IMPLEMENTASI METODE *PENETRATION TESTING EXECUTION STANDARD (PTES)* DALAM MENEMUKAN KERENTANAN *BROKEN ACCESS CONTROL (BAC)* STUDI KASUS *WEBSITE* UNIVERSITAS PENDIDIKAN GANESHA

Oleh

Mochammad Syahrul Kurniawan, NIM 2115091031

Jurusan Teknik Informatika

Program Studi Sistem Informasi

ABSTRAK

Penelitian ini bertujuan untuk mengimplementasikan metode *Penetration Testing Execution Standard (PTES)* dalam mendeteksi kerentanan *Broken Access Control (BAC)* pada ekosistem website Universitas Pendidikan Ganesha. BAC merupakan kerentanan kritis yang memungkinkan pengguna tidak sah mengakses data atau fungsi di luar wewenangnya, yang sering kali sulit dideteksi oleh alat pemindai otomatis karena sifatnya yang terikat pada logika bisnis sistem. Metodologi penelitian ini mengadopsi tujuh tahapan PTES: *pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation,* dan *reporting*. Pengujian dilakukan pada 15 subdomain target menggunakan alat bantu seperti *ParamSpider*, *Kxss*, dan *DalFox*, serta divalidasi melalui verifikasi manual. Hasil penelitian mengungkap kerentanan signifikan pada subdomain *http://lib.undiksha.ac.id* pada parameter *halaman* dan *module*. Melalui teknik eksploitasi manual, ditemukan bahwa celah *Cross-Site Scripting (XSS)* dapat dimanfaatkan sebagai vektor serangan untuk melakukan *session hijacking* dan *vertical privilege escalation*. Analisis risiko menggunakan metodologi OWASP Risk Rating menempatkan temuan ini pada kategori *MEDIUM* (skor *Likelihood* 4.125 dan *Impact* 4.75). Guna memperkuat objektivitas temuan, dilakukan *cross-validation* menggunakan CVSS v4.0 yang menghasilkan skor 8.3 (*HIGH*), yang mengkonfirmasi bahwa secara intrinsik kerentanan ini memiliki tingkat keparahan teknis yang tinggi pada aspek kerahasiaan data (*confidentiality*). Dampak dari celah ini mencakup potensi kebocoran informasi pribadi mahasiswa serta manipulasi data sistem perpustakaan. Penelitian ini merekomendasikan penguatan pertahanan berlapis melalui penerapan *server-side access control* berbasis *role* dan *input sanitation* yang menyeluruh untuk memitigasi risiko keamanan di masa mendatang.

Kata Kunci: *Penetration Testing Execution Standard, Broken Access Control, OWASP Risk Rating, CSVV v4.0.*

IMPLEMENTATION OF THE *PENETRATION TESTING EXECUTION STANDARD (PTES)* METHOD TO FIND VULNERABILITIES *BROKEN ACCESS CONTROL (BAC)* WEBSITE CASE STUDY UIVERSITAS PENDIDIKAN GANESHA

By

Mochammad Syahrul Kurniawan, NIM 2115091031

Department of Informatics Engineering

Information Systems Study Program

ABSTRACT

This study aims to implement the *Penetration Testing Execution Standard (PTES)* method in detecting *Broken Access Control (BAC)* vulnerabilities in the Universitas Pendidikan Ganesha website ecosystem. BAC is a critical vulnerability that allows unauthorized users to access data or functions beyond their authority, which is often difficult to detect by automated scanning tools because it is tied to the system's business logic. This research methodology adopts seven PTES stages: pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. Testing was conducted on 15 target subdomains using tools such as *ParamSpider*, *Kxss*, and *DalFox*, and validated through manual verification. The results of the study revealed significant vulnerabilities in the *http://lib.undiksha.ac.id* subdomain in page and module parameters. Through manual exploitation techniques, it was found that *Cross-Site Scripting (XSS)* vulnerabilities can be exploited as an attack vector for session hijacking and vertical privilege escalation. Risk analysis using the OWASP Risk Rating methodology places this finding in the MEDIUM category (Likelihood score of 4.125 and Impact score of 4.75). To strengthen the objectivity of the findings, cross-validation was performed using CVSS v4.0, which resulted in a score of 8.3 (HIGH), confirming that this vulnerability intrinsically has a high technical severity level in terms of data confidentiality. The impact of this vulnerability includes the potential for leaking students' personal information and manipulating library system data. This study recommends strengthening layered defenses through the implementation of role-based server-side access control and comprehensive input sanitation to mitigate future security risks.

Keywords: *Penetration Testing Execution Standard, Broken Access Control, OWASP Risk Rating, CSVV v4.0.*