Technomedia Journal (TMJ)
Vol. 11, No. 1, Juni 2026, pp. 12∼22
E-ISSN: 2528-6544 | P-ISSN: 2620-3383, DOI: 10.33050

Vulnerability Assessment Strategy Using OWASP ZAP to Support Digital Transformation in Education

Strategi Evaluasi Kerentanan Website Menggunakan OWASP ZAP untuk Mendukung Transformasi Digital Pendidikan

Muhammad Hafied Hermawan[1], Firman Jaya[2*], Rahmat Shofan Razaqi[3]
[1,2,3]Department of Information Technology Education, STKIP PGRI Situbondo, Indonesia
[1]hafiedsv@gmail.com, [2]altamis1922@gmail.com, [3]fanslaught@gmail.com
***Penulis Korespondensi**

Article Info

Article History:

Penyerahan Maret 17, 2026
Revisi Mei 15, 2026
Diterima Juni 21, 2026
Diterbitkan Juni 24, 2026

Keywords:
OWASP ZAP
Digital Transformation
Security
Configuration
Data Protection

Kata Kunci:
OWASP ZAP
Transformasi Digital
Keamanan
Konfigurasi
Pelindungan Data

ABSTRACT

School websites function as public educational service platforms that must ensure the confidentiality, integrity, and availability of information. **This study evaluates** the security of the SMK Negeri 2 Situbondo website using OWASP ZAP as a Dynamic Application Security Testing tool within the public-access scope. **The novelty** of this research lies in the cross-comparison of three school websites within the same region, the mapping of findings to OWASP A05 Security Misconfiguration, and the integration of the results with educational digital transformation governance, data protection policies, and Sustainable Development Goals. **The scanning results** of the primary website identified 26 alert types, consisting of 0 High, 12 Medium, 7 Low, and 7 Informational findings. The dominant vulnerabilities were related to weaknesses in Content Security Policy, HTTP security header configuration, cookie controls, and third-party resource governance. The comparison websites exhibited similar vulnerability patterns, although with different quantities and severity levels. Priority recommendations include hardening Content Security Policy, HSTS, anti-clickjacking mechanisms, X-Content-Type-Options, cookie attributes, anti-CSRF tokens, and Subresource Integrity implementation. **These findings** provide an operational baseline for school administrators to strengthen the security of digital education services gradually and systematically.

ABSTRAK

Website sekolah merupakan kanal layanan publik pendidikan yang harus menjaga kerahasiaan, integritas, dan ketersediaan informasi. **Penelitian ini** mengevaluasi keamanan *website* SMK Negeri 2 Situbondo menggunakan pendekatan OWASP ZAP sebagai alat *Dynamic Application Security Testing* pada area publik. **Kebaruan penelitian** terletak pada pembandingan lintas tiga *website* sekolah di wilayah yang sama, pemetaan temuan terhadap OWASP A05 *Security Misconfiguration*, serta pengaitan hasil dengan tata kelola transformasi digital pendidikan, kebijakan pelindungan data, dan *Sustainable Development Goals*. **Hasil pemindaian** website fokus menunjukkan 26 jenis *alert*, terdiri atas 0 *High*, 12 *Medium*, 7 *Low*, dan 7 *Informational*. Temuan dominan berkaitan dengan kelemahan *Content Security Policy*, konfigurasi HTTP *security header*, kontrol *cookie*, dan tata kelola sumber pihak ketiga. *Website* pembanding menunjukkan pola

kerentanan yang serupa, meskipun jumlah dan tingkat keparahannya berbeda. Rekomendasi prioritas mencakup *hardening* CSP, HSTS, *anti-clickjacking*, *X-Content-Type-Options*, *atribut cookie*, token anti-CSRF, dan *Subresource Integrity*. **Temuan ini menjadi** *baseline* operasional bagi pengelola sekolah untuk memperkuat keamanan layanan pendidikan digital secara bertahap dan terukur.

DOI: https://doi.org/10.33050/tmj.v11i1.2645

1. PENDAHULUAN

Transformasi digital pendidikan mendorong sekolah memanfaatkan *website* sebagai pusat informasi, publikasi, komunikasi, dan layanan administratif [1, 2]. Pada saat yang sama, perluasan fungsi digital tersebut memperbesar permukaan serangan yang dapat berdampak pada ketersediaan layanan, kepercayaan publik, dan pelindungan data warga sekolah [3]. Dalam konteks Indonesia, relevansi keamanan *website* pendidikan menguat karena agenda percepatan transformasi digital layanan publik menekankan keterpaduan layanan digital serta penguatan keamanan siber dan keamanan informasi [4], sementara pelindungan data pribadi telah menjadi kewajiban hukum yang perlu dipertimbangkan oleh pengelola sistem elektronik [5].

Website sekolah tidak selalu menghadapi risiko karena eksploitasi yang kompleks [6]. Banyak kelemahan muncul dari konfigurasi protektif yang belum konsisten, seperti ketiadaan HTTP *security header*, *Content Security Policy* (CSP) yang terlalu permisif, kontrol *cookie* yang belum lengkap, serta pemuatan sumber pihak ketiga tanpa pembatasan yang memadai [7]. Pola ini beririsan dengan *OWASP A05 Security Misconfiguration*, yaitu kategori risiko yang mencakup konfigurasi tidak aman, kontrol keamanan yang tidak lengkap, dan informasi teknis yang tidak semestinya terekspos [8].

Penelitian ini berangkat dari kebutuhan praktis untuk menghasilkan *baseline* keamanan *website* sekolah yang mudah dipahami oleh pengelola sistem, bukan sekadar daftar *alert* teknis [9, 10]. Oleh karena itu, hasil pemindaian OWASP ZAP diposisikan sebagai indikator risiko yang perlu ditriase, diverifikasi, dan diterjemahkan menjadi prioritas *hardening* [11, 12]. Pendekatan ini sejalan dengan Web *Security Testing Guide* OWASP yang menekankan pengujian sistematis terhadap konfigurasi aplikasi web, kontrol *transport*, dan mekanisme sisi klien [13, 14].

Signifikansi penelitian bagi ruang lingkup Technomedia Journal terletak pada hubungan antara keamanan aplikasi web, inovasi berbasis teknologi, dan transformasi digital pendidikan [15, 16]. Keamanan *website* bukan hanya persoalan teknis, melainkan bagian dari tata kelola layanan digital, keberlanjutan operasional, dan kepemimpinan transformasi digital [17–19]. *Website* yang aman mendukung keberlanjutan layanan pendidikan, kualitas akses informasi, dan kepercayaan pemangku kepentingan [20, 21]. Dengan demikian, penelitian ini juga terkait dengan SDGs 4 tentang pendidikan berkualitas dan SDGs 9 tentang infrastruktur yang tangguh dan inovasi [22, 23]. Dengan demikian, kontribusi penelitian ini adalah:

- Menyajikan profil kerentanan *website* sekolah yang difokuskan pada *security misconfiguration* dan HTTP *security header*.
- Membandingkan hasil pada tiga *website* sekolah untuk memperoleh posisi keamanan relatif.
- Menambahkan implikasi manajerial agar hasil teknis dapat digunakan oleh pengambil keputusan sebagai dasar prioritas keamanan digital.

2. PERMASALAHAN

Permasalahan utama penelitian adalah belum terpetakannya profil kerentanan *website* sekolah pada aspek konfigurasi protektif berbasis HTTP *response header* [24]. Kontrol seperti CSP, HSTS, *X-Frame-Options* atau *frame-ancestors*, *X-Content-Type-Options*, dan atribut *cookie* berfungsi sebagai lapisan perta-

hanan browser terhadap XSS, *clickjacking*, MIME sniffing, CSRF, *downgrade* koneksi, serta risiko *supply chain* pada sumber pihak ketiga [25, 26].

Berdasarkan observasi awal menggunakan OWASP ZAP, isu yang perlu dianalisis bukan hanya total *alert*, tetapi pola temuan yang berulang [27]. Pola tersebut meliputi kelemahan CSP, konfigurasi CORS yang perlu ditinjau, kontrol *cookie* yang belum konsisten, dan penggunaan JavaScript atau CSS lintas domain tanpa penguatan *Subresource Integrity* [28]. Kondisi ini dapat menurunkan efektivitas pertahanan *default browser* meskipun tidak otomatis membuktikan adanya kompromi sistem [29, 30].

Rumusan masalah penelitian ini adalah, bagaimana profil kerentanan yang berkaitan dengan konfigurasi HTTP *security header* pada website SMK Negeri 2 Situbondo berdasarkan hasil pemindaian OWASP ZAP, dan bagaimana posisi risikonya jika dibandingkan dengan *website* sekolah lain? [31, 32]. Tujuan penelitian adalah menganalisis temuan OWASP ZAP yang relevan dengan *security header*, menyusun rekomendasi *hardening* yang operasional bagi pengelola *website*, serta membandingkan hasil dengan dua *website* sekolah sebagai *baseline* kontekstual [33, 34].

3. METODOLOGI PENELITIAN

Penelitian menggunakan pendekatan *Dynamic Application Security Testing* (DAST) berbasis OWASP ZAP [35, 36]. ZAP digunakan untuk melakukan *crawling, passive scan*, dan *active scan* terbatas pada area publik *website* [37, 38]. Proses pengujian dibatasi pada observasi *request-response*, pencatatan *alert*, dan klasifikasi risiko penelitian tidak melakukan eksploitasi manual, akses administratif server, audit kode sumber, maupun uji ketahanan layanan yang bersifat destruktif [39, 40].

Objek fokus uji adalah https://smkn2situbondo.sch.id/. Website pembanding adalah https://sman2situbondo.sch.id/ dan https://www.smkn1panji-sit.sch.id/. Pemilihan pembanding dilakukan untuk memperoleh *baseline* kontekstual pada *website* sekolah di wilayah yang sama, bukan untuk menilai kualitas pengelolaan institusi lain.

Gambar 1. Alur Metode Penelitian Berbasis OWASP ZAP

Mengacu pada alur penelitian pada Gambar 1, tahapan penelitian meliputi penetapan *scope* dan batasan etis, *crawling endpoint* publik, *passive scan* dan *active scan* terbatas, ekstraksi *alert*, tingkat risiko, jumlah instans, dan bukti respons, triase temuan terhadap OWASP A05 *Security Misconfiguration*, pembandingan lintas *website*, dan penyusunan rekomendasi mitigasi [41, 42]. Data dianalisis secara deskriptif-komparatif dengan indikator jumlah *alert* per tingkat risiko, kemunculan temuan dominan, dan keterkaitan temuan dengan kontrol keamanan *browser*.

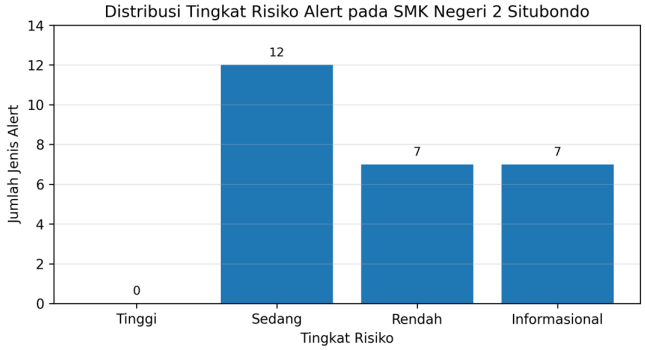
Tabel 1. Operasionalisasi Analisis Keamanan *Website*

Komponen	**Indikator**	**Sumber Data**	***Output* Analisis**
DAST OWASP ZAP	*Crawling*, *passive scan*, *active scan* terbatas	*Request-response* area publik	Daftar *alert* dan bukti teknis
Security Misconfiguration	CSP, HSTS, anti *clickjacking*, *nosniff*, CORS	*Alert* OWASP ZAP dan *header* HTTP	Pemetaan ke risiko konfigurasi
Komparasi *Website*	*High*, *Medium*, *Low*, *Informational*	Tiga *website* sekolah	Posisi keamanan relatif
Tata Kelola Digital	Prioritas mitigasi dan pemilik kontrol	Hasil triase teknis	Implikasi manajerial

Tabel 1 menyajikan operasionalisasi analisis keamanan *website* yang digunakan dalam penelitian ini, meliputi komponen yang dianalisis, indikator pengukuran, sumber data, serta output yang dihasilkan dari proses evaluasi kerentanan.

4. HASIL DAN PEMBAHASAN

Hasil pemindaian pada *website* SMK Negeri 2 Situbondo menunjukkan tidak ada *alert* kategori *High*. Kategori *Medium* mendominasi dengan 12 jenis *alert*, diikuti 7 jenis *alert Low* dan 7 jenis *alert Informational*. Distribusi tersebut mengindikasikan bahwa risiko utama tidak berada pada bukti kompromi langsung, tetapi pada area *hardening* konfigurasi yang dapat menurunkan efektivitas perlindungan *browser* dan kontrol *transport*.



Gambar 2. Distribusi Tingkat Risiko *Alert* pada *Website* Fokus

Gambar 2 memperlihatkan distribusi tingkat risiko *alert* pada *website* SMK Negeri 2 Situbondo. Kategori risiko sedang mendominasi dengan 12 jenis *alert*, sementara kategori risiko rendah dan informasional masing-masing berjumlah 7 jenis *alert*. Tidak ditemukan *alert* dengan tingkat risiko tinggi, sehingga prioritas perbaikan difokuskan pada penguatan konfigurasi keamanan dan kontrol protektif yang teridentifikasi.

Tabel 2. Rekapitulasi *Alert* OWASP ZAP pada *Website* SMK Negeri 2 Situbondo

No	***Alert***	***Risk***	**Instans**	**Kelompok Kontrol**
1.	*Absence of Anti-CSRF Tokens*	*Medium*	0	Kontrol CSRF
2.	*CSP: Failure to Define Directive with No Fallback*	*Medium*	6	CSP
3.	*CSP: Wildcard Directive*	*Medium*	6	CSP
4.	*CSP: script-src unsafe-eval*	*Medium*	4	CSP
5.	*CSP: script-src unsafe-hashes*	*Medium*	4	CSP
6.	*CSP: script-src unsafe-inline*	*Medium*	2	CSP
7.	*CSP: style-src unsafe-inline*	*Low*	6	CSP
8.	*Content Security Policy Header Not Set*	*Medium*	0	CSP
9.	*Cross-Domain Misconfiguration*	*Medium*	6	CORS
10.	*HTTP to HTTPS Insecure Transition in Form Post*	*Medium*	0	*Transport*
11.	*Missing Anti-clickjacking Header*	*Medium*	0	*Clickjacking*
12.	*Subresource Integrity Attribute Missing*	*Low*	0	*Third Party*
13.	*CSP: Notices*	*Informational*	6	CSP
14.	*Cookie without SameSite Attribute*	*Low*	0	*Cookie*
15.	*Cross-Domain JavaScript Source File Inclusion*	*Medium*	0	*Third Party*

16.	*Server Leaks Version Information via Server Header*	*Low*	4	*Information Disclosure*
17.	*Strict-Transport-Security Header Not Set*	*Low*	0	*Transport*
18.	*Timestamp Disclosure - Unix*	*Low*	0	*Information Disclosure*
19.	*X-Content-Type-Options Header Missing*	*Low*	0	*MIME Sniffing*
20.	*Content Security Policy Report-Only Header Found*	Informational	5	CSP
21.	*Information Disclosure - Suspicious Comments*	Informational	7	*Information Disclosure*
22.	*Modern Web Application*	Informational	0	*Informational*
23.	*Re-examine Cache-control Directives*	Informational	0	*Cache*
24.	*Retrieved from Cache*	Informational	8	*Cache*
25.	*Session Management Response Identified*	Informational	0	*Session*
26.	*User Controllable HTML Element Attribute Potential XSS*	Medium	3	*Input/Output Control*

Berdasarkan rekapitulasi pada Tabel 2, temuan kerentanan didominasi oleh *alert* yang berkaitan dengan konfigurasi CSP dan kontrol keamanan berbasis *header* HTTP. Dominasi *alert* CSP menunjukkan bahwa kebijakan pembatasan sumber daya masih perlu diperkuat. CSP yang memuat *wildcard*, *unsafe-inline*, atau *unsafe-eval* dapat menurunkan kemampuan *browser* untuk membatasi skrip berisiko. Penerapan CSP sebaiknya dilakukan bertahap dari mode *report-only*, inventarisasi domain eksternal yang benar-benar dibutuhkan, pengurangan *wildcard*, hingga penerapan nonce atau hash untuk kebutuhan *inline* yang tidak dapat dihindari [22, 23].

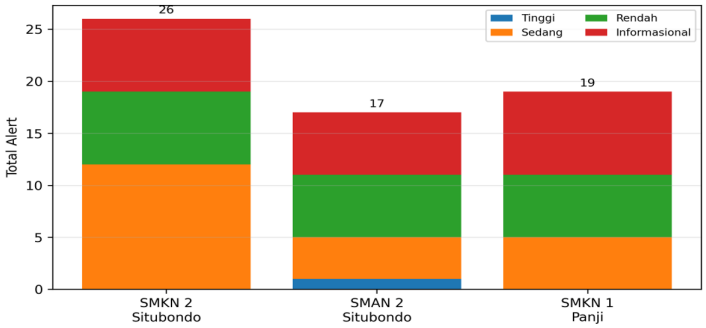
Temuan HSTS, transisi HTTP-HTTPS, dan *X-Content-Type-Options* berkaitan dengan kontrol *transport* dan pencegahan MIME *sniffing* [43]. HSTS perlu diterapkan setelah seluruh *resource* kompatibel dengan HTTPS agar tidak menimbulkan gangguan akses, sedangkan *X-Content-Type-Options nosniff* membantu mencegah *browser* menafsirkan konten secara keliru ketika tipe MIME tidak ketat [44]. Temuan *anti-clickjacking* dapat ditangani melalui *X-Frame-Options* atau *directive frame-ancestors* pada CSP [23].

Temuan CORS, pemuatan JavaScript lintas domain, dan SRI memperlihatkan bahwa risiko *website* sekolah juga dipengaruhi oleh rantai kepercayaan sumber pihak ketiga. Penggunaan CDN, *widget*, *font*, *analytics*, atau skrip eksternal perlu dibatasi melalui *allowlist*, SRI, dan evaluasi dependensi [45]. Dalam konteks tata kelola, pengelola perlu membedakan risiko yang dapat dikendalikan melalui konfigurasi domain sendiri dan risiko yang melekat pada layanan eksternal [46].

Tabel 3. Perbandingan Tingkat Risiko *Alert* pada *Website* Sekolah

Website	***High***	***Medium***	***Low***	***Informational***	**Total**
SMK Negeri 2 Situbondo	0	12	7	7	26
SMA Negeri 2 Situbondo	1	4	6	6	17
SMK Negeri 1 Panji	0	5	6	8	19

Tabel 3 menyajikan perbandingan tingkat risiko *alert* pada tiga *website* sekolah yang menjadi objek analisis. *Website* SMK Negeri 2 Situbondo memiliki jumlah temuan tertinggi dengan 26 *alert*, yang didominasi oleh kategori *Medium* sebanyak 12 temuan. Sementara itu, SMA Negeri 2 Situbondo merupakan satu-satunya *website* yang memiliki temuan risiko *High*, sedangkan SMK Negeri 1 Panji menunjukkan jumlah *alert* informasional tertinggi. Hasil ini menunjukkan bahwa setiap *website* memiliki karakteristik kerentanan yang berbeda, meskipun secara umum temuan didominasi oleh kategori *Medium*, *Low*, dan *Informational*.



Gambar 3. Perbandingan *Alert* OWASP ZAP antar *Website* Sekolah

Gambar 3 memperlihatkan perbandingan distribusi tingkat risiko *alert* pada ketiga *website* sekolah yang menjadi objek analisis. Secara kuantitatif, *website* SMK Negeri 2 Situbondo memiliki jumlah *alert* tertinggi dibandingkan dua *website* pembanding. Namun, interpretasi risiko tidak boleh berhenti pada total *alert* karena tingkat keparahan dan jenis kontrol yang terdampak lebih menentukan prioritas mitigasi. SMA Negeri 2 Situbondo menunjukkan satu *alert High*, sedangkan SMK Negeri 1 Panji tidak memiliki *alert High* tetapi memiliki beberapa temuan *Medium* dan *Informational*. Pola ini menunjukkan bahwa setiap *website* memerlukan triase terpisah berdasarkan konteks aset, konfigurasi, dan *exposure* layanan [47]. Dokumentasi visual pada Gambar 4 digunakan sebagai bukti observasional untuk memperjelas konteks *alert High* pada *website* pembanding.

Gambar 4. Indikasi *Defacement* pada *Website* SMA Negeri 2 Situbondo

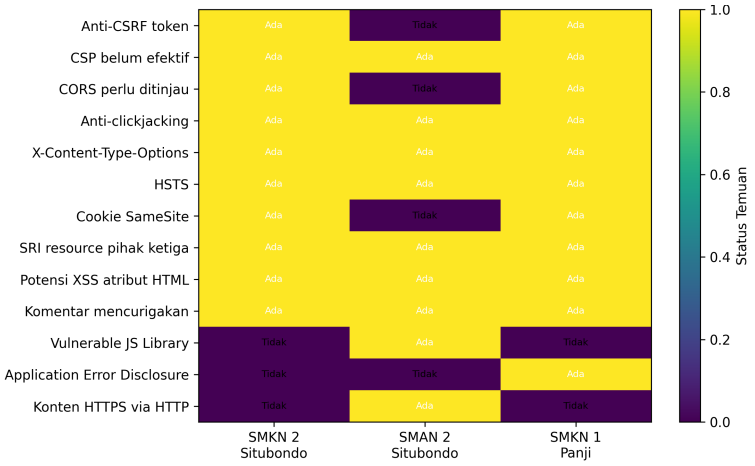
Indikasi *defacement* pada *website* pembanding dapat diamati pada Gambar 4. Dokumentasi visual tersebut menunjukkan perubahan tampilan portal dan sisipan konten tidak relevan dengan layanan pendidikan. Dalam penelitian ini, gambar diperlakukan sebagai bukti observasional untuk mendukung analisis *alert* kategori *High*, bukan sebagai atribusi pelaku atau uraian teknik serangan. Bukti visual ini menegaskan bahwa risiko *High* perlu diprioritaskan karena dapat berdampak pada integritas informasi, reputasi layanan, dan kepercayaan pengguna [48].

Tabel 4. Matriks Ringkas Temuan Dominan Lintas *Website*

Temuan Dominan	**SMKN 2**	**SMAN 2**	**SMKN 1**
Anti-CSRF token belum optimal	Ada	Tidak	Ada
CSP belum efektif	Ada	Ada	Ada
CORS perlu ditinjau	Ada	Tidak	Ada
Anti-clickjacking belum lengkap	Ada	Ada	Ada
X-Content-Type-Options belum disetel	Ada	Ada	Ada
HSTS belum konsisten	Ada	Ada	Ada
Cookie SameSite belum konsisten	Ada	Tidak	Ada
SRI *resource* pihak ketiga belum lengkap	Ada	Ada	Ada
Potensi XSS atribut HTML	Ada	Ada	Ada
Komentar mencurigakan	Ada	Ada	Ada

Vulnerable JS Library	Tidak	Ada	Tidak
Application Error Disclosure	Tidak	Tidak	Ada
Konten HTTPS tersedia melalui HTTP	Tidak	Ada	Tidak

Tabel 4 menyajikan matriks ringkas temuan dominan yang ditemukan pada ketiga *website* sekolah. Secara umum, sebagian besar temuan berkaitan dengan konfigurasi keamanan berbasis *header* HTTP, implementasi CSP, HSTS, *anti-clickjacking*, serta pengelolaan sumber daya pihak ketiga. Meskipun terdapat beberapa perbedaan pada temuan tertentu, pola kerentanan yang relatif serupa menunjukkan bahwa penguatan konfigurasi keamanan dasar masih menjadi kebutuhan utama dalam mendukung keamanan layanan pendidikan digital.



Gambar 5. Matriks Temuan Dominan Lintas *Website*

Gambar 5 menyajikan visualisasi matriks temuan dominan pada ketiga *website* yang dianalisis. Terlihat bahwa sebagian besar temuan, seperti kelemahan CSP, *anti-clickjacking*, HSTS, *X-Content-Type-Options*, SRI, serta potensi XSS atribut HTML, ditemukan secara konsisten pada seluruh *website*. Di sisi lain, beberapa temuan hanya muncul pada *website* tertentu, seperti *Vulnerable JS Library* pada SMA Negeri 2 Situbondo, *Application Error Disclosure* pada SMK Negeri 1 Panji, dan konten HTTPS yang masih dapat diakses melalui HTTP pada SMA Negeri 2 Situbondo. Pola ini menunjukkan adanya kesamaan kelemahan konfigurasi dasar sekaligus karakteristik risiko yang berbeda pada masing-masing *website*.

4.1. Pembahasan Teoretis dan Keterkaitan Kebijakan

Hasil penelitian memperkuat asumsi bahwa *security misconfiguration* merupakan risiko yang sering muncul pada layanan web yang sangat bergantung pada konfigurasi server, CMS, plugin, dan sumber eksternal [5]. Dalam kerangka CIA triad, kelemahan *header* dan *cookie* terutama berpengaruh pada integritas interaksi *browser*, kerahasiaan sesi pengguna, serta ketersediaan layanan ketika serangan berbasis *browser* atau *supply chain* terjadi [49]. Temuan ini juga mendukung pandangan bahwa keamanan aplikasi web harus diposisikan sebagai bagian dari tata kelola teknologi, bukan hanya aktivitas teknis insidental.

Dari sisi kebijakan publik, hasil penelitian relevan dengan UU Pelindungan Data Pribadi karena *website* sekolah berpotensi memproses data warga sekolah dan pemangku kepentingan. Perpres tentang percepatan transformasi digital layanan nasional menekankan pelayanan digital yang tepercaya dan penguatan keamanan informasi. Selain itu, regulasi Satu Data Pendidikan, Kebudayaan, Riset, dan Teknologi menempatkan data pendidikan sebagai aset yang perlu dikelola secara tertib dan dapat dipertanggungjawabkan [26]. Oleh karena itu, *hardening website* sekolah merupakan bentuk dukungan teknis terhadap kepatuhan, tata kelola data, dan layanan publik pendidikan yang aman.

Keterkaitan dengan SDGs tampak pada dua dimensi. Pertama, SDGs 4 menekankan pendidikan berkualitas dan akses pembelajaran yang inklusif, *website* sekolah yang aman membantu menjaga kesinambungan akses informasi pendidikan. Kedua, SDGs 9 menekankan infrastruktur yang tangguh dan inovasi, pen-

guatan *header*, sesi, dan dependensi pihak ketiga merupakan komponen kecil tetapi penting dalam membangun infrastruktur pendidikan digital yang lebih andal [22, 50].

5. IMPLIKASI MANAJERIAL

Temuan teknis perlu diterjemahkan menjadi keputusan manajerial agar dapat diimplementasikan oleh pengelola sekolah atau penyedia hosting. Implikasi manajerial utama adalah perlunya menetapkan keamanan *website* sebagai indikator tata kelola layanan digital sekolah, bukan hanya tugas teknis tambahan setelah *website* berjalan. Pengelola perlu memiliki daftar prioritas hardening, jadwal pemindaian berkala, mekanisme dokumentasi perubahan, dan pembagian tanggung jawab antara admin sekolah, penyedia hosting, dan pengembang *website*.

Penguatan keamanan *website* perlu difokuskan pada perbaikan konfigurasi CSP, HSTS, *nosniff*, dan *anti-clickjacking* melalui penerapan *hardening* yang terstruktur. Pengelolaan sumber daya eksternal seperti CORS, CDN, dan JavaScript pihak ketiga juga perlu dievaluasi secara berkala untuk mengurangi risiko yang berasal dari dependensi eksternal. Selain itu, kontrol sesi, *cookie*, dan CSRF harus diperkuat guna mendukung pelindungan data pengguna. Monitoring keamanan secara berkala serta peningkatan kompetensi *administrator* terkait konfigurasi keamanan dan *patching* menjadi langkah penting untuk memastikan efektivitas mitigasi dan keberlanjutan keamanan layanan digital sekolah.

Rekomendasi mitigasi difokuskan pada penguatan kontrol keamanan yang paling dominan ditemukan selama proses evaluasi. Pada aspek *transport*, pengelola *website* perlu mengaktifkan pengalihan HTTP ke HTTPS secara konsisten serta menerapkan *Strict-Transport-Security* (HSTS) setelah seluruh sumber daya berjalan stabil pada HTTPS. Untuk mencegah *clickjacking*, dapat ditambahkan *X-Frame-Options* dengan nilai *DENY* atau *SAMEORIGIN*, maupun menggunakan *directive frame-ancestors* pada CSP. Risiko *MIME sniffing* dapat diminimalkan dengan mengonfigurasi *X-Content-Type-Options: nosniff* pada seluruh *response* yang relevan. Penguatan CSP perlu dilakukan secara bertahap melalui mode *report-only*, inventarisasi sumber yang diperlukan, pengurangan penggunaan *wildcard*, serta menghindari *unsafe-inline* dan *unsafe-eval* jika memungkinkan. Selain itu, keamanan *cookie* dan sesi perlu ditingkatkan dengan menerapkan atribut *Secure*, *HttpOnly*, dan *SameSite*, serta mengombinasikannya dengan token anti-CSRF pada *endpoint* yang melakukan perubahan status. Dari sisi sumber daya pihak ketiga, diperlukan audit terhadap JavaScript dan CSS eksternal, penerapan *Subresource Integrity* pada sumber daya CDN, serta pengurangan dependensi terhadap domain yang tidak diperlukan.

6. KESIMPULAN

Pemindaian OWASP ZAP pada website SMK Negeri 2 Situbondo menghasilkan 26 jenis *alert* dengan distribusi 0 *High*, 12 *Medium*, 7 *Low*, dan 7 Informational. Temuan didominasi risiko menengah dan rendah yang berkaitan dengan konfigurasi HTTP *security header*, kebijakan CSP, kontrol *cookie*, serta pemuatan sumber pihak ketiga.

Dibandingkan *website* pembanding, *website* SMK Negeri 2 Situbondo memiliki jumlah temuan total lebih banyak, tetapi pola kerentanan yang muncul cenderung sejenis. Risiko dominan berada pada area OWASP *Security Misconfiguration*, khususnya ketidakkonsistenan konfigurasi protektif pada lapisan *browser* dan *transport*.

Secara teoretis, hasil penelitian memperkuat pentingnya *security misconfiguration* sebagai isu tata kelola teknologi pada transformasi digital pendidikan. Secara praktis, penelitian ini memberikan *baseline* perbaikan yang dapat diuji ulang, sedangkan secara sosial penelitian mendukung SDG 4 dan SDG 9 melalui penguatan keamanan layanan pendidikan digital.

7. SARAN

Pengelola *website* disarankan menjadikan hasil pemindaian sebagai *baseline hardening*, kemudian melakukan perbaikan bertahap berdasarkan prioritas risiko. Perbaikan awal sebaiknya difokuskan pada HSTS, *X-Content-Type-Options*, *X-Frame-Options* atau *frame-ancestors*, CSP, atribut *cookie*, token anti-CSRF, dan SRI.

Penelitian lanjutan disarankan menambahkan verifikasi manual terhadap *alert* prioritas, terutama CSP, HSTS, *clickjacking*, CSRF, atribut *cookie*, dan validasi sumber pihak ketiga. Cakupan juga perlu diperluas ke

endpoint terautentikasi agar kerentanan yang hanya muncul setelah *login* dapat dianalisis. Untuk meningkatkan kontribusi teknis, penelitian berikutnya dapat mengintegrasikan OWASP ZAP dengan alat lain seperti Nmap, Nikto, WPScan, atau *scanner* CMS yang relevan. Uji ulang setelah mitigasi juga perlu dilakukan agar efektivitas perbaikan dapat diukur secara empiris.

8. DEKLARASI

8.1. Tentang Penulis

Muhammad Hafied Hermawan (MH) https://orcid.org/0009-0003-3695-9854
Firman Jaya (FJ) https://orcid.org/0009-0005-0503-3033
Rahmat Shofan Razaqi (RS) https://orcid.org/0009-0005-8365-2665

8.2. Kontribusi Penulis

Konseptualisasi: MH; Metodologi: FJ; Perangkat Lunak: RS; Validasi: MH dan FJ; Analisis Formal: RS dan MH; Investigasi: FJ; Sumber daya: RS; Kurasi Data: MH; Penulisan Draf Awal: FJ dan RS; Peninjauan dan Penyuntingan Tulisan: MH dan FJ; Visualisasi: RS; Semua penulis, MH, FJ dan RS telah membaca dan menyetujui naskah yang telah diterbitkan.

8.3. Pernyataan Ketersediaan Data

Data yang disajikan dalam studi ini tersedia atas permintaan dari penulis terkait.

8.4. Pendanaan

Penulis tidak menerima dukungan finansial untuk penelitian, kepenulisan, dan/atau penerbitan artikel ini.

8.5. Deklarasi Konflik Kepentingan

Penulis menyatakan bahwa mereka tidak memiliki konflik kepentingan, konflik kepentingan finansial yang diketahui, atau hubungan pribadi yang dapat memengaruhi pekerjaan yang dilaporkan dalam makalah ini.

DAFTAR PUSTAKA

[1] S. A. Purnama, "Analisis vulnerability assessment sistem informasi pendidikan, pelatihan pt azure samudera karsa menggunakan zap," *BETRIK*, vol. 16, no. 02, pp. 240–251, 2025.
[2] R. A. R. B. Firdaus and T. I. Widyawan, "Pengujian kerentanan website menggunakan metode penetration testing dengan owasp (studi kasus: Pemerintah kabupaten semarang)," *Cyber Security dan Forensik Digital*, vol. 8, no. 2, pp. 114–123, 2025.
[3] S. N. Pattikawa and G. Hasan, "Pengaruh kepercayaan dan minat repurchase terhadap perilaku konsumen dalam berbelanja di e-commerce kota batam," *Technomedia Journal*, vol. 8, no. 1 Juni, pp. 52–66, 2023.
[4] D. E. Narhudin, B. Irawan, and A. Bahtiar, "Evaluasi keamanan website menggunakan metode owasp: Penilaian terhadap serangan injeksi sql dan cross-site scripting (xss)," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 1, pp. 675–680, 2024.
[5] J. I. N. S. Marbun, C. Trinata, and M. Rosmaya, "Kajian literatur analisis keamanan website," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 3, pp. 4474–4480, 2025.
[6] T. Hidayat, D. Manongga, Y. Nataliani, S. Wijono, S. Y. Prasetyo, E. Maria, U. Raharja, I. Sembiring *et al.*, "Performance prediction using cross validation (gridsearchcv) for stunting prevalence," in *2024 IEEE International Conference on Artificial Intelligence and Mechatronics Systems (AIMS)*. IEEE, 2024, pp. 1–6.
[7] D. Irawan, A. D. Ruliyanti, M. F. Zulfikar, M. Z. Fu'adhi, M. F. Rozi, M. Kholifah, and I. Thoib, "Functional testing of nganjuk runners website using black box testing method," *Jurnal Ilmiah Sistem Informasi*, vol. 4, no. 3, pp. 959–972, 2025.
[8] H. Hermanto and H. Haeruddin, "Peningkatan sistem keamanan website menggunakan metode owasp," *Jurnal Ilmu Komputer dan Bisnis*, vol. 13, no. 1, pp. 94–104, 2022.
[9] U. Rahardja, I. D. Hapsari, P. H. Putra, and A. N. Hidayanto, "Technological readiness and its impact on mobile payment usage: A case study of go-pay," *Cogent Engineering*, vol. 10, no. 1, p. 2171566, 2023.

[10] G. P. I. Fanani, M. A. Mu'min, and N. Tristanti, "Analisis dan pengujian kerentanan website menggunakan owasp zap," *Jurnal Riset Sistem dan Teknologi Informasi*, vol. 3, no. 1, pp. 36–50, 2025.
[11] D. Y. Prapaskia and C. Umam, "Analisis keamanan website upt rsud raa soewondo pati berdasarkan hasil penetration testing menggunakan owasp," *Jurnal Algoritma*, vol. 23, no. 1, pp. 1042–1050, 2026.
[12] N. N. Rafiana, "Technopreneurship strategy to grow entrepreneurship career options for students in higher education," *ADI Journal on Recent Innovation*, vol. 5, no. 2, pp. 110–126, 2024.
[13] N. Herawati, V. Budiyanto *et al.*, "Analisis keamanan sebuah domain menggunakan open web application security project (owasp) zap," *Jurnal Teknologi Technoscientia*, pp. 27–36, 2023.
[14] M. Alzril, M. I. Yamin, H. Effendi, M. Febriansyah *et al.*, "Analisis keamanan situs web rumah sakit menggunakan metode penetration testing owasp," *SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI*, vol. 35, no. 2, pp. 99–100, 2025.
[15] A. Iriani, Q. Aini, E. Maria, A. Khoirunisa, and N. Septiani, "Kekuatan pendorong utama di balik adopsi pemasaran digital oleh startup," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 3, no. 2, pp. 150–156, 2022.
[16] A. S. Gupta and A. Chakraborty, "Impact of digital education on attainment of sdg 4," *J. Inform. Educ. Res*, vol. 5, pp. 1–15, 2025.
[17] A. Dudhat and V. Agarwal, "Indonesia's digital economy's development," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 4, no. 2, pp. 109–118, 2023.
[18] A. R. Saputra, B. I. Aditya, N. T. Sunggono, and M. B. Ryando, "Analisis keamanan website global academic information system menggunakan owasp zap dan model ai lokal," *Jurnal Teknologi Informasi dan Multimedia*, vol. 7, no. 3, pp. 490–503, 2025.
[19] A. Pambudi, N. Lutfiani, M. Hardini, A. R. A. Zahra, and U. Rahardja, "The digital revolution of startup matchmaking: Ai and computer science synergies," in *2023 Eighth International Conference on Informatics and Computing (ICIC)*. IEEE, 2023, pp. 1–6.
[20] H. Rodiansyah and H. F. Muttaqin, "Studi analisis celah keamanan website spin laboratorium kalibrasi menggunakan metode pemindaian owasp zap, burp suite, dan nessus." *Journal of Syntax Literate*, vol. 10, no. 7, 2025.
[21] C. Sriliasta and D. S. S. Wuisan, "Stepping forward: Enhancing cognitive learning outcomes through hybrid rccr-based learning on circulatory system material," *International Transactions on Artificial Intelligence*, vol. 2, no. 1, pp. 49–59, 2023.
[22] G. Dede, A. M. Petsa, S. Kavalaris, E. Serrelis, S. Evangelatos, I. Oikonomidis, and T. Kamalakis, "Cybersecurity as a contributor toward resilient internet of things (iot) infrastructure and sustainable economic growth," *Information*, vol. 15, no. 12, p. 798, 2024.
[23] I. Alvarez-Icaza and O. Huerta, "Augmented intelligence for open education: Bridging the digital gap with inclusive design methods," in *Frontiers in Education*, vol. 9. Frontiers Media SA, 2024, p. 1337932.
[24] J. B. Hendrawidjaja, B. W. Soetjipto, R. D. Kusumastuti, and O. Jayanagara, "Ecosystem exchange, strategic capabilities, and firm performance with agility and innovation mediators," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 226–238, 2026.
[25] M. A. Mu'min, A. Fadlil, and I. Riadi, "Analisis keamanan sistem informasi akademik menggunakan open web application security project framework," *J. Media Inform. Budidarma*, vol. 6, no. 3, p. 1468, 2022.
[26] C. J. P. Abuda and C. E. Dumdumaya, "A multi-vector framework for injection attack detection using nlp lexical–semantic fusion with reinforcement learning dqn–based calibration." *International Journal of Advanced Computer Science & Applications*, vol. 17, no. 3, p. 957, 2026.
[27] Y. H. Dulanlebit, H. Hernani, L. Liliasari, M. B. Amran, and G. A. Pangilinan, "Technopreneurship and market feasibility of modified carrageenan hydrogel for industrial heavy metal remediation," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 199–210, 2026.
[28] A. F. Hasibuan, D. Handoko *et al.*, "Analisis keretanan website dengan aplikasi owasp zap," *Jurnal Ilmu Komputer dan Sistem Informasi*, vol. 2, no. 2, pp. 141–154, 2023.
[29] F. A. Hassanaha, E. Ryansyaha, F. M. Setiawana, R. Alamsyaha, A. Susilo, and Y. Irawana, "Analisis kerentanan keamanan menggunakan owasp zap dan pengujian manual pada tampilan antarmuka laman pddikti," *Jurnal Elektronik Ilmu Komputer Udayana p-ISSN*, vol. 2301, p. 5373, 2025.
[30] M. Pereira, I. Guvlor *et al.*, "Implementation of artificial intelligence framework to enhance human resources competency in indonesia," *International Journal of Cyber and IT Service Management*, vol. 4, no. 1, pp. 64–70, 2024.

[31] Kasmawi, N. Hidayasari, and Mansur, "Vulnerability analysis using owasp zap on higher education websites," in *AIP Conference Proceedings*, vol. 2665, no. 1. AIP Publishing LLC, 2023, p. 030015.
[32] D. Monika, M. Magta, D. E. Rose *et al.*, "Peran program kelas dalam membina literasi sains pada anak usia dini," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 2, no. 2, pp. 176–187, 2024.
[33] M. W. S. Utomo, "Vulnerability assessment web instansi a menggunakan owasp zap, nmap, dan analisis konfigurasi ssl/tls," in *Prosiding Seminar Nasional Informatika Bela Negara (SANTIKA)*, vol. 5, no. 2, 2025, pp. 80–85.
[34] E. Sana, A. Fitriani, D. Soetarno, M. Yusuf *et al.*, "Analysis of user perceptions on interactive learning platforms based on artificial intelligence," *CORISINTA*, vol. 1, no. 1, pp. 26–32, 2024.
[35] H. Pahlawansah, M. F. Basmar, and M. Yusuf, "Analisis kerentanan website smk muhammadiyah 2 bontoala makassar menggunakan metode owasp (open web application security project)," *BIOS: Jurnal Teknologi Informasi dan Rekayasa Komputer*, vol. 6, no. 2, pp. 92–100, 2025.
[36] S. Suryanto, A. A. A. Zawawi, and M. Morales, "Optimalisasi media sosial sebagai sarana peningkatan keterlibatan sosial umat islam: Optimizing social media as a means of increasing social involvement of muslims," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 2, no. 1, pp. 97–106, 2025.
[37] D. Sigalov and D. Gamayunov, "Dead or alive: Discovering server http endpoints in both reachable and dead client-side code," *Journal of Information Security and Applications*, vol. 82, p. 103746, 2024.
[38] A. P. N. Sihombing, A. Prabowo, I. D. Id, and T. Melia, "Analisis kerentanan keamanan pada sistem informasi akademik berbasis web menggunakan owasp-zap," *INFOTECH: Jurnal Informatika & Teknologi*, vol. 7, no. 1, pp. 150–158, 2026.
[39] H. Tahalli, R. Albar, M. D. Payana, and M. B. Wibawa, "Pengujian keamanan website terhadap serangan deface dan redirect injection melalui simulasi dengan owasp zap (studi kasus: Website universitas ubudiyah indonesia)," *JOURNAL OF INFORMATICS AND COMPUTER SCIENCE*, vol. 11, no. 2, pp. 104–111, 2025.
[40] N. H. Farhansyah and H. Fabroyir, "Entrepreneurial applications of augmented reality in product placement on shelves," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 185–198, 2026.
[41] Bid TIK Polda Kepulauan Riau. (2026, Apr.) Teknik keamanan aplikasi web dengan owasp. Bidang Teknologi Informasi dan Komunikasi Polda Kepulauan Riau. [Online]. Available: https://bidtik.kepri.polri.go.id/teknik-keamanan-aplikasi-web-dengan-owasp/
[42] R. Indrawan, A. Ratih, H. Agustian, and R. Evans, "Governance models for blockchain integrated iot ecosystems," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 219–229, 2026.
[43] A. W. Kuncoro, S. Fayruz Rahma, and M. ENG, "Analisis metode open web application security project (owasp) pada pengujian keamanan website: Literature review," *Automata*, vol. 3, no. 1, 2022.
[44] G. Kydyrbayeva, D. Makhmetova, G. Kulzhanbekova, R. Anayatova, A. Otetileuova, and Z. Tashenova, "The initial state of educating future primary school teachers in a multilingual context," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 152–165, 2026.
[45] A. Hannousse, S. Yahiouche, and M. C. Nait-Hamoud, "Twenty-two years since revealing cross-site scripting attacks: A systematic mapping and a comprehensive survey," *Computer Science Review*, vol. 52, p. 100634, 2024.
[46] I. Sembiring, B. K. Aji, and T. I. Bayu, "Consortium blockchain framework for secure digital medical record innovation," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 138–151, 2026.
[47] T. Ariyadi, H. Fadli, T. Akbar, and M. B. Prihandoko, "Implementasi owasp untuk analisis kerentanan dan keamanan pada sistem informasi akademik terintegrasi universitas bina darma," *STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer*, vol. 4, no. 1, pp. 1–7, 2025.
[48] Y. Vidhiastutik, "Pengaruh pola diet dash terhadap tekanan darah pada penderita hipertensi: Literature review the effect of the dash diet on blood pressure in hypertension patients," *Well Being*, vol. 8, no. 2, pp. 159–169, 2023.
[49] S. S. Mahmood, "Sql injection detection using machine learning and explainability," *Journal of Internet Services and Information Security*, vol. 15, no. 2, pp. 309–324, 2025.
[50] D. Hariyani, P. Hariyani, and S. Mishra, "Digital technologies for the sustainable development goals," *Green Technologies and Sustainability*, vol. 3, no. 3, p. 100202, 2025.