Jurnal Informatika Press
Volume 10, Nomor 1, Juni 2026, ***Page*** **12-19**
ISSN 3032-6834 (Online - Elektronik)
Available Online at https://ejurnal.stmikmethodistbinjai.ac.id/jip

Kajian Risiko SQL *Injection* pada Sistem Informasi Pemerintah Kota Binjai Menggunakan NIST RMF 2.0

Alan Andriansyah[1], Riandy Yap[1], Marwa Halim[2,*]

[123] Teknik Informatika, STMIK Methodist Binjai, Binjai, Indonesia
Email: [1] alanandriansyah1207@gmail.com, [2] rianz12junior@gmail.com, [3,*]marwahalim@stmikmethodist.ac.id
Email Penulis Korespondensi: alanandriansyah1207@gmail.com

Abstrak−Perkembangan sistem informasi berbasis web dalam layanan pemerintahan meningkatkan efisiensi pelayanan publik, namun juga membuka peluang terjadinya ancaman keamanan siber. Salah satu ancaman yang sering terjadi pada aplikasi web adalah serangan SQL Injection, yaitu teknik eksploitasi yang memanfaatkan kelemahan validasi input pada sistem basis data. Penelitian ini bertujuan untuk menganalisis risiko serangan SQL Injection pada infrastruktur sistem informasi Pemerintah Kota Binjai dengan menggunakan kerangka kerja NIST Risk Management Framework (RMF) 2.0. Metode penelitian yang digunakan adalah pendekatan deskriptif dengan strategi studi kasus melalui pengujian keamanan menggunakan teknik penetration testing. Proses pengujian dilakukan menggunakan tools Burp Suite dan SQLMap untuk mengidentifikasi kerentanan pada parameter URL yang berinteraksi dengan basis data. Hasil penelitian menunjukkan bahwa beberapa endpoint pada aplikasi web Pemerintah Kota Binjai memiliki kerentanan SQL Injection pada parameter id_kategori dengan tingkat risiko tinggi. Kerentanan tersebut memungkinkan penyerang melakukan manipulasi query basis data yang dapat berdampak pada kebocoran informasi, perubahan data, hingga gangguan layanan sistem. Selain itu, sistem juga masih menampilkan pesan kesalahan basis data yang dapat mengungkap informasi internal aplikasi. Berdasarkan temuan tersebut, diperlukan penerapan kontrol keamanan seperti validasi input yang lebih ketat, penggunaan prepared statement atau parameterized query, serta implementasi Web Application Firewall untuk meminimalkan risiko serangan terhadap sistem informasi pemerintah.

Kata Kunci: SQL Injection; Keamanan Sistem Informasi; Penetration Testing; NIST Risk Management Framework; Website Pemerintah

Abstract−*The development of web-based information systems in government services has improved the efficiency and accessibility of public services. However, the increasing reliance on digital systems also introduces significant cybersecurity risks. One of the most common threats targeting web applications is SQL Injection, a technique that exploits weaknesses in input validation to manipulate database queries. This study aims to analyze the risk of SQL Injection attacks on the information system infrastructure of the Binjai City Government using the NIST Risk Management Framework (RMF) 2.0. The research employs a descriptive approach with a case study strategy through security testing using penetration testing techniques. The testing process was conducted using tools such as Burp Suite and SQLMap to identify vulnerabilities in URL parameters interacting with the database. The results indicate that several endpoints of the Binjai City Government website contain SQL Injection vulnerabilities in the id_kategori parameter, which are classified as high-risk vulnerabilities. These weaknesses allow attackers to manipulate database queries, potentially leading to information disclosure, data manipulation, or service disruption. In addition, the system still exposes database error messages that reveal internal application information. Therefore, security improvements are necessary, including strict input validation, the use of prepared statements or parameterized queries, and the implementation of a Web Application Firewall to reduce the risk of attacks on government information systems.*

Keywords: *SQL Injection; Information System Security; Penetration Testing; NIST Risk Management Framework; Government Website*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital dalam berbagai sektor, termasuk pemerintahan. Implementasi layanan berbasis elektronik atau *e-government* memungkinkan pemerintah meningkatkan efisiensi, transparansi, serta kualitas pelayanan publik kepada Masyarakat [1], [2]. Berbagai instansi pemerintah saat ini memanfaatkan sistem informasi berbasis web untuk mengelola data, menyediakan layanan administrasi, serta mempermudah akses informasi bagi Masyarakat [3], [4]. Namun, meningkatnya penggunaan sistem digital juga diikuti oleh meningkatnya risiko ancaman keamanan siber yang dapat mengganggu stabilitas layanan publik.

Ancaman keamanan siber terhadap sistem informasi pemerintah dapat terjadi dalam berbagai bentuk, mulai dari pencurian data hingga gangguan terhadap layanan publik. Salah satu jenis serangan yang sering menargetkan aplikasi web adalah *SQL Injection*, yaitu teknik serangan yang memanfaatkan kelemahan pada validasi input untuk mengakses atau memanipulasi basis data secara tidak sah [5], [6]. Kerentanan ini dapat berdampak pada kebocoran data sensitif, perubahan informasi secara ilegal, hingga gangguan terhadap operasional sistem informasi [7], [8].

Untuk mengurangi risiko serangan siber, berbagai pendekatan keamanan sistem informasi telah dikembangkan. Salah satu pendekatan yang banyak digunakan adalah penerapan algoritma kriptografi untuk melindungi data digital. Penelitian yang dilakukan oleh Manullang, Alwine, dan Sembiring [9] menunjukkan bahwa penggunaan algoritma *Advanced Encryption Standard* (AES) dengan metode *Cipher Block Chaining* mampu meningkatkan keamanan data dokumen digital. Selain itu, penggunaan teknik kriptografi juga terbukti mampu memperkuat perlindungan terhadap data digital dalam berbagai sistem informasi [10].

Submitted: **01/03/2026**; Accepted: **01/04/2026**; Published: **01/06/2026**

Jurnal Informatika Press
Volume 10, Nomor 1, Juni 2026, ***Page*** **12-19**
ISSN 3032-6834 (Online - Elektronik)
Available Online at https://ejurnal.stmikmethodistbinjai.ac.id/jip

Selain pengamanan data, perlindungan sistem jaringan juga dapat dilakukan melalui mekanisme deteksi serangan. Penelitian oleh Allwine dan Alwinang [11]menunjukkan bahwa penerapan *Intrusion Detection System* (IDS) dapat membantu mengidentifikasi aktivitas mencurigakan pada jaringan komputer sehingga potensi serangan dapat dideteksi lebih awal. Implementasi sistem keamanan jaringan yang baik menjadi salah satu komponen penting dalam menjaga keamanan sistem informasi yang terhubung dengan jaringan internet [4], [12].

Di sisi lain, peningkatan literasi digital juga berperan penting dalam menghadapi ancaman keamanan siber. Pemahaman mengenai kejahatan siber serta regulasi yang berlaku dapat membantu meningkatkan kesadaran organisasi maupun masyarakat terhadap pentingnya keamanan data digital [12]. Hal ini menunjukkan bahwa keamanan sistem informasi tidak hanya bergantung pada teknologi, tetapi juga pada kesiapan sumber daya manusia dalam mengelola serta melindungi sistem informasi dari berbagai ancaman [1], [13].

Dalam pemerintahan daerah, berbagai sistem informasi berbasis web telah digunakan untuk mendukung layanan publik seperti pengelolaan administrasi, penyediaan informasi, dan layanan pengaduan masyarakat. Penelitian yang dilakukan oleh Tania et al. [13]menunjukkan bahwa penerapan algoritma keamanan pada sistem informasi berbasis web dapat meningkatkan perlindungan terhadap data digital yang dikelola oleh instansi pemerintah. Namun demikian, sistem informasi yang terhubung dengan jaringan internet tetap memiliki potensi kerentanan terhadap berbagai serangan siber apabila tidak disertai dengan pengelolaan risiko keamanan yang sistematis [14], [15].

Berdasarkan kondisi tersebut, diperlukan pendekatan manajemen risiko keamanan informasi yang terstruktur untuk mengidentifikasi serta mengendalikan potensi ancaman yang dapat terjadi pada sistem informasi pemerintah. Salah satu kerangka kerja yang dapat digunakan adalah *NIST Risk Management Framework (RMF) 2.0*, yang menyediakan tahapan sistematis dalam pengelolaan risiko keamanan sistem informasi. Oleh karena itu, penelitian ini bertujuan untuk menganalisis risiko serangan *SQL Injection* terhadap infrastruktur sistem informasi Pemerintah Kota Binjai dengan menggunakan pendekatan *NIST Risk Management Framework (RMF) 2.0*, sehingga diharapkan dapat memberikan rekomendasi mitigasi risiko guna meningkatkan keamanan sistem informasi pada lingkungan pemerintahan daerah.

2. METODOLOGI PENELITIAN

3.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode deskriptif dengan pendekatan *studi kasus* untuk menganalisis tingkat keamanan sistem informasi pada *website* Pemerintah Kota Binjai. Pendekatan ini dipilih karena penelitian difokuskan pada satu objek penelitian secara mendalam guna mengidentifikasi potensi kerentanan terhadap serangan siber, khususnya *SQL Injection*. Proses penelitian dilakukan melalui simulasi pengujian keamanan menggunakan metode *penetration testing* untuk mengetahui kemungkinan eksploitasi celah keamanan pada sistem. Pendekatan ini memungkinkan peneliti memperoleh gambaran komprehensif mengenai kondisi keamanan *website* serta memberikan rekomendasi perbaikan berdasarkan temuan yang diperoleh.

3.2 Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui tiga metode utama yaitu observasi, eksperimen, dan dokumentasi. Observasi dilakukan dengan meninjau secara langsung struktur halaman *website*, parameter URL, serta berbagai *form input* yang berpotensi menjadi titik masuk serangan. Selanjutnya eksperimen dilakukan melalui pengujian keamanan menggunakan teknik *penetration testing* untuk mendeteksi kerentanan *SQL Injection* pada sistem web yang diuji. Seluruh proses pengujian kemudian didokumentasikan dalam bentuk catatan teknis dan tangkapan layar (*screenshot*) sebagai bukti proses penelitian serta sebagai bahan analisis dalam penyusunan hasil penelitian.

3.3 Teknik Analisis Data

Analisis data dalam penelitian ini mengacu pada kerangka kerja *NIST Risk Management Framework (RMF) 2.0* yang terdiri dari tahapan *prepare*, *categorize*, *select*, *implement*, *assess*, *authorize*, dan *monitor*. Tahapan tersebut digunakan untuk mengidentifikasi kerentanan, menilai dampak risiko berdasarkan aspek *Confidentiality*, *Integrity*, dan *Availability (CIA)*, serta menentukan kontrol keamanan yang sesuai untuk mitigasi risiko [16]. Pengujian kerentanan dilakukan menggunakan *tools* seperti *Burp Suite* dan *SQLMap* untuk mensimulasikan serangan *SQL Injection*. Hasil pengujian kemudian dianalisis menggunakan pendekatan penilaian risiko seperti *OWASP Risk Rating Methodology* dan *Common Vulnerability Scoring System (CVSS)* guna menentukan tingkat risiko serta menyusun rekomendasi mitigasi keamanan sistem.

3. HASIL DAN PEMBAHASAN

Submitted: **01/03/2026**; Accepted: **01/04/2026**; Published: **01/06/2026**

Jurnal Informatika Press
Volume 10, Nomor 1, Juni 2026, *Page* 12-19
ISSN 3032-6834 (Online - Elektronik)
Available Online at https://ejurnal.stmikmethodistbinjai.ac.id/jip

3.1 Implementasi

Setelah penelitian dilakukan, diperoleh tingkat dan jenis-jenis kerentanan *(vulnerability)* yang terdapat pada infrastruktur sistem informasi Pemerintah Kota Binjai. Untuk melakukan analisis kerentanan tersebut, peneliti menggunakan indikator klasifikasi tingkat risiko yaitu *Critical*, *High*, *Medium*, *dan Low*, guna mengelompokkan setiap kerentanan berdasarkan tingkat keparahannya.

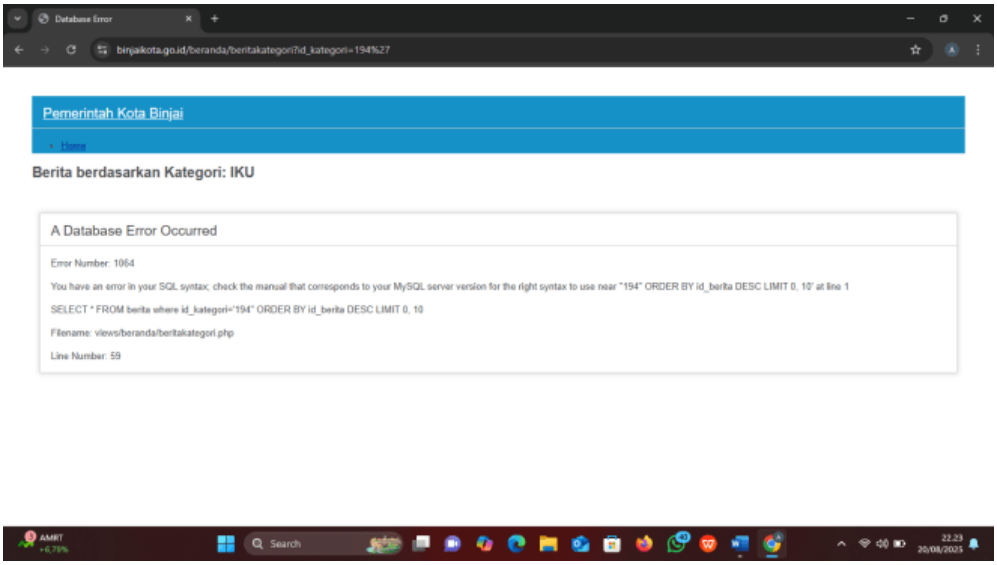
Proses pengujian keamanan *(penetration testing)* difokuskan pada identifikasi ancaman serangan *SQL Injection* yang berpotensi mengeksploitasi kelemahan pada sistem, khususnya pada sisi basis data. Hasil pengujian ini kemudian dianalisis dengan menggunakan kerangka kerja *NIST RMF 2.0*, sehingga diperoleh gambaran tingkat risiko yang dapat dijadikan acuan bagi pengambil keputusan dalam menentukan strategi mitigasi.

Data dan informasi yang diperoleh selanjutnya akan dituangkan dalam bentuk laporan resmi yang ditujukan kepada pihak *administrator* sistem informasi Pemerintah Kota Binjai. Laporan tersebut berfungsi sebagai rekomendasi perbaikan dan peningkatan keamanan agar kerentanan yang ditemukan tidak dapat dieksploitasi oleh pihak yang tidak berwenang.

3.2 Komponen Utama Dalam Implementasi

Perangkat yang digunakan terdiri dari perangkat keras dan perangkat lunak. Perangkat keras yang digunakan meliputi PC dengan prosesor Intel Core i5, SSD minimal 256 GB dengan memori 8 GB, layar LCD berukuran 12 inci, serta perangkat pendukung berupa keyboard dan mouse. Sementara itu, perangkat lunak yang digunakan dalam proses pengujian dan analisis meliputi sistem operasi *Windows 11 Pro*, *VirtualBox* sebagai platform virtualisasi, serta *Kali Linux* yang digunakan untuk melakukan pengujian keamanan dan simulasi serangan terhadap sistem.

3.3 Kerentanan pada Infrastruktur Sistem Informasi Pemerintah Kota Binjai



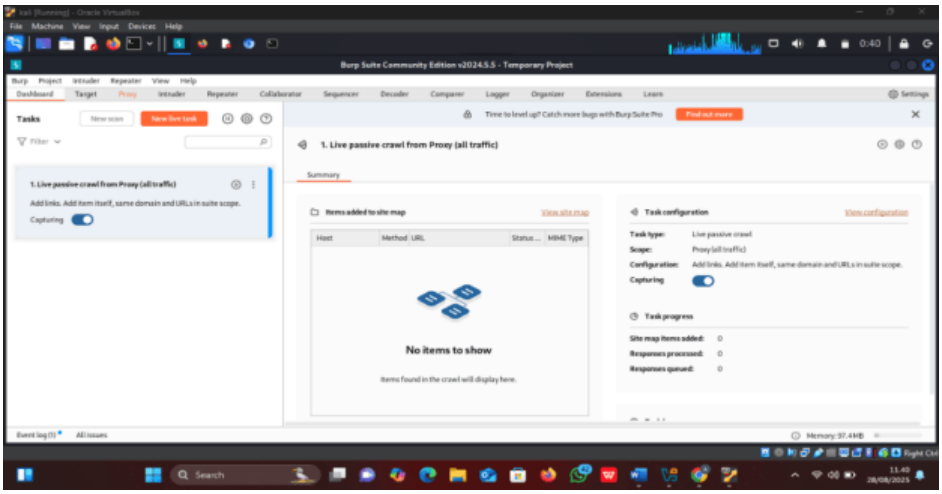
Gambar 1. Kerentanan *Web*

Infrastruktur sistem informasi Pemerintah Kota Binjai menghadapi berbagai kelemahan krusial yang berpotensi membuka pintu bagi serangan *SQL Injection.* Di antaranya adalah kurangnya mekanisme validasi dan sanitasi input secara menyeluruh, yang memungkinkan data berbahaya mudah masuk ke sistem. Selain itu, penggunaan *query SQL* yang dibangun secara dinamis tanpa penerapan prepared statements atau parameterized queries membuat database sangat rentan terhadap injeksi perintah berbahaya. Infrastruktur juga belum didukung dengan monitoring dan deteksi ancaman secara real-time yang efektif, sehingga aktivitas mencurigakan sulit teridentifikasi sejak awal. Kurangnya pelatihan keamanan bagi pengelola sistem menambah risiko kesalahan konfigurasi dan pemeliharaan, sehingga memperbesar kemungkinan terjadinya pelanggaran keamanan yang serius. Kombinasi dari faktor-faktor ini menciptakan lingkungan yang rawan terhadap serangan yang dapat merusak integritas, kerahasiaan, dan ketersediaan data penting pemerintah Kota Binjai.

3.4 Pengujian Identifikasi Kerentanan

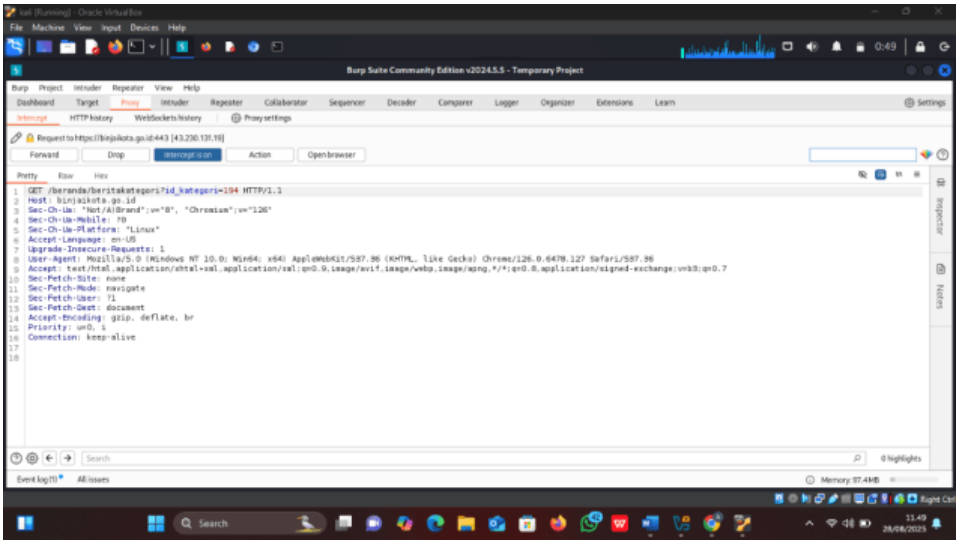
Submitted: **01/03/2026**; Accepted: **01/04/2026**; Published: **01/06/2026**

Jurnal Informatika Press
Volume 10, Nomor 1, Juni 2026, ***Page*** **12-19**
ISSN 3032-6834 (Online - Elektronik)
Available Online at https://ejurnal.stmikmethodistbinjai.ac.id/jip



Gambar 2. Tampilan *Brupsuite*

Berikut ini tampilan utama brup suite dapat disimpulkan bahwa perangkat ini menyediakan antarmuka yang komprehensif untuk mendukung proses penetration testing secara sistematis



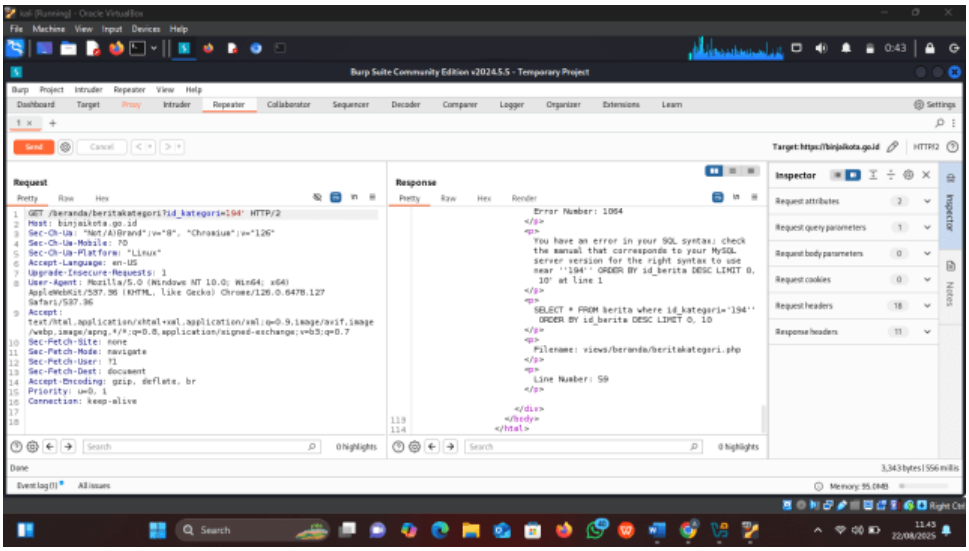
Gambar 3. *Proxy*

Pengujian dilakukan menggunakan *Burp Suite* dengan pendekatan *black-box*. Seluruh trafik *HTTP/HTTPS* dari peramban diarahkan ke *proxy Burp* untuk memungkinkan intersepsi dan modifikasi permintaan sebelum dikirim ke *server*. Fokus pengujian pada tahap ini adalah endpoint yang menerima parameter *GET* berkaitan dengan pemanggilan data berita. Selama pengujian, peneliti mengirimkan *baseline request* terlebih dahulu untuk memastikan perilaku normal aplikasi.

Permintaan kemudian dimodifikasi di *Burp Repeater* dengan menambahkan karakter tunggal (') pada nilai parameter numerik (id_berita=194'). Modifikasi minimal ini digunakan untuk menguji apakah input pengguna digabungkan langsung ke *query* SQL tanpa *parameterization* yang tepat.

Submitted: **01/03/2026**; Accepted: **01/04/2026**; Published: **01/06/2026**

Jurnal Informatika Press
Volume 10, Nomor 1, Juni 2026, *Page* 12-19
ISSN 3032-6834 (Online - Elektronik)
Available Online at https://ejurnal.stmikmethodistbinjai.ac.id/jip



Gambar 4. Tampilan *Repeater*

Server mengembalikan pesan kesalahan basis data berikut: *"You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '194' ORDER BY id_berita DESC LIMIT 0, 10' at line 1."* Kemunculan pesan kesalahan MySQL tersebut mengindikasikan dua hal penting, yaitu terjadinya penggabungan input pengguna secara langsung ke dalam pernyataan SQL yang menunjukkan indikasi kuat kerentanan *error-based SQL Injection*, serta aplikasi yang mengekspos detail internal seperti tipe DBMS dan potongan query (*ORDER BY id_berita DESC LIMIT 0, 10*) sehingga meningkatkan risiko *information disclosure*. Karakter tanda petik tunggal (') yang disisipkan pada konteks numerik menyebabkan struktur query terputus sehingga MySQL menghasilkan *syntax error*. Kondisi ini umumnya terjadi ketika aplikasi tidak menggunakan *prepared statement* atau *parameterized query*, tidak melakukan validasi tipe data (misalnya memastikan parameter *id_berita* selalu berupa bilangan bulat), serta tidak menerapkan mekanisme penanganan kesalahan yang bersifat generik sehingga pesan kesalahan detail dari DBMS langsung ditampilkan kepada klien.

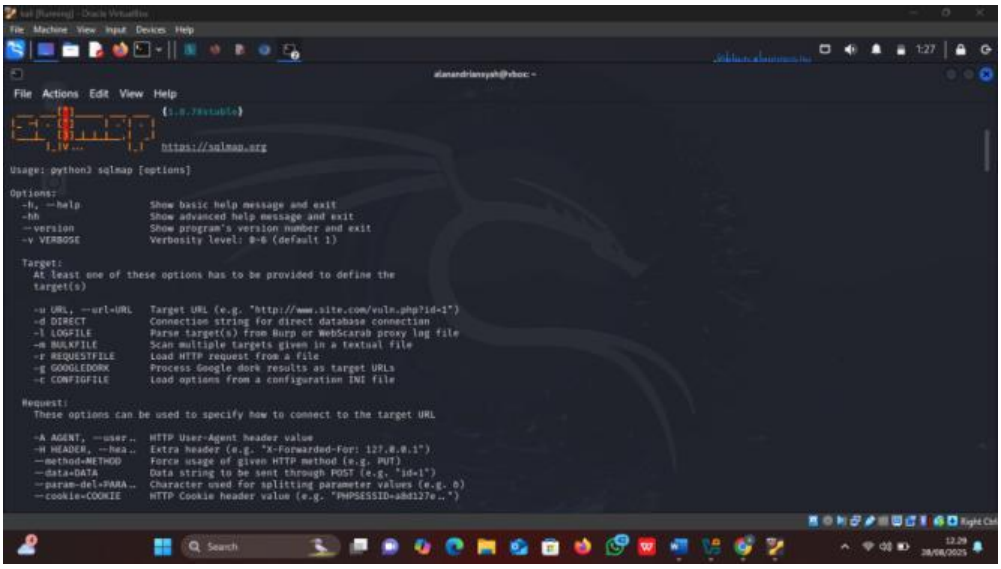
3.5 Evaluasi Efektivitas Kontrol

Gambar 5. Kali *Linux*

Setelah titik kerentanan berhasil diidentifikasi menggunakan *Burp Suite*, langkah berikutnya adalah melakukan *eksploitas*i lebih lanjut menggunakan *kali linux* untuk menilai tingkat keparahan kerentanan dan efektivitas kontrol keamanan yang diterapkan aplikasi.

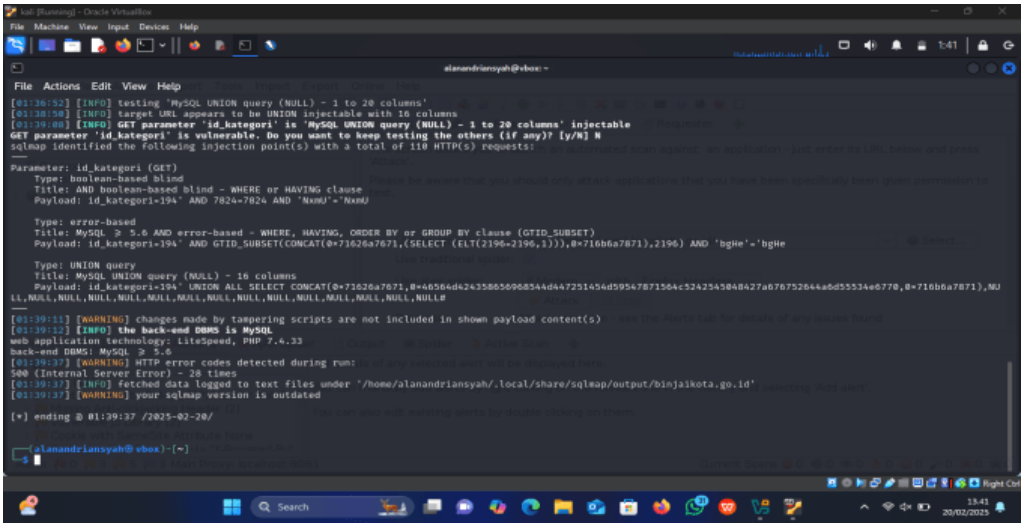
Submitted: **01/03/2026**; Accepted: **01/04/2026**; Published: **01/06/2026**

Jurnal Informatika Press
Volume 10, Nomor 1, Juni 2026, *Page* 12-19
ISSN 3032-6834 (Online - Elektronik)
Available Online at https://ejurnal.stmikmethodistbinjai.ac.id/jip



Gambar 6. SQL Map

Pada tahap ini, peneliti menggunakan *SQLMap*, yaitu sebuah *open-source penetration testing tool* yang dirancang khusus untuk mendeteksi serta mengeksploitasi kelemahan *SQL Injection*.



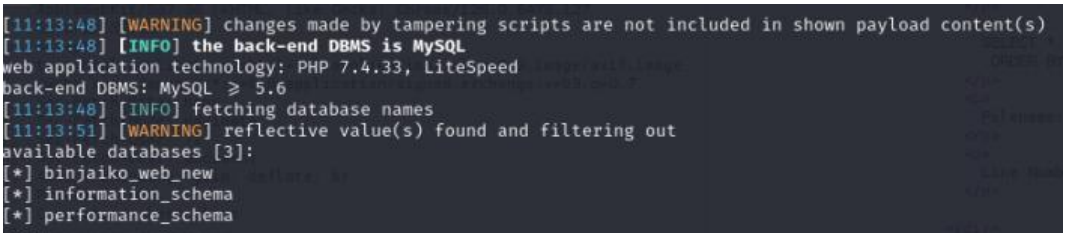
Gambar 7. Pengujian Gagal

Berdasarkan hasil eksekusi *SQLMap* terhadap parameter id_kategori, alat berhasil mengidentifikasi bahwa endpoint tersebut rentan terhadap beberapa jenis *SQL Injection*, yakni *boolean-based blind*, *error-based*, dan *union query injection*. *SQLMap* juga mendeteksi bahwa teknologi backend menggunakan *LiteSpeed* dengan *PHP 7.4.33*, serta basis data yang digunakan adalah *MySQL* versi 5.6 atau lebih tinggi. Meskipun demikian, proses enumerasi basis data tidak berhasil menampilkan nama database secara eksplisit. Hal ini disebabkan karena server beberapa kali memberikan respons *HTTP 500 Internal Server Error* ketika *SQLMap* menjalankan payload lanjutan. *Error 500* ini menunjukkan adanya mekanisme proteksi di sisi server, baik berupa pembatasan eksekusi *query*, penanganan *error* yang lebih ketat,*waf* yang aktif, maupun batasan konfigurasi yang secara tidak langsung menghambat upaya eksploitasi otomatis dengan demikian peneliti mencoba menggunakan temper skrip agar peneliti dapat tau apakah proteksi atau waf dapat di *baypass* atau tidak.

Submitted: **01/03/2026**; Accepted: **01/04/2026**; Published: **01/06/2026**

Jurnal Informatika Press
Volume 10, Nomor 1, Juni 2026, ***Page*** **12-19**
ISSN 3032-6834 (Online - Elektronik)
Available Online at https://ejurnal.stmikmethodistbinjai.ac.id/jip

3.6 Temuan dan Rekomendasi



Gambar 8. Percobaan Berhasil

Berdasarkan hasil pengujian menggunakan *SQLMap*, ditemukan bahwa parameter id_kategori pada aplikasi *web* masih rentan terhadap beberapa teknik serangan *SQL Injection*, antara lain *boolean-based blind*, *error-based*, dan *UNION-based injection*. Hal ini menunjukkan bahwa mekanisme validasi input yang digunakan pada aplikasi belum memadai Selain itu, selama pengujian ditemukan bahwa sistem masih menampilkan pesan kesalahan (*error message*) *MySQL* secara langsung ke pengguna. Pesan seperti *"You have an error in your SQL syntax..."* memberikan informasi tambahan kepada penyerang mengenai query yang dijalankan oleh aplikasi. Kondisi ini dikategorikan sebagai *information disclosure* yang dapat dimanfaatkan untuk menyusun payload lanjutan, Temuan lain menunjukkan adanya respon *HTTP 500 Internal Server Error* ketika *SQLMap* melakukan payload eksplorasi lebih dalam. Meskipun hal ini dapat dianggap sebagai bentuk kontrol terbatas di sisi *server*, kenyataannya tidak cukup untuk mencegah serangan *SQL Injection* secara keseluruhan. Hal ini terbukti dari tetap berhasilnya *SQLMap* mengekstraksi nama *database* yang ada.

4. KESIMPULAN

Berdasarkan hasil penelitian, pengujian SQL Injection pada aplikasi web Pemerintah Kota Binjai menunjukkan adanya kerentanan pada parameter URL yang ditandai dengan munculnya pesan kesalahan sintaks SQL dari server. Hal ini mengindikasikan bahwa input pengguna tidak divalidasi dengan baik sehingga memungkinkan terjadinya injeksi kode berbahaya ke dalam query basis data. Kerentanan tersebut berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses, mengubah, atau menghapus data penting pada sistem, serta mengekspos informasi internal seperti jenis basis data yang digunakan, yaitu MySQL. Pengujian dilakukan menggunakan metode black box testing dengan bantuan tools seperti Burp Suite dan SQLMap yang mampu mendeteksi titik lemah sistem tanpa memerlukan akses langsung ke kode sumber aplikasi. Oleh karena itu, diperlukan peningkatan keamanan sistem melalui penerapan validasi input yang ketat, penggunaan prepared statement atau parameterized query, serta implementasi Web Application Firewall (WAF) untuk mencegah serangan serupa. Selain itu, audit keamanan dan penetration testing secara berkala serta peningkatan kapasitas sumber daya manusia dalam bidang keamanan aplikasi web juga perlu dilakukan agar kerentanan keamanan dapat diminimalkan dan sistem informasi pemerintah dapat beroperasi secara lebih aman dan andal.

REFERENCES

[1] W. L. Jaelani, Y. Yanto, and F. Khoirunnisa, "Penetration Testing Website dengan Metode Black Box Testing untuk Meningkatkan Keamanan Website pada Instansi," *Naratif J. Nas. Riset, Apl. dan Tek. Inform.*, vol. 5, no. 1, pp. 1–8, 2023.

[2] R. G. Putra *et al.*, "Pentingnya Manajemen Security di Era Digitalisasi," *J. Ilmu Multi Disiplin*, vol. 2, no. 1, pp. 305–332, 2022.

[3] T. Tumija and P. A. Erlambang, "Implementasi Sistem Informasi Pemerintahan Daerah (SIPD) dalam Perencanaan Anggaran Daerah Kabupaten Ogan Komering Ulu Provinsi Sumatera Selatan," *J. Media Birokrasi*, pp. 155–169, 2023, doi: 10.33701/jmb.v5i2.3696.

[4] G. Ardiansyah, E. Irawadi, A. Widya, and M. Gaffar, "Analisis Keamanan Website SIAKAD menggunakan Pentest Tools," *J. Ilm.*, vol. 1, no. 4, pp. 379–388, 2024.

[5] P. G. S. Adinata, I. P. W. P. Putra, N. P. A. I. Juliantari, and K. D. A. Sutrisna, "Analisis Perbandingan Tools SQL Injection Menggunakan SQLmap, SQLsus dan The Mole," *Inform. J. Ilmu Komput.*, vol. 18, no. 3, pp. 286–292, 2022.

[6] M. Baklizi, I. Atoum, N. Abdullah, O. A. Al-Wesabi, A. A. Otoom, and M. A. S. Hasan, "A Technical Review of SQL Injection Tools and Methods: A Case Study of SQLMap," *Int. J. Intell. Syst. Appl. Eng.*, vol. 10, no. 3, pp. 75–85, 2022.

[7] A. Paul, "SQL Injection Attack: Detection, Prioritization and Prevention," *Int. J. Inf. Secur. Sci.*, 2024,

Submitted: **01/03/2026**; Accepted: **01/04/2026**; Published: **01/06/2026**

doi: 10.1016/j.future.2024.103456.

[8] H. S. Potti, H. T. Chen, and H. M. Sun, "Security Testing Framework for Web Applications: Benchmarking ZAP V2.12.0 and V2.13.0 by OWASP as an Example," *arXiv Prepr.*, 2025, [Online]. Available: https://arxiv.org/abs/2401.04356

[9] S. F. Manullang, Allwine, and J. Sembiring, "PENGAMANAN DATA FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD MODE CHIPER BLOCK CHAINING," vol. 17, no. 1, pp. 53–67, 2023.

[10] M. Halim and Wulan Sri Lestari, "Steganography Menggunakan Advanced Encryption Standard dan Metode Least Significant Bit pada File Bitmap 24-bit," *J. Armada Inform.*, vol. 7, no. 2, pp. 295–300, 2023, doi: 10.36520/jai.v7i2.76.

[11] Allwine and A. O. D. Aritonang, "Keamanan Jaringan Terpusat Mengunakan Intrusion Detection System (Ids) Di Stmik Methodist Binjai : Keamanan Jaringan Terpusat Mengunakan Intrusion Detection System (Ids) Di Stmik Methodist Binjai ," *J. Armada Inform.*, vol. 1, no. 1 SE-Articles, pp. 1–11, 2022, [Online]. Available: http://jurnal.stmikmethodistbinjai.ac.id/index.php/jai/article/view/20

[12] I. Sidabutar, L. Neri Tarigan, and M. Melisa Br Ginting, "Seminar : Peningkatan Kecakapan Literasi Digital dan Pengenalan Undang-Undang Cybercrime," *J. Pengabdi. Masy. Variasi*, vol. 1, no. 1, pp. 9–12, 2024, [Online]. Available: https://idpress.ac.id/jpmv

[13] M. Tania, T. S. Alasi, and R. Yap, "Algoritma Aes Untuk Keamanan Data Digital Berbasis Web Di Kantor Desa Aman Damai," *J. TIMES*, vol. 13, no. 2, pp. 142–149, 2024, doi: 10.51351/jtm.13.2.2024781.

[14] N. Luthfah, "Serangan siber sebagai penggunaan kekuatan bersenjata dalam perspektif hukum keamanan nasional Indonesia," 2021, [Online]. Available: https://www.researchgate.net/publication/355468298_Serangan_Siber_Sebagai_Penggunaan_Kekuatan_Bersenjata_dalam_Perspektif_Hukum_Keamanan_Nasional_Indonesia_Cyber_Attacks_as_the_Use_of_Force_in_the_Perspective_of_Indonesia_National_Security_Law

[15] R. Primartha, *Security Jaringan Komputer Berbasis CEH*. Informatika, 2022.

[16] P. Calderon, *Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips*. Packt Publishing Ltd, 2021.

Submitted: **01/03/2026**; Accepted: **01/04/2026**; Published: **01/06/2026**