ABSTRAK

Penggunaan internet dan aplikasi *web* semakin meningkat di berbagai sektor, termasuk pendidikan, kesehatan, keuangan, dan hiburan. Meskipun demikian, aplikasi web sangat rentan terhadap berbagai jenis serangan siber seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, dan injeksi kode, yang dapat mengancam kerahasiaan, ketersediaan, dan integritas data. Seiring dengan perkembangan teknologi Permenkes tahun 2022 mewajibkan seluruh fasilitas kesehatan di Indonesia untuk mengimplementasikan Rekam Medis Elektronik (RME). Rumah Sakit Universitas Andalas (RS UNAND) telah melaksanakan kebijakan ini dengan mengembangkan RME berbasis *web*. Penelitian ini bertujuan untuk mengevaluasi dan menganalisis keamanan aplikasi RME yang digunakan di RS UNAND. Proses *Vulnerability Assessment* dalam penelitian ini dilakukan menggunakan *tool Acunetix Web Vulnerability Scanner* yang dirancang untuk mengidentifikasi dan mengevaluasi kerentanan pada aplikasi *web*. Hasil *scanning* pertama menunjukkan bahwa aplikasi RME RS UNAND memiliki kerentanan yang signifikan dengan *threat level* 3 (*high*). Pada penelitian ini terdapat 573 *alert* yang terdiri dari 1 *level high*, 253 *level medium*, 2 *level low* dan 317 *level informational*. Identifikasi masalah ini diikuti dengan rekapitulasi dan analisis lebih lanjut untuk menentukan langkah-langkah optimalisasi. Beberapa kerentanan utama yang ditemukan meliputi *HTML Form Without CSRF Protection*, *User Credentials are Sent in Clear Text*, *Directory Listing*, *Source Code Disclosure*, *Git Repository Found*, *Multiple Vulnerabilities Fixed in PHP Versions*, dan *Slow HTTP Denial of Service Attack*. Langkah-langkah optimalisasi kemudian diambil melalui review menyeluruh terhadap *source code* dan peningkatan fitur keamanan pada aplikasi RME. Setelah dilakukan optimalisasi, *scanning* kedua menunjukkan penurunan yang signifikan dalam tingkat ancaman, dengan *threat level* aplikasi RME RS UNAND turun menjadi *level* 1 (*low*) dengan rincian 10 *alert* yang terdiri dari 0 *level high* dan *medium*, 7 *level low* dan 3 *level informational* hal ini menunjukkan penurunan sebanyak 98%. Hasil penelitian ini menekankan pentingnya melakukan *assessment* keamanan secara berkala dan mengoptimalkan fitur keamanan untuk melindungi data sensitif dalam sistem rekam medis elektronik.

Kata Kunci : **Aplikasi *Web*, Serangan Siber, *Vulnerability Assesment, Acunetix*, Rekam Medis Elektronik**.

ABSTRACT

The use of the internet and web applications is increasing across various sectors, including education, healthcare, finance, and entertainment. However, web applications are highly vulnerable to various types of cyberattacks such as SQL Injection, Cross-Site Scripting (XSS), and code injection, which can threaten the confidentiality, availability, and integrity of data. With the advancement of technology, the 2022 Ministry of Health Regulation mandates all healthcare facilities in Indonesia to implement Electronic Medical Records (EMR). Rumah Sakit Universitas Andalas (RS UNAND) has adhered to this policy by developing a web-based EMR system. This study aims to evaluate and analyze the security of the EMR application used at RS UNAND. The Vulnerability Assessment process in this research was conducted using the Acunetix Web Vulnerability Scanner tool, designed to identify and evaluate vulnerabilities in web applications. The initial scan revealed significant vulnerabilities in the RS UNAND EMR application with a threat level of 3 (high). The study identified 573 alerts, consisting of 1 high level, 253 medium level, 2 low level, and 317 informational level alerts. This identification was followed by a detailed review and analysis to determine optimization steps. Key vulnerabilities found included HTML Form Without CSRF Protection, User Credentials Sent in Clear Text, Directory Listing, Source Code Disclosure, Git Repository Found, Multiple Vulnerabilities Fixed in PHP Versions, and Slow HTTP Denial of Service Attack. Optimization measures were then taken through a comprehensive review of the source code and enhancement of security features in the EMR application. After optimization, the second scan showed a significant reduction in threat level, with the RS UNAND EMR application's threat level dropping to 1 (low) with 10 alerts, consisting of 0 high and medium levels, 7 low levels, and 3 informational levels. This represents a 98% reduction in alerts, highlighting the effectiveness of the optimization process. The findings of this study underscore the importance of conducting regular security assessments and optimizing security features to protect sensitive data within electronic medical record systems.

Keywords: Web Application, Cyber Attack, Vulnerability Assessment, Acunetix, Electronic Medical Records.