BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan mengenai penerapan *reverse proxy* sebagai upaya peningkatan keamanan *web server* terhadap serangan *SQL injection*, dapat disimpulkan beberapa poin penting.implementasi *reverse proxy* terbukti efektif dalam menyembunyikan arsitektur internal *web server* dari penyerang. Dengan demikian, informasi vital mengenai *IP address* asli dan konfigurasi *backend server* dapat terlindungi, mempersulit penyerang untuk mengidentifikasi dan menargetkan kelemahan spesifik pada infrastruktur. Hal ini secara signifikan meningkatkan *security posture* keseluruhan sistem. *reverse proxy* mampu berperan sebagai lini pertahanan pertama yang memadai terhadap serangan *SQL injection*. Melalui konfigurasi dan aturan yang tepat, *reverse proxy* dapat melakukan filtrasi dan validasi terhadap setiap permintaan HTTP yang masuk sebelum mencapai *web server* utama. Serangan *SQL injection* yang mengandung karakter atau pola *payload* berbahaya dapat diidentifikasi dan diblokir secara proaktif pada lapisan *reverse proxy*, sehingga mencegah eksekusi *query* jahat pada basis data dan mitigasi risiko kebocoran data atau kerusakan sistem. penggunaan *reverse proxy* juga memberikan fleksibilitas dalam hal manajemen lalu lintas dan *load balancing*, yang secara tidak langsung berkontribusi pada ketersediaan dan kinerja *web server* tanpa mengorbankan keamanan. Dengan distribusi beban yang efisien, *web server* dapat beroperasi secara lebih stabil, bahkan saat menghadapi lalu lintas tinggi atau upaya serangan.Secara keseluruhan, penelitian ini menunjukkan bahwa integrasi *reverse proxy* merupakan strategi keamanan yang *viable* dan sangat direkomendasikan untuk *web server*, khususnya dalam menghadapi ancaman *SQL injection*.

5.2 Saran

Pengembangan sistem keamanan web dapat terus ditingkatkan dengan menerapkan aturan filtrasi yang lebih canggih, seperti memanfaatkan pendekatan berbasis *machine learning* untuk mendeteksi serangan SQL injection yang lebih kompleks. Selain itu, pelaksanaan uji penetrasi dan uji beban secara berkala sangat disarankan guna memastikan ketahanan dan keandalan sistem dalam menghadapi berbagai skenario serangan. Integrasi log dari reverse proxy dengan sistem *Security Information and Event Management* (SIEM) juga dapat dilakukan untuk memungkinkan pemantauan keamanan secara real-time dan respons yang lebih cepat terhadap potensi ancaman. Pendekatan proteksi lain seperti penerapan *Web Application Firewall* (WAF) maupun validasi input pada sisi aplikasi perlu dieksplorasi sebagai lapisan perlindungan tambahan. Di samping itu, peningkatan kesadaran dan pemahaman mengenai keamanan informasi di kalangan pengembang dan administrator sistem menjadi aspek penting yang harus terus didorong demi menciptakan ekosistem yang lebih aman.