JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i3.6507

PEMANFAATAN *SQLMAP* UNTUK DETEKSI *SQL INJECTION* PADA SITUS WEB

Hulwa Salsabila[1*], Raka Fazah Fithra[2]

[1,2]Universitas Singaperbangsa Karawang, Jl.HS.Ronggo Waluyo, Puseurjaya, Telukjambe Timur, Karawang, Jawa Barat 41361, Telp. (0267) 641177

Keywords:
SQL Injection, *SQLMAP*, Keamanan Web, *Kali Linux*, *Database*.

Corespondent Email:
hulwaslsbl11@gmail.com

Abstrak. *SQL Injection* merupakan ancaman serius terhadap keamanan situs web dinamis yang banyak digunakan di internet. Serangan ini dapat mengekspos informasi sensitif dan merusak integritas sistem. Oleh karena itu, penelitian ini dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanannya pada situs web menggunakan alat *SQLMAP*. Alat ini memungkinkan pemindaian dan pengambilan data dari *database* yang rentan terhadap serangan *SQL Injection*. Penelitian dimulai dengan pemindaian situs web untuk mengidentifikasi *database* yang digunakan, dilanjutkan dengan eksplorasi tabel-tabel dan akhirnya melakukan dumping data dari tabel yang dipilih. Hasil penelitian menunjukkan bahwa *SQLMAP* dapat digunakan secara efektif untuk mendeteksi dan mengeksploitasi kerentanan pada situs web yang memiliki celah *SQL Injection*. Meskipun efektif, penggunaannya membutuhkan pemahaman teknis yang mendalam tentang SQL dan pengaturan server. Hasil ini penting dalam konteks pengujian keamanan situs web, serta memberikan kontribusi bagi pengembangan alat yang lebih efektif dalam mendeteksi dan mengatasi potensi serangan *SQL Injection*. Penelitian ini diharapkan dapat meningkatkan kesadaran dan pemahaman tentang pentingnya pengamanan situs web terhadap serangan *SQL Injection*.

Abstract. *SQL Injection is a serious threat to the security of dynamic websites widely used on the internet. This attack can expose sensitive information and compromise system integrity. Therefore, this research was conducted to identify and exploit vulnerabilities in websites using the SQLMAP tool. This tool allows for scanning and extracting data from databases vulnerable to SQL Injection attacks. The research started by scanning the website to identify the database in use, followed by exploring the tables, and finally dumping data from the selected table. The results of the study show that SQLMAP can be effectively used to detect and exploit vulnerabilities in websites with SQL Injection flaws. Although effective, its use requires a deep technical understanding of SQL and server configurations. These findings are significant in the context of website security testing and contribute to the development of more effective tools to detect and address potential SQL Injection attacks. This research is expected to raise awareness and understanding of the importance of securing websites against SQL Injection attacks.*

1. PENDAHULUAN

Pada era digital saat ini, hampir semua aplikasi web modern mengandalkan sistem *database* terpusat untuk mentransfer dan mengelola informasi. Seiring dengan meningkatnya ketergantungan pada aplikasi web, ancaman terhadap keamanan sistem informasi juga semakin berkembang [1]. Salah satu ancaman yang paling signifikan adalah

serangan *SQL Injection*. Serangan ini terjadi ketika penyerang memanfaatkan kelemahan dalam sistem untuk mengirimkan perintah SQL berbahaya ke server *database* [2]. Biasanya, serangan ini mengeksploitasi saluran input yang tidak divalidasi dengan baik, yang memungkinkan penyerang untuk menyisipkan perintah SQL yang tidak sah. Dalam konteks ini, celah keamanan pada aplikasi web memungkinkan penyerang untuk menggunakan skrip SQL khusus guna mengelabui server web. Dengan demikian, penyerang dapat memperoleh otentikasi dan mengakses *database*, yang kemudian memungkinkan mereka untuk mencuri atau memanipulasi data yang ada [3].

Serangan *SQL Injection* memungkinkan penyerang untuk mengakses sistem tanpa memerlukan kredensial atau akses yang sah, cukup dengan mengeksploitasi celah dalam aplikasi [4]. Selain mencuri data sensitif seperti email dan kata sandi, serangan ini juga memungkinkan penyerang untuk mengubah atau menghapus data dalam *database*, atau bahkan menonaktifkan *database* web tersebut sehingga layanan menjadi tidak tersedia [5]. Oleh karena itu, untuk memahami lebih dalam mengenai teknik ini dan cara melindungi aplikasi web dari serangan tersebut, penggunaan alat seperti *SQLMAP* menjadi sangat penting. *SQLMAP* merupakan alat yang digunakan untuk mengidentifikasi dan mengeksploitasi celah keamanan dalam aplikasi web yang rentan terhadap SQL Injection [6]. Alat ini dapat dijalankan pada sistem operasi Kali Linux yang terkenal dengan kemampuannya dalam melakukan pengujian penetrasi. Penggunaan SQLMAP pada server Ubuntu memungkinkan pengguna untuk melakukan serangan SQL Injection, serta meningkatkan efektivitas dalam mengeksploitasi kerentanannya pada aplikasi web [7]. SQLMAP memudahkan pengguna dalam mendeteksi celah keamanan, mengakses data secara otomatis tanpa memerlukan langkah manual yang rumit. Alat ini juga efisien karena mampu mengidentifikasi berbagai jenis DBMS dan memberikan informasi yang diperlukan dengan lebih cepat. [8].

Penelitian yang dilakukan oleh [9] menunjukkan hasil yang signifikan. Penelitian ini berhasil mengidentifikasi berbagai celah keamanan dengan memanfaatkan alat *SQLMAP* pada sistem operasi *Kali Linux*. Temuan dari penelitian ini menunjukkan bahwa banyak situs web masih rentan terhadap serangan *SQL Injection*. Penelitian ini juga menemukan kelemahan dalam memperoleh data yang sensitif, seperti otentikasi yang lemah, serta struktur tabel dan kolom yang tidak aman. Pengujian terhadap serangan *SQL Injection* dilakukan dengan metode yang sederhana namun efektif, dengan menekankan pentingnya pengamanan sistem agar lebih tahan terhadap ancaman dari administrator dan pengelola situs [10]. Penelitian ini bertujuan untuk menganalisis serangan *SQL Injection* menggunakan *SQLMAP* pada situs web yang memiliki potensi kerentanannya, dengan memanfaatkan *Kali Linux* sebagai platform untuk melakukan eksploitasi. Penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam mengenai cara kerja *SQLMAP* dalam mengeksploitasi celah keamanan dan memberikan rekomendasi untuk penguatan sistem keamanan yang lebih baik guna melindungi aplikasi web dari ancaman *SQL Injection*.

2. TINJAUAN PUSTAKA

2.1 SQL Injection

SQL Injection merupakan tipe serangan yang sering digunakan oleh peretas karena banyak situs web yang masih belum mengoptimalkan perlindungan terhadap celah keamanan dalam sistem mereka [11]. Serangan ini terjadi ketika penyerang memanfaatkan kelemahan pada aplikasi web yang tidak memvalidasi input dengan benar, memungkinkan mereka untuk menyisipkan perintah SQL berbahaya [9]. Ketika aplikasi web tidak melakukan validasi atau penyaringan yang cukup terhadap input pengguna, penyerang dapat mengeksploitasi celah ini untuk mengakses atau memanipulasi *database* tanpa izin. Hal ini menunjukkan pentingnya pengembang aplikasi untuk mengimplementasikan langkah-langkah pengamanan yang memadai dalam menangani input dari pengguna untuk mencegah serangan *SQL Injection* [3].

2.2 SQLMAP

SQLMAP merupakan sebuah alat yang digunakan untuk mendeteksi dan

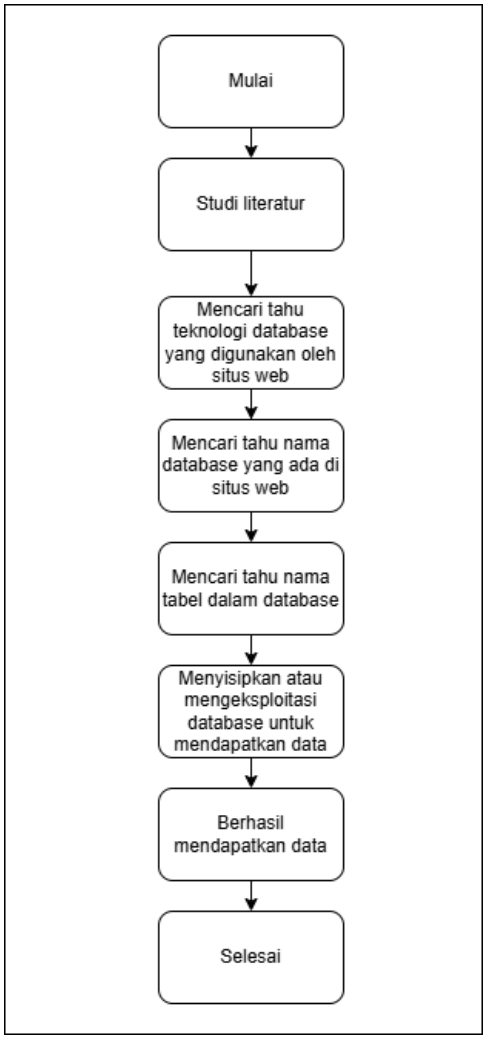
mengeksploitasi celah keamanan pada aplikasi web yang rentan terhadap serangan *SQL Injection.* Alat ini memanfaatkan celah keamanan pada aplikasi web untuk mengekstrak informasi sensitif, seperti data autentikasi dan struktur *database*. Dalam penelitian ini, *SQLMAP* digunakan untuk menganalisis berbagai aplikasi web yang diketahui memiliki celah *SQL Injection*, dengan tujuan untuk memahami bagaimana alat ini dapat mengidentifikasi dan mengeksploitasi kerentanannya. Berdasarkan studi kasus yang dilakukan, *SQLMAP* terbukti efektif dalam mengakses informasi sensitif yang terdapat dalam *database* target dengan memanfaatkan celah keamanan yang ada. Eksperimen yang dilakukan menggunakan *Virtual machine* Ubuntu dan Oracle VM *VirtualBox* menunjukkan tingkat keberhasilan yang tinggi dalam menjalankan serangan *SQL Injection*. Selain itu, penelitian ini juga mencakup analisis efektivitas strategi mitigasi, seperti penggunaan Web *Application Firewall*, untuk melindungi aplikasi web dari serangan serupa. Data yang dikumpulkan dari eksperimen ini memberikan wawasan penting mengenai cara *SQLMAP* beroperasi dan strategi mitigasi yang dapat diterapkan untuk meningkatkan keamanan aplikasi web dari ancaman *SQL Injection* [8].

2.3 Kali Linux

Kali Linux merupakan sistem operasi berbasis sumber terbuka yang banyak digunakan untuk pengujian penetrasi dan analisis keamanan siber. Salah satu keunggulan utama *Kali Linux* adalah ketersediaan lebih dari 600 alat keamanan yang telah terinstal sebelumnya, yang memungkinkan pengguna untuk melakukan berbagai jenis pengujian penetrasi dengan efisien tanpa perlu menginstal alat tambahan. Alat-alat ini mencakup berbagai fungsi, seperti analisis jaringan, eksploitasi kerentanannya, dan analisis forensik, yang sangat penting dalam pengujian kerentanannya aplikasi web, termasuk dalam pengujian *SQL Injection*. Dengan kemampuan untuk mendukung berbagai perangkat keras dan platform virtual, *Kali Linux* menawarkan fleksibilitas tinggi bagi profesional keamanan untuk menjalankan pengujian di berbagai lingkungan. Kemampuan tersebut menjadikan *Kali Linux* pilihan populer di kalangan profesional yang bekerja dengan infrastruktur TI yang beragam, memungkinkan mereka untuk melakukan analisis lebih efektif [12].

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah pendekatan penelitian tindakan, yang dipilih karena fokusnya yang langsung pada objek yang diteliti, yaitu pengolahan database dalam situs web. Penelitian dimulai dengan mengidentifikasi situs web yang ditargetkan untuk memperoleh data sensitif dari situs tersebut. Adapun langkah-langkah yang akan dilakukan dalam penelitian ini adalah sebagai berikut:



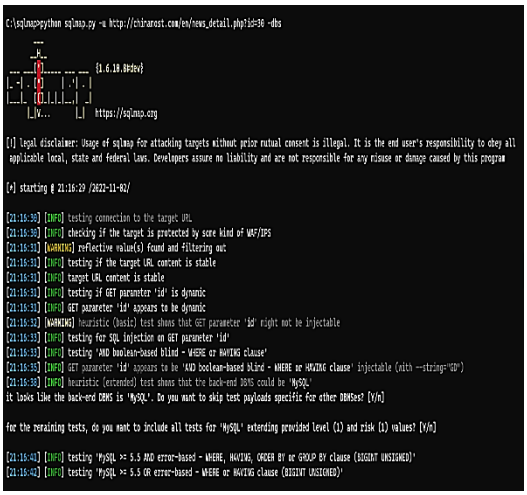
Gambar 1. Alur Penelitian

Tahapan penelitian ini adalah:

1. Studi literatur untuk mempelajari lebih lanjut mengenai *SQL Injection, SQLMAP*, dan keamanan *database*.

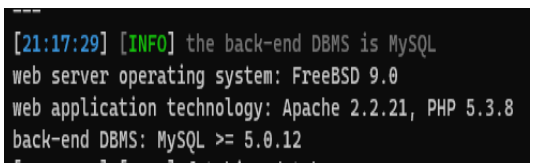
2. Mencari tahu teknologi *database* yang digunakan website tersebut.
3. Mencari tahu nama *database* yang ada di website tersebut.
4. Mencari tahu nama tabel website tersebut.
5. Mendapatkan data pada website tersebut.

4. HASIL DAN PEMBAHASAN



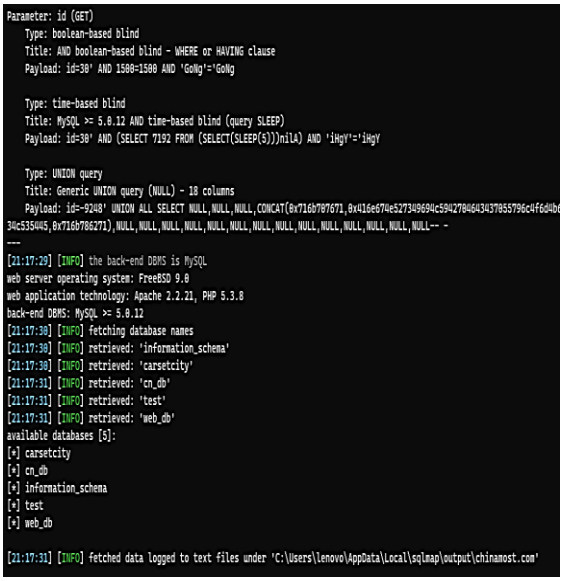
Gambar 2. Web *SQLMAP*

Pada gambar 2, proses pemindaian dilakukan terhadap situs web ***Chinamost*** (http://chinamost.com/en/news_detail.php?id=30) dengan menggunakan *SQLMAP*. Pemindaian dimulai dengan menjalankan perintah untuk mendapatkan informasi mengenai *database* yang digunakan oleh situs tersebut, yaitu dengan menggunakan *query python SQLMAP.py -u http://chinamost.com/en/news_detail.php?id=30 --dbs*. Perintah ini bertujuan untuk mendeteksi adanya kerentanannya terhadap serangan *SQL Injection* dan mengakses informasi sensitif yang mungkin ada di dalam *database* situs web yang ditargetkan.



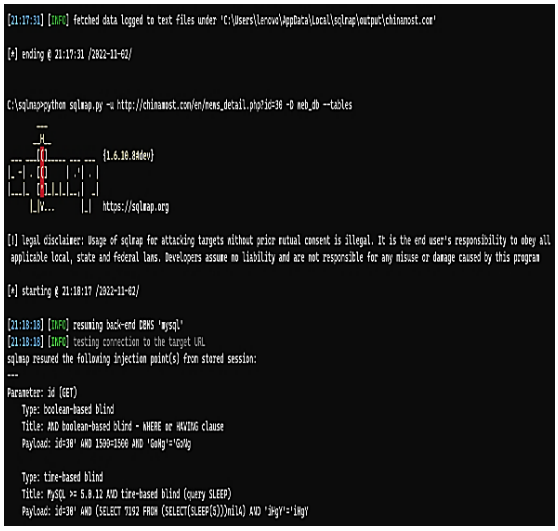
Gambar 3. Mendapatkan database yang digunakan

Pada gambar 3, *SQLMAP* berhasil mengidentifikasi informasi terkait server web dan teknologi yang digunakan oleh situs web target. Dalam hasil pemindaian ini, terlihat bahwa sistem operasi yang digunakan oleh server web adalah *FreeBSD 9.0*, dengan teknologi aplikasi web Apache 2.2.21 dan PHP 5.3.8. Selain itu, *SQLMAP* juga mendeteksi bahwa *database* yang digunakan oleh situs web ini adalah MySQL dengan versi 5.0.12 atau lebih tinggi. Informasi ini sangat berguna untuk mengetahui lebih lanjut mengenai infrastruktur situs web yang sedang diuji dan membantu dalam merencanakan langkah-langkah pengujian keamanan lebih lanjut.



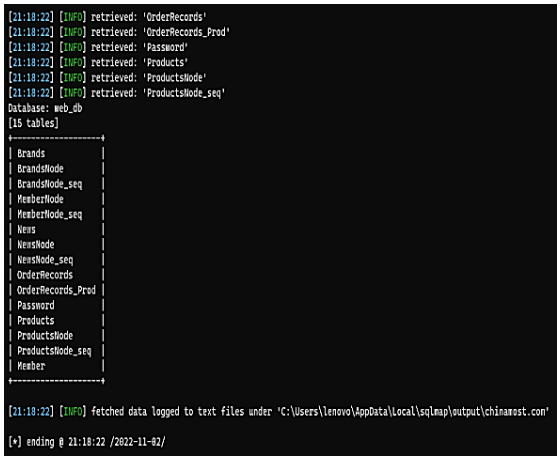
Gambar 4. Mendapatkan *database*

Pada gambar 4, hasil pemindaian menggunakan *SQLMAP* menunjukkan *database* yang ada di server situs web target. Setelah proses pemindaian berhasil, *SQLMAP* berhasil mengidentifikasi beberapa *database* yang digunakan oleh situs web tersebut. *Database* yang terdeteksi meliputi information_schema, carcicity, test, dan web_db. Informasi ini memberikan gambaran tentang struktur dan isi *database* yang terdapat pada server, yang penting untuk langkah selanjutnya dalam pengujian kerentanannya, terutama dalam mencari celah atau informasi sensitif yang mungkin dapat diakses melalui *SQL Injection*.



Gambar 5. Menargetkan *database*

Pada gambar 5, untuk mendapatkan informasi tentang tabel yang ada dalam *database* situs web target, kami menjalankan perintah *SQLMAP* dengan menambahkan parameter -D diikuti nama *database* yang sudah terdeteksi sebelumnya, serta menambahkan --tables. Perintah yang digunakan adalah python *SQLMAP*.py http://chinamost.com/en/news_detail.php?id=30 -D (nama *database*) --tables. Langkah ini bertujuan untuk mengidentifikasi tabel-tabel yang ada dalam *database* tersebut, yang merupakan langkah penting untuk mengakses data lebih lanjut atau menguji kerentanannya.

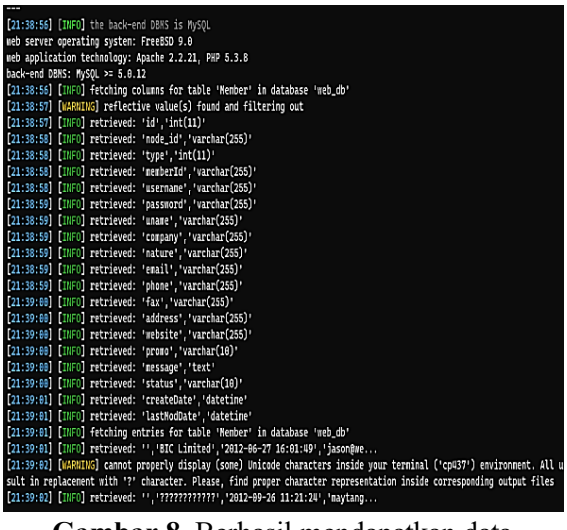


Gambar 6. Perintah *SQLMAP*

Pada gambar 6, *SQLMAP* berhasil mengidentifikasi dan menampilkan tabel-tabel yang ada dalam *database* web_db pada situs web target. Beberapa tabel yang terdeteksi antara lain Brands, OrderRecords, Products, dan Member. Informasi ini menunjukkan struktur data dalam situs web yang dapat digunakan untuk langkah pengujian lebih lanjut.

Gambar 7. Mendapatkan data pada tabel

Pada gambar 7, untuk melakukan dumping data dari tabel Member yang telah teridentifikasi sebelumnya, kami menjalankan perintah *SQLMAP* dengan menambahkan parameter -D untuk nama *database*, -T untuk nama tabel, dan --dump untuk mengambil data dari tabel tersebut. Perintah yang digunakan adalah python *SQLMAP*.py http://chinamost.com/en/news_detail.php?id=30 -D web_db -T Member --dump. Langkah ini bertujuan untuk mengekstrak informasi dari tabel Member yang terdapat dalam *database* web_db.



Gambar 8. Berhasil mendapatkan data member

Pada gambar 8, *SQLMAP* berhasil menampilkan data dari tabel Member yang ada dalam *database* web_db. Proses ini dilakukan setelah memilih kolom-kolom yang relevan dalam tabel Member, seperti name, email, password, dan address. *SQLMAP* kemudian mengekstrak dan menampilkan data yang berhasil ditemukan, meskipun ada peringatan terkait masalah tampilan karakter yang tidak dapat ditampilkan dengan benar. Hasilnya menunjukkan informasi sensitif dari situs web target yang berhasil diekstraksi.

5. KESIMPULAN

a. Penelitian ini berhasil menggunakan *SQLMAP* untuk mengidentifikasi dan memperoleh informasi sensitif dari situs web target melalui teknik *SQL Injection*, yang mencakup pemindaian *database*, penemuan nama *database* dan tabel, serta proses dumping data yang berhasil menampilkan informasi member.
b. Kelebihan penggunaan *SQLMAP* terletak pada kemampuannya yang efisien untuk mendeteksi dan mengambil data dari situs web yang rentan terhadap *SQL Injection*. Namun, efektivitasnya sangat bergantung pada pemahaman teknis pengguna serta konfigurasi dan perlindungan situs web yang diuji.
c. Meskipun alat ini efektif dalam pengujian kerentanannya, pengembangan lebih lanjut dapat dilakukan untuk meningkatkan kemampuannya dalam menghadapi serangan yang lebih kompleks dan meningkatkan antarmuka pengguna agar lebih ramah bagi profesional yang tidak terbiasa dengan penggunaan baris perintah.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dalam penelitian ini, serta kepada rekan-rekan yang telah memberikan masukan dan kritik konstruktif selama penelitian.

DAFTAR PUSTAKA

[1] A. M. Albaehaqi, M. I. Andriana, R. H. Hidayat, T. Informatika, and U. M. Bakti, "NUTRICHIVE : APLIKASI MOBILE UNTUK DETEKSI BAHAN MAKANAN DAN REKOMENDASI RESEP GUNA," *JITET (Jurnal Inform. dan Tek. Elektro Ter.*, vol. 13, no. 1, 2025.

[2] T. I. M. Pratama, M. D. F. Songida, and I. Gunawan, "Analisis Serangan dan Keamanan pada SQL Injection: Sebuah Review Sistematik," *JIIFKOM (Jurnal Ilm. Inform. dan Komputer)*, vol. 1, no. 2, pp. 27–32, 2022, doi: 10.51901/jiifkom.v1i2.230.

[3] R. Hermawan, "Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux," *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 6, no. 2, p. 210, 2021, doi: 10.30998/string.v6i2.11477.

[4] A. Andria and R. Pamungkas, "Penetration Testing Database Menggunakan Metode SQL Injection Via SQLMap di Termux," *Indonesian Journal of Applied Informatics*, vol. 5, no. 1. p. 1, 2021. doi: 10.20961/ijai.v5i1.40845.

[5] D. Al, A. ; Endang, and W. Pamungkas, "Analisis Keamanan Database Aplikasi Web Dengan Sql Injection Menggunakan Penetration Tools," pp. 1–22, 2023.

[6] N. Christina Sari *et al.*, "Deteksi Kerentanan SQL Injection pada Website Menggunakan Vulnerability Assessment Info Artikel," *J. Data Insights*, vol. 2, no. 1, pp. 9–17, 2024, [Online]. Available: http://journalnew.unimus.ac.id/index.php/jodi

[7] A. Dos Santos, G. S. Pereira, R. A. Syuhada, and E. M. S. Sakti, "Uji Coba Keamanan Database Website Menggunakan Python Dan Sqlmap Melalui Command Prompt Pada Sistem Operasi Windows," *J. Ilm. Tek. Inform.*, vol. 25, no. 1, pp. 146–153, 2024, [Online]. Available: https://doi.org/10.37817/tekinfo.v25i1

[8] D. U. Khabibah, Y. Nurrohman, K. Dewandaru, S. J. D. H. Balian, and A. Setiawan, "Strategi Mitigasi SQL Injection dengan Implementasi SQLMap dan Web Application Firewall," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 12, 2024, doi: 10.47134/jtsi.v1i4.2656.

[9] A. Riyanti, B. M. Rahmanto, D. R. Hardianto, R. D. A. Yuristiawan, and A. Setiawan, "Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 9, 2024, doi: 10.47134/pjise.v1i4.2623.

[10] L. A. Nugraha, I. A. Kautsar, and A. S.

Fitrani, “SQL Injection: Analisis Efektivitas Uji Penetrasi dalam Aplikasi Web,” *Smatika J.*, vol. 14, no. 01, pp. 111–123, 2024, doi: 10.32664/smatika.v14i01.1224.

[11] J. Desmon, S. Hidayatulloh, and Y. Jumaryadi, “Systematic Literature Review: Serangan Deface Website Sebagai Bentuk Kejahatan Siber,” *Just IT J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 14, no. 2, pp. 80–149, 2024, [Online]. Available: https://jurnal.umj.ac.id/index.php/just-it/index

[12] Y. Natanael, R. Felicia, and E. M. S. Sakti, “Analisis Keamanan Informasi Bagi Pengguna Website Menggunakan Kalilinux Melalui Teknik SQL Injection,” *J. Ilm. Tek. Inform. ...*, vol. 25, no. 1, pp. 123–132, 2024, [Online]. Available: https://ojs.upi-yai.ac.id/index.php/TEKINFO/article/download/3903/2967