguna, biasanya dengan username dan password, biometrik, atau token.

6. Privacy (Privasi):

Hak individu untuk mengontrol bagaimana data pribadinya dikumpulkan, digunakan, dan dibagikan.

ISO (International Organization for

Standardization): Organisasi internasional yang mengembangkan standar, termasuk ISO/IEC 27001

yang mengatur sistem manajemen keamanan informasi.