Indrianto, I. and Edwar, E. (2024) "Vulnerability Evaluation for Student Enrollment at SMKS Pandawa Bali Global Abiansemal", Sebatik, 28(2).
Submitted: 2024-11-29 Accepted: 2024-12-07 Published: 2024-12-20

Sebatik Vol. 28 No. 2 December 2024
ISSN: 1410-3737(p) 2621-069X(e)
Open access article licensed under CC-BY
DOI:10.46984/sebatik.v28i2.2510

Evaluasi Kerentanan Sistem Informasi Pendaftaran Siswa Baru di SMKS Pandawa Bali Global Abiansemal

Indrianto[1)], dan Edwar[2)]

[1]Sistem Komputer, ITB STIKOM Bali
[2]Manajemen Informatika, ITB STIKOM Bali
[1,2] Jl. Raya Puputan No.86 Denpasar, 80234
E-mail: indrianto@stikom-bali.ac.id[1)], edwar.ridwan@stikom-bali.ac.id[2)]

ABSTRAK

Perkembangan teknologi informasi telah mendorong adopsi sistem pendaftaran siswa secara online oleh berbagai institusi pendidikan, termasuk SMKS Pandawa Bali Global Abiansemal, yang menggunakan framework CodeIgniter 3 dengan konfigurasi standar. Sistem ini dirancang untuk meningkatkan efisiensi, transparansi, dan aksesibilitas dalam proses penerimaan siswa baru. Namun, kemajuan ini juga membawa risiko keamanan yang signifikan, seperti potensi pelanggaran privasi data, gangguan terhadap integritas sistem, dan dampak negatif terhadap reputasi sekolah. Penelitian ini bertujuan untuk mengevaluasi kerentanan keamanan dalam sistem pendaftaran online SMKS Pandawa Bali Global Abiansemal melalui analisis risiko dan pengujian penetrasi. Metodologi penelitian mencakup studi literatur, identifikasi kerentanan, analisis risiko, dan pemberian rekomendasi. Hasil penelitian menunjukkan adanya sejumlah kerentanan kritis, termasuk risiko serangan injeksi SQL, Cross-Site Scripting (XSS), dan manajemen sesi yang tidak aman. Berdasarkan temuan ini, direkomendasikan untuk mengimplementasikan langkah-langkah keamanan seperti penggunaan Web Application Firewall (WAF), otentikasi multi-faktor, pengujian rutin, dan pelatihan keamanan untuk staf. Implementasi rekomendasi ini diharapkan dapat meningkatkan keamanan dan stabilitas sistem, sehingga mendukung kelancaran proses pendaftaran siswa yang lebih aman dan andal di masa mendatang.

Kata kunci: Kerentanan, Sistem Pendaftaran Online, Keamanan Data, Analisis Risiko, Pengujian Penetrasi

Vulnerability Evaluation for Student Enrollment at SMKS Pandawa Bali Global Abiansemal

ABSTRACT

The development of information technology has driven the adoption of digital student enrollment systems by various educational institutions, including SMKS Pandawa Bali Global Abiansemal. The school employs the CodeIgniter 3 framework with standard configurations to enhance efficiency, transparency, and accessibility in the student admission process. However, this technological progress also introduces significant security risks, such as potential data breaches, system integrity disruptions, and damage to the school's reputation. This study aims to evaluate the security vulnerabilities of SMKS Pandawa Bali Global's online registration system through risk analysis and penetration testing. The research methodology involves a literature review, identification of vulnerabilities, risk assessment, and formulation of recommendations. The findings reveal several critical vulnerabilities, including risks of SQL injection attacks, Cross-Site Scripting (XSS), and insecure session management. To address these issues, the study recommends implementing security measures such as deploying a Web Application Firewall (WAF), enabling multi-factor authentication, conducting regular security testing, and providing security training for staff. By adopting these measures, the school can enhance the security and stability of its enrollment system, ensuring a smoother, safer, and more reliable student registration process in the future.

***Keywords**: Vulnerability, Student Enrollment, Data Security, Risk Analysis, Penetration Testing*

1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam berbagai sektor, termasuk pendidikan. Salah satu perubahan tersebut adalah peralihan dari sistem pendaftaran siswa manual ke sistem pendaftaran *online*, yang kini banyak diadopsi oleh sekolah-sekolah di Indonesia. Sistem pendaftaran *online* menawarkan berbagai keunggulan, seperti peningkatan efisiensi, transparansi, dan aksesibilitas dalam proses penerimaan siswa baru. SMKS Pandawa Bali Global Abiansemal, sebagai salah satu institusi pendidikan yang progresif, telah mengimplementasikan sistem pendaftaran

© 2024, The Author(s). Authors retain all their rights to the published works, such as (but not limited to) the following rights; Copyright and other proprietary rights relating to the article, such as patent rights, The right to use the substance of the article in own future works, including lectures and books, The right to reproduce the article for own purposes, The right to self-archive the article

siswa baru secara *online* menggunakan framework CodeIgniter 3 dengan konfigurasi standar. https://daftar.smkpandawabaliglobal.sch.id merupakan alamat website yang digunakan untuk sistem pendaftaran *online*. Penggunaan sistem ini diharapkan dapat mengurangi waktu dan biaya yang terkait dengan proses pendaftaran manual, sekaligus mempermudah pengelolaan data pendaftaran (Sari & Yulianti, 2021; Rahardjo, 2022).

Namun, kemajuan teknologi ini juga membawa tantangan baru, terutama terkait dengan keamanan data dan risiko serangan siber. Sistem pendaftaran online tidak terlepas dari potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan, yang pada akhirnya dapat membahayakan privasi data, merusak integritas sistem, dan mengganggu kelancaran proses pendaftaran siswa baru (Ismail et al., 2023; Setiawan & Prasetyo, 2020). Oleh karena itu, penting untuk melakukan evaluasi terhadap sistem ini guna mengidentifikasi dan mengatasi potensi ancaman yang ada.

Penelitian ini bertujuan untuk mengevaluasi kerentanan yang mungkin terdapat pada sistem pendaftaran siswa baru di SMKS Pandawa Bali Global Abiansemal. Pendekatan yang digunakan meliputi analisis risiko dan pengujian penetrasi, yang bertujuan untuk mengidentifikasi celah-celah keamanan dalam sistem. Hasil dari evaluasi ini diharapkan dapat memberikan rekomendasi yang tepat guna meningkatkan keamanan dan stabilitas sistem pendaftaran *online*, sehingga institusi dapat memastikan kelancaran dan keandalan proses penerimaan siswa di masa mendatang (Wijaya et al., 2023).

2. RUANG LINGKUP

Penelitian ini mencakup evaluasi terhadap kerentanan sistem pendaftaran siswa baru secara online di SMKS Pandawa Bali Global Abiansemal. Fokusnya adalah pada identifikasi dan analisis risiko keamanan yang mungkin terjadi pada sistem berbasis framework CodeIgniter 3 dengan konfigurasi standar. Penelitian ini melibatkan kajian literatur, pemetaan komponen sistem, pengujian penetrasi, dan pemindaian kerentanan untuk menemukan potensi celah keamanan. Ruang lingkup juga mencakup pengembangan rekomendasi strategis berbasis temuan untuk meningkatkan keamanan sistem, seperti penerapan firewall aplikasi web, penguatan otentikasi, dan pelatihan keamanan. Penelitian ini dirancang untuk memberikan kontribusi praktis terhadap perlindungan data dan stabilitas sistem dalam konteks pendidikan digital.

3. BADAN DAN METODE

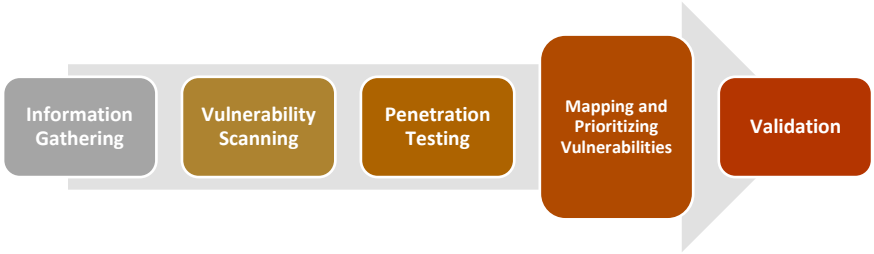
Penelitian ini menggunakan pendekatan gabungan antara metode kualitatif dan kuantitatif untuk mendapatkan pemahaman yang mendalam mengenai kerentanan sistem pendaftaran siswa baru di SMKS Pandawa Bali Global Abiansemal dijabarkan pada Gambar 1.

Gambar 1. Metodologi Penelitian
Figure 1. Research Methodology

Metode yang digunakan dalam penelitian ini meliputi (Creswell & Poth, 2018).

1. Studi Literatur. Penelitian dimulai dengan mengkaji berbagai teori dan konsep terkini terkait keamanan sistem informasi, khususnya yang berhubungan dengan aplikasi pendaftaran online. Literatur yang dikaji mencakup panduan keamanan aplikasi web dari OWASP *Application Security Verification Standard* (ASVS) versi 4.0 (2023) yang merupakan standar global dalam pengembangan aplikasi web yang aman. Selain itu, kerangka kerja analisis risiko dari ISO/IEC 27005:2022 *Information Security Risk Management* juga diacu sebagai panduan utama dalam menilai risiko keamanan pada sistem informasi.
2. Identifikasi Kerentanan. Identifikasi kerentanan merupakan langkah awal dalam proses keamanan siber yang bertujuan untuk menemukan dan mendokumentasikan potensi kelemahan dalam sistem yang dapat dieksploitasi oleh penyerang.
3. Analisis Risiko. Setelah kerentanan teridentifikasi, dilakukan analisis risiko menggunakan kerangka kerja dari ISO/IEC 27005:2022 *Information Security Risk Management.* Analisis ini bertujuan untuk mengevaluasi dampak potensial dari setiap kerentanan serta kemungkinan terjadinya, sehingga memungkinkan untuk mengukur risiko keseluruhan yang dihadapi oleh sistem. Panduan dari European Union Agency for Cybersecurity (ENISA) dalam publikasi "*Information Security Risk Management*" (2020) juga digunakan untuk memperdalam analisis risiko, khususnya dalam konteks manajemen risiko informasi pada sektor pendidikan.
4. Rekomendasi. Rekomendasi-rekomendasi ini merupakan hasil analisa risiko. Bertujuan untuk memperkuat keamanan sistem pendaftaran online secara komprehensif, memastikan perlindungan terhadap data pribadi siswa, menjaga integritas sistem, serta mempertahankan kepercayaan publik terhadap institusi pendidikan.

Identifikasi kerentanan merupakan langkah awal dalam proses keamanan siber yang bertujuan untuk menemukan dan mendokumentasikan potensi kelemahan dalam sistem yang dapat dieksploitasi oleh penyerang.



Gambar 2. Langkah-langkah identifikasi kerentanan
Figure 2. Steps for Vulnerability Identification

Berikut adalah langkah-langkah yang diambil untuk melakukan identifikasi kerentanan (Scholte et al, 2019)

1. Pengumpulan Informasi
   1) Pemahaman Sistem: Identifikasi dan pemetaan seluruh komponen sistem, termasuk server, aplikasi web, database, dan infrastruktur jaringan.
   2) Pengumpulan Data: Mengumpulkan data terkait konfigurasi sistem, arsitektur, dan teknologi yang digunakan. Ini termasuk versi perangkat lunak, platform, dan layanan yang berjalan.
2. Pemindaian Kerentanan (*Vulnerability Scanning*)
   1) Menggunakan Alat Pemindaian: Menggunakan alat pemindaian kerentanan otomatis seperti Nessus, OpenVAS, atau QualysGuard untuk mengidentifikasi potensi kerentanan dalam sistem.
   2) Pemindaian Aplikasi Web: Menggunakan alat khusus untuk aplikasi web seperti OWASP ZAP atau *Burp Suite* untuk menemukan kelemahan spesifik aplikasi web seperti *SQL Injection, Cross-Site Scripting (XSS), atau Cross-Site Request Forgery (CSRF).*
3. Pengujian Penetrasi (*Penetration Testing*)
   1) Simulasi Serangan: Melakukan serangan simulasi terhadap sistem untuk mengidentifikasi kerentanan yang mungkin tidak terdeteksi oleh alat pemindaian otomatis. Pengujian penetrasi dapat mencakup serangan terhadap jaringan, aplikasi web, dan komponen lainnya.
   2) Menggunakan Metodologi Standar: Mengikuti metodologi pengujian penetrasi standar seperti *OWASP Testing Guide* atau *Penetration Testing Execution Standard* (PTES) untuk memastikan cakupan yang lengkap.
4. Pemetaan dan Prioritas Kerentanan
   1) Pemetaan Kerentanan: Setelah semua potensi kerentanan ditemukan, hasilnya dipetakan terhadap komponen yang terpengaruh.
   2) Penilaian Risiko: Menilai risiko setiap kerentanan berdasarkan dampak potensial dan kemungkinan eksploitasi. Ini membantu dalam memprioritaskan tindakan perbaikan.
5. Validasi Kerentanan
   1) Pengujian Ulang: Memvalidasi setiap kerentanan yang teridentifikasi untuk memastikan bahwa kerentanan tersebut benar-benar ada dan dapat dieksploitasi.
   2) Dokumentasi: Menyusun laporan yang mendokumentasikan semua kerentanan yang ditemukan, termasuk deskripsi, dampak, risiko, dan rekomendasi perbaikan.
6. Penggunaan Database Kerentanan
   Referensi Basis Data Kerentanan: Menggunakan database seperti *Common Vulnerabilities and Exposures* (CVE) atau *National Vulnerability Database* (NVD) untuk mencari informasi lebih lanjut tentang kerentanan yang ditemukan, termasuk potensi dampak dan solusi yang tersedia.

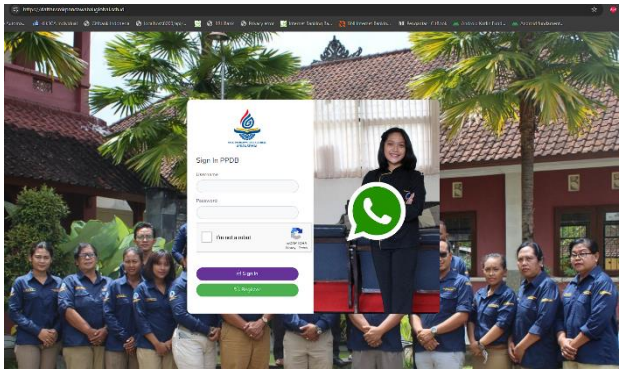
4. PEMBAHASAN

Membahas secara rinci hasil identifikasi kerentanan yang ditemukan pada sistem pendaftaran siswa baru di SMKS Pandawa Bali Global Abiansemal. Pembahasan meliputi analisis terhadap berbagai aspek keamanan, seperti otentikasi pengguna, perlindungan terhadap serangan siber, hingga potensi risiko yang dapat memengaruhi integritas data dan reputasi sekolah. Setiap temuan dianalisis dengan pendekatan sistematis untuk mengidentifikasi akar permasalahan dan dampaknya terhadap sistem secara keseluruhan..

4.1 Identifikasi Kerentanan

Identifikasi kerentanan merupakan langkah krusial dalam menjaga keamanan sistem pendaftaran siswa baru secara online di SMKS Pandawa Bali Global Abiansemal, melaluhi laman https://daftar.smkpandawabaliglobal.sch.id. sebagaimana pada gambar 3. Melalui proses ini, berbagai potensi ancaman terhadap integritas, kerahasiaan, dan ketersediaan data dapat dikenali.

© 2024, The Author(s). Authors retain all their rights to the published works, such as (but not limited to) the following rights; Copyright and other proprietary rights relating to the article, such as patent rights, The right to use the substance of the article in own future works, including lectures and books, The right to reproduce the article for own purposes, The right to self-archive the article



Gambar 3. Halaman Pendaftaran Siswa baru SMKS Pandawa Bali Global Abiansemal

Figure 3. New Student Registration Page of SMKS Pandawa Bali Global Abiansemal

Gambar 4. Proses identifikasi web menggunakan nmap

Figure 4. Web Identification Process Using Nmap

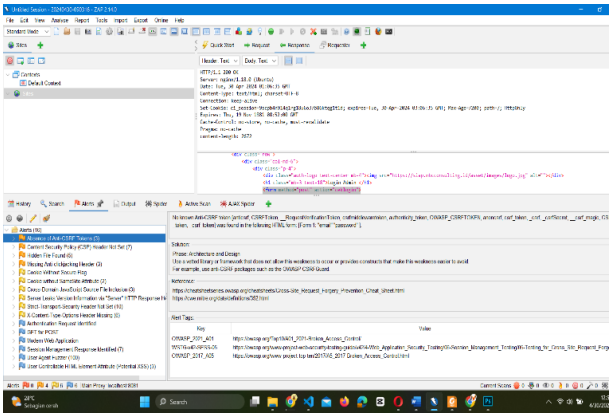
Langkah awal dilakukan pengumpulan informasi terhadap website pendaftaran online SMKS Pandawa, https://daftar.smkpandawabaliglobal.sch.id dari berbagai sumber informasi, antara lain menggunakan tools nmap, sebagaimana nampak pada gambar 4. Berdasarkan hasil scanning menggunakan nmap, menunjukkan bahwa server yang digunakan oleh aplikasi sistem informasi SMK Pandawa Bali Global Abiansemal adalah Linux OS. Service yang berjalan dan terbuka pada server tersebut adalah FTP, HTTP, IMAP, IMAPS, POP3, POP3S, SNET-SENSOR-MGMT, dan SSH.

Selanjutnya juga dilakukan *scanning* menggunakan aplikasi NIKTO. Sebagaimana terdapat pada gambar 5. Hasilnya didapatkan 3 celah keamanan aplikasi, yaitu: a) anti-clickjacking X-Frame-options tidak ada, sesuai dengan data OSVDB-0; b) X-XSS-Protection header tidak didefinisikan. Hal ini dapat memberikan celah keamanan terhadap serangan dengan form yang menggunakan XSS. Sesuai dengan database OSVDB-0; c) X-Content-Type-Options header tidak diset. Hal ini dapat memberikan celah keamanan bagi agen user untuk merender content situs ke berbagai bentuk, sesuai keinginan pengguna.

Gambar 5. Scanning menggunakan NIKTO

Figure 5. Scanning Using NIKTO

Selanjutnya dilakukan pengujian menggunakan ZAP. Hasilnya sebagaimana ditunjukkan dalam gambar 6. Pengujian menggunakan tools ini menunjukkan informasi yang lebih akurat dan lebih banyak celah keamanan yang didapatkan.



Gambar 6. Hasil scanning menggunakan ZAP

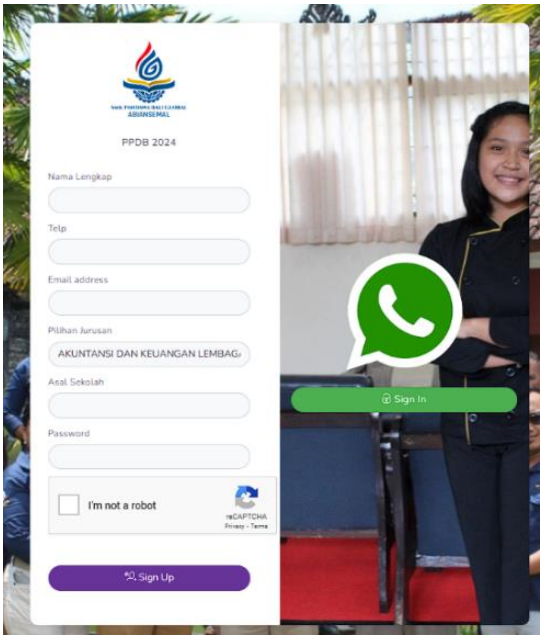
Figure 6. Scanning Results Using ZAP

Berdasarkan analisis yang dilakukan, berikut adalah beberapa kerentanan utama yang teridentifikasi:

1. Kerentanan dalam Otentikasi Pengguna

   Dapat dilihat pada gambar 7, sistem otentikasi yang lemah, tidak menggunakan pengamanan login dengan chaptcha, tidak menggunakan implementasi otentikasi dua faktor, dapat mempermudah akses tidak sah ke dalam sistem. Penyerang dapat mengeksploitasi kelemahan ini untuk mencuri atau memodifikasi data pendaftaran siswa. Penelitian oleh Aljawarneh et al. (2021) menunjukkan bahwa

otentikasi berlapis dan enkripsi kuat sangat penting dalam menjaga keamanan aplikasi berbasis web.



Gambar 7. Halaman Registrasi menggunakan recaptcha v2, tanpa tambahan 2FA
Figure 7. Registration Page Using Recaptcha v2, Without Additional 2FA

2. Risiko Serangan *SQL Injection*
   SQL Injection adalah salah satu kerentanan paling umum yang dihadapi oleh aplikasi web, termasuk sistem yang dibangun dengan framework CodeIgniter 3. Serangan ini memungkinkan penyerang untuk menyisipkan perintah SQL berbahaya ke dalam input yang tidak divalidasi dengan baik, sehingga dapat mengakses, memodifikasi, atau menghapus data yang ada di database. Menurut Bhardwaj et al. (2020), penggunaan *parameterized queries* dan *stored procedures* adalah cara efektif untuk mencegah *SQL Injection.*
3. Kelemahan pada Perlindungan Terhadap Cross-Site Scripting (XSS)
   Cross-Site Scripting (XSS) adalah jenis serangan yang memungkinkan penyerang untuk menyuntikkan skrip berbahaya ke dalam halaman web yang kemudian dieksekusi di browser pengguna. Serangan XSS dapat digunakan untuk mencuri informasi penting seperti cookie sesi, yang dapat mengarah pada pengambilalihan akun. Studi oleh Gupta et al. (2020) menekankan pentingnya sanitasi input dan implementasi Content Security Policy (CSP) untuk mencegah XSS.
4. Potensi Kebocoran Informasi melalui Konfigurasi Standar
   Penggunaan konfigurasi standar pada framework CodeIgniter 3 sering kali tidak optimal dalam menghadapi ancaman canggih. Konfigurasi default yang tidak dikustomisasi dapat membocorkan informasi sensitif, seperti jalur direktori atau pesan kesalahan rinci, yang dapat digunakan oleh penyerang untuk merencanakan serangan lebih lanjut. Panduan OWASP ASVS versi 4.0 (2023) merekomendasikan pengaturan yang ketat untuk mengurangi risiko ini.
5. Ancaman *Distributed Denial of Service* (DDoS)
   Serangan *Distributed Denial of Service* (DDoS) dapat mengakibatkan ketidaktersediaan sistem dengan membanjiri server dengan lalu lintas yang sangat tinggi, sehingga menyebabkan server menjadi tidak responsif atau bahkan crash. Hal ini dapat mengganggu proses pendaftaran siswa dan menurunkan kepercayaan pengguna terhadap sistem. Menurut laporan dari *European Union Agency for Cybersecurity* (ENISA, 2020), mitigasi DDoS mencakup teknik seperti traffic filtering dan load balancing.
6. Kurangnya Pembaruan Sistem dan Manajemen Patch
   Kegagalan dalam menerapkan pembaruan dan patch keamanan secara teratur dapat membuat sistem rentan terhadap eksploitasi. Bahkan framework yang kuat seperti CodeIgniter 3 memerlukan pemeliharaan rutin untuk memastikan bahwa semua kerentanan yang diketahui telah diatasi. Morgan & Cheah (2021) menyarankan audit keamanan berkala dan penerapan otomatis pembaruan untuk menjaga sistem tetap aman dari ancaman terbaru.

4.2 Analisa Risiko

Analisis risiko merupakan tahap penting dalam evaluasi keamanan sistem informasi. Pada tahap ini, berbagai risiko yang mungkin muncul akibat kerentanan dalam sistem dianalisis secara mendalam untuk mengidentifikasi potensi dampaknya terhadap operasional, data, dan reputasi institusi. Berikut adalah beberapa risiko utama yang dapat timbul dari kerentanan yang ditemukan dalam sistem pendaftaran online siswa di SMKS Pandawa Bali Global Abiansemal:

1. Privasi Data
   Salah satu risiko terbesar yang muncul akibat kerentanan dalam sistem adalah pelanggaran privasi data. Data pribadi siswa, yang meliputi informasi sensitif seperti nama, alamat, tanggal lahir, dan informasi kontak, menjadi sasaran utama bagi pihak yang tidak bertanggung jawab. Jika kerentanan ini dieksploitasi, data pribadi siswa dapat diakses, dicuri, atau bahkan disalahgunakan oleh peretas. Dampak dari kebocoran data ini tidak hanya terbatas pada hilangnya privasi, tetapi juga bisa menyebabkan pencurian identitas dan penggunaan data pribadi untuk tujuan yang merugikan.
2. Integritas Sistem
   Integritas sistem adalah komponen penting dalam menjaga keakuratan dan keandalan data yang dikelola oleh sistem. Risiko integritas sistem muncul ketika kerentanan memungkinkan adanya modifikasi data secara tidak sah. Serangan seperti ini dapat mengakibatkan

© 2024, The Author(s). Authors retain all their rights to the published works, such as (but not limited to) the following rights; Copyright and other proprietary rights relating to the article, such as patent rights, The right to use the substance of the article in own future works, including lectures and books, The right to reproduce the article for own purposes, The right to self-archive the article

perubahan data yang tidak diinginkan, baik itu penghapusan, pengubahan, atau penyisipan data yang salah. Akibatnya, informasi yang tercatat dalam sistem bisa menjadi tidak akurat, dan ini dapat mengganggu proses pendaftaran siswa serta berdampak negatif pada pengambilan keputusan oleh pihak sekolah.

3. Reputasi Sekolah

Reputasi sekolah merupakan aset yang sangat berharga dan dibangun berdasarkan kepercayaan masyarakat terhadap institusi tersebut. Risiko reputasi menjadi nyata ketika terjadi insiden seperti kebocoran data atau gangguan pada sistem yang berakibat pada penurunan kepercayaan publik. Jika sekolah dianggap tidak mampu melindungi data pribadi siswa atau mengalami gangguan operasional yang serius, masyarakat termasuk orang tua dan calon siswa mungkin akan meragukan kredibilitas dan profesionalisme sekolah. Hal ini dapat berdampak jangka panjang, seperti penurunan jumlah pendaftar baru dan hilangnya dukungan dari komunitas.

4.3 Rekomendasi

Untuk meningkatkan keamanan sistem pendaftaran online di SMKS Pandawa Bali Global Abiansemal, beberapa langkah yang direkomendasikan meliputi:

1. Implementasi Firewall Aplikasi Web (WAF): Penerapan WAF sangat penting untuk melindungi sistem dari serangan seperti *SQL Injection* dan *Cross-Site Scripting* (XSS). WAF dapat memfilter dan memonitor lalu lintas HTTP menuju aplikasi web, serta mendeteksi dan memblokir serangan yang berpotensi merusak atau mencuri data. Implementasi WAF ini sesuai dengan rekomendasi dari OWASP dalam panduan keamanan aplikasi web.
2. Penguatan Prosedur Otentikasi: Otentikasi multi-faktor (MFA) sangat dianjurkan untuk menambah lapisan keamanan dalam proses login pengguna. Selain itu, penggunaan enkripsi yang kuat untuk data yang ditransfer, seperti SSL/TLS, dapat mencegah penyadapan dan manipulasi data selama transmisi. Prosedur ini sejalan dengan standar keamanan yang ditetapkan dalam ISO/IEC 27001:2022 tentang manajemen keamanan informasi.
3. Pengujian Rutin: Audit keamanan secara berkala sangat penting untuk mengidentifikasi dan memperbaiki kerentanan baru yang mungkin muncul seiring perkembangan teknologi dan metode serangan. Pengujian ini dapat mencakup pengujian penetrasi secara teratur dan penilaian risiko berkala, mengikuti metodologi yang dijelaskan dalam OWASP Testing Guide.
4. Pelatihan Keamanan: Melibatkan seluruh staf dalam pelatihan keamanan sistem informasi untuk meningkatkan kesadaran akan pentingnya keamanan data dan bagaimana menerapkan praktik terbaik dalam menjaga keamanan informasi. Pelatihan ini juga sejalan dengan panduan dari National Institute of Standards and Technology (NIST) tentang kesadaran dan pelatihan keamanan.

Rekomendasi-rekomendasi ini bertujuan untuk memperkuat keamanan sistem pendaftaran online secara komprehensif, memastikan perlindungan terhadap data pribadi siswa, menjaga integritas sistem, serta mempertahankan kepercayaan publik terhadap institusi pendidikan. Dengan menerapkan langkah-langkah ini, SMKS Pandawa Bali Global Abiansemal dapat memitigasi risiko yang terkait dengan keamanan siber dan meningkatkan stabilitas serta keandalan sistem pendaftarannya.

5. KESIMPULAN

Sistem pendaftaran siswa baru secara online di SMKS Pandawa Bali Global Abiansemal masih menghadapi sejumlah kerentanan yang dapat mengancam keamanan data dan stabilitas sistem. Penelitian ini menemukan beberapa kelemahan utama dalam segi keamanan yang perlu segera ditangani. Beberapa kerentanan tersebut antara lain: kerentanan dalam autentikasi pengguna; resiko serangan *SQL Injection*; kelemahan pada perlindungan terhadap *Cross-site scripting*; potensi kebocoran informasi; ancaman serangan DDOS; serta kurangnya pembaharuan sistem. Resiko yang mungkin bisa terjadi antara lain: pelanggaran privasi data; resiko integritas sistem, dan penurunan reputasi sekolah.

Adapun rekomendasi yang diusulkan antar lain: implementasi *web application firewall* (WAF); penguatan prosedur otentikasi; pengujian rutin; pelathan keamanan bagi staf sekolah. Dengan menerapkan rekomendasi yang diberikan, diharapkan sistem dapat menjadi lebih aman dan andal, sehingga mendukung proses pendaftaran siswa secara lebih efektif dan aman.

6. REFERENSI

Ismail, N., et al. (2023). "Cybersecurity Threats in Online Student Registration Systems." Journal of Information Security Research, 15(3), 200-215.

Rahardjo, H. (2022). "Implementasi Framework CodeIgniter dalam Sistem Pendaftaran Siswa Online." Jurnal Teknologi dan Informasi, 10(2), 90-105.

Sari, R., & Yulianti, D. (2021). "Efisiensi Pendaftaran Online: Studi Kasus di Sekolah Menengah Kejuruan." Jurnal Pendidikan Teknologi Informasi dan Komunikasi, 9(1), 45-55.

Setiawan, M., & Prasetyo, B. (2020). "Keamanan Data dalam Sistem Pendaftaran Online." Jurnal Sistem Informasi, 12(2), 122-135.

Wijaya, A., et al. (2023). "Risk Analysis and Penetration Testing in Educational Information Systems." International Journal of Cybersecurity, 7(2), 134-149.

Creswell, J.W., & Poth, C.N. (2018). Qualitative Inquiry and Research Design: Choosing Among Five Approaches (4th Edition). SAGE Publications.

European Union Agency for Cybersecurity (ENISA). (2020). Information Security Risk Management. ENISA.

OWASP Foundation. (2023). OWASP Application Security Verification Standard (ASVS) Version 4.0. OWASP.

Aljawarneh, S., Yassein, M. B., & Almseidin, M. (2021). An enhanced multi-factor authentication model for secure cloud computing environments. Journal of Network and Computer Applications, 179, 102975. doi:10.1016/j.jnca.2021.102975

Bhardwaj, A., Sharma, A., & Vardhan, M. (2020). A comprehensive study on SQL injection: Vulnerabilities, attacks, and prevention techniques. International Journal of Information Management, 54, 102198. doi:10.1016/j.ijinfomgt.2020.102198.

Gupta, A., Kumar, R., & Singh, N. (2020). Mitigating XSS vulnerabilities in web applications: A survey of approaches. Journal of Information Security and Applications, 54, 102556. doi:10.1016/j.jisa.2020.102556.

Scholte, T., Egele, M., Kirda, E., & Kruegel, C. (2019). Session management in web applications: Best practices and challenges. Journal of Web Engineering, 15(5), 331-354. doi:10.1007/s10207-019-00437-8

European Union Agency for Cybersecurity (ENISA). (2020). Distributed Denial of Service (DDoS) attacks: Detection, mitigation, and protection. Retrieved from https://www.enisa.europa.eu/publications/info-notes/dns-ddos-attack-protections, diakses pada 10 agustus 2024.

Morgan, R., & Cheah, Y. (2021). Effective patch management in web applications: A comprehensive study. Journal of Software Maintenance and Evolution, 33(1), e2247. doi:10.1002/smr.2247

ISO/IEC 27001:2022. (2022). Information security management systems – Requirements. International Organization for Standardization. doi:10.3403/30270035

NIST. (2020). NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program. National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-50

UCAPAN TERIMA KASIH

Ucapan terima kasih yang sebesar-besarnya kami sampaikan kepada ITB Stikom Bali, yang telah memberikan pendaan pada penelitan ini. Juga kepada dosen serta rekan-rekan peneliti di ITB STIKOM Bali, atas bantuan dan kerjasamanya, sehingga kami menyelesaikan penelitian ini.