**Keamanan Aplikasi Web: Serangan dan Pencegahan**

1. **Cross-Site Scripting (XSS)**

XSS dilakukan ketika penyerang menyisipkan skrip jahat ke dalam aplikasi web yang tidak memvalidasi input pengguna dengan benar. Skrip ini biasanya dimasukkan melalui formulir input atau URL, kemudian dijalankan oleh browser korban saat membuka halaman tersebut. Penyerang dapat menggunakan skrip ini untuk mencuri data seperti cookie sesi, mengarahkan pengguna ke situs phishing, atau memanipulasi konten halaman.

Dampak:

- Pencurian informasi sensitif (cookie, data sesi).

- Pengarahan ke situs phishing.

- Perubahan konten web yang terlihat oleh korban.

Cara Pencegahan:

- Validasi dan sanitasi input pengguna.

- Gunakan Content Security Policy (CSP).

- Terapkan encoding pada data pengguna yang akan ditampilkan di halaman web.

1. **SQL Injection**

Serangan ini terjadi ketika penyerang menyisipkan perintah SQL berbahaya melalui input aplikasi, seperti kolom pencarian atau parameter URL. Input yang tidak difilter dengan baik memungkinkan perintah tersebut dijalankan oleh server, memberikan penyerang akses untuk membaca, menghapus, atau memanipulasi data di database. Penyerang sering menggunakan karakter khusus seperti ' OR 1=1 untuk menyisipkan kode mereka.

Dampak:

- Pencurian data penting seperti kredensial pengguna.

- Penghapusan atau modifikasi data.

- Potensi pengambilalihan kontrol server.

Cara Pencegahan:

- Gunakan parameterized queries atau prepared statements.

- Validasi input dengan ketat untuk mencegah simbol SQL tidak sah.

- Hindari membangun kueri SQL dengan menggabungkan string langsung dari input pengguna.

1. **Distributed Denial of Service (DDoS)**

DDoS dilakukan dengan mengirimkan permintaan palsu dalam jumlah besar ke server secara bersamaan, biasanya melalui jaringan botnet yang terdiri dari perangkat yang terinfeksi malware. Permintaan ini membanjiri server hingga sumber dayanya habis dan tidak dapat melayani pengguna sah. Penyerang memanfaatkan skala serangan yang besar untuk memastikan server lumpuh.

Dampak:

- Gangguan layanan (downtime) yang memengaruhi pengalaman pengguna.

- Kerugian bisnis akibat ketidakmampuan server merespons permintaan.

Cara Pencegahan:

- Gunakan layanan mitigasi DDoS seperti Cloudflare atau Akamai.

- Terapkan pembatasan laju (rate limiting).

- Monitor lalu lintas secara aktif untuk deteksi dini.

1. **Man-in-the-Middle (MITM) Attack**

MITM terjadi ketika penyerang menyadap komunikasi antara pengguna dan server, seringkali pada koneksi tidak aman seperti HTTP atau jaringan Wi-Fi publik. Penyerang dapat menyadap, memodifikasi, atau mencuri data yang dikirim, termasuk kredensial login atau informasi pembayaran. Serangan ini sering dilakukan menggunakan perangkat lunak packet sniffer atau dengan mengatur Wi-Fi palsu.

Dampak:

- Pencurian data sensitif (seperti kata sandi atau data kartu kredit).

- Pengalihan pengguna ke situs phishing.

Cara Pencegahan:

- Gunakan HTTPS dengan sertifikat SSL/TLS.

- Hindari jaringan Wi-Fi publik tanpa perlindungan VPN.

- Terapkan autentikasi tambahan pada data yang dikirim.

1. **File Inclusion Attacks (LFI/RFI)**

File Inclusion dilakukan dengan memanipulasi input pada aplikasi web yang menentukan file mana yang akan diakses. Penyerang dapat memasukkan file berbahaya dari server mereka (Remote File Inclusion) atau membaca file lokal yang sensitif (Local File Inclusion), seperti file konfigurasi server. Serangan ini sering memanfaatkan parameter seperti ?file= yang tidak divalidasi dengan baik.

Dampak:

- Akses tidak sah ke file server yang sensitif.

- Eksekusi kode berbahaya yang dapat mengambil alih server.

Cara Pencegahan:

- Batasi file yang dapat diakses dengan daftar putih (whitelisting).

- Validasi input pengguna dengan ketat.

- Nonaktifkan fungsi allow\_url\_include di pengaturan server.