ANALISIS KEAMANAN INFORMASI PADA SISTEM AKADEMIK TERPADU MENGGUNAKAN FRAMEWORK COMPTIA SECURITY+

Putri Bilkist Ramadani, Awang Andhyka, Syahri Mu'min
Sistem Informasi, Universitas Nahdlatul Ulama Sidoarjo
Rangkah Kidul, Kec. Sidoarjo, Kabupaten Sidoarjo, Jawa Timur, Indonesia
Bilkistputri1@gmail.com

ABSTRAK

Sistem Akademik Terpadu (SAT) merupakan sistem informasi utama perguruan tinggi yang mengelola proses akademik dan data penting secara terintegrasi, sehingga berpotensi menjadi target ancaman keamanan informasi. Permasalahan penelitian ini adalah belum adanya analisis keamanan yang sistematis untuk menilai kesiapan SAT dalam menghadapi ancaman siber. Penelitian ini bertujuan untuk menganalisis tingkat keamanan informasi pada SAT menggunakan kerangka CompTIA Security+ yang mencakup lima domain utama. Metode penelitian yang digunakan adalah pendekatan deskriptif evaluatif melalui observasi konfigurasi sistem, analisis log server, dan pengujian kerentanan pada modul utama SAT. Hasil penelitian menunjukkan adanya kelemahan pada kontrol autentikasi, konfigurasi server, serta prosedur respons insiden. Tingkat kepatuhan keamanan berdasarkan domain CompTIA Security+ menunjukkan nilai rata-rata sebesar 58%, yang mengindikasikan bahwa SAT masih memerlukan peningkatan keamanan. Hasil analisis ini digunakan sebagai dasar penyusunan rekomendasi peningkatan keamanan yang lebih terstruktur dan berkelanjutan.

Kata kunci: *Keamanan informasi, sistem akademik, CompTIA Security+, analisis risiko, log server.*

1. PENDAHULUAN

Transformasi digital di lingkungan perguruan tinggi mendorong peningkatan penggunaan Sistem Akademik Terpadu (SAT) sebagai platform utama dalam mendukung proses akademik dan administrasi. SAT berperan penting dalam pengelolaan data mahasiswa, pelaksanaan perkuliahan, transaksi keuangan, hingga layanan administratif lainnya yang terintegrasi secara digital. Tingginya ketergantungan institusi terhadap sistem berbasis teknologi menjadikan aspek keamanan informasi sebagai faktor krusial yang harus diperhatikan. Kerahasiaan, integritas, dan ketersediaan data akademik perlu dijaga secara konsisten agar operasional perguruan tinggi dapat berjalan dengan baik serta terhindar dari gangguan akibat ancaman siber.

Dalam beberapa tahun terakhir, insiden keamanan informasi pada sistem pendidikan tinggi di Indonesia semakin sering terjadi. Berbagai bentuk serangan seperti malware, SQL injection, pengambilalihan akun, dan kebocoran data menunjukkan bahwa sistem akademik berbasis web memiliki potensi risiko yang tinggi apabila tidak dilengkapi dengan mekanisme keamanan yang memadai. Meskipun sebagian perguruan tinggi telah menerapkan pengamanan teknis, evaluasi keamanan sering kali dilakukan secara parsial dan tidak terstruktur. Evaluasi tersebut umumnya berfokus pada aspek operasional sehari-hari tanpa mengacu pada kerangka standar keamanan yang diakui secara internasional. Kondisi ini menimbulkan kesenjangan antara implementasi kontrol keamanan teknis dan kebutuhan pengelolaan risiko yang lebih komprehensif.

Salah satu kerangka yang dapat digunakan sebagai acuan evaluasi keamanan adalah CompTIA Security+ [1]. Kerangka ini mencakup lima domain utama, yaitu *Threats, Attacks and Vulnerabilities*, *Architecture and Design*, *Implementation*, *Operations and Incident Response*, serta *Governance, Risk and Compliance*. Security+ menyediakan pendekatan evaluasi yang bersifat teknis dan operasional sehingga memungkinkan identifikasi area kritis keamanan secara sistematis. Kerangka ini dinilai relevan untuk mengevaluasi SAT yang memiliki tingkat interaksi pengguna tinggi serta integrasi dengan berbagai layanan internal dan eksternal.

Permasalahan utama dalam penelitian ini adalah belum adanya kajian keamanan informasi pada Sistem Akademik Terpadu yang secara khusus menggunakan kerangka CompTIA Security+ sebagai landasan analisis. Padahal, SAT mengelola proses penting seperti penerimaan mahasiswa baru, pengelolaan data akademik, transaksi pembayaran, serta sinkronisasi data ke Pangkalan Data Pendidikan Tinggi (PDDIKTI). Di banyak institusi pendidikan, pengelolaan keamanan informasi masih menghadapi kendala berupa keterbatasan sumber daya teknis, minimnya dokumentasi kebijakan keamanan, serta belum optimalnya mekanisme pemantauan log server untuk mendeteksi anomali sejak dini. Kondisi ini berpotensi menimbulkan risiko terhadap kerahasiaan, integritas, dan ketersediaan data akademik.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis keamanan informasi pada Sistem Akademik Terpadu menggunakan kerangka CompTIA Security+ sebagai instrumen evaluasi. Tujuan khusus penelitian ini meliputi: mengidentifikasi tingkat kerentanan sistem berdasarkan lima domain utama Security+; mengevaluasi kesesuaian konfigurasi sistem, prosedur operasional, serta kontrol keamanan yang telah

diterapkan; serta menyusun rekomendasi peningkatan keamanan berdasarkan temuan analisis dan tingkat risiko yang dihasilkan. Rencana penyelesaian masalah dilakukan melalui pendekatan evaluatif dengan analisis konfigurasi sistem, pemeriksaan log server, dan penilaian kerentanan. Dengan demikian, penelitian ini diharapkan mampu memberikan gambaran kondisi keamanan SAT secara menyeluruh serta menghasilkan rekomendasi perbaikan yang dapat diterapkan secara praktis oleh pengelola sistem akademik.

2. TINJAUAN PUSTAKA

2.1. Sistem Akademik Terpadu (SAT)

Sistem Akademik Terpadu (SAT) merupakan sistem informasi utama yang digunakan perguruan tinggi untuk mendukung seluruh proses akademik dan administrasi secara digital. SAT umumnya mencakup rangkaian proses mulai dari pendaftaran mahasiswa baru, verifikasi pembayaran menggunakan Virtual Account (VA) perbankan, pengelolaan Kartu Rencana Studi (KRS), penilaian, hingga penyimpanan histori akademik mahasiswa. Selain itu, SAT juga terhubung dengan layanan eksternal seperti gateway pembayaran bank, sistem keuangan internal, serta layanan Pelaporan Pendidikan Tinggi (PDDIKTI) untuk sinkronisasi data akademik secara berkala. Dengan demikian, SAT [1] tidak hanya berfungsi sebagai sistem transaksi akademik, tetapi juga sebagai pusat integrasi antar-layanan yang wajib menjaga konsistensi, keutuhan, dan keamanan data.

Kompleksitas arsitektur SAT menjadikannya sangat rentan terhadap berbagai ancaman keamanan, terutama karena melibatkan banyak titik akses pengguna (mahasiswa, dosen, admin), integrasi API, serta pertukaran data dengan pihak ketiga. Pada tahap pendaftaran mahasiswa, proses pembayaran VA menjadi salah satu titik kritis yang harus diamankan karena melibatkan data identitas dan transaksi finansial. Pada tahap akademik, aktivitas KRS yang terjadi secara masif dalam periode tertentu sering menimbulkan lonjakan trafik [2] sehingga berpotensi dieksploitasi oleh serangan otomatis maupun celah autentikasi. Proses sinkronisasi ke PDDIKTI juga memiliki risiko keamanan akibat penggunaan API, token autentikasi, serta potensi kebocoran data apabila konfigurasi server tidak memadai [3].

Sejumlah penelitian menunjukkan bahwa sistem akademik di Indonesia kerap mengalami serangan terhadap server seperti SQL injection, pencurian kredensial, penyalahgunaan akses admin, brute force login, dan serangan bot pada modul pendaftaran [4]. Masalah umum lainnya mencakup kurangnya dokumentasi keamanan, minimnya pemantauan log server, serta belum adanya penerapan standar keamanan yang konsisten. Oleh karena itu, SAT menjadi objek penting untuk dianalisis secara komprehensif guna memastikan bahwa seluruh alur layanan, mulai dari pendaftaran mahasiswa hingga sinkronisasi PDDIKTI, berjalan aman dan sesuai praktik keamanan yang direkomendasikan [5]. Analisis yang terstruktur diharapkan mampu mengidentifikasi titik lemah sistem, menilai efektivitas kontrol keamanan yang telah diterapkan, serta memberikan dasar pengambilan keputusan dalam upaya peningkatan keamanan informasi di lingkungan perguruan tinggi.

2.2. Keamanan Informasi

Keamanan informasi merupakan serangkaian proses, kebijakan, dan kontrol yang dirancang untuk melindungi aset informasi dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data. Dalam konteks perguruan tinggi, keamanan informasi menjadi semakin penting seiring meningkatnya digitalisasi layanan akademik dan administratif. Sistem Akademik Terpadu (SAT) menyimpan data sensitif seperti identitas mahasiswa, nilai, data transaksi keuangan, dan rekaman aktivitas akademik yang wajib dilindungi dari akses tidak sah maupun manipulasi. Prinsip Confidentiality, Integrity, Availability (CIA) menjadi dasar untuk memastikan bahwa setiap komponen sistem dapat bekerja secara aman dan konsisten.

Ancaman terhadap keamanan informasi pada SAT dapat berasal dari faktor internal maupun eksternal. Ancaman internal dapat berupa kesalahan konfigurasi server, lemahnya pengelolaan kredensial administrator, hingga kelalaian pengguna dalam menjaga kerahasiaan akun. Sementara ancaman eksternal mencakup serangan SQL injection, cross-site scripting, pencurian kredensial, serangan bot terhadap modul login atau pendaftaran, percobaan eksploitasi celah aplikasi, serta serangan otomatis pada API integrasi. Lemahnya pengawasan log, tidak adanya sistem deteksi intrusi, dan kontrol akses yang tidak memadai sering menjadi penyebab utama terjadinya pelanggaran keamanan informasi di institusi pendidikan.

Berbagai standar keamanan seperti ISO/IEC 27001, NIST Cybersecurity Framework, dan OWASP Top Ten telah digunakan untuk meningkatkan keamanan aplikasi dan infrastruktur. Namun, penerapan standar tersebut sering dianggap kompleks untuk lingkungan perguruan tinggi yang memiliki keterbatasan sumber daya teknis. Oleh karena itu, diperlukan kerangka evaluasi keamanan yang lebih praktis namun tetap mencakup aspek-aspek fundamental keamanan [6], sehingga dapat digunakan sebagai acuan bagi administrator sistem dalam menilai kesiapan keamanan SAT dan menentukan prioritas perbaikan.

2.3. Kerangka Evaluasi CompTIA Security+

CompTIA Security+ merupakan salah satu kerangka kompetensi keamanan informasi yang banyak digunakan sebagai standar kemampuan dasar di industri. Framework ini mencakup lima domain yang saling melengkapi: [7] Threats, Attacks and Vulnerabilities, [1] Architecture and Design, [8]

Implementation, [2] Operations and Incident Response, dan [6] Governance, Risk and Compliance. Berbeda dengan standar keamanan formal seperti ISO 27001 yang lebih fokus pada kebijakan manajemen organisasi, Security+ lebih bersifat teknis dan operasional sehingga sesuai untuk mengevaluasi sistem yang memiliki intensitas interaksi pengguna dan integrasi layanan yang tinggi, seperti SAT.

Setiap domain dalam Security+ memberikan perspektif yang berbeda terhadap risiko keamanan. Domain Threats, Attacks and Vulnerabilities membantu mengidentifikasi bentuk ancaman yang relevan bagi SAT, termasuk serangan yang menargetkan modul login, API internal, atau proses pembayaran VA. Domain Architecture and Design digunakan untuk menilai apakah arsitektur SAT telah menerapkan prinsip keamanan seperti segmentasi jaringan, keamanan basis data, dan pengamanan API. Domain Implementation mengevaluasi keamanan autentikasi, enkripsi data, serta konfigurasi server. Domain Operations and Incident Response menilai kesiapan institusi dalam melakukan pemantauan log, deteksi anomali, serta penanganan insiden.

Sementara itu, domain Governance, Risk and Compliance mengukur kesesuaian kebijakan keamanan, manajemen risiko, dan kepatuhan terhadap regulasi seperti pelaporan PDDIKTI atau peraturan perlindungan data. Penggunaan Security+ sebagai kerangka evaluasi memberikan manfaat berupa kemudahan interpretasi, kesesuaian dengan praktik keamanan modern, serta ruang adaptasi yang fleksibel terhadap kebutuhan institusi pendidikan. Kerangka ini membantu menghasilkan pemetaan kondisi keamanan yang lebih terukur [9] sehingga dapat menjadi dasar penyusunan rekomendasi perbaikan bagi administrator SAT.

2.4. Analisis Log dan Deteksi Kerentanan

Analisis log merupakan proses penting dalam keamanan informasi karena memberikan catatan rinci mengenai aktivitas pengguna, akses sistem, error, dan percobaan serangan yang terjadi pada aplikasi maupun infrastruktur. Dalam SAT, analisis log dapat mengungkap berbagai aktivitas abnormal seperti percobaan *brute force* pada modul login, lonjakan trafik yang tidak wajar saat periode KRS, percobaan injeksi SQL pada endpoint pendaftaran, anomali transaksi VA, hingga akses tidak sah pada API yang digunakan untuk sinkronisasi data ke PDDIKTI. Log server web, log WAF, log aplikasi, dan log database menjadi sumber data utama dalam mendeteksi potensi ancaman.

Selain analisis log, deteksi kerentanan (*vulnerability assessment*) digunakan untuk mengidentifikasi kelemahan dalam arsitektur, konfigurasi, maupun kode aplikasi. Kerentanan dapat muncul akibat penggunaan parameter yang tidak tervalidasi, kesalahan konfigurasi firewall, pemakaian versi aplikasi yang rentan, hingga akses admin yang tidak dibatasi. Penilaian kerentanan ini penting dilakukan secara berkala karena lingkungan SAT selalu berubah mengikuti siklus akademik dan integrasi sistem, sehingga risiko keamanan juga berubah dari waktu ke waktu. Integrasi antara analisis data log dan deteksi kerentanan memberikan gambaran keamanan yang lebih komprehensif. Log menunjukkan aktivitas yang benar-benar terjadi, sementara deteksi kerentanan menunjukkan potensi risiko yang mungkin belum dieksploitasi. Kombinasi keduanya memungkinkan administrator SAT untuk mengidentifikasi area risiko prioritas, memitigasi ancaman lebih cepat, serta menyesuaikan kebijakan keamanan sesuai kebutuhan operasional kampus.

2.5. Penelitian Terdahulu

Sejumlah penelitian terdahulu telah membahas aspek keamanan sistem informasi di lingkungan perguruan tinggi dengan berbagai pendekatan dan kerangka kerja. Nugroho dan Pradana [11] melakukan analisis keamanan sistem informasi akademik menggunakan pendekatan risiko dan menemukan bahwa kelemahan utama terletak pada kontrol autentikasi dan pengelolaan akses pengguna. Penelitian tersebut menekankan pentingnya evaluasi keamanan berbasis risiko untuk mengidentifikasi area kritis pada sistem akademik.

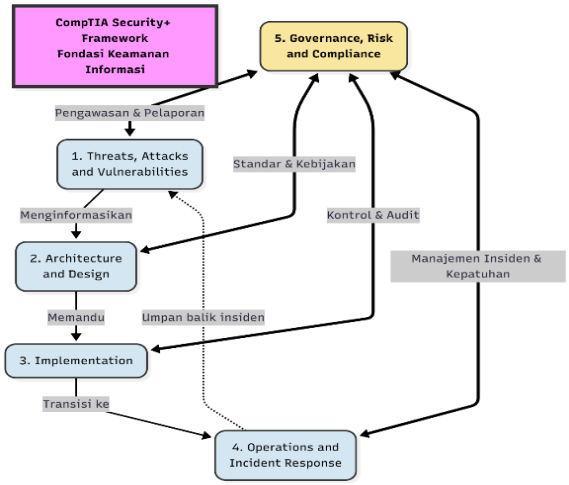
Penelitian lain oleh Rosyid dan Santoso [12] mengevaluasi keamanan aplikasi web akademik menggunakan OWASP Top Ten dan ISO/IEC 27001. Hasil penelitian menunjukkan bahwa sebagian besar kerentanan berasal dari kesalahan konfigurasi server dan validasi input yang tidak memadai. Meskipun standar tersebut mampu memberikan gambaran kebijakan keamanan, penerapannya dinilai cukup kompleks untuk lingkungan perguruan tinggi dengan keterbatasan sumber daya teknis. Alshamrani dan Ghorbani [13] meneliti efektivitas analisis log dalam mendeteksi serangan aplikasi web dan menyimpulkan bahwa log server dan Web Application Firewall (WAF) merupakan sumber data penting dalam mengidentifikasi serangan serta anomali lalu lintas. Namun, penelitian tersebut juga mencatat adanya tantangan false positive yang dapat berdampak pada ketersediaan layanan apabila tidak dikelola dengan baik.

Berbeda dengan penelitian sebelumnya, penelitian ini menggunakan kerangka CompTIA Security+ yang bersifat teknis dan operasional untuk mengevaluasi keamanan Sistem Akademik Terpadu secara menyeluruh. Pendekatan ini mengombinasikan analisis konfigurasi sistem, pemeriksaan log server, dan penilaian kerentanan sehingga mampu memberikan gambaran kondisi keamanan yang lebih praktis dan terukur. Dengan demikian, penelitian ini melengkapi penelitian terdahulu dengan menghadirkan evaluasi keamanan berbasis domain yang lebih adaptif terhadap kebutuhan operasional sistem akademik.

3. METODE PENELITIAN

3.1. Desain Penelitian

Penelitian ini menggunakan pendekatan deskriptif evaluatif untuk menganalisis tingkat keamanan Sistem Akademik Terpadu (SAT) yang digunakan di Universitas Nahdlatul Ulama Sidoarjo (UNUSIDA). Evaluasi yang dilakukan berdasarkan kerangka CompTIA Security+ dengan melakukan analisis terhadap konfigurasi sistem, pemeriksaan log server, integrasi layanan, serta penilaian kerentanan pada modul-modul utama SAT.



Gambar 1. Kerangka Keamanan CompTIA Security+.

Gambar 1 menunjukkan hubungan lima domain utama dalam kerangka CompTIA Security+ yang digunakan sebagai acuan evaluasi. Setiap domain saling berinteraksi dalam proses pengamanan sistem, mulai dari identifikasi ancaman, perancangan arsitektur, implementasi kontrol, operasi dan respons insiden, hingga manajemen tata kelola dan kepatuhan. Kerangka ini menjadi dasar dalam pemetaan temuan keamanan pada SAT.

Lingkup analisis mencakup proses Penerimaan Mahasiswa Baru (PMB) yang terhubung dengan Sistem Informasi Manajemen (SIM), transaksi pembayaran menggunakan Virtual Account (VA), proses akademik seperti pengisian Kartu Rencana Studi (KRS), serta mekanisme sinkronisasi data akademik ke Pangkalan Data Pendidikan Tinggi (PDDIKTI).

3.2. Objek dan Lingkup Penelitian

Objek penelitian adalah Sistem Akademik Terpadu (SAT) UNUSIDA yang mencakup:

a. Proses Penerimaan Mahasiswa Baru Terintegrasi dengan Sistem Informasi Manajemen (SIM).
b. Transaksi pembayaran Virtual Account (VA) Menggunakan API bank untuk verifikasi otomatis.
c. Proses akademik mahasiswa, seperti:
   - Pengisian Kartu Rencana Studi (KRS)
   - Manajemen nilai
   - Aktivitas login dan autentikasi pengguna
d. Sinkronisasi data ke PDDIKTI
   Meliputi integrasi API dan proses validasi data.

Lingkup analisis difokuskan pada aspek keamanan aplikasi, server, autentikasi, jaringan, dan log aktivitas. Sinkronisasi data ke PDDIKTI meliputi integrasi API dan proses validasi data. Lingkup analisis difokuskan pada keamanan aplikasi, server, autentikasi, jaringan, serta pemantauan log aktivitas sistem.

3.3. Sumber dan Teknik Pengumpulan Data

a. Observasi Sistem
   Pengamatan langsung terhadap arsitektur SAT, konfigurasi server, modul PMB, KRS, VA, dan integrasi PDDIKTI.
b. Analisis Log
   Mengumpulkan log dari:
   - Web server (error & access log)
   - Log aplikasi SAT
   - Log autentikasi
   - Log firewall/WAF seperti ModSecurity
   - Log transaksi VA.
c. Pengujian Kerentanan
   Meliputi:
   - SQL Injection
   - XSS
   - Weak Authentication
   - Misconfiguration server
   - API vulnerability
d. Dokumentasi
   Pengumpulan SOP, kebijakan keamanan, dokumen akses admin, dan pedoman sinkronisasi PDDIKTI.

3.4. Sumber dan Teknik Pengumpulan Data

Instrumen ini berfungsi untuk memetakan temuan keamanan secara sistematis sehingga hasil evaluasi dapat dijelaskan secara terukur dan dapat dibandingkan antar-domain. Tabel berikut menyajikan indikator penilaian pada masing-masing domain Security+ yang digunakan dalam penelitian ini.

Tabel 1. Instrumen Evaluasi Keamanan

Domain	Indikator Penilaian
Threats Vulnerabilities	Jenis serangan, anomali log, kerentanan aplikasi/server
Architecture Design	Struktur sistem, perlindungan database, keamanan API
Implementation	Password policy, enkripsi, konfigurasi server, validasi input
Operations & Incident Response	Monitoring log, deteksi anomali, prosedur respons insiden
Governance, Risk & Compliance	Kebijakan keamanan, perlindungan data, kepatuhan PDDIKTI

Tabel 1 tersebut menjadi dasar pengelompokan temuan keamanan selama proses evaluasi. Setiap indikator digunakan untuk menilai kondisi aktual pada domain yang bersangkutan, sehingga hasil analisis

dapat disajikan secara terstruktur dan mendukung proses penentuan tingkat kepatuhan serta risiko keamanan.server,

4. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil evaluasi keamanan Sistem Akademik Terpadu (SAT) berdasarkan lima domain CompTIA Security+. Evaluasi dilakukan melalui analisis log server, pengujian kerentanan, observasi arsitektur sistem, serta telaah terhadap kebijakan keamanan yang diterapkan pada lingkungan operasional SAT. Proses evaluasi ini mencakup pengumpulan data teknis dari aktivitas server, analisis pola serangan, pemeriksaan konfigurasi aplikasi dan API, serta pemetaan kontrol keamanan yang berlaku pada setiap modul sistem.

Untuk memperoleh gambaran yang komprehensif, seluruh temuan yang diperoleh selama proses analisis diklasifikasikan ke dalam modul-modul utama SAT, seperti PMB, pembayaran Virtual Account (VA), pengisian KRS, integrasi PDDIKTI, dan dashboard administrasi. Klasifikasi ini bertujuan memudahkan interpretasi hasil dengan memisahkan area yang paling sering mengalami potensi ancaman dari area yang memiliki kontrol keamanan relatif lebih stabil.

Tabel 2. Daftar Temuan Keamanan per Modul SAT

Modul Sistem	Temuan	Keterangan
PMB/SIM	Validasi input kurang, brute force login	Berpotensi akses ilegal; memerlukan aturan WAF tambahan
Pembayaran VA	Error log bocor info sistem	Risiko kebocoran data; perlu sanitasi dan masking log
KRS	Beban server tinggi, tidak ada rate limit	Dapat menyebabkan gangguan layanan; perlu pembatasan request
API PDDIKTI	Token tidak rotasi	Risiko penyalahgunaan akses; perlu kebijakan rotasi token.
Dashboard Admin	Password policy lemah	Perlu enforcement password kuat

Tabel 2 menampilkan ringkasan temuan keamanan pada beberapa modul SAT yang menjadi dasar identifikasi area rawan. Untuk memperoleh gambaran yang lebih terstruktur, temuan ini kemudian dipetakan ke dalam domain evaluasi Security+ untuk mengetahui bagian keamanan mana yang masih memerlukan perhatian lebih dalam proses perbaikan. Selain itu, pemetaan temuan ke dalam domain Security+ memungkinkan proses penilaian dilakukan secara sistematis berdasarkan standar kompetensi keamanan informasi yang diakui secara luas. Hasil-hasil tersebut kemudian disajikan dalam bentuk tabel dan visualisasi untuk memberikan gambaran yang lebih jelas mengenai tingkat kerentanan dan kekuatan keamanan pada masing-masing domain. Pemetaan temuan ke domain Security+ memungkinkan penilaian sistematis, dengan hasil disajikan dalam tabel untuk memperjelas tingkat kerentanan tiap domain.

Tabel 3. Temuan Keamanan Berdasarkan Domain

Domain	Temuan	Dampak	Kategori
Threats & Vulnerabilities	Brute force login, input tidak tervalidasi	Akses ilegal	Tinggi
Architecture & Design	API tanpa rate limiting	Beban server, eksploitasi	Sedang
Implementation	Password lemah, SSL tanpa HSTS	Kebocoran data	Tinggi
Operations & Incident Response	Monitoring belum rutin	Serangan tidak terdeteksi	Sedang
Governance, Risk & Compliance	Kebijakan umum	Risiko pelanggaran regulasi	Sedang

Tabel 3 diatas memberikan gambaran mengenai posisi temuan keamanan pada masing-masing domain Security+. Dari pemetaan tersebut terlihat bahwa beberapa domain memiliki kelemahan yang lebih menonjol, terutama pada area yang berkaitan terhadap sistem.

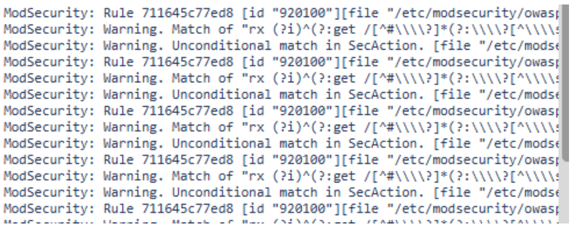
Gambar 2. Log Apache Serangan SQL Injection.

Analisis terhadap Gambar 2 log Apache menunjukkan adanya pola aktivitas mencurigakan yang mengarah pada upaya eksploitasi, seperti permintaan berulang dari alamat IP yang sama, percobaan brute force, serta mengindikasikan serangan SQL Injection maupun scanning otomatis.

Tabel 4. Penilaian Kepatuhan Keamanan per Domain

Domain	Kontrol Dipenuhi	Total Kontrol	Kepatuhan (%)
Threats & Vulnerabilities	4	7	57%
Architecture & Design	5	8	62%
Implementation	3	7	43%
Operations & Incident Response	4	6	67%
Governance, Risk & Compliance	5	8	62%
Rata-rata	-	-	**58%**

Tingkat kepatuhan yang ditampilkan pada Tabel 3 perlu dianalisis lebih lanjut untuk mengetahui besarnya risiko yang ditimbulkan oleh setiap temuan. Oleh karena itu, dilakukan penilaian risiko berdasarkan tingkat kemungkinan dan dampak dari masing-masing temuan. Analisis ini penting karena tingkat kepatuhan saja tidak selalu menggambarkan tingkat ancaman secara keseluruhan. Beberapa kontrol mungkin tidak terpenuhi tetapi memiliki dampak rendah, sementara sebagian lainnya meskipun jumlahnya sedikit dapat menimbulkan risiko yang signifikan terhadap operasional SAT. Dengan melakukan penilaian risiko, setiap temuan dapat dipetakan berdasarkan prioritas penanganan, sehingga institusi mampu menentukan langkah mitigasi yang paling mendesak. Proses ini juga memungkinkan pemahaman yang lebih mendalam mengenai hubungan antara kelemahan kontrol dan potensi eksploitasi yang mungkin terjadi pada sistem



```
ModSecurity: Rule 711645c77ed8 [id "920100"][file "/etc/modsecurity/owasp
ModSecurity: Warning. Match of "rx (?i)^(?:get /[^#\\\\?]*(?:\\\\?[^\\\\s
ModSecurity: Warning. Unconditional match in SecAction. [file "/etc/modse
ModSecurity: Rule 711645c77ed8 [id "920100"][file "/etc/modsecurity/owasp
ModSecurity: Warning. Match of "rx (?i)^(?:get /[^#\\\\?]*(?:\\\\?[^\\\\s
ModSecurity: Warning. Unconditional match in SecAction. [file "/etc/modse
ModSecurity: Rule 711645c77ed8 [id "920100"][file "/etc/modsecurity/owasp
ModSecurity: Warning. Match of "rx (?i)^(?:get /[^#\\\\?]*(?:\\\\?[^\\\\s
ModSecurity: Warning. Unconditional match in SecAction. [file "/etc/modse
ModSecurity: Rule 711645c77ed8 [id "920100"][file "/etc/modsecurity/owasp
ModSecurity: Warning. Match of "rx (?i)^(?:get /[^#\\\\?]*(?:\\\\?[^\\\\s
ModSecurity: Warning. Unconditional match in SecAction. [file "/etc/modse
ModSecurity: Rule 711645c77ed8 [id "920100"][file "/etc/modsecurity/owasp
```

Gambar 3. Log ModSecurity – Upaya Akses Berkas

Gambar 3 memperlihatkan percobaan akses terhadap berkas sensitif yang diblokir oleh ModSecurity. Aktivitas ini menunjukkan adanya potensi eksploitasi yang perlu diperhatikan karena dapat memengaruhi kerahasiaan konfigurasi aplikasi dan meningkatkan risiko kompromi sistem. Temuan ini menjadi indikator bahwa SAT tidak hanya menghadapi ancaman berbasis input berbahaya, tetapi juga upaya akses langsung ke berkas kritis. Berdasarkan kondisi tersebut, penilaian risiko dilakukan untuk menentukan tingkat ancaman dan Hasil penilaiannya disajikan pada Tabel 5.

Tabel 5. Penilaian Risiko (Risk Assessment)

Temuan	L	I	Skor	Kat.
Brute force login	4	4	16	Tinggi
Password policy lemah	5	3	15	Tinggi
API tanpa rate limiting	3	3	9	Sedang
Log tidak rutin	3	4	12	Sedang
Data pribadi kurang terlindungi	2	4	8	Sedang

Tabel 5 diatas menampilkan hasil penilaian risiko berdasarkan temuan kerentanan yang teridentifikasi. Kolom "L" menunjukkan tingkat kemungkinan (likelihood) terjadinya ancaman, sedangkan kolom "I" menggambarkan besarnya dampak (impact) jika ancaman tersebut terjadi. Nilai "Skor" diperoleh dari perkalian keduanya, yang kemudian diklasifikasikan dalam kolom "Kat." untuk menentukan tingkat risiko masing-masing temuan. Rekomendasi ini membantu menentukan prioritas mitigasi pada setiap domain keamanan.

Tabel 6. Rekomendasi Perbaikan Keamanan

Domain	Masalah	Mitigasi	Prioritas
Threats & Vulnerabilities	Brute force login	Implementasi rate limit & captcha	Tinggi
Architecture & Design	API tidak dilindungi	Tambah API gateway & rate limiting	Sedang
Implementation	Password lemah	Terapkan strong password policy & HSTS	Tinggi
Operations & Incident Response	Monitoring pasif	Buat dashboard log & alert otomatis	Tinggi
Governance, Risk & Compliance	Kebijakan umum	Penyusunan SOP dan kebijakan teknis	Sedang

Tabel 6 merangkum rekomendasi perbaikan yang disesuaikan dengan tingkat risiko dan temuan pada setiap domain keamanan. Rekomendasi ini menjadi dasar bagi institusi untuk menentukan langkah prioritas dalam meningkatkan keamanan SAT, baik pada aspek teknis maupun kebijakan operasional.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengevaluasi tingkat keamanan Sistem Akademik Terpadu (SAT) menggunakan kerangka CompTIA Security+ melalui analisis log, pemeriksaan konfigurasi, dan penilaian kerentanan pada lima domain utama. Hasil penelitian menunjukkan bahwa tingkat kepatuhan keamanan SAT berada pada kategori cukup, dengan nilai rata-rata kepatuhan sekitar 58%, di mana domain *Implementation dan Threats & Vulnerabilities* menjadi area yang paling lemah dengan tingkat kepatuhan masing-masing di bawah 50% serta risiko tertinggi pada temuan seperti *brute force login, password policy* yang tidak memadai, dan kurangnya pembatasan akses pada API. *Domain Operations and Incident Response* juga ditemukan belum optimal karena tidak adanya mekanisme pemantauan log dan respons insiden yang terstruktur. Analisis risiko menunjukkan bahwa beberapa temuan memiliki skor risiko tinggi dengan nilai mencapai 15–16, yang menandakan perlunya upaya mitigasi segera. Berdasarkan temuan tersebut, penelitian ini merekomendasikan peningkatan pada kontrol autentikasi, penguatan konfigurasi server, penerapan rate limiting, optimalisasi sanitasi log, serta penyusunan kebijakan keamanan informasi yang lebih komprehensif, khususnya terkait perlindungan data dan integrasi PDDIKTI. Untuk penelitian selanjutnya, disarankan menggunakan dataset log yang lebih panjang, menambah variasi indikator risiko, serta

mengintegrasikan metode deteksi anomali otomatis berbasis machine learning untuk memperoleh hasil yang lebih komprehensif, prediktif, dan akurat dalam menilai ketahanan keamanan SAT.

DAFTAR PUSTAKA

[1] Y. Alabdan, "A survey on cybersecurity awareness in higher education," *Applied Computing and Informatics,* pp. no. 1, pp. 90–102, 2022, vol. 18

[2] A. M. Dener, "Evaluation of intrusion detection systems for web-based applications," *IEEE Access,* pp. pp. 115931–115944, 2021, vol. 9

[3] M. A. a. A. Ghorbani, "A study on log-based anomaly detection techniques," *IEEE Communications Surveys & Tutorials,* pp. no. 4, pp. 1–24, 2021., vol. 23

[4] A. Y. T. a. H. M. Hasan, "Security analysis of university information systems using NIST and ISO standards".

[5] S. K. H. a. M. S. Hossain, "Web application vulnerability assessment using OWASP and automated tools," in 2020 IEEE International Conference on Computer and Information Technologyin 2020 IEEE International Conference on Computer and Information Technology, p. pp. 341–346.

[6] M. F. A. a. N. F. Z. N. S. Sultan, "Security risk assessment for academic information systems: A systematic review," Journal of Information Security and Applications, pp. pp. 1–12, 2021, vol. 58.

[7] S. G. Raj, "Risk assessment model for information systems using likelihood–impact metrics," International Journal of Information Security Science, pp. no. 2, pp. 45–54, 2022, vol. 11.

[8] S. U. a. M. H. Rahman, "A review of the CompTIA Security+ domains and their application in organizational security assessment," International Journal of Cyber Research and Education, pp. pp. 22–30, 2020, vol. 5, no. 1.

[9] Z. H. a. M. X. W. Li, "Machine learning-based intrusion detection for cloud services," IEEE Transactions on Cloud Computing, pp. no. 3, pp. 2345–2358, 2022, vol. 10.

[10] M. H. K. a. T. Ahmed, "Assessment of password security policies in higher education systems," in 2020 IEEE Region 10 Symposium (TENSYMP), p. pp. 580–585.

[11] R. A. N. a. S. Abdullah, "A framework for evaluating API security in integrated information systems," Indonesian Journal of Electrical Engineering and Computer Science, p. vol. 23, vol. 23.

[12] K. S. R. a. L. S. Reddy, "Security configuration weaknesses in server deployments: A measurement study," in 2022 IEEE World Conference on Computing and Communication Technologies, p. pp. 142–148.

[13] A. Ibrahim, "WAF effectiveness in mitigating web application attacks: An empirical study," IEEE Access, pp. pp. 50123–50135, 2022, vol. 10.

[14] D. N. a. A. Pradana, "Analisis keamanan sistem informasi akademik menggunakan pendekatan risiko," Jurnal Teknologi Informasi dan Ilmu Komputer, pp. pp. 475–484, 2021, vol. 8 no. 3.

[15] H. F. R. a. M. Santoso, "Evaluasi keamanan aplikasi web akademik berbasis OWASP dan ISO 27001," Jurnal RESTI, pp. pp. 335–344, 2023, vol. 7, no. 2.

[16] A. M. B. R. M. J. a. C. S. A. Febriani, "Analisis Kerentanan Keamanan Sistem Informasi Akademik Menggunakan OWASP-ZAP Di Universitas Islam Indragir," Jurnal Sistem Informas, Vols. vol. 2, no. 6, p. pp. 409–420, 2024.

[17] E. A. a. D. Syamsuar, "Assessment Risk Terhadap Penggunaan Sistem Informasi Akademik Universitas EA Menggunakan Metode ISO 27001," Jurnal Teknologi Informasi Mura, Vols. vol. 15, no. 1, p. pp. 1–13, 2023.

[18] G. M. A. S. a. D. M. S. A. I. G. A. S. Sanjaya, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," Jurnal Ilmiah Merpati, Vols. vol. 8, no. 2, p. pp. 113–124, 2020.

[19] R. A. R. a. Y. A. Nurhuda, "Analisis Keamanan Website Menggunakan Metode NIST SP 800-115," Jurnal Ilmiah Informatika Global, Vols. vol. 12, no. 2, p. pp. 67–72, 2021.

[20] F. N. K. a. R. Syaifudin, "Evaluasi Tingkat Kematangan Keamanan Informasi Menggunakan Indeks KAMI (Studi Kasus: Perguruan Tinggi XYZ)," Jurnal Transformatika, Vols. vol. 18, no. 2, pp. pp. 185–194, 2021., 2021.