PISCES
Progressive Information, Security, Computer, and Embedded System

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

Deteksi Serangan SQL Injection pada Website dengan Menggunakan Metode Reguler Expression

[1]Reni Supartini
[1]Pendidikan Teknik Informatika dan Komputer, Universitas Negeri Makassar, Jl. A.P. Pettarani, Kota Makassar, Sulawesi Selatan
Email: reniisupartinii@gmail.com[1]

Received : 20 Juli 2023
Accepted : 29 Agustus 2023
Published : 25 September 2023

ABSTRAK

Dengan kemajuan teknologi yang terus berkembang, keamanan informasi data di dalam sebuah situs web menjadi sangat rentan terhadap ancaman di dunia internet, seperti serangan terhadap kerentanan keamanan pada lapisan database yang dikenal sebagai SQL Injection. SQL Injection merupakan suatu metode yang memanfaatkan penyisipan perintah SQL melalui input aplikasi untuk mendapatkan akses ke dalam database. Serangan ini berpotensi untuk mengakses informasi sensitif seperti username, password, dan data lainnya yang tersimpan dalam database. Oleh karena itu, SQL Injection merupakan salah satu metode serangan yang populer dan sering dimanfaatkan karena kemudahan penggunaannya. Jika basis data situs web dapat diakses, seorang peretas dapat dengan mudah mencuri berbagai informasi rahasia, bahkan dapat memanipulasi atau merusak data pada situs tersebut. Artikel ini bertujuan untuk menguji efektivitas serangan SQL Injection dengan menggunakan metode regular expression. Hasil penelitian mencakup akurasi waktu pencarian database dan ketepatan informasi yang ditemukan dari database.

Kata Kunci: Injeksi SQL, Ekspresi Reguler, Deteksi Intrusi

ABSTRACT

With the current advancement in technology, the security of information data within a website is highly vulnerable to cybercrimes in the internet world, such as attacks on security vulnerabilities in the database layer commonly known as SQL Injection. SQL Injection is a method used to inject SQL commands as input through an application to gain access to the database. This type of attack can reveal sensitive information such as usernames, passwords, and other data stored in the database. Therefore, SQL Injection is a popular and frequently employed method for exploiting security loopholes in systems due to its ease of use. If the website's database is accessible, a hacker can easily steal various confidential data and even manipulate or damage the data on the website. This article aims to test the effectiveness of SQL Injection attacks using the regular expression method. The research results include the accuracy of database search times and the precision of information retrieved from the database.

Keywords: SQL Injection, Reguler Expression, Intrusion Detection

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

1. PENDAHULUAN

Di era modernisasi, perkembangan teknologi informasi dan komunikasi terus berkembang seiring dengan perubahan zaman. Teknologi ini digunakan untuk mengelola, memproses, mendapatkan, menyusun, dan menyimpan data dengan berbagai cara guna menghasilkan informasi berkualitas dan sesuai dengan fakta (Dan, 2023). Meskipun teknologi informasi dan komunikasi memberikan kemudahan akses informasi bagi masyarakat, pertumbuhan ini juga membawa dampak negatif terutama dalam hal keamanan informasi.

Keamanan informasi merupakan upaya perlindungan terhadap segala jenis informasi dari penyalahgunaan oleh pihak yang tidak bertanggung jawab (Dalimunthe & Sahren, 2020). Dalam menghadapi perkembangan teknologi, keamanan informasi menjadi tantangan bagi masyarakat dan pengembang website. Tidak ada jaminan pasti terkait dengan keamanan sistem digital, dan seringkali terdapat cara atau celah untuk melakukan serangan pada sistem website, yang dapat menimbulkan kerugian bagi pemiliknya. Ancaman keamanan dapat melibatkan aspek integritas, kerahasiaan, dan ketersediaan data, dan oleh karena itu, penting untuk melindungi sistem berbasis digital dari ketiga aspek tersebut.

Sebuah website, sebagai layanan informasi, dibangun untuk memenuhi kebutuhan banyak pengguna. Ada empat elemen dasar dalam sebuah situs web, yaitu browser, server, URL, dan halaman (Imam et al., 2022). Sifatnya dapat bersifat statis jika informasinya tetap tidak berubah, atau bersifat dinamis jika informasi berubah-ubah dan interaktif dua arah antara pemilik dan pengguna. Server web berisi halaman web yang mengandung informasi dan dokumen yang ingin didistribusikan oleh pengguna.

Salah satu ancaman umum terhadap website adalah SQL Injection, yang merupakan ancaman utama dalam daftar kerentanan website (Friadi & Septian, 2021). Serangan ini memanfaatkan celah keamanan pada query dengan menyisipkan pernyataan SQL. Pemilik website seringkali tidak menyadari celah ini, sehingga menganggap bahwa keamanan website mereka sempurna tanpa menyadari adanya celah ancaman keamanan dari "pintu belakang" website tersebut. SQL Injection dapat mencuri data administrator dan bahkan mengambil alih kepemilikan website karena input pengguna tidak divalidasi, menciptakan celah keamanan. Serangan SQL Injection sangat berbahaya karena penyerang yang berhasil masuk ke dalam database dapat memanipulasi data yang ada di dalamnya, menyebabkan kerugian bagi pemilik website yang terkena serangan.

2. PENELITIAN TERKAIT

SQL Injection merupakan jenis serangan yang menargetkan aplikasi berbasis web yang terhubung ke database, di mana kode berbahaya dapat dimasukkan, diproses, dan dijalankan. Kerentanan ini muncul ketika aplikasi web tidak melakukan validasi input dengan baik. Aplikasi web yang dirancang secara kurang baik dapat diserang dengan menyisipkan kode berbahaya untuk mendapatkan akses ke database. Menurut Jemal et al. (2020), Serangan Structured Query Language Injection (SQLI) dianggap sebagai serangan paling berbahaya dalam kategori injeksi karena mengancam layanan keamanan utama seperti kerahasiaan, otentikasi, otorisasi, dan integritas.

Teknik Ekspresi Regular digunakan untuk mendeteksi pola perilaku pengunjung website yang dilakukan oleh klien. Ekspresi Regular (Regexp, Regex, RE) adalah bahasa mini untuk menggambarkan string atau teks. Ini dapat digunakan untuk mencocokkan sebuah string dengan pola tertentu. Dalam konteks ini, peneliti akan menganalisis website untuk mendeteksi potensi serangan, memungkinkan administrator website untuk menerapkan langkah-langkah pencegahan dan mengatasi masalah pada website yang dikelolanya (Yogi et al., 2019).

Aplikasi web atau website banyak digunakan untuk menyediakan fungsionalitas yang memungkinkan perusahaan membangun dan memelihara hubungan dengan pelanggannya. Informasi yang disimpan oleh aplikasi web seringkali bersifat rahasia, dan jika diperoleh oleh penyerang jahat, dapat mengakibatkan kerugian besar bagi konsumen dan perusahaan (Mutedi & Tjahjono, 2022). Menurut studi Riadi et al. (2018), aplikasi web sangat rentan terhadap berbagai serangan, termasuk SQL Injection, yang dapat memberikan akses penyerang ke database jika sebuah website memiliki kerentanan.

Berdasarkan temuan Mukhtar & Azer (2020), pengujian website terhadap SQL Injection telah terbukti efisien dalam memblokir serangan berdasarkan iterasi SQLMAP. Perlu dicatat bahwa teknik SQLI terus berkembang. Untuk mencapai perlindungan yang diperlukan, penting untuk secara rutin memperbarui aturan SQLMAP guna memblokir teknik serangan injeksi SQL baru yang muncul setiap hari.

Kebutuhan akan sistem untuk memahami dan mendeteksi pola perilaku pengunjung terhadap aplikasi web sangat penting untuk pengembangan halaman website yang lebih baik di masa depan. Oleh karena itu, artikel ini bertujuan untuk membangun sistem yang dapat mengidentifikasi pola perilaku pengunjung pada aplikasi web dengan menggunakan teknik Ekspresi Regular. Tujuan penelitian ini adalah untuk mengkaji masalah deteksi dan pencegahan serangan SQL Injection.

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini mencakup langkah-langkah sistematis untuk mengidentifikasi, menganalisis, dan mengatasi potensi serangan SQL Injection pada aplikasi web. Penelitian ini memanfaatkan pendekatan kualitatif dengan fokus pada analisis pola perilaku pengunjung dan penerapan teknik Regular Expression.

Pertama-tama, penelitian ini melakukan analisis mendalam terhadap aplikasi web yang menjadi objek penelitian. Langkah awal melibatkan pemahaman mendalam terhadap struktur dan fungsionalitas website, termasuk identifikasi potensi celah keamanan yang mungkin dapat dimanfaatkan untuk melakukan serangan SQL Injection. Pada tahap ini, peneliti juga mengumpulkan informasi terkait dengan kebijakan keamanan yang telah diterapkan oleh pemilik atau pengelola website.

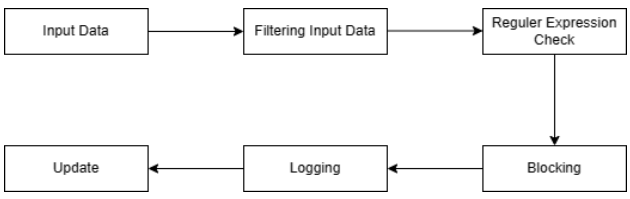
Setelah identifikasi potensi celah keamanan, langkah selanjutnya adalah pengembangan sistem deteksi menggunakan teknik Regular Expression. Penelitian ini merinci pola perilaku pengunjung yang mencurigakan, yang dapat menjadi indikator adanya serangan SQL Injection. Teknik Regular Expression digunakan untuk membuat pola yang sesuai dengan karakteristik serangan tersebut, sehingga dapat secara otomatis mendeteksi potensi ancaman pada aplikasi web.

Setelah implementasi sistem deteksi, penelitian ini melibatkan pengujian dan evaluasi kinerja sistem yang telah dikembangkan. Pengujian dilakukan dengan menghadapi berbagai skenario serangan yang umum terjadi, dan kemudian mengevaluasi sejauh mana sistem dapat mendeteksi serangan SQL Injection dengan akurasi tinggi. Hasil evaluasi tersebut menjadi dasar untuk menentukan efektivitas sistem deteksi yang diusulkan.

Terakhir, penelitian ini mencakup pengembangan rekomendasi dan pedoman pencegahan serangan SQL Injection bagi administrator website. Berdasarkan temuan dan analisis, rekomendasi ini bertujuan untuk membantu pemilik atau pengelola website dalam meningkatkan keamanan aplikasi web mereka, mengurangi risiko terjadinya serangan SQL Injection, dan mengimplementasikan langkah-langkah pencegahan yang tepat. Seluruh metodologi penelitian ini dirancang untuk memberikan kontribusi positif dalam meningkatkan keamanan aplikasi web melalui pendekatan deteksi dini dan tindakan pencegahan yang efektif.

4. HASIL DAN PEMBAHASAN

Untuk mendeteksi serangan SQL Injection pada Website ini, dapat menggunakan arsitektur sistem yang terdiri dari beberapa komponen berikut:



Gambar 1. Arsitektur Sistem

PISCES
Progressive Information, Security, Computer, and Embedded System

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

Dari gambar 1 diatas dapat dijelaskan bahwa input Data dimana data yang diambil dari form input pada website oleh pengguna. Selanjutnya, Filtering Input Data dimana data yang diinputkan oleh pengguna akan dilakukan filtering untuk memastikan data yang masuk merupakan data yang diizinkan dan tidak mengandung karakter khusus yang dapat menyebabkan serangan SQL injection.

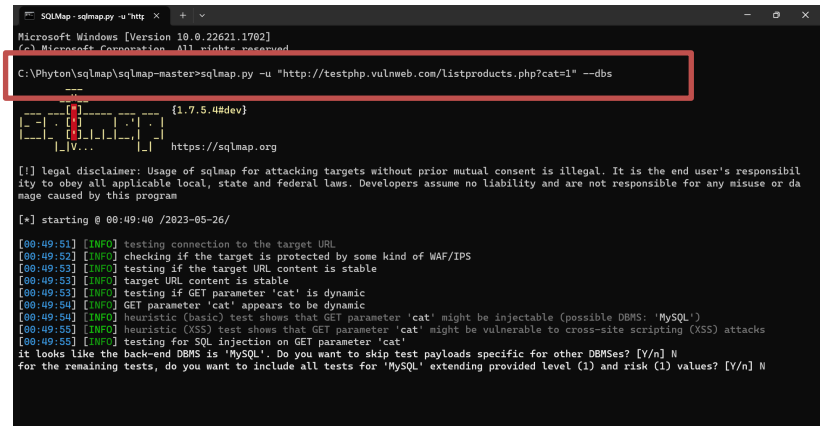
Reguler Expression Check dimana data yang telah difilter akan diperiksa menggunakan *regular expression* untuk mendeteksi apakah terdapat karakter khusus yang dapat menyebabkan serangan *SQL injection. Regular expression* adalah sebuah pola atau aturan yang digunakan untuk mencari suatu karakter atau susunan karakter tertentu pada suatu string. (Purbawa et al., 2018)

Blocking or Alerting Jika ditemukan karakter khusus yang mencurigakan, maka akan dilakukan tindakan blocking atau alerting. *Blocking* adalah menghentikan pengguna dari melakukan akses pada *website* dan *alerting* adalah memberi notifikasi pada pengelola website atau pengguna tentang adanya percobaan serangan *SQL injection.* (Tanang Anugrah et al., 2022)

Logging yaitu seluruh aktivitas dari sistem deteksi akan dicatat dan direkam pada file log untuk keperluan analisis dan investigasi lebih lanjut. Dan update sistem deteksi harus selalu diperbarui secara berkala untuk memperbaiki kelemahan dan mendeteksi serangan baru yang muncul. Hal ini dapat dilakukan dengan melakukan penelitian dan mengikuti perkembangan terbaru tentang serangan *SQL injection.*

Adapun sistem keamanan dan petunjuk pelaporan untuk keamanan atau gangguan dari serangan terhadap Web Server akan dilakukan, dengan menggunakan Instrusi Sistem Deteksi dan *SQLMAP*. Serangan yang akan terdeteksi dan diblokir adalah Serangan Injeksi *SQL*. Dapat dilihat pada Gambar 3, serangan akan dilakukan pada sebuah server tanpa keamanan. Keamanan *SQL* Serangan injeksi yang akan menggunakan alat *SQLMap* yang dijalankan melalui baris perintah:

#python sqlmap.py –u “http://testphp.vulnweb.com/listproducts.php?cat=1” –dbs

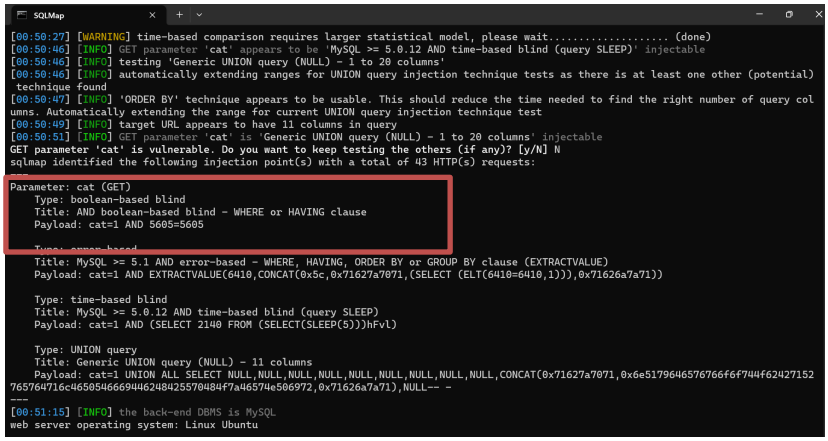


Gambar 2. Tampilan *SQLMAP*

PISCES
Progressive Information, Security, Computer, and Embedded System

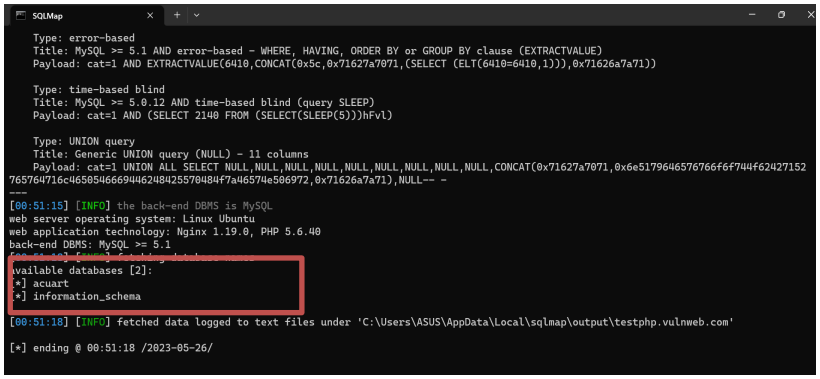
E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023



Gambar 3. Tampilan Output Parameter

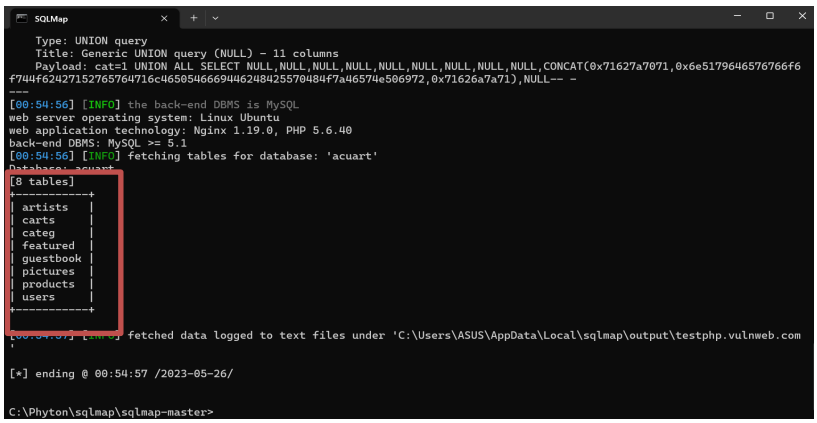
Dari gambar 3 diatas dapat diketahui bahwa parameter yang digunakan yaitu Get dengan type Boolean. Adapun output berikut yang menunjukkan bahwa ada dua database yang tersedia.



Gambar 4. Tampilan Database

Selanjutnya, untuk mencoba dan mengakses salah satu database, dengan menggunakan -D untuk menentukan nama database yang ingin diakses, dan setelah memiliki akses ke database, selanjutnya kita dapat mengakses table dengan menggunakan kueri –-tables.

#phyton sqlmap.py -u “http://testphp.vulnweb.com/listproducts.php?cat=1” -D acuart –tables



Gambar 5. Tampilan Tables

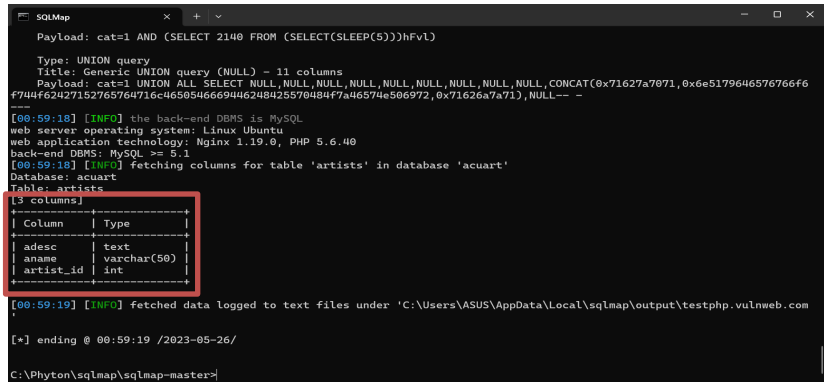
E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES
Progressive Information, Security, Computer, and Embedded System

PISCES Volume 01 Nomor 02 September 2023

Dari gambar 5 diatas dapat diketahui bahwa dalam database acuart terdiri dari 8 tables yang digunakan. Selanjutnya, untuk melihat columns yang terdapat pada tables artists.

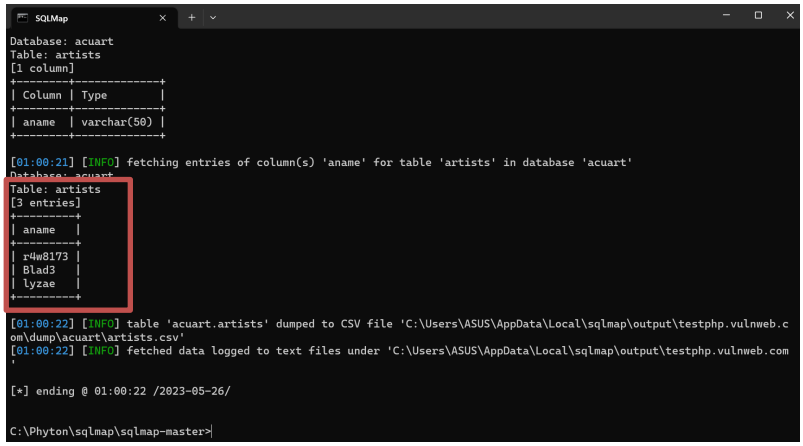
#phyton sqlmap.py –u “http://testphp.vulnweb.com/listproducts.php?cat=1”-D acuart -T artists –colums



Gambar 6. Tampilan Colums

Selanjutnya, memasukkan perintah --dump pada SQLMap digunakan untuk mengekstrak dan menampilkan data yang berhasil diambil dari basis data yang rentan terhadap serangan SQL injection.

#phyton sqlmap.py -u “http://testphp.vulnweb.com/listproducts.php?cat=1"-D acuart -T artis -C aname –dump



Gambar 7. Tampilan Akhir

Berdasarkan uji coba “http://testphp.vulnweb.com/listproducts.php?cat=1" bahwa *URL* ini rentan terhadap serangan *SQL Injection* dikarenakan pengembang situs tersebut tidak benar-benar mengamankan parameter id. Pada *URL* tersebut hanya menambahkan satu kutipan pada parameter id. Jika *URL* ini melempar kesalahan atau bereaksi dengan cara yang tidak normal maka jelas bahwa database telah mendapat kutipan tunggal yang tak tertuga sehingga aplikasi tidak mampu mengamankannya dengan benar. Jadi, dalam hal ini parameter input “id” ini rentan terhadap *SQL Injection.*

5. KESIMPULAN DAN SARAN

Dari analisa yang telah dilaksanakan dapat disimpulkan bahwa salah satu cara pencegahan serangan injection adalah dengan memfilter kata yang masuk dan karakter yang masuk karena selalu ada celah untuk menyerang selama ada inputan–inputan user.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

Dengan *reguler expression* kita dapat membuat script untuk memfilter dan mengamankan form inputan yang ada pada user. Metode *reguler expression* dapat digunakan sebagai salah satu alat dalam deteksi serangan *SQL injection.* Metode ini memungkinkan pencarian dan pencocokan pola dalam teks, yang dapat membantu mengidentifikasi karakter berbahaya, kata kunci *SQL*, tanda kutip yang tidak seimbang, dan karakter khusus yang terkait dengan serangan *SQL injection*.

Namun, penting untuk diingat bahwa penggunaan metode reguler ekspresi saja tidak cukup untuk memberikan perlindungan lengkap terhadap serangan *SQL injection.* Serangan *SQL injection* yang lebih canggih dapat menggunakan teknik penghindaran yang rumit, seperti enkripsi atau pengabungan, yang tidak dapat terdeteksi dengan metode reguler ekspresi sederhana.

Oleh karena itu, penggunaan metode reguler ekspresi dalam deteksi serangan *SQL injection* sebaiknya dikombinasikan dengan teknik dan strategi keamanan lainnya, seperti penggunaan *prepared statements* atau *parameterized queries,* validasi input, kontrol akses yang tepat, serta perlindungan terhadap serangan *SQL Injection.* Deteksi serangan *SQL injection* adalah bagian penting dari praktik keamanan aplikasi web. Dalam upaya melindungi aplikasi Anda dari serangan ini, penting untuk mengadopsi pendekatan yang holistik dan menggunakan berbagai metode pengamanan yang sesuai dengan tingkat kompleksitas serangan yang mungkin terjadi.

REFERENSI

Dalimunthe, R. A., & Sahren, S. (2020). Intrusion Detection System and Modsecurity for Handling Sql Injection Attacks. … Social, Sciences and Information …, 4509, 187–194. https://jurnal.stmikroyal.ac.id/index.php/ICoSSIT/article/view/711

Dan, J. I. (2023). PENGUKURAN EFEKTIVITAS SQL INJECTION PADA WEBSITE DENGAN MENGGUNAKAN TOOLS JSQL , HAVIJ , dan THE MOLE. 3(1), 35–42.

Friadi, J., & Septian, S. (2021). ZONA TEKNIK: JURNAL ILMIAH Aplikasi Machine Learning Untuk Deteksi Serangan Code Injection. x(x), 443–451. http://dx.doi.org/10.37776/zt.vxix.xxxOpenAccess:http://ejurnal.univbatam.ac.id/index.php/Teknik

Imam, T., Pratama, M., Danni, M., Songida, F., Gunawan, I., Teknik, J., Sekolah, E., Ronggolawe, T. T., Informatika, J., Tinggi, S., & Ronggolawe, T. (2022). Analisis Serangan dan Keamanan pada SQL Injection: Sebuah Review Sistematik. 2, 27–32.

Purbawa, D. P., Ulhaq, A. J., Ikhsan, G., & Shiddiqi, A. M. (2018). An enhanced sql injection detection using ensemble method. 21–29.

Tanang Anugrah, F., Ikhwan, S., & Gusti A.G, J. (2022). Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection. Techné : Jurnal Ilmiah Elektroteknika, 21(2), 199–210. https://doi.org/10.31358/techne.v21i2.320

Yogi, Ruslianto, I., & Bahri, S. (2019). Analisa Log Web Server Untuk Mengetahui Pola Perilaku Pengunjung Website Menggunakan Teknik Regular Expressions. Coding: Jurnal Komputer Dan Aplikasi, 07(01), 120–130. https://httpd.apache.org/docs/2.4/logs.HTM