

1. Jelaskan menurut anda apa itu keamanan informasi!

Keamanan informasi adalah upaya untuk melindungi informasi dari berbagai ancaman agar tetap aman, utuh, dan dapat diakses oleh pihak yang berwenang. Tujuannya adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi.

2. Jelaskan menurut anda apa itu Confidentiality, Integrity dan Availability!

- Confidentiality (Kerahasiaan): Menjaga informasi agar tidak diakses oleh pihak yang tidak berwenang.
- Integrity (Integritas): Menjamin data tidak dimodifikasi secara tidak sah.
- Availability (Ketersediaan): Memastikan data selalu tersedia saat dibutuhkan oleh pengguna yang berwenang.

3. Sebutkan jenis-jenis kerentanan keamanan yang anda ketahui!

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Brute Force Attack
- Insecure Deserialization
- Man in the Middle (MitM)

4. Jelaskan minimal dua istilah keamanan hash dan encryption!

- Hash: Fungsi satu arah untuk mengubah data menjadi string tetap, seperti bcrypt() atau sha256, umumnya untuk menyimpan password.
- Encryption: Proses menyandikan data agar tidak bisa dibaca oleh pihak tidak berwenang, dan dapat didekripsi kembali dengan kunci tertentu.

5. Jelaskan menurut anda apa itu session dan authentication!

- Session: Mekanisme penyimpanan sementara informasi user setelah login.
- Authentication: Proses memverifikasi identitas pengguna (contoh: login menggunakan email dan password).

6. Jelaskan menurut anda apa itu privacy dan ISO!

- Privacy: Hak individu untuk mengontrol bagaimana data pribadinya dikumpulkan dan digunakan.
- ISO: Standar internasional (seperti ISO/IEC 27001) untuk sistem manajemen keamanan informasi yang digunakan untuk menjaga dan mengatur keamanan data.