INTISARI

ANALISIS KERENTANAN DAN PENILAIAN RISIKO *SECURITY MISCONFIGURATION* PADA *WEBSITE* INDIBIZ MENGGUNAKAN *OWASP RISK RATING*

Faiza Septiya Ningrum

21/480602/SV/19661

Perkembangan teknologi digital yang pesat menuntut organisasi untuk memperkuat keamanan informasi, termasuk dalam pengelolaan *website*. Salah satu ancaman umum yang sering terjadi adalah *security misconfiguration*, yaitu kesalahan dalam konfigurasi sistem yang dapat membuka celah bagi serangan siber. *Website* IndiBiz milik PT Telkom Indonesia memiliki peran penting sebagai media promosi dan interaksi dengan pengguna, sehingga berpotensi menjadi target serangan jika tidak dikelola dengan aman. Penelitian ini bertujuan untuk mengidentifikasi dan menilai risiko *security misconfiguration* pada *website* IndiBiz menggunakan metode *OWASP Risk* Rating. Proses identifikasi dilakukan melalui pemindaian otomatis menggunakan alat OWASP ZAP. Hasil pemindaian menemukan sembilan kerentanan, enam di antaranya merupakan security misconfiguration yang menjadi fokus analisis. Penilaian risiko dilakukan dengan menentukan nilai *likelihood* dan *impact* untuk masing-masing temuan, disertai pengujian *proof of concept* untuk membuktikan potensi eksploitasi. Hasil analisis menunjukkan tiga risiko tinggi, satu sedang, dan dua rendah, dengan aset publik sebagai area paling terdampak. Berdasarkan temuan tersebut, disusun rekomendasi mitigasi teknis untuk mengurangi potensi eksploitasi. Evaluasi ini diharapkan dapat membantu PT Telkom Indonesia dalam memperkuat keamanan website IndiBiz dan meningkatkan kepercayaan pengguna terhadap platform digital tersebut.

Kata Kunci: *Security Misconfiguration*, *OWASP Risk Rating, Proof of concept*

ABSTRACT

VULNERABILITY ANALYSIS AND RISK ASSESSMENT OF SECURITY MISCONFIGURATION ON THE INDIBIZ WEBSITE USING OWASP RISK RATING

Faiza Septiya Ningrum

21/480602/SV/19661

The rapid development of digital technology demands that organizations strengthen information security, including in website management. One common threat is security misconfiguration, which refers to system configuration errors that can create vulnerabilities for cyberattacks. The IndiBiz website, owned by PT Telkom Indonesia, plays a vital role as a promotional platform and a medium for user interaction, making it a potential target if not securely managed. This study aims to identify and assess the risk of security misconfiguration on the IndiBiz website using the OWASP Risk Rating Methodology. Vulnerability identification was carried out through automated scanning using the OWASP ZAP tool. The scan detected nine vulnerabilities, six of which were classified as security misconfigurations and became the focus of this analysis. Risk assessment was conducted by determining the likelihood and impact scores for each finding, supported by proof of concept testing to demonstrate exploitability. The analysis revealed three high-risk, one medium-risk, and two low-risk issues, with public-facing assets being the most affected area. Based on these findings, technical mitigation recommendations were formulated to reduce exploitation potential. This evaluation is expected to assist PT Telkom Indonesia in strengthening the security of the IndiBiz website and enhancing user trust in the digital platform.

Keywords: Security Misconfiguration, OWASP Risk Rating, OWASP ZAP