DAFTAR RUJUKAN

[1] ‘Top 10 Trending Technologies - Must Learn In 2021’, *Edureka*, Dec. 22, 2017. https://www.edureka.co/blog/top-10-trending-technologies/ (accessed Nov. 06, 2021).

[2] ‘Top 9 New Technology Trends for 2021’, *Simplilearn.com*, Aug. 08, 2018. https://www.simplilearn.com/top-technology-trends-and-jobs-article (accessed Nov. 06, 2021).

[3] D. I. R. A. G. G. M.Sc, *Cyber Warfare: Sudah Siapkah Kita Menghadapinya?* UNHAN Press, 2021.

[4] ‘Cybersecurity Statistics for 2021’, *Packetlabs*, Aug. 03, 2021. https://www.packetlabs.net/cybersecurity-statistics-2021/ (accessed Nov. 05, 2021).

[5] ‘Protecting against cyber threats during COVID-19 and beyond’, *Google Cloud Blog*. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond/ (accessed Nov. 05, 2021).

[6] ‘How Many Cyber Attacks Happen Per Day? [2021 Stats and Facts]’, *TechJury*, Jul. 15, 2020. https://techjury.net/blog/how-many-cyber-attacks-per-day/ (accessed Nov. 05, 2021).

[7] ‘2021 Cyber Security Statistics Trends & Data’, *PurpleSec*, Nov. 08, 2020. https://purplesec.us/resources/cyber-security-statistics/ (accessed Nov. 05, 2021).

[8] ‘Cost of a Data Breach Report 2020’, p. 82.

[9] A. Yusuf, *Laporan Tahunan 2020 Honeynet Project BSSN - IHP*. Badan Siber dan Sandi Negara, 2020.

[10] ‘Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun - Teknologi Katadata.co.id’, Jun. 25, 2021. https://katadata.co.id/desysetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehatan-disebut-bikin-rugi-negara-rp-600-triliun (accessed Nov. 11, 2021).

[11] M. Akbar and M. A. F. Ridha, ‘SQL Injection and Cross Site Scripting Prevention Using OWASP Web Application Firewall’, p. 7.

[12] Y. Putra, Y. Yunus, and S. Sumijan, ‘Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) Terhadap Seragan Cross Site Scripting’, *JSisfotek*, Sep. 2020, doi: 10.37034/jsisfotek.v3i2.110.

[13] Y. Yulianingsih, ‘Melindungi Aplikasi dari Serangan Cross Site Scripting dengan Metode Metacharacter’, *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 3, no. 1, Art. no. 1, Apr. 2017, doi: 10.25077/TEKNOSI.v3i1.2017.83-88.

[14] M. F. Kurniawan and W. Setianto, ‘Optimasi Metode Otomatisasi Penghilangan Kerentanan Terhadap Serangan XSS Pada Aplikasi Web’, no. 2, p. 8, 2020.

[15] A. Anggara and R. Somya, ‘Pengembangan Sistem Informasi Manajemen Persediaan Barang Dagang Berbasis Web menggunakan Library XSS Filtering’, p. 7, 2021.

[16] D. A. Prasetio, K. Kusrini, and M. R. Arief, ‘Cross-site Scripting Attack Detection Using Machine Learning with Hybrid Features’, *J.INFOTEL*, vol. 13, no. 1, pp. 1–6, Feb. 2021, doi: 10.20895/infotel.v13i1.606.

[17] A. Amruthavalli *et al.*, ‘Machine Learning for Web Vulnerability detection: The Case of Cross Site Request Forgery’, vol. 12, no. 6, pp. 121–131, 2021.

[18] M. N. Khalid, H. Farooq, M. Iqbal, M. T. Alam, and K. Rasheed, ‘Predicting web vulnerabilities in web applications based on machine learning’, 2018, pp. 473–484.

[19] S. Calzavara, M. Conti, R. Focardi, A. Rabitti, and G. Tolomei, ‘Machine Learning for Web Vulnerability Detection: The Case of Cross-Site Request Forgery’, *IEEE Secur. Privacy*, vol. 18, no. 3, pp. 8–16, May 2020, doi: 10.1109/MSEC.2019.2961649.

[20] I. Jemal, O. Cheikhrouhou, H. Hamam, and A. Mahfoudhi, ‘SQL Injection Attack Detection and Prevention Techniques Using Machine Learning’, vol. 15, no. 6, p. 12, 2020.

[21] K. D. Ayunda, A. Widjajarto, and A. Budiono, ‘Implementation and Analysis ModSecurity on Web-Based Application with OWASP Standards’, vol. 8, no. 3, p. 12, 2021.

[22] T. D. Sobola, P. Zavarsky, and S. Butakov, ‘Experimental Study of ModSecurity Web Application Firewalls’, in *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, Baltimore, MD, USA,

May 2020, pp. 209–213. doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00045.

[23] J.-M. Grunwaldt, ‘A Comparison of Modern Backend Frameworks Protections against Common Web Vulnerabilities’, p. 9.

[24] M. Kaluza, M. Kalanj, and B. Vukelić, ‘A Comparison of Back-end Framework for Web Application Development’, *Zbornik Veleučilišta u Rijeci*, vol. 7, no. 1, pp. 317–332, May 2019, doi: 10.31784/zvr.7.1.10.

[25] F. M. M. Mokbal, W. Dan, A. Imran, L. Jiuchuan, F. Akhtar, and W. Xiaoxi, ‘MLPXSS: An Integrated XSS-Based Attack Detection Scheme in Web Applications Using Multilayer Perceptron Technique’, *IEEE Access*, vol. 7, pp. 100567–100580, 2019, doi: 10.1109/ACCESS.2019.2927417.

[26] B. Buz, B. GülçiÇek, and Ş. BahtiYar, ‘A Hybrid Machine Learning Model to Detect Reflected XSS Attack’, *Balkan Journal of Electrical and Computer Engineering*, Aug. 2021, doi: 10.17694/bajece.927417.

[27] A. W. Marashdih and Z. F. Zaaba, ‘Cross Site Scripting: Removing Approaches in Web Application’, *Procedia Computer Science*, vol. 124, pp. 647–655, 2017, doi: 10.1016/j.procs.2017.12.201.

[28] B. B. Gupta, S. Gupta, S. Gangwar, M. Kumar, and P. K. Meena, ‘Cross-Site Scripting (XSS) Abuse and Defense: Exploitation on Several Testing Bed Environments and Its Defense’, *Journal of Information Privacy and Security*, vol. 11, no. 2, pp. 118–136, Apr. 2015, doi: 10.1080/15536548.2015.1044865.

[29] M. Hasan, Z. Balbahaith, and M. Tarique, ‘Detection of SQL Injection Attacks: A Machine Learning Approach’, in *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, Ras Al Khaimah, United Arab Emirates, Nov. 2019, pp. 1–6. doi: 10.1109/ICECTA48151.2019.8959617.

[30] B. Kranthikumar and R. L. Velusamy, ‘SQL injection detection using REGEX classifier’, p. 10, 2020.

[31] P. Singh, K. Thevar, P. Shetty, and B. Shaikh, ‘Detection of SQL Injection and XSS Vulnerability in Web Application’, *IJEAS*, vol. 2, no. 3, p. 257981, Mar. 2015.

[32] J. Zhao, Y. Lu, K. Zhu, Z. Chen, and H. Huang, ‘Cefuzz: An Directed Fuzzing Framework for PHP RCE Vulnerability’, *Electronics*, vol. 11, no. 5, p. 758, Mar. 2022, doi: 10.3390/electronics11050758.

[33] M. Triwibowo, ‘Deteksi dan Pencegahan Serangan Remote Code Execution Terhadap WING FTP Web Server Menggunakan SNORT’. Universitas Muhammadiyah Surakarta, 2016.

[34] S. Biswas, ‘A Study on Remote Code Execution Vulnerability in Web Applications’, p. 8, 2018.

[35] S. Mishra, ‘SQL Injection Detection Using Machine Learning’, Master of Science, San Jose State University, San Jose, CA, USA, 2019. doi: 10.31979/etd.j5dj-ngvb.

[36] A. P. Sagane and S. S. Dhande, ‘Malicious Code Detection Using Naïve Bayes Classifier.’, vol. 3, no. 4, p. 5, 2014.

[37] W. Stallings, *Effective cybersecurity: understanding and using standards and best practices*. Upper Saddle River, NJ: Addison-Wesley, 2019.

[38] M. U. Bokhari, N. Agrawal, and D. Saini, Eds., *Cyber Security: Proceedings of CSI 2015*, vol. 729. Singapore: Springer Singapore, 2018. doi: 10.1007/978-981-10-8536-9.

[39] S. E. Donaldson, S. G. Siegel, C. K. Williams, and A. Aslam, *Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats*. New York, NY: Apress, 2015.

[40] B. Akhgar, A. Staniforth, and F. Bosco, ‘Cyber Crime and Cyber Terrorism Investigator’s Handbook’, p. 399.

[41] N. Lee, *Counterterrorism and Cybersecurity*. Cham: Springer International Publishing, 2015. doi: 10.1007/978-3-319-17244-6.

[42] A. F. Doss, *Cyber privacy: who has your data and why you should care*. Dallas, TX: BenBella Books, Inc, 2020.

[43] K. Odayan, ‘Artificial Intelligence controlling Cyber Security’, p. 190.

[44] D. Cherry, ‘Securing SQL Server: Protecting Your Database from Attacker 3rd Edition’, in *Securing SQL Server*, Elsevier, 2015, p. iii. doi: 10.1016/B978-0-12-801275-8.00016-6.

[45] S. Sen, S. Patel, and P. Richhariya, ‘A Critical Review for Remote Code Execution Vulnerability Detection’, p. 8.

[46] S. -, I. Riadi, and P. Ananda, ‘Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework’, *IJACSA*, vol. 10, no. 11, 2019, doi: 10.14569/IJACSA.2019.0101118.

[47] H. Kim and D.-C. Kim, Eds., *Information Security and Cryptology – ICISC 2017: 20th International Conference, Seoul, South Korea, November 29 - December 1, 2017, Revised Selected Papers*, vol. 10779. Cham: Springer International Publishing, 2018. doi: 10.1007/978-3-319-78556-1.

[48] OWASP, 'A04 Insecure Design - OWASP Top 10:2021'. https://owasp.org/Top10/A04_2021-Insecure_Design/ (accessed Nov. 18, 2021).

[49] Y. Diogenes, E. Ozkaya, and Safari Books Online (Firm), *Cybersecurity - Attack and Defense Strategies - Second Edition*. 2019. Accessed: Nov. 12, 2021. [Online]. Available: https://safarijv.auth0.com/authorize?client_id=UtNi1m1IRXgzYFIwZrhSxell9EDRaL2v&response_type=code&connection=queensland-university-of-technology&redirect_uri=https://www.safaribooksonline.com/complete/auth0-oauth2/&state=/library/view/-/9781838827793/?ar

[50] 'A06 Vulnerable and Outdated Components - OWASP Top 10:2021'. https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/ (accessed Nov. 18, 2021).

[51] F. Cleary and M. Felici, Eds., *Cyber Security and Privacy*, vol. 530. Cham: Springer International Publishing, 2015. doi: 10.1007/978-3-319-25360-2.

[52] 'A08 Software and Data Integrity Failures - OWASP Top 10:2021'. https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/ (accessed Nov. 18, 2021).

[53] 'A09 Security Logging and Monitoring Failures - OWASP Top 10:2021'. https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/ (accessed Nov. 18, 2021).

[54] B. Jabiyev, O. Mirzaei, A. Kharraz, and E. Kirda, 'Preventing server-side request forgery attacks', in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, Virtual Event Republic of Korea, Mar. 2021, pp. 1626–1635. doi: 10.1145/3412841.3442036.

[55] V. K. Singh and M. Govindarasu, 'A Cyber-Physical Anomaly Detection for Wide-Area Protection Using Machine Learning', *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3514–3526, Jul. 2021, doi: 10.1109/TSG.2021.3066316.

[56] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, 'A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids', *IEEE Access*, vol. 7, pp. 80778–80788, 2019, doi: 10.1109/ACCESS.2019.2920326.

[57] V. Dutta, M. Choraś, M. Pawlicki, and R. Kozik, ‘A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection’, *Sensors*, vol. 20, no. 16, p. 4583, Aug. 2020, doi: 10.3390/s20164583.

[58] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. 2016. Accessed: Nov. 16, 2021. [Online]. Available: https://go.oreilly.com/university-of-alberta/library/view/-/9781439839430/?ar

[59] J. Herron, ‘Machine Learning: The Ultimate Guide for Beginners to Programming and Deep Learning With Python.’, p. 86.

[60] J. Bell, *Machine learning: hands-on for developers and technical professionals*, 2nd ed. Indianapolis: John Wiley & Son Ltd, 2020.

[61] J. P. Mueller and L. Massaron, *Machine learning for dummies*, 2nd edition. Indianapolis: John Wiley & Sons, 2021.

[62] Y. Xin *et al.*, ‘Machine Learning and Deep Learning Methods for Cybersecurity’, *IEEE Access*, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[63] E. Tsukerman, *Machine learning for cybersecurity cookbook: over 80 recipes on how to implement machine learning algorithms for building security systems using Python*. 2019.

[64] S. Bird, ‘Natural Language Processing with Python’, p. 504.

[65] Z. ANTIC, *PYTHON NATURAL LANGUAGE PROCESSING COOKBOOK over 50 recipes to understand, analyze, and generate... different texts to implement language processing t.* S.l.: PACKT PUBLISHING LIMITED, 2021.

[66] T. Rains and an O. M. C. Safari, *Cybersecurity Threats, Malware Trends, and Strategies*. 2020. Accessed: Nov. 22, 2021. [Online]. Available: https://learning.oreilly.com/library/view/-/9781800206014/?ar

[67] P. Ganapathi and D. Shanmugapriya, Eds., *Handbook of Research on Machine and Deep Learning Applications for Cyber Security:* IGI Global, 2020. doi: 10.4018/978-1-5225-9611-0.

[68] M. Woschek, ‘OWASP Cheat Sheets’, p. 315.

[69] G. Weidman, *Penetration testing: a hands-on introduction to hacking*. San Francisco: No Starch Press, 2014.

[70] ‘Framework’, *Arachni - Web Application Security Scanner Framework*, Mar. 10, 2013. https://www.arachni-scanner.com/features/framework/ (accessed Nov. 22, 2021).

[71] D. Thakkar, *Preventing Digital Extortion.* Birmingham: Packt Publishing, 2017. Accessed: Nov. 22, 2021. [Online]. Available: http://www.myilibrary.com?id=1013213

[72] J. Chen *et al.*, 'A Multi-Layer Security Scheme for Mitigating Smart Grid Vulnerability against Faults and Cyber-Attacks', *Applied Sciences*, vol. 11, no. 21, p. 9972, Oct. 2021, doi: 10.3390/app11219972.

[73] Z. Fan, Q. Xu, W. Zhu, and C. Tan, 'A Cyber Attack Situation Evaluating Method Based on Multi-Dimensional Features Analysis in SDNs', vol. 30, no. 5, p. 20, 2019.

[74] B. Miller and X. Zhang, 'A MULTI-LAYER APPROACH TO DETECTING AND PREVENTING IOT-BASED BOTNET ATTACKS', *IIS*, 2020, doi: 10.48009/3_iis_2020_168-178.

[75] G. Betarte, E. Gimenez, R. Martinez, and A. Pardo, 'Improving Web Application Firewalls through Anomaly Detection', in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Orlando, FL, Dec. 2018, pp. 779–784. doi: 10.1109/ICMLA.2018.00124.

[76] P. Prabhudesai, A. A. Bhalerao, and R. Prabhudesai, 'Web Application Firewall: Artificial Intelligence Arc', vol. 06, no. 04, p. 4, 2019.

[77] 'Web application firewalls bypasses collection and testing tools', *Web application firewalls bypasses collection and testing tools*. https://waf-bypass.com/ (accessed Nov. 22, 2021).

[78] '10 Best Web Development Frameworks to Use in 2021 [Updated]', *Hackr.io*. https://hackr.io/blog/web-development-frameworks (accessed Nov. 23, 2021).

[79] 'How Secure Are Popular Web Frameworks? Here Is a Comparison', *Veracode*. https://www.veracode.com/blog/secure-development/how-secure-are-popular-web-frameworks-here-comparison (accessed Nov. 23, 2021).

[80] J.-M. Martinez-Caro, A.-J. Aledo-Hernandez, A. Guillen-Perez, R. Sanchez-Iborra, and M.-D. Cano, 'A Comparative Study of Web Content Management Systems', *Information*, vol. 9, no. 2, p. 27, Jan. 2018, doi: 10.3390/info9020027.

[81] C. A. Contu, E. C. Popovici, O. Fratu, and M. G. Berceanu, 'Security issues in most popular content management systems', in *2016 International Conference on Communications (COMM)*, Bucharest, Romania, Jun. 2016, pp. 277–280. doi: 10.1109/ICComm.2016.7528327.

[82] S. K.Patel, V. R. Rathod, and J. B. Prajapati, ‘Performance Analysis of Content Management Systems Joomla, Drupal and WordPress’, *IJCA*, vol. 21, no. 4, pp. 39–43, May 2011, doi: 10.5120/2496-3373.

[83] R. A. Alghofaili, ‘Security Anallysis of Open Source Content Management System Wordpress, Joomla, and Drupal’, 2018.

[84] ‘CMS Comparison - Most Popular CMS 2021 (Statistic)’. https://www.experte.com/website/cms-software (accessed Oct. 30, 2021).

[85] C. Pitt and J. Mancuso, ‘Creating Middleware’, in *The Definitive Guide to Masonite: Building Web Applications with Python*, C. Pitt and J. Mancuso, Eds. Berkeley, CA: Apress, 2020, pp. 135–141. doi: 10.1007/978-1-4842-5602-2_8.

[86] S. Varghese, ‘HTTP Middleware’, in *Web Development with Go: Building Scalable Web Apps and RESTful Services*, S. Varghese, Ed. Berkeley, CA: Apress, 2015, pp. 99–120. doi: 10.1007/978-1-4842-1052-9_6.

[87] T. Pranckevičius and V. Marcinkevičius, ‘Comparison of Naive Bayes, Random Forest, Decision Tree, Support Vector Machines, and Logistic Regression Classifiers for Text Reviews Classification’, *BJMC*, vol. 5, no. 2, 2017, doi: 10.22364/bjmc.2017.5.2.05.

[88] S. T. Indra, L. Wikarsa, and R. Turang, ‘Using logistic regression method to classify tweets into the selected topics’, in *2016 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, Malang, Indonesia, Oct. 2016, pp. 385–390. doi: 10.1109/ICACSIS.2016.7872727.

[89] F. Mereani and J. Howe, ‘Exact and Approximate Rule Extraction from Neural Networks with Boolean Features’, Jul. 2022, pp. 424–433. Accessed: Jul. 01, 2022. [Online]. Available: https://www.scitepress.org/Link.aspx?doi=10.5220/0008362904240433

[90] *payloadbox/xss-payload-list*. Payload Box, 2022. Accessed: Jul. 01, 2022. [Online]. Available: https://github.com/payloadbox/xss-payload-list

[91] F. M. M. Mokbal, D. Wang, and X. Wang, ‘Detect Cross-Site Scripting Attacks Using Average Word Embedding and Support Vector Machine’, p. 9, 2022.

[92] T. HERMITA, D. Stiawan, and A. Bardadi, ‘SISTEM KLASIFIKASI SERANGAN SQL INJECTION & XSS PADA RAMA REPOSITORY DENGAN METODE SUPPORT VECTOR MACHINE (SVM)’, undergraduate, Sriwijaya University, 2021. Accessed: Jul. 20, 2022. [Online]. Available: https://repository.unsri.ac.id/50967/

[93] M. Sharma and S. Singh Tomar, ‘Attack Detection and Security in Remote Code Execution’, *IJCA*, vol. 114, no. 14, pp. 9–15, Mar. 2015, doi: 10.5120/20045-1475.

[94] C. Wijayarathna and N. Gamagedara Arachchilage, ‘Fighting Against XSS Attacks. A Usability Evaluation of OWASP ESAPI Output Encoding’, presented at the Hawaii International Conference on System Sciences, 2019. doi: 10.24251/HICSS.2019.877.

[95] Bangkit Wiguna, W. Adi Prabowo, and R. Ananda, ‘Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website’, *Digitalzone*, vol. 11, no. 2, pp. 245–256, Nov. 2020, doi: 10.31849/digitalzone.v11i2.4867.

[96] R. Wood, *DAMN VULNERABLE WEB APPLICATION*. 2022. Accessed: Jul. 20, 2022. [Online]. Available: https://github.com/digininja/DVWA

[97] ‘OWASP WebGoat | OWASP Foundation’. https://owasp.org/www-project-webgoat/ (accessed Jul. 20, 2022).

[98] ‘bWAPP, a buggy web application!’ http://www.itsecgames.com/ (accessed Jul. 20, 2022).