Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

DAFTAR PUSTAKA

[1] B. Rianto dan I. Alsa, "Perancangan Aplikasi Promosi Universitas Islam Indragiri Berbasi Multimedia Interaktif," Selodang Mayang: Jurnal Ilmiah Badan Perencanaan Pembangunan Daerah Kabupaten Indragiri Hilir, vol. 7, no. 1, hlm. 39–43, 2021.

[2] A. Muni, B. Rianto, dan M. Jalil, "Analisis Kerentanan Keamanan Sistem Informasi Akademik Menggunakan Owasp-Zap Di Universitas Islam Indragiri," Teknofile: Jurnal Sistem Informasi, vol. 2, no. 6, hlm. 409–420, 2024.

[3] A. Prahendratno dkk., Strategi Bisnis Digital: Optimalisasi & Otomtisasi Sebuah Bisnis Menggunakaan Media Digital. PT. Sonpedia Publishing Indonesia, 2023.

[4] A. D. Madya, B. D. Haryanto, D. P. Ningsih, dan F. Sinlae, "Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity," Indonesian Journal of Education And Computer Science, vol. 1, no. 3, hlm. 127–135, 2023.

[5] G. Alfaren, "Analisis Serangan Penetration Testing: Sebuah Review Sistematik," Jiifkom (Jurnal Ilmiah Informatika dan Komputer), vol. 1, no. 2, hlm. 21–26, 2022.

[6] M. Huda, Keamanan Informasi. Nulisbuku, 2020.

[7] M. R. Ardiansyah dkk., "Analisis Kerentanan Keamanan Website Menggunakan Metode Ptes (Penetration Testing Execution And Standart)," Nuansa Informatika, vol. 18, no. 2, hlm. 145–153, 2024.

[8] M. Tahir dan M. R. Ardiansyah, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode Ptes (Penetration Testing Execution Standard)," Jurnal Teknik Informatika Unika Santo Thomas, hlm. 118–125, 2024.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

[9] F. Tinambunan, A. Junaidi, dan A. M. Rizki, "Pengujian Sistem Informasi Akademik Universitas X Melalui Pendekatan Penetration Testing Berdasarkan Owasp Top 10," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 8, no. 1, hlm. 1062–1069, 2024.

[10] A. F. Hasibuan dan D. Handoko, "Analisis Keretanan Website Dengan Aplikasi Owasp Zap," Jurnal Ilmu Komputer dan Sistem Informasi, vol. 2, no. 2, hlm. 257–270, 2023.

[11] K. Nisa, M. A. Putra, R. A. Siregar, dan M. D. Irawan, "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)," Bulletin of Information Technology (BIT), vol. 3, no. 4, hlm. 216–308, 2022.

[12] J. N. Ginting, "Perancangan dan Pembuatan Sistem Informasi Penerimaan Mahasiswa Baru Berbasis Website," Jurnal Nasional Teknologi Komputer, vol. 2, no. 2, hlm. 51–59, 2022.

[13] W. Wiyanto, S. Fadhilah, dan A. Siswandi, "E-Tourism Sebagai Media Wisata Kabupaten Bekasi Berbasis Website," Journal of Practical Computer Science, vol. 2, no. 1, hlm. 1–14, 2022, doi: 10.37366/jpcs.v2i1.1035.

[14] B. Rianto, "WESITE PENYEDIAN INFORMASI RUMAH KOS KAB. INHIL Studi Kasus: Sebagian Rumah Kos Yang Ada Di Tembilahan," JUTI UNISI, vol. 3, no. 1, hlm. 35–42, 2019.

[15] B. Rianto, L. Lidya, dan G. W. Nurcahyo, "Pemodelan Arsitektur Enterprise Menggunakan Metode Togaf ADM Studi Kasus Dinas Kesehatan Kabupaten Indragiri Hilir," Jurnal Komputer Terapan, vol. 2, no. 1, hlm. 55–68, 2016.

[16] S. Hidayatulloh dan D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," Jurnal Algoritma, vol. 18, no. 1, hlm. 77–86, 2021.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

[17] D. F. Priambodo, A. D. Rifansyah, dan M. Hasbi, "Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating," Teknika, vol. 12, no. 1, hlm. 33–46, 2023.

[18] H. H. Muhammad, A. I. Hadiana, dan H. Ashaury, "Pengamanan Aplikasi Web Dari Serangan Sql Injection Dan Cross Site Scripting Menggunakan Web Application Firewall," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 7, no. 5, hlm. 3265–3273, 2023.

[19] D. S. Wibowo, M. Nishom, dan T. Abidin, "Pengumpulan Informasi pada Situs Web Dengan Menyusun Kerangka Kerja Keamanan Siber NIST," Jurnal Informatika: Jurnal Pengembangan IT, vol. 9, no. 1, hlm. 1–6, 2024.

[20] M. Idris, I. Syarif, dan I. Winarno, "Web Application Security Education Platform Based On OWASP API Security Project," EMITTER international journal of engineering technology, hlm. 246–261, 2022.

[21] G. Guntoro, L. Costaner, dan M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika), vol. 5, no. 1, hlm. 45–55, 2020.

[22] Y. Mulyanto, E. Haryanti, dan J. Jumirah, "Analisis Keamanan Website Sman 1 Sumbawa Menggunakan Metode Vulnerability Asesement: Analisis Keamanan Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Asesement," Jurnal Informatika Teknologi dan Sains (Jinteks), vol. 3, no. 3, hlm. 394–400, 2021.

[23] P. Jarupunphol, S. Seatun, dan W. Buathong, "Measuring Vulnerability Assessment Tools' Performance on the University Web Application.," Pertanika J Sci Technol, vol. 31, no. 6, 2023.

[24] Y. Yudiana, A. Elanda, dan R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan

Hak Cipta Dilindungi Undang-Undang
1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.
Universitas Islam Indragiri

Menggunakan OWASP Top 10," CESS (Journal of Computer Engineering, System and Science), vol. 6, no. 2, hlm. 185–191, 2021.

[25] N. Albalawi, N. Alamrani, R. Aloufi, M. Albalawi, A. Aljaedi, dan A. R. Alharbi, "The Reality of Internet Infrastructure and Services Defacement: A Second Look at Characterizing Web-Based Vulnerabilities," Electronics (Basel), vol. 12, no. 12, hlm. 2664, 2023.

[26] H. Poston, "Mapping The OWASP Top Ten to Blockchain," Procedia Comput Sci, vol. 177, hlm. 613–617, 2020.

[27] K. Qian, R. M. Parizi, dan D. Lo, "Owasp Risk Analysis Driven Security Requirements Specification For Secure Android Mobile Software Development," dalam 2018 IEEE Conference on Dependable and Secure Computing (DSC), IEEE, 2018, hlm. 1–2.

[28] S. Khandelwal, "Critical RCE Flaw Discovered In Blockchain-Based EOS Smart Contract System," The Hacker News. Retrieved February, vol. 4, hlm. 2023, 2018.

[29] I. F. Ashari, V. Oktarina, R. G. Sadewo, dan S. Damanhuri, "Analysis of Cross Site Request Forgery (CSRF) Attacks on West Lampung Regency Websites Using OWASP ZAP Tools," Jurnal Sisfokom (Sistem Informasi dan Komputer), vol. 11, no. 2, hlm. 276–281, 2022.

[30] I. Riadi, A. Fadlil, dan M. A. Mu'min, "OWASP Framework-based Network Forensics to Analyze the SQLi Attacks on Web Servers," MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 22, no. 3, hlm. 481–494, 2023.

[31] G. H. Editya dan S. Mulyati, "Aplikasi Mobile One Time Password Menggunakan Algoritma MD5 dan SHA1 untuk Meningkatkan Keamanan Website," SKANIKA: Sistem Komputer dan Teknik Informatika, vol. 1, no. 2, hlm. 618–623, 2018.

[32] J. T. Santoso, “Teknologi Keamanan Siber (Cyber Security),” Penerbit Yayasan Prima Agus Teknik, hlm. 1–173, 2023.

[33] Y. T. A. Rosaliah, J. Jayanta, dan B. Hananto, “Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx,” dalam Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya, 2021, hlm. 752–761.

[34] B. Ghozali, K. Kusrini, dan S. Sudarmawan, “Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating,” Creative Information Technology Journal, vol. 4, no. 4, hlm. 264–275, 2019.

[35] H. Sofyan, M. Sugiarto, dan B. M. Akbar, “Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN ‘Veteran’ Yogyakarta,” Telematika: Jurnal Informatika dan Teknologi Informasi, vol. 20, no. 2, hlm. 153–162, 2023.

[36] F. Fachri, A. Fadlil, dan I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” J. Inform, vol. 8, no. 2, hlm. 183–190, 2021.

[37] H. S. Abdullah, “Evaluation of open source web application vulnerability scanners,” Academic Journal of Nawroz University, vol. 9, no. 1, hlm. 47–52, 2020.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

Universitas Islam Indragiri