BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan penelitian dan pengujian yang telah dilakukan mengenai "Implementasi Sistem Keamanan *Web server* Berbasis *Web Application Firewall* (WAF) ModSecurity dengan Monitoring Serangan dan Notifikasi Telegram", diperoleh simpulan sebagai berikut:

1. Implementasi *Web* Application Firewall (WAF) ModSecurity pada *web server* Apache2 berhasil dilakukan dan mampu mendeteksi serta mencegah berbagai jenis serangan umum, seperti *Cross-Site Scripting* (XSS), SQL *Injection* (SQLI), *Local File Inclusion* (LFI), *Remote File Inclusion* (RFI), dan *Scanner Detection*. Hal ini membuktikan bahwa ModSecurity dapat meningkatkan keamanan *web server* terhadap ancaman siber.
2. Sistem monitoring berbasis *web* dan notifikasi Telegram berhasil dirancang serta diintegrasikan dengan ModSecurity. Sistem ini mampu menampilkan log serangan melalui *web* monitoring sesuai pengujian *BlackBox*. Dan memberikan peringatan cepat kepada administrator melalui Telegram, sehingga mempermudah proses identifikasi serta mitigasi ancaman.
3. Hasil evaluasi kinerja sistem monitoring menunjukkan performa yang baik, dengan notifikasi Telegram terkirim kurang dari satu detik pada semua jenis serangan kecuali *Scanner Detection* yang membutuhkan waktu sekitar 16 detik akibat proses inisialisasi *tools*. Secara keseluruhan, sistem mampu memberikan informasi *real-time*, akurat, dan relevan untuk mendukung kesiapan administrator dalam merespons serangan siber.

Simpulan di atas menegaskan bahwa sistem keamanan *web server* yang dirancang mampu mendeteksi dan memblokir berbagai jenis serangan umum, serta memberikan notifikasi cepat dan pemantauan. Sistem ini dapat

diimplementasikan sebagai solusi keamanan pada lingkungan *server* berbasis Apache2.

5.2 Saran

Berdasarkan hasil penelitian dan evaluasi yang telah dilakukan, beberapa saran yang dapat dipertimbangkan untuk pengembangan sistem ke depannya adalah sebagai berikut:

1. Sistem dapat dikembangkan dengan menambahkan mekanisme pemblokiran otomatis terhadap IP yang melakukan serangan berulang, misalnya dengan integrasi iptables atau fail2ban.
2. Pembaruan berkala terhadap *rules*et ModSecurity sangat disarankan, agar sistem tetap mampu mendeteksi pola serangan terbaru seiring berkembangnya ancaman siber.