JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1603-1608

Analisis Kerentanan Website Setjen Kemendagri Menggunakan Penetrasi SQL Injection

Saprudin[1*], Syaid Agil Al Munawar[2], Rafika Himmatul Aliyah[3], Najwa Chantika A[4], Wahyu Ramadhan[5]

[1,2,3,4,5]Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
Email : [1*]dosen00845@gmail.com, [2]syaidagil21@gmail.com, [3]rafikaaliyah30@gmail.com, [4]najwachantika7@gmail.com, [5]wahyurmdhn030919@gmail.com
(* : coressponding author)

Abstrak - Di era digital, keamanan informasi adalah aspek yang sangat penting, terutama di sektor pemerintahan. Penetration testing berbasis SQL-Injection adalah metode yang efektif untuk mengidentifikasi kerentanan pada sebuah situs web dan meningkatkan keamanannya. Studi ini menggunakan teknik pengujian penetrasi dengan menggunakan alat SQLMAP pada situs web setjen.kemendagri.go.id. Hasil studi menunjukkan bahwa situs web tersebut rentan terhadap serangan SQL Injection, yang dapat menyebabkan risiko serius seperti kebocoran data dan manipulasi informasi. Studi ini bertujuan untuk mengedukasi pihak-pihak terkait tentang pentingnya keamanan situs web pemerintah dan memberikan wawasan serta mendorong penerapan langkah-langkah pencegahan dan korektif untuk melindungi integritas dan kerahasiaan data strategis pemerintah. Dengan upaya ini, sistem informasi pemerintah diharapkan menjadi lebih tangguh terhadap ancaman siber.

Kata Kunci: *Cyber Security*, *Penetration Test, SQL Injection, Website*

Abstract **-** In the digital era, information security is a very important aspect, especially in the government sector. SQL Injection-based penetration testing is one effective method to identify vulnerabilities on a website and improve its security. This study uses penetration testing techniques by utilizing the SQLMAP tool on the setjen.kemendagri.go.id website. The results of the study indicate that the website is vulnerable to SQL Injection attacks, which can result in serious risks such as data leakage and information manipulation. This study is expected to provide education and insight to related parties regarding the importance of government website security, as well as encourage the implementation of preventive and corrective measures to protect the integrity and confidentiality of strategic government data. With this effort, the government information system is expected to become more resilient to cyber threats.

Keywords: *Cyber Security*, *Penetration Test, SQL Injection, Website*

1. PENDAHULUAN

Di era digital, situs web telah menjadi sarana penting untuk menyediakan informasi dan layanan publik secara efektif, terutama bagi lembaga pemerintah. Instruksi Presiden No. 3 tahun 2003 menekankan pentingnya pengembangan administrasi elektronik untuk meningkatkan efisiensi dan transparansi layanan publik melalui digitalisasi. Salah satu contohnya adalah situs web setjen.kemendagri.go.id, yang menyediakan layanan strategis untuk masyarakat luas. (Dewi, 2022).

Namun, perkembangan ini juga disertai dengan meningkatnya ancaman keamanan siber. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa serangan siber di Indonesia terus meningkat, dengan insiden SQL Injection menjadi salah satu ancaman yang paling sering dilaporkan. (Irawati, 2024). SQL-Injection memanfaatkan kelemahan dalam validasi input pada aplikasi web untuk menyisipkan perintah SQL berbahaya, yang dapat menyebabkan kebocoran data atau manipulasi informasi penting. (Risky, 2021).

Sebuah studi lain menunjukkan bahwa sektor pemerintah, mengingat jumlah besar data strategis yang dikelola oleh sistem mereka, sangat rentan terhadap serangan ini. (Fathurrahman & Ramadhan, 2020). Telah terbukti bahwa teknik mitigasi seperti penerapan kueri parametrik dan penguatan validasi input dapat mengurangi risiko serangan SQL Injection. (Santoso, 2021). Selain itu, pengujian penetrasi dengan alat seperti SQLMAP telah terbukti efisien dalam mendeteksi dan mengevaluasi celah keamanan yang signifikan pada situs web publik. (Haryadi & Widodo, 2019).

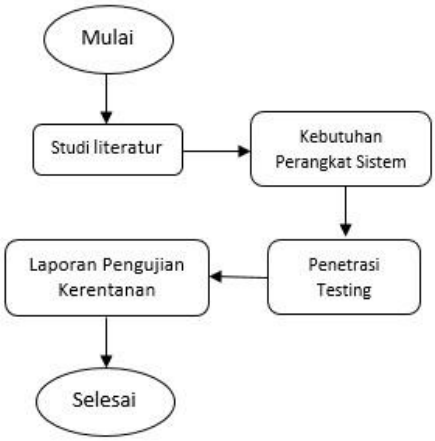
Tujuan dari studi ini adalah untuk melakukan pengujian penetrasi pada situs web setjen.kemendagri.go.id dengan menggunakan teknik SQL-Injection menggunakan alat SQLMAP.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1603-1608

Dengan mengidentifikasi potensi celah keamanan, studi ini bertujuan untuk memberikan rekomendasi mitigasi yang efektif guna meningkatkan keamanan situs web pemerintah.

2. METODE PENELITIAN

Kerangka penelitian adalah langkah sistematis yang bertujuan untuk memastikan bahwa penelitian terstruktur dan dapat diterima oleh semua pihak yang terlibat. Kerangka penelitian yang diterapkan dalam studi ini ditunjukkan dalam Gambar 1.



Gambar 1. Metode Penelitian

Berdasarkan Gambar 1, terlihat bahwa metode penelitian yang digunakan dalam jurnal terdiri dari studi literatur, persyaratan perangkat sistem, uji penetrasi, analisis dan desain, serta laporan dan kesimpulan.

2.2. Studi Literatur

Pada tahap ini, penulis mengumpulkan berbagai referensi dan teori yang menjadi dasar penyusunan jurnal ini. Teori-teori pendukung mencakup pemahaman tentang berbagai celah keamanan web yang mudah diserang menggunakan SQLI, penggunaan alat SQL Map untuk pengujian penetrasi, dan referensi dari jurnal penelitian atau jurnal terkait yang relevan dengan topik ini.

2.3 Kebutuhan Perangkat Sistem

Pada fase ini, identifikasi perangkat yang digunakan dilakukan, termasuk perangkat keras dan perangkat lunak. Perangkat keras yang digunakan dalam studi ini adalah laptop Lenovo Ideapad 3 dengan prosesor AMD Ryzen 3 5000U, RAM 8 GB, SSD 512 GB, dan sistem operasi Linux Ubuntu yang mendukung proses pengujian sistem. Perangkat lunak yang digunakan adalah SQL Map, yang dapat digunakan untuk melakukan pengujian di situs web.

2.4 Penetrasi Testing

Pada tahap ini dilakukan identifikasi celah kerentanan SQL Injection (SQLI) pada website setjen.kemendagri.go.id, proses pengujian keamanan dilaksanakan melalui dua tahap penetrasi testing. Tahap pertama melibatkan pengujian manual dengan menyisipkan payload SQLI pada berbagai titik rentan seperti URL, form pencarian, form login, form pendaftaran, dan form input komentar/saran.

Selanjutnya, pada tahap kedua, dilakukan pengujian menggunakan alat bantu SQLMAP untuk menganalisis lebih mendalam potensi kerentanan keamanan website tersebut. Melalui pendekatan komprehensif ini, tujuan utama adalah mendeteksi dan mengidentifikasi celah keamanan yang berpotensi dapat dieksploitasi melalui serangan SQL Injection.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1603-1608

2.5 Laporan Pengujian Kerentanan

Pada fase terakhir penyelidikan, data yang diperoleh melalui proses pemindaian dan pemanfaatan dianalisis untuk membuat laporan yang dapat digunakan oleh pengembang sebagai referensi dalam meningkatkan keamanan situs web. Data akan dikelompokkan berdasarkan jenis kerentanan, sumber kerentanan, dan solusi mitigasi untuk memudahkan analisis. Informasi yang diperoleh selama pengujian dijelaskan secara rinci menggunakan terminologi teknis yang mudah dipahami, sehingga laporan ini dapat menjadi sumber informasi yang berguna dan relevan bagi manajer situs web dalam perbaikan. Laporan investigasi ini juga mencakup pendekatan yang diterapkan selama pengujian penetrasi dan proses penilaian keamanan.

3. HASIL DAN PEMBAHASAN

3.1 Tahapan Analisa

Dalam proses analisis ini, dilakukan pengujian untuk mengidentifikasi celah keamanan pada situs web setjen.kemendagri.go.id terhadap serangan SQL-Injection (SQLI). Pengujian dilakukan dengan alat SQLMAP, yang secara otomatis mendeteksi kerentanan SQL-Injection dengan menganalisis respons server terhadap berbagai payload yang dihasilkan.

Proses kerja SQLMAP mencakup penyisipan payload ke dalam parameter input yang rentan dan menganalisis respons server untuk mengidentifikasi potensi kerentanan. Jika parameter yang rentan ditemukan, SQLMAP dapat mengeksploitasi kerentanan tersebut, misalnya dengan membaca data dari basis data, untuk menunjukkan risiko keamanan yang ada. Hasil ini memberikan gambaran menyeluruh tentang tingkat kerentanan situs web, termasuk risiko kebocoran data strategis pemerintah.

Berdasarkan kerangka penelitian yang mencakup studi literatur, persyaratan perangkat sistem, pengujian penetrasi, dan laporan pengujian kerentanan, analisis data dari hasil pengujian dilakukan untuk memberikan rekomendasi keamanan. Untuk mempermudah proses analisis, sebuah diagram alir telah dibuat yang menjelaskan tahap-tahap pengujian kerentanan, seperti yang ditunjukkan pada Gambar 2.

Gambar 2. Tahapan Analisa

3.2 Informasi

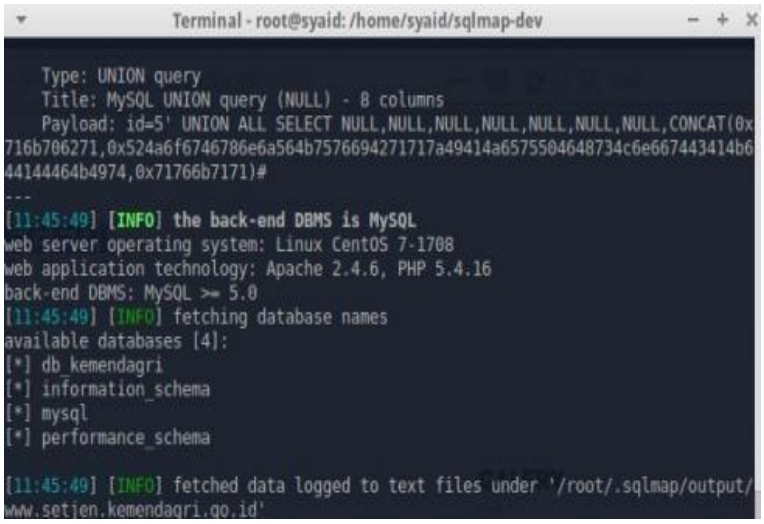
Informasi yang digunakan dalam studi ini berasal dari situs web Sekretariat Jenderal Kementerian Dalam Negeri. Data yang dikumpulkan mencakup nama situs, domain, dan alamat IP situs web yang ditentukan melalui proses pemindaian manual. Berdasarkan data yang dikumpulkan, uji coba sampel dilakukan untuk memahami alur kerja situs.

Uji coba sampel dimulai dengan URL, di mana penambahan tanda kutip tunggal (‘) di akhir URL dengan parameter menghasilkan pesan kesalahan. Informasi dari uji coba sampel ini menjadi dasar untuk analisis lebih lanjut.

3.3 Teknik SQLI

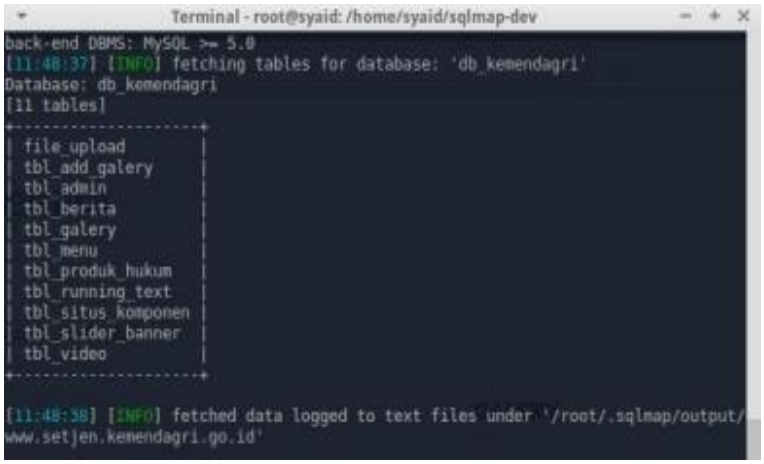
Proses awal penetrasi testing pada penelitian ini yaitu menggunakan teknik SQLI dengan cara menyisipkan karakter spesial di akhir url yang memiliki parameter. Yang kemudian url yang memiliki parameter tersebut di eksekusi menggunakan tool SQLMAP seperti gambar 4.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1603-1608



Gambar 3. SQLMAP Mendapatkan Database

Setelah validasi dengan SQLMAP, ternyata situs web tersebut rentan terhadap serangan SQLInjection, dan alat tersebut berhasil mengakses database situs web. Hasil pengujian menunjukkan bahwa database *db_kemendagri* berisi data penting.



Gambar 4. Database

Seperti yang ditunjukkan pada Gambar 5, basis data tersebut mengandung data administrator yang sangat sensitif. Jika data ini jatuh ke tangan pihak yang tidak bertanggung jawab seperti *Blackhat-Hacker*, risiko keamanan menjadi sangat serius. Data tersebut dapat digunakan untuk mengambil alih sistem, memanipulasi informasi, atau bahkan mencuri data strategis lainnya. Oleh karena itu, perlindungan terhadap kerentanan SQL Injection sangat penting untuk mencegah jenis eksploitasi ini.

3.4 Hasil

Setelah melakukan analisis terhadap situs web setjen.kemendagri menggunakan teknik SQLInjection (SQLI), sebuah laporan dibuat yang berisi rincian tentang kerentanan yang ditemukan, kemungkinan dampak dari serangan tersebut, dan rekomendasi untuk metode pencegahan guna mengatasi kerentanan tersebut.

Laporan ini dimaksudkan untuk digunakan oleh pengembang situs web serupa sebagai referensi untuk mengevaluasi dan meningkatkan keamanan sistem mereka. Langkah-langkah yang disarankan termasuk penerapan pembaruan perangkat lunak, peningkatan parameter input, dan

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1603-1608

penguatan sistem keamanan untuk mengurangi risiko serangan di masa depan. Dengan demikian, situs web diharapkan menjadi lebih aman dan lebih tahan terhadap ancaman siber.

Tabel 1. Efek Dan Pencegahan Kerentanan

NO	Kerentanan	Efek Kerentanan	Pencegahan Kerentanan
1	Sensitive Data Exposure	Penyerang dapat mengakses informasi sensitif seperti kunci enkripsi, token, dan konfigurasi server yang dapat dieksploitasi untuk mendapatkan akses tidak sah, memanipulasi data, atau mengganggu operasi sistem secara keseluruhan.	Perlu untuk membatasi akses publik ke file konfigurasi dengan memastikan bahwa file tersebut disimpan di luar direktori root publik. Selain itu, izin minimum harus diterapkan sehingga hanya pemilik file yang memiliki izin untuk membaca atau menulis file, guna mencegah akses tidak sah dan melindungi informasi sensitif.
2	SQL Injection untuk mendapatkan database website	Penyerang dapat mengambil data penting dan memanfaatkan database yang bersifat pribadi atau rahasia untuk diperjual belikan / untuk hal negatif lainnya	Gunakan kueri parametrik atau instruksi yang dipersiapkan agar masukan pengguna tidak langsung diinterpretasikan sebagai bagian dari perintah SQL. Selain itu, validasi dan pembersihan input harus
			dilakukan untuk memastikan bahwa hanya data yang sesuai yang dapat diproses, sehingga karakter jahat yang berpotensi disalahgunakan dapat dihilangkan. Hak akses basis data juga harus dibatasi sesuai dengan prinsip hak istimewa terkecil, sehingga hanya akses minimal yang diberikan untuk operasi yang benar-benar diperlukan, guna meminimalkan risiko jika terjadi pelanggaran.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa situs web setjen.kemendagri.go.id rentan terhadap serangan SQL-Injection (SQLI), yang memungkinkan akses tidak sah ke data strategis seperti informasi administrator dan basis data penting lainnya. Pengujian dengan alat SQLMAP telah berhasil mengidentifikasi celah keamanan dalam parameter input situs web, yang dapat dieksploitasi untuk kebocoran data, manipulasi informasi, atau pengambilalihan sistem. Untuk mengatasi kelemahan ini, studi merekomendasikan langkah-langkah mitigasi seperti validasi dan pembersihan input, penggunaan kueri parametrik, pembatasan hak akses database, dan pengamanan data rahasia. Hasil penelitian ini dimaksudkan untuk menjadi panduan bagi pengembang situs web pemerintah dalam meningkatkan keamanan siber dan dengan demikian melindungi integritas dan kerahasiaan data strategis dari ancaman di masa depan.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1603-1608

REFERENCES

Dewi, B. T. (2022). Kajian literatur: Metode dan tools pengujian celah keamanan aplikasi berbasis web. *Jurnal Teknologi Informasi, 5*(2), 34–45.

Fathurrahman, R., & Ramadhan, W. (2020). Analisis kerentanan aplikasi web pemerintah terhadap serangan SQL Injection. *Jurnal Informatika dan Keamanan Siber, 8*(1), 23–31.

Haryadi, M., & Widodo, A. (2019). Implementasi SQLMAP dalam pengujian keamanan web pemerintah. *Jurnal Teknologi dan Sistem Informasi, 6*(2), 45–53.

Irawati. (2024, Oktober 31). Ngeri! Ada 122,79 juta serangan siber ke RI, sektor ini target utamanya. Diambil kembali dari Infobanknews: https://infobanknews.com/ngeriada-12279-juta-serangan-siber-ke-ri-sektor-ini-target-utamanya/

Risky, M. A. (2021). Optimalisasi dalam penetrasi testing keamanan website menggunakan teknik SQL Injection dan XSS. *Jurnal Sistem Informasi dan Teknologi, 3*(4), 215– 220.

Santoso, E. (2021). Strategi pencegahan SQL Injection pada sistem informasi akademik. *Jurnal Teknik Informatika, 9*(3), 89–98.

Widjaja, R., & Andriani, P. (2020). Studi kasus keamanan data pada website instansi pemerintah. *Jurnal Sistem dan Keamanan, 10*(1), 12–20.

Yuliana, A. (2019). Penggunaan SQLMAP untuk menguji keamanan aplikasi web publik. *Jurnal Teknologi Informasi Terapan, 7*(4), 55–63.