**TUTORIAL MENJALANKAN FILE SIMULASI CLICKJACKING & CARA PERBAIKAN SERVER**

**Bagian 1: Menjalankan File Simulasi Clickjacking**

Langkah-langkah:

1. Unduh file HTML simulasi clickjacking dari sumber yang disediakan.  
2. Buka lokasi penyimpanan file tersebut di komputer kamu.  
3. Klik dua kali (double-click) pada file HTML untuk membukanya di browser bawaan.  
4. Halaman akan terbuka dan menampilkan tombol palsu. Saat tombol diklik, file akan otomatis terunduh.  
5. Ini adalah simulasi dari bagaimana pengguna bisa tertipu dan mendownload malware.

**Catatan:**

- Simulasi ini bisa berjalan langsung tanpa perlu server atau koneksi khusus.  
- Pastikan tidak mengubah struktur file saat membuka agar simulasi bekerja dengan baik.

**Bagian 2: Cara Memperbaiki dan Mencegah Clickjacking pada Server**

Solusi Teknis untuk Admin Server:

1. Tambahkan header `X-Frame-Options` ke konfigurasi server:  
 - `DENY`: Mencegah semua iframe.  
 - `SAMEORIGIN`: Hanya iframe dari domain yang sama yang diizinkan.  
  
 Contoh pada server Apache (.htaccess):  
 Header set X-Frame-Options "SAMEORIGIN"  
  
2. Gunakan Content Security Policy (CSP):  
 Tambahkan header berikut:  
 Content-Security-Policy: frame-ancestors 'self';  
  
3. Periksa dan batasi akses file yang bisa diunduh secara langsung dari iframe.  
4. Audit rutin keamanan website dan hindari penggunaan iframe dari sumber tidak terpercaya.

**Rekomendasi Tambahan:**

- Update CMS dan plugin yang digunakan.  
- Gunakan firewall aplikasi web (WAF).  
- Edukasi pengguna agar waspada terhadap link mencurigakan.