BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, maka dapat ditarik kesimpulan sebagai berikut:

a. Aplikasi Log Parser berbasis Go (Golang) berhasil dibangun dan mampu memproses 45.645 baris log server SIAKAD UMB secara otomatis. Aplikasi menghasilkan output CSV terstruktur yang memudahkan investigasi forensik lebih lanjut.

b. Konfigurasi log server perlu disesuaikan agar mencatat header *X-Forwarded-For* atau *X-Real-IP* yang diteruskan oleh *reverse proxy*, sehingga IP address asli penyerang dapat diidentifikasi dan fitur analisis IP pada aplikasi Log Parser dapat berfungsi secara optimal untuk keperluan forensik.

c. Verifikasi pola menggunakan Wireshark pada simulasi lab menunjukkan konsistensi parsing *rule-based*, meskipun validasi terhadap trafik produksi SIAKAD tidak dapat dilakukan karena keterbatasan akses log *edge*.

d. Penelitian menghasilkan rekomendasi mitigasi keamanan kepada UPTIK UMB, antara lain implementasi *Web Application Firewall* (WAF), penerapan rate limiting pada endpoint login, serta monitoring log secara real-time.

5.2 Saran

Berdasarkan hasil penelitian ini, saran yang dapat diberikan untuk pengembangan lebih lanjut adalah:

a. Aplikasi Log Parser dapat dikembangkan dengan menambahkan fitur analisis real-time menggunakan mekanisme file *watcher*, sehingga dapat mendeteksi serangan langsung tanpa menunggu log terkumpul.

b. Integrasi dengan sistem notifikasi otomatis (email atau aplikasi pesan) dapat ditambahkan agar administrator segera mendapat peringatan ketika terdeteksi aktivitas mencurigakan dalam jumlah besar.

c. Penelitian selanjutnya dapat mengembangkan model *machine learning* untuk meningkatkan akurasi klasifikasi dibandingkan pendekatan *rule-based* yang digunakan saat ini.

d. Pihak UPTIK UMB disarankan segera mengimplementasikan *Web Application Firewall* (WAF) pada server SIAKAD guna memblokir serangan SQL *Injection* secara otomatis sebelum mencapai *application layer*.

e. Fase *Preservation* dalam penelitian ini hanya mencakup penjaminan integritas data melalui hashing *MD5*. Untuk penelitian selanjutnya, disarankan menerapkan *preservation* yang lebih lengkap meliputi *write blocker* dan *chain of custody documentation* sesuai standar forensik digital.