ANALISIS KERENTANAN PADA *DOMAIN REPOSITORY.UNJAYA.AC.ID* MENGGUNAKAN METODE *OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL* (OSSTMM)

Nofa Shintia[1], Chanief Budi Setiawan[2], Arief Ikhwan Wicaksono[3]

INTISARI

Latar Belakang: Kerugian dalam ruang lingkup perguruan tinggi akibat *cybercrime* meliputi penurunan kredibilitas akademik, pelanggaran kebijakan institusi, pembatasan karier akademik, kerusakan hubungan interpersonal, dan biaya hukum dan finansial. *Website Repository* Unjaya menunjukkan masalah keamanan dengan notifikasi *"Not Secure"* yang menunjukkan koneksi tidak dienkripsi, sehingga rentan terhadap peretasan dan penyadapan.

Tujuan: Penelitian ini dilakukan untuk menganalisis tingkat keamanan *website repository.unjaya.ac.id* untuk menemukan kerentanan dan mengkategorikan keamanan sistem berdasarkan RAV *Score* yang diperoleh menggunakan metode *Open Source Security Testing Methodology Manual* (OSSTMM) versi 3.0.

Metode Penelitian: Metode *Open Source Security Testing Methodology Manual (*OSSTMM) digunakan karena memiliki kerangka kerja komprehensif yang dirancang untuk pengujian dan analisis keamanan dan berfokus pada pemahaman dan verifikasi keamanan operasional sistem, jaringan, dan proses. Metode Ini melibatkan empat langkah penting dalam OSSTMM *reconnaissance/information gathering* menggunakan *tools* Netcraft, *scanning network* menggunakan *tools* Nmap, *scanning vulnerability* menggunakan Nikto *Scanner*, dan *penetration testing* menggunakan OWASP ZAP.

Hasil: Penelitian ini menemukan bahwa *website Repository* Unjaya memiliki berbagai kerentanan, khususnya pada aspek *Operational Security*, *Loss Control*, dan *Limitation*. *RAV Score* yang diperoleh sebesar 82,8676 dan masuk kedalam kategori *website* dengan keamanan kurang.

Kesimpulan: Analisis kerentanan menggunakan metode *Open Source Security Testhing Methodology Manual* (OSSTMM) berhasil menemukan kerentanan pada *Oprational Security*, *Loss Control* dan *Limitation.*

Kata-kunci: *Cybercrime*, *Website*, *Repository* Unjaya, OSSTMM, *RAV Score*

VULNERABILITY ANALYSIS ON REPOSITORY.UNJAYA.AC.ID DOMAINS USING THE OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) METHOD

Nofa Shintia[1], Chanief Budi Setiawan[2], Arief Ikhwan Wicaksono[3]

ABSTRACT

***Background**: Losses in the scope of universities due to cybercrime include decreased academic credibility, violation of institutional policies, restrictions on academic careers, damage to interpersonal relationships, and legal and financial costs. The Unjaya Repository website shows security issues with a "Not Secure" notification indicating the connection is not encrypted, making it vulnerable to hacking and eavesdropping.*

***Objective**: This study was conducted to analyze the security level of repository.unjaya.ac.id websites to find vulnerabilities and categorize system security based on RAV Score obtained using the Open Source Security Testing Methodology Manual (OSSTMM) version 3.0 method.*

***Method**: The Open Source Security Testing Methodology Manual (OSSTMM) method is used because it has a comprehensive framework designed for security testing and analysis and focuses on understanding and verifying the operational security of systems, networks, and processes. This method involves four important steps in OSSTMM reconnaissance/information gathering using Netcraft tools, scanning network using Nmap tools, scanning vulnerabilities using Nikto Scanner, and penetration testing using OWASP ZAP.*

***Results**: This study found that the Unjaya Repository website has various vulnerabilities, especially in the aspects of Operational Security, Loss Control, and Limitation. The RAV Score obtained was 82.8676 and was included in the category of websites with less security.*

***Conclusion**: Vulnerability analysis using the Open Source Security Thing Methodology Manual (OSSTMM) method successfully found vulnerabilities in Oprational Security, Loss Control and Limitation.*

***Keywords**: Cybercrime, Website, Repository Unjaya, OSSTMM, RAV Score*