

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan dengan judul "Implementasi WAF pada Aplikasi Fishku Berbasis Google Cloud Armor", beberapa kesimpulan dapat diambil sebagai berikut:

1. Implementasi *Web Application Firewall* (WAF) menggunakan layanan Google Cloud Armor berhasil meningkatkan tingkat keamanan aplikasi *web* Fishku terhadap jenis serangan, termasuk *Local File Inclusion* (LFI), *Vulnerability Scanner*, dan *Protocol Attack*. Penerapan WAF ini menghasilkan perubahan signifikan pada respon server dari sebelumnya yang cenderung positif (respon kode 200) menjadi lebih aman dengan penolakan akses (respon kode 403), menunjukkan keberhasilan perlindungan yang lebih baik.
2. Pengujian juga melibatkan konfigurasi *Load Balancer*, yang memungkinkan distribusi lalu lintas aplikasi secara efisien di antara beberapa sumber daya server. Hal ini dapat meningkatkan ketersediaan dan kinerja aplikasi, serta mengoptimalkan tata letak data untuk mengurangi risiko *overloading* pada satu server.
3. Penggunaan fitur *Log-Based Alerts* juga telah memberikan dampak positif dalam menginformasikan secara cepat jika terjadi serangan atau aktivitas mencurigakan. Notifikasi melalui email memungkinkan *respons* cepat dari tim keamanan untuk mengidentifikasi dan merespon ancaman segera setelah terdeteksi.
4. Analisis data *metric* dan visualisasi grafik menjadi alat yang penting dalam pemantauan kinerja aplikasi dan deteksi dini ancaman. Metrik performa yang diambil dari Google Cloud Platform memberikan wawasan yang lebih dalam tentang bagaimana aplikasi beroperasi

5.2 Saran

Penelitian yang telah dilakukan memiliki beberapa saran yang dapat digunakan untuk melakukan pengembangan penelitian selanjutnya. Berikut merupakan beberapa saran yang dapat digunakan.

1. Melakukan uji coba yang lebih kompleks dengan variasi parameter dan serangan-serangan yang lebih diversifikasi dapat membantu mengidentifikasi celah keamanan yang lebih kompleks.
2. Melakukan eksplorasi teknologi adaptive protection yang ditawarkan oleh layanan cloud seperti Google Cloud Platform. Teknologi ini secara otomatis menyesuaikan level proteksi berdasarkan tingkat ancaman yang terdeteksi, memberikan perlindungan yang lebih *responsif* terhadap ancaman baru.
3. Mempertimbangkan penggunaan teknik machine learning dan analisis big data yang dapat mengintegrasikan data dari berbagai sumber, termasuk *alerts* dan *metric*, untuk meningkatkan deteksi dini serangan berbasis anomali. Hal ini dapat membantu mengidentifikasi pola serangan yang tidak terdeteksi sebelumnya dan mengurangi risiko serangan yang lebih kompleks.