ABSTRAK

Integrasi sistem digital pada ekosistem akademis perguruan tinggi mempermudah manajemen data, namun sekaligus memperluas permukaan serangan siber yang mengancam integrasi informasi. Penelitian ini mengevaluasi kekuatan proteksi pada aplikasi SINTESYS Universitas Siliwangi dari potensi eksploitasi pihak ketiga. Pengujian dilakukan melalui pendekatan *Web Application Penetration Testing* (WAPT) berbasis kerangka kerja OWASP Top 10 dan OWASP WSTG. Pemindaian awal menggunakan OWAS ZAP menghasilkan 13 *alerts* (2 *medium,* 7 *low,* dan 4 *informational).* Berdasarkan analisis metrik CVSS dan validasi eksploitasi manual terkendali, ditemukan 2 celah *True Positive* berisiko sedang *(Medium Risk),* yaitu *Clickjacking* (CVSS: 6.8) akibat ketiadaan *header* X-Frame-Options, serta risiko *Session Hijacking* (CVSS:6.8) akibat ketiadaan atribut HttpOnly paa cookie sesi siliwangi_integrated_system_session. Sebalikya, pengujian injeksi menghasilkan 3 *Negative Finding/True Negative* pada *Reflected Cross-Site Scripting* (XSS), SQL Injection, dan *Insecure Direct Object Reference* (IDOR). Hal ini membuktikan bahwa mekanisme filtrasi input dan otorisasi backend SINTESYS telah berjalan tangguh. Berdasarkan matriks manajemen risiko, diusulkan 9 poin rekomendasi remidiasi teknis dengan prioritas utama penguatan atribut cookie dan penerapan kebijakan *framing* guna menjamin kerahasiaan dan integritas data.

Kata Kunci: *Penetration Testing,* Aplikasi *Web*, OWASP Top 10, SYNTESIS, CVSS

ABSTRACT

The integration of digital platforms into higher education frameworks optimizes data management but concurrently expands cyber attack vectors that threaten information integrity. This study evaluates the defensive capabilities of the SINTESYS application at Siliwangi University against unauthorized third-party exploitation. The assessment was executed through Web Application Penetration Testing (WAPT) aligned with the OWASP Top 10 and OWASP WSTG v4.2 frameworks. Automated scanning via OWASP ZAP revealed 13 alerts (2 Medium, 7 Low, and 4 Informational). Based on CVSS v3.1 quantitative scoring and controlled manual exploit validation, 2 True Positive vulnerabilities of Medium Risk were identified: Clickjacking (CVSS: 5.4) due to missing X-Frame-Options headers, and Session Hijacking susceptibility (CVSS: 6.8) caused by the absence of the HttpOnly flag on the siliwangi_integrated_system_session cookie. Conversely, injection tests yielded 3 Negative Findings/True Negatives across Reflected Cross-Site Scripting (XSS), SQL Injection, and Insecure Direct Object Reference (IDOR) scenarios, proving the resilience of SINTESYS's backend input filtering and authorization controls. Based on the risk management matrix, 9 technical remediation measures are prioritized to ensure data confidentiality and integrity.

Keywords: *Penetration Testing, Web Appliaction, OWASP Top 10, SINTESYS, CVSS*