**Jurnal Informatika Universitas Pamulang** **ISSN: 2541-1004**
**Penerbit: Program Studi Teknik Informatika Universitas Pamulang** **e-ISSN: 2622-4615**
**Vol. 7, No. 1, Maret 2022 (151-156)** **10.32493/informatika.v7i1.17590**

# Systematic Literature Review: Preventing SQL Injection Attacks Using Tools OWASP CSR Web Application Firewall

**Ahmad Mutedi[1], Budi Tjahjono[2]**

FASILKOM, Universitas Esa Unggul, Jakarta, Indonesia 11510
e-mail: [1]mutedy00@student.esaunggul.ac.id, [2]budi.tjahjono@esaunggul.ac.id*

Submitted Date: January 19th, 2022 Reviewed Date: February 01st, 2022
Revised Date: February 02nd, 2022 Accepted Date: March 31st, 2022

**Abstract**

SQL Injection Attacks are a common threat for web-based applications that use insecure input validation to target database attacks. This becomes a very serious problem in web-based applications because successful execution causes loss of integrity and confidentiality and this makes it a very sensitive software security issue. This study presents a Systematic Literature Review (SLR) using PICOC Method on Preventing SQL Injection Attacks Using OWASP Tools. This study provides an overview of SQL Injection Attacks, detection, and prevention techniques. In the end, an evaluation of the effectiveness of detection and prevention using the OWASP CSR Web Application firewall was carried out. It should be noted that the OWASP Tools can also detect and prevent SQL Injection Attacks.

Keywords: SQL Injection; Prevent; OWASP CSR; Systematic Literature Review; WAF

**Abstrak**

SQL Injection Attacks adalah ancaman umum untuk aplikasi berbasis web yang menggunakan validasi input yang kurang aman untuk dijadikan target serangan pada database. Ini menjadi masalah yang sangat serius dalam aplikasi berbasis web karena eksekusi yang berhasil menyebabkan hilangnya integritas dan kerahasiaan dan ini menjadikannya masalah keamanan perangkat lunak yang sangat sensitif. Studi ini menyajikan Review Literatur Sistematis (SLR) menggunakan Metode PICOC tentang Preventing SQL Injection Attacks Using Tools OWASP. Penelitian ini memberikan tinjauan tentang SQL Injection Attacks, teknik deteksi dan pencegahan. Pada akhirnya dilakukan evaluasi Kembali ke efektifan Deteksi dan pencegahan menggunakan OWASP CSR Web Application firewall. Harus dicatat bahwa Tools OWASP juga dapat mendeteksi dan mencegah SQL Injection Attacks.

Kata Kunci: SQL Injection; Prevent; OWASP CSR; Systematic Literature Review; WAF

## 1. Introduction

SQL Injection Attack adalah sebuah jenis serangan yang targetnya adalah aplikasi berbasis web yang terhubung ke database tempat dimana kode berbahaya akan dimasukkan, diproses, dan dijalankan. Kerentanan ini terjadi ketika aplikasi web tidak melakukan validasi input yang tepat. Aplikasi web yang dirancang dengan buruk dapat diserang dengan memasukkan kode berbahaya untuk mendapatkan akses ke dalam database.

Ada banyak prosedur keamanan di sisi server tetapi tidak membantu dalam skala besar dikarenakan kerumitan dalam penerapan, dan di sisi klien, menginstal aplikasi keamanan memperburuk kondisi klien.

Menurut (Jemal et al., 2020) Serangan Structured Query Language Injection (SQLI) dianggap sebagai serangan paling berbahaya dari kategori injeksi karena membahayakan layanan keamanan utama: kerahasiaan, otentikasi, otorisasi, dan integritas.

Berdasarkan studi (Robinson et al., 2018) 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, hal ini dapat mengakibatkan kerugian besar bagi konsumen dan perusahaan. (Mate Vibhakti, 2014). Ada banyak

teknik yang biasa digunakan oleh para penyerang seperti SQL Injection, Cross Site Scripting, Brute Force, Worm, deface, dll untuk menyusup ke aplikasi web. Dengan menggunakan metode yang secara khusus ditujukan untuk mengeksploitasi potensi titik lemah dalam aplikasi web, para penyerang dapat dengan mudah dideteksi oleh Sistem dengan akurasi yang cukup. SQL Injection adalah serangan yang bertujuan kerentanan database aplikasi web.

Pada studi (Riadi et al., 2018) Aplikasi Website sangat rentan terhadap berbagai serangan salah satunya menggunakan SQL Injection, jika sebuah website terdapat celah maka penyerang dapat mengakses database. Situs web yang tidak memiliki keamanan yang baik memiliki potensi risiko keamanan yang dapat digunakan oleh penyerang. Ada sepuluh kerentanan yang terdapat dalam situs web yang dirilis oleh Open Web Application Security Project (OWASP) 10-2017 teratas, kurangnya pengembang situs web pada keamanan situs web menimbulkan risiko besar yang akan dieksploitasi oleh penyerang untuk menghancurkan, mengambil atau menghapus basis data di situs web.

Berdasarkan kesimpulan dari studi (Mukhtar & Azer, 2020), telah melakukan tes ModSecurity Web Application Firewall melawan SQL Injaction dan terbukti efisien untuk memblokir serangan kami berdasarkan iterasi SQLMAP. Perlu dikatakan bahwa teknik SQLI berkembang terus menerus. Untuk mencapai perlindungan yang diperlukan, perlu memperbarui aturan ModSecurity secara teratur untuk dapat memblokir teknik baru serangan injeksi SQL yang berkembang setiap hari.

Namun metode tersebut tidaklah cukup, sehingga sampai saat ini **masih diperlukan peningkatan ModSecurity dan membutuhkan Web Application Firewall yang efektif dalam mecegah SQL Injection Attack** pada Aplikasi Website perusahaan atau client terutama pada Windows Server.

Tujuan dari penelitian ini adalah untuk mengkaji masalah deteksi dan pencegahan serangan SQL Injection. Ulasan ini didasarkan pada empat pertanyaan yang diajukan dan dijawab.

## 2. Method

Research questions: Penelitian ini mencoba menjawab pertanyaan penelitian:

- RQ1: Teknik SQL Injection Attack apa yang saat ini dan banyak digunakan?
- RQ2: Apa saja Tools Web Application Firewall dalam keamanan website dari serangan SQL Injection.
- RQ3: Apakah Tools OWASP CSR Web Application Firewall Dapat mendeteksi SQL Injection Attack
- RQ4: Seberapa Efektif jenis Web Application Firewall OWASP CSR dalam menangkal SQL Injection Attack?

## 3. Planing Phase

Demi kelancaran dalam systematic literature review dibutuhkan eksekusi perencanaan yang matang. Research questions adalah bagian penting dari systematic literature review. Sesuai dengan pedoman yang diusulkan oleh Petticrew dan Roberts (2006), kriteria untuk merangkum pertanyaan penelitian adalah berdasarkan PICOC. Untuk studi ini, PICOC didefinisikan seperti berikut ini:

Table 1. Planing Phase PICOC

| | |
|---|---|
| Population (P): | Structured Query Language (SQL) Database |
| Intervention (I) | Serangan Injection untuk mendapatkan akses ke dalam database |
| Comparison (C) | Teknik deteksi dan Teknik pencegahan menggunakan tools |
| Outcomes (O) | Efektifitas Deteksi dan Pencegahan pada tools OWASP untuk menghindari Serangan SQL Injection |
| Context (C) | Review atas studi yang ada tentang Serangan SQL Injection |

Mengenai RQ1, studi ini akan melihat berbagai metode yang digunakan dalam menjalankan serangan terhadap database dengan memanfaatkan kolom input pengguna pada aplikasi berbasis web.

Pada RQ2, studi ini akan membahas Apa saja Tools Web Application firewall yang sudah ada untuk keamanan website dari Serangan SQL Injection.

Pada RQ3, studi ini akan membahas Tools OWASP CSR Web Application Firewall dapat mendeteksi Serangan SQL Injection.

Dan yang terakhir dalam pertanyaan penelitian RQ4 studi ini memeriksa tingkat efektifitas tools OWASP CSR Web Application Firewall Untuk mencegah beberapa Serangan SQL Injection tertentu yang tertera pada RQ1.

## 4. Search Procedure

Studi yang digunakan untuk SLR diperoleh melalui pencarian online Jurnal International pada Google Scholar. Pencarian dilakukan dengan kata kunci: (Preventing OR Detection OR OWASP) AND SQL Injection attacks. Hanya journals dan conferences relevan yang disimpan untuk tinjauan lebih lanjut.

Inclusion and exclusion criteria Inclusion
Inclusion:
• Artikel dengan judul yang berkaitan dengan deteksi atau pencegahan SQL Injection Attack using OWASP.
• Artikel yang diterbitkan pada tahun 2018-2021
Exclusion:
• Artikel yang diterbitkan sebelum tahun 2018
• Artikel yang dalam judulnya tidak berkaitan dengan deteksi atau pencegahan SQL Injection Attack
• Artikel diterbitkan dalam bahasa selain Bahasa Inggris.

## 5. Pembahasan

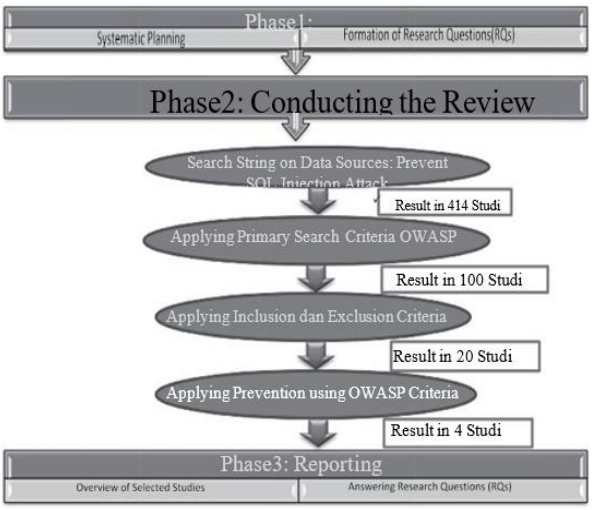


Figure 1. Kerangka Berpikir

PEMETAAN JURNAL

A. Berdasarkan faktor

Table 2. Pemetaan Jurnal Berdasarkan Faktor.

| No | Faktor | Paper Penelitian | Jumlah |
|---|---|---|---|
| 1 | SQL Injection Attacks | (Robinson et al., 2018),(Jemal et al., 2020),(Olalere et al., 2018),(D. Chen et al., 2021),(Muttaqin & Yaddarabullah, 2020),(Alenezi et al., 2021), (Zhang et al., 2019),(Hubskyi et al., 2020),(Harshavardhan & Maheshwari, 2020),(Xie et al., 2019), (Li et al., 2019),(Myrutenko & Oksiiuk, 2020),(Z. Chen & Guo, 2018),(Castillo et al., 2019),(Fang et al., 2018), | 20 |
| 2 | Detection and Prevention | (Robinson et al., 2018),(Jemal et al., 2020),,(Olalere et al., 2018),(D. Chen et al., 2021),(Li et al., 2019),(Myrutenko & Oksiiuk, 2020), (Z. Chen & Guo, 2018),(Castillo et al., 2019),(Fang et al., 2018),(Bisht et al., 2018),(Gautam et al., 2018) | 11 |
| 3 | Using OWASP | (Robinson et al., 2018),(Riadi et al., 2018),(Mukhtar & Azer, 2020), (Laksono & Santoso, 2021) | 4 |

B. Berdasarkan Tahun.

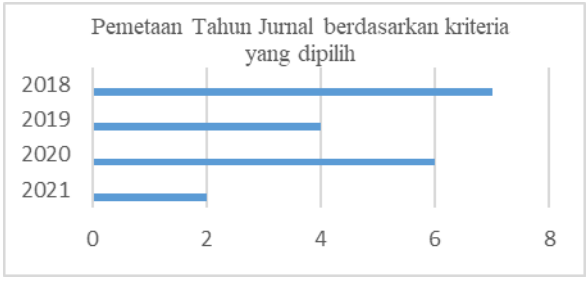


Figure 2. Pemetaan Jurnal Berdasarkan Tahun

Jurnal yang dipilih berdasarkan kriteria berkaitan dengan Prevention SQL Injection yang berhubungan dengan menggunakan OWASP, dari 20 jurnal yang dipilih paling banyak tahun 2018 yaitu 7 jurnal dan 2020 sebanyak 6 jurnal, tahun 2019 4 jurnal, sedangkan 2021 hanya 3 jurnal yang dipilih.

**RQ1, Teknik SQL Injection Attack apa yang saat ini dan banyak digunakan?**

Menurut Open Web Application Security Project (OWASP), kerentanan injeksi terus menjadi kerentanan yang paling banyak ditemukan di aplikasi web.

**Tautologies**: Pernyataan Query ini selalu benar karena telah ditambahkan oleh pernyataan tautologi ('a' = 'a'). Tanda hubung ganda "-" menginstruksikan parser SQL bahwa pernyataan lainnya adalah komentar dan tidak boleh dijalankan.

| | |
|---|---|
| Smith<br>' OR 'a'='a | SELECT name FROM member WHERE username='Smith' AND password= ' ' OR 'a'= 'a' |
| ' OR 'a'='a<br>' OR 'a'='a | SELECT name FROM member WHERE username = ' ' OR 'a'='a' AND password=' ' OR 'a'='a' |
| 'OR 'a'='a'<br>- - | SELECT name FROM member WHERE username = ' ' OR 'a'='a' - - ' AND password=' ' |

Figure 3. Tautologies

**Malformed Queries**: Pesan kesalahan menyebabkan penyerang secara tepat membedakan parameter mana yang rentan dalam aplikasi dan garis besar total database yang mendasarinya. Situasi ini disalahgunakan oleh token SQL buatan penyerang atau input sampah yang menyebabkan kesalahan sintaks, jenis campur aduk, atau kesalahan logika ke dalam database. Untuk mengenali parameter yang dapat diinjeksi, kesalahan sintaks dapat digunakan. Jenis kesalahan dapat diterapkan untuk menyimpulkan jenis informasi dari atribut tertentu atau untuk menghapus informasi. Kesalahan logika bisa keluar nama tabel dan nama atribut yang menyebabkan kesalahan atau error tersebut.

**Union Query**: Dalam teknik ini, penyerang menyuntikkan pernyataan tidak valid digabungkan dengan Query yang valid dengan menggunakan kata kunci UNION. Penyerang menyalahgunakan pernyataan Query dari struktur "UNION <injected query>" sebisa mungkin membuatnya menjadi statement yang sah. Hal ini membuat aplikasi mengembalikan informasi dari hasil Query asli dan juga informasi dari tabel lain. Kemudian penyerang akan menggabungkan Statement yang ada dengan dengan tanda hubung ganda "- -" untuk meng comment Query yang tidak dia perlukan.

```
SELECT name FROM member WHERE
username="UNION SELECT password
FROM member WHERE username='admin' -
- AND password="
```

***Piggy-backed Queries***: Dalam serangan berbasis kueri yang didukung piggy, penyerang mencoba menambahkan kueri tambahan ke dalam string pertanyaan pertama. Ini menyalahgunakan database dengan pemisah kueri, misalnya, ";" untuk menambahkan kueri tambahan ke kueri pertama. Jika serangan itu berhasil, database mendapatkan dan menjalankan pernyataan kueri yang berisi banyak pertanyaan tertentu. Query pertama adalah query asli yang sah, yaitu untuk mengeksekusi database sedangkan query kedua, query jahat adalah menyalahgunakan database.

**Inference**: Database berperilaku berbeda bergantung pada hasil Query yang dihasilkannya. Ada dua jenis serangan inferensi yaitu blind injection dan timing attacks

**Stored Procedure Queries**: Dalam pendekatan ini, prosedur tersimpan menjadi korban bagi penyerang untuk mengeksploitasi database.

Prosedur yang disimpan adalah kode yang disimpan dalam database dan dijalankan langsung oleh mesin database.

**RQ2, Apa saja Tools Web Application Firewall dalam keamanan website dari serangan SQL Injection?**

**Open Web Application Security Project (OWASP) ModSecurity Core Rule Set (CRS)** adalah firewall aplikasi web yang dapat membantu administrator mengamankan server web.

OWASP beroperasi dengan memblokir Alamat IP yang mencoba melanggar aturan keamanan, memantau lalu lintas jaringan, dan mencegah permintaan jaringan yang mencurigakan dari luar. ModSecurity bekerja dengan mengumpulkan muatan berbahaya dari berbagai sumber web dan menggabungkannya ke dalam daftar hitam. Aturan ModSecurity kemudian menggunakan algoritma pencocokan pola cepat untuk memeriksa html keluar untuk tanda-tanda kode berbahaya ini. ModSecurity kemudian dapat memperingatkan /memblokir /membersihkan kode berbahaya untuk mencegah menginfeksi aplikasi web.

**Atomic ModSecurity Rules**: Tools ini adalah aturan Web Application Firewall (WAF) komprehensif yang ditetapkan dengan ratusan aturan WAF ModSecurity untuk melindungi aplikasi dari serangan web dan didukung penuh oleh dukungan ahli.

Atomicorp mengembangkan kumpulan aturan ModSecurity pertama dan mempertahankan jumlah terbesar aturan WAF aktif yang mendukung jenis server dari Tomcat dan Nginx hingga IIS, LightSpeed, dan Apache.

Aturan ModSecurity Atom adalah aturan WAF paling komprehensif yang ditetapkan di industri, memiliki tingkat kualitas tertinggi dan didukung penuh oleh dukungan ahli.

**RQ3, Apakah Tools OWASP CSR Web Application Firewall Dapat mendeteksi SQL Injection Attack?**

Berdasarkan hasil dari jurnal (Robinson et al., 2018) OWASP ModSecurity berhasil 100% mendeteksi dan mengamankan aplikasi web dari SQL Injection setelah 15 kali pengujian menggunakan 3 Sistem Operasi Linux yang berbeda.

**RQ4, Seberapa Efektif jenis Web Application Firewall OWASP CSR dalam menangkal SQL Injection Attack?**

Dalam Jurnal (Robinson et al., 2018), Telah dilakukan penelitian. Setelah 15 kali pengujian serangan untuk setiap jenis SQL Injection menggunakan 3 perbedaan pada kedua web server, hasilnya akan ditampilkan pada table:

Table 3, SQL Injection Attack Result
(Robinson et al., 2018)

| Attack | Result | |
|---|---|---|
| | OWASP | NOOWASP |
| Tautology | Failed | Success |
| Logically | Success | Success |
| Union Queries | Failed | Success |
| Piggy-backed | Failed | MySQL countered |
| Stored Procedure | Failed | MySQL countered |
| Blind Injection | Failed | MySQL countered |
| Timing Attacks | Failed | MySQL countered |

Dari Tabel di atas:

- Status Failed: berarti OWASP ModSecurity berhasil mengamankan web server dan mendeteksi log serangan/ Hit List dari serangan tersebut.
- Status Success berarti penyerang berhasil menyuntikkan kueri SQL ke server web.
- MYSQL Countered berarti kueri SQL tersebut telah ditambal oleh MySQL itu sendiri.

Dan pengujian kedua menggunakan SQLmap Exploitation, Pengujian serangan kedua menggunakan alat eksploitasi SQLmap yang akan memindai server web dan menyuntikkan ribuan kueri SQL ke server web. Setiap serangan dilakukan 10 kali ( OWASP 10 kali, NOOWASP 10 kali ) pada 3 macam Sistem Operasi. Hasilnya akan ditampilkan di Tabel berikut:

Table 4, SQLMap Exploitation Result
(Robinson et al., 2018)

| OS | Result | |
|---|---|---|
| | OWASP | NOOWASP |
| Kali Linux | Failed | Success |
| Back Box | Failed | Success |
| Parrot | Failed | Success |

Hasilnya menunjukkan bahwa OWASP berhasil mengamankan web server dari semua eksploitasi SQLmap dan mendeteksi serangan pada Hit List seperti yang ditunjukkan pada Gambar berikut:

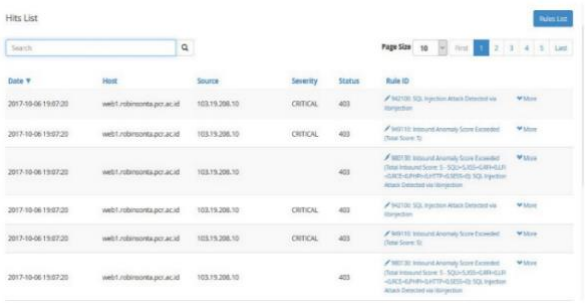


Figure 4. Hasil Test OWASP (Robinson et al., 2018)

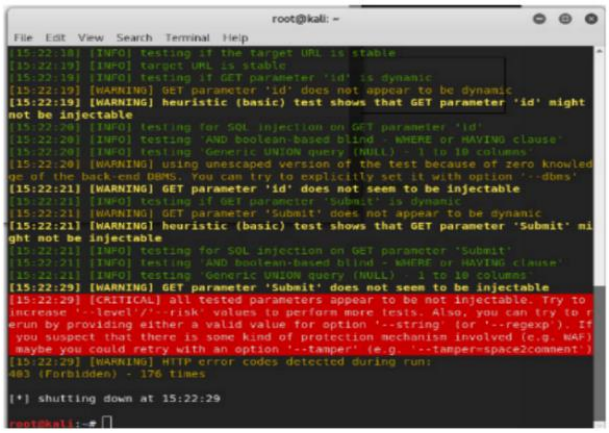


Figure 5. Hasil Test OWASP (Robinson et al., 2018)

## 6. Conclusion

Penelitian ini dibuat berdasarkan Systematic Literatur Review. Berbagai jenis teknik SQL injection attacks telah diidentifikasi dan dijelaskan. Selanjutnya, tools Web Application Firewall telah disebutkan salah satunya OWASP CSR, kemudian Efektifitas OWASP CSR dalam mencegah SQL Injection sudah ada dan telah di uji pada 3 Server Linux berbeda. Akhirnya perlu dilakukan penelitian lebih lagi terkait deteksi dan pencegahan SQL Injection menggunakan tools OWASP CSR Web Application Firewall Running On IIS ModSecurity. Current Issu yang perlu dibahas lebih lanjut lagi dari penelitian ini berdasarkan pemetaan jurnal yang didapat:

- Menguji deteksi dan pencegahan menggunakan tools OWASP CSR Web Application Firewall (WAF) running on IIS ModSecurity.
- Evaluasi keefektifan pencegahan tools OWASP CSR running on IIS terhadap SQL injection attacks.

## References

Alenezi, M., Nadeem, M., & Asif, R. (2021). SQL injection attacks countermeasures assessments. In *Indonesian Journal of Electrical …*. researchgate.net. https://www.researchgate.net/profile/Mamdouh-

Alenezi-2/publication/344597081_SQL_Injection_Attacks_Countermeasures_Assessments/links/5fcc5c6345851568d142b19a/SQL-Injection-Attacks-Countermeasures-Assessments.pdf

Bisht, P., Pant, D., & Rauthan, M. S. (2018). Analyzing and Defending Web Application Vulnerabilities through Proposed Security Model in Cloud Computing. *Journal of Graphic …*. https://www.journal.riverpublishers.com/index.php/JGEU/article/view/2592

Castillo, R. E., Caliwag, J. A., Pagaduan, R. A., & ... (2019). Prevention of SQL injection attacks to login page of a website application using prepared statement technique. *Proceedings of the 2019 …*. https://doi.org/10.1145/3322645.3322704

Chen, D., Yan, Q., Wu, C., & Zhao, J. (2021). Sql injection attack detection and prevention techniques using deep learning. *Journal of Physics: Conference …*. https://iopscience.iop.org/article/10.1088/1742-6596/1757/1/012055/meta

Chen, Z., & Guo, M. (2018). Research on SQL injection detection technology based on SVM. *MATEC Web of Conferences*. https://www.matec-conferences.org/articles/matecconf/abs/2018/32/matecconf_smima2018_01004/matecconf_smima2018_01004.html

Fang, Y., Peng, J., Liu, L., & Huang, C. (2018). WOVSQLI: Detection of SQL injection behaviors using word vector and LSTM. *… of the 2nd International Conference on …*. https://doi.org/10.1145/3199478.3199503

Gautam, B., Tripathi, J., & Singh, S. (2018). A secure coding approach for prevention of SQL injection attacks. In *International Journal of Applied …*. ripublication.com. https://www.ripublication.com/ijaer18/ijaerv13n11_158.pdf

Harshavardhan, G., & Maheshwari, M. (2020). *SQL Injection-Biggest vulnerability of the era*. wwww.easychair.org. https://wwww.easychair.org/publications/preprint_download/mptV

Hubskyi, O., Babenko, T., Myrutenko, L., & ... (2020). Detection of sql injection attack using neural networks. *International Scientific …*. https://doi.org/10.1007/978-3-030-58124-4_27

Jemal, I., Cheikhrouhou, O., Hamam, H., & Mahfoudhi, A. (2020). SQL Injection Attack Detection and Prevention Techniques Using Machine Learning. *International Journal of Applied Engineering Research*.

Laksono, A. T., & Santoso, J. D. (2021). Analysis of Website Security of SMKN 1 Pangandaran Against SQL Injection Attack Using OWASP Method. *… of Informatics and …*. http://ejurnal.stmik-budidarma.ac.id/index.php/ijics/article/view/3208

Li, Q., Li, W., Wang, J., & Cheng, M. (2019). A SQL injection detection method based on adaptive deep forest. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/8854182/

Mukhtar, B. I., & Azer, M. A. (2020). Evaluating the Modsecurity Web Application Firewall Against SQL Injection Attacks. *2020 15th International Conference on …*. https://ieeexplore.ieee.org/abstract/document/9334626/

Muttaqin, M. F., & Yaddarabullah, S. (2020). Implementation of AES-128 and Token-Base64 to Prevent SQL Injection Attacks via HTTP. In *International Journal*. academia.edu. https://www.academia.edu/download/63904066/ijatcse60932020202007 12-21480-1dnfwt1.pdf

Myrutenko, L., & Oksiiuk, O. (2020). Detection of SQL Injection Attack Using Neural Networks. *… and Simulation of Systems (MODS'2020 …*. https://books.google.com/books?hl=en&lr=&id=jw36DwAAQBAJ&oi=fnd&pg=PA277&dq=prevent+sql+injection+attack+using+owasp&ots=qEAmOU_HB6&sig=pffwDMT8gNa0DaVuqyvI52BBMZg

Olalere, M., Egigogo, R. A., Umar, R., & Abdulhamid, S. M. (2018). *A Systematic Literature Review on Detection, Prevention and Classification with Machine Learning Approach*. repository.futminna.edu.ng. http://repository.futminna.edu.ng:8080/jspui/handle/123456789/10422

Riadi, I., Umar, R., & Sukarno, W. (2018). Vulnerability of Injection Attacks Against The Application Security of Framework Based Bebsites Open Web Access Security Project (OWASP). In *J. Inform*. core.ac.uk. https://core.ac.uk/download/pdf/324200022.pdf

Robinson, Akbar, M., & Ridha, M. A. F. (2018). SQL injection and cross site scripting prevention using OWASP web application firewall. *International Journal on Informatics Visualization*. https://doi.org/10.30630/joiv.2.4.107

Xie, X., Ren, C., Fu, Y., Xu, J., & Guo, J. (2019). Sql injection detection for web applications based on elastic-pooling cnn. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/8877739/

Zhang, H., Zhao, B., Yuan, H., Zhao, J., Yan, X., & ... (2019). SQL injection detection based on deep belief network. *Proceedings of the 3rd …*. https://doi.org/10.1145/3331453.3361280