

ABSTRAK

Seiring dengan kemudahan yang ditawarkan oleh teknologi, ancaman kejahatan siber merupakan tantangan serius dalam menjaga keamanan informasi. Salah satu metode serangan yang umum digunakan untuk mengeksploitasi celah keamanan dalam aplikasi *web* yang dapat mengakibatkan kebocoran data sensitif dan kerusakan sistem adalah *SQL injection*. Di sisi lain, e-Kinerja merupakan salah satu platform yang masih aktif digunakan dalam sektor pemerintahan dalam mengelola data kinerja Pegawai Negeri Sipil (PNS). Dalam penelitian ini, pendekatan *black box testing* diterapkan untuk mengevaluasi keamanan *database* tanpa memerlukan akses ke kode sumber aplikasi. Proses analisis dilakukan berdasarkan kerangka kerja ISSAF (*Information Systems Security Assessment Framework*) yang dirancang khusus untuk menilai keamanan sistem informasi secara menyeluruh. Hasil analisis menunjukkan bahwa *website* e-Kinerja Kabupaten Aceh Utara aman dari celah kerentanan keamanan yang disebabkan oleh serangan *SQL injection* karena telah dilindungi oleh WAF (*Web Application Firewall*) dan IPS (*Intrusion Prevention System*). Penelitian ini juga menyoroti pentingnya pendekatan perlindungan melalui penggunaan *firewall* sebagai langkah preventif dalam mendeteksi serta memblokir upaya penyerangan yang dilakukan *hacker*. Dengan demikian, penelitian ini tidak hanya memberikan wawasan terkait dengan keamanan *database*, tetapi juga menawarkan rekomendasi konkret untuk meningkatkan ketahanan sistem informasi di era digital yang semakin kompleks. Selain itu, penting bagi pengembang aplikasi untuk terus memperbarui dan meningkatkan protokol keamanan mereka agar dapat menghadapi ancaman baru yang muncul. Dengan menjaga sistem tetap aman, kita dapat meminimalisir kerugian akibat kebocoran data sensitif serta kerusakan sistem yang ditimbulkan akibat kejahatan siber.

Kata Kunci : Keamanan Informasi, *SQL Injection*, e-Kinerja, *Blackbox Testing*, ISSAF.

ABSTRACT

Along with the convenience offered by technology, the threat of cybercrime is a serious challenge in maintaining information security. One of the commonly used attack methods to exploit security gaps in web applications that can result in sensitive data leakage and system damage is SQL injection. On the other hand, e-Kinerja is a platform that is still actively used in the government sector to manage Civil Servant (PNS) performance data. In this research, a black box testing approach is applied to evaluate database security without requiring access to the application source code. The analysis process is carried out based on the ISSAF (Information Systems Security Assessment Framework) framework which is specifically designed to assess the security of information systems as a whole. The analysis results show that the North Aceh Regency e-Kinerja website is safe from security vulnerabilities caused by SQL injection attacks because it is protected by WAF (Web Application Firewall) and IPS (Intrusion Prevention System). This research also highlights the importance of a protective approach through the use of firewalls as a preventive measure in detecting and blocking attack attempts by hackers. Thus, this research not only provides insights related to database security, but also offers concrete recommendations for increasing the resilience of information systems in an increasingly complex digital era. Additionally, it is important for application developers to continually update and improve their security protocols to be able to deal with new threats as they arise. By keeping the system secure, we can minimize losses due to leaks of sensitive data and system damage caused by cybercrime.

Keywords: *Information Security, SQL Injection, e-Kinerja, Blackbox Testing, ISSAF.*