Laporan Analisis Keamanan Website: darunnajah.ac.id

# 1. Pendahuluan

Laporan ini merupakan hasil analisis keamanan pada website https://www.darunnajah.ac.id berdasarkan pendekatan model OSI Layer. Pengujian dilakukan dari sisi external network menggunakan tools seperti ping, traceroute, curl, sslyze, dan nikto.

# 2. Analisis Berdasarkan OSI Layer

## Layer 7 - Application Layer

Pengujian dilakukan dengan tools seperti curl dan nikto. Ditemukan beberapa potensi kerentanan pada HTTP Response Header seperti tidak adanya X-Frame-Options dan X-Content-Type-Options. Hal ini dapat menyebabkan risiko clickjacking dan content-type sniffing.  
  
Contoh hasil:  
- X-Frame-Options: Tidak ada  
- X-Content-Type-Options: Tidak ada  
- Server: cloudflare  
- HTTP Redirect (301) dari http ke https terdeteksi.

## Layer 6 - Presentation Layer

Pengujian TLS dilakukan dengan sslyze dan openssl. Ditemukan bahwa website mendukung TLS 1.2 dan 1.3 dengan cipher suite yang kuat, serta tidak rentan terhadap serangan renegotiation dan Heartbleed.  
  
Cipher yang diterima:  
- TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256  
- TLS\_AES\_128\_GCM\_SHA256 (TLS 1.3)  
- dll.

## Layer 4 - Transport Layer

Port 80 (HTTP) dan 443 (HTTPS) ditemukan dalam keadaan terbuka. Website juga mendukung HTTP/2 dan mengiklankan HTTP/3 via alt-svc header. Tidak ditemukan port lain yang terbuka saat dilakukan scanning dasar.

## Layer 3 - Network Layer

Pengujian menggunakan ping dan traceroute menunjukkan bahwa situs dapat diakses dengan baik melalui IPv6.  
Hasil traceroute menunjukkan rute internasional menuju Cloudflare.  
- IP IPv6: 2606:4700:3035::ac43:bd4b  
- Tidak ada packet loss  
- TTL normal

# 3. Kesimpulan

Website darunnajah.ac.id menunjukkan konfigurasi keamanan yang cukup baik terutama dari sisi TLS dan transport layer. Namun, perlu dilakukan perbaikan pada HTTP response header dan penguatan konfigurasi di application layer untuk menghindari potensi exploitasi umum seperti clickjacking dan MIME sniffing.