Laporan Temuan Kerentanan Website

# 1. Informasi Umum

Tanggal Pemeriksaan: 14 April 2025

Target: https://santri.darunnajah.com

Metode Pemeriksaan: Pengujian keamanan menggunakan pendekatan Blackbox dengan bantuan tools seperti Nikto, browser, dan manual testing.

# 2. Temuan Kerentanan

## 2.1 Clickjacking

Clickjacking adalah teknik serangan di mana penyerang menyisipkan halaman web target ke dalam elemen <iframe> pada halaman palsu yang dibuat sedemikian rupa untuk mengecoh pengguna agar mengklik sesuatu yang berbeda dari apa yang mereka kira.

Dalam pengujian yang dilakukan, ditemukan bahwa website https://santri.darunnajah.com tidak memiliki proteksi terhadap clickjacking. Hal ini diketahui dari hasil uji menggunakan iframe, di mana halaman target berhasil dimuat tanpa adanya pembatasan.

### Bukti PoC (Proof of Concept):

Berikut adalah potongan kode HTML sederhana yang digunakan dalam pengujian:

<style>  
 iframe {  
 opacity: 0.1;  
 position: absolute;  
 top: 0;  
 left: 0;  
 z-index: 2;  
 }  
 button.fake {  
 position: relative;  
 z-index: 3;  
 background-color: red;  
 color: white;  
 padding: 20px;  
 font-size: 20px;  
 }  
 </style>  
  
 <iframe src="https://santri.darunnajah.com" width="1000" height="700"></iframe>  
 <button class="fake">Klik Untuk Dapat Hadiah</button>

Tampilan dari halaman uji menunjukkan bahwa konten website dapat ditampilkan dalam frame dan elemen tambahan (seperti tombol palsu) dapat ditumpangkan di atasnya.

# 3. Rekomendasi

Untuk mencegah serangan clickjacking, disarankan agar pengelola situs menambahkan header HTTP berikut pada konfigurasi server:

1. X-Frame-Options: DENY  
2. Atau menggunakan Content-Security-Policy: frame-ancestors 'none';

Penambahan header ini akan mencegah browser menampilkan situs di dalam elemen iframe dari domain yang tidak diizinkan.

# 4. Penutup

Demikian laporan ini dibuat untuk memberikan gambaran teknis terhadap kerentanan yang ditemukan dan langkah mitigasi yang dapat dilakukan. Diharapkan pihak pengelola dapat segera mengambil tindakan untuk mengamankan situs dari potensi eksploitasi.