INTISARI

Perkembangan sistem informasi di perguruan tinggi mendukung layanan akademik dan administratif, namun turut meningkatkan risiko ancaman keamanan siber, seperti Insecure Direct Object Reference (IDOR), yaitu kerentanan yang memungkinkan akses tidak sah terhadap data atau sumber daya milik pengguna lain. Tujuan dari penelitian ini adalah untuk mengetahui dan mengevaluasi potensi kerentanan IDOR pada sistem Portal Mahasiswa Universitas Amikom Purwokerto yang memuat informasi akademik dan administratif mahasiswa. Metode yang digunakan adalah pengujian keamanan (penetration testing) dengan pendekatan grey-box yang mengacu pada standar Web Security Testing Guide (WSTG) bagian WSTG-ATHZ-04. Pengumpulan data dilakukan melalui studi literatur, wawancara, observasi, dan eksperimen langsung dengan bantuan alat seperti Burp Suite dan FoxyProxy. Hasil pengujian menunjukkan bahwa sebagian besar fitur telah memiliki kontrol akses berbasis sesi yang cukup baik, namun terdapat beberapa titik kelemahan pada parameter tertentu yang memungkinkan akses data oleh pengguna yang tidak berhak. Berdasarkan hasil tersebut, disarankan agar pihak pengelola sistem menerapkan validasi otorisasi berbasis objek, memperkuat kontrol akses pada sisi server, dan melaksanakan audit keamanan secara berkala untuk mencegah penyalahgunaan akses oleh pihak yang tidak berwenang.

Kata kunci: IDOR, Penetration Testing, Website, Portal Mahasiswa Amikom, Keamanan Website.

ABSTRACT

The advancement of information systems in higher education has significantly enhanced academic and administrative services; however, it has also introduced increased risks of cybersecurity threats, one of which is Insecure Direct Object Reference (IDOR). IDOR is a vulnerability that allows unauthorized users to access data or resources belonging to other users by manipulating direct object references. This study aims to identify and evaluate potential IDOR vulnerabilities within the Student Portal system of Universitas Amikom Purwokerto, which manages sensitive academic and administrative information. The research employs a security testing approach, specifically penetration testing using a gray-box method, in accordance with the Web Security Testing Guide (WSTG), particularly section WSTG-ATHZ-04. Data collection methods include literature review, interviews, observation, and hands-on experimentation utilizing tools such as Burp Suite and FoxyProxy. The results of the testing indicate that while most features are equipped with adequate session-based access controls, several parameters remain vulnerable, potentially enabling unauthorized data access. In light of these findings, it is recommended that the system administrators implement object-level authorization checks, enhance server-side access controls, and conduct regular security audits to mitigate the risk of unauthorized access and ensure the protection of student data.

Keywords: IDOR, Penetration Testing, Website, Student Portal Amikom, Website Security.