Analisis Dan Pengujian Kerentanan Pada Website Kantor Desa Lanta Barat Menggunakan Framework Issaf

Nurfatun[1], Muhammad Amirul Mu'min[2], Dahlan[3]
Universitas Muhammadiyah Bima
[1]nurfatun890@gmail.com, [2]mhamirulmumin@gmail.com, [3]dahlanlanggudu@gmail.com

Diajukan: 27 April 2026 ; Direvisi: 18 Mei 2026; Diterima: 20 Mei 2026

Abstrak

Penelitian ini bertujuan untuk menganalisis tingkat keamanan sistem berbasis website dengan mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Metode yang digunakan meliputi pengujian keamanan menggunakan tiga tools pemindaian port untuk mendeteksi layanan aktif pada server, dan pengujian kerentanan website untuk mengidentifikasi kelemahan sistem. Hasilnya menunjukkan beberapa port terbuka yang mengindikasikan layanan aktif, yang berpotensi menjadi titik masuk bagi penyerang jika tidak dikonfigurasi dengan benar. Lebih lanjut, beberapa kerentanan diidentifikasi dalam website yang terkait dengan konfigurasi keamanan dan hak perlindungan terhadap serangan tertentu. Analisis lebih lanjut juga mengungkapkan informasi dalam header permintaan yang dapat dieksploitasi untuk mengidentifikasi karakteristik sistem. Meskipun tidak ada kerentanan berisiko tinggi yang diidentifikasi. Berdasarkan hasil pengujian, tiga tingkat klasifikasi kerentanan telah diidentifikasi: *high, medium* dan *low*. Dari semua kerentanan yang teridentifikasi, serangan SQL Injection adalah yang paling signifikan dan memerlukan perhatian khusus karena potensinya membahayakan keamanan data dan mengganggu keberlangsungan website. Oleh karena itu, tindakan perbaikan dan pengamanan segera diperlukan untuk meminimalkan risiko serangan dan meningkatkan keamanan sistem situs web.

Kata kunci: *Keamanan Website, pengujian kerentanan, pemindaian port, analisis keamanan.*

Abstract

This study aims to analyze the security level of a web-based system by identifying potential vulnerabilities that could be exploited by malicious parties. The methods used included security testing using three port scanning tools to detect active services on the server, and website vulnerability testing to identify system weaknesses. The results revealed several open ports indicating active services, which could potentially become entry points for attackers if not configured properly. Furthermore, several vulnerabilities were identified in the web application related to security configuration and protection rights against certain attacks. Further analysis also revealed information in request headers that could be exploited to identify system characteristics. Although no high-risk vulnerabilities were identified, the results of this study confirm that the system still has security gaps that need to be addressed to improve protection against potential future attacks.

Keywords*: Website security, vulnerability testing, port scanning, security analysis.*

1. Pendahuluan

Saat ini, teknologi informasi telah menjadi bagian penting dari berbagai sektor seperti pemerintahan, pendidikan, kesehatan, ekonomi, dan pelayanan publik [1]. Penggunaan situs website sebagai media untuk layanan online dan manajemen data memberikan akses mudah ke informasi, tetapi juga meningkatkan risiko ancaman keamanan dan privasi pengguna. Berbagai laporan menunjukkan bahwa serangan terhadap situs website semakin kompleks, terutama pada sistem yang menyimpan data penting dan sensitif [2]. Di Indonesia, Badan Siber dan Kriptografi Nasional mencatat lebih dari 370 juta upaya serangan siber pada tahun 2024, dengan sebagian besar menargetkan situs website pemerintah daerah [3]. Selain itu, Kementerian Komunikasi dan Informatika melaporkan bahwa banyak situs website pemerintah desa masih memiliki sistem keamanan yang lemah [4].

Situs website Kantor Desa Lanta Barat belum pernah menjalani pengujian keamanan komprehensif, sehingga tingkat kerentanannya tidak diketahui dan berpotensi menimbulkan risiko seperti

kebocoran data, gangguan layanan, dan akses tidak sah [5]. Hal ini diperkuat oleh insiden gangguan layanan pada tahun 2021, yang mengindikasikan masalah ketersediaan sistem. Oleh karena itu, diperlukan analisis keamanan yang sistematis dan terukur untuk mengidentifikasi kelemahan dan mengembangkan langkah-langkah mitigasi yang tepat.

Penelitian ini menggunakan pendekatan Kerangka Kerja ISSAF yang mengacu pada pengujian standar keamanan seperti Panduan Pengujian OWASP dan NIST SP 800-115 [6]. Proses penilaian kerentanan dilakukan dengan menggunakan tiga tools utama, yaitu Nmap, OWASP ZAP, dan Burp Suite, yang masing-masing berfungsi untuk Pemindaian port, pengujian keamanan, dan analisis website, [7][8]. Penggunaan tiga tools tersebut merupakan perbedaan antara penelitian ini dengan penelitian sebelumnya yang umumnya hanya menggunakan satu atau dua tools dalam pengujian, Selain itu objek penelitian yang berfokus pada situs website Kantor Desa Lanta Barat yang masih jarang di analisis keamanannya, sehingga Memberikan kontribusi baru terhadap implementasi ISSAF di lingkungan pemerintah desa [9].

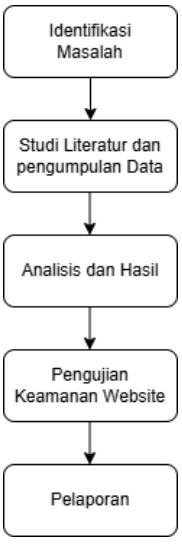
Penelitian ini berkontribusi dalam memberikan analisis terstruktur mengenai tingkat dan karakteristik kerentanan pada situs website Kantor Desa Lanta Barat serta menyusun rekomendasi teknis berdasarkan standar keamanan informasi. Hasil penelitian diharapkan dapat meningkatkan keamanan sistem, meminimalkan risiko gangguan layanan dan berfungsi sebagai referensi untuk penelitian lebih lanjut di bidang keamanan situs website.

2. Metode Penelitian

Dalam penelitian ini, menggunakan penelitian deskriptif eksperimental dengan pendekatan *security assessment study*,Pendekatan ini dipilih karena penelitian berfokus pada pengujian, identifikasi dan analisis. Penelitian dilakukan dengan melakukan pengujian secara langsung terhadap sistem untuk mengetahui tinggkat kemanan Website serta potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertangung jawab. Website Kantor Desa Lanta Barat Kecamatan Lambu ditetapkan sebagai objek penelitian karena berperan sebagai platform layanan yang menyediakan informasi dan akses administratif bagi masyarakat. Website tersebut digunakan untuk menyediakan berbagai layanan digital, seperti penyampaian informasi desa, pengumuman, dokumentasi kegiatan, serta akses layanan administratif masyarakat. Namun, hingga saat ini belum terdapat evaluasi keamanan dan analisisi yang dilakukan secara sistematis, sehingga tingkat keamnan website terhadap ancaman siber belum dapa dipastikan. Objek penelitian berlokasi di Desa Lanta Barat, Kecamatan Lambu, Kabupaten Bima. Dalam proses pengujian keamanan, penelitian ini menggunakan framework ISSAF (Information System Security Assesment Framework) dengan tahapan informasi gathering, Vulnerability Identification, penetration Attempt, dan Reporting. Adapun tools yang digunakan dalam penelitian ini meliputi Nmap untuk identifikasi port dan layanan yang aktif, OWASP ZAP untuk melakukan scanning kerentanan, dan Burp Suite untuk menganalisis lalu lintas HTTP dan identifikasi potensi kelemahan keamanan pada website.

2.1. Alur Penelitian

Pada penelitian ini, tahapan disusun secara berurutan mulai dari identifikasi masalah hingga penyusunan rekomendasi.

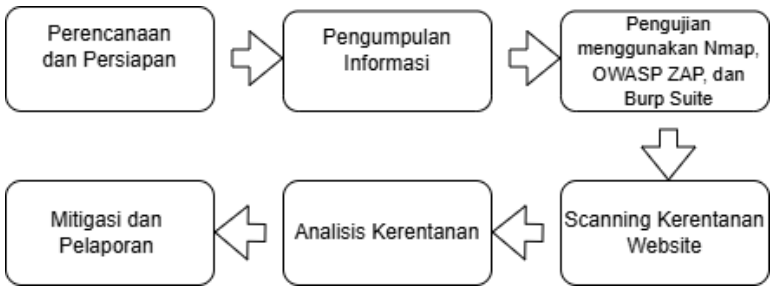


Gambar 1. Bagan Alur Penelitian

Gambar 1. Merupakan alur penelitian yang menjelaskan tahapan-tahapan yang dilalui secara sistematis, mulai dari proses identifikasi masalah, pengumpulan data, pemilihan framework, pengujian keamanan, hingga penyusunan rekomendasi berdasarkan hasil analisis.

2.2. Tahap Pengujian ISSAF

Pada penelitian ini, proses analisis dan pengujian keamanan website Kantor Desa Lanta Barat dilakukan menggunakan framework ISSAF (Information System Security Assesment Framework). Tahapan pengujian meliputi perencanaan dan persiapan, pengumpulan informasi, pemindaian sistem menggunakan Nmap untuk mengidentifkasi port dan layanan yang aktif, Vulnerability Identification menggunakan OWASP ZAP untuk mendeteksi kerentanan, serta penetration Attempt dan analisis menggunakan Burp Suite untuk menganalisis lalu lintas HTTP dan potensi kelemahan keamanan sistem. Hasil pengujian kemudian digunakan sebagai dasar dalam penyusunan rekomendasi mitigasi keamanan.

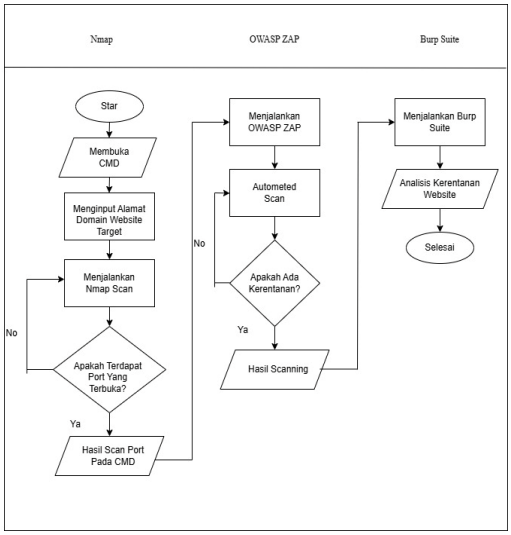


Gambar 2. Tahap Penggujian ISSAF

Gambar 2.2 menunjukkan metodologi pengujian keamanan situs website, dimulai dengan tahap perencanaan dan persiapan, diikuti dengan pengumpulan informasi tentang sistem target. Selanjutnya, pengujian dilakukan menggunakan Nmap, OWASP ZAP, dan Burp Suite untuk mengidentifikasi kerentanan keamanan. Pemindaian dan analisis kerentanan kemudian dilakukan berdasarkan tingkat risiko. Tahap terakhir adalah mitigasi dan pelaporan, termasuk rekomendasi untuk perbaikan dan dokumentasi hasil pengujian.

2.3. Flowchart Tahap Pengujian Nmap, OWASP ZAP, Burp Suite

Dalam penelitian ini, analisis kerentanan terhadap situs website Kantor Desa Lanta Barat dilakukan dengan menggunakan kerangka kerja ISSAF sebagai panduan pengujian yaitu *Information Gathering*, *Vulnerability Identification*, *Penetration Attempt*, dan *Reporting*. Pada tahap *Information Gathering* dilakukan pengumpulan informasi terkait target. Proses pengujian menggunakan Nmap untuk pengumpulan informasi jaringan, OWASP ZAP untuk pemindaian kerentanan, dan Burp Suite untuk analisis dan validasi temuan. Proses pengujian disajikan dalam bentuk flowchart.



Gambar 3. Flowchart Tahap Pengujian Menggunakan Nmap, OWASP ZAP dan Burp Suite.

Pada Gambar 2.3 mengilustrasikan proses pengujian keamanan situs website menggunakan tiga tools utama yaitu Nmap, OWASP ZAP, dan Burp Suite, yang dilakukan secara bertahap dan saling melengkapi. Proses dimulai dengan Nmap menggunakan Command Prompt untuk memasukkan URL target dan menjalankan perintah pemindaian untuk mengidentifikasi port terbuka sebagai indikasi awal potensi kerentanan keamanan. Selanjutnya, OWASP ZAP digunakan untuk melakukan pemindaian otomatis situs website, yang kemudian dievaluasi untuk menentukan ada atau tidaknya kerentanan, menghasilkan laporan pemindaian yang lebih detail. Tahap terakhir dilakukan menggunakan Burp Suite, yang berfokus pada analisis yang lebih mendalam terhadap kerentanan situs website yang telah diidentifikasi sebelumnya.

2.4. Alat dan Bahan Penelitian

Dalam pelaksanaan penelitian ini, diperluhkan sejumlah alat dan bahan yang berfungsi sebagai pendukung utama dalam proses analisis dan pengujian kerentanan pada website Kantor Desa Lanta Barat. Alat dan bahan tersebut digunakan untuk memastikan bahwa seluruh tahapan penelitian, mulai dari pengumpulan data, proses pemindaian, hingga verifikasi digunakan dalam penelitian ini.

Tabel 1. Perangkat Keras (Hadware)

No	Alat dan Bahan	Jenis	Fungsi Dalam Penelitian
1	Laptop	Perangkat Keras	Digunakan untuk menjalankan tools keamanan, melakukan analisis, dan menyusun laporan penelitian.
2	Mouse dan Flashdisk	Perangkat Pendukung	Mengakses website Kantor Desa Lanta serta menjalankan proses pemindaian secara online.

Tabel 2. Perangkat Lunak (Sofware)

No	Alat dan Bahan	Jenis	Fungsi dan Penelitian
1	Sistem Operasi (Windows)	Perangkat Lunak	Menjadi platform untuk menjalankan Owasp Zap dan sofware pendukung lainnya.
2	Nmap, Owasp Zap, dan Burp Suite	Perangkat Lunak	Tools utama untuk melakukkan Scanning kerentanan dan menganalisis keamanan website.
3	Web Browser (Crome/Mozilla)	Perangkat Lunak	Digunakan untuk observasi manual. Inpeksi elemen dan verifikasi hasil pemindaian.

3. Hasil dan Pembahasan

Bab ini menyajikan hasil dan diskusi pengujian keamanan pada situs website Kantor Desa Lanta Barat. Pengujian dilakukan untuk mengidentifikasi potensi kerentanan sebagai bentuk evaluasi tingkat keamanan sistem [10]. Proses pengujian mengacu pada Informasi System Security Assessment Framework (ISSAF), yang berfungsi sebagai pedoman dalam penentuan target, proses pemindaian, serta anal isis hasil pengujian. [11].

Penelitian ini menggunakan tiga tools utama, yaitu Nmap, OWASP ZAP, dan Burp Suite. Nmap digunakan untuk mengidentifikasi port dan layanan aktif pada server, OWASP ZAP untuk mendeteksi kerentanan secara otomatis, dan Burp Suite untuk menganalisis komunikasi antara klien dan server [12]. Hasil pengujian disajikan dalam bentuk tabel dan gambar agar mudah dipahami, kemudian dianalisis berdasarkan tingkat risiko dan dampaknya. Pembahasan disusun dalam beberapa subbab, yang mencakup hasil pengujian untuk setiap tools dan rekomendasi mitigasi sesuai dengan kerangka kerja ISSAF.

3.1. Tahap Pengujian Sistem Menggunakan Nmap, OWASP ZAP dan Burp Suite

Tahap pengujian keamanan dilakukan secara sistematis menggunakan kerangka kerja ISSAF. Proses dimulai dengan tahap perencanaan dan diakhiri dengan pengumpulan informasi target menggunakan metode WHOIS untuk memperoleh data terkait domain dan server yang digunakan. Selain itu, beberapa tools yang digunakan untuk menyelesaikan proses pemindaian, yaitu Nmap untuk mengidentifikasi port dan layanan aktif, OWASP ZAP untuk menemukan kerentanan secara otomatis, dan Burp Suite untuk memeriksa komunikasi antara klien dan server. Tujuan dari tahapan ini adalah untuk memperoleh gambaran awal mengenai potensi celah keamanan pada sistem yang diuji.

Gambar 4. Hasil Pengumpulan Informasi Menggunakan Whois

Pada Gambar 3.1 menunjukkan hasil identifikasi domain WHOIS, yang menunjukkan bahwa domain menggunakan layanan DNS Cloudflare dengan name server chuck.ns.cloudflare.com dan sandra.ns.cloudflare.com. Status domain tercatat aktif (ok), menunjukkan bahwa domain dalam kondisi operasional. Selain itu, karena DNSSEC masih belum diaktifkan, ini merupakan salah satu elemen yang dapat diperhatikan dalam peningkatan keamanan domain.

3.2. Hasil dan Analisis

Berdasarkan hasil pengujian dengan menggunakan tiga tools yaitu, Nmap, OWASP ZAP, dan Burp Suite, menunjukan bahwa ada ancaman yang mungkin terjadi pada sistem.

Tabel 3. Hasil Analisis Menggunakan Nmap

Port	Service	Status	Analisis Risiko
21	FTP	Open	Layanan FTP transfer file aktif, potensi menimbulkan risiko kebocoran data apabila menggunakan autentifikasi tanpa enkripsi.
22	SSH	Open	Layanan remote login server terdeteksi dan relatif aman apabila menggunakan konfigurasi autentifikasi yang kuat serta pembatas akses.
23	Telnet	Open	Layanan Telnet memiliki risiko tinggi karena komunikasi dilakukan tanpa enkripsi sehingga data login dapat disadap oleh penyerang.
25	SMTP	Open	Port SMTP diperlukan untuk layanan email, namun dapat dimanfaatkan untuk spam atau mail abuse apabila tidak dikonfigurasi dengan baik.
53	DNS	Open	Layanan DNS diperluhkan untuk resolusi nama domain, tetapi dapat menjadi target serangan DNS amplification apabila konfigurasi lemah.

Hasil pengujian Menggunakan *Nmap* menunjukkan bahwa lima port berada dalam status terbuka (open). Port-port ini adalah 21, 22, 23, 25, dan 53. Port-port ini memungkinkan layanan FTP, SSH, Telnet, SMTP, dan DNS. Sementara layanan yang aktif ini menunjukkan bahwa sistem menyediakan beberapa layanan jaringan penting, itu juga dapat menjadi titik masuk serangan jika tidak dikonfigurasi dengan baik. Akibatnya, pengamanan seperti enkripsi akses, serta penonaktifan layanan yang tidak digunakan.

Tabel 4. Hasil Analisis Menggunakan OWASP ZAP

Level Risiko	Jumlah	Presentase
High	1	5%
Medium	5	25%
Low	8	40%
Information	6	30%
Total	20	100%

Berdasarkan hasil pengujian menggunakan OWASP ZAP, ada 20 kerentanan diidentifikasi, yang terbagi menjadi empat tingkat risiko: Tinggi (5%), Sedang (25%), Rendah (40%), dan Informasi (30%). Hasil ini menunjukkan bahwa sebagian besar temuan termasuk dalam kategori Rendah dan Informasi, sehingga memiliki dampak yang relatif rendah pada sistem. Namun, keberadaan kerentanan pada tingkat Tinggi tetap menjadi perhatian karena berpotensi berdampak signifikan pada keamanan sistem. Oleh karena itu, diperlukan langkah-langkah mitigasi, terutama untuk kerentanan dengan tingkat risiko tinggi dan sedang, untuk meningkatkan keamanan sistem secara keseluruhan.

Tabel 5. Hasil Analisis Menggunakan Burp Suite

Temuan	Deskripsi	Level Risiko
Information Disclosure (User-Agent)	Header menampilkan informasi browser dan sistem client yang digunakan saat melakukan akses ke website. Informasi tersebut dapat dimanfaatkan oleh penyerang untuk melakukan proses fingerprinting dan menentukan jenis serangan yang sesuai terhadap target sistem.	Low / Information

Pada pengujian menggunakan Burp Suite dilakukan dengan metode intercept request dan response HTTP untuk menganalisis header, cookie, dan parameter komunikasi antara client dan server. Hasil analisis menunjukkan adanya informasi pada header HTTP berupa User-Agent disclosure yang dapat digunakan unttuk proses identifikasi sistem oleh penyerang. Meskipun termasuk kategori risiko rendah, informasi tersebut tetap berpotensi membantu penyerang dalam menentukan metode serangan yang lebih spesifik terhdap sistem target.

3.3. Mitigasi Kerentanan

Hasil pengujian menunjukan adanya beberapa kerentan yang memerluhkan penanganan lebih lanjut. Oleh karena itu, rekomendasi mitigasi disusun untuk meminimalkan risioko keamanan. Rincian mitigasi disajikan pada tabel berikut.

Tabel 6. Mitigasi Berdasarkan Port yang Terbuka

Tools	Port	Status	Layanan	Deskripsi	Dampak	Mitigasi
Nmap	21	Open	FTP (File Tranfer Protocol)	FTP digunakan untuk tranfer file antara clien dan server, namun tidak menggunakan enkripsi.	Data yang dikirim (Username &Passwoard) dapat disadap (Sniffing) olehAttacker.	Gunakan SFTP atau FTPS, nonaktifkan FTP jika tidak diperlukan, dan batasi akses dengan firewall.
	22	Open	SSH (Secure Shell)	SSH digunakan untuk akses remote server secara aman dengan enkripsi.	Jika konfigurasi lemah (Passwoard mudah), rentan terhadap brute force attack.	Gunakan key-based authentication, ganti port default, dan batasi akses IP.
	23	Open	Telnet	Telnet digunakan untuk remote access, tetapi tidaak terenskripsi.	Data login dapat disadap dengan mudah sehingga berisiko tinggi terhadap pencurian kredensial.	Nonaktifkan telnet dan ganti dengan SSH yang lebih aman.
	25	Open	SMTP (Simple mail transfer protocol).	SMTP digunakan untuk pengiriman email antar server.	Dapat disalah gunakan untuk spam, emailspoofing, atau serangan phishing.	Gunakan SMTP authentication, aktifkan filtering spam, dan batasi akses server.
	53	Open	DNS (Domain Name System)	DNS digunakan untuk menerjemahkan nama domain menjadi alamat IP.	Rentan terhadap DNS spoofing, cache poisoning, atau DDoS attack.	Gunakan DNSSEC, batasi query eksternal, dan konfigurasi firewall dengan bbenar.

Tabel 7. Mitigasi Berdasarkan Alert Kerentanan

Tools	Alert	Deskripsi	Dampak	Mitigasi
OWASP ZAP	A01- Absence of Anti-CRF Tokens	CSR terutama digunakan untuk melakukan tindakan terhadap situs target menggunakan hak akses korban, tetapi teknis terbaru telah ditemukan untuk membocorkan informasi dengan memanfaatkan akses ke respons. Risiko kebocoran informasi meningkat secara dramatis ketika situs target rentan terhadap *XSS*, karena *XSS* dapat digunakan sebagai *platform* untuk beroperasi dalam batasan kebijakan.	Kerentanan ini memunggkinkan penyerang melakukan aksi tanpa izin atas nama pengguna, yang berpotensi menyebabkan pennyalahgunaan akun, perubahan data tidak sah, serta kebocoran informasi sensitif.	Dengan menerapkan anti-CSRF (Nonce) pada setiap permintaan, menggunakan *Framework* atau *library* yang aman, menghindari penggunaan metode *GET* untuk perubahan data, serta memastikan aplikasi bebas dari kerentanan *XSS*.
	A03- SQL Injection-SQLite (Time Based)	SQL Injection merupakan kerentanan yang terjadi ketika input pengguna tidak divalidasi dengan baik sehingga memungkinkan penyerang menyisipkan perintah SQL berbahaya ke dalam query yang dijalankan oleh sistem.	Kerentanan ini dapat menyebabkan akses tidak sah ke basis data, kebocoran dan manipulasi data, serta potensi pengambilalihan sistem oleh penyerang.	Dengan menggunakan pernyataan yang telah disiapkan, validasi input pada sisi server, dan penerapan prinsip batas hak akses pada basis data.
	A05- Content Security Policy (CSP) Header Not Set	Content Security Policy (CSP) adalah lapisan keamanan tambahan yang membantu mendeteksi dan mengurangi jenis serangan tertentu, termasuk Cross Site Scripting (XSS) dan serangan injeksi data. Serangan ini digunakan untuk berbagai hal, mulai dari pencurian data hingga perusakan situs atau penyebaran malware. CSP menyediakan serangkaian header HTTP standar yang memungkinkan pemilik situs web untuk menyatakan sumber konten yang disetujui yang boleh dimuat oleh browser di halaman tersebut — jenis yang tercakup adalah JavaScript, CSS, frame HTML, font, gambar, dan objek yang dapat disematkan seperti applet Java, ActiveX, file audio, dan video.	Serangan seperti Cross-Site Scripting (XSS) dan injeksi data dapat terjadi jika peningkatan peraturan keamanan konten (CSP) tidak diterapkan. Serangan ini dapat menyebabkan pencurian data sensitif, manipulasi tampilan situs (defacement), dan penyebaran malware kepada pengguna.	Pastikan server web, server aplikasi, load balancer, dll. Anda dikonfigurasi untuk mengatur header Content-Security-Policy.

	A05- Cross-Domain Misconfiguration	Pengumpulan data melalui peramban web mungkin terjadi karena kesalahan konfigurasi Cross Origin Resource Sharing (CORS) pada server web.	Kesalahan konfigurasi Cross-Origin Resource Sharing (CORS) dapat memungkinkan akses tidak sah terhadap data dari domain lain, memungkinkan penyerang membaca atau mencuri data sensitif melalui browser pengguna. Hal ini dapat menyebabkan pelanggaran kerahasiaan data dan enkripsi sumber daya aplikasi.	Pastikan data sensitif tidak tersedia dengan cara yang tidak terautentikasi (misalnya, menggunakan daftar putih alamat IP). Konfigurasikan header HTTP "Access-Control-Allow-Origin" ke kumpulan domain yang lebih ketat, atau hapus semua header CORS sepenuhnya, untuk memungkinkan browser web menerapkan Kebijakan Asal yang Sama (SOP) dengan cara yang lebih ketat.
	A05- Missing Anti-clickjacking Header	Respons tersebut tidak melindungi dari serangan 'ClickJacking'. Respons tersebut harus menyertakan Content-Security-Policy dengan arahan 'frame-ancestors' atau X-Frame-Options.	Jika tidak ada mekanisme perlindungan terhadap clickjacking, penyerang dapat menipu pengguna untuk melakukan sesuatu tanpa mereka sadari melalui tindakan antarmuka, seperti mengklik tombol atau tautan tersembunyi. Hal ini dapat menyebabkan tindakan ilegal seperti pencurian data, perubahan konfigurasi akun, atau transaksi tanpa izin pengguna.	Browser web modern mendukung header HTTP Content-Security-Policy dan X-Frame-Options. Pastikan salah satunya diatur pada semua halaman web yang dikembalikan oleh situs/aplikasi Anda. Jika Anda mengharapkan halaman tersebut hanya dibingkai oleh halaman di server Anda (misalnya, halaman tersebut merupakan bagian dari FRAMESET), maka Anda perlu menggunakan SAMEORIGIN, jika tidak, jika Anda tidak pernah mengharapkan halaman tersebut dibingkai, Anda harus menggunakan DENY. Atau, pertimbangkan untuk menerapkan arahan "frame-ancestors" dari Content Security Policy.
	A05- Server Leaks Version Information	Server web/aplikasi membocorkan informasi versi melalui header respons HTTP "Server". Akses ke informasi tersebut dapat mempermudah penyerang mengidentifikasi kerentanan lain yang mungkin dialami server web/aplikasi Anda.	Ketika informasi versi server bocor, penyerang dapat dengan mudah mengetahui jenis dan versi perangkat lunak yang digunakan, yang memungkinkan mereka untuk mengeksploitasi kerentanan tertentu terhadap versi tersebut, yang dapat meningkatkan kemungkinan sistem serangan yang lebih terarah dan efektif.	Pastikan server web, server aplikasi, load balancer, dll. Anda dikonfigurasi untuk menekan header "Server" atau memberikan detail umum.
	A05- Strict-Transport-Security Header Not Set	HTTP Strict Transport Security (HSTS) adalah mekanisme kebijakan keamanan web di mana server web menyatakan bahwa agen pengguna yang patuh (seperti peramban web) hanya boleh berinteraksi dengannya menggunakan koneksi HTTPS yang aman (yaitu HTTP yang dilapisi di atas	Jika HTTP Strict Transport Security (HSTS) tidak diterapkan, komunikasi antara klien dan server akan dilakukan melalui protokol HTTP yang tidak aman, yang meningkatkan risiko serangan Man-in-the-Middle (MITM). Hal ini dapat menyebabkan penyadapan, manipulasi, dan pencurian data pribadi selama transmisi.	Pastikan server web, server aplikasi, load balancer, dll. Anda dikonfigurasi untuk menerapkan Strict-Transport-Security.

		TLS/SSL). HSTS adalah protokol standar IETF dan ditentukan dalam RFC 6797.		
	A05- X-Content-Type-Options Header Missing	Header Anti-MIME-Sniffing X-Content-Type-Options tidak diatur ke 'nosniff'. Hal ini memungkinkan versi Internet Explorer dan Chrome yang lebih lama untuk melakukan MIME-sniffing pada isi respons, yang berpotensi menyebabkan isi respons diinterpretasikan dan ditampilkan sebagai tipe konten selain tipe konten yang dideklarasikan. Versi Firefox saat ini (awal 2014) dan versi lama akan menggunakan tipe konten yang dideklarasikan (jika ada yang diatur), daripada melakukan MIME-sniffing.	Jika header X-Content-Type-Options tidak digunakan, browser dapat melakukan sniffing MIME, yang mengakibatkan pemrosesan konten sebagai tipe yang berbeda dari yang seharusnya. Hal ini dapat menyebabkan eksekusi konten berbahaya seperti skrip yang disisipkan. Serangan seperti Cross-Site Scripting (XSS) dapat berguna.	Pastikan bahwa aplikasi/server web mengatur header Content-Type dengan tepat, dan bahwa ia mengatur header X-Content-Type-Options ke 'nosniff' untuk semua halaman web. Jika memungkinkan, pastikan pengguna akhir menggunakan browser web modern dan sesuai standar yang sama sekali tidak melakukan MIME-sniffing, atau yang dapat diarahkan oleh aplikasi web/server web untuk tidak melakukan MIME-sniffing.
	A06- Vulnerable JS Library	Pustaka yang diidentifikasi tampaknya rentan.	Penggunaan arsip yang memiliki kerentanan dapat memberi kesempatan penyerang untuk menggunakan celah keamanan yang telah diketahui, yang dapat menyebabkan akses ilegal, eksekusi kode berbahaya, dan kompromi terhadap sistem dan data pengguna.	Perbarui ke versi terbaru dari pustaka yang bermasalah.
	A08- Cross-Domain JavaScript Inclusion	Halaman ini menyertakan satu atau lebih file skrip dari domain pihak ketiga.	Penggunaan file script dari domain pihak ketiga dapat meningkatkan risiko keamanan jika sumbernya tidak terpercaya atau telah dikompromikan. Penyerang dapat memasukkan kode berbahaya ke dalam sistem klien, yang dapat mencuri data, mengubah konten, atau menyebarkan malware kepada pengguna.	Pastikan file sumber JavaScript hanya dimuat dari sumber tepercaya, dan sumber tersebut tidak dapat dikendalikan oleh pengguna akhir aplikasi.

Tabel 4.6 Mitigasi Berdasarkan Analisis HTTP Request

Tools	Temuan	Deskripsi	Dampak	Mitigasi
Burp Suite	Information Disclosure (User-Agent)	Header menampilkan informasi browser.	Dapat digunakan untuk figerprinting.	Membatasi informasi header.

4. Kesimpulan

Berdasarkan hasil pengujian keamanan website Kantor Desa Lanta Barat menggunakan Nmap, OWASP ZAP, dan Burp Suite, ditemukan beberapa kerentanan dengan tingkat risiko High, Medium, dan Low yang berkaitan dengan konfigurasi keamanan server, layanan pada port terbuka, serta kelemahan pada konfigurasi keamanan website. Hasil Pengujian menunjukkan bahwa port yang terbuka tanpa pengamanan yang memandai potensi dimanfaatkan oleh pihak yang tidak bertangung jawab sebagai titik masuk serangan. Selain itu, hasil pemindaian menggunakan OWASP ZAP mengidentifikasi beberapa kelemahan

keamanan website, seperti kurangnya konfigurasi header keamanan dan potensi kerentanan yang dapat untuk menyerang sistem. Pengujian menggunakan Burp Suite juga menunjukkan adanya informasi pada headerHTTP, seperti User-Agent disclosure, yang dapat membantu penyerang dalam menngidentifikasi sistem target dan menentukan jenis serangan yang sesuai. Berdasarkan hasil tersebut, mitigasi yang perlu segera dilakukan adalah menutup port yang tidak digunakan, memperkuat konfigurasi kemanan server, menerapkan firewall memperbarui sistem dan layanan secara berkala, serta membattasi informasi yang ditampilkan pada header HTTP. Selain itu, penerapan security header, validasi input pengguna, dan monitoring keamanan secara berkala juga perlu dilakukan untuk meminimalkan potensi serangan dan mencegah terjadinya eksploitasi kerentanan pada website.

Secara keseluruhan, meskipun tidak ada kerentanan kritis yang teridentifikasi, website masih memiliki beberapa kelemahan keamanan yang perluh segera ditangani guna menjaga kerahasiaan, integritas, dan ketersediaan layanan website. Penelitian selanjutnya dapat berfokus pada implementasi mitigasi yang direkomendasikan dan melakukan pengujian lebih lanjut untuk menentukan efektivitas peningkatan keamanan tersebut.

Daftar Pustaka

[1] D. Julianti, "Strategi Kebijakan Penguatan Pelayanan Publik Dan Pengawasan Perizinan Berusaha Dengan Aplikasi Berbasis Teknologi Informasi," *Kybernology J. Ilmu Pemerintah. dan Adm. Publik*, vol. 2, no. 2, pp. 324–363, 2024, doi: 10.71128/kybernology.v2i2.131.

[2] A. E. Prayogi, F. G. Permana, G. N. Ardhana, and ..., "Waspada Terhadap Aplikasi Atau Website Berbahaya Yang Mengatasnamakan Instansi Tertentu Untuk Mengambil Data Pribadi," *J. INDIMAS Indones. Mengabdi Kpd. Masy.*, vol. 1, no. 2, pp. 40–44, 2023, [Online]. Available: http://jurnal.publikasitecno.id/index.php/indimas/article/view/129%0Ahttps://jurnal.publikasitecno.id/index.php/indimas/article/download/129/67

[3] B. A. Darumaya, S. Maarif, T. Toruan, Y. Swastanto, P. Doktoral, and F. Strategi, "Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan Thoughts on the Potential Threat of Cyber War in Indonesia: a Defense Strategy Study," *J. Keamanan Nas.*, vol. 9, no. 2, pp. 299–324, 2023, [Online]. Available: https://ejurnal.ubharajaya.ac.id/index.php/kamnas

[4] S. D. Hilda, N. Heryana, and A. A. Ridha, "Website Security Analysis Curug Village Government Using Open Web Application Security Project (Owasp)," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 3S1, 2024, doi: 10.23960/jitet.v12i3s1.5236.

[5] M. Fatkhullah, M. A. F. Habib, and K. K. Nisa, "Identifikasi dan Manajemen Risiko untuk Mereduksi Kerentanan Pada Masyarakat," *Ekon. Keuangan, Investasi dan Syariah*, vol. 3, no. 4, pp. 856–867, 2022, doi: 10.47065/ekuitas.v3i4.1529.

[6] M. Kusuma, D. Hariyadi, H. Kurniawan, and F. F. F. Muttaqin, "Pengujian sistem keamanan wireless router pada ekosistem rumah cerdas berbasis NIST sp800-115," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 4, no. 3, pp. 645–650, 2023, doi: 10.37859/coscitech.v4i3.6315.

[7] N. A. Widiyono and U. Y. Oktiawati, "Implementasi Web Application Firewall (WAF) pada Aplikasi Fishku Berbasis Google Cloud Armor," *J. Internet Softw. Eng.*, vol. 5, no. 2, pp. 75–85, 2024, doi: 10.22146/jise.v5i2.9980.

[8] F. Septarita and W. Anggraini, "Analisis Kerentanan Website Prodi Teknologi Informasi Ubb Menggunakan Metode Application Scanning," *J. Comput. Technol.*, vol. 3, no. 1, pp. 26–38, 2025, [Online]. Available: https://doi.org/10.69916/comtechno.v3i1.333

[9] D. Sudirman and Akma Nurul Yaqin, "Network Penetration dan Security Audit Menggunakan Nmap," *SATIN - Sains dan Teknol. Inf.*, vol. 7, no. 1, pp. 32–44, 2021, doi: 10.33372/stn.v7i1.702.

[10] R. Saputra, D. Abdullah, M. Daud, and F. R. Maulana, "Analisis Assesment Vulnerability pada Website dan Aplikasi Publik di Dinas Komunikasi Informatika dan Statistik Kota Banda Aceh," *J. Janitra Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 87–91, 2024, doi: 10.59395/q6jdk177.

[11] Muhammad Fauzan Rifqi, Oris Krianto Sulaiman, and Aulia Ichsan, "Pemindai Kerentanan Aplikasi Web Dinas Kearsipan Dan Perpustakaan Daerah Kabupaten Semarang Menggunakan Information System Security Assessment Framework (Issaf)," *J. Ris. Multidisiplin Edukasi*, vol. 2, no. 7, pp. 777–792, 2025, doi: 10.71282/jurmie.v2i7.720.

[12] M. Khosiri, Hoiriyah, and Anwari, "Pengujian dan Analisis Kerentanan Keamanan Website Fakultas Teknik Universitas Islam Madura Menggunakan OWASP ZAP, Burp Suite, dan Nikto," vol. 11, no. 1, pp. 10–16, 2025, [Online]. Available: https://ft.uim.ac.id