Perancangan Sistem Informasi Guna Meningkatkan Efektivitas Koordinasi Dalam Pengolahan Data Antar Kelurahan, Puskesmas, Dan Posyandu Di Wilayah Rancabolang

1st Michelle Ananda Putri
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
michelleaps@student.telkomuniversity.ac.id

2nd Sofia Naning Hertiana
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
sofiananing@telkomuniversity.ac.id

3rd Sri Astuti
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
sriastuti@telkomuniversity.ac.id

***Abstrak* — Penelitian ini mengkaji pemanfaatan teknologi informasi untuk meningkatkan koordinasi layanan kesehatan di Kelurahan Rancabolang, Bandung. Fokus utamanya adalah pengembangan sistem informasi terintegrasi antara kelurahan, puskesmas, dan posyandu untuk mengatasi masalah akses dan pengelolaan data. Metodologi penelitian meliputi studi literatur, instalasi perangkat lunak, dan pengujian keamanan website menggunakan OWASP ZAP. Hasil pengujian mengungkapkan berbagai tingkat kerentanan keamanan, mulai dari informational hingga high, dengan analisis rinci untuk setiap kategori. Temuan ini menyoroti pentingnya perbaikan keamanan berkelanjutan dalam pengembangan sistem informasi kesehatan terintegrasi.**

***Kata kunci* — Teknologi, Informasi, Integrasi, Keamanan, Data, Website, OWASP ZAP**

I. PENDAHULUAN

Di Indonesia, terdapat program seperti posyandu yang bertujuan untuk menyediakan pelayanan kesehatan yang memadai bagi penduduknya. Namun, kendala yang muncul adalah kurangnya kesempurnaan dalam sistem koordinasi yang menghubungkan puskesmas, posyandu, dan kelurahan sekitarnya, yang dapat menghambat kelancaran pelayanan masyarakat. Untuk mengatasi permasalahan ini, teknologi informasi dapat dimanfaatkan. Dalam konteks pemanfaatan teknologi, pemahaman dan efektivitas penggunaan dalam pengembangan sistem informasi sangatlah krusial. Sistem informasi yang efektif akan secara signifikan memfasilitasi koordinasi, terutama dalam konteks kesehatan.

Kelurahan Rancabolang, yang terletak di kota Bandung, menyediakan layanan kesehatan kepada warga sekitarnya melalui puskesmas dan posyandu. Namun terdapat beberapa masalah, data masyarakat yang selama ini dimiliki tidak dapat diakses oleh pihak kelurahan. Hal tersebut disebabkan karena akses informasi yang dimiliki tidak terintegrasi antara kelurahan, puskesmas dan posyandu. Selain itu tidak tersedianya platform yang dapat dikelola secara bersama untuk mempermudah proses koordinasi. Sehingga beberapa program kerja terkait pelayanan yang telah disusun tidak dapat berjalan dengan baik, karena proses koordinasi tidak terkomunikasikan. Hal ini menunjukkan perlunya melakukan pembaruan data dengan lebih teliti. Selain itu, ada keadaan di mana puskesmas memerlukan data atau laporan dengan segera, tetapi proses ini memakan waktu yang lama karena data masih dicatat dan dicari secara manual. Tambahan, terdapat hambatan di mana kelurahan hanya memiliki data mengenai jumlah total penduduk tanpa rincian yang lengkap.

Penggunaan metode manual dalam pencatatan data memiliki potensi kesalahan, terutama dalam hal pertukaran data antara kelurahan Rancabolang, puskesmas Rancabolang, dan posyandu di wilayah tersebut. Untuk mengurangi potensi kesalahan yang mungkin terjadi, diperlukan perubahan yang signifikan dalam proses pengolahan data tersebut. Namun, perlu diakui bahwa penting untuk meningkatkan kualitas dari berbagai aspek, termasuk sumber daya manusianya. Dengan adanya peningkatan kompetensi tenaga kerja akan memastikan bahwa teknologi yang diimplementasikan dapat dimanfaatkan dengan maksimal.

II. KAJIAN TEORI

A. WordPress

Di seluruh dunia, WordPress merupakan CMS yang sangat populer dalam pengelolaan konten. Salah satu alasannya platform ini mendapat reputasi adalah karena fleksibilitasnya, kemudahan penggunaan, dan kekayaan ekosistem plugin yang dimilikinya.

1. Fitur Utama WordPress:

a. *Open Source*

Para Pengguna aplikasi dapat menggunakan, memodifikasi, dan mendistribusikan Wordpress secara bebas karena merupakan perangkat lunak *open source* (Rogers, 2019).

b. Plugin dan Tema

Terdapat ribuan plugin dan tema yang bisa digunakan untuk WordPress, sehingga dari pihak pengguna dapat dengan mudah meningkatkan fungsionalitas situs website mereka (Anderson & Smith, 2020).

c. Pengelolaan Konten

Sistem pengelolaan konten WordPress hadir dengan antarmuka yang mudah digunakan, membantu pengguna dalam membuat dan mengatur konten dengan efisiensi (Brown & Johnson, 2018).

d. *SEO Friendly*

Wordpress memiliki struktur yang mendukung optimasi SEO, dengan kesempatan untuk ditingkatkan menggunakan plugin SEO seperti Yoast SEO (White & Green, 2021).

B. WP File Manager WordPress

Plugin WordPress WP File Manager membolehkan pengguna mengatur file file di pelayan mereka menerusi dasbor WordPress.

1. Fitur Utama WP File Manager :

a. Pengelolaan File

Smith (2022) menyatakan bahwa pengguna dapat dengan mudah mengunggah, unduh, edit, dan hapus file.

b. Antarmuka Grafis

Navigasi dan manajemen file dapat dilakukan dengan mudah berkat antarmuka pengguna yang intuitif (Jones, 2021).

c. Keamanan

Brown & Davis (2019) menyatakan bahwa implementasi kontrol akses file yang ketat sangat penting dalam melindungi data sensitif.

C. OWASP ZAP

Para profesional keamanan menggunakan OWASP ZAP (*Zed Attack Proxy*), alat *open-source* untuk pengujian keamanan aplikasi web, guna mengidentifikasi kerentanan dan meningkatkan tingkat keamanannya.

1. Fitur Utama OWASP ZAP :

a. Pemindaian Otomatis

Johnson (2020) menyatakan bahwa pemindaian otomatis dapat digunakan untuk mendeteksi kerentanan umum seperti injection SQL dan XSS (*Cross-Site Scripting*). Selain itu, pemindaian ini mampu memeriksa kerentanan pada banyak titik dalam aplikasi web secara efisien, menghemat waktu bagi penguji keamanan.

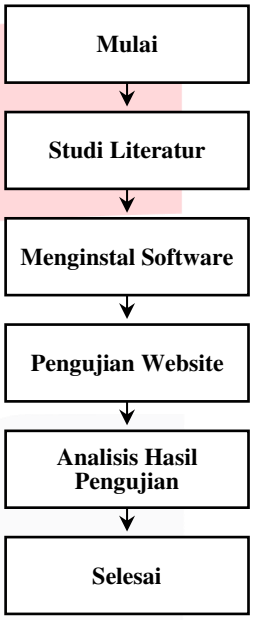
b. *Spidering*

Membuat fitur pemetaan aplikasi web agar pengguna dapat menemukan semua halaman dan fungsi yang tersembunyi. Spidering membantu dalam mengidentifikasi struktur dan hubungan antar halaman, yang sering kali tidak terlihat melalui penelusuran manual biasa. (White & Green, 2018).

c. *Intercepting Proxy*

Pengguna dapat memantau dan mengubah lalu lintas HTTP/HTTPS guna melakukan analisis keamanan (Rogers & Smith, 2021). itur ini memberikan kemampuan untuk menangkap dan memodifikasi permintaan dan respons, memungkinkan penguji keamanan untuk melakukan pengujian yang lebih mendalam dan menemukan kerentanan yang tersembunyi.

III. METODE



GAMBAR 1
Metode

A. Studi Literatur

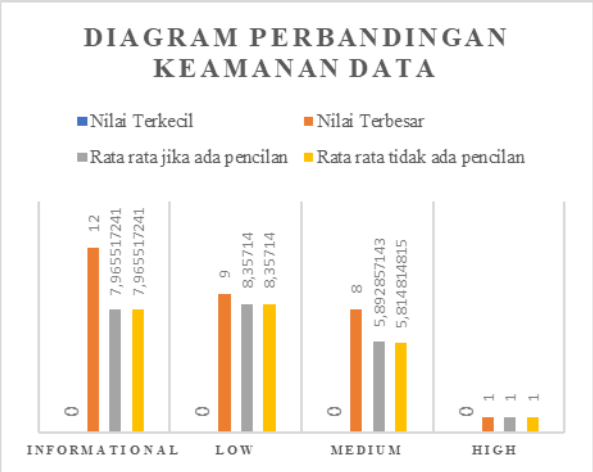
Studi literatur adalah tahapan awal yang dilakukan untuk memahami konsep dasar, teknik dan alat yang akan digunakan dalam pengujian keamanan web. Pada tahap ini, pencarian informasi dilakukan melalui berbagai sumber seperti jurnal, artikel dan dokumentasi dari OWASP ZAP. Tujuannya untuk mendapatkan landasan teori yang kuat dan memahami praktik terbaik dalam menggunakan OWASP ZAP untuk mengidentifikasi kerentanan keamanan pada website.

B. Menginstal Software

Menginstal software OWASP ZAP versi terbaru pada perangkat yang akan digunakan. Proses instalasi mencakup mengunduh installer dari situs resmi OWASP, menjalankan file instalasi dan mengikuti petunjuk yang diberikan untuk menyelesaikan instalasi. Pastikan perangkat yang digunakan memenuhi spesifikasi minimum yang diperlukan untuk menjalankan OWASP ZAP dengan optimal.

C. Pengujian Website

Pengujian website menggunakan OWASP ZAP dilakukan untuk mengidentifikasi kerentanan keamanan pada website. OWASP ZAP sebagai alat pengujian keamanan yang menyediakan berbagai fitur untuk melakukan testing secara otomatis dan manual. Proses pengujian mencakup URL situs web sebagai target pengujian dengan opsi pemindaian menggunakan "spider". ZAP melakukan pemindaian otomatis terhadap situs web target seperti gambar dibawah ini.



GAMBAR 2
Proses pengujian website menggunakan OWASP ZAP

D. Hasil Pengujian dan Analisis

Hasil pengujian keamanan website menggunakan OWASP ZAP menunjukkan beberapa temuan penting yang perlu diperhatikan. Analisis yang dilakukan mengungkapkan adanya beberapa kerentanan dengan tingkat keparahan yang bervariasi.

IV. HASIL DAN PEMBAHASAN

A. Hasil Pengujian Berdasarkan Aspek Keamanan Data

Dalam aspek ini, pengujian dilakukan untuk mengidentifikasi tingkat kerentanan keamanan yang ada didalam sistem informasi dan menguji potensi eksploitasi dari kerentanan yang ditemukan menggunakan *Open Web Application Security Project Zed Attack Proxy*. Pengujian ini bertujuan untuk memastikan bahwa semua celah keamanan dapat diidentifikasi dan diperbaiki sebelum digunakan oleh pihak tidak bertanggung jawab. Dengan demikian, sistem informasi dapat lebih terlindungi dari serangan siber yang berpotensi merugikan.

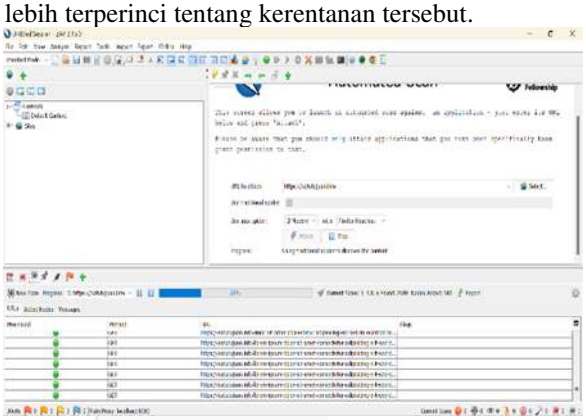
PENGUJIAN KEAMANAN DATA

Pengujian	Tanggal Pengujian	Waktu Pengujian	Risk			
			Informational	Low	Medium	High
1	22 Mei 2024	20:07	12	9	7	1
2	23 Mei 2024	16:14	10	9	7	1
3	24 Mei 2024	12:06	9	9	6	1
4	24 Mei 2024	16:00	10	9	7	1
5	24 Mei 2024	21:28	9	9	7	1
6	24 Mei 2024	22:23	9	9	6	1
7	24 Mei 2024	22:30	9	9	6	1
8	24 Mei 2024	23:47	7	8	5	1
9	25 Mei 2024	00:20	7	8	5	1
10	25 Mei 2024	08:32	8	9	6	1
11	25 Mei 2024	10:47	6	8	5	1
12	25 Mei 2024	11:56	6	8	5	1
13	25 Mei 2024	13:45	8	9	6	1
14	25 Mei 2024	16:26	7	7	5	1
15	25 Mei 2024	17:36	5	8	5	1
16	25 Mei 2024	18:50	6	7	5	1
17	25 Mei 2024	20:18	8	9	6	1
18	25 Mei 2024	21:29	8	9	6	1
19	25 Mei 2024	23:12	8	9	6	1
20	26 Mei 2024	01:06	8	9	6	1
21	26 Mei 2024	10:29	8	9	6	1
22	26 Mei 2024	12:15	8	9	6	1
23	26 Mei 2024	13:14	8	9	6	1
24	26 Mei 2024	15:05	8	9	6	1
25	26 Mei 2024	16:49	8	9	6	1
26	26 Mei 2024	18:48	8	9	6	1
27	26 Mei 2024	20:35	8	9	6	1
28	26 Mei 2024	23:24	6	8	5	1
29	27 Mei 2024	15:35	10	9	7	1
30	27 Mei 2024	16:09	9	9	7	1

GAMBAR 3
Pengujian 30 kali menggunakan OWASP

B. Analisis

OWASP ZAP digunakan untuk melakukan pengujian keamanan data pada website. Pengujian keamanan data website menggunakan OWASP ZAP memberikan hasil yang signifikan dengan berbagai tingkat penilaian kerentanan: informational, low, medium dan high Di bawah ini adalah penjelasan yang lebih terperinci tentang kerentanan tersebut.



GAMBAR 4
Diagram perbandingan dari 4 kerentanan

1. Informational

Pada tingkat penilaian informational, beberapa temuan mencakup berbagai aspek seperti :

a. *Authentication Request Identified*

Bukti menunjukkan adanya permintaan autentikasi yang bisa dieksploitasi untuk serangan brute force. Serangan brute force melibatkan penyerang dalam mencoba semua kemungkinan kombinasi kata sandi untuk menemukan yang benar. Pentingnya mengidentifikasi permintaan autentikasi adalah untuk memastikan penerapan mekanisme perlindungan yang benar, seperti pembatasan jumlah percobaan login atau penguncian akun.

b. *Charset Mismatch*

Ada kesalahan yang terjadi karena perbedaan charset antara yang ditentukan dan data aktual, sehingga karakter mungkin diinterpretasikan dengan salah. Ketidaksesuaian tersebut bisa mengakibatkan

kerusakan data atau kebingungan pengguna, terutama saat menggunakan karakter non-ASCII.

c. Cookie Poisoning

Dapat diperlihatkan bahwa pengguna memiliki kemampuan untuk memodifikasi cookie, yang dapat mengakibatkan data bocor atau peningkatan hak akses yang tidak sah. Cookie poisoning mengacu pada teknik di mana penyerang memanipulasi data dalam cookie untuk mendapatkan akses yang tidak sah atau mencuri informasi sensitif.

d. Information Disclosure-Suspicious Comments

Ada komentar yang mencurigakan dalam kode sumber yang dapat mengungkapkan informasi sensitif. Penyerang dapat memperoleh pemahaman dan mengeksploitasi sistem jika mereka memiliki akses ke komentar yang berisi informasi tentang struktur aplikasi, *bug* yang diketahui, atau catatan pengembang.

e. *Modern Web Application*

Penggunaan teknologi web modern yang mungkin tidak sepenuhnya diketahui atau dijalankan dengan kesejahteraan. Banyak teknologi baru seperti SPA (Single Page), (Applications), WebSockets, dan API yang masih rentan atau belum diimplementasikan dengan baik dalam hal keamanannya. Kerentanan ini dapat dimanfaatkan oleh penyerang untuk menyusup ke dalam sistem, mencuri data sensitif, atau merusak layanan. Oleh karena itu, penting untuk menerapkan praktik keamanan terbaik dan rutin melakukan pengujian serta pembaruan keamanan.

f. Re-examine Cache-control Directives

Jika pengaturan cache control tidak tepat, ada risiko data sensitif akan tetap tersimpan dalam cache. Kesalahan dalam pengaturan cache bisa mengakibatkan penyimpanan informasi pribadi atau data sesi entah di perangkat pengguna maupun di server perantara, sehingga dapat diakses oleh individu yang tidak berwenang.

g. *Retrieved from Cache*

Masalah ini dapat menyebabkan masalah keamanan, menandakan bahwa konten diambil dari cache. Jika data sensitif diambil dari cache, maka terdapat risiko bahwa informasi tersebut tidak akan diperbarui atau dihapus sesuai dengan kebutuhan keamanan.

h. *Session Management Response Identified*

Hal ini menunjukkan bahwa penyerang dapat memanfaatkan respons dari pengelolaan sesi. Kegagalan dalam melakukan manajemen sesi dengan baik, termasuk ketidakteraturan dalam memvalidasi token sesi yang tepat, bisa menjadi penyebab utama terjadi peretasan pada sesi pengguna.

i. *User Agent Fuzzer*

Alat ini meretest berbagai user agent untuk mengidentifikasi kelemahan dalam pengelolaan sesi atau autentikasi. Membantu mengidentifikasi respon aplikasi web terhadap user agent yang berbeda, penggunaan user agent fuzzer dapat menemukan kelemahan dalam keamanan.

j. *User Controllable HTML Element Attribute*

Pengguna dapat mengontrol elemen HTML yang berpotensi menyebabkan XSS *(Cross-Site Scripting).* Jika pengguna memiliki kontrol atas atribut HTML, mereka dapat menyuntikkan skrip berbahaya yang akan dieksekusi di browser pengguna lainnya.

Berdasarkan gambar 4, hasil pengujian ini menunjukkan bahwa rata-rata skor keamanan saat terdapat pencilan adalah 7,965 dengan variasi yang relative kecil (dari 0 hingga 12). Ini menandakan bahwa meskipun beberapa titik mungkin rentang, Sebagian besar poin memiliki skor yang cukup tinggi. Konsistensi rata-rata skor keamanan antara kondisi dengan atau tanpa pencilan menunjukkan stabilitas dalam kualitas keamanan.

2. Low

Pada tingkat penilaian low, beberapa temuan mencakup :

a. *Big Redirect Detected (Potential Sensitive Information Leak)*

Kebocoran informasi sensitif dapat disebabkan oleh adanya pengalihan besar yang terdeteksi. Jika tidak terkontrol dengan baik, penyalihan dapat mengarahkan pengguna ke situs jahat yang berisiko mencuri data atau menginfeksi perangkat mereka dengan malware.

b. *Cookie Not Http Only Flag*

Cookie tidak dilindungi dengan atribut HttpOnly sehingga memberikan kerentanan terhadap serangan XSS. Atribut HttpOnly membantu melindungi cookie dari skrip sisi klien, mengurangi peluang terjadinya serangan XSS.

c. Cross-Domain Javascript Source File Inclusion

Menyertakan file JavaScript dari domain yang berbeda dapat memberikan peluang bagi serangan. Mengimpor file JavaScript dari sumber yang tidak dapat dipercaya berpotensi membuka celah bagi serangan skrip lintas situs dan injeksi kode berbahaya.

d. *Server Leaks Information*

Server telah mengungkapkan informasi yang dapat dieksploitasi oleh penyerang untuk tindakan lebih lanjut. Penyerang dapat mendapatkan petunjuk tentang cara menyerang sistem dengan melihat informasi seperti versi perangkat lunak yang digunakan, konfigurasi server, atau pesan kesalahan. Informasi ini dapat memberikan penyerang keuntungan signifikan, memungkinkan mereka untuk merancang serangan yang lebih efektif dan spesifik

e. *Strict-Transport Security Header Not Set*

Jika *Header Strict-Transport-Security* tidak diatur, maka situs menjadi rentan terhadap serangan *man-in-the-middle*. Header ini memaksa browser untuk selalu menggunakan protokol HTTPS, sehingga dapat mengurangi risiko terjadi intersepsi komunikasi.

f. *Timestamp Disclosure*

Stempel waktu yang dapat diungkapkan untuk menganalisis serangan. Penyerang dapat

menggunakan informasi tentang stempel waktu untuk mempelajari pola penggunaan aplikasi dan merancang serangan yang lebih efisien.

g. *X-Content Type Options Header Missing*

Aplikasi menjadi rentan terhadap serangan MIME sniffing karena tidak ada Header *X-Content-Type-Options* yang disertakan. Header ini mencegah browser agar tidak mengartikan file sebagai tipe yang berbeda dari yang telah ditentukan oleh server, dengan tujuan untuk mengurangi risiko serangan MIME sniffing.

Berdasarkan gambar 4, hasil menunjukkan bahwa skor keamanan rata-rata pada kategori ini sedikit melebihi kategori informational dengan angka 8,357 ada atau tidak adanya pencilan. Ini menunjukkan bahwa masalah keamanan pada tingkat *low* umumnya tidak begitu banyak dan dapat diperbaiki dengan mudah. Tidak ada perbedaan signifikan dalam rata-rata skor keamanan antara kondisi dengan atau tanpa pencilan.

3. Medium

Pada tingkat penilaian medium, beberapa temuan mencakup :

a. *CSP (Wildcard Directive)*

Penggunaan karakter wildcard dalam Content Security Policy dapat berpotensi menyebabkan kebocoran data atau rentan terhadap serangan XSS. Penggunaan wildcard dalam CSP dapat memungkinan semua sumber untuk memuat konten, yang berpotensi menyebabkan kebocoran data atau serangan XSS.

b. CSP (Script-src unsafe-inline)

Penggunaan unsafe-inline pada script-src dapat memudahkan serangan XSS. Memperbolehkan penggunaan unsafe-inline dalam CSP berarti potensi adanya skrip inline yang dapat dieksekusi, yang kemudian meningkatkan risiko serangan XSS.

c. *Missing Anti-clickjacking Header*

Tidak adanya header yang melindungi dari clickjacking, bisa membuat situs menjadi rentan terhadap serangan jenis ini. Penggunaan seperti X-Frame-Options pada header dapat mencegah situs dimuat dalam frame, yang mengurangi risiko clickjacking.

d. *Vulnerable JS Library*

Perpustakaan JavaScript ini rentan terhadap penyalahgunaan dan butuh pembaruan. Jika Anda menggunakan pustaka JavaScript yang tidak aman, maka ada risiko terbuka bagi penyerang untuk memanfaatkan kerentanan yang diketahui.

Berdasarkan gambar 4, hasil, ditemukan bahwa rata-rata skor keamanan pada tingkat ini adalah 5,892 ketika terdapat pencilan dan 5,815 jika tidak ada. Hal ini mengindikasikan bahwa masalah keamanan di tingkat ini kemungkinan membutuhkan perhatian lebih dan tindakan pencegahan yang lebih serius. Besar variasi skor menunjukkan keragaman tingkat keamanan di berbagai bagian sistem.

4. High

Pada penilaian tingkat high, satu aspek penilaian yang termasuk dalam kategori ini adalah :

a. PII Disclosure

Pengungkapan PII dapat menyebabkan konsekuensi yang serius dan membutuhkan tindakan segera. Pelanggaran privasi dan pencurian identitas dapat terjadi sebagai dampak dari PII Disclosure, yang menjadikannya kerentanan yang sangat serius dengan potensi konsekuensi hukum bagi organisasi. Namun, hasil dari pengujian menunjukkan bahwa tingkat keamanan high memiliki nilai yang relatif lebih rendah dibandingkan dengan tingkat keamanan lainnya. Mungkin ada potensi masalah yang perlu dipelajari lebih lanjut dari hal ini. Maka, masalah keamanan tingkat high harus menjadi prioritas utama untuk diperbaiki.

Selanjutnya, tingkatan keamanan medium dan low akan diatasi secara berturut-turut setelahnya. Untuk memastikan keseluruhan kekonsistenan dan keandalan sistem, mungkin perlu melanjutkan evaluasi serta membersihkan titik-titik data yang mencurigakan.

V. KESIMPULAN

Penelitian ini mengidentifikasi adanya kebutuhan untuk mengembangkan sistem informasi terintegrasi antara kelurahan, puskesmas, dan posyandu di Kelurahan Rancabolang, Bandung. Tujuannya adalah untuk mengatasi masalah koordinasi dan akses data yang selama ini menghambat pelayanan kesehatan masyarakat. Penggunaan teknologi informasi, khususnya pengembangan website berbasis WordPress, dipilih sebagai solusi untuk mengatasi permasalahan ini.

Pengujian keamanan website menggunakan OWASP ZAP dilakukan untuk mengidentifikasi potensi kerentanan. Hasil pengujian mengungkapkan berbagai tingkat kerentanan, mulai dari informational hingga high, yang memerlukan perhatian dan tindakan perbaikan. Analisis menunjukkan bahwa meskipun kerentanan tingkat high jumlahnya sedikit, namun memiliki potensi dampak yang serius dan harus menjadi prioritas utama untuk diperbaiki.

Kerentanan tingkat medium dan low juga memerlukan perhatian dan perbaikan untuk meningkatkan keamanan sistem secara keseluruhan. Penelitian ini menekankan pentingnya evaluasi keamanan berkelanjutan dan peningkatan kualitas dalam pengembangan sistem informasi kesehatan terintegrasi. Implementasi sistem informasi yang aman dan terintegrasi diharapkan dapat meningkatkan efektivitas koordinasi dan kualitas layanan kesehatan di tingkat kelurahan.

REFERENSI

[1] Baskin, Wade. “On the Dangers of Stochastic Parrots | Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency.” ACM Digital Library, 2018,

[2] Goeminne, M., & Mens, T. (2023). Analyzing ecosystems for open source software developer communities. ISoftware Ecosystems (Issue April 2013).https://doi.org/10.4337/9781781955628.00021

[3] Goeminne, M., & Mens, T. (2023). Analyzing ecosystems for open source software developer communities. In Software Ecosystems (Issue April 2013). https://doi.org/10.4337/9781781955628.00021