INTISARI

Laporan analisis keamanan pada tahun 2022 mengungkapkan terdapat kerentanan pada sistem informasi website JDIH Kabupaten Banyumas. Dampak yang ditimbulkan dari kerentanan ini berpotensi akan serangan Distributed Denial Of Service (DDOS) yang dapat mengancam ketersediaan system. Langkah efektif yang dapat diambil yaitu melakukan proses identifikasi serta analisis kerentanan dengan mensimulasikan serangan pada sistem untuk memahami dan mengatasi potensi serangan. Penelitian ini bertujuan untuk mengevaluasi keamanan sistem informasi website JDIH Kabupaten Banyumas dengan teknik penetration testing menggunakan framework OWASP. Hasil penelitian menunjukan sistem informasi website JDIH Kabupaten Banyumas memiliki tujuh kerentanan meliputi Private IP Disclosure, SQL Injection, Cross-Site Scripting (XSS), Clickjacking, Hidden file found, Server leak information, dan DDoS dengan tingkat keparahan dari low sampai critical. Kerentanan ini disebabkan karena kurangnya validasi input, konfigurasi server yang kurang aman, dan penggunaan software yang kurang terbaru yang berpengaruh terhadap confidentiality, integrity, dan availability sistem. Berdasarkan hasil pengukuran kerentanan menggunakan Common Vulnerability Scoring System (CVSS) diperoleh skor rata – rata 5,7 yang mengindikasikan tingkat keparahan medium. Penelitian selanjutnya disarankan untuk mengintegrasikan tools scanning tambahan seperti Nuclei, Nessus, dan Dalfox untuk mendapatkan hasil yang komprehensif karena setiap tools memiliki keunggulan terterntu dalam mendeteksi kerentanan. Temuan ini diharapkab menjadi acuan dalam peningkatan keamanan sistem informasi website JDIH Kabupaten Banyumas untuk meminimalisir resiko serangan cyber pada masa mendatang.

Kata kunci: Analisis, Keamanan, OWASP, CVSS, Kerentanan.

ABSTRACT

The security analysis report in 2022 revealed that there were vulnerabilities in the information system of the Banyumas Regency JDIH website. The impact of this vulnerability has the potential for Distributed Denial Of Service (DDOS) attacks that can threaten system availability. Effective steps that can be taken are to identify and analyze vulnerabilities by simulating attacks on the system to understand and overcome potential attacks. This study aims to evaluate the security of the Banyumas Regency JDIH website information system with penetration testing techniques using the OWASP framework. The results showed that the Banyumas Regency JDIH website information system has seven vulnerabilities including Private IP Disclosure, SQL Injection, Cross-Site Scripting (XSS), Clickjacking, Hidden file found, Server leak information, and DDoS with severity levels from low to critical. These vulnerabilities are caused by a lack of input validation, insecure server configuration, and the use of less up-to-date software that affects the confidentiality, integrity, and availability of the system. Based on the results of measuring vulnerabilities using the Common Vulnerability Scoring System (CVSS), an average score of 5.7 was obtained, indicating a medium severity level. Future research is recommended to integrate additional scanning tools such as Nuclei, Nessus, and Dalfox to get comprehensive results because each tool has specific advantages in detecting vulnerabilities. These findings are expected to be a reference in improving the information system security of the Banyumas Regency JDIH website to minimize the risk of cyber attacks in the future.

Keywords: Analysis, Security, OWASP, CVSS, Vulnerabilities.