ABSTRAK

Nama : Sepansya Aria Muhammad Asfian

Program Studi : Teknik Informatika

Judul : Pengujian Keamanan *Website* Rumah Sakit Soeharto Heerdjan Dengan Metode *Penetration Testing*

Website rumah sakit menjadi target utama serangan siber karena menyimpan data sensitif pasien, termasuk rekam medis dan informasi pribadi. Penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi, dan mengelola kerentanan keamanan pada *website* Rumah Sakit Soeharto Heerdjan menggunakan metode *Penetration testing*. Metode ini mengacu pada klasifikasi OWASP *Top 10* 2021 dengan fokus pada tiga kategori kerentanan, yaitu I*njection, Insecure Design*, dan *Security Misconfiguration*. Alat yang digunakan dalam pengujian meliputi OWASP ZAP, Nmap, SSL Labs, Burp Suite, dan Seography.io. Proses pengujian dimulai dengan *information gathering* untuk mengidentifikasi teknologi yang digunakan, diikuti dengan *scanning* untuk mendeteksi port terbuka dan layanan aktif. Setelah itu, dilakukan *exploitation* untuk mengeksploitasi kerentanan yang ditemukan dan mengukur dampaknya. Hasil pengujian mengungkapkan beberapa kerentanan dengan tingkat risiko sedang, seperti *Content Security Policy* (CSP) yang tidak diatur, proteksi *anti-clickjacking* yang lemah, serta *mixed content* pada halaman web. Eksploitasi menunjukkan bahwa kerentanan ini dapat dimanfaatkan oleh peretas untuk mendapatkan akses tidak sah atau memanipulasi data. Sebagai langkah mitigasi, penelitian ini memberikan rekomendasi peningkatan keamanan, seperti pengaturan kebijakan keamanan yang lebih ketat, implementasi proteksi clickjacking, serta penerapan HTTPS secara menyeluruh. Diharapkan, penerapan rekomendasi ini dapat memperkuat ketahanan siber *website* rumah sakit, melindungi data pasien, dan menjaga kelancaran operasional layanan digital rumah sakit.

Kata Kunci: Keamanan Siber, Website Rumah Sakit, *Penetration testing*, OWASP Top 10, Kerentanan, Eksploitasi

ABSTRACT

Name : Sepansya Aria Muhammad Asfian

Study Program : Teknik Informatika

Title : *Security Testing of* Soeharto Heerdjan *Hospital Website with Penetration Testing Method*

Hospital websites are prime targets for cyberattacks due to the sensitive patient data they store, including medical records and personal information. This study aims to identify, evaluate, and manage security vulnerabilities on the Soeharto Heerdjan Hospital website using the Penetration testing method. The testing process follows the OWASP Top 10 2021 classification, focusing on three vulnerability categories: Injection, Insecure Design, and Security Misconfiguration. Tools used in this study include OWASP ZAP, Nmap, SSL Labs, Burp Suite, and Seography.io. The testing process begins with information gathering to identify the technologies used, followed by scanning to detect open ports and active services. Subsequently, exploitation is conducted to assess the impact of identified vulnerabilities. The findings reveal several medium-risk vulnerabilities, such as an unset Content Security Policy (CSP), weak anti-clickjacking protection, and mixed content issues on the website. Exploitation tests demonstrate that these vulnerabilities could be leveraged by attackers to gain unauthorized access or manipulate data. As a mitigation step, this study provides security enhancement recommendations, including stricter security policies, implementation of anti-clickjacking protection, and comprehensive HTTPS enforcement. It is expected that applying these recommendations will strengthen the website's cyber resilience, protect patient data, and ensure the smooth operation of the hospital's digital services.

Keywords: Cybersecurity, Hospital Website, Penetration testing, OWASP Top 10, Vulnerability, Exploitation