BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan Berdasarkan hasil implementasi dan evaluasi empiris yang telah dipaparkan, penelitian ini menghasilkan beberapa kesimpulan utama sebagai berikut:

1. Menjawab rumusan masalah pertama mengenai proses identifikasi serangan, penelitian ini berhasil menerapkan sebuah pendekatan deteksi hibrida. Proses tersebut mengombinasikan analisis fitur leksikal, konteks dari aturan *OWASP Core Rule Set* (CRS), dan representasi N-gram untuk membangun model klasifikasi *Random Forest* yang akurat dan kontekstual. Analisis interpretasi SHAP juga mengonfirmasi bahwa model tidak hanya bergantung pada sinyal CRS, tetapi juga berhasil mempelajari karakteristik intrinsik dari lalu lintas berbahaya.
2. Menjawab rumusan masalah kedua mengenai kinerja, sistem berbasis *machine learning* (ML-RF) yang diusulkan menunjukkan performa yang secara signifikan lebih unggul dibandingkan implementasi standar ModSecurity dengan CRS. Keunggulan tersebut dibuktikan oleh peningkatan F1-Score dari 10.10% menjadi 80.00% dan metrik *recall* dari 5.34% menjadi 72.00%. Hasil ini menegaskan bahwa pendekatan *machine learning* mampu menghasilkan sistem deteksi yang lebih seimbang dan efektif secara keseluruhan.
3. Penelitian ini juga menghasilkan temuan lain saat diterapkan pada data riil. Sejumlah 62.7% dari total anomali yang terdeteksi merupakan kategori

Anomaly_ML_Only, yang membuktikan kemampuan model untuk mengidentifikasi ancaman yang lolos dari deteksi berbasis aturan. Di sisi lain, temuan ini turut menyoroti keterbatasan dalam proses pemetaan otomatis dan potensi ambiguitas hasil. Angka yang tinggi tersebut dapat pula mengindikasikan bahwa model menjadi terlalu sensitif terhadap pola lalu lintas normal bervolume tinggi yang kurang terwakili dalam data latih, sehingga berpotensi menghasilkan *false positive*.

5.2 Saran

Berdasarkan temuan dan keterbatasan yang teridentifikasi selama penelitian, berikut adalah beberapa saran yang diajukan untuk implementasi praktis dan arah penelitian selanjutnya:

1. Melakukan validasi dan kalibrasi secara mendalam terhadap kategori deteksi Anomaly_ML_Only. Analisis *false positive* yang lebih terperinci pada kategori ini direkomendasikan untuk membedakan secara akurat antara ancaman nyata dan kebisingan data.
2. Memperluas kapabilitas pemetaan kategori serangan OWASP dengan mengintegrasikan sumber data tambahan. Untuk dapat mengidentifikasi kelemahan seperti A02 (*Cryptographic Failures*) atau A04 (*Insecure Design*), analisis tidak dapat hanya bergantung pada log WAF, melainkan perlu diperkaya dengan data dari hasil pemindaian keamanan aplikasi (SAST/DAST) atau log audit konfigurasi server.

3. Mengimplementasikan alur kerja MLOps (*Machine Learning Operations*) untuk menjaga relevansi model. Alur kerja ini mencakup proses pelatihan ulang model secara berkala dan otomatis (*automated retraining*) menggunakan data log baru untuk beradaptasi dengan lanskap ancaman yang terus berevolusi, disertai evaluasi performa otomatis sebelum penerapan ke lingkungan produksi.

4. Memperluas cakupan pengujian untuk mengukur ketahanan model secara spesifik. Riset di masa depan dapat mencakup pengujian terhadap *adversarial attacks* guna memahami sejauh mana sistem dapat dimanipulasi oleh penyerang yang memiliki kesadaran terhadap keberadaan pertahanan berbasis *machine learning*.