DAFTAR PUSTAKA

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A., & Mooduto, H. A. (2021, September). Web Application Penetration Testing Using SQL Injection Attack. *JOIV : International Journal on Informatics Visualization, 5*(3), 320-326. doi:https://dx.doi.org/10.30630/joiv.5.3.470

Antono, S. Y. (2023). *PENGEMBANGAN PROGRAM OTOMATISASI UJI PENETRASI CVE-2018-14847 PADA PERANGKAT JARINGAN MIKROTIK BERBASIS PYTHON DAN SHODAN.* Universitas Gadjah Mada, Electrical Engineering and Informatics Department. Yogyakarta: ETD Repository UGM. Retrieved June 28, 2024, from https://etd.repository.ugm.ac.id/penelitian/detail/226751

Auger, R. (2010). *Path traversal*. Retrieved June 29, 2024, from The Web Application Security Consortium: http://projects.webappsec.org/w/page/13246952/Path%20Traversal

Casola, V., Benedicts, A. D., Rak, M., & Villano, U. (2020). A methodology for automated penetration testing of cloud applications. *International Journal of Grid and Utility Computing, 11*(2), 267-277. doi:https://doi.org/10.1145/3442520.3442533

Chawda, M., & Sharma, P. (2022, May 16). Deep Dive into Directory Traversal and *File Inclusion* Attacks leads to Privilege Escalation. *IJSRSET, 8*(3), 115-120. doi:https://doi.org/10.32628/IJSRSET218384

Ervan. (2021). *Mengetahui Cyber Attack Lebih Dalam dan Cara Mencegahnya*. Retrieved from POINSTAR: https://www.pointstar.co.id/blog/cyber-attack-adalah/

Fauzan, F. Y., & Syukhri, S. (2021). Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang. *Voteteknika, 9*(2), 1-7. doi:https://doi.org/10.24036/voteteknika.v9i2.111778

Hassan, M. M., Mustain, U., Khatun, S., Karim, M. S., Nishat, N., & Rahman, M. (2020). Quantitative Assessment of *Remote code execution* Vulnerability in Web Apps. *Lecture Notes in Electrical Engineering. 632.* Singapore: Springer. doi:https://doi.org/10.1007/978-981-15-2317-5_53

Kriti. (n.d.). *Vulnerability in Cyber Security: A Comprehensive Guide*. Retrieved from Internshala Training: https://trainings.internshala.com/blog/vulnerability-in-cyber-security/

Luman, A. (2020, September 28). *Simple File Path traversal*. Retrieved from Medium: https://medium.com/mii-cybersec/simple-*file*-path-traversal-9f61940e7bbf

Maherza, S. A., Hananto, B., & Pradnyana, I. W. (2023). Penetration Testing Terhadap Website Sekolah Menengah Atas ABC dengan Metode NIST SP 800-115. *JURNAL INFORMATIK Edisi ke-19*, 1-17. Retrieved 30 June, 2024, from https://ejournal.upnvj.ac.id/informatik/article/download/4697/2291/17141

Marbun, J. S., Syubbanul, S., Giffari, R. A., & Kardian, A. R. (2024, January). *Remote code execution* (RCE) pada Windows 10 dengan Berkas .docx Menggunakan Framework Metasploit (CVE-2021-40444). *CESS (Journal of Computing Engineering, System and Science)*, 119-127. Retrieved June 29, 2024, from https://jurnal.unimed.ac.id/2012/index.php/cess/article/view/54091/pdf

Nirmala, R. Y. (2023). *RANCANG BANGUN PROGRAM OTOMATISASI PENETRATION TESTING KERENTANAN CVE-2021-41282 PADA FIREWALL PFSENSE BERBASIS PYTHON*. Universitas Gadjah Mada. Yogyakarta: ETD Repository UGM. Retrieved 28 June, 2024, from https://etd.repository.ugm.ac.id/penelitian/detail/225423

NIST. (2021, May 10). *CVE-2021-41773 Detail*. Retrieved from NIST: https://nvd.nist.gov/vuln/detail/CVE-2021-41773

Novindri, G. F., & Saian, P. O. (2022, September). IMPLEMENTASI FLASK PADA SISTEM PENENTUAN MINIMAL ORDER UNTUK TIAP ITEM BARANG DI DISTRIBUTION CENTER PADA PT XYZ BERBASIS WEBSITE. *MNEMONIC, 5*(2), 1-6. doi:http://dx.doi.org/10.36040/mnemonic.v5i2.4670

Ouzan, O. (2023, August 2). *Dissecting and Exploiting CVE-2021–41773 and CVE-2021–42013*. Retrieved from medium: https://medium.com/@ofriouzan/dissecting-and-exploiting-cve-2021-41773-and-cve-2021-42013-7c116f489ee2

Sandhya, & Ponsam, J. G. (2024, May 6). URL Shield: Protecting Users from Phishing Attacks using Flask and ML. *2024 3rd International Conference for Innovation in Technology (INOCON)*, 1-5. doi:https://doi-org.ezproxy.ugm.ac.id/10.1109/INOCON60754.2024.10512235

Sholihah, W., Pripambudi, S., & Mardiyono, A. (2020, May 20). Log Event Management *Server* Menggunakan Elastic Search Logstash Kibana (ELK Stack). *jtim, 2*(1), 12-20. doi:https://doi.org/10.35746/jtim.v2i1.79

Singh, N., Meherhomji, V., & Chandavarkar, B. R. (2021, February 9). Automated versus Manual Approach of Web Application Penetration Testing. *IEEE 19th*

International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 1519-1524. doi:10.1109/TrustCom50675.2020.00207

Wallarm. (2024, February 26). *Path traversal Attack*. Retrieved from wallarm: https://www.wallarm.com/what/path-traversal-attack

Wijayanto, C., & Susetyo, Y. A. (2022, September). IMPLEMENTASI FLASK FRAMEWORK PADA PEMBANGUNAN APLIKASI SISTEM INFORMASI HELPDESK (SIH). *Jurnal Ilmiah Penelitian dan Pembelajaran INFORMATIKA, 7*(3). doi:https://doi.org/10.29100/jipi.v7i3.3161

Xiao, F., Yang, Z., Allen, J., Yang, G., Williams, G., & Lee, W. (2022). Understanding and Mitigating *Remote code execution* Vulnerabilities in Cross-platform Ecosystem. *CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2975 - 2988). ACM. doi:https://doi.org/10.1145/3548606.3559340