

## INTISARI

Berdasarkan hasil wawancara dengan tim IT Universitas Amikom Purwokerto, telah diperoleh hasil bahwa website student service center Universitas Amikom Purwokerto pernah terjadi penyerangan sebelumnya, namun tim IT masih belum dapat memastikan dari mana asal penyerangan tersebut dan berdasarkan hasil observasi secara langsung pada website student service center Universitas Amikom Purwokerto, pada bagian form input tidak menggunakan filter karakter seperti titik koma (;), petik dua (“) dan sebagainya, hal ini menyebabkan berpotensi terjadi serangan SQL injection. Tujuan penelitian ini adalah melakukan vulnerability assessment untuk menganalisis tingkat keamanan website menggunakan tools Nmap, Nikto, Nslookup, OWASP ZAP dan Acunetix. Hasil dari penelitian ini, tools OWASP ZAP dan Acunetix telah berhasil menemukan kerentanan terhadap serangan Cross-Site Scripting (XSS), clickjacking, data injection, dan malware pada website student service center Universitas Amikom Purwokerto. Namun tidak ditemukan kerentanan terhadap serangan SQL injection. Jika menentukan tingkat keamanan website dari level 1 sampai 3, maka website student service center Universitas Amikom Purwokerto memiliki tingkat keamanan level 2 (medium). Hal ini menunjukkan bahwa sistem keamanan yang dibangun telah dirancang dengan baik untuk melindungi database dari serangan SQL injection. Namun, tidak menutup kemungkinan bahwa potensi serangan SQL injection tetap ada.

Kata kunci: Kerentanan, Vulnerability Assessment, SQL Injection, OWASP ZAP

## **ABSTRACT**

*Based on the results of interviews with the IT team of Amikom Purwokerto University, it has been obtained that the Amikom Purwokerto University student service center website has been attacked before, but the IT team still cannot confirm where the attack came from and based on direct observation on the Amikom Purwokerto University student service center website, in the input form section does not use character filters such as semicolons (;), double quotes (") and so on, this causes the potential for SQL injection attacks. The purpose of this research is to conduct a vulnerability assessment to analyze the level of website security using Nmap, Nikto, Nslookup, OWASP ZAP and Acunetix tools. The results of this study, OWASP ZAP and Acunetix tools have successfully found vulnerabilities to Cross-Site Scripting (XSS), clickjacking, data injection, and malware attacks on the Amikom Purwokerto University student service center website. However, no vulnerability to SQL injection attacks was found. If determining the level of website security from level 1 to 3, then the Amikom Purwokerto University student service center website has a level 2 (medium) security level. This shows that the security system built has been well designed to protect the database from SQL injection attacks. However, it does not rule out the possibility that the potential for SQL injection attacks remains.*

*Keywords: Vulnerability, Vulnerability Assessment, SQL Injection, OWASP ZAP*