SAINSTECH
Jurnal Penelitian dan Pengkajian Sains dan Teknologi
Volume 35 No.2
Maret 2025
SINTA 5

Analisis Keamanan Situs Web Rumah Sakit Menggunakan Metode Penetration Testing OWASP

Riadi Marta Dinata[1], Muhammad Alzril[2], Muhammad Ikrar Yamin[3], Harlan Effendi[4], Muhammad Febriansyah[5]

[1,2]Program Studi Teknik Informatika, FSTI, ISTN Jakarta
[3,4,5]Program Studi Teknik Elektro, Fakultas Teknik, ISTN Jakarta
e-mail: [1]riadimrt@gmail.com, [2]alzril.muhammad@gmail.com, [3]ikrar@istn.ac.id,[4]harlan@istn.ac.id, [5]m.febriansyah@istn.ac.id

Abstrak

Di era digital yang semakin terkoneksi, keberadaan situs web sebagai wajah utama sebuah institusi menjadi sangat krusial, terutama dalam sektor pelayanan kesehatan. Penelitian ini mengkaji keamanan situs web rumah sakit rsjsh.co.id dengan pendekatan penetration testing yang merujuk pada panduan OWASP Testing Guide v4. Fokus utama penelitian adalah mengidentifikasi dan memverifikasi kerentanan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab. Metode yang digunakan mencakup pengumpulan informasi (footprinting), pemindaian (scanning), eksploitasi kerentanan, serta evaluasi risiko menggunakan CVSS v3.1 dan OWASP Risk Rating. Hasil analisis menunjukkan adanya 11 kerentanan, di antaranya tiga berkategori sedang: tidak adanya kebijakan Content Security Policy (CSP), anti-clickjacking header, serta keberadaan mixed content. Eksploitasi dilakukan menggunakan berbagai alat seperti Owasp Zap, Burp Suite, dan seography.io. Meskipun beberapa kerentanan tidak dapat dieksploitasi akibat sistem pertahanan yang memadai, temuan valid mengindikasikan perlunya implementasi kebijakan keamanan tambahan, seperti CSP dan konfigurasi HSTS. Penelitian ini merekomendasikan perbaikan proaktif sebagai langkah penting dalam menjaga kerahasiaan data pasien dan meningkatkan kepercayaan publik terhadap sistem digital rumah sakit

Kata kunci: penetration testing, keamanan web, rumah sakit, OWASP, Content Security Policy.

Abstract

In an increasingly connected digital era, the presence of a website as the primary face of an institution has become crucial—particularly in the healthcare sector. This study examines the security of the hospital website rsjsh.co.id using a penetration testing approach based on the OWASP Testing Guide v4. The main focus of the research is to identify and verify vulnerabilities that could potentially be exploited by malicious actors. The methods employed include information gathering (footprinting), scanning, vulnerability exploitation, and risk evaluation using CVSS v3.1 and the OWASP Risk Rating. The analysis revealed 11 vulnerabilities, including three medium-level issues: the absence of a Content Security Policy (CSP), missing anti-clickjacking headers, and the presence of mixed content. Exploitation was carried out using tools such as OWASP ZAP, Burp Suite, and seography.io. Although some vulnerabilities could not be exploited due to adequate defense mechanisms, validated findings indicate the need for additional security policies such as CSP and HSTS configuration. This study recommends proactive remediation as a critical step to protect patient data confidentiality and enhance public trust in the hospital's digital systems.

Keywords: *penetration testing, web security, hospital, OWASP, Content Security Policy.*

DOI : https://doi.org/10.37277/stch.v35i2.2383

1. PENDAHULUAN

1.1. Keamanan Situs Web dan Ancaman Siber

Situs web sebagai antarmuka publik organisasi memiliki risiko keamanan yang signifikan. Menurut (Gupta et al., 2021), serangan umumnya terjadi melalui injeksi kode berbahaya, autentikasi lemah, dan konfigurasi sistem yang tidak aman. Dalam layanan kesehatan, risiko ini meningkat karena data pasien bernilai tinggi di pasar gelap digital (Priambodo et al., 2023). Keamanan situs dapat dicapai dengan memahami konsep ancaman dan memperbarui perangkat lunak secara rutin (J-sika et al., 2020).

Rumah sakit menjadi target empuk karena ketergantungan pada teknologi tanpa pengamanan memadai (Aji, 2022), sehingga pengujian situs web menjadi krusial. Ancaman siber juga sering berasal dari penyalahgunaan teknologi, bukan fungsinya yang semestinya (Ghozali et al., 2019).

Keamanan digital dapat diwujudkan dengan kesadaran akan pentingnya menjaga data, memasang antivirus, firewall, serta membatasi penyebaran informasi—tanggung jawab setiap individu dan organisasi (Tiram Media, 2023). Selain itu, aspek usability atau kemudahan penggunaan sistem juga tidak boleh diabaikan dalam merancang sistem yang aman dan efektif, karena memiliki pengaruh langsung terhadap interaksi dan kepercayaan pengguna (Lewis, 2014)

1.2 Penetration Testing dan OWASP Guide v4

Penetration testing atau uji penetrasi adalah simulasi serangan siber yang bertujuan untuk mengidentifikasi dan mengevaluasi kerentanan dalam sistem informasi. *Penetration Testing* dilakukan oleh peretas etis yang dilakukan dengan teknik peretas aslinya (Syiah Kuala University Press, 2023). Menurut Kaur & Kaur (Mishra, 2021) dalam *Procedia Computer Science*, metode ini telah terbukti efektif dalam mengungkap celah keamanan sebelum dieksploitasi oleh pihak tidak bertanggung jawab.

Penelitian ini mengacu pada *OWASP Testing Guide* v4 (Tohir, 2017), sebuah panduan internasional yang disusun oleh *Open Web Application Security Project* (OWASP), lembaga global yang secara khusus menangani isu keamanan aplikasi web. Pemahaman mengenai *OWASP Testing Guide* berdasarkan *Mastering OWASP* (Springer International Publishing, 2020) panduan ini dapat memberikan metode yang komprehensif untuk melakukan *penetration testing* pada situs web secara luas untuk penekanan pada keamanan situs web.

Gambar 1. Tahapan Pentest
Sumber : https://www.dewaweb.com/

OWASP Testing Guide menyajikan pendekatan sistematis terhadap tahapan pengujian, mulai dari informasi awal (*Information Gathering*), pemindaian (*Scanning*), eksploitasi (*Vulnerability Exploitation*), hingga evaluasi pasca serangan (*Post-Exploitation*). Di dalam panduan tersebut terdapat *OWASP TOP 10* yang menurut Dimas et al. (Cybellium Ltd., 2023) merupakan daftar kerentanan yang berfokus untuk menemukan risiko keamanan aplikasi web yang paling tinggi bahayanya serta yang paling sering ditemukan pada organisasi.

1.3 *Common Vulnerability Scoring System* v3.1

Untuk mengukur tingkat keparahan setiap kerentanan yang ditemukan, digunakan metode penilaian CVSS v3.1 (Nielsen & Molich, 1990) yang dikembangkan oleh *Forum of Incident Response and Security Teams* (FIRST). Sistem ini menggunakan metrik berbobot yang mempertimbangkan vektor serangan (AV), kompleksitas serangan (AC), hak istimewa (PR), interaksi pengguna (UI), hingga dampak terhadap kerahasiaan (C), integritas (I), dan ketersediaan (A). Berdasarkan sudut pandang (Al-Qarni, 2023) pada jurnalnya yang berjudul *Keamanan Informasi dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik* yang

DOI : https://doi.org/10.37277/stch.v35i2.2383

mengangkat studi kasus perlindungan data pribadi di Indonesia, Kerahasiaan atau *confidentiality* yaitu akses yang diperbolehkan terhadap sebuah informasi atau data, yang menunjukan bahwa membuka data atau informasi hanya bisa dilakukan oleh pihak yang memiliki akses tersebut. Kerahasiaan yang ada harus dipahami oleh orang yang mengerti akan keamanan komputer, jika tidak maka data atau informasi yang ada pada komputer sangat rentan untuk diretas dan akan menyebabkan kerugian (Lallie et al., 2021).

Dengan sistem skoring dari 0 hingga 10, CVSS v3.1 (Nielsen & Molich, 1990) membantu tim keamanan dalam memprioritaskan perbaikan kerentanan berdasarkan tingkat risiko teknisnya. Seperti dijelaskan oleh Mell et al. (Kaur & Kaur, 2022) dalam *NIST Special Publication 800-115*, CVSS tidak hanya penting untuk audit teknis, tetapi juga untuk pengambilan keputusan strategis dalam manajemen risiko.

Tabel 1. Klasifikasi Nilai *Base Score* CVSS v3.1 Posisi

Rentang	Risiko	Deskripsi
0.0	*None* (Tidak Ada)	Tidak ada dampak keamanan yang signifikan. Sistem dianggap aman dari kerentanan tertentu yang diuji.
0.1 – 3.9	*Low* (Rendah)	Kerentanan yang ditemukan memiliki dampak terbatas. Eksploitasi biasanya membutuhkan kondisi khusus atau berdampak kecil terhadap sistem.
4.0 – 6.9	*Medium* (Sedang)	Kerentanan dapat dimanfaatkan oleh penyerang dengan tingkat upaya yang moderat. Berpotensi menimbulkan gangguan fungsional atau akses terbatas ke data.
7.0 – 8.9	*High* (Tinggi)	Eksploitasi kerentanan ini cukup mudah dilakukan dan dapat menyebabkan kerugian yang nyata seperti kehilangan data atau gangguan layanan.
9.0 – 10.0	*Critical* (Kritis)	Kerentanan yang sangat berbahaya. Dapat dimanfaatkan secara luas tanpa banyak hambatan dan menimbulkan kerusakan besar, seperti kontrol penuh atas sistem atau kebocoran data massal.

1.4 *OWASP Risk Rating Methodology*

Selain penilaian teknis, OWASP Risk Rating (Silvia et al., 2015) digunakan untuk menilai risiko berdasarkan konteks organisasi, dengan mempertimbangkan Likelihood Factors (seperti keahlian peretas dan peluang eksploitasi) dan Impact Factors (seperti kerugian reputasi dan finansial). Menurut ISSA (2020) (Ziro et al., 2023), metodologi ini merupakan pendekatan sederhana yang disusun berdasarkan pengalaman ahli. Lallie et al. (Dimas et al., 2023) dalam Computers & Security menyebutkan bahwa kombinasi CVSS dan OWASP Risk Rating (Silvia et al., 2015) menghasilkan pemetaan risiko yang akurat secara teknis dan relevan secara organisasi. Penelitian oleh (Bahrun Ghozali,2019) menunjukkan bahwa metode ini berhasil mengidentifikasi 15 kerentanan, enam di antaranya berkategori tinggi, dengan tingkat risiko sedang dan dampak rendah.

Tabel 2. *OWASP Risk Rating Methodology* Posisi Tabel

Kategori	Faktor	Deskripsi
Likelihood Factor	*Skill Level*	Tingkat keahlian teknis yang dibutuhkan untuk eksploitasi.
Likelihood Factor	*Motive*	Alasan atau insentif yang mendorong pelaku melakukan

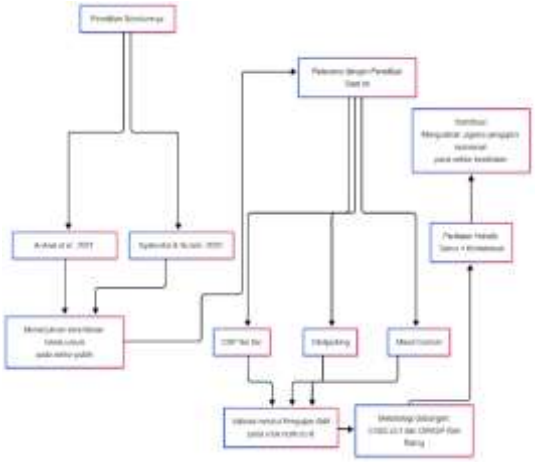
DOI : https://doi.org/10.37277/stch.v35i2.2383

Kategori	Faktor	Deskripsi
		serangan.
Likelihood Factor	*Opportunity*	Ketersediaan akses atau sumber daya untuk melakukan serangan.
Likelihood Factor	*Size*	Jumlah pelaku atau pihak yang mungkin tertarik untuk mengeksploitasi kerentanan.
Likelihood Factor	*Ease of Discovery*	Kemudahan dalam menemukan kerentanan oleh pelaku.
Likelihood Factor	*Ease of Exploit*	Kemudahan dalam melakukan eksploitasi terhadap kerentanan.
Likelihood Factor	*Awareness*	Tingkat kesadaran organisasi terhadap keberadaan kerentanan tersebut.
Likelihood Factor	*Intrusion Detection*	Kemampuan sistem dalam mendeteksi upaya intrusi.
Impact Factor	*Loss of Confidentiality*	Tingkat kerugian terhadap kerahasiaan data.
Impact Factor	*Loss of Integrity*	Kemungkinan perubahan data tanpa izin.
Impact Factor	*Loss of Availability*	Tingkat gangguan terhadap aksesibilitas sistem atau layanan.
Impact Factor	*Loss of Accountability*	Kemampuan untuk melacak aktivitas atau pengguna.
Impact Factor	*Financial Damage*	Potensi kerugian finansial yang ditimbulkan.
Impact Factor	*Reputation Damage*	Dampak terhadap reputasi organisasi.
Impact Factor	*Non-compliance*	Risiko terhadap ketidakpatuhan regulasi atau standar keamanan.
Impact Factor	*Privacy Violation*	Tingkat pelanggaran terhadap privasi pengguna atau data.

1.5 Studi Keamanan Situs Web Sektor Kesehatan

Penelitian sebelumnya yang dilakukan oleh Al-Ansi et al. (Aji, 2022) menyoroti kerentanan umum pada situs web rumah sakit di Yaman, termasuk *XSS*, *SQL injection*, dan *header* keamanan yang tidak lengkap. Temuan serupa diungkapkan oleh Syalendra dan Nuraini (Kusrini, 2007) dalam studi pengujian keamanan pada situs pemerintah di Indonesia yang menunjukkan bahwa sebagian besar situs belum menerapkan praktik keamanan standar seperti *HTTP Secure* dan validasi *input*.

DOI : https://doi.org/10.37277/stch.v35i2.2383



Gambar 2. *State of The Art*

Studi-studi tersebut menjadi inspirasi dan pembanding dalam penelitian ini, khususnya dalam mengevaluasi kerentanan seperti *Content-Security-Policy (CSP) not set*, *clickjacking*, dan *mixed content*, yang secara nyata ditemukan pada situs web rsjsh.co.id.

2. Metode Penelitian

Penelitian ini dirancang untuk menguji tingkat keamanan situs web Rumah Sakit Jiwa Dr. Soeharto Heerdjan (rsjsh.co.id) melalui pendekatan *penetration testing* yang sistematis dan berbasis standar. Setiap tahapan dirancang untuk mereplikasi skenario serangan dunia nyata dan mengidentifikasi celah keamanan yang mungkin belum disadari oleh pengelola situs.

2.1 Rancangan Penelitian

Metode yang digunakan mengacu pada kerangka kerja dari *OWASP Testing Guide* v4 (Tohir, 2017), yang telah diakui secara luas dalam praktik pengujian keamanan aplikasi web. Alur penelitian ini mencakup enam tahap utama:

- Identifikasi Target Uji: Fokus ditujukan pada halaman beranda situs rsjsh.co.id sebagai permukaan serangan awal. Pemilihan ini mempertimbangkan potensi paparan informasi publik dan akses pengguna umum. *Footprinting* dan *Information Gathering*: Yaitu proses pengumpulan informasi dilakukan dengan *tools* seperti nslookup, whois, dan whatweb, untuk mengetahui detail teknis seperti IP server, penyedia *hosting*, sistem yang digunakan, serta teknologi keamanan aktif. *Scanning* dan *Enumeration*: Yaitu dengan menggunakan *Nmap*, *OWASP ZAP*, dan *SSL Labs* untuk menemukan *port* terbuka, konfigurasi SSL/TLS, serta mengidentifikasi direktori tersembunyi dan potensi konfigurasi lemah lainnya. Vulnerability Exploitation: Dimana setelah kerentanan diidentifikasi, pengujian dilanjutkan ke eksploitasi menggunakan *Burp Suite*, *Sqlmap*, skrip HTML *iframe* untuk simulasi *clickjacking*, serta alat *online seography.io* untuk mendeteksi *mixed content*. Eksploitasi dilakukan secara terbatas dan bertanggung jawab, tanpa merusak sistem atau mengakses data pengguna.
- *Post-Exploitation* dan Evaluasi Risiko: Dari masing-masing kerentanan dianalisis menggunakan dua pendekatan: CVSS v3.1 (Nielsen & Molich, 1990) untuk penilaian teknis, dan *OWASP Risk Rating* (Silvia et al., 2015) untuk mempertimbangkan dampak organisasi. Kombinasi ini memberikan perspektif yang seimbang antara kerumitan teknis dan relevansi bisnis.
- Penyusunan Laporan dan Rekomendasi: Yaitu hasil dari setiap tahapan dirangkum dalam laporan akhir yang memuat deskripsi kerentanan, bukti eksploitasi, dampak potensial, dan langkah-langkah mitigasi yang disarankan.

2.2 Alasan Pemilihan Metode

Pendekatan OWASP dipilih karena metodologinya bersifat terbuka, terstruktur, dan telah terbukti digunakan oleh banyak profesional keamanan informasi (Ziro et al., 2023). Kombinasi antara teknik otomatis dan analisis manual memungkinkan proses pengujian yang lebih menyeluruh dan akurat. Di sisi lain, integrasi *Common Vulnerability Scoring System* (CVSS v3.1 (Nielsen & Molich, 1990)) dan *OWASP Risk Rating* (Silvia et al.,

DOI : https://doi.org/10.37277/stch.v35i2.2383

2015) *Methodology* memungkinkan penilaian risiko yang tidak hanya teknis, tetapi juga memperhatikan kemungkinan eksploitasi serta dampaknya terhadap institusi rumah sakit (Lallie et al., 2021). Hal ini sejalan dengan saran dari Lallie et al. (Lallie et al., 2021) dalam jurnal *Computers & Security* yang menyebut pentingnya pendekatan holistik dalam *risk assessment*.

2.3 Alat dan Lingkungan Penelitian

Dalam pelaksanaan penelitian ini, digunakan seperangkat perangkat keras dan perangkat lunak yang saling mendukung untuk menunjang proses pengujian keamanan situs web. Dari sisi perangkat keras, peneliti menggunakan sebuah laptop *Lenovo Ideapad* 3 14IIL05 yang dibekali dengan prosesor *Intel Core* i3-1005G1, memori RAM sebesar 12 GB, serta penyimpanan SSD 500 GB. Spesifikasi ini dipilih karena cukup memadai untuk menjalankan berbagai *tools* analisis keamanan siber, termasuk yang berbasis virtualisasi.

Untuk perangkat lunak, sistem pengujian dilakukan dalam lingkungan *Kali Linux* versi 2024.4 yang dijalankan melalui *VirtualBox* di atas sistem operasi *Windows* 11. *Kali Linux* dipilih karena merupakan distribusi *Linux* yang secara khusus dirancang untuk kebutuhan *penetration testing* dan *ethical hacking*, serta menyediakan berbagai *tools* bawaan yang relevan (Kaur & Kaur, 2022). Beberapa *tools* utama yang digunakan meliputi *OWASP ZAP* v2.15.0 sebagai alat *scanning* kerentanan web, serta *Burp Suite* versi 2024.11.2 untuk eksploitasi dan analisis lalu lintas HTTP (Ziro et al., 2023).

Untuk pengujian injeksi SQL, digunakan *Sqlmap*, sedangkan *SSL Labs* dan *Seography.io* dimanfaatkan secara daring untuk mengevaluasi konfigurasi SSL serta mendeteksi adanya konten campuran (*mixed content*) (Al-Qarni, 2023). Guna mendukung penilaian risiko yang terukur, peneliti mengandalkan dua pendekatan standar, yakni *CVSS Calculator* v3.1 untuk analisis teknis berbasis skor kerentanan, dan *OWASP Risk Rating* (Silvia et al., 2015) *Calculator* untuk menilai tingkat risiko berdasarkan faktor kontekstual dan organisasi. Dengan kombinasi perangkat keras yang memadai dan perangkat lunak yang tepat sasaran, lingkungan penelitian ini memungkinkan proses pengujian berjalan secara optimal dan mendalam, sehingga hasil yang diperoleh dapat merepresentasikan kondisi nyata dari keamanan situs web yang diuji.

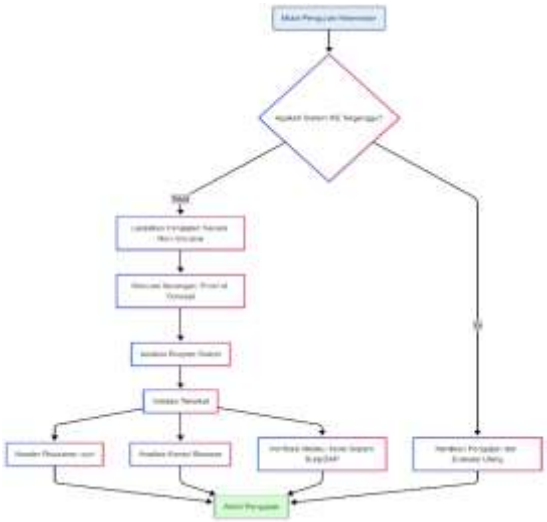
2.4 Validasi dan Etika Pengujian

Proses pengujian keamanan dalam penelitian ini dirancang dengan sangat memperhatikan etika dan prinsip *non-intrusive* terhadap sistem produksi rsjsh.co.id. Hal ini berarti setiap tahapan pengujian dilakukan tanpa mengganggu layanan operasional rumah sakit atau mencoba mengakses data sensitif pasien dan institusi.

Validasi hasil temuan kerentanan dilakukan melalui jalur yang terstruktur, sebagaimana digambarkan pada Gambar 3. Validasi dan Etika Pengujian:

- Simulasi Serangan (*Proof of Concept*): Jalur pertama adalah dengan melakukan simulasi serangan atau *proof of concept*. Ini bertujuan untuk menunjukkan bahwa kerentanan yang teridentifikasi benar-benar dapat dieksploitasi dalam skenario yang terkontrol dan tidak merusak. Setelah simulasi, dilakukan analisis respons sistem untuk memahami perilaku dan dampak potensial kerentanan.
- Konfirmasi Teknis: Jalur kedua melibatkan konfirmasi teknis melalui berbagai metode. Validasi ini mencakup pemeriksaan respons *header* menggunakan perintah curl untuk memverifikasi keberadaan *header* keamanan yang relevan, analisis konsol *browser* untuk mendeteksi anomali atau pesan kesalahan terkait keamanan, serta verifikasi tambahan menggunakan *tools* pengujian seperti *Burp Suite* dan *OWASP ZAP*.

DOI : https://doi.org/10.37277/stch.v35i2.2383



Gambar 3.
Validasi dan Etika Pengujian Posisi

Jika selama proses pengujian terdeteksi adanya indikasi gangguan pada sistem rumah sakit (*"Apakah Sistem RS Terganggu?"*), prosedur akan langsung menginstruksikan untuk menghentikan pengujian dan melakukan evaluasi ulang. Namun, jika tidak ada gangguan (*"Tidak"*), pengujian akan dilanjutkan secara *non-intrusive* sesuai alur yang ditetapkan. Proses validasi teknis ini akan mengkonfirmasi temuan dan, setelah semua tahapan selesai, akan mencapai tahap *Akhir Pengujian*.

3. Hasil dan Pembahasan

Pengujian keamanan terhadap situs web rsjsh.co.id dilakukan melalui pendekatan *penetration testing* berlandaskan kerangka *OWASP Testing Guide* v4 (Tohir, 2017) yang kemudian divalidasi melalui dua dimensi: teknis dan kontekstual organisasi. Penilaian teknis menggunakan CVSS v3.1 (Nielsen & Molich, 1990), sedangkan penilaian konteks risiko menggunakan *OWASP Risk Rating* (Silvia et al., 2015) *Methodology*. Bab ini memaparkan hasil pengujian berdasarkan tahapan serta analisis atas kerentanan yang ditemukan.

3.1 Hasil *Footprinting* dan *Information Gathering*

Pada tahap awal, identifikasi sistem dilakukan menggunakan alat seperti nslookup, whois, dan whatweb. Diperoleh informasi penting, di antaranya:

- Situs menggunakan server *Imunify360-Webshield*, yang menandakan adanya upaya mitigasi dasar terhadap serangan *brute-force* dan DDoS.
- Situs tidak menerapkan DNSSEC, serta tidak memiliki perlindungan keamanan tambahan dari sisi registrar.
- Teknologi yang digunakan tidak mencantumkan *Content Management System* (CMS) secara eksplisit, sehingga celah eksploitasi perlu dicari pada lapisan lain. Hasil *footprinting* ini memperkuat dasar untuk melakukan pemindaian lebih lanjut terhadap potensi celah keamanan.

3.2 Hasil Pemindaian (*Scanning*)

Pengujian dengan *Nmap* menunjukkan bahwa terdapat 12 *port* TCP terbuka, di antaranya *port* 80, 443, 3306—*port* umum untuk HTTP(S) dan basis data *MySQL*. Meskipun *port* ini terlindungi dengan *firewall*, mereka tetap menjadi jalur potensial bagi eksploitasi jika konfigurasi layanan tidak aman. Alat *OWASP ZAP* berhasil mendeteksi 11 temuan kerentanan, terdiri dari:

- 3 risiko sedang (*medium*)
- 4 risiko rendah (*low*)
- 4 bersifat informatif (*informational*)

Sementara itu, *SSL Labs* memberikan penilaian A+ atas konfigurasi TLS, menandakan kekuatan sistem dalam lapisan transport, meskipun celah tetap ditemukan di lapisan aplikasi. Berikut adalah ringkasan nilai *Base Score* CVSS terhadap kerentanan yang divalidasi:

Tabel 3. Nilai *Base Score* CVSS v3.1 Posisi Tabel

No	Kerentanan	CVSS v3.1	Risiko
1	*Content-Security-Policy Not Set*	8.3	Tinggi
2	*Mixed Content*	7.2	Tinggi

DOI : https://doi.org/10.37277/stch.v35i2.2383

No	Kerentanan	CVSS v3.1	Risiko
3	*Anti-Clickjacking Header Not Set*	4.7	Sedang

Nilai Tabel 3 diperoleh dengan memperhitungkan *vector string* lengkap berdasarkan komponen *Attack Vector* (AV), *Attack Complexity* (AC), dan lainnya sesuai standar CVSS.

3.3 Eksploitasi Kerentanan dan Validasi Hasil

Simulasi dilakukan terhadap kerentanan yang dinilai signifikan:

- *Clickjacking* berhasil divalidasi dengan menyisipkan skrip *iframe*, yang memungkinkan manipulasi antarmuka web secara tidak sah.
- CSP *Not Set* dibuktikan dengan menggunakan *Burp Suite* dan validasi *header* melalui *command prompt* dan *browser console*, menunjukkan tidak adanya direktif CSP aktif.
- *Mixed Content* terdeteksi melalui *seography.io*, yang menunjukkan adanya halaman HTTP dalam situs HTTPS dan berhasil diakses sebagai bukti validitas. Namun, upaya eksploitasi jenis XSS (*Stored*, *Reflected*, dan DOM) serta *SQL Injection* tidak membuahkan hasil karena sistem tampaknya telah menerapkan validasi *input* dan *Web Application Firewall* (WAF) yang efektif.

3.4 Evaluasi Risiko dengan *OWASP Risk Rating*

Penilaian Risiko Keamanan *Website* yang lebih kontekstual adalah dengan menggunakan *OWASP Risk Rating* (Silvia et al., 2015) *Calculator*, dengan menunjukkan hasil sebagai berikut:

Tabel 4. *OWASP Risk Rating Calculator* Posisi Tabel

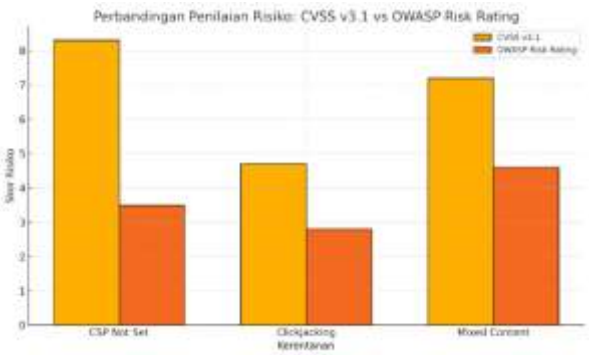
No	Kerentanan	OWASP	Kategori
1	*Content-Security-Policy Not Set*	3.5	*Medium*
2	*Mixed Content*	4.6	*Medium*
3	*Anti-Clickjacking Header Not Set*	2.8	*Low*

Metodologi *OWASP Risk Rating* (Silvia et al., 2015) mengombinasikan *Likelihood Factors* (seperti *Skill Level* dan *Opportunity*) dan *Impact Factors* (seperti *Reputation Damage* dan *Privacy Violation*), menghasilkan skor yang merefleksikan relevansi risiko terhadap organisasi.

3.5 Analisis Komparatif Penilaian Risiko

Terdapat perbedaan penting antara dua metode penilaian risiko:

- CVSS v3.1 (Nielsen & Molich, 1990) lebih menekankan aspek teknis, yaitu seberapa rentan sistem terhadap eksploitasi murni.
- *OWASP Risk Rating* (Silvia et al., 2015) memasukkan dimensi organisasi, yaitu potensi kerugian bisnis, reputasi, dan privasi pengguna.



Gambar 4. Perbandingan CVSS v3.1 dan *OWASP Risk Rating*

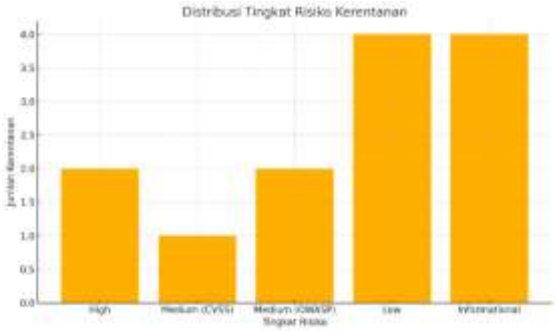
Keduanya saling melengkapi. Sebagai contoh, meskipun CSP *not set* memiliki skor tinggi di CVSS (8.3), dalam OWASP hanya berada di level menengah (3.5) karena mitigasi sudah tersedia meski belum diterapkan.

3.6 Implikasi Temuan dan Rekomendasi Strategis

Temuan membuktikan bahwa situs web layanan publik seperti rumah sakit sangat

DOI : https://doi.org/10.37277/stch.v35i2.2383

penting untuk diamankan pada level aplikasi. Kekurangan kecil pada konfigurasi *security header* dapat membuka celah besar bagi penyerang.



Gambar 5. Data Hasil Pemindaian CVSS dan *OWASP Risk Rating*

Implikasi dari celah seperti CSP dan *mixed content* bukan hanya teknis, namun juga memengaruhi kepercayaan publik dan integritas layanan.

Tabel 5. Perbandingan Skor CVSS vs *OWASP Risk Rating*

Kerentanan	CVSS	*OWASP*
Content-Security-Policy Not Set	8.3 (*High*)	3.5 (*Medium*)
Anti-Clickjacking Header Not Set	4.7(*Medium*)	2.8 (*Low*)
Mixed Content	7.2 (*High*)	4.6(*Medium*)

4. Kesimpulan

Berdasarkan Penelitian ini berhasil mengungkap sejumlah celah keamanan signifikan pada situs web layanan publik rsjsh.co.id, dengan pendekatan pengujian berbasis metode *penetration testing* yang mengacu pada *OWASP Testing Guide* v4 (Tohir, 2017). Dari hasil pengujian yang telah dilakukan, ditemukan total 11 kerentanan, yang terdiri atas 3 kerentanan risiko sedang, 4 risiko rendah, serta 4 kategori informasional. Tiga kerentanan utama yang berhasil divalidasi secara teknis adalah:

- *Content Security Policy* (CSP) *Not Set*,
- *Clickjacking* (*Anti-clickjacking header not set*), dan
- *Mixed Content* (konten HTTP pada halaman HTTPS).

Masing-masing dari kerentanan tersebut memiliki dampak yang nyata. CSP *not set* membuka peluang terhadap serangan XSS, *clickjacking* mengeksploitasi kelemahan antarmuka pengguna, dan *mixed content* berpotensi menurunkan tingkat enkripsi yang seharusnya dijaga oleh HTTPS, membuka pintu bagi serangan *man-in-the-middle*.

Melalui dua pendekatan penilaian risiko, yaitu CVSS v3.1 (Nielsen & Molich, 1990) dan *OWASP Risk Rating* (Silvia et al., 2015), terlihat adanya dimensi yang saling melengkapi: CVSS menyoroti aspek teknikal dan tingkat eksploitasi, sedangkan OWASP mempertimbangkan dampak organisasi seperti reputasi dan kepatuhan regulasi. Misalnya, meskipun CSP *not set* memiliki skor tinggi pada CVSS (8.3 – *High*), namun dalam OWASP dinilai *medium* (3.5) karena mitigasinya dianggap dapat diimplementasikan dengan cepat.

Secara keseluruhan, penelitian ini menyimpulkan bahwa tingkat risiko keamanan situs web rsjsh.co.id berada pada kategori sedang (*medium*). Dengan mempertimbangkan sensitivitas data yang mungkin diproses oleh sistem layanan rumah sakit, maka penerapan strategi keamanan yang holistik menjadi keharusan, terutama dalam memperkuat konfigurasi *security headers*, menerapkan kebijakan konten (*Content Security Policy*), serta menjaga integritas protokol enkripsi seperti HTTPS.

Daftar Pustaka

Aji, M. P. (2022). Sistem keamanan siber dan kedaulatan data di Indonesia dalam perspektif ekonomi politik (studi kasus perlindungan data pribadi). *Jurnal Politica: Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 13*(2), 222–238.

Al-Ansi, S., et al. (2021). A comprehensive analysis of web vulnerabilities in healthcare websites: A case study of Yemen. *International Journal of Advanced Computer Science and Applications, 12*(1), 119–126.

Al-Qarni, E. A. (2023). Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. *International*

DOI : https://doi.org/10.37277/stch.v35i2.2383

Journal of Advanced Computer Science and Applications, 14(5), 135–142.

CISA. (2023). *Healthcare cybersecurity best practices*. Cybersecurity and Infrastructure Security Agency.

Cybellium Ltd. (2023). *Mastering OWASP*.

Dimas, P. V., Saputra, C. A., & Wardhana, R. C. (2023). Analisis kerentanan web berdasarkan OWASP Top 10 menggunakan metode vulnerability assessment dan penetration testing. *Jurnal Sistem Informasi dan Teknologi, 5*(2), 102–110.

Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019, January). Mendeteksi kerentanan keamanan aplikasi website menggunakan metode OWASP (Open Web Application Security Project) untuk penilaian risk rating. *Creative Information Technology Journal, 4*(4), 264–264.

Gupta, T. J., Singh, A. K., & Bhatia, M. P. S. (2021). Cybersecurity in healthcare: Threats, challenges, and solutions. *Journal of Cybersecurity, 5*(1), 1–15.

Kaur, K., & Kaur, P. (2022). A survey on web application penetration testing. *Procedia Computer Science, 200*, 1229–1238.

Kusrini. (2007). *Konsep dan aplikasi sistem pendukung keputusan*. Yogyakarta: Andi.

J-sika, Munawar, Z., & Putri, N. I. (2020). Keamanan jaringan komputer pada era big data. *J-SIKA: Jurnal Sistem Informasi Karya Anak Bangsa, 2*(1), 14–20.

Lallie, J., et al. (2021). Cyber security in the age of COVID-19: A review of cyber threats and how to mitigate them. *Computers & Security, 105*, 102237.

Lewis, J. R. (2014). Usability: Lessons learned… and yet to be learned. *International Journal of Human–Computer Interaction, 30*(9), 663–684.

Tohir, A. S. (2017). Pemodelan sistem data terdistribusi untuk mengintegrasikan data akademik dan keuangan. *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, 1*(1), 44–52.

Mell, M., Scarfone, S., & Roman, J. (2020). *NIST special publication 800-115: Technical guide to information security testing and assessment*. National Institute of Standards and Technology.

Nielsen, J., & Molich, R. (1990). Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 249–256).

Mishra, S. (2021). *Web penetration testing: Hack your way*. India: Shubham Mishra.

Nurdiansyah, D., Anindira, Y. D., Muhibin, S. S., & Putri, A. H. (2023, February). Sosialisasi digital security dalam meningkatkan edukasi bermedia digital di lingkungan masyarakat Depok Baru. *Karunia: Jurnal Hasil Pengabdian Masyarakat Indonesia, 2*(1), 109–120.

Priambodo, D. F., Rifansyah, A. D., & Hasbi, M. (2023, February). Penetration testing Web XYZ berdasarkan OWASP risk rating. *Teknika, 12*(1), 33–46.

Springer International Publishing. (2020). *Information and cyber security: 19th International Conference, ISSA 2020, Pretoria, South Africa, August 25–26, 2020, Revised selected papers*. Cham, Switzerland.

Silvia, S., Leonita, C., Virginia, V., Candra, Y. J., & Sevani, N. (2015). Aplikasi diagnosis karies pada gigi manusia berbasis web. *Ultima Journal of Informatics, 7*(1), 43– 49.

Syalendra, D., & Nuraini, A. (2020). Analisis keamanan website pemerintah menggunakan OWASP Top 10. *Jurnal Ilmiah Teknologi Informasi dan Komunikasi, 1*(2), 97–104.

Syiah Kuala University Press. (2023). *Kejahatan siber ancaman dan permasalahannya: Tinjauan yuridis pada upaya pencegahan dan pemberantasannya di Indonesia*.

Tiram Media. (2023). *Panduan praktis dasar-dasar pembuatan website*.

T. (2023). Improved method for penetration testing of web applications. In *IntelITSIS'2023: 4th International Workshop on Intelligent Information Technologies and Systems of Information Security* (pp. 35–45).

Ziro, M. E., Gnatyuk, S. M., & Toibayeva, S. (2023). *Improved method for penetration testing of web applications. In IntelITSIS'2023: 4th International Workshop on Intelligent Information*

DOI : https://doi.org/10.37277/stch.v35i2.2383
Technologies and Systems of Information Security (pp. 35–45).