Jurnal Minfo Polgan (JMP)
Volume 15, Nomor 3, September-Desember 2026
DOI : https://doi.org/10.33395/jmp.v15i3.16615
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Analisis Keamanan Website Ells Amikom Purwokerto Menggunakan Metode *Vulnerability Assesment* Dengan Kerentanan Tingkat Menengah

[1]Isa Nur Fathoni, [2] Mohammad Imron, [3]Darso
[1*,2,3]Sistem Informasi & Informatika, Fakultas Ilmu Komputer
Universitas Amikom Purwokerto, Banyumas, Indonesia
*Korespondensi: isnurfathoni@email.com

Submit : 29 Jun 2026 | **Diterima** : 27 Jul 2026 | **Terbit** : 04 Sept 2026

ABSTRACT

Website security has become an essential aspect of digital service implementation, particularly within higher education institutions. The ELLS (E-Learning System) of AMIKOM Purwokerto serves as an online learning platform that stores various academic information, making the confidentiality, integrity, and availability of its data critical concerns. This study aims to analyze the security level of the ELLS AMIKOM Purwokerto website using the Vulnerability Assessment method. The research was conducted through four main stages: information gathering, vulnerability scanning, result analysis, and remediation. During the information gathering phase, WHOIS, DNS Lookup, Nmap, and WhatWeb were utilized to collect information regarding the domain, IP address, network services, and web technologies employed by the target website. Vulnerability scanning was subsequently performed using OWASP Zed Attack Proxy (OWASP ZAP) through both passive and active scanning techniques. The findings indicate that no high-risk vulnerabilities were identified. However, the assessment revealed four medium-risk vulnerabilities, five low-risk vulnerabilities, and five informational findings. The medium-risk vulnerabilities consist of Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header, and Subresource Integrity Attribute Missing. Based on these findings, several remediation measures are recommended, including the implementation of Anti-CSRF mechanisms, Content Security Policy (CSP), security headers, Subresource Integrity (SRI), and improvements to server security configurations in accordance with OWASP recommendations. The results demonstrate that the Vulnerability Assessment approach is effective in identifying website security weaknesses and can serve as a foundation for enhancing web application security through continuous evaluation and improvement.

***Keywords**: Vulnerability Assessment, OWASP ZAP, Website Security, Information Gathering, Web Application Security.*

ABSTRAK

Website merupakan salah satu komponen penting dalam penyelenggaraan layanan digital, termasuk pada lingkungan perguruan tinggi. Website ELLS (E-Learning System) AMIKOM Purwokerto digunakan sebagai media pembelajaran daring yang menyimpan berbagai informasi akademik sehingga aspek keamanan menjadi faktor penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Penelitian ini bertujuan untuk menganalisis tingkat keamanan website ELLS AMIKOM Purwokerto menggunakan metode Vulnerability Assessment. Penelitian dilakukan melalui empat tahapan utama, yaitu *information gathering*, *vulnerability scanning*, *result analysis*, dan *remediation*. Tahap *information gathering* memanfaatkan WHOIS, DNS Lookup, Nmap, dan WhatWeb untuk memperoleh informasi mengenai domain, alamat IP, layanan jaringan, serta teknologi yang digunakan oleh website. Selanjutnya dilakukan pemindaian kerentanan menggunakan OWASP Zed Attack Proxy (OWASP ZAP) melalui mekanisme *passive scanning* dan *active scanning*. Hasil penelitian menunjukkan bahwa tidak ditemukan kerentanan dengan tingkat risiko tinggi, namun berhasil diidentifikasi 4 kerentanan tingkat menengah, 5 kerentanan tingkat rendah, serta 5 temuan informasional. Kerentanan tingkat menengah meliputi *Absence of Anti-CSRF Tokens*, *Content Security Policy (CSP) Header Not Set*, *Missing Anti-clickjacking Header*, dan *Sub Resource Integrity Attribute Missing*. Berdasarkan hasil tersebut disusun rekomendasi berupa penerapan mekanisme Anti-CSRF, implementasi *Content Security Policy*, penambahan *security headers*, penerapan *Subresource*

Integrity, serta peningkatan konfigurasi keamanan server sesuai rekomendasi OWASP. Penelitian ini menunjukkan bahwa metode Vulnerability Assessment efektif dalam mengidentifikasi kelemahan konfigurasi keamanan website sehingga dapat menjadi dasar dalam meningkatkan keamanan aplikasi web secara berkelanjutan.

Kata Kunci: Vulnerability Assessment, OWASP ZAP, Website Security, Information Gathering, Web Application Security.

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong berbagai institusi, termasuk perguruan tinggi, untuk memanfaatkan teknologi berbasis web dalam mendukung proses bisnis dan layanan akademik (Fatkhussarifin & Wicaksono, 2025). Website menjadi salah satu media utama dalam menyediakan layanan informasi, administrasi, hingga pembelajaran secara daring(Nugraha et al., 2025). Pemanfaatan website tidak hanya meningkatkan efisiensi pelayanan, tetapi juga mempermudah akses informasi bagi mahasiswa, dosen, maupun tenaga kependidikan(Siddiq et al., 2025). Oleh karena itu, keberadaan website yang memiliki performa dan keamanan yang baik menjadi faktor penting dalam mendukung kualitas layanan institusi pendidikan(Razak, 2020).

Website ELLS (Electronic Learning Systems) AMIKOM Purwokerto merupakan salah satu sistem berbasis web yang digunakan sebagai media pendukung pembelajaran di Universitas AMIKOM Purwokerto. Sistem ini menyediakan layanan autentikasi pengguna, penyampaian materi pembelajaran, serta berbagai aktivitas akademik yang melibatkan data pengguna. Sebagai aplikasi yang diakses melalui jaringan internet, website ELLS berpotensi menjadi sasaran berbagai serangan siber apabila tidak didukung dengan mekanisme keamanan yang memadai. Laman login yang diakses publik setiap hari rentan terhadap ancaman siber seperti SQL Injection, Cross-Site Scripting (XSS), dan phishing yang berisiko memicu kebocoran data sensitif hingga manipulasi nilai. Sehingga diperlukan evaluasi mendalam dan pemetaan risiko guna merumuskan strategi mitigasi demi mewujudkan platform pembelajaran digital yang aman dan stabil (Brito et al., 2022) .

Ancaman keamanan terhadap aplikasi web terus mengalami peningkatan seiring berkembangnya teknologi informasi. Berbagai jenis serangan seperti Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, Clickjacking, hingga kesalahan konfigurasi keamanan (*Security Misconfiguration*) merupakan ancaman yang umum ditemukan pada aplikasi berbasis web(Schagen et al., 2020). Kerentanan tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk memperoleh akses tidak sah, mencuri informasi sensitif, memanipulasi data, maupun mengganggu ketersediaan layanan. Oleh sebab itu, pengujian keamanan secara berkala menjadi langkah penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi (Viega et al., n.d.).

Salah satu metode yang banyak digunakan untuk mengevaluasi keamanan aplikasi web adalah Vulnerability Assessment (VA) . Vulnerability Assessment merupakan proses sistematis yang bertujuan untuk mengidentifikasi, menganalisis, dan mengklasifikasikan potensi kerentanan keamanan pada suatu sistem informasi (Moret, 2021). Tahapan dalam Vulnerability Assessment meliputi proses Network discovery atau Information gathering, identifikasi layanan yang berjalan, pemindaian kerentanan (*vulnerability scanning*), analisis tingkat risiko berdasarkan hasil temuan, serta penyusunan rekomendasi mitigasi sesuai standar keamanan informasi(Mukhopadhyay & Luther, 2025a). Metode ini banyak digunakan karena mampu memberikan gambaran kondisi keamanan sistem secara menyeluruh tanpa melakukan eksploitasi yang dapat mengganggu operasional sistem (Vaño et al., 2025).

Penelitian terdahulu yang dilakukan oleh Tara Rizkayanti dan Yunanri (2023) dengan judul *"Analisis Keamanan Website Sistem Informasi Administrasi Kependudukan Menggunakan Metode Vulnerability Assessment"* menjadi salah satu referensi dalam penelitian ini. Penelitian tersebut menerapkan tahapan *information gathering* menggunakan Nslookup, Whois, dan Nmap, kemudian dilanjutkan dengan proses pemindaian kerentanan menggunakan OWASP ZAP (Alboqmi & Gamble, 2025). Hasil penelitian menunjukkan bahwa website yang diuji memiliki 14 temuan keamanan, yang terdiri atas 3 kerentanan tingkat Medium dan 11 kerentanan tingkat Low, dengan beberapa temuan utama berupa tidak adanya Anti-CSRF Token, X-Frame-Options, serta atribut keamanan pada cookie (Evans et al., 2025). Penelitian tersebut menunjukkan bahwa pengujian keamanan secara berkala mampu membantu organisasi dalam mengidentifikasi kelemahan konfigurasi keamanan sebelum dimanfaatkan oleh pihak yang tidak

bertanggung jawab (Andrade et al., 2025).

Penelitian lain dilakukan oleh Darojat et al. (2022) yang mengevaluasi keamanan website *e-government* menggunakan metode Vulnerability Assessment berdasarkan pedoman NIST SP 800-115 dan OWASP. Penelitian tersebut membandingkan hasil dua *web vulnerability scanner* dan menunjukkan bahwa masing-masing alat mampu mengidentifikasi kategori kerentanan yang serupa, meskipun terdapat perbedaan pada jumlah temuan, jenis kerentanan, dan durasi proses pemindaian.

Selanjutnya, Hafsari dan Harjono (2024) menerapkan metode Vulnerability Assessment pada website Pendaftaran Mahasiswa Baru Universitas Muhammadiyah Purwokerto. Penelitian tersebut menunjukkan bahwa tahapan *information gathering* dan *vulnerability scanning* mampu mengidentifikasi berbagai kelemahan konfigurasi keamanan sehingga dapat digunakan sebagai dasar dalam penyusunan rekomendasi mitigasi untuk meningkatkan keamanan aplikasi web (Okonkwo et al., 2025).

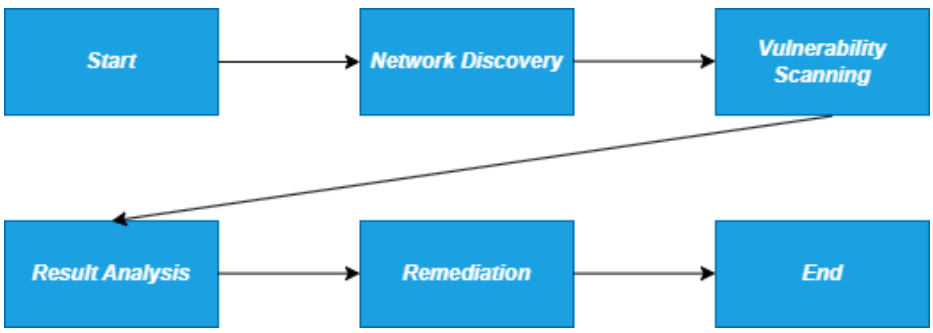
Berbeda dengan penelitian sebelumnya, penelitian ini memfokuskan analisis pada Website ELLS AMIKOM Purwokerto dengan menerapkan metode Vulnerability Assessment menggunakan beberapa tools keamanan, yaitu Whois, DNS Lookup (Nslookup), WhatWeb Nmap, dan OWASP ZAP (Ilman Sholihin, 2025). Tahapan pengujian diawali dengan proses *information gathering* untuk memperoleh informasi mengenai target, kemudian dilanjutkan dengan proses *vulnerability scanning* menggunakan beberapa alat pemindai guna memperoleh hasil yang lebih komprehensif (Ilman Sholihin, 2025). Seluruh proses pengujian dilakukan dengan izin dari pengelola sistem sehingga penelitian tetap memperhatikan aspek etika dalam pengujian keamanan (Mukhopadhyay & Luther, 2025).

Berdasarkan hasil pengujian yang dilakukan, diperoleh 14 temuan keamanan, yang terdiri atas 4 kerentanan tingkat Medium, 5 kerentanan tingkat Low, dan 5 temuan Informational. Empat kerentanan tingkat Medium yang ditemukan meliputi Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header, dan Sub Resource Integrity Attribute Missing. Temuan-temuan tersebut menunjukkan bahwa meskipun tidak ditemukan kerentanan dengan tingkat risiko tinggi (*High*), masih terdapat beberapa konfigurasi keamanan yang perlu diperbaiki agar mampu mengurangi potensi serangan terhadap aplikasi web.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis tingkat keamanan Website ELLS AMIKOM Purwokerto menggunakan metode Vulnerability Assessment, mengidentifikasi kerentanan yang ditemukan, menentukan tingkat risiko setiap kerentanan berdasarkan hasil pemindaian, serta memberikan rekomendasi mitigasi sesuai praktik terbaik keamanan aplikasi web yang mengacu pada standar OWASP. Hasil penelitian ini diharapkan dapat menjadi bahan evaluasi bagi pengelola Website ELLS AMIKOM Purwokerto dalam meningkatkan keamanan sistem, sekaligus menjadi referensi bagi penelitian selanjutnya yang membahas pengujian keamanan aplikasi web menggunakan metode Vulnerability Assessment.

METODE PENELITIAN

Penelitian ini menggunakan metode Vulnerability Assessment (VA) sebagai pendekatan utama untuk mengidentifikasi dan menganalisis kerentanan keamanan pada Website ELLS AMIKOM Purwokerto. Metode ini dipilih karena mampu memberikan gambaran kondisi keamanan aplikasi web secara menyeluruh melalui proses identifikasi kerentanan tanpa melakukan eksploitasi yang dapat mengganggu operasional sistem. Selain mengidentifikasi kelemahan keamanan, metode ini juga menghasilkan rekomendasi perbaikan sebagai upaya mitigasi terhadap potensi serangan siber.



Gambar 1 Metode Penelitian

Tahapan penelitian terdiri atas Network discovery atau Information gathering, Vulnerability Scanning, Result Analysis, dan Remediation. Seluruh proses pengujian dilakukan terhadap Website ELLS AMIKOM Purwokerto dengan izin dari pengelola sistem sehingga tetap memperhatikan aspek etika dalam pengujian keamanan.

Tahap awal penelitian adalah Network discovery atau Information gathering Tahap ini bertujuan untuk mengumpulkan informasi awal mengenai target pengujian, seperti informasi domain, alamat IP, konfigurasi DNS, teknologi web yang digunakan, serta layanan jaringan yang aktif. Pada penelitian ini digunakan beberapa tools, yaitu Whois untuk memperoleh informasi registrasi domain, DNS Lookup (Nslookup) untuk mengidentifikasi konfigurasi DNS, WhatWeb untuk mendeteksi teknologi web yang digunakan oleh website, serta Nmap untuk melakukan pemindaian port dan identifikasi layanan (*service detection*) yang berjalan pada server. Informasi yang diperoleh dari tahap ini digunakan sebagai dasar dalam menentukan ruang lingkup pengujian keamanan pada tahap berikutnya.

Setelah informasi dasar berhasil diperoleh, penelitian dilanjutkan pada tahap Vulnerability Scanning. Tahap ini bertujuan untuk mengidentifikasi potensi kerentanan yang terdapat pada Website ELLS AMIKOM Purwokerto menggunakan beberapa alat pemindai keamanan. Nikto digunakan untuk mengidentifikasi kelemahan konfigurasi web server, seperti konfigurasi HTTP Header yang kurang aman, keberadaan file sensitif, serta konfigurasi server yang berpotensi menimbulkan risiko keamanan. Selanjutnya, Nuclei digunakan untuk melakukan pemindaian berbasis template terhadap kerentanan yang telah terdokumentasi oleh komunitas keamanan siber. Selain itu, penelitian ini menggunakan OWASP ZAP (Zed Attack Proxy) sebagai alat utama dalam melakukan pengujian keamanan aplikasi web melalui mekanisme Spider, Passive Scan, dan Active Scan terhadap seluruh halaman publik Website ELLS AMIKOM Purwokerto. Proses ini dilakukan untuk mengidentifikasi berbagai kelemahan keamanan pada header HTTP, formulir (*form input*), parameter URL, cookie, maupun konfigurasi keamanan aplikasi web.

Tahap berikutnya adalah Result Analysis, yaitu proses analisis terhadap seluruh hasil pemindaian yang diperoleh dari Nikto, Nuclei, dan OWASP ZAP. Analisis dilakukan dengan mengelompokkan setiap temuan berdasarkan tingkat risiko yang diberikan oleh OWASP ZAP, yaitu High, Medium, Low, dan Informational. Selanjutnya setiap temuan dianalisis berdasarkan potensi dampaknya terhadap aspek Confidentiality, Integrity, dan Availability (CIA) serta dikaitkan dengan standar keamanan seperti OWASP Top 10 dan Common Weakness Enumeration (CWE). Berdasarkan hasil pengujian diperoleh 14 temuan, yang terdiri atas 4 kerentanan tingkat Medium, 5 kerentanan tingkat Low, 5 temuan Informational, serta tidak ditemukan kerentanan tingkat High.

Tahap terakhir adalah Remediation, yaitu penyusunan rekomendasi perbaikan terhadap seluruh kerentanan yang ditemukan selama proses Vulnerability Assessment. Rekomendasi disusun berdasarkan dokumentasi resmi OWASP, Mozilla Developer Network (MDN), serta praktik terbaik dalam pengamanan aplikasi web. Fokus rekomendasi meliputi penerapan Anti-CSRF Token, implementasi Content Security Policy (CSP), konfigurasi X-Frame-Options atau Content-Security-Policy frame-ancestors sebagai perlindungan terhadap serangan *Clickjacking*, penggunaan Subresource Integrity (SRI) pada sumber daya eksternal, serta penguatan konfigurasi keamanan server dan HTTP Security Header. Diharapkan rekomendasi tersebut dapat menjadi acuan bagi pengelola Website ELLS AMIKOM Purwokerto dalam meningkatkan keamanan aplikasi web dan mengurangi risiko eksploitasi di masa mendatang.

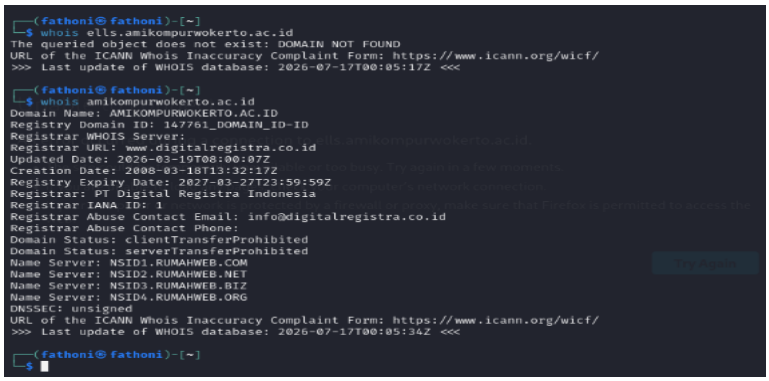
HASIL DAN PEMBAHASAN

Information Gathering

Uji Tahap Network discovery atau Information gathering merupakan langkah awal yang sangat krusial dalam proses pengujian penetrasi (penetration testing). Tujuan utama fase ini adalah untuk mengumpulkan berbagai informasi awal sebanyak mungkin mengenai sistem target, yang nantinya akan menjadi dasar dalam tahap-tahap pengujian lanjutan. Informasi yang dikumpulkan meliputi struktur jaringan, sistem operasi yang digunakan, layanan yang berjalan, serta potensi celah yang dapat dimanfaatkan untuk akses tidak sah. Meskipun bersifar pasif dan non-intrusif, fase ini memiliki peran strategis dalam membentuk gambaran awal mengenai topologi dan kerentanan sistem target.

Salah satu teknik yang digunakan dalam tahap Information Gathering atau Network discovery adalah analisis WHOIS terhadap domain target. WHOIS merupakan protokol yang digunakan untuk memperoleh informasi registrasi suatu domain, seperti registrar, status

domain, *name server*, tanggal registrasi, masa berlaku domain, serta informasi administratif lainnya. Pada penelitian ini dilakukan analisis terhadap domain amikompurwokerto.ac.id, karena subdomain ells.amikompurwokerto.ac.id tidak memiliki data registrasi tersendiri dan mengembalikan pesan *DOMAIN NOT FOUND*. Hasil pengujian menunjukkan bahwa domain amikompurwokerto.ac.id terdaftar pada PT Digital Registra Indonesia dengan Registry Domain ID 147761_DOMAIN_ID-ID. Domain tersebut pertama kali didaftarkan pada 18 Maret 2008, memiliki masa berlaku hingga 27 Maret 2027, serta menggunakan empat *name server* milik Rumahweb, yaitu NSID1.RUMAHWEB.COM, NSID2.RUMAHWEB.NET, NSID3.RUMAHWEB.BIZ, dan NSID4.RUMAHWEB.ORG. Selain itu, status domain menunjukkan clientTransferProhibited dan serverTransferProhibited, yang mengindikasikan bahwa domain telah diberikan mekanisme perlindungan terhadap proses transfer domain tanpa otorisasi.



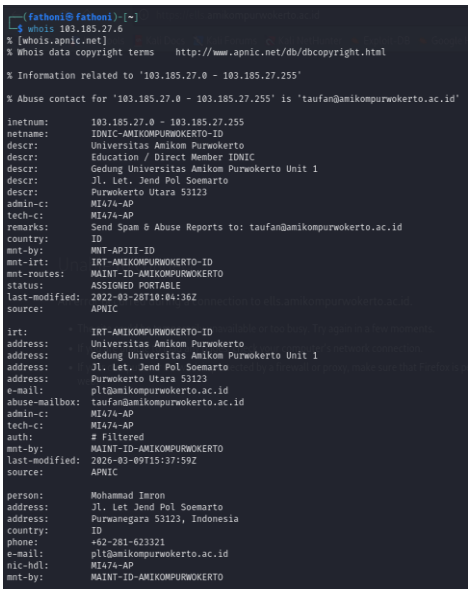
Gambar 2 Proses Analisis

Berdasarkan gambar, diketahui bahwa domain amikompurwokerto.ac.id terdaftar pada PT Digital Registra Indonesia dan menggunakan empat name server milik rumah web

Selanjutnya dilakukan DNS Lookup menggunakan perintah dig +short untuk mengetahui alamat IP dari domain target. Hasil pemetaan menunjukkan bahwa domain ells.amikompurwokerto.ac.id mengarah ke alamat IP 103.185.27.6. Informasi ini menjadi dasar untuk melakukan identifikasi kepemilikan alamat IP melalui WHOIS IP.

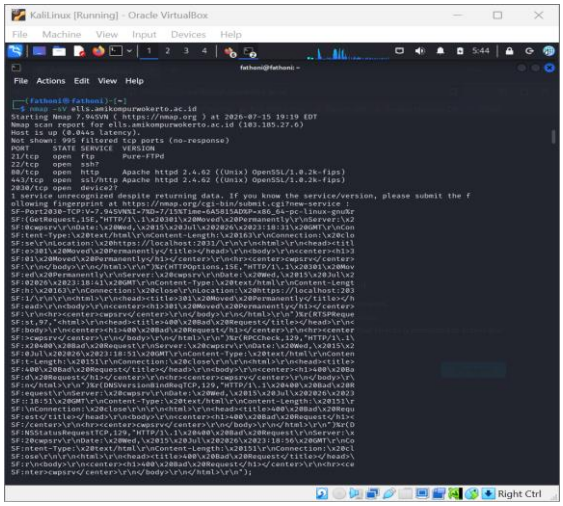
Gambar 3 Alamat IP

Setelah alamat IP berhasil diperoleh, dilakukan analisis WHOIS terhadap IP tersebut. Hasil menunjukkan bahwa alamat IP 103.185.27.6 berada dalam alokasi jaringan Universitas Amikom Purwokerto dengan rentang alamat 103.185.27.0–103.185.27.255 yang terdaftar pada APNIC. Informasi ini mengonfirmasi bahwa server website berada pada jaringan yang dikelola oleh institusi tersebut.



Gambar 4 Pemindaian Port

Selain WHOIS, dilakukan pula pemindaian port menggunakan perangkat lunak Nmap. Nmap atau Network Mapper merupakan salah satu tools standar dalam dunia keamanan jaringan yang digunakan untuk mendeteksi port mana saja yang terbuka (open), layanan apa yang berjalan di atasnya, serta versi perangkat lunak yang digunakan. Pemindaian dilakukan terhadap IP yang sama untuk mengetahui eksposur layanan di sisi jaringan. Hasilnya menunjukan bahwa terdapat beberapa port yang berada dalam kondisi terbuka, yaitu port 21 (FTP), port 22 (SSH), port 80 (HTTP), dan port 443 (HTTPS) sebagaimana ditunjukan pada gambar. Selain itu, Nmap berhasi mengidentifikasi bahwa layanan web dijalankan menggunakan Apache HTTP Server versi 2.4.62 (Unix) dengan dukungan OpenSSL 1.0.2k-fips, sedangkan layanan FTP menggunakan Pure-FTPd.

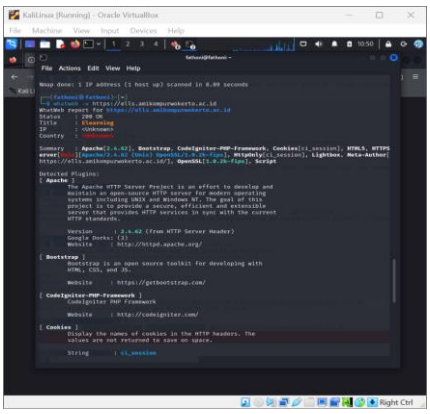


Gambar 5 Analisis Layanan Utama

Keberadaan port-port tersebut menunjukkan bahwa server menyediakan beberapa layanan utama yang mendukung operasional website, yaitu layanan FTP untuk proses transfer berkas, SSH untuk administrasi server secara jarak jauh, serta layanan HTTP dan HTTPS sebagai media akses aplikasi web oleh pengguna. Informasi mengenai versi perangkat lunak yang digunakan juga memberikan gambaran mengenai konfigurasi server yang nantinya dapat menjadi acuan dalam proses identifikasi kerentanan.

Meskipun pada tahap ini tidak ditemukan indikasi eksploitasi secara langsung, keberadaan port yang terbuka tetap berpotensi meningkatkan attack surface apabila layanan yang berjalan tidak dikelola dengan baik, menggunakan konfigurasi yang kurang aman, atau tidak memperoleh pembaruan keamanan secara berkala. Oleh karena itu, informasi yang diperoleh dari hasil pemindaian Nmap digunakan sebagai dasar dalam tahap Vulnerability Assessment, khususnya untuk mengidentifikasi potensi kerentanan pada layanan yang tersedia.

Setelah dilakukan identifikasi layanan menggunakan Nmap, tahap berikutnya adalah melakukan web fingerprinting menggunakan tool WhatWeb. Tujuan dari proses ini adalah untuk mengidentifikasi teknologi, framework, web server, serta komponen pendukung yang digunakan oleh website target. Informasi tersebut penting karena setiap teknologi memiliki karakteristik dan potensi kerentanan yang berbeda sehingga dapat menjadi dasar dalam proses Vulnerability Assessment.



Gambar 6 Identifikasi menggunakan WhatWeb 1

Berdasarkan hasil identifikasi menggunakan WhatWeb, website ELLS AMIKOM Purwokerto terdeteksi menggunakan Apache HTTP Server versi 2.4.62 yang berjalan pada sistem operasi berbasis Unix dengan dukungan OpenSSL 1.0.2k-fips sebagai implementasi protokol SSL/TLS. Selain itu, aplikasi web dibangun menggunakan framework CodeIgniter dan memanfaatkan framework antarmuka Bootstrap untuk pengembangan tampilan halaman web. Hasil identifikasi juga menunjukkan penggunaan cookie sesi ci_session, yang mengindikasikan bahwa mekanisme manajemen sesi dikelola oleh framework CodeIgniter. Pada sisi aplikasi, website telah menggunakan HTML5, serta memanfaatkan pustaka Lightbox sebagai komponen JavaScript untuk menampilkan gambar dan konten multimedia.

Dari informasi header HTTP yang diperoleh, server memberikan respons HTTP/1.1 200 OK yang menunjukkan bahwa layanan web dapat diakses dengan normal. Selain itu, turut teridentifikasi beberapa header HTTP seperti Content-Type, Cache-Control, Content-Encoding, dan Set-Cookie, yang kemudian menjadi salah satu objek analisis pada tahap vulnerability scanning menggunakan OWASP ZAP. Informasi mengenai versi perangkat lunak, framework, serta konfigurasi server tersebut memberikan gambaran mengenai teknologi yang digunakan sekaligus membantu dalam menentukan kemungkinan kerentanan yang berkaitan dengan konfigurasi keamanan server.

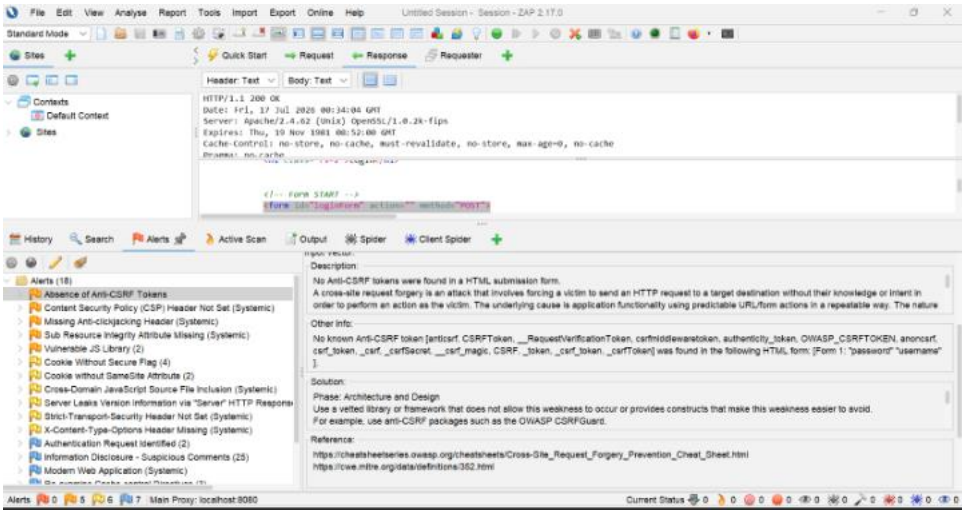
Secara keseluruhan, hasil identifikasi menggunakan WhatWeb melengkapi informasi yang diperoleh pada tahap sebelumnya. Apabila Nmap berfokus pada identifikasi port dan layanan jaringan, maka WhatWeb memberikan informasi yang lebih spesifik mengenai teknologi aplikasi web yang berjalan pada server target. Informasi tersebut menjadi dasar penting dalam proses analisis kerentanan karena memungkinkan peneliti mengidentifikasi potensi kelemahan yang berkaitan dengan konfigurasi server, framework aplikasi, maupun komponen pihak ketiga yang digunakan sebelum dilakukan pemindaian menggunakan OWASP ZAP.

Vulnerability scanning

Tahap Vulnerability scanning merupakan langkah lanjutan dalam proses pengujian keamanan yang bertujuan untuk mendeteksi secara aktif berbagai potensi kerentanan (vulnerabilities) yang terdapat pada sistem atau aplikasi web. Setelah informasi dasar mengenai struktur dan layanan website berhasil dikumpulkan, proses pemindaian ini dilakukan untuk menguji secara menyeluruh setiap komponen dan endpoint yang sebelumnya telah terpetakan. Dalam penelitian ini, alat yang digunakan adalah OWASP ZAP (Zed Attack Proxy), yaitu salah satu tools open-source yang dikembangkan khusus untuk mendeteksi kelemahan keamanan pada aplikasi berbasis web.

Pemindaian dimulai dengan eksplorasi struktur situs menggunakan fitur Spidering pada OWASP ZAP. Tahap ini berfungsi untuk menjelajahi seluruh halaman dan parameter yang dapat diakses, baik melalui tautan langsung maupun input formulir. Semua halaman dan titik interaksi pengguna yang ditemukan akan dicatat dan disiapkan untuk pengujian lanjutan. Setelah struktur website terpetakan, OWASP ZAP melanjutkan dengan melakukan Passive Scanning, yaitu analisis terhadap lalu lintas data selama proses crawling tanpa mengirimkan payload eksploitasi. Pada tahap ini, teridentifikasi sejumlah temuan awal seperti absennya pengaturan header keamanan (misalnya X-Frame-Options), cookie tanpa atribut HTTPOnly dan Secure, serta pengungkapan informasi server melalui header HTTP.

Setelah tahap pasif selesai, dilanjutkan dengan Active Scanning, di mana OWASP ZAP secara aktif mengirimkan berbagai payload serangan ke parameter dan form yang telah ditemukan. Tujuan dari tahap ini adalah untuk menguji apakah sistem target rentan terhadap serangan umum seperti SQL Injection, Cross-Site Scripting (XSS), Directory Traversal, serta berbagai bentuk security misconfiguration. Berdasarkan hasil pengujian, OWASP ZAP melaporkan beberapa kerentanan, termasuk kemungkinan adanya kelemahan pada parameter yang menerima input langsung dari pengguna tanpa validasi yang memadai. Selain itu, beberapa konfigurasi server juga dinilai kurang aman, seperti adanya halaman login yang tidak selalu terlindungi oleh protokol HTTPS secara konsisten.



Gambar 7 Tahap Vulnerability scanning

Seluruh hasil pemindaian diklasifikasikan berdasarkan tingkat keparahan, mulai dari tingkat tinggi (High), sedang (Medium), rendah (Low), hingga informasional. OWASP ZAP menyertakan bukti teknis dari setiap temuan, seperti URL spesifik, parameter yang diuji, dan payload yang digunakan. Informasi ini sangat penting dalam proses analisis lanjutan, karena memberikan konteks jelas mengenai cara kerja celah dan dieksploitasi. Vulnerability potensi Dengan dampaknya apabila demikian, scanning tidak tahap hanya menghasilkan daftar kerentanan, tetapi juga memberikan dasar yang kuat untuk proses mitigasi pada tahap berikutnya.

Result Analysis

Setelah proses vulnerability scanning selesai dilakukan, data hasil pemindaian dianalisis secara mendalam untuk menilai validitas, tingkat risiko, serta potensi dampak dari setiap kerentanan yang teridentifikasi pada website target. Analisis ini dilakukan dengan mengacu pada standar keamanan yang diakui secara luas, seperti OWASP ZAP guna memastikan bahwa temuan yang dianggap kritis mendapatkan perhatian prioritas.

Berdasarkan hasil pemindaian menggunakan OWASP ZAP, ditemukan sejumlah kerentanan yang dapat dikelompokkan berdasarkan tingkat keparahan sebagai berikut:

Table 1 Hasil pemindaian menggunakan OWASP ZAP

No	Tingkat resiko	Jumlah temuan	Keterangan
1	High	0	Menunjukkan kerentanan dengan dampak sangat serius yang dapat dieksploitasi secara langsung, Harus segera diperbaiki karena berpotensi menyebabkan kebocoran data.
2	Medium	4	Merupakan kerentanan dengan risiko moderat. Biasanya tidak memberikan akses langsung ke sistem, tetapi dapat menjadi titik awal serangan atau memperbesar dampak jika dikombinasika n dengan kelemahan lain. Perlu segera diperbaiki untuk mencegah penyalahgunaa n lebih lanjut.
3	Low	5	Celah dengan dampak terbatas yang sulit dieksploitasi atau memiliki efek kecil terhadap sistem.
4	Informational	5	Bukan kerentanan langsung, tetapi informasi yang bisa digunakan penyerang untuk memetakan sistem dan merancang serangan di masa depan.

Remediation

Setelah hasil analisis temuan kerentanan selesai, tahap selanjutnya adalah melakukan remediation atau perbaikan untuk menutup celah keamanan yang ditemukan. Proses remediasi ini harus dilakukan secara prioritas berdasarkan tingkat risiko, mulai dari yang berisiko tinggi

hingga rendah, untuk meminimalkan potensi serangan yang dapat terjadi. Berikut ini adalah beberapa rekomendasi perbaikan berdasarkan saran dari tools OWASP ZAP :

Table 2 Hasil Remidiation

Resiko	Kerentanan	Deskripsi	Rekomendasi
Medium	Absence of Anti-CSRF Tokens	Formulir tidak memiliki token Anti-CSRF sehingga rentan terhadap serangan CSRF.	Terapkan token Anti-CSRF pada setiap formulir.
Medium	Content Security Policy (CSP) Header Not Set	Header CSP tidak dikonfigurasi sehingga meningkatkan risiko XSS.	Pastikan server web, server aplikasi, load balancer, dan perangkat lainnya telah dikonfigurasi untuk menyertakan header Content-Security-Policy.
Medium	Missing Anti-clickjacking Header	Respons tidak melindungi dari serangan 'ClickJacking'. Respons tersebut seharusnya menyertakan salah satu dari Content-Security-Policy dengan direktif 'frame-ancestors' atau X-Frame-Options.	Konfigurasi X-Frame-Options atau frame-ancestors.
Medium	Sub Resource Integrity Attribute Missing	Script eksternal tidak menggunakan atribut integrity.	Sediakan atribut integrity yang valid pada tag tersebut.
Low	Cookie Without Secure Flag	Sebuah cookie telah dikonfigurasi tanpa menggunakan atribut secure (secure flag), yang berarti cookie tersebut dapat diakses melalui koneksi yang tidak terenkripsi.	Kapan pun sebuah cookie berisi informasi sensitif atau merupakan sebuah token sesi (session token), maka cookie tersebut harus selalu dikirimkan menggunakan saluran yang terenkripsi. Pastikan atribut secure (secure flag) telah dikonfigurasi untuk cookie yang berisi informasi sensitif tersebut.
Low	Cross-Domain JavaScript Source File Inclusion	Halaman ini memuat satu atau beberapa berkas script dari domain pihak ketiga (third-party domain).	Pastikan berkas sumber JavaScript hanya dimuat dari sumber yang tepercaya, dan

Resiko	Kerentanan	Deskripsi	Rekomendasi
			sumber-sumber tersebut tidak dapat dikendalikan oleh pengguna akhir (end user) dari aplikasi.
Low	Server Leaks Version Information via "Server" HTTP Response Header Field	Server web/aplikasi membocorkan informasi versi melalui header respons HTTP "Server". Akses terhadap informasi tersebut dapat memudahkan penyerang dalam mengidentifikasi kerentanan lain yang ada pada server web/aplikasi Anda.	Pastikan server web, server aplikasi, load balancer, dan perangkat sejenisnya telah dikonfigurasi untuk menyembunyikan header "Server" atau hanya menyediakan informasi yang bersifat umum (generic).
Low	Strict-Transport-Security Header Not Set	HTTP Strict Transport Security (HSTS) adalah sebuah mekanisme kebijakan keamanan web di mana server web menyatakan bahwa user agent yang patuh (seperti browser web) harus berinteraksi dengannya hanya dengan menggunakan koneksi HTTPS yang aman (yaitu HTTP yang dilapisi di atas TLS/SSL).	Pastikan server web, server aplikasi, load balancer, dan perangkat sejenisnya telah dikonfigurasi untuk menegakkan Strict-Transport-Security.
Low	X-Content-Type-Options Header Missing	Header Anti-MIME-Sniffing X-Content-Type-Options tidak diatur ke nilai 'nosniff'. Hal ini memungkinkan versi lama dari Internet Explorer dan Chrome untuk melakukan MIME-sniffing pada isi respons (response body), yang berpotensi menyebabkan isi respons tersebut ditafsirkan dan ditampilkan sebagai jenis konten (content type) lain, bukan sebagai jenis konten	Pastikan server aplikasi/web mengatur header Content-Type dengan tepat, dan mengatur header X-Content-Type-Options ke 'nosniff' untuk semua halaman web. Jika memungkinkan, pastikan pengguna akhir (end user) menggunakan browser web modern yang patuh pada standar dan tidak melakukan MIME-sniffing sama sekali, atau browser yang

Resiko	Kerentanan	Deskripsi	Rekomendasi
		yang telah dinyatakan.	dapat diarahkan oleh aplikasi/server web untuk tidak melakukan MIME-sniffing.
Informational	Authentication Request Identified	Permintaan (request) yang diberikan telah diidentifikasi sebagai sebuah permintaan autentikasi. Kolom 'Other Info' berisi serangkaian baris dengan format kunci=nilai (key=value) yang mengidentifikasi setiap kolom yang relevan.	Ini adalah peringatan yang bersifat informasional, bukan sebuah kerentanan, sehingga tidak ada yang perlu diperbaiki.
Informational	Information Disclosure - Suspicious Comments	Respons tampaknya mengandung komentar mencurigakan yang dapat membantu seorang penyerang (attacker).	Hapus semua komentar yang mengembalikan informasi yang dapat membantu seorang penyerang, dan perbaiki masalah mendasar apa pun yang dirujuk oleh komentar tersebut.
Informational	Modern Web Application	Aplikasi tersebut tampaknya merupakan aplikasi web modern. Jika Anda perlu menjelajahinya secara otomatis, Client Spider kemungkinan besar akan jauh lebih efektif daripada spider standar.	Ini adalah peringatan yang bersifat informasional, sehingga tidak ada perubahan yang diperlukan.
Informational	Re-examine Cache-control Directives	Header Cache-Control belum diatur dengan benar atau tidak ditemukan, sehingga memungkinkan browser dan proksi untuk menyimpan konten dalam tembolok (cache). Untuk aset statis seperti file CSS, JS, atau gambar, hal ini mungkin memang disengaja. Namun, sumber daya (resources) tersebut	Untuk konten yang aman (sensitif), pastikan header HTTP Cache-Control diatur dengan nilai "no-cache, no-store, must-revalidate". Jika suatu aset memang harus disimpan dalam cache, pertimbangkan untuk mengatur direktif "public, max-age, immutable".

Resiko	Kerentanan	Deskripsi	Rekomendasi
		harus ditinjau kembali untuk memastikan tidak ada konten sensitif yang akan tersimpan dalam cache.	
Informational	Session Management Response Identified	Respons yang diberikan telah diidentifikasi mengandung token manajemen sesi. Kolom 'Other Info' (Informasi Lainnya) berisi sekumpulan token header yang dapat digunakan dalam Metode Manajemen Sesi Berbasis Header.	Ini adalah peringatan yang bersifat informasional dan bukan sebuah kerentanan, sehingga tidak ada yang perlu diperbaiki.

KESIMPULAN

Penelitian ini mengevaluasi keamanan Website ELLS AMIKOM Purwokerto menggunakan metode *Vulnerability Assessment* melalui tahapan *information gathering*, *vulnerability scanning* dengan OWASP ZAP, analisis hasil, dan penyusunan rekomendasi perbaikan. Tahap *information gathering* menggunakan WHOIS, DNS Lookup, Nmap, dan WhatWeb untuk mengidentifikasi informasi domain, jaringan, serta teknologi website. Hasil pemindaian menunjukkan tidak ditemukan kerentanan tingkat tinggi (*High*), tetapi terdapat 4 kerentanan *Medium*, 5 *Low*, dan 5 *Informational*. Temuan utama meliputi tidak adanya Anti-CSRF Token, Content Security Policy (CSP), header anti-clickjacking, dan Subresource Integrity (SRI), serta beberapa kelemahan konfigurasi HTTP Header dan cookie. Kerentanan tersebut berpotensi meningkatkan risiko serangan seperti CSRF, XSS, dan *Clickjacking*. Rekomendasi perbaikan meliputi penerapan Anti-CSRF Token, CSP, X-Frame-Options atau *frame-ancestors*, SRI, penguatan konfigurasi HTTP Header dan cookie, pembaruan perangkat lunak secara berkala, serta pelaksanaan *Vulnerability Assessment* secara rutin. Hasil penelitian menunjukkan bahwa metode *Vulnerability Assessment* dapat membantu mengidentifikasi kelemahan keamanan dan memberikan rekomendasi teknis untuk meningkatkan keamanan Website ELLS AMIKOM Purwokerto serta meminimalkan risiko serangan siber. Hasil penelitian ini menunjukkan bahwa penerapan metode Vulnerability Assessment mampu memberikan gambaran mengenai kondisi keamanan website secara menyeluruh serta menghasilkan rekomendasi teknis yang dapat digunakan sebagai acuan dalam meningkatkan keamanan Website ELLS AMIKOM Purwokerto. Dengan melakukan evaluasi keamanan secara berkala dan menerapkan rekomendasi yang dihasilkan, diharapkan tingkat risiko serangan siber dapat diminimalkan sehingga kerahasiaan, integritas, dan ketersediaan layanan website tetap terjaga.

REFERENSI

Alboqmi, R., & Gamble, R. F. (2025). Enhancing Microservice Security Through Vulnerability-Driven Trust in the Service Mesh Architecture. *Sensors*, *25*(3). https://doi.org/10.3390/s25030914

Andrade, F., Resende, A., Roquette Viana, C., Simões Figueiredo, A., & Loureiro, F. (2025). An Overview of Instruments to Assess Vulnerability in Healthcare: A Scoping Review. In *Healthcare (Switzerland)* (Vol. 13, Number 17). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/healthcare13172251

Brito, T., Lopes, P., Santos, N., & Santos, J. F. (2022). Wasmati: An efficient static vulnerability scanner for WebAssembly. *Computers and Security*, *118*. https://doi.org/10.1016/j.cose.2022.102745

Evans, S., Cooney, G., Young, D., O'Donnell, U., & Tiffin, P. A. (2025). Measuring the care needs of young people with intellectual difficulties: Construct validity of the learning disability

vulnerability assessment scale and utility in establish the care needs of young people. *Journal of Intellectual Disabilities*. https://doi.org/10.1177/17446295251392108

Fatkhussarifin, F., & Wicaksono, D. (2025). PENGEMBANGAN WEBSITE INTERAKTIF BERBASIS NANO-LEARNING UNTUK PENGUATAN KOMPETENSI PEDAGOGIK DIGITAL GURU SD MUHAMMADIYAH INOVATIF MERTOYUDAN. *SULIWA: Jurnal Multidisiplin Teknik, Sains, Pendidikan Dan Teknologi*, *2*(2), 148–152. https://doi.org/10.62671/suliwa.v2i2.83

Ilman Sholihin. (2025). *PENERAPAN APLIKASI MOBILE SIEM BERBASIS WAZUH UNTUK NOTIFIKASI REAL-TIME DAN REKOMENDASI PENANGANAN AWAL*.

Moret, W. (2014). *Vulnerability Assessment Methodologies: A Review of the Literature*.

Mukhopadhyay, A., & Luther, K. (2025a, April 26). OSINT Clinic: Co-designing AI-Augmented Collaborative OSINT Investigations for Vulnerability Assessment. *Conference on Human Factors in Computing Systems - Proceedings* . https://doi.org/10.1145/3706598.3713283

Mukhopadhyay, A., & Luther, K. (2025b, April 26). OSINT Clinic: Co-designing AI-Augmented Collaborative OSINT Investigations for Vulnerability Assessment. *Conference on Human Factors in Computing Systems - Proceedings* . https://doi.org/10.1145/3706598.3713283

Nugraha, W. T. S., Permana, M. F. J., Sundari, F. R., Ikhsaniyah, N., Abdurrahman, H., Pradeka, D., & Adiwilaga, A. (2025). Pengembangan Website Interaktif Untuk Memfasilitasi Minat Kebersihan Kelas di Kalangan Siswa Menengah Pertama. *JIKO (Jurnal Informatika Dan Komputer)*, *9*(2), 251. https://doi.org/10.26798/jiko.v9i2.1340

Okonkwo, P. C., Nwokolo, S. C., Udo, S. O., Obiwulu, A. U., Onnoghen, U. N., Alarifi, S. S., Eldosouky, A. M., Ekwok, S. E., Andráš, P., & Akpan, A. E. (2025). Solar PV systems under weather extremes: Case studies, classification, vulnerability assessment, and adaptation pathways. In *Energy Reports* (Vol. 13, pp. 929–959). Elsevier Ltd. https://doi.org/10.1016/j.egyr.2024.12.067

Razak, B. (2020). PENERAPAN METODE DESIGN THINKING PADA APLIKASI KOMUNITAS PENGHOBI BATU MULIA NUSANTARA. *Ekono Insentif*, *14*(2), 129–140. https://doi.org/10.36787/jei.v14i2.402

Schagen, N., Koning, K., Bos, H., & Giuffrida, C. (2018, April 23). Towards automated vulnerability scanning of network servers. *Proceedings of the 11th European Workshop on Systems Security, EuroSec 2018*. https://doi.org/10.1145/3193111.3193116

Siddiq, H., Auliana, S., & Darip, M. (2025). PERANCANGAN WEBSITE E-TOURISM SEBAGAI MEDIA PROMOSI DIGITAL PARIWISATA DI KECAMATAN PULOSARI MENGGUNAKAN FRAMEWORK LARAVEL. *INFOTECH Journal*, *11*(2), 192–199. https://doi.org/10.31949/infotech.v11i2.15025

Vaňo, S., Duchková, H., Bašta, P., Jančovič, M., Geletič, J., Lorencová, E. K., & Suchá, L. (2025). From scenarios to strategies: Integrated methodology for addressing urban heat vulnerability in an uncertain future. *Sustainable Cities and Society*, *121*. https://doi.org/10.1016/j.scs.2025.106202

Viega, J., Bloch, J. T., Kohno, Y., & Mcgraw, G. (n.d.). *ITS4: A Static Vulnerability Scanner for C and C++ Code*. Retrieved http://www.rstcorp.com