BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pembahasan penelitian dalam naskah skripsi ini, maka dapat diambil beberapa kesimpulan yaitu:

1. Untuk mengidentifikasi jenis serangan cross site scripting (XSS), directory traversal dan brute force dibutuhkan melakukan penambahan rule pada file local_rule.xml berdasarkan rule_id, sedangkan untuk serangan SQL injection dan serangan DDoS tidak diperlukan penambahan rule.
2. Serangan yang dianalisis menggunakan metode OWASP *risk rating assessment* mendapatkan 2 kategori risiko, yaitu *High* untuk serangan cross site scripting, directory traversal, SQL injection dan DDoS, sedangkan serangan brute force masuk kedalam kategori risiko *Medium*.

5.2 Saran

Sebagai penutup penelitian skripsi ini, penulis berharap semoga apa yang penulis sajikan dapat memberikan banyak manfaat bagi pembaca dan penulis. Penulis menyadari sepenuhnya bahwa skripsi ini yang berujudul implementasi wazuh sebagai SIEM menggunakan metode OWASP *risk rating assessment* masih memiliki kekurangan, oleh karena itu saran yang dapat penulis berikan diantaranya adalah:

1. Penelitian ini mengimplementasikan wazuh hanya sebagai SIEM hanya untuk mendeteksi serangan dengan konfigurasi standar atau default, untuk penelitian selanjutnya dapat menggunakan wazuh untuk mitigasi serangan secara langsung.
2. Pada penelitian ini hanya melakukan pengujian serangan tanpa adanya *recovery* untuk sistem yang diuji. Untuk penelitian selanjutnya dapat melakukan langkah *recovery* agar penelitian lebih kompleks.