JIIFKOM (Jurnal Ilmiah Informatika & Komputer) STTR Cepu
E-Mail: jiifkom@sttrcepu.ac.id

Analisis Penerapan CAPTCHA, Autentikasi, dan Access Control pada Keamanan Informasi Website Akademik

Panggah Widiandana[a*], Muhammad Azam Muttaqin[b], Habib Muhammad Riziq[c], Fadhlan Al Muiz[d]
panggah.widiandana@uim-yogya.ac.id[a]

Program Studi Informatika, Fakultas Sains Teknologi dan Kesehatan, Universitas Islam Mulia Yogyakarta, Yogyakarta, Indonesia[a,b,c,d]

Kata kunci:
Keamanan Informasi, CAPTCHA, Autentikasi Kampus, Kontrol Akses, Sistem Informasi Akademik

Intisari

Keamanan informasi merupakan elemen penting dalam pengelolaan sistem informasi akademik berbasis web guna melindungi data dan mengontrol akses pengguna. Penelitian ini bertujuan menganalisis penerapan serta efektivitas mekanisme keamanan informasi berupa CAPTCHA, autentikasi kampus, dan kontrol akses berbasis sesi yang diterapkan pada *website* Sistem Informasi Akademik Universitas Islam Mulia Yogyakarta (SISKADUIMY). Metode penelitian yang digunakan adalah deskriptif kualitatif dengan pendekatan studi kasus melalui observasi langsung terhadap fungsionalitas sistem dan analisis kode program. Hasil analisis menunjukkan bahwa implementasi CAPTCHA pada halaman log masuk admin efektif dalam mencegah upaya akses otomatis dan serangan *brute force* oleh *bot*. Sementara itu, mekanisme autentikasi kampus pada fitur unduh jadwal kuliah format PDF berfungsi sebagai verifikasi kontekstual tambahan untuk menjamin validitas akses pengguna dan mencegah eksploitasi berkas. Pengamanan tersebut diperkuat oleh kontrol akses berbasis sesi yang secara ketat membatasi hak akses administratif dari manipulasi tautan langsung. Kombinasi ketiga instrumen ini memberikan kontribusi signifikan dalam meningkatkan aspek kerahasiaan, integritas, dan akuntabilitas sistem akademik.

Tentang naskah:
-diterima, 17 Juni 2026
-diterbitkan, 1 Juli 2026

Abstract

Information security is a critical element in managing web-based academic information systems as it directly relates to data protection and user access control. This study aims to analyze the implementation and effectiveness of information security mechanisms, including CAPTCHA, campus authentication, and session-based access control applied to the Academic Information System website of Universitas Islam Mulia Yogyakarta (SISKADUIMY). The research method employed is descriptive qualitative with a case study approach through direct observation of system functionalities and source code analysis. The analysis results indicate that the implementation of CAPTCHA on the admin login page effectively prevents automated access and brute force attacks by bots. Meanwhile, the campus authentication mechanism on the PDF schedule download feature serves as an additional contextual verification to ensure the validity of user access and prevent document exploitation. This security is further reinforced by session-based access control, which strictly restricts administrative privileges from direct URL manipulation. The combination of these three instruments contributes significantly to enhancing the confidentiality, integrity, and accountability aspects of the academic system.

Keywords:
Information Security, CAPTCHA, Campus Authentication, Access Control, Academic Information System

1. Pendahuluan

Pemanfaatan sistem informasi akademik berbasis web telah menjadi kebutuhan utama dalam lingkungan perguruan tinggi. Sistem ini mendukung penyampaian informasi secara cepat dan efisien, namun di sisi lain meningkatkan risiko terhadap ancaman keamanan data. Berbagai kerentanan pada platform edukasi sering kali dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan eksploitasi, seperti serangan packet sniffing yang mengintai transmisi data sensitif mahasiswa dan dosen (Rahmahdany dkk., 2024), hingga taktik

footprinting serta vulnerability scanning untuk memetakan kelemahan sistem sebelum meluncurkan serangan utama (Allo & Widiasari, 2024).

Modus operan di kejahatan siber yang kian berkembang juga mencakup penyebaran situs phishing yang meniru portal resmi kampus (Nagalay dkk., 2024). Berdasarkan audit keamanan eksternal yang memanfaatkan metode pemetaan jaringan (network mapper) dan penilaian kerentanan (vulnerability assessment), ditemukan bahwa banyak portal akademik di Indonesia masih rentan terhadap kebocoran data akibat lemahnya protokol enkripsi dan manajemen sesi (Fronita, 2023)(Syahab, 2023).

Evaluasi kesiapan keamanan informasi menjadi sangat krusial menggunakan parameter terstandarisasi seperti Indeks KAMI guna memetakan tingkat kematangan proteksi aset digital institusi (Jenny, 2024). Ketidaktersediaan infrastruktur pengamanan yang memadai seperti Intrusion Detection System (IDS) pada jaringan internal universitas memicu tingginya probabilitas keberhasilan infiltrasi ilegal (Hidayat, 2023). Ancaman nyata tersebut meliputi serangan *bot* otomatis, akses tidak sah (unauthorized access), serta manipulasi hak istimewa pengguna (Arifin dkk., 2024)(Ariyadi dkk., 2025). Guna mereduksi dampak risiko kebocoran, beberapa tata kelola teknologi informasi mulai mengadopsi kerangka kerja internasional secara ketat untuk melindungi integritas operasional sistem (Wijayakusuma dkk., 2026)(Ys dkk., 2024). Fenomena ini menegaskan bahwa kebutuhan proteksi data bukan lagi sekadar pelengkap teknis, melainkan pilar utama keberlanjutan organisasi (Humairah & Mardiati, 2026).

Website Sistem Informasi Akademik Universitas Islam Mulia Yogyakarta (SISKADUIMY) merupakan salah satu platform yang dirancang untuk menyajikan informasi jadwal perkuliahan secara daring kepada civitas akademika. Efisiensi penjadwalan kuliah melalui digitalisasi memang terbukti meningkatkan performa layanan administrasi perguruan tinggi secara signifikan (Widiandana dkk., 2024), mirip dengan efisiensi integrasi data pada sistem pelayanan publik tingkat kelurahan (Panggah Widiandana dkk., 2025). Kendati demikian, fungsionalitas utama SISKADUIMY yang krusial seperti fitur unduh jadwal dalam format PDF dan panel administrasi berpotensi menjadi objek manipulasi eksploitatif jika tidak diproteksi dengan baik. Serangan *automated bot* berulang serta manipulasi tautan unduhan langsung (direct URL manipulation) menjadi ancaman yang jamak ditemukan pada situs pendidikan berskala menengah (Febriansyah & Tedyyana, 2025)(Nisa dkk., 2024).

Kegagalan dalam mengamankan elemen-elemen ini dapat menyebabkan modifikasi jadwal ilegal oleh pihak luar ataupun pelumpuhan server melalui banjir permintaan otomatis (brute force). Untuk menjaga aspek kerahasiaan dan integritas data tersebut, pengembang menerapkan kombinasi mekanisme pengamanan berlapis (layered security), di antaranya menyematkan CAPTCHA pada halaman login admin serta membatasi fitur unduh jadwal kuliah melalui teknik verifikasi tambahan. Penetrasi pengujian (penetration testing) secara periodik membuktikan bahwa pemasangan pertahanan di level otentikasi awal mampu menurunkan tingkat keberhasilan eksploitasi otomatis secara drastis (Nurrizki, 2024)(Putra & Santoso, 2025).

Selain itu, sistem manajemen pengajuan akses berbasis web yang terstruktur terbukti mempermudah pelacakan aktivitas pengguna dan memperkuat akuntabilitas operasional (Kusumo, 2024). Meskipun analisis risiko menggunakan kerangka kerja formal seperti FMEA dan ISO 27002 merekomendasikan perlindungan komprehensif di seluruh arsitektur jaringan (Sahira dkk., 2025), penerapan pertahanan modular di gerbang autentikasi dinilai sebagai langkah awal yang taktis dan efisien.

Gap analysis dari penelitian ini menunjukkan bahwa sebagian besar analisis keamanan sistem informasi akademik terdahulu berfokus pada pengujian penetrasi eksternal (penetration testing) secara menyeluruh atau audit tata kelola menggunakan instrumen standar. Masih sedikit literatur studi kasus yang secara spesifik membedah efektivitas integrasi tiga komponen pengaman sederhana yaitu CAPTCHA teks, autentikasi kontekstual berbasis institusi,

dan pembatasan sesi (session-based access control) pada web akademik berskala kecil hingga menengah. Oleh karena itu, penelitian ini bertujuan untuk menganalisis penerapan, mekanisme kerja, serta tingkat efektivitas instrumen CAPTCHA, autentikasi kampus, dan kontrol akses berbasis sesi dalam memproteksi kerahasiaan, integritas, serta akuntabilitas data pada *website* SISKADUIMY.

2. Kerangka Teori

2.1 Teori Tiga Pilar Keamanan Informasi

Keamanan informasi pada platform berbasis web bersandar pada proteksi tiga pilar utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*), visualisasi tiga pilar utama dapat dilihat pada Gambar 1.

Gambar 1 Diagram CIA

Gambar 1 mengilustrasikan CIA Triad (atau Segitiga CIA) yang merupakan fondasi mendasar dalam arsitektur keamanan informasi. Segitiga ini memetakan tiga pilar utama yang saling berkaitan untuk melindungi sistem, yaitu *Availability* (Ketersediaan) untuk memastikan data dapat diakses oleh pihak berwenang saat dibutuhkan, *Integrity* (Integritas) untuk menjaga keaslian dan mencegah modifikasi data yang tidak sah, serta *Confidentiality* (Kerahasiaan) untuk membatasi hak akses data hanya kepada pengguna yang memiliki otoritas resmi.

Di dalam ekosistem sistem informasi akademik, tantangan terbesar muncul dari bagaimana mengelola hak akses pengguna secara presisi demi mencegah kebocoran data sensitif ataupun manipulasi berkas administrasi. Penerapan otentikasi yang tangguh menjadi benteng pertahanan pertama dalam memverifikasi identitas pengguna sebelum mereka diberikan hak untuk berinteraksi dengan basis data internal sistem (Godzali dkk., 2024). Evaluasi terhadap mekanisme otentikasi ini menunjukkan bahwa model pengamanan tradisional yang hanya bergantung pada pasangan nama pengguna dan kata sandi statis memiliki kerentanan tinggi terhadap serangan berbasis tebakan otomatis (*brute-force attacks*) maupun intersepsi sesi oleh pihak luar. Oleh sebab itu, adopsi teknologi otentikasi yang modern dan berlapis sangat direkomendasikan untuk menjamin bahwa identitas yang mengklaim hak akses tersebut sepenuhnya valid (Yeovandi dkk., 2025).

2.2 Teori Kontrol Akses

Selain komponen otentikasi di pintu masuk utama, arsitektur keamanan web memerlukan instrumen kontrol akses (*access control*) yang membatasi hak istimewa pengguna sesuai dengan peran atau modul yang diizinkan. Salah satu pendekatan yang paling banyak diterapkan pada aplikasi tingkat perusahaan hingga institusi pendidikan adalah *Role-Based Access Control* (RBAC), yang mengaitkan izin operasional secara spesifik ke dalam peran kerja fungsional tertentu (Sahyudi & Susanto, 2025). Dalam implementasi praktisnya, otorisasi hak akses ini juga dapat diperkuat dengan memanfaatkan token digital terenkripsi seperti JSON Web Token (JWT). Integrasi kontrol akses yang ketat berbasis token atau enkripsi sesi terbukti mampu meminimalkan risiko eksploitasi celah berupa peningkatan hak istimewa sepihak (*privilege escalation*) yang sering menjadi target penyerang untuk mengunduh dokumen internal secara ilegal (Darmawan dkk., 2023). Pengujian berkala terhadap efektivitas kontrol akses ini sangat vital demi mendeteksi adanya celah keamanan sebelum diaplikasikan penuh pada sistem produksi (Gymnastiar dkk., 2025).

2.3 Teori Penerapan Praktis Instrumen (CAPTCHA, Autentikasi Kampus, *Session-Based Access Control*)

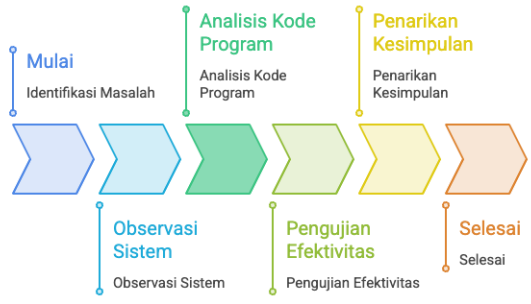
Secara teknis, naskah dalam penelitian *website* SISKADUIMY ini mengevaluasi tiga instrumen proteksi utama secara deskriptif. Instrumen pertama adalah CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*), sebuah skema uji tantangan-tanggapan (*challenge-response test*) yang dirancang untuk memastikan bahwa input

dilakukan oleh manusia dan bukan oleh skrip *bot* otomatis. Instrumen kedua adalah sistem autentikasi kontekstual internal kampus, yang bertindak sebagai lapis verifikasi kedua ketika pengguna mencoba mengakses berkas sensitif, seperti mengunduh berkas jadwal perkuliahan dalam format PDF. Instrumen ketiga adalah kontrol akses berbasis sesi (*session-based access control*), di mana server akan menerbitkan ID sesi unik yang mencatat aktivitas pengguna secara berkala, membatasi durasi aktif melalui *session timeout*, serta menghancurkan data sesi (*destroy session*) begitu pengguna keluar dari sistem guna mencegah pembajakan sesi oleh pihak ketiga yang tidak sah.

3. Metodologi

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi kasus untuk memperoleh gambaran mendalam mengenai penerapan mekanisme keamanan informasi pada *website* SISKADUIMY. Objek penelitian difokuskan pada *website* SISKADUIMY yang dapat diakses melalui tautan resmi sistem. Data dikumpulkan melalui teknik observasi langsung terhadap fitur keamanan yang tersedia pada antarmuka sistem, khususnya pada halaman login admin dan halaman jadwal mingguan, serta diperkuat dengan studi literatur terhadap referensi ilmiah yang relevan.

Secara sistematis, tahapan pelaksanaan penelitian ini dipecah ke dalam beberapa fase terstruktur yang dapat dilihat pada Gambar 2.



Gambar 2. Diagram Alir Tahapan Pelaksanaan Penelitian

Gambar 2 menjelaskan alur tahapan penelitian mulai dari identifikasi masalah, observasi sistem, analisis kode program, pengujian efektivitas, sampai ke penarikan kesimpulan, uraian tahapan sebagai berikut:

3.1 Fase Identifikasi Masalah

Melakukan pemetaan awal terhadap risiko keamanan informasi pada *website* akademik, khususnya ancaman serangan *bot*, akses tidak sah (*unauthorized access*), serta manipulasi URL langsung pada fitur sensitif.

3.2 Fase Observasi Sistem

Melakukan pengamatan langsung terhadap implementasi tiga mekanisme pengamanan utama yang tertanam pada platform SISKADUIMY, yaitu CAPTCHA teks pada halaman login admin, dialog autentikasi kampus pada fitur unduh PDF, dan *session-based authentication* pada halaman administratif.

3.3 Fase Analisis Kode Program

Memeriksa struktur kode program PHP yang mengatur kontrol akses berbasis sesi guna memahami bagaimana server memverifikasi variabel sesi sebelum menampilkan konten khusus admin.

3.4 Fase Pengujian Efektivitas

Melakukan simulasi pengujian fungsional untuk mengevaluasi respons sistem ketika menerima input CAPTCHA yang salah, pengisian nama institusi yang tidak valid, serta upaya pengaksesan halaman admin secara langsung melalui URL tanpa proses login.

3.5 Fase Penarikan Kesimpulan

Menganalisis bagaimana integrasi ketiga mekanisme tersebut berkontribusi dalam mendukung prinsip dasar keamanan informasi yang meliputi aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan akuntabilitas (*accountability*).

4. Hasil dan Pembahasan

Website Sistem Informasi Akademik Universitas Islam Mulia Yogyakarta (SISKADUIMY) mengimplementasikan tiga instrumen pertahanan utama pada gerbang autentikasi dan kontrol akses guna melindungi data jadwal perkuliahan dari eksploitasi otomatis. Berdasarkan observasi langsung dan analisis fungsional terhadap kode program, hasil tahapan penerapan serta tingkat efektivitas dari masing-masing instrumen pengamanan tersebut dijabarkan melalui poin-poin capaian yang dapat dilihat pada Tabel 1.

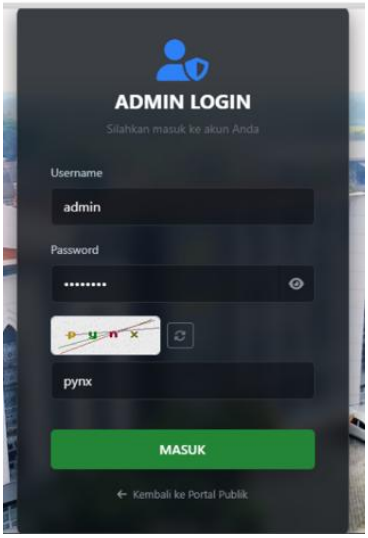
Tabel 1. Hasil Pengujian Mekanisme Keamanan *Website* SISKADUIMY

No	Instrumen Keamanan	Skenario Pengujian	Hasil di Lapangan	Status
1	CAPTCHA	Menginput teks alfanumerik salah	Login ditolak, muncul pesan error	✓
2	Autentikasi Kampus	Menginput nama institusi keliru	Dialog unduh terkunci, kembali ke menu	✓
3	Kontrol Akses Sesi	Menembak langsung URL halaman admin	Sistem otomatis menendang ke login.php	✓

Tabel 1. menjelaskan hasil pengujian mekanisme *website* SISKADUIMY dengan uraitan instrument keamanan sebagai berikut:

4.1 Mekanisme CAPTCHA pada Halaman Login Admin

Komponen pertahanan pertama diletakkan pada halaman log masuk administrator (*login admin*) menggunakan skema *Completely Automated Public Turing test to tell Computers and Humans Apart* (CAPTCHA) berbasis gambar teks alfanumerik acak. Implementasi CAPTCHA dapat dilihat pada Gambar 3.

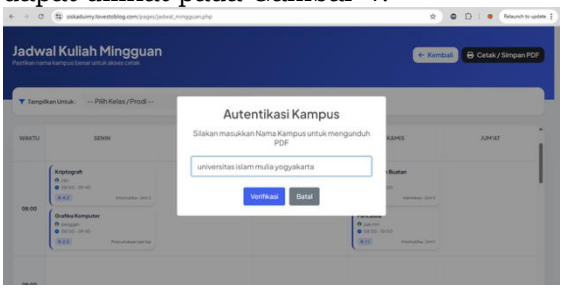


Gambar 3. Tampilan Antarmuka Halaman Login Admin dengan Fitur CAPTCHA

Gambar 3 merupakan implementasi CAPTCHA agar Pengguna diwajibkan menginput kembali karakter yang muncul secara tepat sebelum server memeriksa keabsahan kata sandi. Tahapan analisis menunjukkan bahwa instrumen ini bekerja efektif sebagai penyaring awal untuk memblokir serangan *bot* otomatis dan percobaan *brute-force*. Karakteristik matriks gambar yang terdistorsi menyulitkan skrip *bot* konvensional untuk melakukan pengisian formulir secara massal, sehingga permintaan login otomatis akan langsung dipotong dan ditolak oleh server.

4.2 Autentikasi Kontekstual pada Fitur Unduh Jadwal PDF

Mekanisme kedua merupakan lapis verifikasi sekunder (*secondary verification*) yang diterapkan ketika pengguna umum atau mahasiswa mencoba mengunduh dokumen jadwal perkuliahan dalam format PDF. Implementasi Autentikasi dapat dilihat pada Gambar 4.



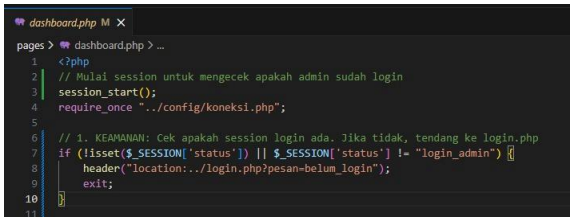
Gambar 4. Autentikasi kampus untuk cetak pdf

Gambar 4 merupakan implementasi dari autentikasi kampus untuk cetak pdf, ketika tombol unduh ditekan, sistem tidak langsung memberikan akses berkas secara bebas, melainkan memicu munculnya kotak dialog yang meminta konfirmasi nama institusi resmi, yaitu "Universitas Islam Mulia Yogyakarta". Hasil pengujian membuktikan bahwa verifikasi kontekstual ini sangat andal untuk meminimalkan risiko manipulasi tautan unduhan langsung (*direct URL manipulation*) serta menahan aktivitas *bot* pengumpul data (*web scraper*) yang berniat mengunduh dokumen internal secara masif tanpa melalui antarmuka web yang sah.

4.3 Kontrol Akses Berbasis Sesi (Session-Based Access Control)

Mekanisme ketiga beroperasi di sisi server untuk mengunci aktivitas administrasi setelah administrator berhasil masuk ke dalam sistem. Server akan menerbitkan ID sesi (*Session ID*) unik yang dicatat pada memori server dan disimpan sebagai *cookie* temporer pada sisi klien. Setiap navigasi menu dan manipulasi data di dalam panel admin selalu melewati tahapan validasi variabel sesi global. Hasil analisis kode skrip PHP

menunjukkan bahwa kontrol akses ini memblokir secara absolut setiap upaya pemanggilan langsung berkas administratif melalui bilah alamat browser jika sesi aktif tidak terdeteksi. Sistem ini juga dilengkapi dengan fungsi *destroy session* saat tombol *logout* ditekan untuk memastikan sesi benar-benar dihancurkan. Implementasi dari kontrol akses dapat dilihat pada Gambar 5.



Gambar 5. Implementasi Skrip Kontrol Akses Berbasis Sesi PHP

Gambar 5 menampilkan implementasi kontrol akses berbasis sesi (session-based access control) menggunakan bahasa pemrograman PHP pada berkas dashboard.php. Kode program tersebut bekerja dengan mengaktifkan fungsi session_start() untuk memulai pelacakan sesi , kemudian melakukan validasi keamanan melalui pengondisian if untuk memeriksa keberadaan variabel $_SESSION['status']. Apabila sesi login tidak ditemukan atau status pengguna tidak sama dengan "login_admin", sistem secara otomatis akan menolak hak akses, menghentikan eksekusi skrip, dan mengalihkan (redirect) pengguna kembali ke halaman login utama (login.php) guna mencegah modifikasi data oleh pihak yang tidak berwenang.

Secara integratif, penerapan ketiga instrumen pengamanan ini memberikan kontribusi yang signifikan terhadap penguatan pilar keamanan informasi pada *website* SISKADUIMY. Aspek kerahasiaan (*confidentiality*) jadwal perkuliahan internal terlindungi dari akses massal tidak sah berkat kombinasi autentikasi kampus dan kontrol sesi. Sementara itu, aspek integritas (*integrity*) data akademik pada panel kontrol tetap terjaga karena celah modifikasi jadwal ilegal telah ditutup oleh proteksi ganda CAPTCHA dan otorisasi sesi admin. Meskipun demikian, hasil evaluasi menemukan adanya ruang perbaikan pada sistem berjalan, di antaranya adalah ketiadaan fitur batas waktu sesi (*session timeout*) otomatis yang dapat memicu risiko pembajakan sesi jika perangkat admin ditinggalkan dalam keadaan aktif, serta penggunaan CAPTCHA berbasis teks statis yang lambat laun berpotensi ditembus oleh teknologi *Optical Character Recognition* (OCR) berbasis kecerdasan buatan masa kini.

5. Simpulan

Penerapan mekanisme pengamanan berlapis pada *website* Sistem Informasi Akademik Universitas Islam Mulia Yogyakarta (SISKADUIMY) terbukti memberikan kontribusi yang signifikan dalam memperkuat pilar keamanan informasi secara teoretis maupun praktis. Sinergi antara instrumen CAPTCHA pada gerbang masuk administratif, autentikasi kontekstual internal institusi pada fitur unduhan dokumen PDF, serta kontrol akses berbasis sesi di sisi server berhasil membentuk arsitektur pertahanan modular yang efisien untuk melindungi aset data akademik dari ancaman eksploitasi otomatis dan akses tidak sah. Sebagai penutup, meskipun integrasi komponen pengaman ini andal dalam meminimalkan risiko kebocoran data, pengembangan sistem ke depan masih memerlukan pembaruan adaptif seperti penerapan batas waktu sesi otomatis serta penggunaan teknologi reCAPTCHA terkini untuk mengantisipasi dinamika ancaman siber yang terus berkembang.

Daftar Pustaka

Allo, A. K., & Widiasari, I. R. (2024). Analisis Keamanan Website SIASAT Menggunakan Teknik Footprinting dan Vulnerability Scanning. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, *8*(2), 316–323. https://doi.org/10.35870/jtik.v8i2.1723

Arifin, H., Angraini, A., Ahsyar, T. K., & Syaifullah, S. (2024). Analisis Keamanan Sistem Informasi Menggunakan Cobit 2019 pada Sistem Sawit Rakyat Online (SRO) Studi Kasus PTPN V. *Jurnal Teknologi Sistem Informasi dan Aplikasi*, *7*(3), 903–911. https://doi.org/10.32493/jtsi.v7i3.39650

Ariyadi, T., Fadli, H., Akbar, T., & Prihandoko, M. B. (2025). Implementasi OWASP untuk Analisis Kerentanan dan Keamanan pada Sistem Informasi Akademik Terintegrasi Universitas Bina Darma. *STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer*, *4*(1), 1–7. https://doi.org/10.55123/storage.v4i1.4737

Darmawan, I., Mansyur, M. U., Imam, K. Z., Syahdan, Moh., & Fawaid, A. (2023). Evaluasi Keamanan Privilege Terintegerasi JSON Web Token pada Sistem Informasi Akademik. *Jurnal Informasi dan Teknologi*,120–128. https://doi.org/10.37034/jidt.v5i2.368

Febriansyah, M. Z., & Tedyyana, A. (2025). ANALISA DAN PERBAIKAN KEAMANAN PADA WEBSITE SDN 9 BANTAN. *Jurnal Sistem Informasi dan Sains Teknologi*, *7*(2). https://doi.org/10.31326/sistek.v7i2.2408

Fronita, M. (2023). ANALISIS CELAH KEAMANAN WEBSITE SITASI MENGGUNAKAN VULNERABILITY ASSESSMENT. *Jurnal Ilmiah*

Rekayasa dan Manajemen Sistem Informasi, *9*(1), 1–1. https://doi.org/10.24014/rmsi.v9i1.21823

Godzali, G. A., Athallah, R. I., & Rivalni, E. (2024). Evaluasi Keamanan Autentikasi Pengguna pada Sistem Operasi Windows dan Linux. *Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi*, *3*(1), 31–40. https://doi.org/10.61132/neptunus.v3i1.590

Gymnastiar, P., Nuraini, N., & Kusnana, K. (2025). Analisis Keamanan dan Pengujian Access Control pada Website Pendidikan: Studi Kasus di Universitas Hamzanwadi Lombok. *Proceedings of the National Conference on Electrical Engineering, Informatics, Industrial Technology, and Creative Media*, *4*(1), 951–959. https://doi.org/10.20895/centive.v4i1.317

Hidayat, A. M. N. (2023). PENERAPAN SISTEM KEAMANAN IDS PADA JARINGAN NIRKABEL (HOTSPOT). *AnoaTIK: Jurnal Teknologi Informasi dan Komputer*, *1*(2), 68–70. https://doi.org/10.33772/anoatik.v1i2.12

HUMAIRAH, M., & MARDIATI, D. (2026). ANALISIS KEBUTUHAN INFORMASI UNTUK PENGEMBANGAN SISTEM INFORMASI KEAMANAN DATA PADA PERUSAHAAN TEKNOLOGI. *JURNAL DATA SAINS DAN TEKNOLOGI INFORMASI (DASTIS)*, *3*(2), 1–13. https://doi.org/10.62003/bgrxns09

Jenny, M. S. (2024). Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks Kami) Versi 4.2 Pada Sistem Informasi Akademi (SIMAK) Universitas Siliwangi. *Jurnal SITECH : Sistem Informasi dan Teknologi*, *7*(1), 73–80. https://doi.org/10.24176/sitech.v7i1.12390

Kusumo, B. (2024). Sistem Informasi Pengajuan dan Analisis Kelayakan Kredit Berbasis Website Menggunakan Metode AHP Simulasi Pada Bank Perkreditan Rakyat Cibitung. *JURNAL KRIDATAMA SAINS DAN TEKNOLOGI*, *6*(2), 702–721. https://doi.org/10.53863/kst.v6i02.1379

Nagalay, F. S. S., Sriyanto, S., & Zarnelly, Z. (2024). ANALISIS PENERAPAN ALGORITMA DECISION TREE DALAM KEAMANAN SIBER UNTUK KELASIFIKASI SITUS WEBSITE PHISHING. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, *10*(1), 1–1. https://doi.org/10.24014/rmsi.v10i1.28401

Nisa, F., Nurfebruary, N. S., & Ikhwani, M. (2024). Analisis Keamanan Sistem Informasi Website Portal Akademik Universitas Malikussaleh Menggunakan OWASP ZAP. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, *7*(6). https://doi.org/10.32672/jnkti.v7i6.8345

Nurrizki, M. A. (2024). Analisis Keamanan Website Desa Budaya DIY Dengan Metode Penetration Testing (Pentest) dan OWASP ZAP. *Jurnal Aplikasi Teknologi Informasi dan Manajemen (JATIM)*, *5*(1), 22–27. https://doi.org/10.31102/jatim.v5i1.2620

Panggah Widiandana, Wicaksono Yuli Sulistyo, Rokhayati, Afwa Aulia Rahma, & Ahmad Fatih Riziq. (2025). Implementasi Digitalisasi Layanan Posyandu Melalui Sistem Informasi Pandurejo Untuk Meningkatkan Efektivitas Pelayanan Kesehatan Di Kalurahan Demangrejo. *Jubaedah : Jurnal Pengabdian dan Edukasi Sekolah (Indonesian Journal of Community Services and School Education)*. https://doi.org/10.46306/jub.v5i3

Putra, B. S., & Santoso, D. B. (2025). Analisis Keamanan Website Berbasis WordPress melalui Penetration Testing untuk Meningkatkan Keamanan Digital. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, *9*(3), 981–990. https://doi.org/10.35870/jtik.v9i3.3692

Rahmahdany, S., Lamada, M., & Jaya, H. (2024). ANALISIS KEAMANAN WEBSITE TERHADAP SERANGAN PACKET SNIFFING DI JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER FAKULTAS TEKNIK UNIVERSITAS NEGERI MAKASSAR. *Jurnal Sains dan Sistem Teknologi Informasi*, *6*(1), 1–8. https://doi.org/10.59811/xrjkp375

Sahira, M. S., Indriati, R., & Ristyawan, A. (2025). Analisis Risiko Website Sistem Keamanan Informasi Menggunakan Metode Fmea dan Framework ISO/IEC 27002:2022. *JSITIK: Jurnal Sistem Informasi dan Teknologi Informasi Komputer*, *3*(2), 128–138. https://doi.org/10.53624/jsitik.v3i2.722

Sahyudi, M., & Susanto, E. R. (2025). Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning. *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, *5*(1), 105–116. https://doi.org/10.54259/satesi.v5i1.3997

Syahab, A. S. (2023). ANALISIS AUDIT KEAMANAN INFORMASI WEBSITE MENGGUNAKAN METODE NETWORK MAPPER DAN QUALYS SSL. *Jurnal Manajemen Informatika dan Sistem Informasi*, *6*(1), 39–47. https://doi.org/10.36595/misi.v6i1.742

Widiandana, P., Surya, R. A., Aulia, M. I., Sakmar, M., Hartinah, S., & Aly, M. H. (2024). *Optimizing Lecture Schedules with the Scheduling Information System*. *2*(1).

Wijayakusuma, M. G., Surojudin, N., & Sanudin . (2026). Analisis Risiko Keamanan Informasi pada Website Perusahaan Menggunakan ISO/IEC 27001 dan ISO/IEC 27005. *JURNAL INFORMATIKA*, *15*(1), 73–86. https://doi.org/10.55340/jiu.v15i1.2711

Yeovandi, F., Sabariman, S., & Prasetyo, S. E. (2025). Evaluasi Keamanan Sistem Autentikasi Biometrik pada Smartphone dan Rekomendasi Implementasi Optimal. *JTIM : Jurnal Teknologi Informasi dan Multimedia*, *7*(1), 133–148. https://doi.org/10.35746/jtim.v7i1.653

Ys, Moh. A. F., Zen, B. P., & Wasitarini, D. E. (2024). Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. *Cyber Security dan Forensik Digital*, *6*(2), 76–82. https://doi.org/10.14421/csecurity.2023.6.2.4190