INTISARI

Website MI Diponegoro 03 Karangklesem berfungsi sebagai media informasi dan layanan akademik sekolah, namun pada kondisi awal belum didukung oleh konfigurasi keamanan teknis yang optimal. Penelitian ini bertujuan untuk meningkatkan keamanan *website* melalui penerapan metode *hardening* dengan konfigurasi TLS/HTTPS dan HTTP *Security Headers*. Metode penelitian yang digunakan adalah *quasi-eksperimental* dengan desain *One-Group Pretest–Posttest*. Pengujian keamanan dilakukan sebelum dan sesudah penerapan *hardening* menggunakan Qualys SSL Labs dan SecurityHeaders.com. Hasil pengujian awal menunjukkan tingkat keamanan TLS/HTTPS sebesar 80% (*grade* A), sedangkan penerapan HTTP *Security Headers* masih 0% (*grade* F). Implementasi *hardening* dilakukan dengan mengaktifkan *Strict-Transport-Security* (HSTS), menonaktifkan protokol TLS lama, mengoptimalkan *cipher suite*, serta menerapkan *header* keamanan seperti *Content-Security-Policy*, X-*Frame-Options*, X-*Content-Type-Options*, *Referrer-Policy*, dan *Permissions-Policy*. Hasil pengujian ulang menunjukkan bahwa tingkat keamanan TLS/HTTPS meningkat menjadi 100% (*grade* A+) atau naik 20%, sementara penerapan HTTP *Security Headers* meningkat dari 0% menjadi 100% (*grade* A). Pengujian manual juga membuktikan bahwa komunikasi data telah terenkripsi dan serangan berbasis *browser* seperti *sniffing*, dan *clickjacking* dapat dicegah. Kesimpulan penelitian menunjukkan bahwa metode *hardening* efektif meningkatkan keamanan *website* sekolah. Disarankan agar pengelola *website* melakukan evaluasi keamanan secara berkala serta mempertimbangkan penerapan mekanisme keamanan lanjutan.

Kata kunci: Keamanan *Website*, *Hardening*, TLS/HTTPS, HTTP *security headers*

ABSTRACT

The MI Diponegoro 03 Karangklesem website functions as a medium for information dissemination and academic services; however, in its initial condition, it was not supported by optimal technical security configurations. This study aims to improve website security through the implementation of hardening methods by configuring TLS/HTTPS and HTTP Security Headers. The research employed a quasi-experimental method with a One-Group Pretest–Posttest design. Security testing was conducted before and after the hardening implementation using Qualys SSL Labs and SecurityHeaders.com. The initial test results showed that the TLS/HTTPS security level was 80% (grade A), while the implementation of HTTP Security Headers was still at 0% (grade F). The hardening implementation involved enabling Strict-Transport-Security (HSTS), disabling legacy TLS protocols, optimizing cipher suites, and applying security headers such as Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy. Post-test results indicated that the TLS/HTTPS security level increased to 100% (grade A+), representing a 20% improvement, while the implementation of HTTP Security Headers increased from 0% to 100% (grade A). Manual testing also confirmed that data communication was encrypted and that browser-based attacks such as sniffing, clickjacking, and XSS could be effectively prevented. The study concludes that the hardening method is effective in enhancing the security of school websites. It is recommended that website administrators conduct regular security evaluations and consider implementing advanced security mechanisms.

Keywords: Website Security, Hardening, TLS/HTTPS, HTTP security headers