BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terhadap website SMP Muhammadiyah 1 Depok menggunakan tiga alat *Dynamic Application Security Testing (DAST)* yaitu, hasil pemindaian menunjukkan Jenis kerentanan yang ditemukan mencakup kelemahan pada konfigurasi keamanan transport, seperti *HTTP Strict Transport Security* (HSTS) yang tidak diterapkan, *cipher suite* TLS/SSL yang lemah, serta sertifikat SSL yang mendekati masa kedaluwarsa. Selain itu, ditemukan pula kerentanan pada pengelolaan *cookie*, antara lain *cookie* tanpa *atributHttpOnly* dan *SameSite*. Kerentanan lain yang teridentifikasi meliputi kelemahan kebijakan keamanan browser, seperti *Content Security Policy* (CSP) yang tidak lengkap, *clickjacking*, serta *anti-clickjacking header* yang tidak diterapkan. Beberapa temuan juga berkaitan dengan kebocoran informasi, seperti server *version disclosur*, *backup file*, dan informasi sistem melalui header HTTP. Sebagian jenis kerentanan tersebut terdeteksi oleh lebih dari satu alat, meskipun dengan tingkat risiko yang berbeda, yang menunjukkan adanya perbedaan sensitivitas dan metode penilaian antar tools.

Berdasarkan hasil analisis, OWASP ZAP mendeteksi dengan jumlah temuan terbanyak yaitu 23 kerentanan, terdiri dari 7 tingkat medium, 8 tingkat low, dan 8 bersifat informatif dengan waktu pemindaian paling singkat 50 menit. Alat ini memiliki sensitivitas tinggi dalam mendeteksi kerentanan yang berkaitan dengan kebijakan keamanan aplikasi, seperti CSP, *cookie*, dan pengelolaan sesi. Acunetix mendeteksi 15 temuan kerentanan, terdiri dari 3 tingkat medium, 9 tingkat low, dan 3 bersifat informatif dengan waktu 90 menit. Keunggulan dalam deteksi konfigurasi server, keamanan transport, dan laporan yang lebih rinci. Sementara itu, Burp Suite Professional dengan jumlah temuan paling sedikit yaitu 5 kerentanan, terdiri 1 tingkat high, 1 tingkat low, dan 3 bersifat informatif dengan waktu 65 menit. Namun, unggul dalam analisis komunikasi HTTP dan interaksi sisi klien, seperti kesalahan konfigurasi CORS dan manipulasi parameter HTTP.

5.2 Saran

Berdasarkan hasil penelitian yang telah diperoleh, beberapa saran yang dapat diberikan:

1. Bagi pihak pengelola website SMP Muhammadiyah 1 Depok, disarankan untuk menerapkan kebijakan HTTP *Strict Transport Security (HSTS)* dan memperbarui sertifikat SSL secara berkala, mengonfigurasi *Content Security Policy (CSP)* secara ketat untuk mencegah *serangan Clickjacking dan Cross-Site Scripting (XSS)*, mengaktifkan atribut keamanan *HttpOnly* dan *SameSite* pada *cookie* untuk mencegah pencurian sesi pengguna, menonaktifkan informasi versi server dan file konfigurasi yang dapat diakses publi, serta melakukan pemindaian keamanan secara berkala menggunakan lebih dari satu alat DAST untuk memastikan hasil evaluasi yang lebih menyeluruh
2. Bagi peneliti selanjutnya, disarankan untuk mengembangkan penelitian dengan menambahkan alat uji lain seperti Nikto atau Nessus untuk memperluas cakupan deteksi kerentanan, melakukan pengujian terhadap aplikasi dengan autentikasi pengguna untuk menilai keamanan sisi login dan manajemen sesi Mengombinasikan metode *Dynamic Testing dengan Static Application Security Testing (SAST)* agar hasil pengujian lebih mendalam dari sisi kode dan konfigurasi server, serta melakukan *time-based benchmarking* terhadap performa pemindaian agar efektivitas alat dapat diukur tidak hanya dari jumlah deteksi tetapi juga dari efisiensi proses pemindaian.