DAFTAR ISTILAH

Attacker	:Pihak yang melakukan serangan.
Walkthrough	:Sebuah langkah-langkah dalam menyelesaikan suatu pekerjaan.
Illegal	:Suatu kegiatan yang dilakukan tanpa izin.
Vulnerability	:Kerentanan atau celah keamanan pada suatu sistem.
Threat	:Sebuah ancaman keamanan yang sewaktu-waktu bisa dilakukan eksploitasi.
Control	:Sebuah langkah untuk mengelola ancaman.
Web Application Firewall	:Suatu metode untuk mengamankan aplikasi web dari serangan.
Software	:Program atau aplikasi yang diisikan ke dalam memori internal komputer.
Hardware	:Perangkat dan peranti yang mendukung sistem komputer.
Severity	:Pengklasifikasian tingkat risiko yang ditimbulkan oleh kerentanan.
Activity Diagram	:Gambaran aliran aktivitas dari sebuah sistem atau proses bisnis.
Data Flow Diagram	:Gambaran visualisasi bagaimana suatu proses dilaksanakan.
SQL Injection	:Teknik penyerangan web menggunakan kode SQL untuk memanipulasi *database*.
Cross-Site Scripting	:Serangan pada web menggunakan injeksi kode pada sisi *client*.

Local File Inclusion	:Kerentanan yang memungkinkan *attacker* membaca file local yang tersimpan pada *server.*
Brute Force	:Serangan pada aplikasi web untuk mendapatkan akses dengan menebak *username* dan *password*.
Clickjacking	:Serangan pada aplikasi web dengan menyisipkan sebuah tautan pada suatu *button* yang berbahaya apabila di klik oleh *user*.