Pendas : Jurnal Ilmiah Pendidikan Dasar,
ISSN Cetak : 2477-2143 ISSN Online : 2548-6950
Volume 10 Nomor 03, September 2025

KAJIAN LITERATUR : METODE PENGUJIAN KEAMANAN SISTEM APLIKASI BERBASIS WEB

Sapta Kusuma Azhari [1], Cakra Trinata [2] , Besse Hartati [3]
[1,2,3]Manajemen Teknologi Keimigrasian, Politeknik Pengayoman Indonesia
[1]saptakusumaazhari@gmail.com, [2]cakra.trinata@poltekim.ac.id,

ABSTRACT

This document discusses the importance of information system security in the digital era, where much data and information is stored in website-based applications. Information system security is crucial to prevent various threats, such as data manipulation, information theft, and sabotage. This study aims to explore security testing methods, especially Penetration Testing, to identify and address vulnerabilities in web-based applications. The methods used in this study include a search for relevant literature, with a systematic approach using the PRISMA method. The results of the study indicate that there are several methods that are often used in application security testing, including Penetration Test, OWASP ZAP, and Vulnerability Assessment.

Keywords: system security testing, *penetration test,* OWASP, *vulnerabilty assement,* ISSAF

ABSTRAK

Dokumen ini membahas pentingnya keamanan sistem informasi dalam era digital, dimana banyak data dan informasi disimpan dalam aplikasi berbasis website. Keamanan sistem informasi sangat krusial untuk mencegah berbagai ancaman, seperti manipulasi data, pencurian informasi, dan sabotase. Penelitian ini bertujuan untuk mengeksplorasi metode pengujian keamanan, khususnya *Penetration Testing*, untuk mengidentifikasi dan mengatasi kerentanan dalam aplikasi berbasis web. Metode yang digunakan dalam penelitian ini meliputi pencarian literatur yang relevan, dengan pendekatan sistematis menggunakan metode PRISMA. Hasil penelitian menunjukkan bahwa terdapat beberapa metode yang sering digunakan dalam pengujian keamanan aplikasi, termasuk *Penetration Test*, OWASP ZAP, dan *Vulnerability Assessment*.

Kata Kunci: pengujian keamanan sistem, *penetration test,* OWASP, *vulnerabilty assement,* ISSAF

A. Pendahuluan

Dalam era digital sekarang, semua aspek dari dari suatu negara telah bertransformasi kepada digitalisasi data yang berbasis website atau aplikasi. Dengan digitalisasi seperti sekarang memiliki manfaat bagi negara berkembang atau negara maju seperti Indonesia. Tetapi dari manfaat tersebut terdapat suatu ancaman dari digitalisasi ini, yaitu keamanan sistem informasi yang disimpan diberbagai instansi baik pemerintah atau swasta. Sistem informasi data pribadi mempunyai peran penting dalam administrasi. Fokus lebih diberikan terhadap keamanan sistem karena dapat menimbulkan celah keamanan. Contoh dalam lapangan ada manipulasi data, perubahan kode program atau file, pencurian data, sabotase, dan segala macam tindakan penyalahgunaan data informasi (Ifani et al., 2024). Sistem informasi yang terdigitalisasi ini dapat meningkatkan kualiatas dari instansi. Maka dari itu akses terhadap suatu informasi juga perlu dikelola untuk dibatasi agar meminimalisir penyalahgunaan data dan dapat merugikan baik dari instansi yang bersangkutan ataupun pihak luar yang terkait. Ancaman-ancaman yang menyerang sistem keamanan ini dapat merusak tingkat kepercayaan dari suatu instansi karena tidak dapat menjaga data informasi pribadi atau instansi terkait.

Perhatian lebih terhadap keamanan sistem informasi perlu ditingkatkan. Tujuannya adalah untuk mencegah dan mendeteksi serangan yang dapat terjadi dan berpotensi merusak sistem. Aspek-aspek di dalam keamanan sistem informasi ada 3 yaitu, *confidentiality* (kerahasiaan) yaitu informasi harus diakses hanya dengan orang yang memiliki wewenang yang menjamin kerahasiaan, *integrity* (integritas) yaitu menjamin infromasi tidak dimanipulasi oleh pihak yang tidak berwenang, dan *availability* (ketersediaan) yaitu memastikan bahwa informasi dapat diakses oleh pihak berwenang jika dibutuhkan (Sanjaya et al., 2020). Transformasi era digital yang membuat berbagai informasi dan data dapat diakses ini, menimbulkan permasalahan baru yaitu dengan diperlukannya keamanan sistem yang kuat agar dapat mengantisipasi terjadinya serangan terhadap sistem yang dapat menimbulkan kerugian.

Di Indonesia, masalah keamanan informasi adalah hal yang kurang diperhatikan oleh pemerintah. Hal ini

harus diberikan perhatian yang lebih agar instansi pemerintah terhindar dari gangguan (serangan siber). Di dalam internet banyak ditemukan berbagai gangguan keamanan. Sebagai contoh ada Malware, Eksploitasi, Injeksi database dan lain sebagainya. Pada 2016, Badan Pengawas Lalu Lintas Internet mencatat 90% kejahatan internet dilakukan dalam penyerangan aplikasi web. Injeksi database merupakan serangan yang paling sering dilakukan dengan 47,06% serangan. Kepedulian terhadap isu keamanan sistem kurang diperhatikan, padahal semakin banyak berkembangnya cara perusakan dan pencurian data. Solusi pengamanan web dari gangguan atau serangan hacker dapat dilaksanakan cara self test. Pengujian ini dilakukan secara legal dengan mensimulasikan aktivitas penyerang (*hacker*). *Self test* dapat dilakukan dengan beberapa metode *Penetration Testing* salah satunya adalah *Information Systems Security Assessment Framework* (ISSAF), *Open Web Application Security Project* (OWASP) versi 4 dan *Open Source* yaitu: Penetapan Kriteria Kelayakan, Penetapan Sumber Informasi, Seleksi Literatur, dan Pengumpulan Data Security Testing Methodology Manual (OSSTMM) (Kusuma, 2022).

Dengan demikian kajian ini bertujuan untuk mencari metode pengujian *Penetration Test* terhadap aplikasi berbasis website dan mengidentifikasi serrta mengatasi kerentanan serangan siber terhadap keamanan suatu aplikasi.

B. Metode Penelitian

Metode yang digunakan dalam pengerjaaan penelitian ini adalah melakukan pencarian terhadap berbagai artikel, jurnal, hasil penetilian atau dokumen-dokumen yang relevan dengan permasalahan yang diteliti. Sehingga informasi yang didapatkan bisa dijadikan rujukan untuk memperkuat data dukung dalam penggunaan metode *Penetration Test* dalam menguji aplikasi berbasis website. Tinjauan sistematis yang digunakan agar dapat membuat penelitian ini adalah metode PRISMA (*Preferred Reporting Items for Systematic Review and Meta-analisis*). Proses ini diklasifikasi menjadi 4 (empat) tahap ;

Tahap 1 : kriteria kelayakan artikel di tentukan oleh *inclusion criteria* (IC) yaitu :

A. IC1 : artikel harus merupakan penulisan asli yang telah dipelajari dan ditulis dalam bahasa indonesia dan bahasa inggris
B. IC2 : artikel diterbitkan antara 2015 hingga 2024
C. IC3 : artikel ini bertujuan untuk menganalisis metode penetration terhadap keamanan aplikasi

Tahap 2 : penerapan sumber literatur

A. Literatur dicari menggunakan basis data repositori signifikan untuk studi akademis seperti *goggle scholar*

Tahap 3 : pemilihan literatur

A. Kata kunci yang digunakan adalah "keamanan data", "analisis keamanan sistem", dan "pengujian keamanan sistem"
B. Dilakukan pencarian dan mengindentifikasi dari judul, abstrak, serta artikel
C. Kata kunci yang diperoleh dari hasil pencarian kelayakan ini adalah kriteria yang telah ditentukan diawal
D. Artikel yang sudah dibaca tidak dihilangkan, tapi diseleksi lagi menjadi yang mana bisa ditinjau dan sesuai dengan kriteria
E. Artikel terpilih dinilai kembali untuk menemukan penelitian yang relevan

Tahap 4 : pengumpulan data

Data dikumpulkan secara manual dengan rentang waktu 2015-2025 dan mendapatkan hasil 302.000 jurnal berdasarkan kata kunci "keamanan data", 270.000 jurnal berdasarkan kata kunci "analisis keamanan sistem", 126.000 jurnal berdasarkan kata "pengujian keamanan sistem" dan seluruh sumber 50 jurnal terpilih memenuhi syarat untuk penelitian ini. setelah ditinjau kembali terpilih 22 jurnal untuk mendukung penelitian ini.

Tabel 1 Kumpulan Data

Sumber	Keamanan Data	Analisis Keamanan Sistem	Pengujian Keamanan Sistem	Kandidat	Terpilih
Crossref	2.334.700	263.625	105.424	0	0
Goggle Scholar	302.000	270.000	126.000	50	29
Sematic Scholar	10.400.000	92.900	42.200	10	2
Total	13.036.700	626.525	273.624	60	31

B. Hasil Penelitian dan Pembahasan

Tabel 2 Penulis, Judul, Tahun Terbit dan Metode

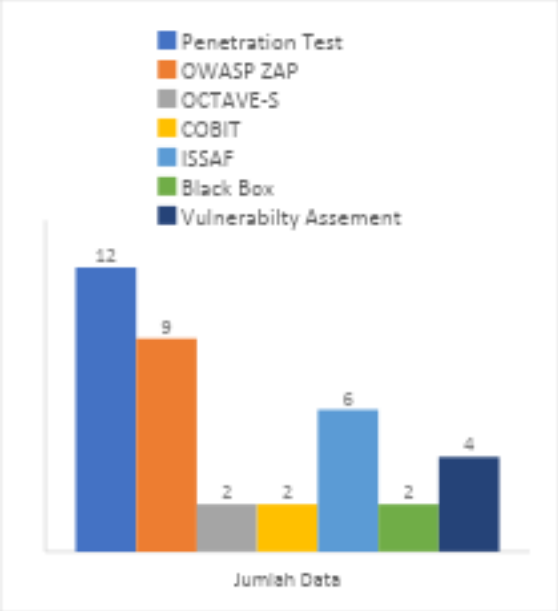
No	Penulis	Judul	Metode
1	(M Ayyas, A Fauzi, 2023)	Studi Komparatif Teknik Analisis Keamanan Sistem Informasi e-Government: *Penetration Testing* VS Vulnerability Assessment	*Penetration Test* dan Vulnerability *Assesment*
2	(Silmina et al., 2022)	Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan *Penetration Test* Dan Issaf	*Penetration Test* dan ISSAF
3	(I Made Edy Listartha, 2024)	PENGUJIAN KEAMANAN DENGAN METODE *PENETRATION TESTING* EXECUTION STANDARD (PTES) UNTUK MENEMUKAN KERENTANAN	*Penetration Test*
4	(Kusuma, 2022)	Implementasi OWASP ZAP Untuk Pengujian Keamanan Sistem Informasi Akademik	OWASP ZAP
5	(Zirwan, 2022)	Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner	*Vulnerability Assesment*
6	(Ibrahim et al., 2022)	Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode *Vulnerability Assesment* and *Penetration Testing* (VAPT)	*Penetration Test* dan *Vulnerability Assesment*
7	(Simanjuntak et al., 2024)	Analisis Keamanan Sistem menggunakan Metode *Penetration Testing* pada Website …	*Penetration Test*
8	(Nurelasari & Gumilang Al Farabi, 2024)	ANALISIS KEAMANAN SISTEM WEBSITE MENGGUNAKAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA SIMANTEP. ID ….	OWASP ZAP
9	(Haeruddin & Kurniadi, 2021)	Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode *Penetration Testing* (Studi Kasus: TP-Link Archer A6)	*Penetration Testing*
10	(Sari et al., 2018)	ANALISIS RESIKO KEAMANAN SISTEM E-PROCUREMENT	OCTAVE-S

		MENGGUNAKAN METODE OCTAVE-S (Studi Kasus: Unit Layanan Pengadaan Provinsi Riau)	
11	(Sanjaya et al., 2020)	Evaluasi Keamanan Website Lembaga X Melalui *Penetration Testing* Menggunakan Framework ISSAF	*Penetration Test* dan ISSAF
12	(Aufan et al., 2015)	Analisis Keamanan Sistem Informasi Akademik Dengan Web *Penetration Testing*	*Penetration Test*
13	(Umar et al., 2019)	Analisis keamanan sistem informasi berdasarkan framework COBIT 5 menggunakan Capability Maturity Model Integration (CMMI)	COBIT
14	(Cholifah et al., 2018)	Pengujian black box *testing* pada aplikasi action &strategy berbasis android dengan teknologi phonegap	Black Box
15	(Guntoro et al., 2020)	Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)	ISSAF dan OWASP ZAP
16	(Mulyanto et al., 2022)	Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode *Penetration Testing* (Pentest)	*Penetration Test*
17	(Zahra et al., 2023)	ANALISIS KEAMANAN SISTEM INFORMASI PADA WEBSITE PT SENTRA VIDYA UTAMA (SEVIMA) MENGGUNAKAN METODE OWASP	OWASP ZAP
18	(Kristara & Adiguna, 2023)	PENGUJIAN CELAH KEAMANAN INPUT VALIDATION PADA APLIKASI WEBSITE MENGGUNAKAN FRAMEWORK OWASP	OWASP ZAP
19	(Yudiana et al., 2021)	Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website pada STMIK Rosma dengan Menggunakan OWASP Top 10	OWASP ZAP
20	(Elanda & Buana, 2020)	Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security	OWASP ZAP

		Project (OWASP) Versi 4: Systematic Review	
21	(Tarigan, 2017)	Analisis Perbandingan *Penetration Testing* Tool untuk Aplikasi Web	*Penetration Test*
22	(Priyaungga et al., 2020)	Pengujian Black Box pada Aplikasi Perpustakaan Menggunakan Teknik Equivalence Partitions	Black Box
23	(Gusni et al., 2021)	Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019	COBIT
24	(Wardhana & Seta, 2021)	Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ	ISSAF
25	(Umar et al., 2023)	Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF	ISSAF
26	(Agus Rochman, Rizal Rohian Salam, 2021)	Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit …	ISSAF dan OSWASP ZAP
27	(Alwi & Ilmawan, 2021)	Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assesment	Vulnerability Assesment
28	(Kusumarini, 2021)	Analisis Keamanan Sistem Informasi Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Penetration Testing Execution Standard (PTES) Pada …	Penetration Test
29	(Rido Butar Butar et al., 2023)	Analisis Manajemen Risiko Keamanan Sistem Pengolahan Data Accurate Menggunakan Metode OCTAVE-S	OCTAVE
30	(Huzaini, 2024)	ANALISIS SISTEM KEAMANAN JARINGAN WIRELESS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD) STUDI KASUS PADA PT …	*Penetration Test*
31	(WIBOWO, 2019)	ANALISIS KERENTANAN KEAMANAN DENGAN METODE OWASP RISK RATING PADA SISTEM INFORMASI PARKIR BERBASIS ANDROID	OWASP

Hasil dan pembahasan dari 34 literatur yang telah dikaji untuk di jadikan referensi sebagai penulis dalam

memilih metode *Penetration Test* dalam menganilisis dan menguji celah keamanan aplikasi berbasis website.



Dari grafik di atas terdapat 7 metode yang biasanya di pakai sebagai metode pengujian keamaan sistem aplikasi berbasis website. Hasil review paper didapatkan hasil yaitu terdapat 4 metode yang sering digunakan dalam proses pengujiaan keamanan aplikasi berbasis website yaitu metode *Penetration Test*, OWASP ZAP, *Vulnerabilty Assement*, dan ISSAF yang dapat dilihat dari hasil grafik jumlah data atau metode yang sering digunakan.

D.Kesimpulan

Berdasarkan kajian literatur yang telah dilakukan, maka terdapat hasil metode yang sering digunakan dalam menganalisis keamanan sistem aplikasi website. *Penetration Test* dan OWASP ZAP sebagai metode yang sering digunakan dalam jurnal yang dijadikan data studi literatur ini. Dalam pengaplikasianya *Penetration Test* merupakan sebuah metode dalam pengujian sistem keamanan aplikasi website yang memuat tahapan perencanaan dan persiapan; pengumpulan informasi; analisis kerentanaan; eksploitasi; dan Pelaporan, lalu untuk OWASP merupakan suatu aplikasi yang hasil datanya dapat diolah ke dalam tahapan-tahapan *Penetration Test*. Sehingga didapatkan hasil dalam analisis kerentanaan dan pelaporan hasil test pengujian. Jadi penulis akan menjadikan melakukan uji *Penetration Test* terhadap aplikasi berbasis website dengan aplikasi OSWAB ZAP.

DAFTAR PUSTAKA

Agus Rochman, Rizal Rohian Salam, Dan S. A. M. (2021). Analisis

Keamanan Website Dengan Information System Security Assessment Framework (Issaf) Dan Open Web Application Security Project (Owasp) Di Rumah Sakit XYZ. Pharmacognosy Magazine, 75(17), 399–405.

Alwi, E. I., & Ilmawan, L. B. (2021). Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment. *INFORMAL: Informatics Journal*, *6*(3), 131. https://doi.org/10.19184/isj.v6i3.27053

Aufan, Imron, & Rosadi. (2015). Analisis Keamanan Sistem Informasi Akademik Dengan Web Penetraion Testing. *Digilib.Esaunggul.Ac.Id*, 12. https://digilib.esaunggul.ac.id/public/UEU-Undergraduate-10961-jurnal.Image.Marked.pdf

Cholifah, W. N., Yulianingsih, Y., & Sagita, S. M. (2018). Pengujian Black Box Testing pada Aplikasi Action & Strategy Berbasis Android dengan Teknologi Phonegap. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *3*(2), 206. https://doi.org/10.30998/string.v3i2.3048

Elanda, A., & Buana, R. L. (2020). Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review. *CESS (Journal of Computer Engineering, System and Science)*, *5*(2), 185. https://doi.org/10.24114/cess.v5i2.17149

Guntoro, G., Costaner, L., & Musfawati, M. (2020). 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)*, *5*(1), 45. https://doi.org/10.29100/jipi.v5i1.1565

Gusni, R. S. A., Kraugusteeliana, K., & Pradnyana, I. W. W. (2021). Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019. *Konferensi Nasional Ilmu Komputer (KONIK) 2021*, *September*, 434–439. https://prosiding.konik.id/index.php/konik/article/view/92

Haeruddin, H., & Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). *CoMBInES-Conference on Management …*, *1*(1), 508–515. https://journal.uib.ac.id/index.php/combines/article/view/4475

Huzaini, farhan thariq. (2024). ANALISIS SISTEM KEAMANAN JARINGAN WIRELESS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD) STUDI KASUS PADA PT MITRA BHAKTI INFORMASI. *Αγαη*, *15*(1), 37–48.

I Made Edy Listartha, G. A. J. S. (2024). *PENGUJIAN KEAMANAN DENGAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES) UNTUK MENEMUKAN KERENTANAN*

MISCONFIGURATIONS PADA PERANGKAT SECURITY TESTING WITH PENETRATION TESTING EXECUTION STANDARD (PTES) METHODS TO FIND MISCONFIGURATIONS VULNERABIL. *10*(2).

Ibrahim, A. M., Defisa, T., Seta, H. B., & P, I. W. W. (2022). Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT). *Senamika*, *April*, 312–325. https://conference.upnvj.ac.id/index.php/senamika/article/view/2002

Ifani, A. Z., Aspar, N. F., Setiawan, A. D., & Azlam, M. (2024). Pengujian Keamanan Sistem Informasi Data Kependudukan Menggunakan Metode Pentetration Testing. *Jurnal Fokus Elektroda: Energi Listrik, Telekomunikasi, Komputer, Elektronika Dan Kendali)*, *9*(2), 73–78.

Kristara, F. S., & Adiguna, M. A. (2023). Pengujian Celah Keamanan Input Validation Pada Aplikasi Website Menggunakan Framework Owasp. *Jurnal Penelitian Ilmu Komputer*, *1*(4), 50–55.

Kusuma, G. (2022). Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik. *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, *16*(2), 178–186. https://doi.org/10.47111/jti.v16i2.3995

Kusumarini, alvita izana. (2021). Analisis Keamanan Sistem Informasi Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Penetration Testing Execution Standard (PTES) Pada. *Pharmacognosy Magazine*, *75*(17), 399–405.

M Ayyas, A Fauzi, S. W. (2023). Studi Komparatif Teknik Analisis Keamanan Sistem Informasi e-Government: Penetration Testing VS Vulnerability Assessment. *SATIN - Sains Dan Teknologi Informasi*, *9*(2), 01–11. https://doi.org/10.33372/stn.v9i2.1000

Mulyanto, Y., Zaen, M. T. A., Yuliadi, Y., & Sihab, S. (2022). Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest). *Journal of Information System Research (JOSH)*, *4*(1), 202–209. https://doi.org/10.47065/josh.v4i1.2335

Nurelasari, E., & Gumilang Al Farabi, D. (2024). Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (Owasp) Pada Simantep.Id. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 3049–3054. https://doi.org/10.36040/jati.v8i3.9314

Priyaungga, B. A., Aji, D. B., Syahroni, M., Aji, N. T. S., & Saifudin, A. (2020). Pengujian Black Box pada Aplikasi Perpustakaan Menggunakan Teknik Equivalence Partitions. *Jurnal Teknologi Sistem Informasi Dan Aplikasi*, *3*(3), 150. https://doi.org/10.32493/jtsi.v3i3.5343

Rido Butar Butar, F., Saputra, E., Marsal, A., Hamzah, M. L., Fronita, M., Studi, P., Informasi, S., Sains,

F., Teknologi, D., & Riau, K. (2023). Analisis Manajemen Risiko Keamanan Sistem Pengolahan Data Accurate Menggunakan Metode OCTAVE-S. *Jurnal Sains Komputer & Informatika (J-SAKTI*, *7*(2), 675–685.

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *8*(2), 113. https://doi.org/10.24843/jim.2020.v08.i02.p05

Sari, J. P., Hr, J., & No, S. (2018). *ANALISIS RESIKO KEAMANAN SISTEM E-PROCUREMENT MENGGUNAKAN METODE OCTAVE-S (Studi Kasus : Unit Layanan Pengadaan Provinsi Riau) Periode Wisuda : November 2018 Program Studi Sistem Informasi Fakultas Sains dan Teknologi RISK SECURITY ANALYSIS OF E-PROCURE*.

Silmina, E. P., Firdonsyah, A., & Amanda, R. A. A. (2022). Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf. *Transmisi*, *24*(3), 83–91. https://doi.org/10.14710/transmisi.24.3.83-91

Simanjuntak, C. P., Arsanti, U. D., & Sudarmana, L. (2024). *ANALISIS KEAMANAN SISTEM MENGGUNAKAN METODE*. *November*, 1236–1246.

Tarigan, D. (2017). Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *1*(3), 206–214.

Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*, *9*(1), 47. https://doi.org/10.21456/vol9iss1pp47-54

Umar, R., Riadi, I., Ihya, M., & Elfatiha, A. (2023). Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF. *Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *12*(1), 280–292.

Wardhana, A. W., & Seta, H. B. (2021). Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ. *Informatik : Jurnal Ilmu Komputer*, *17*(3), 226. https://doi.org/10.52958/iftk.v17i3.3653

WIBOWO, C. (2019). *Analisis Kerentanan Keamanan Dengan Metode Owasp Risk Rating Pada Sistem Informasi Parkir Berbasis Android*. https://etd.repository.ugm.ac.id/penelitian/detail/178249

Yudiana, Y., Elanda, A., & Buana, R. L. (2021). Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10. *CESS (Journal of Computer Engineering, System and Science)*, *6*(2), 185. https://doi.org/10.24114/cess.v6i2.24777

Zahra, N. A., Zidane, F. H., & Kuslaila, N. R. (2023). Analisis Keamanan Sistem Informasi Pada Website Pt Sentra Vidya Utama (Sevima) Menggunakan Metode Owasp. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *3*(1), 384–393. https://doi.org/10.33005/sitasi.v3i1.564

Zirwan, A. (2022). Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner. *Jurnal Informasi Dan Teknologi*, *4*(1), 70–75. https://doi.org/10.37034/jidt.v4i1.190