1. Keamanan informasi adalah sebuah perlindungan pada data dan system informasi, mulai dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan. Tujuan dar keamanan ini adalah untuk memastikan kerahasiaan informasi, atau bisa disebut dengan CIA Triad.
2. Dalam konteks keamanan informasi Confidentiality atau kerahasiaan berguna dalam meastikan bahwa data hanya diakses oleh pihak yang berwenang. Ini melindungi informasi sensitive dari pengungkapan yang tidak sah. Integrity atau integritas ialah menjamin agar data tetap akurat, lengkap, dan tidak diubah atau dimodifikasi tanpa izin, hal ini merujuk pada perlindungan manipulasi pada data baik sengaja maupun tidak disengaja. Availability merujuk pada data dan system informasi dapat diakses oleh pengguna yang berwenang kapan saja dibutuhkan.
3. Jenis jenis kerentanan keamanan meliputi :
    1. SQL injection
    2. Cross-site scripting (XSS)
    3. Phising
    4. Malware
    5. Denial of Service (DoS)
4. Hash adalah proses mengubah data seperti password menjadi string tetap dengan menggunakan algoritma seperti Bcrypt, sehingga tidak bisa dikembalikan ke bentuk asli dan digunakan untuk verifikasi integritas atau penyimpanan aman.

    Encryption merupakan proses dua atah yang mengubah data sensitive seperti nomor induk menjadi chypertext dengan kunci yang bisa dienkripsi Kembali oleh pihak berwenang menggunakan kunci yang sama ataupun berbeda.
5. Session merupakan mekanisme yang yang mengacu pada penyimpanan informasi pengguna sementara selama user masih berinteraksi dengan system, misalnya setelah login. Dalam Laravel, session dienkripsi dan dikelola dengan aman guna mencegah manipulasi pada data oleh pihak luar.

    Authentication adalah proses memverifikasi identitas pengguna sebelum memberi akses, contohnya dengan memeriksa username dan password terhadap database. Authentikasi bertugas dalam mencegah akses yang tidak sah ke data sensitif seperti data pribadi,
6. Privacy merujuk pada perlindungan data pribadi pengguna agar hanya dapat diakses pengguna yang sah. Data tersebut mencakup data yang sensitive seperti data pribadi, atau Perusahaan agar tidak bocor ke pihak yang tidak berwenang.

    ISO merupakan kerangka kerja internasional yang banyak digunakan dalam mengelola dan melindungi informasi dengan system manajemen keamanan informasi. Standar ini membantu organisasi mengidentifikasi risiko, menerapkan control keamanan seperti authentifikasi dan backup, serta kepatuhan dalam praktik yang terbaik.