BIOS : Jurnal Teknologi Informasi dan Rekayasa Komputer
Vol. 6, No. 2, September 2025, hlm. 92-100
e-ISSN: 2722-0850

Analisis Kerentanan Website SMK Muhammadiyah 2 Bontoala Makassar Menggunakan Metode OWASP (*Open Web Application Security Project*)

Haniwijaya Pahlawansah[1], Muh. Fahmi Basmar[2], Muhammad Yusuf[3]
[1] Teknik Informatika, Poliktenik Maritim AMI Makassar, *haniwijaya.p@gmail.com*
[2]Teknik Informatika, Universitas Pejuang Republik Indonesia, *fahmi.basmar@gmail.com*
[3] Teknik Informatika, Universitas Pejuang Republik Indonesia, *yusufhasanuddin68@gmail.com*

Keywords

Vulnerability Analysis,
Web Security,
OWASP Top 10,
Penetration Testing,
Educational Website

ABSTRACT

The official website of SMK Muhammadiyah 2 Bontoala Makassar plays a crucial role as a medium for information and services. However, its significance is often not matched by a verified security posture. The primary problem addressed in this study is the potential for unidentified cybersecurity vulnerabilities on the website, which malicious actors could exploit. To address this problem, a systematic vulnerability analysis was conducted based on the Open Web Application Security Project (OWASP) Top 10 framework. The testing process combined automated scanning using the OWASP ZAP tool with manual validation via penetration testing to ensure the accuracy of the findings. The assessment successfully identified several critical security flaws, primarily in the categories of Cross-Site Scripting (XSS) (A03:2021), Security Misconfiguration (A05:2021), and Vulnerable and Outdated Components (A06:2021). These vulnerabilities directly expose the website to risks of data breaches, unauthorized content modification, and service disruption. This study concludes by providing concrete technical recommendations for administrators to mitigate the identified vulnerabilities and strengthen the website's overall security posture.

Kata Kunci

Analisis Kerentanan,
Keamanan Web,
OWASP Top 10,
Penetration Testing,
Website Pendidikan.

ABSTRAK

Website SMK Muhammadiyah 2 Bontoala Makassar memegang peranan krusial sebagai media informasi dan layanan, namun signifikansinya seringkali tidak diimbangi dengan jaminan keamanan yang terverifikasi. Permasalahan utama yang diangkat dalam penelitian ini adalah adanya potensi kerentanan keamanan siber yang belum teridentifikasi pada website tersebut, yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Untuk menjawab permasalahan ini, dilakukan analisis kerentanan secara sistematis menggunakan kerangka kerja Open Web Application Security Project (OWASP) Top 10. Proses pengujian mengkombinasikan pemindaian otomatis dengan tools OWASP ZAP dan validasi manual melalui pengujian penetrasi untuk memastikan akurasi temuan. Hasil asesmen berhasil mengidentifikasi beberapa celah keamanan kritis, terutama dalam kategori Cross-Site Scripting (XSS) (A03:2021), Security Misconfiguration (A05:2021), dan Vulnerable and Outdated Components (A06:2021). Kelemahan ini secara langsung membuka risiko kebocoran data, modifikasi konten tanpa izin, dan gangguan layanan. Penelitian ini menyimpulkan dengan memberikan rekomendasi teknis yang konkret bagi administrator untuk memitigasi kerentanan yang ada dan memperkuat postur keamanan website secara menyeluruh.

Korespondensi Penulis:

Muh. Fahmi Basmar
Universitas Pejuang Republik Indonesia,
Jl. Nipa-Nipa Antang No. 23 Makassar (90234)
Telepon : +6282337937298
Email: *fahmi.basmar@gmail.com*

Submitted : 08-09-2025; Accepted : 19-09-2025;
Published : 28-09-2025

PENDAHULUAN

Di tengah percepatan transformasi digital global, institusi pendidikan kini mengoperasikan aset digital yang krusial, salah satunya adalah website resmi. Website tidak lagi berfungsi sebagai brosur statis, melainkan telah menjadi ekosistem digital terintegrasi yang melayani berbagai fungsi strategis. Bagi institusi seperti SMK Muhammadiyah 2

Bontoala Makassar, website merupakan gerbang utama interaksi digital, pusat diseminasi informasi akademik, platform pendaftaran siswa baru secara daring, dan medium untuk membangun citra publik. Mengingat peran sentral ini, ketersediaan (availability), integritas (integrity), dan kerahasiaan (confidentiality) data menjadi pilar fundamental yang harus dijaga. Meskipun belum ada laporan insiden siber berskala besar, observasi awal pada website sekolah menunjukkan adanya beberapa anomali minor, seperti waktu muat yang lambat secara tidak wajar dan beberapa tautan yang tidak berfungsi, yang dapat menjadi indikator awal dari masalah keamanan yang lebih dalam. Menyadari bahwa institusi pendidikan lain di Indonesia telah menjadi target serangan seperti defacement dan pencurian data, maka muncul urgensi untuk melakukan audit keamanan secara proaktif. Penelitian ini dilakukan untuk mengidentifikasi dan memitigasi kerentanan tersebut sebelum insiden yang lebih merusak benar-benar terjadi dan mengganggu operasional sekolah.

Namun, peningkatan signifikansi digital ini diiringi oleh eskalasi ancaman siber yang menjadikan sektor pendidikan sebagai salah satu target utama. Institusi pendidikan seringkali dipandang sebagai "sasaran empuk" oleh para pelaku kejahatan siber karena dua faktor kunci: kekayaan data sensitif yang dimiliki (informasi pribadi siswa, data guru, dan detail administratif) dan alokasi sumber daya yang seringkali terbatas untuk postur pertahanan siber [8]. Realitas ini tercermin dalam berbagai temuan empiris di Indonesia. Studi-studi yang dilakukan secara terpisah telah secara konsisten mengidentifikasi keberadaan kerentanan kritis pada website sekolah. Pratama dan Riadi (2021) serta Sari dan Susanto (2019) sama-sama menyoroti prevalensi celah keamanan fundamental seperti *SQL Injection* dan *Cross-Site Scripting* (XSS) pada domain web SMA/SMK [4, 3].

Keberadaan kerentanan ini bukan sekadar anomali teknis, melainkan gerbang terbuka bagi serangkaian dampak destruktif. Serangan *Cross-Site Scripting* (XSS), misalnya, memungkinkan penyerang untuk menyuntikkan skrip berbahaya yang dapat mencuri sesi (*session hijacking*) pengguna, termasuk akun administrator, yang pada akhirnya memberikan kendali penuh atas konten website [7]. Sementara itu, serangan *SQL Injection* dapat dieksploitasi untuk memanipulasi, mencuri, atau bahkan menghapus seluruh basis data yang menjadi sandaran operasional sekolah. Konsekuensi dari serangan semacam ini jauh melampaui gangguan teknis; ia dapat menyebabkan kerugian finansial, kerusakan reputasi yang sulit dipulihkan, pelanggaran kepatuhan terhadap regulasi privasi data, dan hilangnya kepercayaan dari masyarakat.

Untuk menghadapi lanskap ancaman yang dinamis ini, pendekatan keamanan yang bersifat reaktif—menunggu insiden terjadi baru kemudian merespons—sudah tidak lagi relevan. Diperlukan sebuah paradigma proaktif yang berfokus pada identifikasi dan remediasi kerentanan secara sistematis sebelum dapat dieksploitasi. Di sinilah metodologi pengujian keamanan terstruktur seperti *Penetration Testing* memegang peranan krusial [6]. Agar proses pengujian ini efektif dan komprehensif, diperlukan sebuah kerangka kerja standar yang diakui secara global. OWASP (*Open Web Application Security Project*) Top 10 hadir sebagai standar de facto dalam industri keamanan siber, menyediakan daftar sepuluh kategori risiko keamanan aplikasi web yang paling kritis dan sering ditemukan [1]. Relevansi dan efektivitas OWASP Top 10 sebagai pedoman asesmen telah terbukti dalam berbagai studi, baik pada domain pendidikan tinggi [2] maupun pada platform komersial yang kompleks [5].

Berangkat dari urgensi tersebut, penelitian ini dilaksanakan untuk melakukan analisis kerentanan keamanan secara mendalam pada website SMK Muhammadiyah 2 Bontoala Makassar. Dengan mengadopsi metodologi *Penetration Testing Execution Standard* (PTES) [8] dan menggunakan kerangka acuan risiko OWASP Top 10 edisi 2021 [1], penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan melaporkan celah keamanan secara terstruktur. Hasil dari penelitian ini diharapkan dapat memberikan manfaat pada dua tingkatan yang berbeda. Manfaat Umum (Bagi Komunitas Akademik & Pendidikan), Secara umum, penelitian ini berkontribusi sebagai sebuah studi kasus empiris. Hasilnya dapat menjadi referensi dan model penerapan asesmen keamanan siber bagi institusi pendidikan lain di Indonesia yang menghadapi tantangan serupa, namun memiliki sumber daya teknis yang terbatas. Manfaat Khusus (Bagi SMK Muhammadiyah 2 Bontoala Makassar), Manfaat yang diterima oleh sekolah bersifat langsung dan praktis. Penelitian ini tidak hanya memberikan potret akurat mengenai kondisi keamanan website saat ini, tetapi yang lebih penting, menyajikan sebuah peta jalan strategis. Peta jalan ini berisi daftar prioritas kerentanan beserta rekomendasi teknis konkret yang dapat segera ditindaklanjuti oleh administrator. Manfaat utamanya adalah untuk memperkuat benteng pertahanan digital, melindungi aset informasi berharga seperti data siswa dan guru, serta mencegah potensi gangguan layanan yang dapat merusak kegiatan operasional dan reputasi sekolah

1. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metodologi studi kasus untuk melakukan asesmen keamanan siber pada website SMK Muhamadiyah 2 Bontoala Makassar. Proses asesmen ini diimplementasikan melalui simulasi serangan etis yang dikenal sebagai *Penetration Testing*. Pendekatan yang dipilih adalah Black Box Testing, di mana penguji memposisikan diri sebagai penyerang eksternal tanpa pengetahuan sebelumnya mengenai arsitektur internal, kode sumber, atau infrastruktur target [7]. Pendekatan ini diadopsi karena mampu menyimulasikan skenario serangan dari dunia nyata secara akurat, di mana penyerang biasanya memulai aksinya dengan informasi yang minim tentang target [6].

2.1 Kerangka Kerja Penelitian

Seluruh alur penelitian ini distrukturkan berdasarkan kerangka kerja *Penetration Testing Execution Standard* (PTES), sebuah standar yang membagi proses pengujian penetrasi ke dalam beberapa tahapan logis

untuk memastikan pengujian berjalan secara sistematis, terukur, dan dapat diulang (*replicable*) [8]. Sementara itu, untuk identifikasi dan klasifikasi jenis kerentanan, penelitian ini mengacu sepenuhnya pada standar industri OWASP Top 10 edisi 2021 [1].

Gambar 2.1. kerangka kerja *Penetration Testing Execution Standard* (PTES)

2.2 Tahap Penelitian

Proses penelitian dibagi ke dalam empat tahapan utama yang diadaptasi dari kerangka kerja PTES, sebagai berikut:

a. Tahap Perencanaan dan Pengintaian (*Planning & Reconnaissance*)

Tahap awal ini berfokus pada pengumpulan informasi pasif dan aktif mengenai target. Tujuannya adalah untuk membangun pemahaman awal tentang jejak digital website dan teknologi yang digunakannya. Aktivitas yang dilakukan meliputi:

1. Pemetaan Domain dan Subdomain: Mengidentifikasi semua domain dan subdomain yang terkait dengan target.
2. Identifikasi Teknologi: Menggunakan teknik fingerprinting untuk mengidentifikasi sistem manajemen konten (CMS), versi server web (misalnya Apache, Nginx), bahasa pemrograman backend (misalnya PHP), dan platform basis data yang digunakan.
3. Enumerasi Titik Interaksi: Memetakan semua titik di mana pengguna dapat berinteraksi dengan aplikasi, seperti formulir login, kolom pencarian, formulir kontak, dan parameter URL. Informasi ini krusial untuk merencanakan fase pengujian selanjutnya.

b. Tahap Pemindaian dan Analisis Kerentanan (*Scanning & Vulnerability Analysis*)

Pada tahap ini, pemindaian aktif dilakukan terhadap target untuk mengidentifikasi potensi celah keamanan secara otomatis, yang kemudian divalidasi secara manual.

1. Pemindaian Otomatis: Perangkat lunak OWASP *Zed Attack Proxy* (ZAP) [10] digunakan sebagai alat pemindaian utama. OWASP ZAP dipilih karena merupakan proyek andalan dari OWASP, bersifat open-source, dan telah digunakan secara luas dalam penelitian sejenis [2, 11]. Proses ini melibatkan spidering untuk memetakan seluruh struktur direktori dan halaman website, diikuti dengan active scanning yang mengirimkan ribuan payload berbahaya untuk menguji kerentanan umum sesuai daftar OWASP Top 10.
2. Verifikasi Manual dan Eliminasi False Positive: Hasil dari pemindaian otomatis tidak diterima begitu saja. Setiap temuan diverifikasi secara manual untuk mengonfirmasi keberadaan kerentanan dan menghilangkan temuan yang keliru (false positive). Proses ini melibatkan pembuatan payload khusus dan analisis respons dari server, sebuah teknik yang diuraikan secara mendalam dalam literatur peretasan aplikasi web [9]. Sebagai contoh, untuk memvalidasi temuan XSS, penguji secara manual menyuntikkan skrip pada kolom input dan mengamati apakah skrip tersebut dieksekusi oleh peramban.

c. Tahap Eksploitasi (*Exploitation*)

Tahap ini dilakukan secara terkendali dengan tujuan untuk mendemonstrasikan dampak nyata dari kerentanan yang telah divalidasi. Penting untuk dicatat bahwa eksploitasi hanya dilakukan sebatas pembuktian konsep (*Proof of Concept - PoC*) dan tidak bertujuan untuk menyebabkan kerusakan, mencuri data, atau mempertahankan akses. Misalnya, pada temuan *Stored* XSS, eksploitasi hanya dilakukan dengan menyuntikkan skrip *alert()* sederhana untuk membuktikan bahwa celah tersebut memang ada dan dapat dieksekusi.

d. Tahap Pelaporan dan Rekomendasi (*Reporting*)

Tahap akhir dari metodologi ini adalah dokumentasi seluruh temuan dalam sebuah laporan yang terstruktur. Laporan ini mencakup:

1. Deskripsi Kerentanan: Penjelasan teknis mengenai setiap celah keamanan yang ditemukan.

2. Klasifikasi Risiko: Setiap kerentanan diklasifikasikan berdasarkan kategori OWASP Top 10 [1] dan diberi peringkat risiko (misalnya, Tinggi, Sedang, Rendah) berdasarkan potensi dampaknya terhadap kerahasiaan, integritas, dan ketersediaan sistem.
3. Bukti Konsep (PoC): Lampiran tangkapan layar dan langkah-langkah replikasi untuk setiap kerentanan.
4. Rekomendasi Mitigasi: Saran perbaikan teknis yang konkret dan dapat ditindaklanjuti untuk setiap kerentanan, seperti melakukan pembaruan versi CMS, menerapkan validasi input (input sanitization), dan memperbaiki konfigurasi keamanan server.

2.3 Tahap Pemindaian dan Analisis Kerentanan (*Scanning & Vulnerability Analysis*)

Tahap Pemindaian dan Analisis Kerentanan adalah fase paling kritis dalam metodologi penelitian ini, di mana proses identifikasi celah keamanan secara aktif dilaksanakan. Fase ini beralih dari pengumpulan informasi pasif ke interaksi agresif yang terkendali dengan aplikasi web target. Tujuannya adalah untuk mengungkap kelemahan teknis yang dapat dieksploitasi oleh penyerang. Untuk mencapai hasil yang akurat dan komprehensif, penelitian ini mengadopsi strategi pemindaian hibrida, yang mengkombinasikan kecepatan dan cakupan luas dari alat pemindai otomatis dengan ketajaman analisis dan intuisi kontekstual dari verifikasi manual.

a. Fase 1: Pemindaian Otomatis Berbasis Luas (*Automated Broad-Based Scanning*)

Fase pertama berfokus pada penggunaan perangkat lunak khusus untuk memindai seluruh permukaan serangan (*attack surface*) website secara efisien. Alat utama yang digunakan adalah OWASP *Zed Attack Proxy* (ZAP) [10], yang dipilih karena selaras dengan kerangka kerja OWASP dan telah terbukti efektif dalam penelitian sejenis [2, 11].

Proses ini dibagi lagi menjadi dua sub-tahapan kritis:

1. *Discovery & Spidering* (Penemuan & Perayapan): Sebelum melancarkan serangan simulasi, ZAP diinstruksikan untuk melakukan *spidering* atau perayapan mendalam terhadap seluruh domain target. ZAP secara rekursif menavigasi setiap tautan, formulir, dan skrip untuk membangun peta situs (*sitemap*) yang komprehensif. Proses ini sangat fundamental karena tujuannya adalah untuk mengidentifikasi semua titik masuk potensial (*entry points*) yang dapat dieksploitasi, termasuk halaman yang mungkin tidak terhubung langsung dari halaman utama atau parameter URL yang tersembunyi. Hasil dari tahap ini adalah sebuah inventaris lengkap dari seluruh permukaan serangan yang akan diuji.
2. *Active Scanning* (Pemindaian Aktif): Setelah peta situs lengkap, *active scanner* ZAP diaktifkan. Pada tahap inilah ZAP bertransformasi dari pengamat pasif menjadi penyerang aktif. ZAP mengirimkan ribuan *payload* berbahaya yang telah dikalibrasi ke setiap titik masuk yang ditemukan pada tahap *spidering*. *Payload* ini merupakan variasi dari teknik serangan yang diketahui, dirancang untuk memicu respons dari aplikasi yang mengindikasikan adanya kerentanan. Serangan-serangan ini secara spesifik menargetkan kategori risiko dalam OWASP Top 10, seperti:
   1) Injeksi SQL: Mengirimkan karakter khusus dan perintah SQL untuk menguji apakah aplikasi rentan terhadap manipulasi basis data.
   2) *Cross-Site Scripting* (XSS): Menyuntikkan tag skrip untuk menguji apakah input pengguna divalidasi dengan benar sebelum ditampilkan kembali.
   3) *Path Traversal*: Mencoba mengakses file atau direktori di luar *folder root web* untuk menguji kontrol akses.

Hasil dari pemindaian aktif adalah sebuah laporan awal yang berisi daftar panjang potensi kerentanan, yang masing-masing diberi peringkat risiko awal oleh ZAP.

b. Fase 2: Analisis Manual, Triase, dan Validasi Kontekstual

Ini adalah fase di mana kecerdasan manusia mengambil alih untuk menyempurnakan hasil mentah dari pemindai otomatis. Setiap temuan dari ZAP diperlakukan sebagai hipotesis, bukan sebagai fakta, dan harus melalui proses validasi yang ketat.

1. Triase dan Eliminasi *False Positive*: Langkah pertama adalah melakukan triase, yaitu memilah dan memprioritaskan temuan. Tim peneliti secara manual mereplikasi setiap potensi kerentanan yang dilaporkan. Misalnya, jika ZAP melaporkan adanya celah XSS pada kolom komentar, peneliti akan mencoba menyuntikkan *payload JavaScript* non-destruktif secara manual, seperti "><script>alert(document.domain)</script>. Jika sebuah kotak peringatan muncul menampilkan domain website, kerentanan tersebut divalidasi sebagai temuan yang sah. Sebaliknya, jika tidak ada reaksi atau input tersebut dibersihkan (*sanitized*) oleh server, temuan tersebut ditandai sebagai *false positive* dan dieliminasi dari laporan akhir.
2. Analisis Dampak Kontekstual: Setelah divalidasi, setiap kerentanan dianalisis dalam konteks fungsinya di dalam aplikasi. Sebuah kerentanan tidak dinilai hanya berdasarkan tingkat keparahan teknisnya, tetapi juga berdasarkan dampak bisnisnya. Sebagai contoh, kerentanan *SQL Injection* pada fitur pencarian publik memiliki dampak yang berbeda dengan kerentanan yang sama pada formulir login administrator. Analisis kontekstual ini memungkinkan peringkat risiko yang lebih akurat dan relevan bagi institusi.

3. Identifikasi Rantai Serangan (*Attack Chain*): Pada tahap ini, peneliti juga mencari kemungkinan bagaimana beberapa kerentanan berisiko rendah atau sedang dapat dirangkai (*chained*) bersama untuk menciptakan serangan dengan dampak yang jauh lebih besar. Misalnya, kebocoran informasi (risiko rendah) dapat memberikan petunjuk untuk mengeksploitasi kontrol akses yang rusak (risiko sedang) guna mengakses data sensitif.

Tujuan akhir dari keseluruhan tahap pemindaian dan analisis ini adalah untuk menghasilkan sebuah daftar kerentanan yang telah divalidasi sepenuhnya, dinilai secara kontekstual, dan dapat dipertanggungjawabkan secara teknis, yang menjadi dasar yang kokoh untuk bab Hasil dan Pembahasan.

2. HASIL DAN ANALISIS

3.1 Hasil Penelitian

Pengujian keamanan siber yang dilakukan secara metodis terhadap website SMK Muhammadiyah 2 Bontoala Makassar telah berhasil mengidentifikasi dan memvalidasi lima kerentanan keamanan yang berbeda. Berdasarkan matriks evaluasi risiko yang mengacu pada standar OWASP Top 10 2021, temuan ini diklasifikasikan ke dalam dua kerentanan dengan tingkat dampak Tinggi, yang mengindikasikan potensi kompromi sistem secara signifikan, dan tiga kerentanan dengan tingkat dampak Sedang, yang berfungsi sebagai vektor pendukung untuk serangan yang lebih kompleks. Rangkuman eksekutif dari setiap temuan disajikan pada Tabel 1.

Tabel 1. Hasil Identifikasi Kerentanan

ID Kerentanan	Kategori OWASP (2021)	Tingkat Risiko	Deskripsi	Dampak Potensial	Rekomendasi Perbaikan
VULN-01	*A03: Injection (Stored XSS)*	TINGGI	Aplikasi gagal melakukan validasi dan sanitasi input pada fitur buku tamu, memungkinkan penyerang menyimpan skrip berbahaya di database.	1. Pencurian *cookie* sesi 2. Pengambilalihan akun 3. Pengalihan ke situs phishing	1. Terapkan validasi input sisi *server* 2. Lakukan output encoding 3. Gunakan *Content Security Policy (CSP)*
VULN-02	*A06: Vulnerable and Outdated Components*	TINGGI	*Website* menggunakan versi CMS dan plugin yang usang dan memiliki catatan kerentanan publik (CVE) yang dapat dieksploitasi.	1. Kompromi total *server* 2. Eksekusi kode jarak jauh 3. Kebocoran seluruh *database*	1. Perbarui inti CMS dan semua *plugin* ke versi terbaru 2. Hapus komponen yang tidak terpakai 3. Lakukan manajemen patch secara rutin
VULN-03	*A05: Security Misconfiguration*	SEDANG	*server* menampilkan pesan kesalahan yang terlalu detail (misalnya, *path directory*), yang membocorkan informasi internal aplikasi.	1. Membantu penyerang memetakan struktur aplikasi 2. Mempermudah penemuan celah lain	1. Konfigurasi *server* untuk menampilkan halaman error generik 2. Matikan *mode debug* di lingkungan produksi
VULN-04	*A01: Broken Access Control (IDOR)*	SEDANG	Aplikasi memungkinkan akses langsung ke dokumen melalui *URL* tanpa memeriksa hak akses, hanya dengan mengubah *ID file*.	1. Kebocoran data atau dokumen sensitif 2. Pelanggaran privasi data pengguna	1. Terapkan pemeriksaan hak akses di sisi *server* untuk setiap permintaan *file* 2. Gunakan ID acak (UUID) untuk referensi *file*

ID Kerentanan	Kategori OWASP (2021)	Tingkat Risiko	Deskripsi	Dampak Potensial	Rekomendasi Perbaikan
VULN-05	*A07: Identification and Authentication Failures*	SEDANG	Halaman login administrator tidak memiliki proteksi terhadap serangan *brute-force* (penebakan kata sandi berulang kali).	1. Pengambilalihan akun administrator 2. Peningkatan beban pada *server*	1. Terapkan penguncian akun setelah beberapa kali gagal *login* 2. Gunakan *CAPTCHA* 3. Terapkan kebijakan kata sandi yang kuat

Tabel 1 menyajikan rekapitulasi temuan dari proses pemindaian dan asesmen keamanan yang telah dilakukan. Tabel ini berfungsi sebagai ringkasan eksekutif dari seluruh celah keamanan yang berhasil diidentifikasi. Setiap baris dalam tabel merepresentasikan satu kerentanan unik, yang dirinci ke dalam beberapa kolom informatif:

1. ID Kerentanan: Kode identifikasi unik (misalnya, VULN-01) yang diberikan untuk setiap temuan guna mempermudah pelacakan dan referensi dalam laporan.
2. Kategori OWASP: Klasifikasi kerentanan berdasarkan standar OWASP Top 10 edisi 2021, yang menunjukkan jenis kelemahan fundamental pada aplikasi web.
3. Deskripsi Temuan: Penjelasan teknis yang spesifik mengenai di mana dan bagaimana kerentanan tersebut ditemukan pada website target.
4. Tingkat Risiko: Penilaian dampak potensial dari kerentanan tersebut terhadap sistem, yang dikategorikan sebagai Tinggi atau Sedang.
5. Rekomendasi Perbaikan: Ini disajikan didasarkan pada panduan mitigasi resmi dan praktik terbaik yang telah distandarisasi oleh komunitas keamanan siber, terutama yang dirilis oleh OWASP, untuk setiap kategori kerentanan yang relevan, Langkah-langkah mitigasi yang konkret dan dapat ditindaklanjuti yang disarankan untuk pengelola website guna memperbaiki celah keamanan yang bersangkutan.

Tabel ini dirancang untuk memberikan gambaran yang jelas dan terstruktur mengenai postur keamanan website saat ini serta menjadi dasar untuk perencanaan perbaikan.

3.2 Analisis dan Pembahasan Mendalam

Analisis terhadap temuan ini melampaui sekadar enumerasi kelemahan teknis; ia menyingkap sebuah narasi tentang postur keamanan yang reaktif dan adanya celah fundamental dalam praktik tata kelola keamanan digital. Pembahasan berikut menguraikan signifikansi strategis dari setiap temuan dan menganalisis bagaimana interaksi antar kerentanan ini menciptakan sebuah "rantai serangan" (*attack chain*) yang sangat mungkin dieksploitasi.

a. Kerentanan Risiko Tinggi: Titik Rawan Eskalasi Serangan

Dua kerentanan berisiko tinggi yang teridentifikasi, A03:2021-*Injection (Stored XSS)* dan A06:2021-Vulnerable and Outdated Components, merupakan ancaman paling akut dan mendesak karena kemampuannya untuk berfungsi sebagai gerbang utama bagi kompromi sistem secara penuh.

1. VULN-01 (Stored XSS): Eksploitasi Kepercayaan dan Ancaman Internal Persisten: Temuan *Stored Cross-Site Scripting* (XSS) pada VULN-01 merepresentasikan ancaman yang sangat berbahaya karena sifatnya yang persisten dan kemampuannya mengeksploitasi elemen paling berharga: kepercayaan pengguna. Ketika penyerang berhasil menyuntikkan skrip berbahaya ke dalam basis data, website sekolah secara tidak sadar menjadi inang sekaligus distributor *malware*. Setiap pengunjung, mulai dari siswa, orang tua, hingga staf administrasi, yang mengakses halaman terinfeksi akan secara otomatis menjalankan skrip tersebut di peramban mereka. Hal ini sejalan dengan analisis S. et al. (2019) mengenai XSS sebagai vektor utama untuk pembajakan sesi [7]. Skenario serangan yang dapat terjadi sangat beragam dan merusak, mulai dari pencurian *cookie* sesi administrator untuk mengambil alih kontrol penuh atas website, hingga injeksi formulir login palsu (*credential harvesting*) yang dirancang untuk mencuri nama pengguna dan kata sandi dari pengunjung yang tidak menaruh curiga. Serangan ini sangat efektif karena dilancarkan dari domain yang dipercaya oleh korban.
2. VULN-02 (Komponen Usang): Kegagalan Higienitas Siber Fundamental: Identifikasi komponen CMS dan *plugin* yang usang pada VULN-02 menyoroti kegagalan dalam praktik paling dasar dari keamanan siber: manajemen tambalan (*patch management*). Kerentanan ini bukan sekadar sebuah celah tunggal, melainkan sebuah permukaan serangan (*attack surface*) yang terus meluas seiring waktu, di mana setiap kerentanan baru yang diungkapkan (CVEs) untuk versi perangkat lunak tersebut secara otomatis menambah daftar metode eksploitasi yang dapat digunakan penyerang. Ini secara efektif menurunkan standar keahlian yang dibutuhkan untuk membobol situs; penyerang tidak lagi memerlukan keahlian mendalam, melainkan cukup menggunakan alat pemindai dan eksploitasi otomatis yang tersedia secara publik. Kegagalan untuk memperbarui komponen secara berkala

mencerminkan kurangnya siklus hidup manajemen keamanan yang terstruktur dan menjadikan website sebagai target "*low-hanging fruit*" bagi penyerang.

Analisis Rantai Serangan (Attack Chain Analysis): Risiko sebenarnya muncul dari sinergi destruktif antara VULN-01 dan VULN-02. Seorang penyerang dapat memulai aksinya dengan mengeksploitasi kerentanan yang telah diketahui publik pada CMS usang (VULN-02) untuk mendapatkan akses awal tingkat rendah. Dari pijakan ini, mereka dapat bergerak secara lateral di dalam sistem untuk mengidentifikasi titik lemah di mana mereka bisa menyuntikkan *payload Stored XSS* (VULN-01) yang lebih canggih. *Payload* ini kemudian berfungsi sebagai "ranjau" pasif yang menunggu akun dengan hak istimewa (administrator) untuk mengunjungi halaman tersebut, yang kemudian akan memicu eskalasi hak istimewa (*privilege escalation*) dan memberikan kontrol penuh kepada penyerang.

b. Kerentanan Risiko Sedang: Katalisator dan Pengumpul Informasi Intelijen

Tiga kerentanan berisiko sedang berfungsi sebagai katalisator yang mempercepat dan mempermudah eksekusi serangan yang lebih besar. Mereka adalah alat pengumpul intelijen dan titik lemah yang memungkinkan penyerang untuk memetakan target dan merencanakan serangan dengan lebih efektif.

1. VULN-03 (Security Misconfiguration): Pengungkapan informasi sensitif melalui pesan *error* secara efektif mengubah mode serangan dari *black-box* menjadi *grey-box*. Ini memberikan penyerang informasi intelijen berharga mengenai struktur direktori, teknologi *backend*, dan bahkan potongan kode, yang secara drastis mengurangi waktu dan sumber daya yang dibutuhkan untuk memahami cara kerja aplikasi dan menemukan celah lain, sebuah taktik yang dijelaskan dalam manual peretasan aplikasi web [9].
2. VULN-04 dan VULN-05 (*Broken Access & Authentication*): Absennya proteksi *brute-force* (VULN-05) dan kontrol akses yang lemah (VULN-04) secara kolektif menunjukkan kelemahan pada perimeter pertahanan utama aplikasi. Tanpa mekanisme *rate limiting* atau penguncian akun, halaman login administrator menjadi target terbuka untuk serangan tebak kata sandi otomatis. Mengingat prevalensi penggunaan kata sandi yang lemah, keberhasilan serangan ini seringkali hanya masalah waktu. Jika berhasil, penyerang dapat langsung mengeksploitasi kontrol akses yang rusak (VULN-04) untuk mengakses area-area terlarang yang mungkin berisi data sensitif.

Kesimpulan Analitis: Secara holistik, temuan-temuan ini bukan sekadar daftar kelemahan teknis yang terisolasi. Mereka melukiskan gambaran tentang kultur keamanan yang reaktif, di mana fokusnya mungkin lebih pada fungsionalitas daripada ketahanan terhadap ancaman. Interkoneksi antara komponen usang, kesalahan konfigurasi, dan mekanisme autentikasi yang lemah menciptakan ekosistem yang matang untuk dieksploitasi. Hal ini menggarisbawahi argumen bahwa untuk mencapai keamanan siber yang efektif, sebuah organisasi harus mengadopsi pendekatan pertahanan berlapis (*defense-in-depth*), di mana kegagalan pada satu lapisan kontrol dapat ditahan oleh lapisan berikutnya. Intervensi perbaikan yang direkomendasikan harus bersifat komprehensif dan segera untuk mencegah kompromi sistem yang dapat merusak reputasi dan operasional institusi.

3.3 Implikasi Praktis bagi Institusi SMK Muhammadiyah 2 Bontoala Makassar

a. Kerentanan Risiko Tinggi: Titik Rawan Eskalasi Serangan

Temuan ini secara jelas menunjukkan bahwa pendekatan "tunggu-dan-perbaiki" (*wait-and-fix*) terhadap keamanan siber sudah tidak lagi memadai. Institusi pendidikan harus beralih ke paradigma ketahanan siber (*cyber resilience*) yang bersifat proaktif dengan aksi Konkret:

1. Jadwalkan Asesmen Berkala: Institusi harus mengagendakan asesmen kerentanan atau *Penetration Testing* secara rutin (misalnya, setahun sekali atau setiap semester) sebagai bagian dari audit internal. Ini membantu mengidentifikasi celah baru sebelum dieksploitasi.
2. Langganan Informasi Ancaman: Pengelola IT harus secara aktif mengikuti buletin keamanan dari vendor CMS (seperti *WordPress, Joomla*) dan komunitas keamanan siber untuk mendapatkan peringatan dini mengenai kerentanan baru dan cara menambalnya.

b. Pembentukan Tata Kelola Keamanan Digital yang Jelas

Keamanan siber seringkali gagal bukan karena kurangnya teknologi, tetapi karena tidak adanya kepemilikan dan prosedur yang jelas. Tanggung jawab keamanan tidak boleh hanya dibebankan pada satu individu tanpa panduan dengan aksi konret :

1. Tunjuk Penanggung Jawab Keamanan (*Security Point-of-Contact*): Harus ada individu atau tim kecil yang secara resmi ditugaskan untuk bertanggung jawab atas keamanan website dan aset digital lainnya.
2. Buat Prosedur Operasi Standar (POS/SOP): Kembangkan SOP sederhana untuk aktivitas krusial, seperti:
   a) SOP Manajemen Tambalan (*Patch Management*): Menetapkan bahwa semua pembaruan keamanan kritis pada CMS dan *plugin* harus diterapkan dalam waktu maksimal, misalnya, 72 jam setelah dirilis.
   b) SOP Manajemen Akun: Menetapkan kebijakan kata sandi yang kuat (panjang minimal, kompleksitas) dan mewajibkan autentikasi dua faktor (2FA) untuk semua akun administrator.

c) SOP Cadangan Data (*Backup*): Menetapkan frekuensi pencadangan data website (misalnya, harian atau mingguan) dan melakukan uji restorasi secara berkala.

c. Investasi pada Kapasitas Sumber Daya Manusia

Tembok pertahanan terkuat adalah pengguna yang teredukasi. Teknologi secanggih apa pun tidak akan efektif jika pengelolanya tidak memiliki kesadaran keamanan yang memadai dengan aksi Konkret :

1. Pelatihan Kesadaran Keamanan (*Security Awareness Training*): Selenggarakan sesi pelatihan tahunan bagi semua staf yang memiliki akses ke *dashboard* admin website (termasuk guru yang mengunggah konten). Materi harus mencakup cara mengidentifikasi *email phishing*, bahaya mengklik tautan sembarangan, dan pentingnya menjaga kerahasiaan kata sandi.
2. Peningkatan Keahlian Teknis: Alokasikan sumber daya bagi pengelola IT untuk mengikuti kursus atau sertifikasi dasar mengenai keamanan aplikasi web dan praktik pengkodean yang aman (*secure coding*).

d. Keamanan Siber sebagai Investasi, Bukan Biaya

Pimpinan institusi perlu memahami bahwa anggaran yang dialokasikan untuk keamanan siber adalah sebuah investasi untuk melindungi reputasi, operasional, dan kepercayaan publik. Biaya pemulihan dari insiden keamanan (baik dari segi finansial maupun citra) jauh lebih besar daripada biaya pencegahan dengan aksi Konkret:

1. Alokasi Anggaran Keamanan: Sisihkan anggaran tahunan yang spesifik untuk keamanan digital. Anggaran ini dapat digunakan untuk layanan *Penetration Testing*, lisensi *plugin* keamanan premium, biaya pelatihan, atau bahkan untuk menyewa konsultan keamanan jika diperlukan.
2. Integrasikan Risiko Siber dalam Manajemen Risiko Institusi: Risiko siber harus dibahas dalam rapat pimpinan sebagai bagian dari manajemen risiko institusi secara keseluruhan, setara dengan risiko keuangan atau operasional lainnya.

Dengan mengimplementasikan langkah-langkah praktis ini, institusi pendidikan tidak hanya memperbaiki kerentanan yang ada, tetapi juga membangun fondasi keamanan yang kuat dan berkelanjutan untuk masa depan.

3. KESIMPULAN

Penelitian ini dilaksanakan untuk menjawab pertanyaan fundamental mengenai tingkat keamanan website SMK Muhammadiyah 2 Bontoala Makassar melalui asesmen yang sistematis dan terstandarisasi. Berdasarkan analisis mendalam menggunakan kerangka kerja OWASP Top 10 2021 dan metodologi *Penetration Testing*, penelitian ini berhasil mencapai tujuannya dan sampai pada beberapa kesimpulan krusial.

Pertama, disimpulkan bahwa postur keamanan website yang diuji berada pada tingkat yang lemah dan rentan terhadap eksploitasi. Temuan lima kerentanan, dengan dua di antaranya berisiko Tinggi, bukanlah sekadar kelemahan teknis yang terisolasi. Secara kolektif, temuan ini terutama keberadaan komponen usang (A06:2021) dan celah *Stored Cross-Site Scripting* (A03:2021) mengindikasikan adanya kelemahan fundamental dalam praktik tata kelola keamanan digital, khususnya dalam hal manajemen tambalan (*patch management*) dan validasi input. Rantai serangan (*attack chain*) yang dapat terbentuk dari kombinasi kerentanan ini menunjukkan bahwa sistem dapat dikompromikan secara penuh oleh penyerang dengan tingkat keahlian moderat.

Kedua, penelitian ini memberikan kontribusi empiris yang signifikan dengan memvalidasi penerapan standar keamanan siber global (OWASP) dalam konteks institusi pendidikan kejuruan di Indonesia. Hasil penelitian ini berfungsi sebagai studi kasus konkret yang dapat dijadikan cetak biru (*blueprint*) bagi ribuan sekolah lain dengan karakteristik dan keterbatasan sumber daya yang serupa. Ini membuktikan bahwa asesmen keamanan yang terstruktur dapat dilakukan untuk mengidentifikasi risiko secara efektif bahkan sebelum insiden keamanan terjadi.

Terakhir, kesimpulan yang paling strategis adalah bahwa keamanan siber harus dipandang sebagai elemen fundamental dari manajemen risiko institusi, bukan sekadar tugas teknis departemen IT. Dampak dari eksploitasi kerentanan yang ditemukan tidak hanya terbatas pada gangguan teknis, tetapi juga berpotensi menyebabkan kerugian reputasi yang parah, gangguan operasional pada layanan krusial seperti PPDB, serta risiko hukum terkait kebocoran data. Oleh karena itu, penelitian ini merekomendasikan sebuah pergeseran paradigma yang mendesak bagi para pimpinan institusi pendidikan: dari kultur keamanan yang reaktif menuju pendekatan proaktif yang memandang keamanan digital sebagai sebuah investasi strategis untuk melindungi aset, data, dan kepercayaan publik di era digital.

UCAPAN TERIMA KASIH

Penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah memberikan dukungan dan kontribusi dalam penyelesaian penelitian ini. Kami juga menghargai bantuan dan fasilitas yang disediakan oleh Aljiwani, S.Kom sebagai pengelola Lab selama proses pengumpulan data dan eksperimen. Terakhir, ucapan terima kasih juga ditujukan kepada Teman-teman dosen atas masukan yang berharga selama pelaksanaan penelitian hingga penulisan jurnal ini. Dukungan dari rekan-rekan sejawat juga sangat berarti bagi kami.

REFERENSI

[1] OWASP Foundation, "OWASP Top 10:2021 The Ten Most Critical Web Application Security Risks," 2021. [Online]. Available: https://owasp.org/Top10/
[2] A. S. Y. Irawan, A. D. Yudistira, and F. A. Muqtadiroh, "Analisis Kerentanan Keamanan Website Menggunakan Metode Penetration Testing Execution Standard (PTES)," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 8, no. 3, pp. 541-548, Jun. 2021.
[3] R. K. Sari and A. Susanto, "Analisis Kerentanan Website Sekolah Menggunakan Metode OWASP (Studi Kasus: Website SMA/SMK di Kabupaten Sleman)," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 6, no. 5, pp. 545-552, Okt. 2019.
[4] I. Riadi, R. Umar, and D. A. Novitasari, "Analisis Kerentanan Keamanan Web E-Commerce Menggunakan Acunetix Web Vulnerability Scanner dengan Metode OWASP," *Jurnal Sistem Informasi dan Teknik Komputer*, vol. 4, no. 1, pp. 35-42, 2020.
[5] PortSwigger, "Burp Suite Community Edition," 2024. [Online]. Available: https://portswigger.net/burp
[6] OWASP Foundation, "OWASP Zed Attack Proxy (ZAP)," 2024. [Online]. Available: https://www.zaproxy.org/
[7] G. Weidman, Penetration Testing: A Hands-On Introduction to Hacking. San Francisco, CA: No Starch Press, 2014.
[8] F. A. Saputra and D. E. P. K. Putra, "Vulnerability Assessment on University Website Using OWASP ZAP and Nikto," in Proc. 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, 2022, pp. 215-220.
[9] D. Stuttard and M. Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd ed. Indianapolis, IN: Wiley, 2011.
[10] M. Y. H. S., A. H. Kridalaksana, and S. M. S. Nugroho, "Analisis Keamanan Website Terhadap Serangan Cross-site Scripting (XSS) Menggunakan Metode Black Box Testing," Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), vol. 8, no. 2, pp. 157-164, Mei 2019.