VISUALISASI DATA SERANGAN SQL *INJECTION* & XSS DENGAN METODE KNN PADA RAMA *REPOSITORY*

SKRIPSI
Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH:
FEBI RUSMIATI
09011181722025

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2022

VISUALISASI DATA SERANGAN SQL *INJECTION* & XSS DENGAN METODE KNN PADA RAMA *REPOSITORY*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh:

FEBI RUSMIATI

09011181722025

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

VISUALIZATION OF SQL *INJECTION* & XSS ATTACK DATA WITH THE KNN METHOD ON THE RAMA REPOSITORY

SKRIPSI

Submitted to Complete of the Term Obtaining a Bachelor Of Computer Engineering

By:

FEBI RUSMIATI

09011181722025

Indralaya, September 2022

Supervisor

Deris Stiawan, M.T., Ph.D., IPU
NIP. 197806172006041002

Co-Supervisor

Ali Bardadi, S.SI., M.Kom.
NIP. 198806292019031007

Head of Department Computer Engineering

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 22 September 2022

Tim Penguji :

1. Ketua Sidang : Ahmad Fali Oklilas, M.T
2. Sekretaris Sidang : Aditya Putra Perdana P, M.T
3. Penguji Sidang : Huda Ubaya, M.T
4. Pembimbing I : Deris Stiawan, M.T., Ph.D., IPU
5. Pembimbing II :Ali Bardadi, S.SI., M.Kom.

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Febi Rusmiati

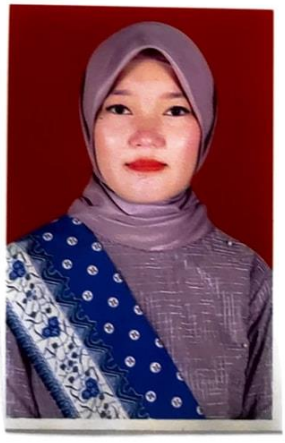
NIM : 09011181722025

Judul : Visualisasi Data Serangan SQL *Injection* & XSS Dengan Metode KNN Pada RAMA *Repository*

Hasil Penyecekan *Software iThenticate/Turnitin* : 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Indralaya, September 2022

Febi Rusmiati
NIM. 09011181722025

HALAMAN PERSEMBAHAN

Aku hampir pernah menyerah,

Namun ingatlah setiap proses seseorang itu berbeda-beda.

Teruslah berjalan, walau banyak rintangan yang harus dihadapi.

Orang lain mungkin tidak akan peduli dengan prosesnya.

Dan kita akan ternilai, ketika hasil dari segala jerih payah kita telah tercapai.

"*Tak perlu menunggu sampai akhir untuk tersenyum,*

Belajarlah bahwa lebih baik tersenyum sesering mungkin,

Jadi, berusahalah lebih sering dan nikmatilah kehidupan."

"*Aku tidak tau kedepannya seperti apa, tapi aku yakin rencana Tuhan luar biasa."*
#Naruto

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji dan syukur penulis selalu panjatkan atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan rahmat dan karunia-Nya, serta memberikan nikmat iman, beserta kesehatan jasmani maupun rohani sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **"Visualisasi Data Serangan SQL *Injection* & XSS Dengan Metode KNN pada RAMA *Repository*"**.

Penulis menyadari dalam selesainya penyusunan Tugas Akhir ini tidak terlepas dari, Do'a dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada yang terhormat :

1. Allah Subhanahu Wata'ala.
2. Orangtua, saudara, serta keluarga besar penulis yang tersayang yang selalu mendukung, menyemangati dan mendo'akan.
3. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D., IPU selaku Dosen Pembimbing Tugas Akhir I di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Ali Bardadi, S.SI., M.Kom. selaku Dosen Pembimbing Tugas Akhir II di Jurusan Sistem Informasi Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Ahmad Zarkasi, M.T. selaku Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Mbak Nurul Afifah, M.Kom. yang telah membantu membimbing dalam menyelesaikan Tugas Akhir.
9. Mbak Reni Virgasari, selaku Admin Jurusan Sistem Komputer yang telah banyak membantu administrasi dalam menyelesaikan Tugas Akhir.

10. Abdi Bimantara, S.Kom dan M. Taufiq Qurahman, selaku teman seperjuangan yang telah membantu dalam menyelesaikan Tugas Akhir.
11. Ahmada Afidin, Meutia Zamieyus, Lisa Melinda, Tia Hermita, Nuzula Rahma Safitri, Aulia, Amartya Bimantara, Agung Setiawan yang merupakan teman seperjuangan Riset selalu memberikan semangat serta dukugan selalu menemani hari-hari penulis dalam menyelesaikan Tugas Akhir dan Tim Grup Riset Comnets yang lainnya yang telah membantu.
12. Aldy Pred, Alif Muhammad Hafidz, Asri Safmi, Xosya Salassa, Piningit Harun Kusuma, Ahmad Fansyuri (Efan), Ikhsan, Ria Esafri, Risqi Abraqa, Tommy mandala putra, Wais Al Qarni, Ghina Aulia, Ayu meilinda merupakan teman seperjuangan PT Sentolop Reborn dari awal masuk perkuliahan sampai saat ini.
13. Dwi Trisnawati, Weni Putri Lestari, Indah Sari Zulaikah team Empat Sekutu di tambah Siti Khotimah, Jeni Veliyanti, Figi Dwi Putra, Rico Ariyanto, Rahmadi orang- orang penting love me yang selalu mendukung dan memberi semangat setiap hari nya.
14. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2017.
15. Civitas Akademik Fakultas Ilmu Komputer Universitas Sriwijaya.
16. Almamater.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih banyak kekurangan, dan masih jauh dari kata sempurna. Karena itu, penulis sangat memohon kritik dan saran yang bersifat membangun. Semoga Proposal Tugas Akhir ini dapat bermanfaat untuk semua yang membaca.

Wassalamu’alaikum Warahmatullahi Wabarakatuh.

Indralaya, September 2022

Penulis

Visualisasi Data Serangan SQL *Injection* dan XSS dengan Metode KNN pada RAMA *Repository*

Febi Rusmiati (09011181722025)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email : febirusmiati@gmail.com

Abstrak

Layanan yang berbasis web merupakan perkembangan teknologi yang mudah di akses setiap saat dan dimanapun semua orang dapat mengaksesnya. Karena sifatnya yang terdistribusi dan terbuka, membuat teknologi aplikasi web secara konsekuen lebih sensitif terhadap keamaan. SQL *Injection* dan XSS merupakan serangan internet yang dapat mengakses dan memanipulasi platform aplikasi web dengan mudah. Serangan SQL *Injection* dan serangan XSS yang memungkinkan pengguna melakukan peretas pada web dengan memasukkan skrip tertentu, sehingga mengakibatkan manipulasi data atau mengotrol web yang dapat disalahartikan sebagai pengguna yang tidak valid. Pada penelitian ini menggunakan dataset dari RAMA *Repository* yang merupakan web yang menampung hasil eksperiman penelitian yang dilakukan berupa laporan tugas akhir. Dari dataset tersebut, berisikan data yang terdampak serangan SQL *Injection* dan XSS yang memungkinkan pengguna melakukan peretasan pada web tersebut. Dengan data tersebut peneliti mecoba membahas tentang visualisasi data dengan metode KNN. KNN dapat digunakan untuk masalah klasifikasi maupun regresi. Dari hasil penelitian yang dilakukan perbandingan dengan mengukur jarak euclidean berdasarkan nilai *k*, dari nilai *k1* sampai *k10* penelitian ini memperoleh nilai akurasi tertinggi sebesar 98.07%.

Kata kunci : SQL *Injection*, XSS, KNN, Visualisasi, RAMA *Repository*.

Mengetahui,

Pembimbing I Tugas Akhir	**Pembimbing II Tugas Akhir**
Deris Stiawan, M.T., Ph.D., IPU.	**Ali Bardadi, S.SI., M.Kom.**
NIP. 197806172006041002	**NIP. 198806292019031007**

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

Visualization of SQL *Injection* and XSS Attack Data With KNN Method on RAMA *Repository*

Febi Rusmiati (09011181722025)
Department of Computer Systems, Faculty of Computer Science,
Sriwijaya University
Email : febirusmiati@gmail.com

Abstract

Web-based services are technological developments that are easy to access at any time and wherever everyone can access them. Due to its distributed and open nature, web application technologies are consequently more sensitive to security. SQL *Injection* and XSS are internet attacks that can easily access and manipulate web application platforms. SQL *injection* attacks and XSS attacks that allow users to hack the web by entering certain scripts, resulting in data manipulation or web control that could be mistaken for an invalid user. In this study using a dataset from the RAMA *Repository* which is a web that accommodates the result of research experiments carried out in the form of a final project report. From the dataset, it contains data affected by SQL *Injectin* and XSS attacks that allow users to hack the web. With this data, the researcher tries to discuss about data visualization with the KNN method. KNN can be used for classification and regression problems. From the results of study, which was compared by measuring the euclidean distance based on the value of *k*, from the value of *k1* to *k10* this study obtained the highest accuracy value of 98.07%.

Keywords : SQL *Injection*, XSS, KNN, Visualisasi, RAMA *Repository*.

Mengetahui,

Pembimbing I Tugas Akhir	**Pembimbing II Tugas Akhir**
Deris Stiawan, M.T., Ph.D., IPU.	**Ali Bardadi, S.SI., M.Kom.**
NIP. 197806172006041002	**NIP. 198806292019031007**

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Layanan yang berbasis web merupakan perkembangan teknologi yang mudah diakses setiap saat dan dimanapun dapat mengaksesnya secara mudah dan cepat di seluruh dunia. Karena sifatnya yang terdistribusi dan terbuka, membuat teknologi aplikasi web secara konsekuen lebih sensitif terhadap keamaan [1][2].

Pada penelitian ini menggunakan dataset dari RAMA *Repository* yang merupakan web yang menampung hasil eksperimen penelitian yang dilakukan berupa laporan tugas akhir yang disusun oleh mahasiswa skripsi S1, S2, dan S3. Dari dataset tersebut, berisikan data yang terdampak serangan SQL *injection* dan serangan XSS yang memungkinkan pengguna melakukan peretasan pada web dengan memasukkan skrip tertentu, sehingga mengakibatkan manupulasi data atau mengontrol pengguna yang dapat disalahartikan sebagai pengguna yang valid [3].

Berdasarkan dataset tersebut, peneliti mencoba akan membahas tentang visualisasi terhadap data serangan SQL *Injection* dan XSS pada RAMA *Repository* dengan metode KNN (*K-Nearest Neighbor).* Algoritma KNN banyak digunakan untuk masalah klasifikasi bahkan dapat digunakan baik untuk klasifikasi maupun regresi. Pengklasifikasi KNN menunjukkan akurasi terbaik dan menghasilkan kinerja yang lebih baik. KNN menentukan nilai ketetapan *k* terdekat untuk meningkatkan akurasi pengklasifikasi dalam klasifikasi serangan yang berbeda [4].

Pada penelitian ini [5] melakukan deteksi malware berdasarkan opcode dalam file yang dapat dieksekusi dengan menggunakan teknik pemrosesan gambar. Dari metode yang diusulkan yang meliputi pembuatan grafik kode operasional dari file yang dapat dieksekusi dan mengubah grafik menjadi gambar untuk mengekstrak fitur. Pada langkah terakhir metode machine learning seperti SVM dan KNN digunakan untuk klasifikasi sehingga mendapatkan hasil kinerja dari penelitian tersebut sebesar 91,72%.

Dipenelitian ini [6] melakukan sistem deteksi menggunakan deep learning terhadap serangan injeksi kode berbasis web. Dimana penelitian ini menggunakan algoritma *convolutional deep neural network* serta meningkatkan efektivitas

melalui sebuah proses *preprocessing* yg mengkondisikan simbol terkait serangan SQL *Injection* dan *XSS* ke dalam hubungan tipe atau nilai. Hasil dari percobaan yang dilakukan deteksi injeksi kode dengan *deep learning* yang digunakan meningkatkan suatu tingkat deteksi data dari kinerja sekitar 75% hingga 95%, 99% presisi serta 92% nilai recall.

Pada penelitian [4] melakukan pengembangan IDS yang berkaitan dengan *network traffic*, dengan merancang IDS untuk klasifikasi serangan menggunakan algoritma pengklasifikasi KNN. Penelitian ini menggunakan dataset ISCX untuk menilai implementasi model. Hasil penelitian menunjukkan bahwa model yang digunakan mencatat peningkatan keakuratan 99,96%.

1.2 Rumusan Masalah

Berikut beberapa rumusan masalh dari penelitian Tugas akhir ini :

1. Bagaimana menyeimbangkan jumlah data yang digunakan untuk proses mengelompokkan serangan SQL *Injection* dan XSS?
2. Bagaimana algoritma KNN dapat mengelompokkan serangan SQL *Injection* dan XSS dengan mengukur nilai *k* terdekat untuk tingkat akurasi terbaik?
3. Bagaimana memvisualisasikan data serangan SQL *Injection* dan XSS ke dalam bentuk grafik?

1.3 Batasan Masalah

Adapun batasan masalh dari penelitian tugas akhir ini, yaitu:

1. Dataset yang digunakan berasal dari database RAMA *Repository*.
2. Metode yang digunakan untuk mengelompokkan data SQL *Injection* dan XSS ini algoritma KNN.
3. Data serangan SQL *Injection* dan XSS di visualisasikan.
4. Tidak membahas bagaimana cara pencegahan serangan SQL *Injection* serta XSS.

1.4 Tujuan

Tujuan dari tugas akhir ini, yaitu:

1. Menerapkan SMOTE untuk menyeimbangkan data pada proses klasifikasi serangan SQL *Injection* dan XSS.

2. Menerapkan metode KNN untuk mengelompokkan serangan SQL *Injection* dan XSS.
3. Memvisualisasikan data serangan SQL *Injection* dan XSS ke dalam bentuk grafik dengan metode KNN.

1.5 Manfaat

Manfaat dari penelitian tugas akhir ini, yaitu:

1. Dapat menyeimbangkan jumlah data yang digunakan.
2. Mendapatkan performa terbaik dengan mengukur *k*-terdekat metode KNN.
3. Dapat memvisualisasikan data serangan SQL *Injection* dan XSS ke dalam bentuk grafik.

1.6 Metodologi Penelitian

Untuk mencapai hasil dari Tugas Akhir ini, berikut tahap-tahap metodologi penelitian yang digunakan :

1. Studi Pustaka

   Dalam tahap ini, tahap yang dilakukan setalah masalh yang akan di bahas telah sesuai dan relevan sebagai penelitian. Tahap ini penulis akan mengumpulkan beberapa referensi sumber seperti jurnal ilmiah, buku, artikel yang mendukung dengan penelitian.

2. Konsultasi

   Tahap ini, melakukan pembahasan untuk proses penelitian yang akan dikerjakan dari tahap kasus yang akan di angkat dan menyiapkan data yang akan diolah.

3. Persisapan Dataset

   Pada tahap ini penulis menyiapkan data yang digunakan untuk penelitian yang menggunakan dataset dari database RAMA *Repository*. Setelah itu proses pengolah data dengan mengekstraksi data dan *preprocessing* data.

4. Perancangan Sistem

   Pada tahap ini, penulis akan mempersiapkan tahapan yang akan dilakukan pada penelitian seperti apa saja yang akan digunakan pada penelitian, kerangka kerja penelitian, dan pengujian, sehingga penelitian dapat terarahkan.

5. Pengujian

   Dalam tahap ini, melakukan pengujian seusai dengan batasan masalah dan perancangan sistem penelitian, sehingga mendapatkan hasil uji yang sesuai dengan penelitan.

6. Hasil dan Analisa

   Setelah pengujian mendapatkan hasil, maka hasil akan dianalisa sesuai dengan permasalahan sehingga tujuan penelitian tercapai. Lalu akan dilakukan penarikan kesimpulan dari hasil penelitian, dan memberikan saran untuk dapat digunakan penelitian selanjutny.

1.7 Sistematika Penulisan

Dalam tugas akhir ini menggunakan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab I ini, berisi tujuaan dasar dari tugas akhir berupa latar belakang, rumusan masalh, batasan masalah, tujuan dan manfaat dari tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Bab II ini, berisi *Literature Riview* yang terkait dengan penelitian tugas akhir yang membahas tentang serangan SQL *injection* & *Cross-Site Scripting* (XSS) yang mengunakan metode KNN.

BAB III METODOLOGI PENELITIAN

Bab III ini, ada beberapa tahap dalam penjelasan bab ini seperti tahap kerangka kerja penelitian, kerangka kerja metodologi penilitian, kebutuhan perangkat, persiapan dataset, ekstraksi dataset, *oversampling* data, dan model penelitian yang digunakn untuk mencapai tujuan dari tugas akhir ini.

BAB IV HASIL DAN ANALISA

Bab IV ini, berisikan hasil eksperimen dari tahap penelitian yang sudah di kerjakan pada tahapn sebelumnya. Dari hasil eksperimen tersebut data yang diperoleh dan telah diuji akan di analisa dan di validasi hasil.

BAB V KESIMPULAN DAN SARAN

Bab V ini, menyampaikan kesimpulan yang telah dicapai dari penelitian tugas akhir ini yang merupakan hasil pencapaian yang sudah ditargetkan dan saran untuk peneliti yang ingin melanjutkan tugas akhir ini.

DAFTAR PUSTAKA

[1] A. Luo, W. Huang, and W. Fan, "A CNN-based Approach to the Detection of SQL Injection Attacks," *Proc. - 18th IEEE/ACIS Int. Conf. Comput. Inf. Sci. ICIS 2019*, pp. 320–324, 2019, doi: 10.1109/ICIS46139.2019.8940196.

[2] M. Hasan, Z. Balbahaith, and M. Tarique, "Detection of SQL Injection Attacks: A Machine Learning Approach," *2019 Int. Conf. Electr. Comput. Technol. Appl. ICECTA 2019*, 2019, doi: 10.1109/ICECTA48151.2019.8959617.

[3] Y. Fang, Y. Li, L. Liu, and C. Huang, "DeepXSS," pp. 47–51, 2018, doi: 10.1145/3194452.3194469.

[4] M. Nikhitha and M. A. Jabbar, "K Nearest Neighbor Based Model for Intrusion Detection System," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2, pp. 2258–2262, 2019, doi: 10.35940/ijrte.b2458.078219.

[5] F. Manavi and A. Hamzeh, "A new method for malware detection using opcode visualization," *19th CSI Int. Symp. Artif. Intell. Signal Process. AISP 2017*, vol. 2018-Janua, pp. 96–102, 2018, doi: 10.1109/AISP.2017.8324117.

[6] S. Abaimov and G. Bianchi, "CODDLE: Code-Injection Detection with Deep Learning," *IEEE Access*, vol. 7, pp. 128617–128627, 2019, doi: 10.1109/ACCESS.2019.2939870.

[7] M. R. Zalbina, T. W. Septian, D. Stiawan, M. Y. Idris, A. Heryanto, and R. Budiarto, "Payload recognition and detection of Cross Site Scripting attack," *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, pp. 172–176, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905285.

[8] Y. Fu, F. Lou, F. Meng, Z. Tian, H. Zhang, and F. Jiang, "An intelligent network attack detection method based on RNN," *Proc. - 2018 IEEE 3rd Int. Conf. Data Sci. Cyberspace, DSC 2018*, pp. 483–489, 2018, doi:

10.1109/DSC.2018.00078.

[9] B. Xu, S. Chen, H. Zhang, and T. Wu, “Incremental k-NN SVM method in intrusion detection,” *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, vol. 2017-Novem, pp. 712–717, 2018, doi: 10.1109/ICSESS.2017.8343013.

[10] E. A. Winanto, A. Heryanto, and D. Stiawan, “Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means,” *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[11] X. Zhang, J. Ran, and J. Mi, “An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic,” *Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2019*, pp. 456–460, 2019, doi: 10.1109/ICCSNT47585.2019.8962490.

[12] V. Bulavas, “Investigation of network intrusion detection using data visualization methods,” *59th Int. Sci. Conf. Inf. Technol. Manag. Sci. Riga Tech. Univ. ITMS 2018 - Proc.*, pp. 1–6, 2018, doi: 10.1109/ITMS.2018.8552977.

[13] P. A. Sonewar and S. D. Thosar, “Detection of SQL injection and XSS attacks in three tier web applications,” *Proc. - 2nd Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2016*, 2017, doi: 10.1109/ICCUBEA.2016.7860069.

[14] P. Tang, W. Qiu, Z. Huang, H. Lian, and G. Liu, “Detection of SQL injection based on artificial neural network,” *Knowledge-Based Syst.*, vol. 190, p. 105528, 2020, doi: 10.1016/j.knosys.2020.105528.

[15] N. M. Sheykhkanloo, “A Learning-based Neural Network Model for the Detection and Classification of SQL Injection Attacks,” *Int. J. Cyber Warf. Terror.*, vol. 7, no. 2, pp. 16–41, 2017, doi: 10.4018/ijcwt.2017040102.

[16] Robinson, M. Akbar, and M. A. F. Ridha, “SQL injection and cross site scripting prevention using OWASP web application firewall,” *Int. J.*

Informatics Vis., vol. 2, no. 4, pp. 286–292, 2018, doi: 10.30630/joiv.2.4.107.

[17] O. C. Abikoye, A. Abubakar, A. H. Dokoro, O. N. Akande, and A. A. Kayode, "A novel technique to prevent SQL injection and cross-site scripting attacks using Knuth-Morris-Pratt string match algorithm," *Eurasip J. Inf. Secur.*, vol. 2020, no. 1, 2020, doi: 10.1186/s13635-020-00113-y.

[18] A. S. Dikhit and K. Karodiya, "Result evaluation of field authentication based SQL injection and XSS attack exposure," *IEEE Int. Conf. Information, Commun. Instrum. Control. ICICIC 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ICOMICON.2017.8279148.

[19] H. Ali, M. N. M. Salleh, R. Saedudin, K. Hussain, and M. F. Mushtaq, "Imbalance class problems in data mining: A review," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 14, no. 3, pp. 1552–1563, 2019, doi: 10.11591/ijeecs.v14.i3.pp1552-1563.

[20] H. Ali *et al.*, "A review on data preprocessing methods for class imbalance problem," *Int. J. Eng. &Technology*, vol. 8, no. 3, pp. 390–397, 2019, doi: 10.14419/ijet.v8i3.29508.

[21] M. Sahare and H. Gupta, "A review of multi-class classification for imbalanced data," *Int. J. Adv. Comput. ...*, no. 3, pp. 1–5, 2012, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.300.8687&rep=rep1&type=pdf

[22] B. Zang, R. Huang, L. Wang, J. Chen, F. Tian, and X. Wei, "An Improved KNN Algorithm Based on Minority Class Distribution for Imbalanced Dataset," *Proc. - 2016 Int. Comput. Symp. ICS 2016*, pp. 696–700, 2017, doi: 10.1109/ICS.2016.0143.