ABSTRAK

ANALISIS KEAMANAN *WEBSITE* YAYASAN PONDOK XYZ MENGGUNAKAN *OWASP WEB SECURITY TESTING GUIDE*

Oleh
M. Ato' ulloh
21102165

Seiring dengan pesatnya perkembangan teknologi digital, situs *website* menjadi salah satu *platform* utama dalam pengelolaan informasi, termasuk bagi lembaga pendidikan seperti Yayasan Pondok XYZ. Meskipun memberikan banyak kemudahan, penggunaan teknologi ini juga menghadirkan ancaman keamanan siber yang semakin berkembang. Keamanan situs *website* menjadi sangat penting, mengingat situs tersebut menyimpan informasi sensitif seperti data pribadi, data pendidikan, dan keuangan santri. Ancaman serangan seperti *Cross-Site Scripting (XSS), SQL Injection, Brute Force, Clickjacking, dan Distributed Denial of Service (DDoS)* dapat mengancam integritas dan kerahasiaan data tersebut. Penelitian ini bertujuan untuk menganalisis keamanan sistem informasi pada situs *website* milik Yayasan Pondok XYZ. Metode yang digunakan dalam penelitian ini adalah Penetration Testing berdasarkan panduan *OWASP Web Security Testing Guide* untuk mendeteksi dan mengevaluasi potensi kerentanannya. Pengujian dilakukan dengan menggunakan berbagai alat pengujian keamanan, seperti *OWASP ZAP, SQLMap, WPScan, Burp Suite, dan LOIC* untuk melakukan simulasi terhadap beberapa jenis serangan, termasuk *Cross-Site Scripting (XSS), Clickjacking, SQL Injection, Brute Force, dan Distributed Denial of Service (DDoS).* Hasil penelitian menunjukkan bahwa situs rentan terhadap beberapa jenis serangan, seperti *Clickjacking dan DDoS*, dengan berhasilnya serangan *Clickjacking* dan DDoS. Namun, situs tidak berhasil dieksploitasi pada serangan *Reflected XSS, SQL Injection, dan Brute Force*. Kerentanannya ditemukan pada konfigurasi server yang tidak optimal, seperti tidak adanya pengaturan *X-Frame-Options* untuk melindungi dari *Clickjacking* dan ketidakmampuan situs untuk menangani serangan DDoS. Rekomendasi perbaikan untuk mengatasi kerentanannya termasuk penambahan *X-Frame-Options* pada respons HTTP, penerapan *Content Security Policy (CSP),* penggunaan *Web Application Firewall (WAF)* untuk melindungi dari serangan DDoS, serta pembaruan rutin tema dan plugin *WordPress* untuk mengatasi kerentanannya pada tema yang digunakan. Pihak mitra Yayasan Pondok XYZ telah mengevaluasi hasil penelitian dan menerima rekomendasi perbaikan. Mereka berkomitmen untuk menambahkan *header X-Frame-Options* dan mempertimbangkan penerapan *Content Security Policy (CSP).* Untuk mengatasi ancaman DDoS, mitra sedang pengadakan *Web Application Firewall (WAF),* namun sementara ini telah menerapkan *traffic filtering* pada router. Mitra juga berencana memperbarui tema dan plugin *WordPress* serta merencanakan pemeliharaan sistem berkala untuk mencegah kerentanan.

Kata kunci: Keamanan *Website*, OWASP, *Penetration Testing*, Pondok Pesantren