ABSTRAK

Di era digital, Sistem Informasi Akademik (SIA) menjadi elemen dari operasional lembaga pendidikan seperti pondok pesantren (ponpes) dengan membantu pengelolaan data akademik dan administrasi dengan lebih efisien. Ponpes Ihsanul Fikri telah mengimplementasikan SIA melalui Sistem Informasi Pondok (SIPOND), yang mendukung kegiatan akademik dan administrasi dengan pengelolaan informasi yang lebih efektif. Tetapi, tantangan keamanan tetap menjadi masalah penting yang harus diperhatikan, terutama terkait potensi ancaman keamanan yang dapat memengaruhi integritas data siswa dan informasi akademik. Penelitian ini bertujuan untuk menganalisis keamanan SIPOND dan mengidentifikasi risiko keamanan yang dapat mengancam integritas data. Selain itu, penelitian ini juga berupaya mengidentifikasi kelemahan keamanan yang mungkin terdapat dalam SIPOND dan dapat dieksploitasi oleh pihak tidak sah. Metode yang digunakan adalah *Penetration Testing Execution Standard* (PTES) dengan acuan dokumen standar *OWASP Top 10*, yang berfokus pada identifikasi kerentanan keamanan aplikasi web. Hasil penelitian menunjukkan beberapa kerentanan dengan tingkat keparahan yang berbeda. Kerentanan *critical* yang ditemukan adalah *Privilege Escalation via API Endpoint* dan *User and Password Data Leakage via API Endpoint*, sementara kerentanan dengan tingkat *high* adalah *Unauthorized Account Creation via API Endpoint*. Beberapa kerentanan lainnya termasuk *Cross-Domain JavaScript Source File Inclusion* (*Low*), *Dangerous JS Functions* (*Medium*), serta sejumlah kerentanan lainnya yang berkaitan dengan pengaturan header keamanan, kebocoran informasi server, dan pengelolaan *cookie*. Rekomendasi perbaikan diberikan pada tahap *reporting* untuk meningkatkan keamanan SIPOND dan memastikan perlindungan data sensitif, sehingga mendukung operasional pendidikan yang lebih aman.

Kata Kunci : Pengujian Keamanan, Keamanan Aplikasi Web, *Penetration Testing Execution Standard*, *OWASP TOP 10 2021*, Kerentanan Keamanan.

ABSTRACT

.

In the digital era, Academic Information Systems (AIS) have become an element of the operations of educational institutions such as Islamic boarding schools by helping manage academic and administrative data more efficiently. Ihsanul Fikri Islamic Boarding School has implemented SIA through the Pondok Information System (SIPOND), which supports academic and administrative activities with more effective information management. However, security challenges remain an important issue that must be considered, especially regarding potential security threats that could affect the integrity of student data and academic information. This research aims to analyze SIPOND security and identify security risks that could threaten data integrity. Apart from that, this research also seeks to identify security weaknesses that may exist in SIPOND and can be exploited by unauthorized parties. The method used is the Penetration Testing Execution Standard (PTES) with reference to the OWASP Top 10 standard document, which focuses on identifying web application security vulnerabilities. The research results show several vulnerabilities with different levels of severity. The critical vulnerabilities found were Privilege Escalation via API Endpoint and User and Password Data Leakage via API Endpoint, while the high level vulnerability was Unauthorized Account Creation via API Endpoint. Some other vulnerabilities include Cross-Domain JavaScript Source File Inclusion (Low), Dangerous JS Functions (Medium), as well as a number of other vulnerabilities related to security header settings, server information leaks, and cookie management. Recommendations for improvements are provided at the reporting stage to improve SIPOND security and ensure the protection of sensitive data, thereby supporting safer educational operations.

Keywords: *Security Testing, Web Application Security, Penetration Testing Execution Standard, OWASP TOP 10 2021, Security Vulnerabilities*.