Router : Jurnal Teknik Informatika dan Terapan
Volume. 2 No. 4 Desember 2024
e-ISSN: 3032-3312; dan p-ISSN: 3026-3611, Hal 01-12
DOI: https://doi.org/10.62951/router.v2i4.268
Available Online at: https://journal.aptii.or.id/index.php/Router

Analisis Keamanan Aplikasi Rekam Medis Elektronik Mengunakan Metode *Penetration Testing* pada UPTD RSD Besemah

Angga Putrawansyah PB [1*], Tata Sutabri [2]
[1,2] Universitas Bina Darma, Indonesia
Email : Ang.putra777@gmail.com [1] , Tata.Sutabri@gmail.com [2]*

Abstract, *Security of electronic medical records (EMR) data is very important in maintaining the confidentiality, integrity, and availability of sensitive patient information. This study aims to conduct a security analysis of the EMR application used at UPTD RSD Besemah Pagar Alam City using the Penetration Testing method. This method is carried out to identify, exploit, and provide solutions to potential vulnerabilities in the EMR application system. Penetration Testing is carried out through several stages, namely information collection, scanning, exploitation, and post-exploitation, using tools such as Nmap, and OWASP ZAP. The results of the study showed several vulnerabilities in the application, including SQL Injection, Cross-Site Scripting (XSS), and weaknesses in authentication management that could allow unauthorized access to patient data. In addition, exposure to sensitive data that was not properly protected was also found. Based on the results of this test, several recommendations were made to improve system security, such as updating security patches, implementing encryption on all sensitive data. By implementing the recommended mitigation steps, the security of the EMR system at UPTD RSD Besemah is expected to be significantly improved, so that the risk of data leakage can be minimized. This research provides a real contribution in strengthening the security of electronic medical record applications. and is expected to be a reference in improving security systems in other health care institutions.*

Keywords: *application security, electronic medical records, penetration testing, vulnerability, mitigation*

Abstrak, Keamanan data rekam medis elektronik (RME) sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi pasien yang bersifat sensitif. Penelitian ini bertujuan untuk melakukan analisis keamanan terhadap aplikasi RME yang digunakan di UPTD RSD Besemah Kota Pagar Alam menggunakan metode *Penetration Testing*. Metode ini dilakukan untuk mengidentifikasi, mengeksploitasi, dan memberikan solusi terhadap potensi kerentanan yang ada pada sistem aplikasi RME tersebut. Penetration Testing dilakukan melalui beberapa tahapan, yakni pengumpulan informasi, scanning, eksploitasi, dan pasca eksploitasi, dengan menggunakan alat seperti Nmap, dan OWASP ZAP. Hasil penelitian menunjukkan adanya beberapa kerentanan pada aplikasi, di antaranya SQL Injection, Cross-Site Scripting (XSS), dan kelemahan dalam pengelolaan otentikasi yang dapat memungkinkan akses tidak sah ke data pasien. Selain itu, ditemukan juga adanya paparan data sensitif yang tidak terlindungi dengan baik. Berdasarkan hasil pengujian ini, disusun beberapa rekomendasi untuk meningkatkan keamanan sistem, seperti memperbarui patch keamanan, mengimplementasikan enkripsi pada seluruh data sensitif. Dengan penerapan langkah mitigasi yang direkomendasikan, keamanan sistem RME di UPTD RSD Besemah diharapkan dapat ditingkatkan secara signifikan, sehingga risiko kebocoran data dapat diminimalisir. Penelitian ini memberikan kontribusi nyata dalam memperkuat keamanan aplikasi rekam medis elektronik. dan diharapkan dapat menjadi acuan dalam meningkatkan sistem keamanan di institusi pelayanan kesehatan lainnya.

Kata kunci: keamanan aplikasi, rekam medis elektronik, penetration testing, kerentanan, mitigasi

1. LATAR BELAKANG MASALAH

Dalam era digitalisasi yang semakin berkembang, sistem informasi kesehatan telah menjadi komponen penting untuk mendukung pelayanan kesehatan yang efisien, akurat, dan cepat. Salah satu sistem yang memainkan peran sentral adalah aplikasi rekam medis elektronik (Electronic Medical Record/EMR), yang digunakan untuk mengelola data medis pasien secara digital. Sistem ini memungkinkan tenaga medis untuk mengakses dan mengelola informasi

Received: September 12,2024; Revised: September 26,2024; Accepted: November 03, 2024; Published: November 06, 2024

pasien dengan lebih mudah, mulai dari riwayat kesehatan, hasil diagnosis, hingga resep obat, yang pada akhirnya dapat meningkatkan kualitas layanan yang diberikan kepada masyarakat. Namun, transformasi digital di bidang kesehatan tidak terlepas dari tantangan besar, salah satunya adalah keamanan data. Data rekam medis pasien mengandung informasi yang sangat sensitif, termasuk informasi pribadi, riwayat penyakit, hingga data kontak darurat yang jika bocor atau disalahgunakan dapat berdampak serius pada privasi dan keselamatan pasien. Di sisi lain, kerentanan terhadap ancaman keamanan siber seperti hacking, malware, dan phishing juga semakin meningkat. Serangan pada sistem informasi kesehatan dapat menimbulkan risiko yang luas, seperti pencurian data, manipulasi informasi medis, dan bahkan penghentian layanan kesehatan.

Studi sebelumnya menunjukkan bahwa sistem informasi kesehatan, termasuk aplikasi rekam medis elektronik, sering kali memiliki kerentanan yang belum teridentifikasi atau tidak tertangani dengan baik. Beberapa penyebabnya antara lain karena kurangnya *security assessment*, terbatasnya pemahaman dan sumber daya untuk menjaga keamanan data, serta belum optimalnya implementasi kebijakan keamanan siber di banyak fasilitas kesehatan. UPTD RSD Besemah, sebagai salah satu fasilitas kesehatan daerah, memiliki tanggung jawab untuk melindungi data rekam medis pasiennya dari potensi ancaman siber. Pentingnya menjaga kerahasiaan dan integritas data ini membuat penetration testing menjadi salah satu metode yang relevan untuk mengidentifikasi kerentanan dalam sistem rekam medis elektronik yang digunakan.

2. RUMUSAN MASALAH

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat keamanan aplikasi rekam medis elektronik yang digunakan di UPTD RSD Besemah saat ini?
2. Apa saja kerentanan yang terdapat pada aplikasi rekam medis elektronik di UPTD RSD Besemah yang dapat dieksploitasi oleh pihak tidak berwenang?
3. Bagaimana metode penetration testing dapat digunakan untuk mengidentifikasi dan mengevaluasi potensi celah keamanan dalam aplikasi rekam medis elektronik di UPTD RSD Besemah?
4. Rekomendasi apa yang dapat diberikan untuk memperbaiki kerentanan keamanan yang ditemukan pada aplikasi rekam medis elektronik di UPTD RSD Besemah?

3. METODE PENELITIAN

Penelitian ini menggunakan metode *penetration testing* untuk menganalisis tingkat keamanan aplikasi rekam medis elektronik di UPTD RSD Besemah. Metode ini melibatkan serangkaian tahapan sistematis untuk mengidentifikasi, mengeksploitasi, dan mengevaluasi kerentanan yang ada pada sistem. Tujuan utamanya adalah untuk mengungkap potensi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang, sehingga memungkinkan perbaikan yang proaktif sebelum terjadi insiden keamanan. Tahapan *penetration testing* yang diterapkan dalam penelitian ini meliputi:

1. **Pengintaian**

   Pada tahap ini, dilakukan pengumpulan informasi awal terkait aplikasi rekam medis elektronik yang akan diuji. Pengintaian dilakukan untuk memahami struktur aplikasi, jaringan yang digunakan, serta kemungkinan adanya celah keamanan yang bisa dieksploitasi. Tahap ini melibatkan dua pendekatan, yaitu *passive reconnaissance* (mengumpulkan informasi tanpa menyentuh langsung sistem) dan *active reconnaissance* (berinteraksi langsung dengan sistem, misalnya melalui pemindaian jaringan).

2. **Scanning and Enumeration**

   Setelah informasi awal diperoleh, tahap berikutnya adalah pemindaian dan enumerasi untuk mendapatkan data lebih detail tentang jaringan, port, layanan, dan perangkat yang terhubung dengan sistem aplikasi. Alat seperti Nmap digunakan untuk menemukan port terbuka dan mengidentifikasi layanan yang berjalan, yang kemudian dianalisis untuk mencari kerentanan yang dapat dimanfaatkan.

3. **Rekomendasi Pelaporan**

   Setelah seluruh proses uji selesai, hasil temuan dirangkum dalam laporan yang komprehensif. Laporan ini mencakup detail kerentanan yang ditemukan, teknik eksploitasi yang berhasil, serta rekomendasi yang disarankan untuk memperbaiki setiap celah keamanan. Rekomendasi disusun berdasarkan dampak risiko dari setiap kerentanan dan langkah yang paling efektif untuk menanganinya.

4. HASIL DAN PEMBAHASAN

Penelitian ini telah dilakukan melalui beberapa tahap pengujian keamanan terhadap sistem Rekam Medis Elektronik (RME) di UPTD RSD Besemah menggunakan metode Penetration Testing. Hasil penelitian dapat dikelompokkan berdasarkan jenis kerentanan yang

ditemukan, dampak potensial dari eksploitasi, dan rekomendasi mitigasi. Berikut adalah hasil lengkap dari setiap tahap pengujian:

1. **Hasil Pengintaian dan Scanning**

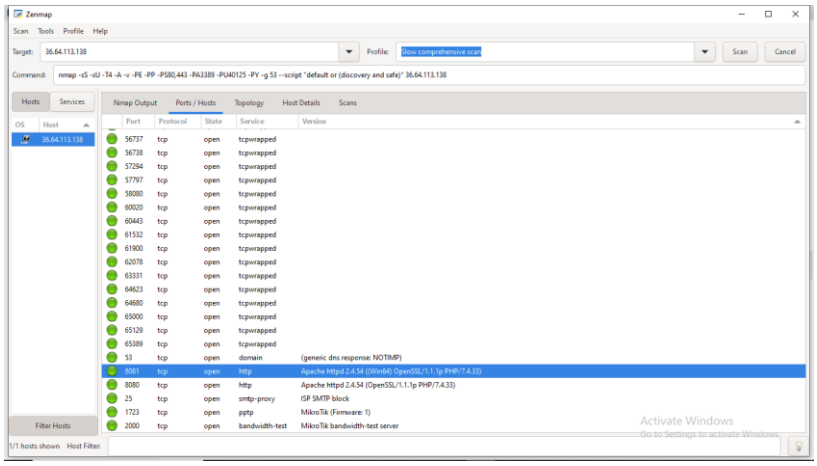
Pada tahap ini, dilakukan pengumpulan informasi mengenai sistem RME, termasuk teknologi yang digunakan, versi perangkat lunak, serta pemindaian jaringan. Alat yang digunakan adalah Nmap untuk scanning port dan identifikasi layanan yang berjalan di server. Beberapa hasil yang diperoleh dari tahapan ini meliputi:

a. Hasil Pengintaian domain dan IP Address

Hasil pengintaian Pada Aplikasi Target RME UPTD RSD Besemah Kota Pagar Alam dengan Situs Aplikasi : https://rsdbesemah.id:8080/simrs/ dengan alat **DNS LOOKUP** sehingga mendapatkan Informasi sebagai berikut :

- Domain Name : rsdbesemah.id
- IP Address : 36.64.113.138

b. Scanning and Enumeration



Dari hasil pengingtaian diatas, informasi yang didapat digunakan untuk scanning yang menggunakan alat Nmap sehingga menghasilkan informasi port 8080 dan 8081 terbuka yang menjalankan Apache, Setelah mengetahui port yang terbuka pada server yang menjalankan **Apache**, Anda dapat melakukan beberapa

jenis serangan yang tergantung pada layanan dan aplikasi yang berjalan di server tersebut. Berikut adalah beberapa serangan yang dapat dipertimbangkan:

1. Serangan SQL Injection

   Jika ada aplikasi web yang menggunakan basis data dan menerima input pengguna (misalnya, melalui parameter URL atau formulir), Anda bisa mencoba melakukan SQL Injection untuk mengeksploitasi database.
2. Cross-Site Scripting (XSS)

   Jika aplikasi web mengizinkan input pengguna yang tidak disanitasi, Anda dapat mencoba menyisipkan skrip JavaScript berbahaya untuk menguji kerentanan XSS.
3. Remote File Inclusion (RFI)

   Jika ada parameter dalam aplikasi yang memungkinkan untuk menyertakan file dari URL, Anda bisa mencoba serangan RFI untuk mengeksekusi file eksternal atau membaca file lokal pada server.
4. Directory Traversal

   Jika aplikasi memungkinkan penggunanya untuk mengakses file di luar direktori yang diizinkan, Anda bisa mencoba melakukan serangan Directory Traversal dengan menyisipkan karakter ../ dalam URL.
5. Serangan Denial of Service (DoS)

   Dengan mengeksploitasi server Apache, Anda dapat mencoba serangan DoS untuk membuat layanan tidak tersedia dengan membanjiri server dengan permintaan yang berlebihan.
6. Pencarian Kerentanan dan Eksploitasi

   Setelah mengetahui versi Apache, Anda bisa mencari kerentanan yang diketahui (misalnya, melalui CVE) dan mengeksploitasi kerentanan tersebut menggunakan alat seperti Metasploit atau eksploit yang telah ditemukan.
7. Brute Force Attacks

   Jika ada halaman login yang terbuka (misalnya, admin panel), Anda dapat mencoba melakukan serangan brute force untuk mendapatkan akses menggunakan alat seperti Hydra atau Burp Suite.

8. Man-in-the-Middle (MitM)

   Jika komunikasi antara klien dan server tidak dienkripsi (misalnya, menggunakan HTTP alih-alih HTTPS), Anda dapat melakukan serangan MitM untuk mencegat dan memanipulasi data yang ditransmisikan.

9. Pengambilan Informasi

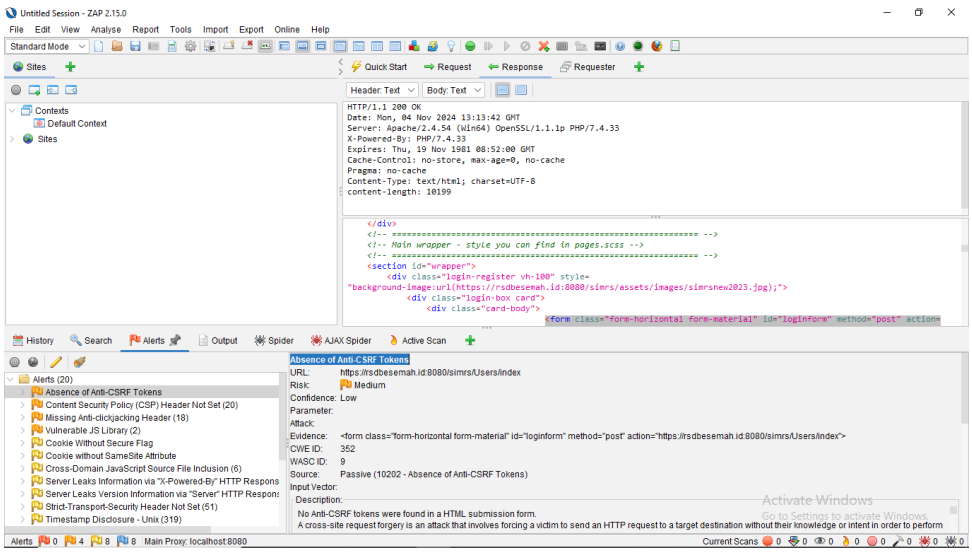
   Dengan menggunakan teknik seperti banner grabbing, Anda dapat mengumpulkan informasi lebih lanjut tentang versi perangkat lunak yang digunakan, konfigurasi server, dan potensi kerentanan.

10. Exploitation of Misconfigured Services

    Jika server Apache mengizinkan akses ke file atau direktori sensitif (misalnya, konfigurasi, file log), Anda bisa mencoba untuk mengakses informasi sensitif yang dapat dieksploitasi lebih lanjut.

Selain menggunanken Nmap Scanning Aplikasi ini juga mengunakan alat OWASP ZAP yang mana dengan menggunakan OWASP ZAP ini Temuan akan diklasifikasikan dengan CWE ID, atau Common Weakness Enumeration Identifier adalah sistem pengklasifikasian yang digunakan untuk mengidentifikasi dan mengategorikan kelemahan keamanan dalam perangkat lunak, pada sacanning yang alat OWASP ZAP ditemukan beberapa kerantaan pada aplikasi ini diataranya:

1. Absence of Anti-CSRF Tokens

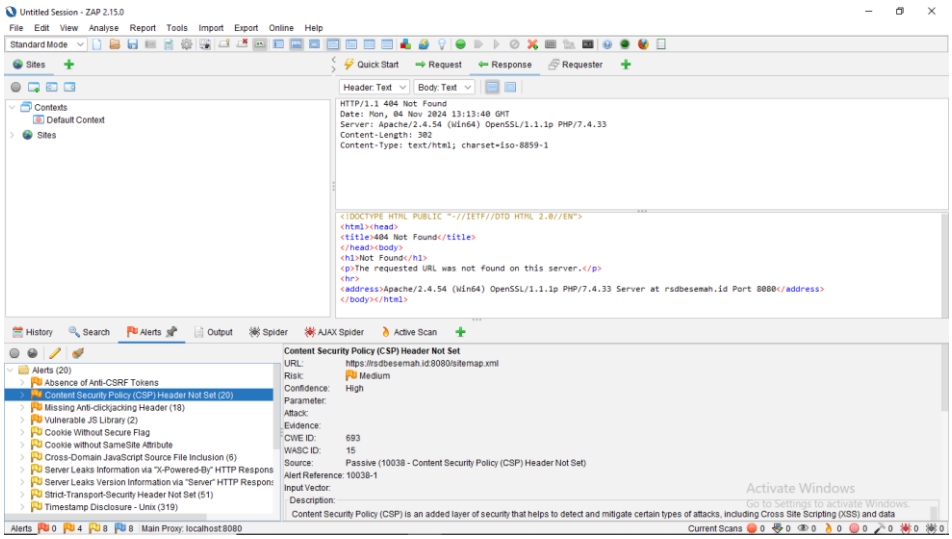


Absence of Anti-CSRF Tokens adalah kelemahan keamanan yang terjadi ketika aplikasi web tidak menerapkan token Anti-CSRF (Cross-Site Request Forgery) untuk melindungi dari serangan CSRF. CSRF adalah jenis

serangan di mana penyerang membajak otentikasi pengguna yang telah masuk untuk membuat permintaan yang tidak sah atas nama pengguna tersebut, sering kali tanpa sepengetahuan mereka, pada temuan ini kelasifikasi Kelemahan Kemanan pada Aplikasi ini adalah CWE ID 352 merujuk pada "Cross-Site Request Forgery (CSRF)". Ini adalah kerentanan keamanan yang terjadi ketika aplikasi web tidak memverifikasi bahwa permintaan yang dikirimkan ke server berasal dari sumber yang tepercaya, yang memungkinkan penyerang untuk melakukan aksi atas nama pengguna yang tidak sadar.

Cross-Site Request Forgery (CSRF) adalah jenis serangan di mana penyerang dapat mengirimkan permintaan yang tidak sah ke aplikasi web yang diotentikasi, memanfaatkan sesi yang sudah ada. Jika pengguna yang sudah masuk ke akun mereka mengklik tautan jahat atau mengunjungi situs yang terinfeksi, permintaan berbahaya dapat dikirimkan ke server yang mengeksekusi tindakan yang tidak diinginkan.

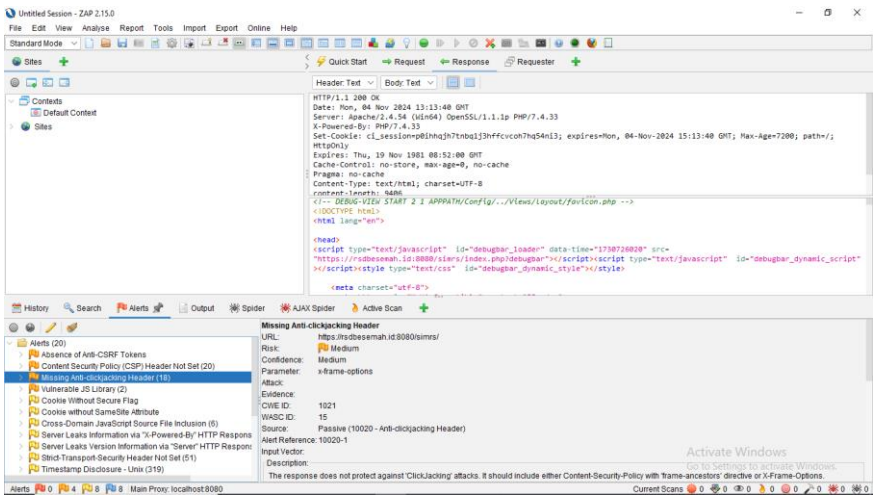
2.Content Security Policy (CSP) Header Not Set



Content Security Policy (CSP) Header Not Set adalah kelemahan keamanan yang terjadi ketika sebuah aplikasi web tidak menerapkan header CSP, yang berfungsi untuk membantu melindungi aplikasi dari berbagai serangan, terutama serangan Cross-Site Scripting (XSS) dan data injection. CSP adalah mekanisme keamanan yang memungkinkan pengembang untuk menentukan sumber daya yang diizinkan untuk dimuat dan dieksekusi oleh browser saat mengunjungi suatu halaman web. Dengan mengatur kebijakan ini, pengembang dapat mencegah penyerang menyisipkan skrip jahat atau

melakukan aksi berbahaya lainnya di situs mereka, pada temuan ini kelasifikasi Kelemahan Kemanan pada Aplikasi ini adalah CWE ID 693 merujuk pada "Protection Mechanism Failure"**.** Ini adalah kerentanan yang terjadi ketika mekanisme perlindungan yang seharusnya ada dalam sebuah aplikasi atau sistem tidak berfungsi dengan baik, tidak diimplementasikan, atau tidak memadai, sehingga memungkinkan penyerang untuk mengeksploitasi kelemahan dalam keamanan. Protection Mechanism Failure mengacu pada situasi di mana sistem keamanan yang dirancang untuk melindungi data atau fungsi penting gagal menjalankan tugasnya. Kegagalan ini bisa disebabkan oleh berbagai faktor, termasuk kesalahan konfigurasi, desain yang buruk, atau kelalaian dalam penerapan mekanisme perlindungan.

3.Missing Anti-clickjacking Header



Missing Anti-clickjacking Header adalah kelemahan keamanan yang terjadi ketika sebuah aplikasi web tidak menerapkan header yang diperlukan untuk melindungi pengguna dari serangan clickjacking. Clickjacking adalah teknik serangan di mana penyerang menipu pengguna untuk mengklik elemen yang berbeda dari yang mereka lihat, biasanya dengan menyisipkan halaman web ke dalam iframe yang tidak terlihat atau terbungkus dalam lapisan transparan, pada temuan ini kelasifikasi Kelemahan Kemanan pada Aplikasi ini adalah CWE ID 1021 merujuk pada "Improper Restriction of Rendered UI Layers or Frames"**.** Ini adalah kerentanan yang terjadi ketika aplikasi gagal untuk membatasi lapisan atau bingkai antarmuka pengguna (UI) dengan benar, memungkinkan pengguna atau penyerang untuk mengakses atau berinteraksi dengan bagian aplikasi yang tidak seharusnya

mereka lihat atau control, Improper Restriction of Rendered UI Layers or Frames mengacu pada kesalahan dalam pengendalian elemen antarmuka pengguna yang bisa menyebabkan pengguna tidak berwenang dapat mengakses atau mengubah informasi sensitif. Ini sering kali terjadi dalam aplikasi web atau desktop di mana elemen UI dapat dikendalikan oleh pengguna, tetapi tidak memiliki batasan atau perlindungan yang memadai.

C. Rekomendasi Pelaporan

Berdasarkan hasil temuan, sejumlah rekomendasi mitigasi telah disusun:

1. Implementasi Parameterized Queries: Untuk mencegah SQL Injection, penting untuk menerapkan parameterized queries dan validasi input pengguna di semua form yang berinteraksi dengan database.
2. Sanitasi dan Validasi Input: Untuk mengatasi kerentanan XSS, sistem harus memastikan bahwa semua input pengguna disanitasi dan divalidasi secara ketat.
3. Peningkatan Keamanan Manajemen Sesi: Menerapkan kebijakan pengelolaan sesi yang ketat, termasuk penggunaan session timeout yang lebih pendek dan pengaturan cookie yang lebih aman.
4. Audit dan Pembaruan Rutin: Melakukan audit keamanan secara berkala dan memastikan bahwa semua perangkat lunak diperbarui untuk melindungi sistem dari kerentanan yang dikenal.

5. KESIMPULAN DAN SARAN

Penelitian ini telah melakukan analisis keamanan terhadap aplikasi Rekam Medis Elektronik (RME) di UPTD RSD Besemah dengan menggunakan metode Penetration Testing. Berdasarkan hasil pengujian dan analisis, dapat diambil beberapa kesimpulan utama sebagai berikut:

1. Penelitian ini mengidentifikasi beberapa kerentanan kritis dalam sistem RME, termasuk SQL Injection, Cross-Site Scripting (XSS), dan manajemen sesi yang lemah. Kerentanan-kerentanan ini berpotensi disalahgunakan oleh penyerang untuk mendapatkan akses tidak sah ke data medis pasien, yang dapat mengakibatkan kebocoran data dan penyalahgunaan informasi.
2. Kerentanan yang ditemukan dapat memiliki dampak serius terhadap keamanan data pasien, termasuk risiko kebocoran informasi pribadi dan kehilangan kepercayaan dari

pasien terhadap layanan kesehatan. Hal ini juga dapat berdampak pada reputasi institusi dan kepatuhan terhadap regulasi perlindungan data yang berlaku.

3. Penelitian ini memberikan rekomendasi mitigasi yang jelas dan praktis, termasuk penerapan parameterized queries untuk mencegah SQL Injection, sanitasi dan validasi input untuk mengatasi XSS, serta peningkatan keamanan manajemen sesi. Selain itu, pentingnya audit keamanan secara berkala dan pembaruan perangkat lunak juga ditekankan.
4. Penelitian ini menunjukkan bahwa kesadaran akan pentingnya keamanan informasi dalam pengelolaan sistem kesehatan harus ditingkatkan. Pelatihan bagi pengembang dan staf IT mengenai praktik keamanan yang baik sangat diperlukan untuk mengurangi risiko kerentanan yang mungkin muncul di masa mendatang.
5. Mengingat sifat sensitif dari data medis, langkah proaktif dalam mengidentifikasi dan mengatasi kerentanan sangat penting. Penerapan langkah-langkah mitigasi yang tepat dapat membantu melindungi data pasien dan menjaga integritas sistem.

Dengan demikian, hasil penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam meningkatkan keamanan aplikasi RME di UPTD RSD Besemah dan menjadi acuan bagi institusi kesehatan lainnya dalam melindungi data sensitif pasien. Penelitian lebih lanjut juga disarankan untuk mengeksplorasi teknik keamanan yang lebih canggih dan mempertimbangkan perkembangan terbaru dalam dunia keamanan siber.

DAFTAR REFERENSI

ANS Institute. (2020). “The Top Cyber Security Trends for 2020.” Diakses dari https://www.sans.org/

Arrofi, R. A., Ajie, R., Hersya, D. A., & Sutabri, T. (2024). Metaverse dan implikasinya pada privasi dan keamanan data pengguna. *IJM: Indonesian Journal of Multidisciplinary, 2*(1), [halaman].

CVE Details. (n.d.). CVE Details. Diambil dari https://www.cvedetails.com/

CWE - Common Weakness Enumeration. (n.d.). Retrieved from https://cwe.mitre.org

Hart, J. (2018). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press.

Imperva. (n.d.). *Understanding Denial of Service Attacks*. Diambil dari https://www.imperva.com/learn/application-security/denial-of-service-attacks/

Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security: Private Communication in a Public World*. Prentice Hall.

Open Web Application Security Project (OWASP). (n.d.). *OWASP Testing Guide*. Diambil dari https://owasp.org/www-project-web-security-testing-guide/

OWASP Foundation. (2021). *OWASP Top Ten: The Ten Most Critical Web Application Security Risks*. Diakses dari https://owasp.org/www-project-top-ten/

Putra, C. A., Pratama, R., & Sutabri, T. (2023). *Analisis Manfaat Machine Learning pada Next-Generation Firewall Sophos XG 330 dalam Mengatasi Serangan SQL Injection*. Program Studi Magister Teknik Informatika, Universitas Bina Darma Palembang.

Skoudis, E., & Liston, T. (2006). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.

Sutabri, T. (2012). *Analisis sistem informasi*. Andi.

Sutabri, T. (2023). Design of a web-based social network information system. *International Journal of Artificial Intelligence Research, 6*(1), 310-316. STMIK Dharma Wacana.

Sutabri, T., Wijaya, A.*, Herdiansyah, M. I., & Negara, E. S. (2024). *Evaluasi Risiko Celah Keamanan Aplikasi E-Office menggunakan Metode OWASP*. Program Studi Teknik Informatika, Universitas Bina Darma, Indonesia.

ZAP (OWASP Zed Attack Proxy). (2022). *OWASP ZAP: The World's Most Popular Free Security Tool*. Diakses dari https://www.zaproxy.org/