PLKUTAK.COM SCAN REPORT

1. Scope

Target: plkutak.com

Assessment Type: Non-intrusive vulnerability assessment

Method: Nmap scanning & configuration analysis

2. Findings

Finding 1 – **Open SSH Port (22)**
Severity: **Medium**
Description: SSH service is publicly accessible.
Risk: Possible brute-force attacks if password authentication is enabled.
Recommendation: Use key-based authentication and restrict SSH via firewall.

Finding 2 – **Missing Security Headers**
Severity: **Low**
Description: Security headers such as HSTS and CSP are not implemented.
Risk: Increased exposure to clickjacking and content injection.
Recommendation: Implement recommended HTTP security headers.

Finding 3 – **TLS Configuration**
Severity: **Informational**
Description: TLS 1.2 and TLS 1.3 enabled with strong ciphers.
Risk: Low
Recommendation: Maintain current configuration.

3. Vulnerability Script Scan Results

Nmap vulnerability scripts were executed against exposed services (SSH, HTTP, HTTPS).
No publicly known vulnerabilities were detected during the automated assessment. This indicates that the server software appears to be up to date and not affected by commonly exploitable CVEs detectable via standard NSE scripts.