

# Laporan Temuan Kerentanan Keamanan Aplikasi Web

## 1. Identitas Penguji

Nama: Ramdhani

Tim: White Hats of Catalyst Generation

Tanggal Pengujian: 14 April 2025

Target: <https://santri.darunnajah.com>

## 2. Ringkasan Temuan

Dalam pengujian keamanan terhadap situs <https://santri.darunnajah.com>, ditemukan potensi kerentanan yang dapat dimanfaatkan untuk serangan Clickjacking. Hal ini terjadi karena tidak adanya konfigurasi header 'X-Frame-Options' pada server target, yang memungkinkan situs dapat di-load di dalam iframe oleh situs berbahaya. Simulasi serangan dilakukan menggunakan halaman HTML lokal yang menyisipkan iframe dan tombol palsu untuk memancing interaksi pengguna.

## 3. Detail Teknis

Berikut adalah temuan teknis berdasarkan pengujian:

- Server tidak memiliki header 'X-Frame-Options'.
- Hal ini memungkinkan halaman dimuat dalam elemen <iframe> dari domain lain.
- Diuji menggunakan halaman lokal dengan file 'test2.html'.
- Tombol palsu ditampilkan di atas iframe untuk menipu pengguna.

## 4. Bukti Visual (Screenshots)

Cuplikan Layar Dari 2025-04-14 13-59-31.png

Cuplikan Layar Dari 2025-04-14 14-01-12.png

Cuplikan Layar Dari 2025-04-14 14-04-05.png

## 5. Rekomendasi

Untuk mencegah serangan Clickjacking, disarankan agar pihak pengelola situs mengimplementasikan header HTTP 'X-Frame-Options' atau 'Content-Security-Policy: frame-ancestors'. Contoh konfigurasi untuk nginx:

```
add_header X-Frame-Options "SAMEORIGIN" always;
```

Langkah ini akan mencegah situs agar tidak dapat di-render dari domain luar melalui iframe.

## 6. Penutup

Demikian laporan ini dibuat dengan sebenar-benarnya untuk dijadikan pertimbangan dalam meningkatkan keamanan aplikasi web. Apabila diperlukan diskusi lebih lanjut, kami siap membantu.