PENETRATION TESTING PADA SISTEM ABC DAN SISTEM XYZ UNIVERSITAS PENDIDIKAN GANESHA

Oleh

Ketut Wawan Arimbawa, NIM 1915101015

Jurusan Teknik Informatika

ABSTRAK

Penelitian ini bertujuan untuk menguji keamanan dua aplikasi web, yaitu sistem ABC dan Sistem XYZ, yang digunakan oleh Universitas Pendidikan Ganesha. Metode yang digunakan adalah uji penetrasi, di mana skenario ancaman umum disimulasikan untuk mengidentifikasi kerentanan dan memberikan rekomendasi keamanan. Pada sistem ABC, beberapa skenario ancaman yang dimodelkan meliputi *sensitive information disclosure*, *cloud meta data potentially exposed*, *hidden file found, dan sql injection*. Sedangkan pada Sistem XYZ, skenario ancaman mencakup *cross site scripting reflected*, *cloud meta data potentially exposed*, *hidden file found*, *sql injection*, dan *arbitrary file upload*. Melalui pengujian ini, alat-alat dan teknik yang relevan digunakan untuk mensimulasikan serangan berdasarkan skenario ancaman yang telah ditentukan. Hasil pengujian tersebut mengidentifikasi beberapa kerentanan dan celah keamanan pada aplikasi web. Rekomendasi keamanan yang disarankan meliputi memperbarui perangkat lunak dengan patch terbaru, mengkonfigurasi firewall dan filter input yang tepat, menerapkan validasi dan sanitasi data yang kuat, menggunakan mekanisme otentikasi yang aman, dan mengaktifkan pemantauan keamanan yang berkelanjutan. Hasil pengujian menunjukkan bahwa pada sistem ABC terdapat 3 kerentanan dengan tingkat kerentanan yang berbeda-beda, yaitu *Sensitive Information Disclosure* (tingkat tinggi), *Hidden file found* (tingkat sedang), dan *Sql Injection* (tingkat sedang). Pada sistem XYZ, kerentanan *Arbitrary File Upload* mendapatkan tingkat kerentanan (tinggi), *Cross Site Scripting Reflected* mendapatkan tingkat kerentanan (sedang), dan *hidden file found* dengan tingkat kerentanan (rendah). Sementara itu, kerentanan lainnya tidak menunjukkan adanya celah atau kerentanan, sehingga dianggap sebagai *true negative*.

Kata kunci: Kerentanan, Penetration testing, Keamanan aplikasi web, Rekomendasi keamanan.

PENETRATION TESTING ON ABC SYSTEM AND XYZ SYSTEM GANESHA UNIVERSITY OF EDUCATION

By

Ketut Wawan Arimbawa, NIM 1915101015
Informatics Engineering

ABSTRACT

This research aims to test the security of two web applications, namely ABC system and XYZ system, used by Ganesha University of Education. The method used is penetration testing, where common threat scenarios are simulated to identify vulnerabilities and provide security recommendations. On ABC system, some modeled threat scenarios include sensitive information disclosure, cloud metadata potentially exposed, hidden file found, and SQL injection. Meanwhile, on XYZ system, the threat scenarios involve cross-site scripting reflected, cloud metadata potentially exposed, hidden file found, SQL injection, and arbitrary file upload. Through this testing, relevant tools and techniques are used to simulate attacks based on the predetermined threat scenarios. The testing results identify several vulnerabilities and security gaps in the web applications. The recommended security measures include updating software with the latest patches, configuring appropriate firewalls and input filters, implementing strong data validation and sanitization, using secure authentication mechanisms, and enabling continuous security monitoring. The testing results indicate that ABC system has 3 vulnerabilities with varying levels of severity, namely Sensitive Information Disclosure (high severity), Hidden file found (medium severity), and SQL Injection (medium severity). On the other hand, XYZ system has Arbitrary File Upload vulnerability (high severity), Cross-Site Scripting Reflected vulnerability (medium severity), and hidden file found vulnerability (low severity). Meanwhile, other vulnerabilities do not show any gaps or vulnerabilities, hence considered as true negatives.

Keywords: *Vulnerabilities, Penetration testing, Web application security, Security recommendations.*