Jurnal Ilmiah
Teknologi Sistem
Informasi

Jitsi

Vol. 6 (2025) No. 1

https://jurnal-itsi.org/index.php/jitsi; E-ISSN: 2722-4600; ISSN: 2722-4619
DOI: 10.62527/jitsi.6.1.329

Analisis Keamanan Website Shih Ka Plastic Boxes Factory Terhadap Ancaman SQL Injection

Muhammad Muhsinin[#], Mukhammad Said Riza Zudi[#], Yekti Adi Prasetyo[#], Ahmad Maulana Arif[#], Susanto[#]

[#] *Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi , Universitas Semarang, Semarang, 50196,Indonesia*
E-mail: sininsinon[at]gmail.com , saidriza6[at]gmail.com, yektiadi5[at]gmail.com, arifpwd7[at]gmail.com, susanto[at]usm.ac.id

A B S T R A C T S

This study discusses security vulnerabilities in web applications, focusing on SQL injection attacks. With the increasing number of internet users and sensitive data being managed, system security on websites has become crucial. This research uses SQLmap to identify and explore potential attacks on the Shih ka Plastic Boxes Factory website. The findings reveal significant security gaps due to insufficient input validation. It was found that attackers could easily access sensitive data through the exploitation of these vulnerabilities. Additionally, recommendations for security improvements are suggested, including the implementation of strict input validation and the use of prepared statements to protect the database.

A B S T R A K

Penelitian ini membahas kerentanan keamanan pada aplikasi web, dengan fokus pada serangan SQL injection. Dengan meningkatnya jumlah pengguna internet dan data sensitif yang dikelola, keamanan sistem pada website menjadi sangat penting. Penelitian ini menggunakan SQLmap untuk mengidentifikasi dan mengeksplorasi potensi serangan pada website Shih ka Plastic Boxes Factory. Hasil penelitian menunjukkan adanya celah keamanan yang signifikan akibat kurangnya validasi input. Ditemukan bahwa penyerang dapat dengan mudah mengakses data sensitif melalui eksploitasi kerentanan tersebut. Selain itu, rekomendasi perbaikan keamanan disarankan, termasuk implementasi validasi input yang ketat dan penggunaan prepared statements untuk melindungi database.

Keywords / Kata Kunci — ***SQL; Situs Web; Sistem Keamanan***

Manuscript received Dec 18, 2024; revised Jan 11, 2025. accepted Mar 09, 2025 Date of publication Mar 31, 2025. International Journal, JITSI : Jurnal Ilmiah Teknologi Sistem Informasi licensed under a Creative Commons Attribution-Share Alike 4.0 International License

CORRESPONDING AUTHOR

Muhammad Muhsinin
Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi , Universitas Semarang, Semarang, 50196,Indonesia
Email: sininsinon[at]gmail.com

1. PENDAHULUAN

Website adalah sumber daya di internet yang menyediakan data dan informasi yang dapat diakses semua orang[1]. Perkembangan teknologi yang semakin pesat menjadikan data salah satu aset yang sangat penting[2], [3]. Selain itu, pertumbuhan internet dan semakin banyaknya pengguna internet turut meningkatkan jumplah pengguna juga meningkatkan resiko serangan. Semakin banyak data sensitif yang disimpan dan proses, semakin besar potensi ancaman [4]. Salah satu satu target utama bagi hacker dan cracker adalah aplikasi web, oleh karena

itu, keamanan sistem pada website sangat penting[5]. Hal ini bertujuan untuk memastikan sistem bebas dari celah atau kerentanan serta mencegah akses dari ancamanan siber dan pihak yang tidak bertanggung jawab[6].

SQL injection merupakan salah satu jeni serangan siber yang umum ditemukan pada website.Teknik serangan siber ini menyerang database yang dimana dapat mengambil dan mengubah data-data yang ada[7]. Structured Query Language (SQL) merupakan kerantanan ini muncul ketika penyerang dapat memanipulisasi query yang dikirim melalui aplikasi ke database back-end. SQL injection terjadi ketika penyerang menyisipkan query SQL atau perintah melalui input yang diterima oleh halaman web atau command prompt, akibat form input pengguna yang tidak disaring dengan benar terhadap karakter khusus, menjadikannya sebagai teknik favorit penyerang untuk menyerang website[8], [9].

Penelitian yang dilakukan oleh Ede Riyanti et al. pada tahun 2024 menunjukkan bahwa dengan memanfaatkan SQLmap di sistem operasi kali linux, penyedang dapat dengan mudah memperoleh data autentikasi penting, seperti nama pengguna dan kata sandi[10]. Oleh karena itu, Penelitian ini akan melakukan pengujian terhadap kerentanan aplikasi web menggunakan SQL untuk mengidentifikasi potensi serangan, seperti SQL injection, guna mengevaluasi sejauh mana keamanan data dapat terancam oleh eksploitasi tersebut

2. METODOLOGI PENELITIAN

1. Tahapan Penelitian

Penelitian ini melibatkan beberapa tahap penting, termasuk persiapan lingkungan pengujian dan penerapan teknik pengujian SQLmap. Penelitian dilakukan secara eksperimental di sistem operasi POP!_OS dengan menggunakan alat bantu SQLmap sebagait berikut :

A. Unduh dan konfigurasi sqlmap
   Langkah pertama dalam penelitian ini adalah mengunduh SQLmap dari repository resmi, kemudian melakukan ekstraksi dan konfigurasi melalui Terminal POP!_OS.
B. Indetifikasi target website
   Target website diidentifikasi dengan memeriksa adanya formulir input atau parameter URL yang dapat diuji[11]. Dalam studi ini, website Shih ka Plastic Boxes Factory dipilih sebagai target, menggunakan URL dengan parameter dinamis seperti products.php?id=1.
C. Teknik pengujian sqlmap sebagai berikut :
   1. Uji awal dilakukan dengan menyisipkan karakter khusus, seperti tanda kutip tunggal ('), ke dalam parameter URL. Apabila sistem memberikan respons berupa pesan kesalahan yang berkaitan dengan SQL, maka ada indikasi adanya potensi kerentanan.
   2. Pemanfaatan SQLmap untuk mengidentifikasi dan mengeksplorasi kerentanan.SQLmap dijalankan menggunakan perintah-perintah dasar, seperti:
      - sqlmap -u "http://example.com/page.php?id=1" --batch –dbs[12], Perintah ini memeriksa apakah parameter id pada URL tersebut rentan terhadap SQL Injection dan menampilkan daftar database jika ditemukan.
      - sqlmap -u "http://example.com/page.php?id=1" -D nama_database –tables, Perintah ini untuk Mengeksploitasi database yang sudah di tangkap dengan cara sebelumnya
      - sqlmap -u "http://example.com/page.php?id=1" -D nama_database -T nama_tabel –dump, Perintah ini untuk Mengeksploitasi data tabel yang sudah di tangkap dengan cara sebelumnya

2. Perlatan Penelitian

Penelitian ini memanfaatkan berbagai peralatan dan perangkat lunak untuk mendukung proses eksplorasi, analisis, dan pengujian. Peralatan yang digunakan meliputi:

1. Komputer atau Laptop
   sebagai perangkat utama untuk menjalankan pengujian dan analisis. Spesifikasi minimum meliputi prosesor yang memadai, memori RAM, dan koneksi internet yang stabil.
2. Sistem Operasi
   Sistem Operasi berbasis Linux, seperti Pop!_OS, digunakan untuk mendukung kompatibilitas dengan berbagai alat keamanan dan pengujian.
3. SQLmap
   Sebuah alat otomatisasi untuk mendeteksi dan mengeksploitasi kerentanan SQL Injection pada aplikasi web.
4. Browser Web
   Digunakan untuk mengakses target website dan memverifikasi hasil pengujian.
5. Editor Teks
   Editor teks seperti VSCode digunakan untuk mencatat hasil pengujian atau menyimpan script yang diperlukan.

6. Jaringan Internet
   Diperlukan koneksi yang stabil untuk mengakses target website dan mengunduh alat tambahan jika diperlukan.

Peralatan di atas memungkinkan proses penelitian dilakukan dengan efisien dan akurat

3. HASIL DAN PEMBAHASAN

1. Skema Hasil Alat Uji Ion Thruster

Penelitian ini mengungkap bahwa website Shih ka Plastic Boxes Factory memiliki kerentanan yang signifikan terhadap serangan SQL Injection. Kerentanan ini muncul akibat kurangnya validasi yang memadai pada input pengguna, sehingga memungkinkan manipulasi kueri SQL melalui parameter URL. Uji awal dengan menyisipkan karakter khusus, seperti tanda kutip tunggal ('), menghasilkan pesan kesalahan terkait SQL, yang menunjukkan adanya celah keamanan. Hal ini mengindikasikan bahwa sistem tidak mampu memfilter input dengan efektif, membuka peluang bagi eksploitasi lebih lanjut.

2. Ekplorasi Database dengan SQLmap

Eksplorasi lebih lanjut dilakukan dengan menggunakan SQLmap. Langkah-langkah awal yang diikuti adalah sebagai berikut:

A. Deteksi kerentanan

Kita akan menggunakan URL http://www.shihka.com.hk/ dan mengidentifikasi parameter URL yang mungkin rentan terhadap SQL Injection. Misalnya, jika URL mengandung parameter seperti:

http://www.shihka.com.hk/en/product.php?catid=3

Di mana `id=1` adalah parameter yang kita curigai dapat dieksploitasi.

B. Deteksi Database

Setelah mendapatkan daftar database, pilih salah satu untuk dieksploitasi lebih lanjut. Misalnya, jika SQLmap menunjukkan database dengan nama `my_database`, kita dapat melanjutkan untuk melihat tabel yang ada di dalamnya dengan perintah berikut:

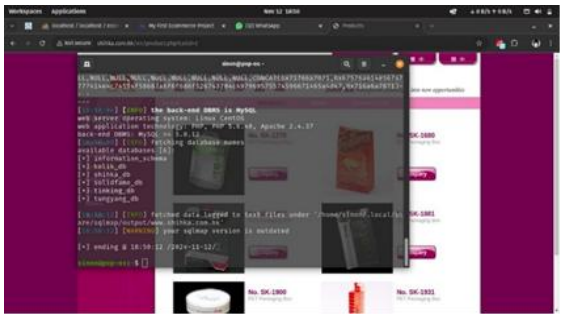
sqlmap -u "http://www.shihka.com.hk/en/product.php?catid=3" -D name_databse –tables, hasil ada di gambar 1.

C. Ekplorasi Struktur Tabel

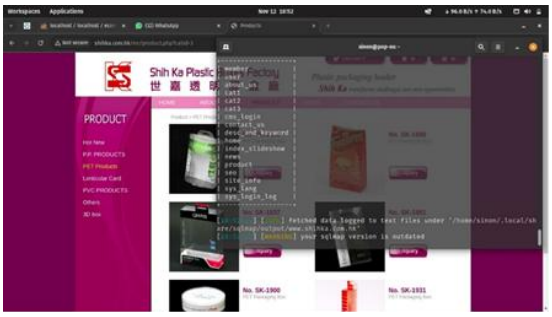
Pada tahap ini, eksplorasi lebih lanjut dilakukan untuk mendapatkan daftar tabel yang ada dalam database yang terdeteksi. Setelah mendapatkan daftar database, pilih salah satu untuk dieksploitasi lebih lanjut. Misalnya, jika SQLmap menunjukkan database dengan nama misal `my_database`, kita dapat melanjutkan untuk melihat tabel yang ada di dalamnya dengan perintah berikut:

sqlmap -u "http://www.shihka.com.hk/en/product.php?catid=3" -D name_databse –tables

Perintah ini berfungsi untuk memeriksa struktur database yang terkait dengan URL yang telah diuji sebelumnya, dan menampilkan daftar tabel yang ada di dalamnya. Hasil dari perintah ini berhasil mengungkap beberapa tabel penting, seperti users, atau product Tabel-tabel ini berisi berbagai informasi sensitif yang sangat relevan, seperti data pengguna, administrator, dan transaksi yang dilakukan di website. Informasi ini dapat dieksploitasi lebih lanjut oleh penyerang jika tidak dilakukan perlindungan yang memadai. Hasil ada pada di gambar 2.



GAMBAR 1. Deteksi Database



GAMBAR 2. Ekplorasi Tabel

D. Tabel

Setelah mengetahui tabel yang ada, Anda dapat memilih tabel tertentu untuk melihat data yang ada. Misalnya, jika tabel `users` ditemukan, Anda dapat mengambil data dari tabel tersebut dengan perintah:

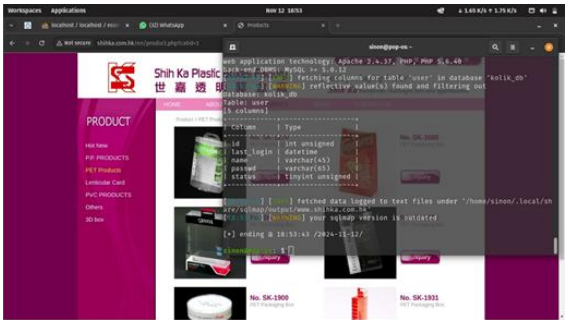
sqlmap -u "http://www.shihka.com.hk/en/product.php?catid=3" -D name_database -T nama_tabel –dump

Perintah ini memungkinkan SQLmap untuk mengekstrak seluruh data yang ada dalam tabel *admin*, yang mencakup informasi sensitif yang bisa dimanfaatkan oleh penyerang jika tidak ada perlindungan yang tepat. Hasil ada di gambar 3

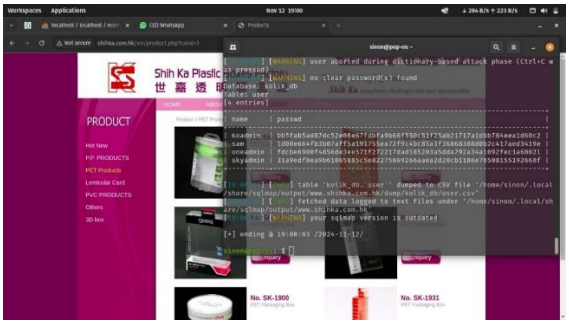
E. Mengambil data columns

Setelah mengetahui columns yang ada, Anda dapat memilih columns tertentu untuk melihat data yang ada. Misalnya, jika columns `name` ditemukan, Anda dapat mengambil data dari columns tersebut dengan perintah:

sqlmap -u "http://www.shihka.com.hk/en/product.php?catid=3" -D name_database -T nama_tabel -C nama_columns –dump dan hasil ada pada di gambar 4



GAMBAR 3. Tabel Database



GAMBAR 4. Data Columns

F. Analisis Password

Beberapa password yang berhasil diekstraksi dari database disimpan dalam bentuk hash menggunakan algoritma seperti MD5 atau SHA-1. Meskipun algoritma ini dimaksudkan untuk mengamankan password, keduanya memiliki celah yang bisa dieksploitasi oleh pihak yang tidak bertanggung jawab. Penyerang dapat menggunakan alat seperti hashcat atau John the Ripper untuk mencoba mendekripsi hash tersebut, yang meningkatkan kemungkinan terjadinya eksploitasi lebih lanjut. Hal ini membuka peluang bagi penyerang untuk mendapatkan akses ke akun pengguna atau administrator secara tidak sah.

G. Analisis Respon Sistem Terhadap Serangan

Respon dari sistem menunjukkan bahwa website website Shih ka Plastic Boxes Factory memiliki perlindungan yang sangat terbatas terhadap ancaman SQL Injection. Beberapa aspek yang menonjol terkait kurangnya perlindungan antara lain :

- Tidak adanya validasi input pada server, yang memungkinkan data berbahaya masuk ke dalam sistem tanpa pengecekan.
- Tidak diterapkannya prepared statements atau parameterized queries, yang seharusnya menjadi teknik dasar untuk melindungi database dari potensi manipulasi oleh input pengguna.
- Karakter khusus pada input SQL tidak di-escape dengan benar, yang memungkinkan karakter seperti tanda kutip tunggal (‘) diterima tanpa pengolahan yang tepat.

Kondisi ini memungkinkan alat seperti SQLmap untuk melakukan eksploitasi tanpa hambatan, termasuk mengakses dan memanipulasi data sensitif di dalam sistem

H. Implikasi Keamanan

Celah keamanan ini berpotensi menimbulkan berbagai dampak besar bagi website website Shih ka Plastic Boxes Factory dan penggunanya, seperti:

1. Akses Data Sensitif
   Penyerang dapat mengakses data pribadi pelanggan, termasuk nama, alamat, nomor telepon, dan informasi pembayaran. Data tersebut dapat disalahgunakan untuk kejahatan seperti penipuan atau pencurian identitas.
2. Pengambilalihan Sistem
   Dengan memperoleh informasi login administrator, penyerang dapat mendapatkan kendali penuh atas sistem, mengubah konten situs, menghapus data penting, atau melakukan serangan terhadap sistem lainnya yang terhubung.
3. Kerusakan Reputasi
   Jika celah ini diketahui publik, hal itu dapat merusak reputasi website Shih ka Plastic Boxes Factory dan mengurangi kepercayaan pelanggan, yang berimbas pada penurunan citra perusahaan dan potensi pendapatan.
4. Pelanggaran Hukum
   Melanggar perlindungan data pelanggan dapat berakibat pada sanksi hukum, terutama di wilayah yang memiliki regulasi ketat seperti GDPR (General Data Protection Regulation), yang dapat menyebabkan denda besar dan kerusakan reputasi lebih lanjut.

I. Rekomendasi Perbaikan Keamanan

Berdasarkan hasil penelitian, beberapa langkah perbaikan yang disarankan untuk meningkatkan keamanan website website Shih ka Plastic Boxes Factory adalah sebagai berikut:

1. Implementasi Validasi Input yang Ketat
   Sangat penting untuk menerapkan proses sanitasi yang tepat pada semua input pengguna, guna memastikan bahwa data yang diterima sistem bebas dari karakter berbahaya yang dapat dimanfaatkan oleh penyerang.
2. Penggunaan Prepared Statements dan Parameterized Queries
   Teknik ini harus diterapkan pada semua interaksi dengan database untuk melindungi sistem dari manipulasi kueri SQL yang berbahaya. Dengan menggunakan prepared statements, input pengguna akan diproses dengan cara yang aman tanpa mempengaruhi struktur kueri SQL.
3. Penyimpanan Data Sensitif dengan Algoritma Hash yang Lebih Aman
   Pastikan bahwa semua data sensitif, seperti password, disimpan menggunakan algoritma hash yang lebih aman, seperti bcrypt, yang jauh lebih kuat dibandingkan algoritma yang lebih lama seperti MD5.
4. Pemasangan Web Application Firewall (WAF)
   Penggunaan WAF dapat membantu mendeteksi dan mencegah serangan berbasis web, termasuk SQL Injection, sebelum dapat memengaruhi sistem. WAF memberikan lapisan perlindungan tambahan yang efektif terhadap upaya eksploitasi yang tidak sah.
5. Audit Keamanan Secara Rutin
   Disarankan untuk melakukan audit keamanan secara berkala, termasuk pengujian penetrasi dan pemeriksaan mendalam pada sistem untuk mengidentifikasi dan menangani celah keamanan yang ada. Langkah ini memastikan bahwa langkah-langkah pencegahan tetap efektif dan sistem terus terlindungi dari potensi ancaman.

Dengan menerapkan langkah-langkah di atas, website website Shih ka Plastic Boxes Factory dapat meningkatkan perlindungan terhadap ancaman siber dan memperkuat kepercayaan pengguna terhadap layanan yang mereka tawarkan.

J. Hasil dari pembasan

Berikut ini adalah hasil dari proses pengujian yang telah dilakukan untuk mengidentifikasi dan mengevaluasi kerentanan keamanan pada website Shih Ka Plastic Boxes Factory yang ada di tabel 1. Pengujian dilakukan secara sistematis menggunakan teknik SQL Injection dengan bantuan alat SQLmap

TABEL 1. Hasil

No	Tahapan Penyerangan	Metode/Alat yang Digunakan	Hasil dan Temuan
1	Identifikasi Target	SQLmap, Browser	Website memiliki parameter yang rentan
2	Uji Injeksi Awal	SQLmap, karakter '	Muncul pesan error SQL, indikasi celah
3	Deteksi Database	sqlmap -u ... –dbs	Database ditemukan: my_database
4	Eksplorasi Struktur Database	sqlmap -u ... -D ... –tables	Tabel ditemukan: users, products
5	Dump Data dari Tabel	sqlmap -u ... -D ... -T ... –dump	Data sensitif seperti username, email, password ditemukan
6	Analisis Password	Hashcat, John the Ripper	Beberapa password dapat dipecahkan
7	Evaluasi Sistem	Observasi Respon Server	Tidak ada validasi input, tidak menggunakan prepared statements
8	Implikasi Keamanan	Analisis Dampak	Risiko pencurian data, akses ilegal, penurunan reputasi
9	Rekomendasi Perbaikan	Implementasi Keamanan	Validasi input, prepared statements, hashing yang lebih kuat, penggunaan WAF

Hasil pengujian menunjukkan bahwa website Shih Ka Plastic Boxes Factory memiliki celah keamanan akibat kurangnya validasi input dan tidak digunakannya prepared statements. SQLmap berhasil mengeksploitasi database, menampilkan struktur tabel, serta mengambil data sensitif seperti username, email, dan password dalam bentuk hash.

Risiko dari celah ini meliputi akses ilegal, pencurian data, dan kerusakan reputasi website. Untuk mengatasinya, diperlukan validasi input yang lebih ketat, penggunaan prepared statements, hashing password dengan bcrypt, serta pemasangan Web Application Firewall (WAF) agar sistem lebih aman dari serangan serupa

4. KESIMPULAN

Penelitian ini menyoroti pentingnya keamanan sistem pada aplikasi berbasis web, terutama terkait dengan ancaman SQL injection. Dengan meningkatnya jumlah pengguna internet dan data sensitif yang disimpan, risiko serangan terhadap web semakin tinggi. Penelitian yang dilakukan menunjukkan bahwa website Shih ka Plastic Boxes Factory memiliki kerentanan signifikan terhadap serangan SQL injection, yang diakibatkan oleh kurangnya validasi input pengguna.

Melalui penggunaan alat SQLmap, penelitian berhasil mengidentifikasi dan mengeksplorasi kerentanan ini, serta menunjukkan bahwa sistem tidak mampu memfilter input dengan efektif. Hal ini membuka peluang bagi penyerang untuk mengeksploitasi data sensitif, yang dapat berujung pada akses data pribadi, pengambilalihan sistem, kerusakan reputasi, dan pelanggaran hukum

REFERENSI

[1] N. Huda and M. Megawaty, "Analisis Kinerja Website Dinas Komunikasi dan Informatika Menggunakan Metode Pieces," Jurnal Sisfokom (Sistem Informasi dan Komputer), vol. 10, no. 2, pp. 155–161, Jul. 2021, doi: 10.32736/sisfokom.v10i2.1018.

[2] C. Adi Putra, R. Pratama, T. Sutabri, J. A. Jenderal Yani No, and S. Selatan, "ANALISIS MANFAAT MACHINE LEARNING PADA NEXT-GENERATION FIREWALL SOPHOS XG 330 DALAM MENGATASI SERANGAN SQL INJECTION", doi: 10.36595/misi.v5i2.

[3] A. W. Wardhana and H. B. Seta, "Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ," vol. 3, p. 2021.

[4] Y. Natanael, R. Felicia, E. Malays, and S. Sakti, "Analisis Keamanan Informasi Bagi Pengguna Website Menggunakan Kalilinux Melalui Teknik SQL Injection", doi: 10.37817/tekinfo.v25i1.

[5] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," Jurnal Informasi dan Teknologi, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.

[6] A. W. Kuncoro, J. Informatika, F. Rahma, and M. E. Jurusan Informatika, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review." [Online]. Available: https://www.sciencedirect.com

[7] R. Yulia Andarini, P. Hendradi, and S. Nugroho, "MENINGKATKAN KEAMANAN TERHADAP SQL INJECTION STUDI KASUS SISTEM KEPEGAWAIAN BNN," Indonesian Journal of Business Intelligence (IJUBI), vol. 6, no. 1, Jun. 2023, doi: 10.21927/ijubi.v6i1.3161.

[8] M. F. Al Azhar and R. Harwahyu, "Implementasi Dashboard Monitoring untuk Pengujian Kerentanan SQL Injection pada Environment GitLab."

[9] R. Hermawan, "STRING (Satuan Tulisan Riset dan Inovasi Teknologi) TEKNIK UJI PENETRASI WEB SERVER MENGGUNAKAN SQL INJECTION DENGAN SQLMAP DI KALILINUX."

[10] 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," Journal of Internet and Software Engineering, vol. 1, no. 4, p. 9, Jun. 2024, doi: 10.47134/pjise.v1i4.2623.

[11] N. Christina Sari et al., "Deteksi Kerentanan SQL Injection pada Website Menggunakan Vulnerability Assessment Info Artikel," vol. 2, no. 1, pp. 9–17, 2024, doi: 10.26714/jodi.

[12] "346325-penetration-testing-database-menggunakan-21bc5d72".