# PENERAPAN RANDOM FOREST CLASSIFIER FEATURE PADA METODE NAÏVE BAYES UNTUK MENGENALI POLA-POLA SERANGAN PADA LAYANAN WEB

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana Komputer**


**DISUSUN OLEH:**

**ADI KESUMA JAYA UTAMA**

**09011381924097**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2023**

# LEMBAR PENGESAHAN

## PENERAPAN RANDOM FOREST CLASSIFIER FEATURE PADA METODE NAÏVE BAYES UNTUK MENGENALI POLA-POLA SERANGAN PADA LAYANAN WEB

## TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

**Oleh :**

**ADI KESUMA JAYA UTAMA**

**09011381924097**

**Mengetahui,**

| Ketua Jurusan Sistem Komputer | Pembimbing Tugas Akhir |
| --- | --- |
| **Dr. Ir. Sukemi, M.T.** | **Ahmad Heryanto, S.Kom, M.T.** |
| **NIP. 196612032006041001** | **NIP. 198701222015041002** |

# HALAMAN PERSETUJUAN

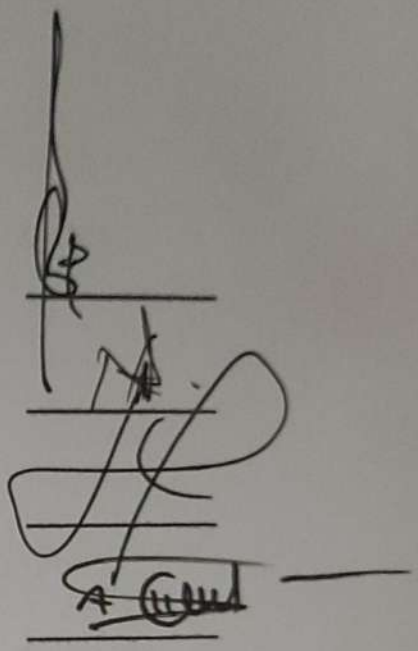
Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 18 Juli 2023

**Tim Penguji :**

1. **Ketua : Sutarno, M.T.**
2. **Sekretaris : Nurul Afifah, S.Kom., M.Kom.**
3. **Penguji : Huda Ubaya, S.T., M.T.**
4. **Pembimbing : Ahmad Heryanto, S.Kom, M.T.**



**Mengetahui,**

**Ketua Jurusan Sistem Komputer**

**Dr. Ir. Sukemi, M.T.**

**NIP. 196612032006041001**

# HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Adi Kesuma Jaya Utama

NIM : 09011181924097

Judul : Penerapan Random Forest Classifier Feature Pada Metode Naïve Bayes Untuk Mengenali Pola-Pola Serangan Pada Layanan Web

Hasil Pengecekan Software Turnitin : 18%

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.

**Palembang, Agustus 2023**


**Adi Kesuma Jaya Utama**

**NIM. 09011181924097**

## HALAMAN PERSEMBAHAN

**“Iringi segala sesuatumu dengan niat dan berdoa”**

**Penulis:**

**“Adi kesuma Jaya Utama”**

Skripsi ini saya persembahkan untuk :

Kedua orang tua saya tercinta yang telah memberikan dukungan dan motivasi pada pembuatan skripsi ini maupun materil dan selalu memanjatkan doa yang luar biasa untuk anaknya ini. Saya sangat berterima kasih juga kepada teman-teman seperjuangan di kelas SK19 Bukit. Kalian semua yang telah mendorong saya dengan motivasi dan juga semangat yang diberikan hingga saya berada di titik ini.

**“Motto Hidup”**

**“Awali setiap langkahmu dengan doa”**

# KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيْم

Assalamu'alaikum Warahmatullahi Wabarakatuh

Marilah kita panjatkan puji serta syukur atas kehadirat Allah SWT karena atas berkat hidayah dan karunia – Nya penulis telah dapat menyelesaikan penyusunan tugas akhir ini yang berjudul "**Penerapan Random Forest Classifier feature pada metode Naïve Bayes untuk mengenali pola-pola serangan pada layanan Web"**

Sebelumnya, penulis ingin memberikan serta mengucapkan terima kasih kepada beberapa pihak yang senantiasa memberikan ide, masukan, kritik, serta motivasi selama penulis melakukan penyusunan Tugas Akhir. Ucapan terima kasih tersebut ingin penulis sampaikan kepada :

1. Allah SWT yang senantiasa telah memberikan rahmat serta karunia – Nya sehingga penulis bisa menyelesaikan penulisan Tugas Akhir ini.
2. Orang tua saya tercinta Alm. Suwari dan Desi Susilawaty yang tidak letih - letih dalam mengasuh serta mendidik saya hingga saat ini dan tak ada hentinya juga dalam memberikan nasihat, semangat, serta juga dalam memberikan motivasi.
3. Bapak Prof. Dr. Ir. M. Said, M.Sc. yang merupakan Plt Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., yang merupakan Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing yang telah berkenan meluangkan waktu dan tenaga dalam membimbing, memberikan saran serta motivasi kepada penulis selama proses penulisan Tugas Akhir ini.
6. Bapak Ahmad Zarkasi M.T.. selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer penulis saat ini.
7. Kakak tingkat saya M Robby Bahari dan M. Agung Al Hafidzin yang telah memberikan berbagai bantuan selama penulis menjalani masa perkuliahan hingga akhir.

8. Mbak Sari Nuzulastri dan Mbak Renny Virgasari selaku admin jurusan sistem komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.
9. Semua pihak yang terlibat yang telah turut ikut membantu, baik itu dalam memberikan masukan dan ide, kritik, maupun juga memberikan semangat kepada penulis yang mana tidak bisa disebutkan satu persatu.

Penulis menyadari bahwasanya penyusunan Tugas Akhir yang telah diselesaikan ini masih tidak mendekati kata sempurna. Maka dari itu penulis meminta kritik, masukan, serta ide yang dapat digunakan oleh penulis agar penyusunan Tugas Akhir akan menjadi jauh lebih baik lagi di masa mendatang.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, Agustus 2022

Penulis,

Adi Kesuma Jaya Utama

NIM. 09011381924097

# RANDOM FOREST CLASSIFIER FUNCTION IN THE NAÏVE BAYES METHODE TO IDENTIFY POLIES OF ATTACKS ON WEB SERVICES

**Adi Kesuma Jaya Utama (09011381924097)**
Faculty Of Computer science, Universitas Sriwijaya
Email : adikju270901@gmail.com

## Abstract

SQL Injection is a hacking attack that is carried out by abusing the security gaps in the SQL layer on a data-based application, Sql Injections is a serious threat to the security of a website. The data set used in this study is CIC-IDS2018 from the Canadian Institute of Cybersecurity. This study discussed the application of the Random forest classifier on the Naïve Bayes method to recognize patterns of attacks on the Web.then the researchers compared the results between hyperparameter on the naïve bayes method, from the results carried out by researchers, that GaussianNB was excellent with an average of 96.33%.

**Keywords** : *Sql Injection, Random forest Classifier,GaussianNB, MultinomialNB, ComplementNB*

**Palembang, 4 August 2023**

**Acknowledged,**

| **Head Of Computer Systems Departements** | **Supervisor** |
|---|---|
| **Dr. Ir. Sukemi, M.T.** | **Ahmad Heryanto, S.Kom, M.T.** |
| **NIP. 196612032006041001** | **NIP. 198701222015041002** |

# PENERAPAN RANDOM FOREST CLASSIFIER FEATURE PADA METODE NAÏVE BAYES UNTUK MENGENALI POLA-POLA SERANGAN PADA LAYANAN WEB

**Adi Kesuma Jaya Utama (09011381924097)**
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : adikju270901@gmail.com

## ABSTRAK

*SQL Injection* adalah serangan dengan meretas yang dilakukan dengan cara menyalahgunakan celah keamanan yang ada di lapisan SQL pada aplikasi berbasis data itu dapat terjadi karena adanya input data pengguna yang tidak difilter dengan benar dan menggunakan form yang salah dalam proses pembuatannya. *Sql Injection* merupakan serangan jadi ancaman serius keamanan sebuah *website*. Dataset yang di gunakan dalam penelitian ini adalah CIC-IDS2018 yang berasal dari *Canadian institute of Cybersecurity*. Penelitian ini membahas tentang Penerapan *Random forest classifier* pada metode *Naïve Bayes* Untuk mengenali Pola – Pola Serangan pada Web.kemudian peneliti membandingkan hasil antara hyperparameter pada metode *naïve bayes*, dari hasil yang dilakukan oleh peneliti ,bahwa *GaussianNB* sangat baik dengan nilai rata-rata 96,33%

**Kata kunci** : *Sql Injection, Random forest Classifier,GaussianNB, MultinomialNB, ComplementNB*

**Palembang, 4 Agustus 2023**
**Mengetahui,**

| **Ketua Jurusan Sistem Komputer,** | **Pembimbing Tugas Akhir,** |
|---|---|
| **Dr. Ir. Sukemi, M.T.** | **Ahmad Heryanto S.Kom, M.T** |
| **NIP. 196612032006041001** | **NIP. 197801212008121003** |

## DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR TABEL

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Serangan *Cyber* semakin hari akan terus meningkat karena bertambah banyaknya pengguna dengan menggunakan dan memanfaatkan jaringan Internet. Berbagai macam serangan yang digunakan contohnya yaitu Serangan pada Smartphone, Komputer, Jaringan ,dan Website. Serangan pada website terdiri dari *phising, spoofing, cracking, ransomeware, Sql Injection* yang jadi ancaman serius keamanan sebuah *website*[1]. Sedangkan XSS adalah serangan *Cross Site Scripting* yang menyerang platform keamanan, serangan ini menjalankan kode jahat, bahkan sebagai serangan phishing[2].

Adapun penelitian sebelumnya yang mengenai tentang *Cross Site Scripting (XSS)* yang berjudul "Analisis Kerentanan Serangan *Cross Site Scripting (XSS)* pada Aplikasi Smart Payment Menggunakan Framework OWASP". Penelitian ini dilakukan untuk mengetahui kerentanan aplikasi Smart Payment dengan cara self test menggunakan tool ZAP. Pengujian ini dilakukan untuk mengamankan aplikasi Smart Payment. Hasil dari penelitian ini ditemukan kerentanan pada aplikasi Smart Payment. Kerentanan yang ditemukan berupa Information Disclosure-Suspicious Comments, X-Frame-Options Header not Set, XContent-Type-Options Header Missing, Timestamp Disclosure-Unix, Web Browser XSS Protection Not Enabled, dan Directory Browsing[3].

Adapun penelitian sebelumnya yang mengenai tentang *SQL Injection* yang berjudul "Klasifikasi *SQL Injection* Menggunakan Algoritma *Naïve Bayes*"[4]. Penelitian tersebut mengatakan bahwa *SQL injection* merupakan salah satu serangan yang mudah dilakukan tetapi sulit untuk dideteksi dan diklasifikasi karena keberagaman jenisnya. Kerentanan *SQLI* dihasilkan dari validasi input yang tidak tepat dari pengguna, Pada penelitian ini telah merancang sebuah model pengklasifikasi untuk mendeteksi serangan *SQL injection*. Serangan yang diklasifikasikan diantaranya, union, tautology, dan blind. Metode yang digunakan

dalam pengklasifikasian adalah *Naive Bayes*. Dari hasil pengujian di peroleh nilai akurasi sebesar 79,82%.

Adapun penelitian sebelumnya yang berjudul "Hybrid method integrating *SQL-IF* and *Naïve Bayes* for *SQL injection* attack avoidance"[5]. Penelitian tersebut Aplikasi web adalah objek yang paling diincar oleh penyerang. Teknik yang paling sering digunakan untuk menyerang aplikasi web adalah *Sql Injection*. Serangan ini dikategorikan berbahaya karena dapat digunakan untuk mengambil, memodifikasi, menghapus data, dan bahkan mengambil alih secara illegal database dan aplikasi web. Untuk mencegah serangan injeksi SQL dieksekusi dengan database, sebuah sistem yang dapat mengidentifikasi pola serangan dan dapat belajar untuk mendeteksi yang baru pola dari berbagai pola serangan yang telah terjadi diperlukan. Studi ini bertujuan untuk membangun sebuah sistem yang bertindak sebagai proxy untuk mencegah serangan injeksi SQL menggunakan HybridMetode yang merupakan kombinasi dari *SQL Injection Free Secure (SQL-IF)* dan metode *Naïve Bayes*. Pengujian dilakukan untuk mengetahui tingkat ketelitian, pengaruh konstanta (K) pada *SQL-IF*, dan jumlah dataset pada Naïve Bayes pada akurasi dan efisiensi(waktu buka rata-rata) halaman web. Hasil pengujian menunjukkan bahwa Metode *Hybrid* dapat meningkatkan akurasi pencegahan serangan injeksi *SQL*. Nilai K lebih kecil dan lebih besar dataset akan menghasilkan akurasi yang lebih baik. Metode *Hybrid* menghasilkan Panjang.

Adapun penelitian sebelumnya yang berjudul "Analisis Forensik Serangan *Sql Injection* Menggunakan Metode Statis Forensik"[6]. Penelitian ini menganalisa Website Kemahasiswaan Universitas Ahmad Dahlan merupakan website yang digunakan sebagai media dan sarana informasi komunikasi Mahasiswa. Sehingga website ini dapat diakses secara luas dan memerlukan keamanan website. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap keamanan website tersebut. Salah satunya adalah dengan melakukan serangan *sql injection*. Dengan menggunakan serangan *sql injection* ini akan dapat mengetahui apakah website tersebut pernah atau sedang ada penyerang yang memanipulasi data. Hasil pengamatan yang dilakukan dengan metode statis forensic yang hasilnya penyerang hanya melihat isi data namun belum mengubah database yang ada di website akan tetapi jika dibandingkan dari hasil pengujian dengan meng

gunakan metode Naive Bayes yang memperoleh nilai akurasi maka dapat di simpulkan bahwa metode Naive Bayes berhasil melakukan mengklasifikasi terhadap serangan *sql injection*.

Berdasarkan uraian latar belakang diatas, maka penelitian tugas akhir berjudul "**Penerapan *Random forest classifier* pada metode *Naïve Bayes* Untuk mengenali Pola – Pola Serangan pada Web**"

## 1.2 Tujuan dan Manfaat

### 1.2.1 Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu :

1. Menemukan poin tertinggi pada fitur *Random Forest Classifier* untuk mendeteksi serangan *sql injection* dengan dataset CIC-ID
2. Penerapan algoritma *Naïve Bayes* untuk mendeteksi serangan *sql injection*
3. Melakukan perbandingan antar hyper parameter pada metode naïve bayes
4. Melakukan perbandingan ROC Curve antar hyper parameter pada metode naïve bayes

### 1.2.2 Manfaat

Manfaat dari penulisan tugas akhir ini, yaitu :

1. Penelitian ini diharapakan dapat menjadi acuan bagi peneliti lain yang membahas tentang deteksi serangan Sql-Injection pada server agar dapat mempertahankan web.
2. Hasil dari penelitian ini dapat digunakan sebagai bahan informasi dan kajian bagi Fakultas Ilmu Komputer Universitas Sriwijaya dalam mempertahankan data

## 1.3 Perumusan dan Batasan Masalah

### 1.3.1 Perumusan Masalah

Penelitian ini dilakukan dengan rumusan masalah dengan beberapa point dibawah ini:

1. Bagaimana cara mengetahui pola serangan pada Web?
2. Apakah dampak dari pola serangan pada Web?
3. Bagaimana menemukan poin tertinggi pada fitur seleksi *Random Forest Classifier* dengan serangan *Sql Injection* pada dataset CIC-IDS2018.
4. Bagaimana penerapan seleksi fitur untuk memperoleh fitur penting dalam deteksi serangan *Sql Injection*?
5. Bagaimana hasil kinerja deteksi Naïve Bayes mempengaruhi nilai akurasi, sensitivi tas, spesifisitas, presisi, F1-Score?

### 1.3.2 Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu :

1. Penelitian menggunakan metode *Naïve Bayes*
2. Penelitian menggunakan dataset dari CICIDS 2018.
3. Penelitian menganalisa sebuah serangan *Sql Injection*

## 1.4 Sistematika Penulisan

Adapun penyusunan penulisan tugas akhir disusun menjadi beberapa sub bab yang akan dijelaskan secara rinci dan mengenai apa saja yang dilakukan oleh penulis pada saat melakukan penelitian. Secara sistematis, tugas akhir ini disusun sebagai berikut:

**BAB I PENDAHULUAN**

Bagian BAB I berisi tentang sebuah latar belakang, tujuan dan manfaat, serta dalam perumusan masalah dan juga sistematika penulisan.

**BAB II TINJAUAN PUSTAKA**

Bagian BAB II berisikan tentang informasi seperti penelitian terdahulu yang telah dilakukan oleh peneliti sebelumnya, kajian literatur, serta juga terdapat landasan teori dari berbagai bahasan.

**BAB III METODOLOGI PENELITIAN**

Bagian BAB III berisikan tentang informasi pengumpulan data, spesifikasi *hardware* dan *software* yang digunakan, serta juga terdapat metode dan *flowchart* yang digunakan dalam penelitian.

**BAB IV – PEMBAHASAN**

Bagian BAB IV berisikan tentang pembahasan inti dari riset yang telah diselesaikan serta juga berisi mengenai analisis hasil dari riset tersebut.

**BAB V – PENUTUP**

Bagian BAB V yang merupakan bab akhir berisikan tentang seperti kesimpulan dan saran.

[1] Hidyat, “No Title طرق تدريس اللغة العربية,” *Pendeteksian Keamanan Website SMA Greenschool Menggunakan Metod. Owasp dengan Penguji. XSS*, p. 32, 2015.

[2] E. Diatmika, P. Charly, I. M. P. Prayoga, I. M. E. Listartha, T. Informatika, and U. P. Ganesha, “Pendeteksian Keamanan Website SMA Greenschool Menggunakan Metode Owasp dengan Pengujian XSS,” vol. 11, pp. 77–82, 2022.

[3] I. Riadi, R. Umar, and T. Lestari, “Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP,” *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 5, no. 3, pp. 146–152, 2020, doi: 10.14421/jiska.2020.53-02.

[4] E. Prasetyo, P. Sukarno, and E. M. Jadied, “Klasifikasi SQL Injection Menggunakan Algoritma Naïve Bayes conf,” vol. 8, no. 5, pp. 10605–10620, 2021.

[5] F. Y. Hernawan, I. Hidayatulloh, and I. F. Adam, “Hybrid method integrating SQL-IF and Naïve Bayes for SQL injection attack avoidance,” *J. Eng. Appl. Technol.*, vol. 1, no. 2, pp. 85–96, 2021, doi: 10.21831/jeatech.v1i2.35497.

[6] I. Riadi, R. Umar, and W. Sukarno, “Analisis Forensik Serangan Sql Injection Meanggunakan Metode Statis Forensik,” *Pros. Interdiscip. Postgrad. Student Conf. 1st*, vol. I, no. I, pp. 102–103, 2016.

[7] Q. Li, W. Li, J. Wang, and M. Cheng, “A SQL Injection Detection Method Based on Adaptive Deep Forest,” *IEEE Access*, vol. 7, pp. 145385–145394, 2019, doi: 10.1109/ACCESS.2019.2944951.

[8] X. Xie, C. Ren, Y. Fu, J. Xu, and J. Guo, “SQL Injection Detection for Web Applications Based on Elastic-Pooling CNN,” *IEEE Access*, vol. 7, pp. 151475–151481, 2019, doi: 10.1109/ACCESS.2019.2947527.

[9] 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.

[10] K. Natarajan and S. Subramani, “Generation of Sql-injection Free Secure Algorithm to Detect and Prevent Sql-Injection Attacks,” *Procedia Technol.*, vol. 4, pp. 790–796, 2012, doi: 10.1016/j.protcy.2012.05.129.

[11] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, “A Deep Learning Ensemble Approach to Detecting Unknown Network Attacks,” *J. Inf. Secur. Appl.*, vol. 67, p. 103196, 2022, doi: 10.1016/j.jisa.2022.103196.

[12] A. Ron, A. Shulman-Peleg, and A. Puzanov, “Analysis and Mitigation of NoSQL Injections,” *IEEE Secur. Priv.*, vol. 14, no. 2, pp. 30–39, 2016, doi: 10.1109/MSP.2016.36.

[13] J. Fonseca, M. Vieira, and H. Madeira, “Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection,” *IEEE Trans. Dependable Secur. Comput.*, vol. 11, no. 5, pp. 440–453, 2014, doi: 10.1109/TDSC.2013.45.

[14] I. Medeiros, M. Beatriz, N. Neves, and M. Correia, “SEPTIC: Detecting Injection Attacks and Vulnerabilities Inside the DBMS,” *IEEE Trans. Reliab.*, vol. 68, no. 3, pp. 1168–1188, 2019, doi: 10.1109/tr.2019.2900007.

[15] L. Zhang, D. Zhang, C. Wang, J. Zhao, and Z. Zhang, “ART4SQLi: The ART of SQL Injection Vulnerability Discovery,” *IEEE Trans. Reliab.*, vol. 68, no. 4, pp. 1470–1489, 2019, doi: 10.1109/TR.2019.2910285.

[16] H. Gu *et al.*, “DIAVA: A Traffic-Based Framework for Detection of SQL Injection Attacks and Vulnerability Analysis of Leaked Data,” *IEEE Trans. Reliab.*, vol. 69, no. 1, pp. 188–202, 2020, doi: 10.1109/TR.2019.2925415.

[17] Q. Li, F. Wang, J. Wang, and W. Li, “LSTM-Based SQL Injection Detection Method for Intelligent Transportation System,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4182–4191, 2019, doi: 10.1109/TVT.2019.2893675.

[18] D. Appelt, C. D. Nguyen, A. Panichella, and L. C. Briand, “A Machine-Learning-Driven Evolutionary Approach for Testing Web Application

Firewalls," *IEEE Trans. Reliab.*, vol. 67, no. 3, pp. 733–757, 2018, doi: 10.1109/TR.2018.2805763.

[19] 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.

[20] L. Erdődi, Å. Å. Sommervoll, and F. M. Zennaro, "Simulating SQL injection vulnerability exploitation using Q-learning reinforcement learning agents," *J. Inf. Secur. Appl.*, vol. 61, no. July, p. 102903, 2021, doi: 10.1016/j.jisa.2021.102903.

[21] M. Y. Kim and D. H. Lee, "Data-mining based SQL injection attack detection using internal query trees," *Expert Syst. Appl.*, vol. 41, no. 11, pp. 5416–5430, 2014, doi: 10.1016/j.eswa.2014.02.041.

[22] R. L. Alaoui and E. H. Nfaoui, "Web attacks detection using stacked generalization ensemble for LSTMs and word embedding," *Procedia Comput. Sci.*, vol. 215, pp. 687–696, 2022, doi: 10.1016/j.procs.2022.12.070.

[23] I. S. Crespo-Martínez, A. Campazas-Vega, Á. M. Guerrero-Higueras, V. Riego-DelCastillo, C. Álvarez-Aparicio, and C. Fernández-Llamas, "SQL injection attack detection in network flow data," *Comput. Secur.*, vol. 127, 2023, doi: 10.1016/j.cose.2023.103093.

[24] Ö. Kasim, "An ensemble classification-based approach to detect attack level of SQL injections," *J. Inf. Secur. Appl.*, vol. 59, no. May, pp. 0–3, 2021, doi: 10.1016/j.jisa.2021.102852.

[25] I. Balasundaram and E. Ramaraj, "An efficient technique for detection and prevention of SQL injection attack using ASCII based string matching," *Procedia Eng.*, vol. 30, no. 2011, pp. 183–190, 2012, doi: 10.1016/j.proeng.2012.01.850.

[26] D. Litchfield, "Exploiting PL / SQL Injection With Only CREATE SESSIO Privileges in Oracle 11g," no. October, 2009.

[27] N. I. Aspriantama, “Pengujian Keamanan Sistem Informasi Uajy Menggunakan Penetration Testing,” 2021, [Online]. Available: http://e-journal.uajy.ac.id/id/eprint/24753.

[28] Y. Putra, Y. Yuhandri, and S. Sumijan, “Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting,” *J. Sistim Inf. dan Teknol.*, vol. 3, pp. 56–63, 2021, doi: 10.37034/jsisfotek.v3i2.44.

[29] A. Kurniawan, “Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based,” *J. Telemat.*, vol. 14, no. 1, pp. 9–18, 2019, [Online]. Available: https://journal.ithb.ac.id/telematika/article/view/267%0Ahttps://journal.ithb.ac.id/telematika/article/download/267/281.

[30] I. Laleb, “Analisis Cross-Site Scripting (Xss) Injection–Reflected Xss and Stored Xss Mengggunakan Framework Owasp 10,” *J. Ilm. Flash*, vol. 8, no. 1, pp. 36–42, 2023.

[31] E. Listartha, G. Arna, J. Saskara, D. Gede, and S. Santyadiputra, “Vulnerability Testing and Security Penetration on Prodi XYZ Thesis Management Web Applications,” *Sci. Comput. Sci. Informatics J.*, vol. 4, no. 2, pp. 1–14, 2021.

[32] B. Arifwidodo, Y. Syuhada, and S. Ikhwan, “Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS,” *Techno.Com*, vol. 20, no. 3, pp. 392–399, 2021, doi: 10.33633/tc.v20i3.4615.

[33] M. Moshinsky, “Analysis DictionaryAttack danModifikasi Password Cracking SertaStrategi Antisipasi,” *Nucl. Phys.*, vol. 13, no. 1, pp. 104–116, 1959.

[34] U. M. D. E. C. D. E. Los, *Intrusion Detection and Prevention System dan Keamanan Jaringan Pada Mikrotik Router*. .

[35] S. A. Valianta, T. Salim, and D. Stiawan, “Identifikasi Serangan Port Scanning dengan Metode String Matching,” *Annu. Res. Semin.*, vol. 2, no.

Fakultas Ilmu Komputer Unsri, pp. 466–471, 2016.

[36] J. Chandra, H. Hermanto, and A. Rahman, “Deteksi Serangan Port Scanning Menggunakan Algoritma Naive Bayes,” *Julyxxxx*, vol. x, No.x, no. x, pp. 1–5, 2021.

[37] M. Anif, S. Hws, and M. D. Huri, “Penerapan Intrusion Detection System ( IDS ) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang,” *J. TELE, Vol. 13 Nomor 1*, vol. 13, no. 1, pp. 25–30, 2015.

[38] E. Guanabara, K. Ltda, E. Guanabara, and K. Ltda, “Membandingkan analisa trafic data pada jaringan komputer antara wireshark dan NMAP.”

[39] E. Manalu, F. A. Sianturi, and M. R. Manalu, “Penerapan Algoritma Naive Bayes Untuk Memprediksi Jumlah Produksi Barang Berdasarkan Data Persediaan dan Jumlah Pemesanan Pada CV. Papadan Mama Pastries,” *J. Mantik Penusa*, vol. 1, no. 2, pp. 16–21, 2017.

[40] D. Wahyuningsih and E. Patima, “Penerapan Naive Bayes Untuk Penerimaan Beasiswa,” *Telematika*, vol. 11, no. 1, p. 135, 2018, doi: 10.35671/telematika.v11i1.665.

[41] A. Saleh, “Penerapan Data Mining Dengan Metode Klasifikasi Naïve Bayes Untuk Memprediksi Kelulusan Mahasiswa Dalam Mengikuti English Proficiency Test,” *Univ. Potensi Utama*, no. June, pp. 1–6, 2015.

[42] D. Alita and A. R. Isnain, “Pendeteksian Sarkasme pada Proses Analisis Sentimen Menggunakan Random Forest Classifier,” *J. Komputasi*, vol. 8, no. 2, pp. 50–58, 2020, doi: 10.23960/komputasi.v8i2.2615.

[43] * P., A. Sunyoto, and E. Pramono, “Deteksi Serangan SQL Injection Menggunakan Hidden Markov Model,” *J. Tecnoscienza*, vol. 5, no. 2, p. 243, 2021, doi: 10.51158/tecnoscienza.v5i2.432.

[44] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.