JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Analisis Keamanan Sistem Akademik Berbasis Web terhadap Serangan SQL Injection

Fathul Barri Akbar[1*], Ariq Fadhilah Pasya Sipayung[2], Afra Dhiya Lisara[3], Nasyatha Syakira[4], Devia Raisa[5]
[1,2,3,4,5]Program Studi Teknik Informatika, Universitas Malikussaleh, Indonesia
[1]fathul.240170221@mhs.unimal.ac.id, [2]ariq.240170197@mhs.unimal.ac.id, [3]afra.24017018@mhs.unimal.ac.id, [4]devia.240170075@mhs.unimal.ac.id, [5]nasyatha.240170093@mhs.unimal.ac.id

ABSTRACT

Web-based academic systems have become an essential component in managing educational data, including student records, lecturer data, grades, class schedules, and other academic administration processes. The implementation of web technology enables educational institutions to improve efficiency, speed, and accuracy in processing academic information in an integrated manner, as well as providing easy access for users anytime and anywhere. However, this openness also introduces various security risks that may threaten data confidentiality and system reliability. One of the most common security threats in web applications is SQL Injection attacks, which exploit weaknesses in user input handling, particularly in applications connected to databases. Through this attack, malicious actors can insert harmful SQL commands to gain unauthorized access, modify data, or delete critical information. This study aims to analyze the vulnerability level of a web-based academic system to SQL Injection attacks and to identify appropriate prevention measures. The research method employs a case study approach and literature analysis with simulated attacks on login forms and data input features. The results indicate that systems lacking input validation, data sanitization, and prepared statements are highly vulnerable to SQL Injection attacks. Therefore, the implementation of proper security mechanisms is essential to protect academic data.

Keywords: *Information System Security, Academic System, SQL Injection, Web Security, Input Validation*

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong institusi pendidikan untuk mengadopsi sistem akademik berbasis web dalam pengelolaan proses administrasi dan kegiatan akademik. Sistem ini memungkinkan pengelolaan data mahasiswa, dosen, nilai, dan jadwal perkuliahan secara terintegrasi serta memberikan kemudahan akses informasi bagi seluruh pengguna, baik mahasiswa, dosen, maupun staf akademik. Pemanfaatan sistem berbasis web dinilai mampu meningkatkan efisiensi, efektivitas, dan akurasi dalam pengelolaan informasi akademik.

Namun, di balik berbagai manfaat yang ditawarkan, penerapan sistem akademik berbasis web juga menghadirkan tantangan serius terkait keamanan informasi. Salah satu ancaman yang paling sering terjadi pada aplikasi web adalah serangan SQL Injection. Serangan ini umumnya disebabkan oleh lemahnya validasi input pengguna dan kesalahan dalam penulisan query SQL yang memungkinkan penyerang menyisipkan perintah berbahaya ke dalam sistem. Jika tidak ditangani dengan baik, serangan SQL Injection dapat mengakibatkan kebocoran data sensitif, manipulasi data akademik, hingga kerusakan sistem secara keseluruhan. Oleh karena itu, analisis keamanan terhadap sistem akademik berbasis web menjadi sangat penting untuk mengidentifikasi potensi kerentanan serta menentukan langkah pencegahan yang tepat guna melindungi data akademik dan menjaga keandalan sistem.

TINJAUAN PUSTAKA

Sistem Akademik Berbasis Web

Sistem akademik berbasis web merupakan aplikasi yang digunakan untuk mengelola, menyimpan, dan menyajikan informasi akademik secara terintegrasi melalui jaringan internet. Sistem ini umumnya mencakup pengelolaan data mahasiswa, dosen, mata kuliah, nilai, jadwal perkuliahan, serta berbagai proses administrasi akademik lainnya, (Alwan, Z. S., & Younis, M. F. (2016). Pemanfaatan teknologi web memungkinkan akses informasi secara real-time dan meningkatkan efisiensi serta efektivitas pengelolaan data akademik (Halfond, W. G., & Orso, A. (2005). Namun, keterbukaan akses melalui jaringan internet juga meningkatkan potensi terjadinya ancaman keamanan apabila sistem tidak dirancang dan diimplementasikan dengan mekanisme perlindungan yang memadai (Halfond,W. G., Viegas, J., & Orso, A. (2006).

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Keamanan Aplikasi Web

Keamanan aplikasi web merupakan serangkaian upaya yang dilakukan untuk melindungi aplikasi dari berbagai ancaman yang dapat merusak sistem, memodifikasi data, atau mencuri informasi sensitif (Kurniawan, Y., & Nugroho, A. (2019). Ancaman keamanan pada aplikasi web dapat muncul akibat kelemahan dalam pengelolaan input pengguna, mekanisme autentikasi dan otorisasi, serta pengelolaan basis data (Mereani, L., & Howells, G. (2012). Oleh karena itu, penerapan prinsip-prinsip keamanan seperti validasi input, enkripsi data, pengelolaan hak akses pengguna, serta pengamanan konfigurasi server menjadi aspek penting dalam pengembangan dan pengelolaan aplikasi berbasis web(Rahman, A., & Hidayat, T. (2020).

SQL Injection

SQL Injection merupakan salah satu jenis serangan yang paling umum dan berbahaya pada aplikasi web yang terhubung dengan basis data (Sadeghian, A., Zamani, B., & Ghorbani, A. A. (2013). Serangan ini terjadi ketika aplikasi gagal melakukan validasi input pengguna secara tepat, sehingga memungkinkan penyerang menyisipkan perintah SQL berbahaya ke dalam query yang dieksekusi oleh sistem (Shar, L. K., Tan, H. B. K., & Briand, L. C. (2013). Melalui serangan SQL Injection, penyerang dapat memperoleh akses tidak sah ke data, memodifikasi atau menghapus data penting, serta mengganggu kinerja dan keandalan sistem secara keseluruhan (Shin, Y., Meneely, A., Williams, L., & Osborne, J. (2011).

Pencegahan SQL Injection

Pencegahan serangan SQL Injection dapat dilakukan melalui penerapan berbagai teknik keamanan pada aplikasi web (Supriyanto, E., & Pratama, R. (2018). Beberapa teknik yang umum digunakan antara lain penggunaan prepared statement atau parameterized query, validasi dan sanitasi input pengguna, pembatasan hak akses pada basis data, serta penerapan mekanisme error handling yang aman agar informasi sistem tidak terungkap kepada pengguna (Tandon, A., & Kumar, R. (2015). Penerapan teknik-teknik tersebut terbukti efektif dalam mengurangi risiko serangan SQL Injection dan meningkatkan tingkat keamanan aplikasi web (Vieira, M., Antunes, N., & Madeira, H. (2009).

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi kasus. Metode ini dipilih untuk menganalisis tingkat keamanan sistem akademik berbasis web terhadap serangan SQL Injection berdasarkan kondisi aktual serta mekanisme keamanan yang diterapkan pada sistem tersebut (Zainal, A., & Setiawan, D. (2021). Pendekatan ini memungkinkan peneliti untuk memahami secara mendalam potensi kerentanan keamanan yang terdapat pada sistem akademik (Wassermann, G., & Su, Z. (2008).

Objek Penelitian

Objek penelitian dalam studi ini adalah sistem akademik berbasis web yang digunakan untuk pengelolaan data akademik, meliputi data mahasiswa, dosen, nilai, dan jadwal perkuliahan. Sistem tersebut dikembangkan menggunakan bahasa pemrograman PHP dan memanfaatkan basis data MySQL sebagai media penyimpanan data.

Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini meliputi studi literatur, observasi sistem, dan simulasi serangan SQL Injection. Studi literatur dilakukan dengan mengumpulkan referensi dari buku, jurnal ilmiah, serta artikel yang berkaitan dengan keamanan sistem informasi dan serangan SQL Injection. Observasi sistem dilakukan dengan mengamati struktur aplikasi web, khususnya pada bagian input data dan proses autentikasi pengguna. Selain itu, simulasi serangan SQL Injection dilakukan pada form login dan fitur input data untuk mengidentifikasi tingkat kerentanan sistem terhadap serangan tersebut.

Teknik Analisis Data

Data yang diperoleh dianalisis dengan mengidentifikasi potensi celah keamanan pada sistem akademik berbasis web. Analisis dilakukan dengan membandingkan kondisi sistem sebelum dan sesudah penerapan teknik pengamanan, seperti validasi input dan penggunaan prepared statement. Hasil analisis ini digunakan untuk menentukan tingkat risiko serangan SQL Injection serta efektivitas mekanisme keamanan yang diterapkan.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Tahapan Penelitian

Tahapan penelitian yang dilakukan dimulai dari identifikasi permasalahan keamanan pada sistem akademik berbasis web, dilanjutkan dengan studi literatur terkait SQL Injection dan keamanan aplikasi web. Tahap selanjutnya adalah pengujian sistem melalui simulasi serangan SQL Injection, kemudian dilakukan analisis terhadap hasil pengujian untuk mengidentifikasi kelemahan serta memberikan rekomendasi perbaikan keamanan sistem.

HASIL DAN PEMBAHASAN

Hasil Analisis Kerentanan SQL Injection

Bagian ini menyajikan hasil pengujian kerentanan SQL Injection yang dilakukan pada sistem akademik berbasis web. Pengujian difokuskan pada titik-titik input pengguna yang umum menjadi target serangan SQL Injection, yaitu form login, fitur pencarian data mahasiswa dan dosen, serta fitur input nilai. Hasil pengujian menunjukkan bahwa sistem masih memiliki sejumlah celah keamanan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab.

Kerentanan pada Form Login

Pengujian pada form login sistem akademik menunjukkan adanya kerentanan terhadap serangan Error-Based SQL Injection. Ketika input *username* atau *password* disisipi dengan karakter SQL yang tidak tervalidasi, sistem merespons dengan menampilkan pesan kesalahan dari basis data. Kondisi ini mengindikasikan bahwa query SQL disusun secara langsung dari input pengguna tanpa mekanisme pengamanan yang memadai.

Pada skenario pengujian, penyerang memasukkan string ' OR 1=1-- pada kolom *username* dan mengosongkan kolom *password*. Input tersebut bertujuan untuk memanipulasi query SQL pada sisi backend agar selalu bernilai benar. Sistem kemudian menampilkan pesan kesalahan SQL yang eksplisit, seperti kesalahan sintaks MySQL, yang mengungkapkan struktur query serta nama tabel dan kolom yang digunakan. Informasi ini dapat dimanfaatkan oleh penyerang untuk melakukan serangan lanjutan dengan tingkat kompleksitas yang lebih tinggi.

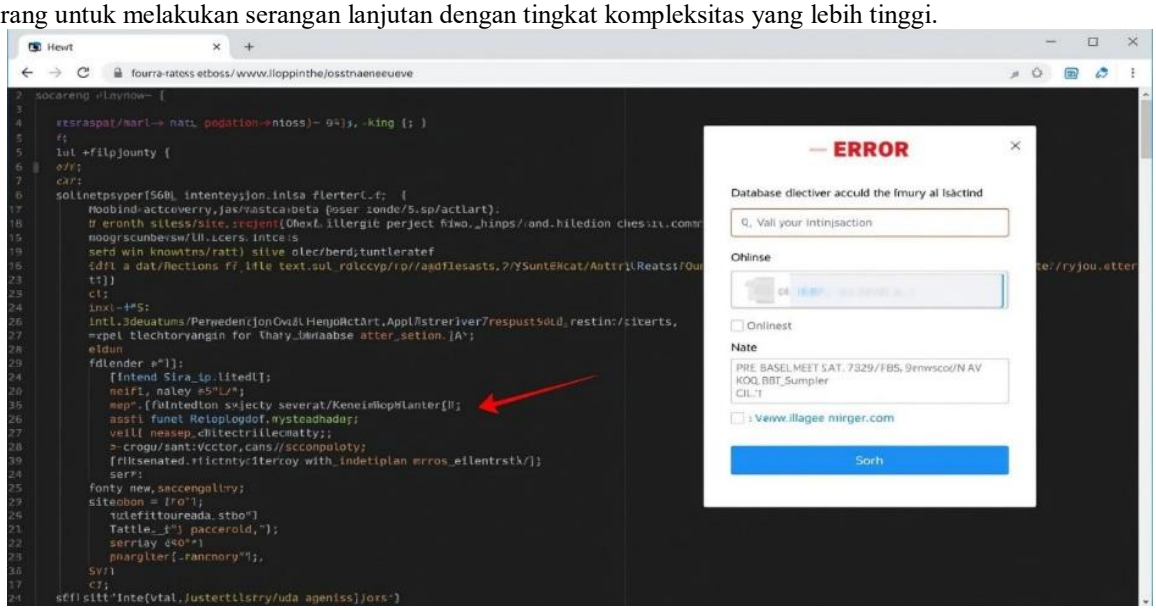

Fig. 1 Caption for fitur Pencarian Data Mahasiswa

Kerentanan pada Fitur Pencarian Data Mahasiswa

Fitur pencarian data mahasiswa ditemukan rentan terhadap serangan Union-Based SQL Injection. Melalui penyisipan klausa *UNION SELECT*, penyerang dapat menggabungkan hasil query asli dengan query berbahaya untuk mengekstrak data dari tabel lain dalam basis data.

Dalam pengujian, penyerang memasukkan payload berupa perintah *UNION SELECT* pada parameter pencarian Nomor Induk Mahasiswa (NIM). Akibatnya, sistem tidak hanya menampilkan data mahasiswa yang dicari, tetapi juga menampilkan data lain yang berasal dari tabel dosen, seperti nama, NIM atau NIP, alamat email, alamat, serta *hash* kata sandi. Temuan ini menunjukkan bahwa sistem tidak melakukan pembatasan query dan validasi input secara memadai, sehingga memungkinkan terjadinya kebocoran data lintas tabel.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

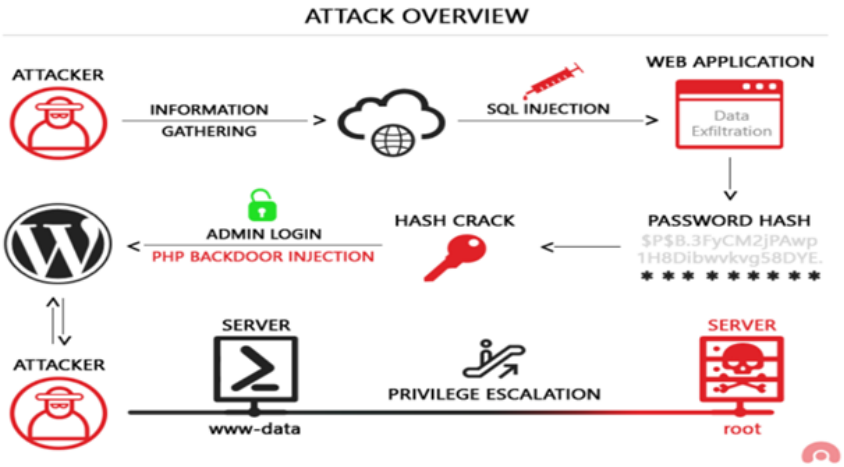

Fig. 2 Caption for Attack Overview

Kerentanan pada Input Nilai Dosen

Pengujian pada fitur input nilai dosen menunjukkan adanya kerentanan terhadap serangan Blind SQL Injection, khususnya tipe Boolean-Based Blind SQL Injection. Kerentanan ini terjadi meskipun sistem tidak menampilkan pesan kesalahan SQL secara langsung kepada pengguna.

Pada skenario pengujian, penyerang memanipulasi parameter identitas nilai dengan menyisipkan perintah SQL bersyarat. Penyerang kemudian mengamati perbedaan respons sistem untuk menentukan apakah kondisi tertentu bernilai benar atau salah. Melalui teknik ini, penyerang dapat menyimpulkan informasi sensitif dalam basis data, seperti *hash* kata sandi administrator, secara bertahap tanpa terdeteksi oleh sistem.

Pembahasan Dampak dan Risiko Serangan SQL Injection

Kerentanan yang teridentifikasi, terutama serangan Union-Based dan Blind SQL Injection, berpotensi menimbulkan dampak serius terhadap keamanan sistem akademik berbasis web. Kebocoran data pribadi mahasiswa dan dosen, seperti nama lengkap, NIM, NIP, alamat, nomor telepon, dan alamat email, dapat dimanfaatkan untuk berbagai serangan lanjutan, termasuk *phishing*, pencurian identitas, dan penipuan.

Selain itu, kebocoran data akademik seperti nilai mata kuliah, riwayat studi, status pendaftaran, dan status kelulusan dapat mengakibatkan manipulasi data akademik dan pemalsuan dokumen. Risiko lain yang tidak kalah penting adalah kebocoran informasi login berupa *hash* kata sandi pengguna, yang apabila berhasil didekripsi dapat memberikan akses tidak sah ke akun pengguna. Bahkan, pada sistem yang terintegrasi dengan modul pembayaran, serangan SQL Injection juga berpotensi membahayakan data keuangan pengguna.

Temuan ini menunjukkan bahwa tanpa penerapan mekanisme keamanan yang memadai, sistem akademik berbasis web memiliki tingkat risiko yang tinggi terhadap serangan SQL Injection dan membutuhkan peningkatan keamanan secara menyeluruh.

KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan, dapat disimpulkan bahwa sistem akademik berbasis web memiliki potensi kerentanan yang tinggi terhadap serangan SQL Injection apabila tidak menerapkan mekanisme keamanan yang memadai. Kelemahan utama sistem terletak pada pengolahan input pengguna yang tidak dilakukan secara valid dan aman, serta penggunaan query SQL tanpa menerapkan prepared statement. Kondisi tersebut memungkinkan terjadinya akses tidak sah dan meningkatkan risiko kebocoran data akademik yang bersifat sensitif. Oleh karena itu, penerapan validasi dan sanitasi input, penggunaan prepared statement, serta pengelolaan hak akses pengguna yang tepat merupakan langkah penting yang harus diterapkan untuk meningkatkan keamanan dan keandalan sistem akademik berbasis web.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Keamanan Sistem Komputer Universitas Malikussaleh yang telah memberikan dukungan akademik dan fasilitas selama pelaksanaan penelitian ini. Ucapan terima kasih juga disampaikan kepada dosen pembimbing dan dosen pengampu mata kuliah yang telah memberikan arahan, bimbingan,

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

serta masukan yang sangat berharga dalam penyusunan jurnal ini. Selain itu, penulis mengapresiasi seluruh pihak yang telah membantu, baik secara langsung maupun tidak langsung, dalam proses pengumpulan data, pengujian sistem, dan penyelesaian penelitian ini. Semoga hasil penelitian ini dapat memberikan kontribusi positif bagi pengembangan keamanan sistem akademik berbasis web.

REFERENSI

Alwan, Z. S., & Younis, M. F. (2016). Detection and prevention of SQL injection attack using pattern matching technique. *International Journal of Computer Science and Network Security*, 16(1), 27–34.

Antunes, N., & Vieira, M. (2010). Comparing the effectiveness of penetration testing and static code analysis on the detection of SQL injection vulnerabilities. *Journal of Systems and Software*, 83(10), 1941–1956.

Halfond, W. G., & Orso, A. (2005). AMNESIA: Analysis and monitoring for neutralizing SQL injection attacks. *IEEE Transactions on Software Engineering*, 31(10), 791–812.

Halfond, W. G., Viegas, J., & Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. *Proceedings of the IEEE International Symposium on Secure Software Engineering*, 13–15.

Kurniawan, Y., & Nugroho, A. (2019). Analisis keamanan aplikasi web terhadap serangan SQL injection. *Jurnal Teknologi Informasi*, 14(2), 85–92.

Mereani, L., & Howells, G. (2012). SQL injection prevention techniques: A review. *International Journal of Computer Science Issues*, 9(3), 1–9.

Rahman, A., & Hidayat, T. (2020). Penerapan prepared statement untuk mencegah SQL injection pada aplikasi web. *Jurnal Sistem Informasi*, 16(1), 45–52.

Sadeghian, A., Zamani, B., & Ghorbani, A. A. (2013). Detection of SQL injection attacks: A survey. *International Journal of Computer Science and Network Security*, 13(1), 1–11.

Shar, L. K., Tan, H. B. K., & Briand, L. C. (2013). Mining SQL injection and cross-site scripting vulnerabilities using hybrid program analysis. *Proceedings of the International Conference on Software Engineering*, 642–651.

Shin, Y., Meneely, A., Williams, L., & Osborne, J. (2011). Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities. *IEEE Transactions on Software Engineering*, 37(6), 772–787.

Supriyanto, E., & Pratama, R. (2018). Analisis keamanan sistem informasi akademik berbasis web. *Jurnal Informatika*, 12(3), 120–128.

Tandon, A., & Kumar, R. (2015). SQL injection attack detection and prevention techniques. *International Journal of Computer Applications*, 113(3), 1–6.

Vieira, M., Antunes, N., & Madeira, H. (2009). Using web security scanners to detect vulnerabilities in web services. *Proceedings of the IEEE/IFIP International Conference on Dependable Systems & Networks*, 566–571.

Wassermann, G., & Su, Z. (2008). Sound and precise analysis of web applications for injection vulnerabilities. *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation*, 32–41.

Zainal, A., & Setiawan, D. (2021). Pengujian keamanan sistem informasi berbasis web menggunakan metode penetration testing. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 5(2), 310–317.