INTISARI

Website UIN Saizu Purwokerto sebagai pusat informasi digital kampus memiliki peran penting dalam mendukung aktivitas akademik dan administrasi. Namun, pada Mei 2025 terjadi insiden peretasan yang mengindikasikan adanya celah keamanan pada sistem informasi tersebut. Penelitian ini bertujuan untuk menganalisis keamanan sistem website Universitas Islam Negeri Profesor Kiai Haji Saifuddin Zuhri Purwokerto menggunakan metode penetration testing berbasis ISSAF (Information System Security Assessment Framework. Tahap penelitian terdiri dari Planning & Preparation, Assessment, dan Reporting, Clean Up & Destroy Artifacts. Hasil pengujian menunjukkan adanya beberapa kerentanan keamanan pada subdomain sipinter.uinsaizu.ac.id, seperti tidak adanya header keamanan CSP (Content Security Policy), HSTS (HTTP Strict Transport Security), dan konfigurasi cookie yang belum aman. Peneliti juga melakukan eksploitasi menggunakan teknik SQL Injection dan XSS (Cross Site Scripting), serta simulasi brute-force login. Berdasarkan temuan yang ditemukan, maka dibuat rekomendasi perbaikan sistem guna untuk meningkatkan keamanan informasi dan mencegah potensi peretasan di masa depan.

Kata kunci: ISSAF, penetration testing, keamanan informasi, UIN Saizu, kerentanan website.

ABSTRACK

The website of UIN Saizu Purwokerto, as the campus's digital information center, plays an important role in supporting academic and administrative activities. However, in May 2025, a hacking incident occurred, indicating a security vulnerability in the information system. This study aims to analyze the security of the website system of the State Islamic University of Professor Kiai Haji Saifuddin Zuhri Purwokerto using the ISSAF-based (Information System Security Assessment Framework) penetration testing method. The research stages consist of Planning & Preparation, Assessment, Reporting, and Clean Up & Destroy Artifacts. The testing results revealed several security vulnerabilities in the subdomain sipinter.uinsaizu.ac.id, such as the absence of security headers like CSP (Content Security Policy), HSTS (HTTP Strict Transport Security), and unsecured cookie configuration. The researcher also performed exploitations using SQL (Structured Query Language) Injection and XSS (Cross Site Scripting) techniques, as well as a brute-force login simulation. Based on these findings, system improvement recommendations were formulated to enhance information security and prevent potential hacking incidents in the futureKeywords: ISSAF, penetration testing, information security, UIN Saizu Purowkerto, website vulnerabilities.

Keywords: ISSAF, penetration testing, information security, UIN Saizu, website vulnerabilities.