BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, dapat ditarik beberapa kesimpulan dari penelitian mengenai pengembangan sistem *Web Application Firewall* berbasis *Machine Learning* sebagai berikut:

1. Penelitian ini berhasil mengembangkan sistem *Web Application Firewall* berbasis *Machine Learning* yang mampu mendeteksi dan memblokir serangan *SQL Injection* dan *Cross-Site Scripting (XSS)* pada aplikasi *web*. Sistem dibangun dengan mengintegrasikan *model Machine Learning* ke dalam aplikasi *web* melalui mekanisme *middleware* dan layanan *API*, sehingga setiap *request* dapat diperiksa sebelum diproses oleh aplikasi.
2. Hasil pengujian *model Machine Learning* menunjukkan bahwa model *Random Forest* memberikan performa yang lebih baik dibandingkan *Decision Tree* dalam mendeteksi serangan *SQL Injection* dan *XSS*. *Random Forest* mampu menghasilkan tingkat akurasi yang tinggi di angka 99,54% untuk pengujian *SQL Injection* dan 100% pada pengujian *XSS,* serta memberikan nilai *false negative* 12 untuk pengujian *SQL Injection* dan 0 untuk pengujian *XSS*, sehingga lebih andal untuk digunakan dalam sistem keamanan aplikasi *web*.
3. Pengujian sistem secara *end-to-end* menunjukkan bahwa integrasi model Machine Learning ke dalam sistem *WAF* berjalan sesuai dengan rancangan. *Middleware WAF* berfungsi efektif sebagai lapisan pengaman awal yang mampu memblokir *request* berbahaya dan tetap mengizinkan *request* normal untuk diproses oleh aplikasi tanpa gangguan.
4. Hasil pengujian *black box* membuktikan bahwa sistem *WAF* berbasis *Machine Learning* berfungsi secara fungsional dan stabil. Seluruh skenario pengujian, termasuk *request* normal, serangan *SQL Injection*, serangan *XSS*, serta kondisi kesalahan, dapat ditangani dengan baik sesuai dengan hasil yang diharapkan.

5. Secara keseluruhan, sistem *WAF* berbasis *Machine Learning* yang dikembangkan tidak hanya efektif secara teoritis melalui pengujian *model*, tetapi juga efektif secara implementatif dalam meningkatkan keamanan aplikasi *web*. Dengan demikian, tujuan penelitian untuk mengembangkan sistem keamanan aplikasi *website* berbasis *Machine Learning* telah tercapai.

5.2 Saran

Berdasarkan hasil penelitian dan keterbatasan yang telah diidentifikasi, terdapat beberapa saran yang dapat dipertimbangkan untuk pengembangan dan penelitian selanjutnya, yaitu:

1. Penelitian selanjutnya dapat memperluas jenis serangan yang dideteksi oleh sistem *WAF*, tidak hanya terbatas pada *SQL Injection* dan *Cross-Site Scripting (XSS)*, tetapi juga mencakup jenis serangan lain seperti *Command Injection, Directory Traversal,* dan *file inclusion*.
2. Pengujian sistem dapat dikembangkan lebih lanjut dengan menerapkan sistem *WAF* pada lingkungan produksi atau simulasi trafik nyata dengan beban yang lebih tinggi, sehingga performa sistem dapat dievaluasi pada kondisi yang lebih kompleks dan dinamis.
3. *Model Machine Learning* dapat dikembangkan dengan memanfaatkan *dataset* yang lebih besar dan beragam, serta mencoba pendekatan *model* lain atau teknik *ensemble* tambahan untuk meningkatkan kemampuan generalisasi sistem dalam mendeteksi pola serangan baru.
4. Pengembangan sistem selanjutnya dapat mempertimbangkan integrasi dengan mekanisme keamanan tambahan, seperti analisis perilaku pengguna *(behavior-based detection)* atau sistem pemantauan *real-time*, guna meningkatkan tingkat keamanan aplikasi *web* secara menyeluruh.

DAFTAR PUSTAKA

Alfando, A., & Hayami, R. (2023). Klasifikasi Teks Berita Berbahasa Indonesia Menggunakan Machine Learning Dan Deep Learning: Studi Literatur. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(1), 681–686.

Andini, N., Taufiq, R., Priyanggodo, D. Y., & Sugiyani, Y. (2023). Penggunaan Metode Prototype Pada Pengembangan Sistem Informasi Imunisasi Posyandu. *JIKA (Jurnal Informatika)*, *7*(4), 431–439.

Ardiansyah, Y., Sunandar, M. A., & Muhyidin, Y. (2023). Implementasi Keamanan Website Dengan Metode Firewall Aplikasi Web (WAF). *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(3), 2018–2025.

Arumuga Maria Devi, T., Akshay Kumar, B., & security, Ms. (n.d.). *Machine Learning with Logistic Regression for Web Application Firewall*. www.ijert.org

Asan Nainar, M. M., & Sibikarthik, B. K. (2025). *ML-Enhanced Behavioral & Anomaly Detection Web Application Firewall*.

Aydos, M., Aldan, Ç., Coşkun, E., & Soydan, A. (2022). Security testing of web applications: A systematic mapping of the literature. *Journal of King Saud University - Computer and Information Sciences*, *34*(9), 6775–6792. https://doi.org/https://doi.org/10.1016/j.jksuci.2021.09.018

Budiman, A., Ahdan, S., & Aziz, M. N. A. (2021). Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment. In *Jurnal Komputasi*. https://doi.org/10.23960/komputasi.v9i2.2800

Cloudlflare. (n.d.). *What is SQL injection?* Cloudflare Learning Centre. Retrieved November 6, 2025, from https://www.cloudflare.com/learning/security/threats/sql-injection/

Dawadi, B. R., Adhikari, B., & Srivastava, D. K. (2023). Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks. In *Sensors*. https://doi.org/10.3390/s23042073

Durmuşkaya, M. E., & Bayraklı, S. (2025). Web application firewall based on machine learning models. *PeerJ Computer Science*, *11*, e2975. https://doi.org/10.7717/peerj-cs.2975

Felício, D., Simão, J., & Datia, N. (2023). RapiTest: Continuous Black-Box Testing of RESTful Web APIs. *Procedia Computer Science*, *219*, 537–545. https://doi.org/https://doi.org/10.1016/j.procs.2023.01.322

Gustiyonoo, A., Alwi, E. I., & Abdullah, S. M. (2024). Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing. *Cyber Security Dan Forensik Digital*, *7*(1), 25–33.

Harahap, B. (2021). Penerapan Keamanan Owasp Terhadap Aplikasi GTFW Pada Website Universitas Battuta. *Jurnal Informatika Dan Teknologi Pendidikan*, *1*(2), 80–86.

Hartama, D., Amalya, N., Studi, P., Informatika, T., Tunas Bangsa, S., Pematangsiantar, K., & Sumatra, P. (2025). Perbandingan Algoritma Decision Tree, ID3, dan Random Forest dalam Klasifikasi Faktor-Faktor yang Mempengaruhi Karier Mahasiswa Ilmu Komputer. In *Jurnal Indonesia : Manajemen Informatika dan Komunikasi (JIMIK)* (Vol. 6, Issue 1). https://journal.stmiki.ac.id

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 210–216.

Kepuska, K., & Tomašević, M. (2024). A Lightweight Framework for Cyber Risk Management in Western Balkan Higher Education Institutions. In *Peerj Computer Science*. https://doi.org/10.7717/peerj-cs.1958

KeyCDN. (2023, March 17). *Web Application Firewall*. https://www.keycdn.com/support/web-application-firewall

Liu, A. J., Mukherjee, A., Hu, L., Chen, J., & Nair, V. N. (n.d.). *Performance and Interpretability Comparisons of Supervised Machine Learning Algorithms: An Empirical Study 1*.

Mani, K., & Shenoy, A. K. B. (2025a). Machine learning models in web applications: A comprehensive review. In *ICT Express*. Korean Institute of Communications and Information Sciences. https://doi.org/10.1016/j.icte.2025.09.001

Mani, K., & Shenoy, A. K. B. (2025b). Machine learning models in web applications: A comprehensive review. *ICT Express*, *11*(6), 1110–1119. https://doi.org/https://doi.org/10.1016/j.icte.2025.09.001

Nair, S. (2024). Securing Against Advanced Cyber Threats: A Comprehensive Guide to Phishing, XSS, and SQL Injection Defense. In *Journal of Computer Science and Technology Studies*. https://doi.org/10.32996/jcsts.2024.6.1.9

Nurhalizah, R. S., Ardianto, R., & Purwono, P. (2024). Analisis Supervised dan Unsupervised Learning pada Machine Learning: Systematic Literature Review. *Jurnal Ilmu Komputer Dan Informatika*, *4*(1), 61–72.

Okta. (2024, August). *Black-Box Testing: Definition, Types & Techniques*. https://www.okta.com/identity-101/black-box-testing/

Ramadhan, R. F., & Ashari, W. M. (2024). Performance Comparison of Random Forest and Decision Tree Algorithms for Anomaly Detection in Networks. In *Journal of Applied Informatics and Computing (JAIC)* (Vol. 8, Issue 2). http://jurnal.polibatam.ac.id/index.php/JAIC

Samyuktha Patnaik. (2022). *Decision Tree*. https://github.com/SamyukthaPatnaik/Decision-Tree?tab=readme-ov-file

Santi, P. A. D. A., Afwani, R., Albar, Moh. A., Anjarwani, S. E., & Mardiansyah, A. Z. (2022). Black Box Testing with Equivalence Partitioning and Boundary Value Analysis Methods (Study Case: Academic Information System of Mataram University). In *Proceedings of the First Mandalika International Multi-Conference on Science and Engineering 2022, MIMSE 2022 (Informatics and Computer Science)* (pp. 207–219). Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-084-8_19

Shaheed, A., & Kurdy, M.-B. (2022). Web Application Firewall Using Machine Learning and Features Engineering. In *Security and Communication Networks*. https://doi.org/10.1155/2022/5280158

Sidik, A. D., & Ansawarman, A. (2022). Prediksi jumlah kendaraan bermotor menggunakan machine learning. *Formosa Journal of Multidisciplinary Research*, *1*(3), 559–568.

Sun, H., Du, Y., & Li, Q. (2023). Deep Learning-Based Detection Technology for SQL Injection Research and Implementation. *Applied Sciences (Switzerland)*, *13*(16). https://doi.org/10.3390/app13169466

whatismyipaddress. (n.d.). *Cross-Site Scripting (XSS): How to Protect Your Website from Attacks*. What Is XSS. Retrieved November 6, 2025, from https://whatismyipaddress.com/what-is-xss

Wikipedia contributors. (2025). *Latency (engineering) — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Latency_(engineering)&oldid=1316659772

Will Koehrsen. (2017). *Random Forest in Python*. Towards Data Science. https://towardsdatascience.com/random-forest-in-python-24d0893d51c0/