Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id

E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November

OPEN ACCESS

https://doi.org/ 10.63447/jmt.v3i2.2130

Analisis Keamanan Sistem Informasi Pada Website Extended E-Ianc Menggunakan Metode PTES, STRIDE, dan CVSS V4.0

Ghefira Putri Nurraya [1], Imam Sutanto [2], Bambang Irawan [3], Hosizah [4*]

[1,2,3,4*] Program Studi Manajemen Informasi Kesehatan, Fakultas Ilmu-Ilmu Kesehatan, Universitas Esa Unggul, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta, Indonesia.

Email: ghefiraputri60@student.esaunggul.ac.id [1], imam.sutanto@esaunggul.ac.id [2], bambang.irawan@esaunggul.ac.id [3], hozisah@esaunggul.ac.id [4*]

Histori Artikel:
Dikirim 17 September 2026; *Diterima dalam bentuk revisi* 10 Oktober 2026; *Diterima* 25 Oktober 2026; *Diterbitkan* 25 November 2026. Semua hak dilindungi oleh Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) STMIK Indonesia Banda Aceh.

Abstrak

Transformasi digital layanan Kesehatan memperluas pemanfaatan sistem informasi berbasis web, namun turut meningkatkan risiko keamanan siber terhadap data pasien yang bersifat sensitif. Extended e-iANC, hasil pengembangan dari Electronic Integrated Antenatal Care yang kini mencakup layanan antenatal, persalinan, nifas, imunisasi, dan keluarga berencana, belum pernah diuji keamanannya secara sistematis. Penelitian ini bertujuan mengukur tingkat keamanan sistem informasi Extended e-iANC terhadap ancaman yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan data pasien. Pengujian menggunakan metode Penetration Testing Execution Standard (PTES) pada lima tahap yaitu, pre-engagement, intelligence gathering, threat modeling, vulnerability analysis, dan reporting, dipadukan dengan pemetaan ancaman STRIDE dan penilaian risiko CVSS v4.0. Hasil pengujian menemukan sepuluh kerentanan, dua berkategori Critical; SQL Injection dan Spring4Shell, dua berkategori High; Path Traversal dan Open Ports, serta enam sisanya berkategori Medium hingga Low. Temuan ini menunjukkan bahwa Extended e-iANC masih memiliki celah keamanan signifikan, sehingga diperlukan mitigasi segera berupa penerapan prepared statement, pembaruan framework, dan segmentasi layanan jaringan guna memperkuat keamanan serta kepatuhan sistem terhadap regulasi perlindungan data kesehatan yang berlaku.

Kata Kunci: : Keamanan Sistem Informasi; Extended E-Ianc; PTES; STRIDE; CVSS v4.0.

Abstract

The growing digitalization of healthcare increases reliance on web-based information systems, raising cybersecurity risks to sensitive patient data. Extended e-iANC, an expanded version of the Electronic Integrated Antenatal Care system now covering antenatal, delivery, postpartum, immunization, and family-planning services, had never undergone systematic security testing. This study evaluates the security level of Extended e-iANC against threats to data confidentiality, integrity, and availability using the Penetration Testing Execution Standard (PTES) across five phases, combined with STRIDE threat modeling and CVSS v4.0 risk scoring. Testing revealed ten vulnerabilities, two rated Critical; SQL Injection and Spring4Shell, two rated High; Path Traversal and Open Ports, and six rated Medium to Low. These results indicate substantial security gaps requiring immediate mitigation, particularly parameterized queries, framework updates, and network segmentation, to strengthen the system's resilience and regulatory compliance.

Keyword: Information System Security; Extended E-Ianc; PTES; STRIDE; CVSS v4.0.

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id

E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November

OPEN ACCESS

https://doi.org/ 10.63447/jmt.v3i2.2130

1. Pendahuluan

Digitalisasi layanan kesehatan mendorong pemakaian sistem informasi berbasis web untuk mencatat dan mengelola data pasien, tetapi juga memperluas celah ancaman siber (Garcia-Perez *et al.*, 2023). Sektor ini menjadi sasaran empuk karena menyimpan data pribadi dan rekam medis bernilai tinggi, sementara sumber daya keamanannya relatif terbatas dibandingkan sektor lain (Ewoh & Vartiainen, 2024). Tinjauan literatur rekam medis elektronik menunjukkan dua pola ancaman dominan, yaitu celah pada arsitektur sistem dan penyalahgunaan kredensial pengguna (Enggar Pramudita Wijayanti & Asti Nurhayati, 2024). Ancaman ini nyata di Indonesia. Pada 2021, data sekitar 279 juta peserta BPJS Kesehatan, yang mencakup NIK, nama, hingga informasi riwayat kesehatan, dilaporkan dijual di forum daring, dan kajian atas kasus tersebut menyimpulkan bahwa lemahnya kontrol akses serta belum optimalnya penerapan standar seperti *ISO 27001* menjadi faktor utama insiden (Nugraha *et al.*, 2021). Di tingkat nasional, hal ini ditegaskan melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mewajibkan setiap pihak pengendali data pribadi, termasuk data kesehatan, menjalankan perlindungan teknis dan organisasional agar data tidak diakses atau dibocorkan tanpa izin (Fauzi *et al.*, 2022), serta diperkuat oleh Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis yang menuntut terpenuhinya prinsip kerahasiaan, integritas, dan ketersediaan pada penyelenggaraan rekam medis elektronik. Objek penelitian ini adalah *Extended e-iANC*, hasil perluasan *Electronic Integrated Antenatal Care* yang kini mencakup layanan antenatal, persalinan, nifas, imunisasi, dan keluarga berencana. Sistem ini dipilih karena tiga alasan. Pertama, ia menyimpan data kesehatan ibu dan anak yang bersifat sangat sensitif dalam satu rangkaian layanan. Kedua, perluasan fungsinya memperbesar *attack surface* sehingga pengujian keamanan berkala tidak dapat ditunda. Ketiga, sistem ini berjalan sebagai sistem produksi yang melayani data kesehatan masyarakat secara langsung, tetapi tingkat keamanannya belum diketahui secara terukur. Penelitian terdahulu telah menerapkan pendekatan-pendekatan yang relevan, tetapi secara terpisah *PTES* terbukti berhasil pada pengujian website instansi pemerintah (Safitra *et al.*, 2023). Untuk memetakan risiko secara lebih terstruktur, banyak penelitian keamanan sistem mengadopsi pendekatan *STRIDE* pada tahap identifikasi ancaman (Widjajarto *et al.*, 2021). Adapun untuk mengukur seberapa parah dampak masing-masing temuan, dibutuhkan metode penilaian yang objektif, di mana *Common Vulnerability Scoring System* (*CVSS*) menjadi acuan yang paling banyak dipakai kalangan praktisi keamanan untuk menyusun prioritas penanganan risiko secara terukur (FIRST.Org, 2023).

Salah satu kerentanan aplikasi web yang terus menjadi sorotan hingga kini adalah *SQL Injection*, mengingat tingkat eksploitasinya pada sistem berbasis basis data masih tergolong tinggi (Abdullayev & Chauhan, 2023). Di luar celah pada level aplikasi, aspek infrastruktur pun patut diwaspadai, yaitu menempatkan beberapa layanan pada satu server yang sama dapat memperlebar *attack surface*, sebab satu layanan yang berhasil dikompromikan berpotensi menjalar ke layanan lain yang berbagi infrastruktur serupa (Hörnemann *et al.*, 2024). Oleh karena itu, memisahkan layanan berdasarkan tingkat sensitivitas datanya melalui segmentasi jaringan terbukti mampu membatasi dampak suatu insiden agar tidak merembet ke seluruh sistem (Baligodugula *et al.*, 2024). Keunikan pendekatan penelitian ini terletak pada keterpaduan tiga metode dalam satu alur. *PTES* menyediakan tahapan pengujian yang dapat ditelusuri dari pengumpulan informasi hingga pelaporan, *STRIDE* memetakan ancaman ke dalam enam kategori, dan *CVSS v4.0* menilai keparahan setiap temuan secara objektif sebagai dasar urutan perbaikan. Pengujian juga mencakup lapisan aplikasi (*SQL Injection*, *Spring4Shell*, *Path Traversal*) dan lapisan infrastruktur (port terbuka, ko-lokasi layanan pada satu server, konfigurasi DNS, dan SSL/TLS). Penelitian ini bertujuan mengukur tingkat keamanan *Extended e-iANC* terhadap ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data pasien, serta merumuskan rekomendasi perbaikan berdasarkan skala prioritas. Secara teoretis, penelitian ini memperkaya penerapan *PTES*, *STRIDE*, dan *CVSS v4.0* pada sistem informasi kesehatan Indonesia. Secara praktis, hasilnya menjadi rujukan bagi pengelola dalam memperkuat keamanan *Extended e-iANC*.

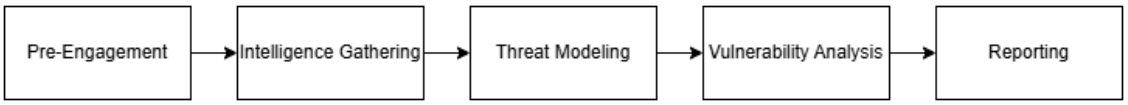
Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

2. Landasan Teori

PTES adalah kerangka pengujian penetrasi yang membagi proses menjadi tujuh tahap, yaitu *pre-engagement interactions*, *intelligence gathering*, *threat modeling*, *vulnerability analysis*, *exploitation*, *post-exploitation*, dan *reporting* (The PTES Team, 2022). Kerangka ini membuat pengujian dapat ditelusuri dan diulang, dan telah diterapkan pada pengujian website pemerintahan (Safitra *et al.*, 2023). Penelitian ini memakai lima dari tujuh tahap, tanpa *exploitation* dan *post-exploitation*, karena objek penelitian adalah sistem produksi. *STRIDE* adalah kerangka pemodelan ancaman yang mengelompokkan ancaman ke dalam enam kategori, yaitu *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service*, dan *Elevation of Privilege*. Setiap kategori melanggar satu properti keamanan, yaitu autentikasi, integritas, nirsangkal, kerahasiaan, ketersediaan, dan otorisasi, sehingga *STRIDE* membantu menghubungkan temuan teknis dengan dampaknya terhadap kerahasiaan, integritas, dan ketersediaan data (Widjajarto *et al.*, 2021). *Common Vulnerability Scoring System* (*CVSS*) adalah standar terbuka untuk menilai keparahan kerentanan. Skor Base (*CVSS-B*) dihitung dari karakteristik kerentanan itu sendiri, yaitu vektor serangan, kompleksitas serangan, prasyarat serangan, hak akses yang dibutuhkan, interaksi pengguna, serta dampak terhadap kerahasiaan, integritas, dan ketersediaan. Skor 0,0–10,0 dikelompokkan menjadi *None*, *Low*, *Medium*, *High*, dan *Critical* (FIRST.Org, 2023). *SQL Injection* masih menjadi kerentanan dengan tingkat eksploitasi tinggi pada sistem berbasis basis data (Abdullayev & Chauhan, 2023), dan parameterisasi kueri serta validasi input telah banyak dibuktikan efektif sebagai mitigasinya (Disawal & Suman, 2023). *Spring4Shell* (CVE-2022-22965) adalah kerentanan eksekusi kode jarak jauh pada aplikasi Spring yang berjalan di JDK 9 atau lebih baru dan memenuhi kondisi tertentu (Database, 2022). Pada tingkat infrastruktur, penempatan beberapa layanan pada satu server memperlebar *attack surface* karena kompromi satu layanan berpotensi menjalar ke layanan lain (Hörnemann *et al.*, 2024), sedangkan segmentasi jaringan berdasarkan sensitivitas data membatasi dampak insiden (Baligodugula *et al.*, 2024).

3. Metode Penelitian

Penelitian ini menggunakan metode kuantitatif, yang bertujuan mengukur dan menggambarkan tingkat keamanan sistem informasi *Extended e-iANC* secara numerik pada satu objek penelitian. Pendekatan ini dipilih karena penelitian ini menghasilkan data terukur berupa skor tingkat keparahan kerentanan yang dapat dianalisis secara objektif, sebagaimana lazim digunakan pada penelitian pengujian keamanan sistem informasi berbasis web (Bunan Imtias *et al.*, 2025). Objek penelitian adalah website *Extended e-iANC*, dengan unit analisis berupa konfigurasi jaringan, aplikasi web, dan layanan pendukung yang dapat diakses secara publik. Pengujian dilaksanakan pada 25–26 Juni 2026 menggunakan perangkat berbasis Windows 10 dengan *Nmap* 7.98 dan *OWASP ZAP* 2.17.0, melalui ISP rumah di Kota Tangerang, Indonesia, terhadap domain e-ianc.id beserta subdomain yang terdeteksi, dengan izin tertulis dari pengelola sistem. Pengujian dilaksanakan dengan menerapkan kerangka kerja *Penetration Testing Execution Standard* (*PTES*), dibatasi pada lima dari tujuh tahap yang tersedia, yaitu *pre-engagement interactions*, *intelligence gathering*, *threat modeling*, *vulnerability analysis*, dan *reporting*. Tahap *exploitation* dan *post-exploitation* tidak dilakukan karena penelitian ini bersifat non-destruktif dan tunduk pada batasan etika penelitian, mengingat objek penelitian merupakan sistem produksi yang melayani data kesehatan masyarakat secara langsung. Alur kelima tahap tersebut disajikan pada Gambar 1.



Gambar 1. Model Proses Penelitian

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

Pada tahap *pre-engagement*, dilakukan penetapan ruang lingkup, batasan aktivitas, serta pengambilan izin tertulis dari pengelola sistem sebelum pengujian dilaksanakan. Tahap *intelligence gathering* dilakukan melalui pengumpulan data pasif dan semi-pasif berupa informasi Whois, analisis DNS record, pemetaan subdomain, serta pemindaian port dan layanan yang terbuka. Tahap *threat modeling* dilakukan dengan memetakan potensi ancaman menggunakan kerangka STRIDE (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*), yang telah terbukti efektif digunakan untuk mengategorikan risiko keamanan sistem secara terstruktur (Widjajarto *et al.*, 2021). Tahap *vulnerability analysis* dilakukan melalui kombinasi pengujian pasif (analisis konfigurasi *security header*, sertifikat SSL/TLS, dan protokol enkripsi) dan pengujian aktif menggunakan *automated scanner* OWASP ZAP untuk mendeteksi kerentanan aplikasi web. Instrumen dan teknik pengumpulan data pada setiap tahap dirangkum pada Tabel 1.

Tabel 1. Instrumen dan Teknik Pengumpulan Data

Tahap PTES	Instrumen/Alat	Output
Pre-Engagement	-	Kejelasan ruang lingkup dan batasan teknis pengujian
Intelligence Gathering	Whois, DNS Record Analysis, Nmap	Informasi domain, IP address, port terbuka, dan teknologi server
Threat Modeling	Framework STRIDE	Daftar ancaman
Vulnerability Analysis	Nmap, OWASP ZAP, SSL/TLS Checker, Security Header Checker.	Daftar kerentanan dan kategori risiko
Reporting	CVSS v4.0 *Calculator*	Skor risiko, *severity,* prioritas perbaikan, rekomendasi.

Alat dipilih berdasarkan tiga pertimbangan. Pertama, alat harus dapat dipakai secara non-destruktif sesuai batasan etika pada sistem produksi. Kedua, alat bersifat terbuka atau dapat diakses publik dan lazim dipakai sehingga pengujian dapat direplikasi. Ketiga, alat sesuai dengan tujuan tiap tahap PTES. Versi, konfigurasi, dan alasan pemilihan setiap alat dirinci pada Tabel 2.

Tabel 2. Alasan Pemilihan Alat

Instrumen/Alat	Alasan Pemilihan
Whois dan DNS	Data domain dan DNS bersifat publik sehingga pengumpulannya pasif dan tidak mengganggu sistem produksi.
Nmap	Pemindai port dan layanan *open-source* yang lazim dipakai untuk memetakan permukaan serangan; pemindaian dibatasi pada deteksi port dan layanan.
OWASP ZAP	Pemindai kerentanan web *open-source* yang mencakup kerentanan umum seperti SQL Injection dan Path Traversal serta merekam *request* dan *response* sebagai bukti.
SSL/TLS Checker, Security Header Checker.	Pemeriksaan eksternal bersifat pasif sehingga tidak memengaruhi layanan.
CVSS v4.0 *Calculator*	Perhitungan mengikuti spesifikasi CVSS v4.0 sehingga skor konsisten antar temuan dan dapat diverifikasi ulang..

Setiap *alert* OWASP ZAP ditinjau dengan memeriksa *request* dan *response* yang tercatat, tingkat *confidence*, dan, bila memungkinkan, pengecekan manual non-destruktif berupa pembandingan respons alert dengan respons normal halaman yang sama (kode status, panjang konten, dan isi), pemeriksaan header *Server* serta versi komponen yang terlihat pada respons, dan penilaian apakah prasyarat teknis kerentanan terpenuhi pada lingkungan yang terdeteksi, untuk mengurangi *false positive*.

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id

E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

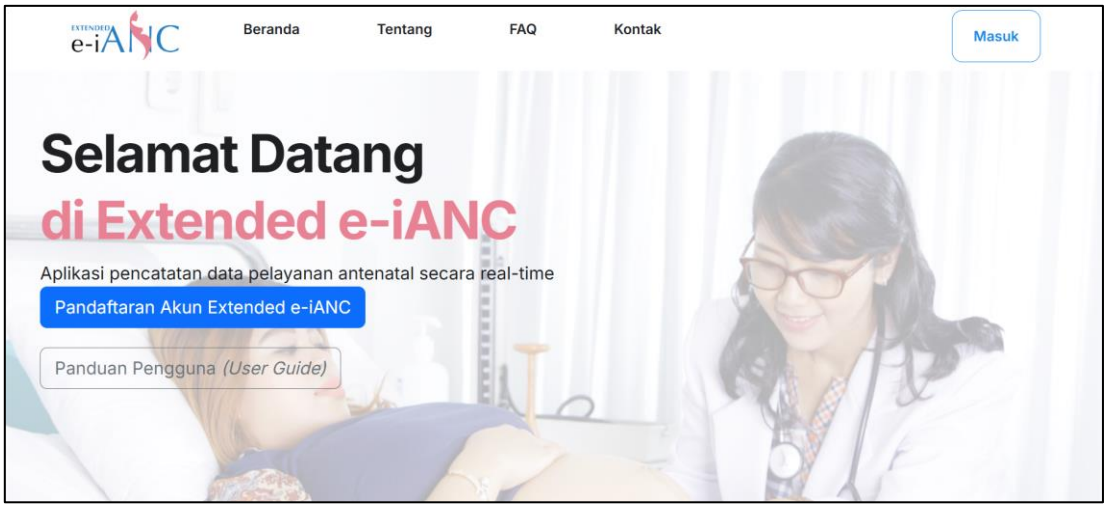
Teknik analisis data dilakukan secara kuantitatif deskriptif. Setiap temuan kerentanan pada tahap *vulnerability analysis* dinilai tingkat keparahannya menggunakan *Common Vulnerability Scoring System* (CVSS) versi 4.0, dengan menghitung skor berdasarkan metrik dasar (*Base Metrics*) yang mencakup vektor serangan, kompleksitas serangan, hak akses yang dibutuhkan, serta dampak terhadap kerahasiaan, integritas, dan ketersediaan sistem. Skor numerik yang dihasilkan (CVSS-B) berkisar antara 0,0 hingga 10,0, kemudian dikategorikan ke dalam empat tingkat keparahan, yaitu *Low*, *Medium*, *High*, dan *Critical*. Selanjutnya, dilakukan analisis distribusi frekuensi terhadap jumlah temuan pada masing-masing kategori keparahan untuk menggambarkan profil risiko keamanan sistem secara keseluruhan, yang menjadi dasar kuantitatif dalam menentukan prioritas rekomendasi perbaikan pada tahap *reporting*

4. Hasil dan Pembahasan

4.1 Hasil

4.1.1 *Pre-Engagement Interactions*

Pada tahap ini, ditetapkan bahwa objek pengujian adalah website Extended e-iANC dengan fokus pada keamanan akses, perlindungan data, konfigurasi keamanan dasar, dan potensi paparan informasi. Ruang lingkup pengujian dibatasi hanya pada area yang dapat diakses secara publik, sedangkan pengujian tidak mencakup pengambilalihan akun, perubahan atau penghapusan data, maupun pengujian langsung terhadap basis data. Penetapan batasan ini penting mengingat Extended e-iANC merupakan sistem produksi yang melayani data kesehatan masyarakat secara langsung, sehingga pengujian harus dilakukan secara non-destruktif dan terkendali (Safitra *et al.*, 2023).



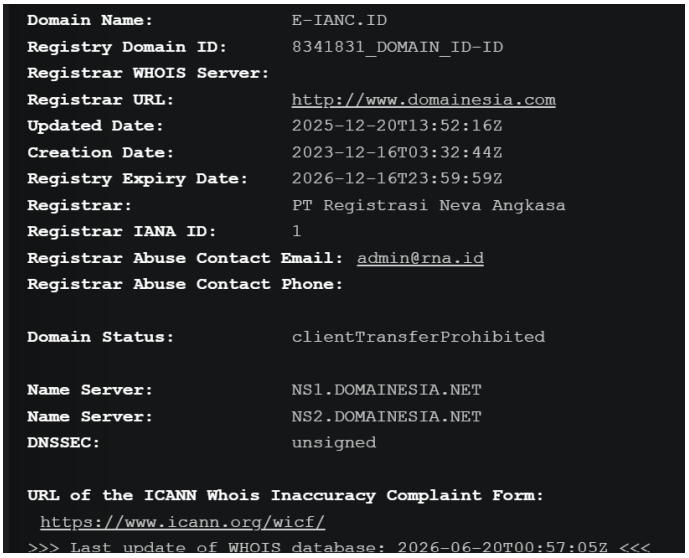
Gambar 2. Tampilan Website Extended e-iANC

4.1.2 Whois

Tahap ini menggunakan *tools* Whois untuk mengumpulkan informasi lebih lanjut tentang domain e-ianc.id. Hasil pencarian menunjukkan domain terdaftar melalui registrar PT Registrasi Neva Angkasa, dibuat pada 16 Desember 2023, dengan status *clientTransferProhibited*, namun konfigurasi DNSSEC masih berstatus *unsigned*, sebagaimana disajikan pada Gambar 3.

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id

E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130



Gambar 3. Hasil Whois

Informasi dari hasil Whois bermanfaat untuk analisis keamanan siber pada penelitian ini, seperti mengidentifikasi asal-usul domain dan mendeteksi potensi ancaman *DNS hijacking*. Status DNSSEC yang belum diaktifkan menjadi catatan penting karena berkaitan langsung dengan integritas resolusi DNS domain tersebut.

4.1.3 DNS Record Analysis

Selanjutnya dilakukan analisis DNS *record* untuk memperoleh gambaran infrastruktur domain secara lebih rinci, sebagaimana ditunjukkan pada Gambar 4.

Question	Type	Record	TTL
e-ianc.id	A	36.50.77.73	10m
e-ianc.id	AAAA	2001:df7:5300:9::49	10m
e-ianc.id	MX	e-ianc.id Preference: 0	10m
e-ianc.id	TXT	v=spf1 ip4:36.50.77.73 +a +mx include:relay.mailchannels.net ~all	10m
e-ianc.id	NS	ns1.domainesia.net	20m
e-ianc.id	NS	ns2.domainesia.net	20m
e-ianc.id	SOA	ns1.domainesia.net Expire: 1209600 Serial: 2026050301 Minimum: 86400 Refresh: 3600 Retry: 1800 RName: admin.domainesia.com.	20m

Gambar 4. DNS Record Analysis

Hasil analisis menunjukkan A record mengarah ke IPv4 36.50.77.73, serta TXT record SPF dengan konfigurasi v=spf1 ip4:36.50.77.73 +a +mx include:relay.mailchannels.net ~all yang masih menggunakan mekanisme *soft-fail* (~all), tergolong lebih lemah dibandingkan mekanisme *hard-fail* (-all). Konfigurasi SPF yang masih bersifat soft-fail ini berisiko memudahkan pemalsuan alamat pengirim e-mail (*email spoofing*), termasuk pengiriman *phishing* yang mengatasnamakan domain resmi e-ianc.id kepada tenaga kesehatan maupun pasien.

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

4.1.4 Subdomain

Pemeriksaan subdomain bertujuan memetakan seluruh subdomain aktif yang terhubung dengan domain utama, seperti terlihat pada Gambar 5

Subdomain	IP address
mail.e-ianc.id	36.50.77.73
ftp.e-ianc.id	36.50.77.73
rme.e-ianc.id	36.50.77.73
www.rme.e-ianc.id	36.50.77.73
www.e-ianc.id	36.50.77.73
ddns.e-ianc.id	180.244.185.51
www.dev.e-ianc.id	Did not resolve.
old.e-ianc.id	Did not resolve.
dev.e-ianc.id	Did not resolve.
www.old.e-ianc.id	Did not resolve.

Gambar 5. Subdomain

Ditemukan lima subdomain aktif (mail, ftp, rme, www.rme, www) yang seluruhnya mengarah ke alamat IP yang sama (36.50.77.73), mengindikasikan bahwa layanan web, email, FTP, dan data rekam medis elektronik berjalan pada satu server yang sama. Temuan ini penting karena ko-lokasi beberapa layanan pada satu server memperluas *attack surface*, sebab kompromi pada satu layanan berpotensi berdampak pada layanan lain yang berbagi infrastruktur yang sama (Hörnemann *et al.*, 2024).

4.1.5 Port & Service Scan

Pemindaian port dan layanan dilakukan untuk mengidentifikasi seluruh port yang terbuka pada server target, sebagaimana ditunjukkan pada Gambar 6.

Port	Protocol	State	Service	Version
80	tcp	open	http	OpenResty web app server 1.29.2.3
443	tcp	open	http	OpenResty web app server 1.29.2.3
2082	tcp	open	http	OpenResty web app server 1.29.2.3
2083	tcp	open	http	nginx
2086	tcp	open	http	OpenResty web app server 1.29.2.3
2087	tcp	open	http	nginx
2095	tcp	open	http	OpenResty web app server 1.29.2.3
2096	tcp	open	http	nginx
52223	tcp	open	http	nginx
52224	tcp	open	http	OpenResty web app server 1.29.2.3
52227	tcp	open	http	nginx
52228	tcp	open	http	OpenResty web app server 1.29.2.3
52229	tcp	open	http	nginx
52230	tcp	open	http	OpenResty web app server 1.29.2.3
52231	tcp	open	http	nginx
52232	tcp	open	http	OpenResty web app server 1.29.2.3

Gambar 6. *Ports/Hosts Scannning*

Hasil pemindaian menemukan port 80 dan 443 (HTTP/HTTPS) terbuka, serta sejumlah port tambahan (2082, 2083, 2086, 2087, 2095, 2096, dan rentang 52223–52232) yang menjalankan layanan OpenResty dan Nginx. Semakin banyak port yang terbuka, semakin besar pula peluang penyerang menemukan celah masuk ke dalam sistem.

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id

E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November

OPEN ACCESS

https://doi.org/ 10.63447/jmt.v3i2.2130

4.1.6 Threat Modeling

Data yang diperoleh selama tahap *Intelligence Gathering* digunakan untuk memetakan potensi ancaman menggunakan kerangka STRIDE, sebagaimana ditunjukkan pada Gambar 7.

STRIDE CATEGORY	ANCAMAN (THREAT)	ATTACK FLOW / JALUR SERANGAN	DAMPAK (IMPACT)	PENCEGAHAN (PREVENTION)	MITIGASI (MITIGATION)
Spoofing Pemalsuan Identitas	• Phishing • Credential stuffing	Pencurian kredensial pengguna (phishing / credential stuffing) → Login to aplikasi web menyamar sebagai user valid → Akses data pasien tanpa izin	• Akses ilegal ile sistem • Penyamaran sebagai pengguna sah	• **Multi-Factor Authentication (MFA)**, rate limiting & account lodmin • **Rate limiting & account lockout** untuk mencegan lovits force / credential stuffing • **CAPTCHA** pada form login	• Deteksi anomail login (IP saing, waktu tidak wajati dengan notifikal otematis • Force logout & reset bredential otematis saet activitas mensungakan terdetesal
Tampering Perubahan Data	• SQL Injection • Manipulati parameter / request API	Mengirim request berbahaya (SQL Injection / parameter tampering) → Request diproses aplikasi tanpa validasi kuat → Data diubah langsung pada database	• Integritas data rusak • Data medis pasian berubah	• **Prepared statement / parameterized query** serta ORM yang aman • Input validation & output sconding berbasis whitalist • **Web Application Firewall (WAF)**	• Database transaction logging & checkisan / integrity verification • Automated backup dengar versioning untuk rellback cepat • Alerting real-time (SIEM) saat terjadi perubahan data anomali
Repudiation Penyangkalan Aktivitas	• Audit trail lemah • Aktivitas tidak tercatat	User / attacker melakukan aktivitas (login, ubah / hapus data) → Sistem tidak mencatat aktivitas secara memarial → Aktivitas tidak dapat ditelusuri	• Sulit melakukan tracking palaku • Menyukikan audit & investigasi	• Audit logging menyaksuh (slapa, apa, sapan, dari manai yang tidak dapat diubah pengguna biasa • Digital signature / hasking pada log • Sinkronisasi watau (NTP) di seluruh server	• Centralized log management (SIEM) dengan retensi log jangka panjang • Penyimpanan log immutable / WORM ager tidak dapat dihapus/diubah • Prosedur forensik digital pasca insiden
Information Disclosure Kebocoran Informasi	• DNS enumeration • Subdomain discovery • Path traversal • Server inisconfiguration	Enumerasi informasi via DNS & subdomain → Eksploitasi misconfiguration (path traversal) → Informasi & file sensitif terekspos	• Kebocoran data pasien • Kebocoran konfigurasi sistem	• Nonaktifkan directory listing & banner grabbing • Enkripsi data sensitif of rect & in transit (TLS 1.2/1.3) • Data masking / tokenization untuk data pasien	• Dats Lass Prevention (DLP) untok mendetsksi transfer data mancurigakan • Proseder notifikasi pelanggaran data seveai UU PDP • Segmentasi jaringan berbasis need-to-know
Denial of Service Gangguan Layanan	• Flooding request • SMTP staste • Overload port service	Membanjiri sistem dengan request berbaliwan / eksploitasi iuysman centosis → Server menjadi overload → Layanan tidak dapat diakses	• Sistem tidak dapat diakses olah pengguan sah	• Rate limiting & troothing API • Protetei DDOS berbasis CDN (ms. Cloudflare) • Load balancer & aato-scaling	• Redundand server multi-region & fallover ctromals • Rensana respons insiden lioutus DDOS (coordined (IDS/IIPS) • Monitoring real-time traffic anomali (IDS/IPS)
Elevation of Privilege Peningkatan Hak Akses	• SQL Injection • SpringSShell exploit • Broken access control	Eksploitasi kerentanan (SQL injection / SpringSShell / broken access control) → Hak akses meningkat dari user biasa menjadi admin → Kontrol penuh, akses file & konfigurasi server	• Full system takeover	• Role-Based Access Control (RBAC) dengan least privilege • Patch management rutin untuk framework/dependency • Vulnerability secaning berkale & secure code review	• Segmentasi jaringan / isolasi layanan skills • Just-in-time access & section recording untuk akun privileged • Incident response & kill switch untuk pensebasan akses expet

Gambar 7. Pemetaan Ancaman STRIDE

Hasil pemetaan ini mencakup enam ragam ancaman — *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service*, dan *Elevation of Privilege* — lengkap dengan aset yang berisiko terdampak, konsekuensinya, serta langkah pencegahan dan mitigasi masing-masing. Dari aset yang berhasil diidentifikasi, dua kategori yakni *Information Disclosure* dan *Elevation of Privilege* menunjukkan tingkat risiko paling signifikan, sebab keduanya berkaitan erat dengan potensi bocornya data pasien dan pengambilalihan hak akses sistem secara tidak sah. Pemetaan semacam ini membantu tim pengujian menyusun langkah mitigasi yang lebih tepat sasaran guna menekan risiko pada sistem (Widjajarto *et al.*, 2021).

4.1.7 Security Header

Pemeriksaan konfigurasi *header* keamanan dilakukan untuk mengetahui *header* apa saja yang belum diterapkan pada website target, sebagaimana ditunjukkan pada Gambar 8.

Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Gambar 8. Security Header

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

Hasil pemeriksaan menunjukkan bahwa *Content-Security-Policy*, *X-Frame-Options*, *X-Content-Type-Options*, *Referrer-Policy*, dan *Permissions-Policy* seluruhnya belum diterapkan pada website Extended e-iANC, sehingga dikategorikan sebagai temuan *Missing Security Headers*. Temuan ini sejalan dengan hasil pemindaian satu juta situs teratas yang menunjukkan bahwa penerapan header seperti CPS, HSTS, dan X-Frame-Option masih belum merata.

4.1.8 SSL/TLS Checker

Pemeriksaan sertifikat SSL/TLS dilakukan untuk memastikan validitas dan konfigurasi enkripsi pada website target, sebagaimana ditunjukkan pada Gambar 9.

Subject	e-ianc.id Fingerprint SHA256: 8f869c55c7f0f13dfd59e4096a5ee835799d73dc799cf77fbe3d5ef78a6d4458 Pin SHA256: Zco1+/WK9YUf2F3oL/Rk0sktlpiiiSmnX++v35WCT58=
Common names	e-ianc.id
Alternative names	*.arizkinewbie.com *.e-ianc.id arizkinewbie.com e-ianc.id www.e-ianc.arizkinewbie.com
Serial Number	06522475403b0a89c94172ca10841ef7b6e4
Valid from	Thu, 30 Apr 2026 12:34:02 UTC
Valid until	Wed, 29 Jul 2026 12:34:01 UTC (expires in 1 month and 3 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R12 AIA: http://r12.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL CRL: http://r12.c.lencr.org/101.crl
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Gambar 9. SSL/TLS *Checker*

Hasil pemeriksaan menunjukkan sertifikat masih valid dengan kunci RSA 2048 bit dan algoritma SHA256withRSA, namun DNS CAA Record belum dikonfigurasi (ditandai "No" pada baris *DNS CAA*), yang berarti belum ada pembatasan resmi otoritas sertifikat mana saja yang boleh menerbitkan sertifikat untuk domain tersebut. Ketidakadaan CAA record ini meningkatkan risiko penerbitan sertifikat SSL/TLS tidak sah oleh otoritas sertifikat yang tidak berwenang, yang berpotensi dimanfaatkan untuk serangan man-in-the-middle terhadap komunikasi data pasien.

4.1.9 Protocol TLS

Pemeriksaan protokol TLS dilakukan untuk memastikan protokol enkripsi lama yang rentan sudah dinonaktifkan, sebagaimana ditunjukkan pada Gambar 10.

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Gambar 10. *Protocol* TLS

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

Hasil pemeriksaan menunjukkan website telah mendukung TLS 1.3 dan TLS 1.2, sementara protokol lama yang rentan (TLS 1.1, TLS 1.0, SSL 3, SSL 2) sudah dinonaktifkan, menunjukkan konfigurasi protokol enkripsi pada aspek ini sudah cukup baik.

4.1.10 Open Ports

Pemindaian ulang port dilakukan secara lebih terfokus untuk memastikan layanan-layanan yang berjalan pada server, sebagaimana ditunjukkan pada Gambar 11.

```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-06-25 17:49 +0700
Nmap scan report for e-ianc.id (36.50.77.73)
Host is up (0.051s latency).
Other addresses for e-ianc.id (not scanned): 2001:df7:5300:9::49
rDNS record for 36.50.77.73: ragna.id.domainesia.com
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE  SERVICE
20/tcp    closed ftp-data
21/tcp    open   ftp
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
21571/tcp closed unknown

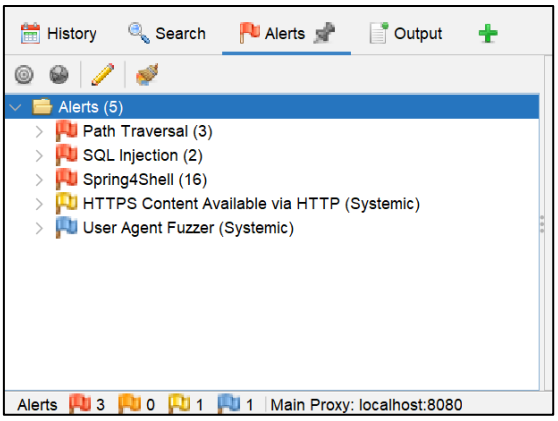
Nmap done: 1 IP address (1 host up) scanned in 17.21 seconds
```

Gambar 11. Open Ports

Ditemukan sebelas port berstatus terbuka, yaitu port 21 (FTP), 25 (SMTP), 53 (DNS), 80 (HTTP), 110 (POP3), 143 (IMAP), 443 (HTTPS), 465 (SMTPS), 587 (Submission), 993 (IMAPS), dan 995 (POP3S). Beberapa di antaranya merupakan protokol lama (FTP, POP3) yang secara umum sudah tidak direkomendasikan untuk diaktifkan pada sistem yang menangani data sensitif. Kedua protokol tersebut mengirimkan kredensial secara plaintext tanpa enkripsi, sehingga rentan terhadap penyadapan (*sniffing*) apabila penyerang berada pada jalur jaringan yang sama.

4.1.11 OWASP ZAP

Pemindaian kerentanan aplikasi web secara menyeluruh dilakukan menggunakan OWASP ZAP, sebagaimana ditunjukkan pada Gambar 12.



Gambar 12. Hasil Scanning menggunakan OWASP ZAP

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

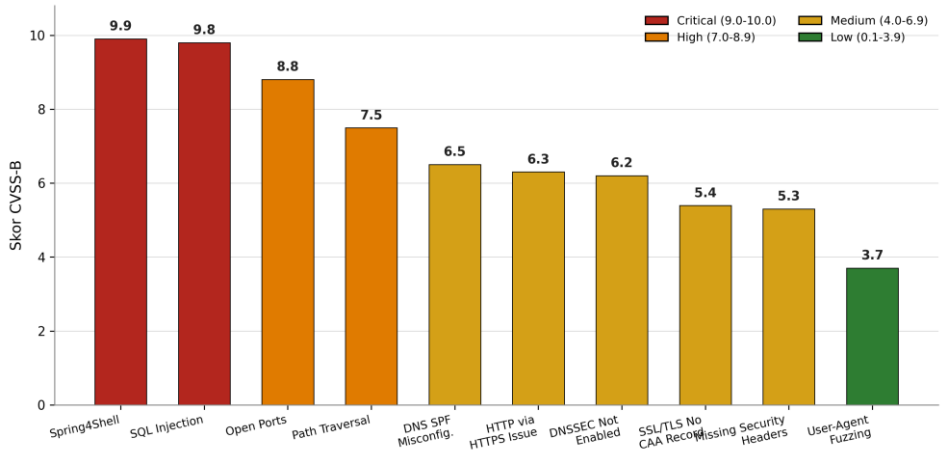
Hasil pemindaian menemukan beberapa alert kerentanan, dengan yang paling kritis adalah Path Traversal, SQL Injection, dan Spring4Shell, selain itu juga ditemukan alert HTTPS Content Available via HTTP dan User Agent Fuzzer. Ketiga kerentanan kritis tersebut selanjutnya dinilai menggunakan CVSS v4.0 dan memperoleh skor tertinggi di antara seluruh temuan yang dicantumkan pada tabel 3, sejalan dengan kajian yang menyatakan SQL Injection masih menjadi kerentanan aplikasi web berbasis basis data yang paling sering dieksploitasi hingga saat ini (Abdullayev & Chauhan, 2023).

4.1.12 Reporting

Berdasarkan seluruh tahap pengujian yang telah dilakukan, terbukti bahwa website Extended e-iANC memiliki sepuluh celah kerentanan dengan tingkat keparahan bervariasi dari *Critical* hingga *Low*, sebagaimana dirangkum pada Tabel 3 dan Gambar 13.

Tabel 3. Hasil Penilaian Risiko Kerentanan Website Extended e-iANC Menggunakan CVSS v4.0

No	Kerentanan	Skor CVSS-B	Kategori
1.	Spring4Shell	9,9	Critical
2.	SQL Injection	9,8	Critical
3.	Open Ports	8,8	High
4.	Path Traversal	7,5	High
5.	DNS SPF Misconfiguration	6,5	Medium
6.	HTTP via HTTPS Issue	6,3	Medium
7.	DNSSEC Not Enabled	6,2	Medium
8.	SSL/TLS No CAA Record	5,4	Medium
9.	Missing Security Headers	5,3	Medium
10.	User-Agent Fuzzing Response Disclosure	3,7	Low



Gambar 13. Distribusi Skor CVSS-B pada Sepuluh Temuan Kerentanan Website Extended e-iANC

Berdasarkan Tabel 3 dan Gambar 13, dua kerentanan berada pada kategori *Critical*, yaitu Spring4Shell dan SQL Injection, yang keduanya berpotensi memberikan kendali penuh atas sistem maupun akses tidak sah terhadap basis data pasien apabila dieksploitasi. Dua kerentanan lain berada pada kategori *High*, yaitu Open Ports dan Path Traversal, yang memperluas permukaan serangan dan berpotensi mengekspos berkas sistem yang seharusnya tidak dapat diakses publik. Lima kerentanan berkategori *Medium* dan satu berkategori *Low* terutama terkait kelemahan konfigurasi DNS, SSL/TLS, dan header keamanan yang, meskipun tidak berdampak langsung, tetap memperbesar peluang serangan lanjutan apabila dibiarkan. Ringkasan dampak dan rekomendasi untuk setiap kerentanan disajikan pada Tabel 4 agar dapat langsung dipakai sebagai dasar tindakan.

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

Tabel 4. Ringkasan Dampak dan Rekomendasi Kerentanan

Kerentanan (skor, kategori)	Kategori STRIDE	Dampak utama	Rekomendasi
Spring4Shell (9,9; Critical)	Elevation of Privilege	Eksekusi kode jarak jauh yang dapat berujung pada pengambilalihan server dan akses ke seluruh data di dalamnya.	Perbarui Spring Framework dan JDK ke versi yang telah ditambal; pasang WAF sebagai perlindungan sementara.
SQL Injection (9,8; Critical)	Tampering, Elevation of Privilege	Data pasien dapat dibaca atau diubah langsung pada basis data sehingga integritas rekam medis terancam.	Terapkan *parameterized query*, validasi dan sanitasi input, serta hak akses basis data minimal.
Open Ports (8,8; High)	Information Disclosure, Denial of Service	Layanan lama (FTP, POP3) dan port yang tidak perlu memperluas permukaan serangan serta rawan penyadapan kredensial.	Tutup port dan layanan yang tidak diperlukan; ganti FTP dan POP3 dengan SFTP dan IMAPS; batasi akses dengan *firewall*.
Path Traversal (7,5; High)	Information Disclosure	Berkas sistem dan konfigurasi di luar direktori web dapat terbaca.	Validasi dan normalisasi path berkas, batasi akses direktori, dan jalankan layanan dengan hak akses minimal.
DNS SPF Misconfiguration (6,5; Medium)	Spoofing	Email palsu yang mengatasnamakan domain lebih mudah lolos karena kebijakan *soft-fail*.	Ubah ~all menjadi -all setelah seluruh pengirim sah terdaftar; tambahkan DKIM dan DMARC.
HTTP via HTTPS Issue (6,3; Medium)	Information Disclosure, Tampering	Konten yang tersedia melalui HTTP dapat disadap atau diubah di jaringan.	Alihkan seluruh HTTP ke HTTPS dan aktifkan HSTS.
DNSSEC Not Enabled (6,2; Medium)	Spoofing, Tampering	Resolusi DNS dapat dipalsukan sehingga pengguna diarahkan ke situs palsu.	Aktifkan DNSSEC melalui registrar dan penyedia DNS.
SSL/TLS No CAA Record (5,4; Medium)	Spoofing	Tidak ada pembatasan otoritas sertifikat sehingga penerbitan sertifikat palsu lebih sulit dicegah.	Tambahkan *CAA record* yang hanya mengizinkan otoritas sertifikat yang dipakai.
Missing Security Headers (5,3; Medium)	Tampering, Information Disclosure	Meningkatkan risiko XSS, *clickjacking*, dan *MIME sniffing*.	Terapkan Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, dan Permissions-Policy.

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

User-Agent Fuzzing Response Disclosure (3,7; Low)	Information Disclosure	Perbedaan respons terhadap User-Agent tertentu dapat membocorkan informasi perilaku server.	Seragamkan respons server dan minimalkan informasi pada respons dan *banner*.

Kerentanan pada lapisan aplikasi (SQL Injection dan Path Traversal) dapat muncul ketika input pengguna diproses tanpa validasi dan parameterisasi yang memadai, sedangkan Spring4Shell berkaitan dengan *dependency* yang belum diperbarui. Kerentanan pada lapisan infrastruktur dan konfigurasi (Open Ports, DNS SPF, DNSSEC, CAA, *security header*, dan HTTP via HTTPS) menunjukkan bahwa konfigurasi dasar belum diperkeras. Pola ini sejalan dengan kajian kasus kebocoran data kesehatan di Indonesia yang menyebut lemahnya kontrol akses dan belum optimalnya standar keamanan sebagai faktor utama (Nugraha *et al.*, 2021). Web, email, FTP, dan rekam medis elektronik yang berbagi satu alamat IP memperbesar dampak setiap kerentanan, karena kompromi satu layanan berpotensi menjalar ke layanan lain (Hörnemann *et al.*, 2024). Karena itu, memisahkan layanan sensitif dari layanan pendukung melalui segmentasi perlu diprioritaskan (Baligodugula *et al.*, 2024). Temuan *Critical* dan *High* berkaitan dengan kategori *Elevation of Privilege*, *Tampering*, dan *Information Disclosure* pada Gambar 7, dengan *Information Disclosure* dan *Elevation of Privilege* sebagai dua kategori yang dinilai paling signifikan. SQL Injection yang dapat dieksploitasi berpotensi membuka atau mengubah data pasien, sedangkan Spring4Shell berpotensi memberikan kendali atas server. Pada layanan yang menyimpan data ibu dan anak, dampaknya tidak hanya teknis, tetapi juga menyangkut kewajiban perlindungan data pribadi dan rekam medis menurut UU Nomor 27 Tahun 2022 dan Permenkes Nomor 24 Tahun 2022. Efektivitas parameterisasi kueri dan validasi input untuk menutup SQL Injection telah banyak dibuktikan (Disawal & Suman, 2023).

Penelitian terdahulu yang menerapkan PTES pada website pemerintahan menemukan sembilan kerentanan berkategori tinggi dari 42 temuan, atau sekitar 21% (Safitra *et al.*, 2023). Pada Extended e-iANC, kerentanan *Critical* dan *High* mencapai empat dari sepuluh temuan (40%). Perbedaan ini perlu ditafsirkan hati-hati karena jumlah temuan, cakupan pengujian, dan sistem penilaian keparahan kedua studi dapat berbeda. Meski demikian, dua temuan *Critical* pada sistem yang memuat data kesehatan ibu dan anak menunjukkan urgensi mitigasi yang lebih tinggi. Selain itu, berbeda dengan studi tersebut, penelitian ini menghubungkan setiap temuan dengan kategori STRIDE dan memasukkan risiko infrastruktur berupa ko-lokasi layanan pada satu server. Urutan penerapan rekomendasi disusun berdasarkan skor CVSS-B dan perkiraan upaya penerapan agar sesuai dengan sumber daya pengelola. Perbaikan yang berisiko tinggi dan dapat dikerjakan cepat didahulukan, sedangkan perbaikan yang membutuhkan sumber daya besar, seperti segmentasi layanan, dijadwalkan lebih lama dengan pembatasan akses *firewall* sebagai langkah sementara yang dilampirkan pada tabel 5.

Tabel 5. Prioritas Penerapan Mitigasi

Prioritas	Tindakan	Temuan terkait	Perkiraan upaya
Segera (maksimal 2 minggu)	Perbarui Spring Framework, JDK, dan *dependency* yang rentan; pasang WAF sementara	Spring4Shell	Sedang
Segera (maksimal 2 minggu)	Terapkan *parameterized query*, validasi input, dan hak akses basis data minimal	SQL Injection	Sedang hingga tinggi (perubahan kode)
Segera (maksimal 2 minggu)	Tutup port dan layanan yang tidak diperlukan; batasi akses dengan *firewall*	Open Ports	Rendah

Jurnal Manajemen dan Teknologi
https://journal.stmiki.ac.id
E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

Segera (maksimal 2 minggu)	Validasi dan normalisasi path berkas; batasi akses direktori	Path Traversal	Sedang
Jangka pendek (maksimal 1 bulan)	Alihkan HTTP ke HTTPS dan aktifkan HSTS; terapkan *security header*; perketat SPF dan tambahkan DKIM dan DMARC	HTTP via HTTPS, Missing Security Headers, DNS SPF	Rendah
Jangka menengah (1–3 bulan)	Aktifkan DNSSEC dan tambahkan CAA record; seragamkan respons server	DNSSEC, No CAA Record, User-Agent Fuzzing	Rendah hingga sedang
Jangka menengah (1–3 bulan)	Pisahkan layanan web, email, FTP, dan rekam medis elektronik pada infrastruktur atau segmen jaringan terpisah	Ko-lokasi layanan pada satu server	Tinggi

Pengujian dibatasi pada area yang dapat diakses publik dan tidak mencakup eksploitasi, sehingga temuan berstatus terdeteksi dan kemungkinan *false positive* tidak dapat sepenuhnya dihilangkan. Skor CVSS-B juga belum memperhitungkan konteks lingkungan sistem. Pengujian ulang setelah perbaikan diperlukan untuk memastikan efektivitas mitigasi.

4.2 Pembahasan

Dalam penelitian ini, analisis keamanan sistem informasi pada website *Extended e-iANC* mengungkapkan adanya sepuluh kerentanan, yang terdiri dari dua kerentanan berkategori *Critical* (Spring4Shell dan *SQL Injection*), dua berkategori *High* (Open Ports dan Path Traversal), serta enam kerentanan lainnya berkategori *Medium* hingga *Low*. Temuan ini menunjukkan bahwa meskipun *Extended e-iANC* telah berfungsi sebagai sistem yang penting dalam pengelolaan data kesehatan, namun tingkat keamanannya masih jauh dari memadai, terutama dalam hal perlindungan terhadap data sensitif pasien. Penelitian ini sejalan dengan temuan oleh Nugraha *et al.* (2021), yang menyatakan bahwa lemahnya kontrol akses dan penerapan standar keamanan yang tidak optimal di sektor kesehatan di Indonesia berkontribusi pada tingginya risiko kebocoran data. Selain itu, hasil yang ditemukan juga mendukung studi oleh Abdullayev & Chauhan (2023) yang menyoroti bahwa *SQL Injection* tetap menjadi salah satu kerentanan paling umum dan berbahaya dalam aplikasi web berbasis data. Dengan demikian, penelitian ini menekankan perlunya langkah mitigasi segera, seperti penerapan *parameterized queries* dan pembaruan *framework*, untuk meningkatkan keamanan sistem informasi kesehatan di Indonesia dan melindungi data pasien dari ancaman yang semakin kompleks.

5. Kesimpulan

Penerapan lima tahap PTES yang dipadukan dengan STRIDE dan CVSS v4.0 mengidentifikasi sepuluh kerentanan pada website Extended e-iANC, yaitu dua *Critical* (Spring4Shell dan SQL Injection), dua *High* (Open Ports dan Path Traversal), lima *Medium*, dan satu *Low*. Temuan ini menunjukkan bahwa sistem masih memiliki celah signifikan terhadap kerahasiaan dan integritas data pasien, terutama pada lapisan aplikasi dan konfigurasi infrastruktur. Tindak lanjut yang diperlukan adalah memperbaiki kerentanan *Critical* dan *High* terlebih dahulu melalui pembaruan *dependency*, penerapan *parameterized query* dan validasi input, penutupan port yang tidak diperlukan, dan pembatasan akses berkas, kemudian memperbaiki konfigurasi DNS, SSL/TLS, dan *security header* serta memisahkan layanan sensitif melalui segmentasi. Setelah perbaikan, pengujian ulang perlu dilakukan dengan ruang lingkup, alat, dan konfigurasi yang sama untuk membandingkan skor CVSS-B sebelum dan sesudah perbaikan serta memastikan tidak muncul kerentanan baru. Targetnya adalah tidak ada lagi temuan *Critical* dan *High*.

E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

6. Ucapan Terima Kasih

Terima kasih penulis sampaikan kepada pengelola website Extended e-iANC atas izin yang diberikan untuk melaksanakan pengujian keamanan pada sistem tersebut, serta kepada Fakultas Ilmu-Ilmu Kesehatan Universitas Esa Unggul atas dukungan fasilitas yang diberikan sepanjang penelitian ini berjalan.

7. Daftar Pustaka

Abdullayev, V., & Chauhan, A. S. (2023). SQL injection attack: Quick view. In *Mesopotamian Journal of CyberSecurity* (Vol. 2023, pp. 30–34). Mesopotamian Academic Press. https://doi.org/10.58496/MJCS/2023/006.

Baligodugula, V. V., Ghimire, A., & Amsaad, F. (2024). An overview of secure network segmentation in connected IIoT environments. *Computing & AI Connect*, 1(1), 1. https://doi.org/10.69709/caic.2024.193182.

Bunan Imtias, M., Umam, K., Mustofa, H., & Hadi Subowo, M. (2025). Comparative analysis of penetration testing frameworks: OWASP, PTES, and NIST SP 800-115 for detecting web application vulnerabilities. In *Journal of Applied Informatics and Computing (JAIC)* (Vol. 9, No. 6). https://doi.org/10.30871/jaic.v9i6.9846.

Database, N. V. (2022). CVE-2022-22965 detail. In *National Vulnerability Database (NVD)*. https://nvd.nist.gov/vuln/detail/cve-2022-22965.

Disawal, S., & Suman, U. (2023). An approach to detect and prevent SQL injection and XSS vulnerability in the web application. *International Journal of Engineering Trends and Technology*, 71(8), 216–224. https://doi.org/10.14445/22315381/IJETT-V71I8P219.

Enggar Pramudita Wijayanti, & Asti Nurhayati. (2024). Evaluasi sistem informasi manajemen rumah sakit (SIMRS) dengan metode Hot-Fit pada unit rawat jalan di Rumah Sakit PKU Muhammadiyah Kartasura. *Jurnal Ilmu Kesehatan dan Gizi*, 2(3), 117–145. https://doi.org/10.55606/jig.v2i3.3092.

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. In *Journal of Medical Internet Research*, 26. JMIR Publications Inc. https://doi.org/10.2196/46904.

Fauzi, E., Alif, N., & Shandy, R. (2022). Hak atas privasi dan politik hukum Undang-Undang Nomor 27 Tahun 2022 tentang pelindungan data pribadi. https://doi.org/10.20885/JLR.vol7.iss3.art1.

FIRST.Org, I. (2023). Common vulnerability scoring system version 4.0 specification document.

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, 121. https://doi.org/10.1016/j.technovation.2022.102583.

Hörnemann, J., Pohlmann, N., Urban, T., & Große-Kampmann, M. (2024). Sharing is caring: Towards analyzing attack surfaces on shared hosting providers. *Lecture Notes in Informatics*

E-ISSN: 3047-8251 | P-ISSN: 3047-826X
Vol. 3 No. 2 (2026) | November
OPEN ACCESS
https://doi.org/ 10.63447/jmt.v3i2.2130

(LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI), P-345, 217–229. https://doi.org/10.18420/sicherheit2024_014.

Nugraha, D. A., Nurfitroh, R., Ul-Haq, N. D., PurnamaDika, R., & Lagontang, S. N. (2021). Kebocoran data BPJS Kesehatan: Ancaman terhadap. *Integrative Perspectives of Social and Science Journal*, 2(3), 4685–4691.

Safitra, M. F., Lubis, M., & Widjajarto, A. (2023). Security vulnerability analysis using penetration testing execution standard (PTES): Case study of government's website. *ACM International Conference Proceeding Series*, 139–145. https://doi.org/10.1145/3592307.3592329.

The PTES Team. (2022). The penetration testing execution standard documentation.

Widjajarto, A., Lubis, M., & Ayuningtyas, V. (2021). Vulnerability and risk assessment for operating system (OS) with framework STRIDE: Comparison between VulnOS and Vulnix. In *Indonesian Journal of Electrical Engineering and Computer Science*, 23(3), 1643–1653. Institute of Advanced Engineering and Science. https://doi.org/10.11591/ijeecs.v23.i3.pp1643-1653.