BAB VI
PENUTUP

Dalam bab ini, akan dijelaskan mengenai hasil dari pengembangan yang telah dilakukan serta pembahasannya. Hasil pengembangan ini dibagi menjadi dua bagian, yaitu kesimpulan dan saran yang dapat diambil dari pengembangan tersebut**.**

6.1 Kesimpulan

Pengembangan aplikasi monitoring serangan menggunakan modsecurity dengan fitur notifikasi intrusi sudah bekerja sesuai dengan rancangan. Adapun rincian yang diperoleh pada penelitian ini sebagai berikut.

(1) Hasil monitoring aplikasi menggunakan *pie chart*, *bar chart,* dan *table log* untuk memvisualisasikan jumlah dan jenis serangan yang tercatat log.
(2) Modsecurity berperan sebagai *Web Application Firewall* pada web dev aktif dalam mendeteksi dan memblokir serangan. Peneliti melakukan *embedding* di virtual host pada web server apache2 dan mengaktifkan “SecRuleEngine On” agar aturan berfungsi dan aturan dapat di kostumisasi untuk memblokir serangan seperti Command Injection, SQL Injection, dan Cross-site Scripting.
(3) Fitur notifkasi intrusi juga sudah dapat mengirim jika mendeteksi adanya anomali dan mengirimkan ke telegram.
(4) Log modsecurity dapat diurai sesuai kebutuhan dan dijalankan melalui skrip daemon-service ubuntu agar penguraian dapat berjalan otomatis.

6.2 Saran

Berdasarkan uraian dari hasil penelitian pada bab diatas, maka saran yang dapat diberikan untuk penelitian selanjutnya adalah sebagai berikut.

(1) Menerapkan teknik *filter false* and *positive* pada *Modsecurity* jika *web server* yang digunakan berbeda supaya mendapatkan informasi dari *log* yang lebih baik.
(2) Memperkuat *bot* dengan *State Management* untuk meningkatkan akurasi bot dalam membaca log dan pengiriman pesan deteksi intrusi ke Telegram.
(3) Diharapkan penelitian selanjutnya dapat meningkatkan fitur bukan hanya memproses log modsecurity tetapi berbagai macam log proses seperti *log snort, suricata, nginx,* dan lainnya. Supaya membangun sistem seperti layaknya SIEM (*Security Information and Event Management).*