JKT Jurnal Komputer Terapan
ISSN : 2443-4159 (Print) ISSN: 2460-5255 (Online)
Politeknik Caltex Riau
Empower You to Global Competition

ANALISIS IMPLEMENTASI NUCKLEI VULNERABILITY DAN OWASP-ZAP SCANNER UNTUK DETEKSI KERENTANAN KEAMANAN (SECURE SYSTEM) PADA PLATFORM WEB BASED

Siti Aulia Rachmini*[1], Indra[1], Nuralamsah Zulkarnaim[1], Muhammad Mukhram[1], Agung Rizaldi[2]
Fakultas Teknik Prodi Informatika Universitas Sulawesi Barat [1]
Fakultas Ekonomi Prodi Akuntansi Universitas Sulawesi Barat[2]
sitiaulia.rachmini@unsulbar.ac.id*, indra@unsulbar.ac.id, nuralamsah@unsulbar.ac.id
muhammadmukhram@unsulbar.ac.id, danipp555@gmail.com
**Penulis Koresponden*

ABSTRAK

Keamanan platform berbasis web merupakan aspek fundamental yang harus dipertimbangkan oleh pengembang web. Namun, masih banyak ditemukan pengembang yang kurang cermat dalam meningkatkan tingkat keamanan situs mereka, sehingga meningkatkan risiko situs tersebut menjadi sasaran peretas. Untuk mengatasi masalah ini, pemanfaatan tools seperti *Nuclei Vulnerability Scanner* dan *Owasp Zap* dapat menjadi solusi efektif untuk mendeteksi potensi peretasan pada platform berbasis web dengan cepat. Penelitian ini melakukan pengujian terhadap aplikasi web dummy yang dikembangkan secara lokal dan pemindaian dilakukan menggunakan *tools Nuclei Vulnerability Scanner* dan *Owasp Zap*. Hasil penelitian menunjukkan bahwa *Nuclei Vulnerability Scanner* efektif dalam mendeteksi kerentanan pada *layer* jaringan, terutama pada protokol SSL/TLS dan konfigurasi proxy. Sebaliknya, *Owasp Zap* lebih terfokus pada kerentanan yang terdapat pada *layer* aplikasi web, terutama terkait konfigurasi *header* keamanan yang dapat dieksploitasi melalui serangan berbasis browser seperti *XSS* dan *clickjacking*. Mitigasi terhadap kerentanan yang ditemukan mampu mengurangi tingkat kerentanannya secara signifikan, dengan pengurangan sebesar 90% pada *Nuclei* dan 80% pada *Owasp Zap*. Kedua tools ini menunjukkan akurasi yamg tinggi serta waktu pemindaian yang efisien, menjadikannya sebagai solusi efektif dalam meningkatkan keamanan baik pada jaringan maupun aplikasi. Penelitian ini merekomendasikan integrasi kedua tools tersebut dalam strategi keamanan siber yang menyeluruh untuk melindungi integritas dan ketersediaan sistem, serta untuk merespons ancaman yang terus berkembang, sesuai dengan prinsip keamanan berlapis yang dianjurkan dalam literature terkini.

Kata kunci: *Cybersecurity*, *Nuclei*, *Owasp Zap*, *Vulnerability Scanner*, *Website Security*

ABSTRACT

Web-based platform security is an important aspect that developers must consider. However, numerous developer still exhibit insufficient attention to enhancing the security level of their websites, thereby increasing the likelihood of these platforms becoming targets of cyber attacks. To address this challenge, the utilization of tools such as Nuclei Vulnerability Scnner and Owasp Zap presents an effective solution for the rapid detection of potential vulnerabilities in web-based platforms. This research involved testing a locally developed dummy web application , with scanning processes conducted using the Nuclei Vulnerability Scanner and Owasp Zap tools. The findings reveal that Nuclei Vulnerability Scanner proves effective in identifying vulnerabilities at the network layer, particularly in relation to SSL/TLS protocols and proxy configurations. In contrast, Owasp Zap is more focused on detecting vulnerabilities within the web application layer, especially concerning security header configurations that may be exploited through browser-based attacks such as XSS and clickjacking. Mitigation of the identified vulnerabilities resulted in a substantial reduction in their severity, with a 90% decrease in Nuclei and an 80% reduction in Owasp Zap. Both tools demonstrated high accuracy and efficient scanning times, establishing them as effective solutions for enhancing security across both network and application layers. This study recommends the integration of these tools into a comprehensive cyber security strategy to safeguard system integrity and availability while addressing the continuously evolving

threat landscape, in alignment with the layered security principle advocated in contemporary literature.

Keywords: *Cybersecurity*, *Nuclei*, *Owasp Zap*, *Vulnerability Scanner*, *Website Security*

Histori Artikel
Diserahkan: 14 Okt 2024 Diterima setelah Revisi: 27 Mei 2025 Diterbitkan: 11 Juni 2025

1. PENDAHULUAN

Keamanan situs web merupakan aspek yang sangat penting dalam proses perancangan sebuah situs. Meskipun demikian, masih banyak ditemui pengembang yang kurang cermat dalam meningkatkan perlindungan situs yang mereka bangun. Sebagai praktik terbaik, pengembang situs seharusnya mengimplementasikan mekanisme keamanan yang memadai sejak tahap perancangan awal, mengingat kemungkinan situs yang telah dibangun akan menjadi sasaran serangan oleh pihak yang berniat merusak. Selain itu, pengembang situs juga perlu secara aktif mengikuti perkembangan tren serangan terbaru agar dapat menjaga integritas dan melakukan perbaikan terhadap situs mereka guna menghindari potensi ancaman yang tidak diinginkan [1].

Sebuah situs web memerlukan tingkat keamanan yang tinggi guna mencegah kebocoran, manipulasi, penghapusan, perubahan, dan pencurian data, serta pemindahan hak pengelolaan yang dapat disebabkan oleh pihak-pihak yang tidak bertanggung jawab. Dalam era kemajuan teknologi yang pesat, situs web memiliki berbagai potensi kerentanannya, yang dapat dimanfaatkan oleh pihak yang berniat merusak, sehingga menjadikannya sasaran yang rentan terhadap berbagai bentuk serangan [1], [2].

Bentuk serangan yang paling umum terjadi pada aplikasi web meliputi *Malware*, *Penetration Testing*, *SQL Injection*, dan lainnya. Penyebab utama dari sebagian besar kerentanan yang teridentifikasi dalam aplikasi web adalah input yang tidak diperiksa, yang diakui sebagai faktor penyebab paling sering muncul. Berdasarkan data terbaru dari WPScan pada tahun 2022, jumlah kerentanan baru yang terdeteksi menunjukkan peningkatan signifikan dalam beberapa tahun terakhir. Pada tahun 2021, lebih dari 5.600 kerentanan baru teridentifikasi, dan pada tahun 2022, terdapat tambahan lebih dari 78 kerentanan baru yang ditemukan [3].

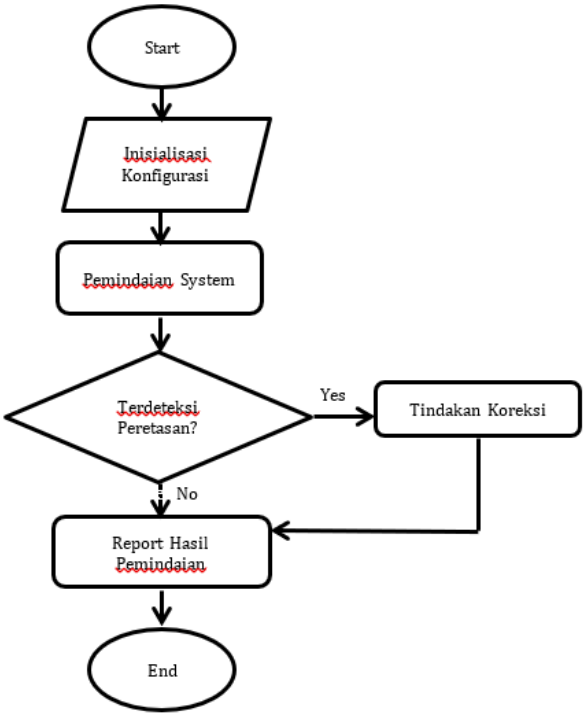
Seiring dengan pesatnya perkembangan teknologi, terjadi perubahan yang terus-menerus dalam ekosistem keamanan informasi. *Nuclei Vulnerability Scanner* telah memperoleh popularitas sebagai alat pemindaian keamanan yang efektif dalam mendeteksi kerentanan pada aplikasi web dan infrastruktur [4]. Dalam sebuah artikel yang berjudul *The Ultimate Guide to Finding Bugs With Nuclei*, yang dikembangkan oleh *Project Discovery*, dijelaskan bahwa *Nuclei* memanfaatkan template yang dapat disesuaikan untuk mengidentifikasi potensi kerentanan keamanan [16].

2. METODE

Jenis penelitian ini menggunakan metode kuantitatif bersifat umum/universal serta menggunakan metode *ethical hacking* dimana nantinya akan di fokuskan pada tahapan *footprinting* dan *vulnerability scanning* [5]. *Ethical hacking* adalah teknik yang digunakan untuk mengidentifikasi kelemahan dan kerentanan dalam sistem komputer atau jaringan. Ini adalah cara untuk mengetahui kelemahan dalam suatu sistem untuk menggambarkan prosedur [6]. Adapun skenario pengujian dan analisis sistem adalah dengan melakukan *footprinting* yaitu proses pengumpulan informasi tentang suatu sistem komputer atau jaringan dengan tujuan untuk mengidentifikasi potensi kerentanan keamanan atau celah yang dapat dimanfaatkan [7]. Selanjutnya dengan melakukan scanning menggunakan *vulnerability scanning* untuk menemukan dan menganalisis kerentanan keamanan yang mungkin ada dalam lingkungan tersebut. Proses ini melibatkan pemindaian sistem atau jaringan untuk mencari kerentanan yang dapat dieksploitasi oleh penyerang. Pada tahapan akan dilakukan pengumpulan informasi *vulnerability* dengan memanfaatkan *tools Nuclei Vulnerability Scanner* untuk mengetahui serangan yang dapat terjadi terhadap kerentanan website yang ada [8]. Setelah itu, dilakukan proses analisis untuk mendapatkan wawasan, pemahaman, atau kesimpulan yang lebih mendalam mengenai suatu masalah, situasi, fenomena, atau topik tertentu. Alur rancangan sistem dapat dilihat pada gambar 1.

3. HASIL DAN PEMBAHASAN

Setelah melakukan pemindaian pada sebuah situs dummy berbasis lokal yang dibangun secara khusus untuk simulasi pemindaian kerentanan keamanan, *Nuclei VulnerabilityScanner* berhasil mendeteksi



Gambar 1. *Flowchart* Rancangan Sistem

sejumlah kerentanan keamanan. Ini termasuk kerentanan umum seperti *SQL injection*, *XSS* [3], [9]. Hasil pemindaian tersebut direkam dalam laporan yang menyediakan rincian tentang kerentanan yang ditemukan, tingkat keparahan, dan rekomendasi penanganan. Tinjau kerentanan yang ditemukan dan kategorikan kerentanannya sesuai dengan tingkat kerentanannya. Kategori yang dapat digunakan seperti *informational* yaitu kerentanan yang muncul karena kurangnya informasi yang terdapat dalam sistem, *low* yaitu kerentanan tidak memungkinkan penyerang untuk mengakses atau memanfaatkan informasi sensitif atau mengambil kendali penuh atas sistem [9]. *Medium* yaitu kerentanan dengan potensi dampak yang lebih signifikan, tetapi masih butuh akses atau tindakan kondisi tertentu untuk eksploitasi sepenuhnya serta *high* yaitu Kerentanan dengan dampak yang serius dan memungkinkan penyerang untuk mendapatkan akses atau mengambil kendali penuh atas sistem yang relatif mudah [10]. Pada table 1 dapat dilihat jenis kerentanan yang ditemukan pada hasil deteksi menggunakan *vulnerability scanner* sementara hasil deteksi menggunakan *Owasp Zap* dapat dilihat pada tabel 2.

Tabel 1. Jenis dan Kategori Kerentanan Yang Ditemukan pada *Nuclei Vulnerability Scanner*

Kerentanan	Tingkat Resiko	Solusi/Mitigasi	Waktu Pemindaian (Deteksi)	True Positif Rate (%)	False Positif Rate (%)	Keakuratan Pemindaian	Pengurangan Jumlah Kerentanan Setelah Mitigasi
Open-Proxy-External	Medium	*Firewall* konfigurasi, pemindaian rutin	2-5 menit	95%	5%	Tinggi	90%
Mistached-SSL-Certificate	Low	Ganti *cipher* suite lebih kuat, pemindaian rutin	2-3 menit	90%	10%	Tinggi	85%
Weak-Cipher-Suites-1.1	Low	Sesuaikan konfigurasi SSL, pembaruan sistem SSL	3-5 menit	92%	8%	Tinggi	80%
Open-Ssl-	Information	Update	1-3 menit	85%	15%	Sedang	70%

Kerentanan	Tingkat Resiko	Solusi/Mitigasi	Waktu Pemindaian (Deteksi)	True Positif Rate (%)	False Positif Rate (%)	Keakuratan Pemindaian	Pengurangan Jumlah Kerentanan Setelah Mitigasi
Detect		*OpenSSL*, pemindaian menyeluruh					

Tabel 2. Jenis dan Kategori Kerentanan Yang Ditemukan Pada *Owasp Zap*

Kerentanan	Tingkat Resiko	Solusi/Mitigasi	Waktu Pemindaian (Deteksi)	True Positif Rate (%)	False Positif Rate (%)	Keakuratan Pemindaian	Pengurangan Jumlah Kerentanan Setelah Mitigasi(%)
X-Content-Type-Options Header Missing	Low	*Aktifkan X-Content-Type-Options di .htaccess untuk mencegah MIME sniffing*	*10 menit*	*85*	*10*	*87*	*75*
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	*,Konfigurasi server untuk menyembunyikan versi server HTTP*	*10 menit*	*90*	*5*	*92*	*80*
Missing Anti-clickjacking Header	Medium	*Tambahkan header X-Frame-Options untuk mencegah clickjacking*	*10 menit*	*80*	*15*	*83*	*70*
Content Security Policy(CSP) Header Not Set	Medium	*Implementasi CSP header untuk membatasi sumber resource,*	*10 menit*	*78*	*12*	*80*	*68*

Pada tabel 1 memperlihatkan hasil pemindaian kerentanan yang dilakukan menggunakan *Nuclei Vulnerability Scanner*, yang khusus menyoroti deteksi kerentanan pada lapisan protokol jaringan, terutama terkait konfigurasi SSL/TLS dan akses proxy. Kerentanan *Open-Proxy-External* dikategorikan sebagai resiko sedang (medium), yang mengindikasikan potensi ancaman signifikan apabila tidak dilakukan mitigasi tepat, karena celah tersebut dapat dimanfaatkan untuk serangan *man-in-the-middle* dan eksfiltrasi data. Metode pemindaian berbasis template mempercepat proses deteksi dengan mempertahankan tingkat *true positif rate* tinggi dan *false positif rate* rendah, sehingga sangat efisien untuk pemindaian cepat dalam infrastruktur jaringan [11]. Selain itu, kerentanan terkait *Mistached-SSL-Certificate* dan *Weak-Cipher-Suites-1.1,* meskipun diklasifikasikan sebagai risiko rendah, tetap relevan untuk ditangani mengingat kelemahan dalam konfigurasi SSL/TLS berpotensi digunakan untuk melakukan serangan *downgrade* dan *intercept*. Konfigurasi protokol SSL yang tidak optimal adalah salah satu vektor serangan yang paling sering dieksploitasi oleh pelaku serangan siber, sehingga pembaruan *chipper suite* dan pemeliharaan SSL secara berkala menjadi langkah mitigasi yang wajib dilakukan [12]. Hasil pemindaian *Nuclei* menunjukkan efisiensi pemindaian dengan rentang waktu 1 hingga 5 menit per sesi deteksi, serta tingkat *true positive rate* yang mencapai 95%. Pendekatan berbasis template yang dilakukan oleh *Nuclei* dapat mengoptimalkan keseimbangan antara kecepatan pemindaian dan akurasi hasil deteksi, sehingga sangat sesuai untuk lingkungan TI yang dinamis. Meskipun terdapat *false positive rate* yang masih muncul dalam angka 5-15%, efektifitas mitigasi yang

tercatat mampu mengurangi kerentanan hingga 90%. Hal ini menunjukkan bahwa *Nuclei* tidak hanya mampu mengidentifikasi kerentanan secara tepat, tetapi juga mendukung proses perbaikan yang signifikan, sesuai dengan prinsip *continuous monitoring* dan *layered security* yang dianjurkan dalam literatur keamanan siber terkini [13]. Secara keseluruhan, hasil pemindaian *Nuclei Vulnerability Scanner* menjelaskan bahwa *tools* ini efektif dalam melakukan deteksi cepat dan akurat terhadap kerentanan jaringan utama, sehingga menkadi komponen penting dalam strategi pertahanan siber modern untuk menjaga integritas dan ketersediaan sistem TI [14].

Pada tabel 2 menunjukkan hasil pemindaian kerentanan yang ditemukan menggunakan *Owasp Zap* secara khusus menargetkan kelemahan konfigurasi header keamanan pada aplikasi web. Kerentanan ini penting untuk diatasi karena berkontribusi pada risiko serangan berbasis browser seperti MIME, *sniffing*, *clickjacking*, dan *cross-site scripting* (XSS), yang sering menjadi vector serangan utama pada aplikasi web modern [15]. Hasil analisis risiko menunjukkan bahwa mayoritas kerentanan memiliki tingkat risiko rendah hingga sedang yang sesuai dengan sifat konfigurasi *header* yang berfungsi sebagai *layer* pertahanan tambahan, namun dapat menjadi pintu masuk bagi serangan apabila tidak di konfigurasi dengan benar [16]. Dalam konteks ini, penerapan header keamanan seperti X-Content-Type-Options dan X-Frame-Options merupakan penerapan terbaik yang terbukti efektif untuk memperkuat keamanan apikasi dan mengurangi pemaparan terhadap serangan berbasis browser [16] [17]. Untuk waktu pemindaian, *Owasp Zap* memerlukan waktu sekitar 10 menit untuk mendeteksi setiap kerentanan. Hal ini mencerminkan kompleksitas pengujian pada *layer* aplikasi dibandingkan dengan pemindaian jaringan [15]. Tingkat true positive rate yang dicapai berada pada 78% hingga 90% sementara *false positive rate* sekitar 5% hingga 15%. Hal ini menunjukkan bahwa hasil pemindaian cukup akurat namun tetap membutuhkan validasi manual oleh tim keamanan [12], [16]. Efektifitas mitigasi terlihat dari kemampuan mengurangi jumlah kerentanan hingga 68%-80%, yang menegaskan pentingnya konfigurasi *header* HTTP yang tepat sebagai bagian dari strategi keamanan aplikasi secara menyeluruh [11], [13]. Penelitian terkini menekankan bahwa pengujian keamanan yang kontinu dan terintegrasi dalam siklus pengembangan aplikasi (*DevSecOps*) sangat krusial untuk mempertahankan ketahanan aplikasi terhadap ancaman yang berkembang secara dinamis [15]. Dari hasil pemindaian secara menyeluruh dapat dilihat bahwa *Owasp Zap* efektif dalam mengidentifikasi dan membantu mitigasi kerentanan pada konfigurasi keamanan aplikasi web, serta disarankan untuk integrasi dalam proses pengembangan dan operasional aplikasi guna memastikan kemanan menggunakan *layer* yang tetap terjaga [16].

4. KESIMPULAN

Berdasarkan hasil peneilitian yang dilakukan dapat disimpulkan bahwa tools *nuclei vulnerability scanner* dan *Owasp Zap* memiliki fokus dan kegunaan yang berbeda, namun keduanya efektif dalam mendeteksi kerentanan di berbagai layer pada sistem. *Nuclei* yang fokus pada pemindaian jaringan, sangat efisien dalam mendeeksi kerentanan pada protokol SSL/TLS dan konfigurasi *proxy* dengan cepat dan akurat. Meskipun terdapat *false positive rate,* alat ini memiliki tingkat deteksi yang tinggi dan mendukung mitigasi yang signifikan terhadap kerentanannya. Hal ini membuat *Nuclei* menjadi *tools* yang tepat untuk pemindaian dalam infrastruktur jaringan, terutama dalam menangani risiko yang terkait dengan serangan man-in-the-middle dan kebocoran data sensitive. Sementara *Owasp Zap* lebih fokus pada keamanan aplikasi web dengan mendeteksi kerentanan pada konfigurasi header keamanan yang melindungi aplikasi dari serangan berbasis browser seperti *clickjacking* dan *XSS*. Meskipun waktu pemindaian lebih lama dibandingkan *Nuclei*, *Owasp Zap* sangat efektif dalam membantu mengidentifikasi kerentanan aplikasi web dan mendukung mitigasi risiko yang relevan. Alat ini sangat penting untuk diterapkan dalam siklus pengembangan aplikasi yang mengintegrasikan keamanan secara berkelanjutan *(DevSecOps).* Secara keseluruhan, integrasi kedua alat ini dalam startegi keamanan siber memberikan pendekatan holistik yang efektif dalam melindungi baik *layer* pada jaringan maupun aplikasi.

DAFTAR PUSTAKA

[1] A. F. Hasibuan and D. Handoko, “Analisis Keretanan Website Dengan Aplikasi Owasp Zap,” *J. Ilmu Komput. dan Sist. Inf.*, vol. 2, no. 2, pp. 257–270, 2023, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/51

[2] P. Gymnastiar, “Analisis Keamanan dan Pengujian Access Control pada Website Pendidikan :

Studi Kasus di Universitas Hamzanwadi Lombok," pp. 951–959, 2024.
[3] T. Anugrah, "Penetration Testing Keamanan Website Stie Samarinda Menggunakan Teknik Sql Injection Dan Xss," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 1, pp. 618–624, 2024, doi: 10.23960/jitet.v12i1.3882.
[4] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *J. Inf. dan Teknol.*, vol. 4, no. 1, pp. 70–75, 2022, doi: 10.37034/jidt.v4i1.190.
[5] A. Kendek Allo and I. R. Widiasari, "Analisis Keamanan Website SIASAT Menggunakan Teknik Footprinting dan Vulnerability Scanning," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 8, no. 2, pp. 316–323, 2024, doi: 10.35870/jtik.v8i2.1723.
[6] M. Munjal, "Ethical Hacking: an Impact on Society," *Cyber Times Int. J. Technol. Manag.*, vol. 7, no. 04, pp. 922–931, 2014.
[7] M. Tahir and M. Risky, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)," vol. 09, pp. 118–125, 2024.
[8] E. Z. Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *J. Sist. Inf. Bisnis*, vol. 12, no. 1, pp. 36–44, 2022, doi: 10.21456/vol12iss1pp36-44.
[9] A. P. Armadhani, D. Nofriansyah, and K. Ibnutama, "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 2, p. 80, 2022, doi: 10.53513/jis.v21i2.6119.
[10] J. I. Sains, "ANALISIS KEAMANAN APLIKASI WEB MENGGUNAKAN ZAP Yuswandi," vol. 6, no. 4, pp. 39–42, 2022.
[11] M. Ozkan-okay, A. A. Yilmaz, E. Akin, A. Aslan, and S. S. Aktug, "A Comprehensive Review of Cyber Security Vulnerabilities ," *Electronics*, vol. 12, no. 1333, 2023.
[12] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, "Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques," *IEEE Access*, vol. 12, pp. 27530–27555, 2024, doi: 10.1109/ACCESS.2024.3367232.
[13] S. Abdelkader *et al.*, "Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks," *Results Eng.*, vol. 23, no. July, p. 102647, 2024, doi: 10.1016/j.rineng.2024.102647.
[14] M. S. Ummah, "No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析 Title," *Sustain.*, vol. 11, no. 1, pp. 1–14, 2019, [Online]. Available: http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI
[15] J. Shahid, M. K. Hameed, I. T. Javed, K. N. Qureshi, M. Ali, and N. Crespi, "A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions," *Appl. Sci.*, vol. 12, no. 8, 2022, doi: 10.3390/app12084077.
[16] M. M. Mlyatu and C. Sanga, "Secure Web Application Technologies Implementation through Hardening Security Headers Using Automated Threat Modelling Techniques," *J. Inf. Secur.*, vol. 14, no. 01, pp. 1–15, 2023, doi: 10.4236/jis.2023.141001.
[17] O. Foundation, "No Title," OWASP Secure Headers Project. [Online]. Available: https://owasp.org/www-project-secure-headers/