DAFTAR PUSTAKA

[1] IBMSecurity, “Cost of a Data Breach Report 2024,” IBM Corporation. [Daring]. Tersedia pada: https://www.ibm.com/reports/data-breach

[2] BSSN, “Laporan Tahunan 2023: Monitoring Keamanan Siber Nasional,” Badan Siber dan Sandi Negara. [Daring]. Tersedia pada: https://bssn.go.id

[3] OWASP, “OWASP Top 10 Web Application Security Risks 2023,” OWASP Foundation. [Daring]. Tersedia pada: https://owasp.org/www-project-top-ten

[4] B. Işiker dan I. Soğukpinar, “Machine Learning Based Web Application Firewall,” dalam *2nd International Informatics and Software Engineering Conference, IISEC 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/IISEC54230.2021.9672335.

[5] A. Shaheed dan M. H. D. B. Kurdy, “Web Application Firewall Using Machine Learning and Features Engineering,” *Security and Communication Networks*, vol. 2022, hlm. 1–14, Jun 2022, doi: 10.1155/2022/5280158.

[6] S. Toprak dan A. G. Yavuz, “Web Application Firewall Based on Anomaly Detection using Deep Learning,” *Acta Infologica*, vol. 6, no. 2, hlm. 219–244, Okt 2022, doi: 10.26650/acin.1039042.

[7] P. Van Hau dan D. T. T. Hien, “Enhancing Web Application Security: A Deep Learning and NLP-based Approach for Accurate Attack Detection,” *Journal of Science and Technology on Information Security*, vol. 20, no. 3, hlm. 77–87, Des 2023, doi: https://doi.org/10.54654/isj.v3i20.

[8] F. Shradha, G. Rutuja, C. Sakshi, A. Khushi, dan K. Srushti, “Detection of Cyber-Attacks and Network Attacks Using Machine Learning,” *World Journal of Advanced Engineering Technology and Sciences*, vol. 12, no. 1, hlm. 128–132, Mei 2024, doi: 10.30574/wjaets.2024.12.1.0184.

[9] A. M. Alnajim, S. Habib, M. Islam, S. M. Thwin, dan F. Alotaibi, “A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things,” *Technologies (Basel).*, vol. 11, no. 6, 2023, doi: 10.3390/technologies11060161.

[10] W. B. Demilie dan F. G. Deriba, “Detection and Prevention of SQLI Attacks and Developing Compressive Framework Using Machine Learning and Hybrid Techniques,” *J. Big Data*, vol. 9, no. 1, hlm. 1–30, Des 2022, doi: 10.1186/s40537-022-00678-0.

[11] I. Riadi, A. Z. Ifani, S. Informasi, U. A. Dahlan, T. Informatika, dan U. A. Dahlan, “Optimasi Keamanan Web Server terhadap Serangan Broken Authentication Menggunakan Teknologi Blockchain,” *JISKa*, vol. 6, no. 3, hlm. 139–148, 2021.

[12] L. Bernardo, S. Malta, dan J. Magalhães, “An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF,” *Electronics (Switzerland)*, vol. 14, no. 7, 2025, doi: 10.3390/electronics14071364.

[13] F. M. Alotaibi dan V. G. Vassilakis, “Toward an SDN-Based Web Application Firewall: Defending against SQL *Injection* Attacks,” *Future Internet*, vol. 15, no. 5, 2023, doi: 10.3390/fi15050170.

[14] G. E. Cárdenas Rosero, C. P. Guevara Vega, dan P. Landeta-López, “Website Protection: An Evaluation of the Web Application Firewall,” *Data and Metadata*, vol. 4, 2025, doi: 10.56294/DM2025190.

[15] M. E. Durmuşkaya dan S. Bayraklı, “Web application firewall based on machine learning models,” *PeerJ Comput. Sci.*, vol. 11, hlm. e2975, 2025, doi: 10.7717/peerj-cs.2975.

[16] C. Fan, M. Chen, X. Wang, J. Wang, dan B. Huang, “A Review on Data Preprocessing Techniques Toward Efficient and Reliable Knowledge Discovery From Building Operational Data,” *Front. Energy Res.*, vol. 9, no. March, hlm. 1–17, 2021, doi: 10.3389/fenrg.2021.652801.

[17] J. Yin, C. Zhang, W. Xie, G. Liang, L. Zhang, dan G. Gui, “Anomaly traffic detection based on feature fluctuation for secure industrial internet of things,” *Peer. Peer. Netw. Appl.*, vol. 16, no. 4, hlm. 1680–1695, 2023, doi: 10.1007/s12083-023-01482-0.

[18] Y. Zhang dan Z. Wang, “Feature Engineering and Model Optimization Based Classification Method for Network Intrusion Detection,” *Applied Sciences (Switzerland)*, vol. 13, no. 16, hlm. 1–25, 2023, doi: 10.3390/app13169363.

[19] D. J. C. Sihombing, “Application of Feature Engineering Techniques and Machine Learning Algorithms for Property Price Prediction,” *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 5, no. 2, hlm. 72–76, 2024, doi: 10.62527/jitsi.5.2.241.

[20] C. Singh, V. Vijayalakshmi, dan H. Raj, “A Machine Learning Approach for Web Application Vulnerability Detection Using *Random Forest*,” *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 10, no. 12, hlm. 2106–2112, Des 2022, doi: 10.22214/ijraset.2022.48397.

[21] I. M. Alkhawaldeh, I. Albalkhi, dan A. J. Naswhan, “Challenges and Limitations of Synthetic Minority Oversampling Techniques in Machine Learning,” *World J. Methodol.*, vol. 13, no. 5, hlm. 373–378, 2023, doi: 10.5662/wjm.v13.i5.373.

[22] J. Allgaier dan R. Pryss, “Cross-Validation Visualized: A Narrative Guide to Advanced Methods,” *Mach. Learn. Knowl. Extr.*, vol. 6, no. 2, hlm. 1378–1388, 2024, doi: 10.3390/make6020065.

[23] S. Moslehi, N. Rabiei, A. R. Soltanian, dan M. Mamani, “Application of Machine Learning Models Based on *Decision Tree*s in Classifying The Factors Affecting Mortality of COVID-19 Patients in Hamadan, Iran,” *BMC Med. Inform. Decis. Mak.*, vol. 22, no. 1, hlm. 1–12, 2022, doi: 10.1186/s12911-022-01939-x.

[24] A. A. Hani *dkk.*, “Comparative Analysis of State-of-the-Art Classifiers for Parkinson’S Disease Diagnosis With Techonlogy,” *Jurnal Ilmiah Ilmu Terapan Universitas Jambi*, vol. 8, no. 2, hlm. 409–423, 2024, doi: 10.22437/jiituj.v8i2.32771.

[25] D. Boldini, F. Grisoni, D. Kuhn, L. Friedrich, dan S. A. Sieber, “Practical Guidelines for The Use of Gradient Boosting for Molecular Property Prediction,” *J. Cheminform.*, vol. 15, no. 1, hlm. 1–13, 2023, doi: 10.1186/s13321-023-00743-7.

[26] M. Environments, “XGBLoc: XGBoost-Based Indoor Localization in Multi-Building Multi-Floor Environments,” *Sensors*, vol. 22, no. 17, hlm. 1–17, 2022, doi: 10.3390/s22176629.

[27] Y. A. Ali, E. M. Awwad, M. Al-Razgan, dan A. Maarouf, “Hyperparameter Search for Machine Learning Algorithms for Optimizing the Computational Complexity,” *Processes*, vol. 11, no. 2, 2023, doi: 10.3390/pr11020349.

[28] R. Laipaka, N. Mustika, dan O. R. Runda, “Penerapan Jupyter Notebook Pada Anaconda Navigator Untuk Visualisasi Data (Studi Kasus : Kapal Titanic),” *Prosiding Seminar Nasional Pengabdian Kepada Masyarakat*, vol. 1, no. 1, hlm. 388–395, 2021, [Daring]. Tersedia pada: https://ejournal.raharja.ac.id/index.php/corisindo/article/view/2438

UPT. PERPUSTAKAAN PUSAT
UNIVERSITAS KATOLIK WIDYA MANDIRA KUPANG
Nomor Pokok Perpustakaan: 5371002D2020114
Jl. Prof Dr. Herman Johanes, Penfui Timur, Kupang Tengah, Kab. Kupang.
Website: https://perpustakaan.unwira.com/ e-mail: lib.unwira@gmail.com

SURAT KETERANGAN HASIL CEK PLAGIASI
Nomor: 0062/WM.H16/SK.CP/2026

Dengan ini menerangkan bahwa:

Nama	:	Joseray Arimateia Lopes Da Cruz
NIM	:	23122196
Fakultas/Prodi	:	Teknik/Ilmu Komputer
Dosen Pembimbing	:	1. Yulianti Paula Bria, S.T., M.T., Ph.D. 2. Donatus Joseph Manehat, S.Si., M.Kom.
Judul Skripsi/Thesis	:	**MODEL *WEB APPLICATION FIREWALL* BERBASIS *MACHINE LEARNING* UNTUK MENCEGAH SERANGAN SIBER**

Skripsi/Thesis yang bersangkutan di atas telah melalui proses cek plagiasi menggunakan Turnitin dengan hasil kemiripan (*similarity*) sebesar **8 (Delapan)%.**
Demikian surat keterangan ini dibuat agar dapat dipergunakan sebagaimana mestinya.

Kupang, 09 Februari 2026
Kepala UPT Perpustakaan,

Damianus Dami, S.Ptk.