Penetration Testing For Cross-Site Scripting (XSS) Detection Using Penetration Testing Execution Standard (PTES) Methodology: A Case Study Of Information Systems In Universitas Pendidikan Ganesha

By

Nabila Aulia Azizah, Student ID 2215091040

Department of Informatics Engineering

Information System Study Program

ABSTRACT

Web-based information systems in educational institutions store and process sensitive data, turning them into a perfect target for cybercriminals, particularly Cross-Site Scripting (XSS). This research aims to identify and evaluate XSS vulnerabilities across twelve web-based information at Institution X using Penetration Testing Execution Standard (PTES) methodology, combined with grey-box technique and black-box technique, and OWASP Risk Rating Methodology to assess the risk of the vulnerabilities. The testing was conducted by the researcher as an insider tester with student-level access, applying black-box testing for systems inaccessible to student and grey-box testing for systems accessible to student. The combination of automated tools including passive reconnaissance, active reconnaissance and manual testing was employed to minimize false positive and validated the vulnerabilities. The total of eleven XSS vulnerabilities across the twelve tested systems, consist of five Reflected XSS was discovered in System C, D, and J, and six Stored XSS was discovered in System I, J, and K. No DOM-Based XSS vulnerabilities were confirmed across all the tested systems. All of identified vulnerabilities were assessed as medium risk based on the OWASP Risk Rating Methodology. These findings demonstrate that XSS vulnerabilities are still present within the educational institution environment indicates that secure input handling was inconsistently implemented across systems. The result highlights the importance of adopting remediation to secure coding practices, implementing proper input sanitization, output encoding, and Content Security Policy (CSP), as well as conducting regular security assessment to strengthen the overall security posture in an information system within educational institution.

Keywords: Cross-Site Scripting, Penetration Testing, PTES, OWASP, Risk Rating.

Pengujian Penetrasi untuk Deteksi Cross-Site Scripting (XSS) Menggunakan Metodologi Penetration Testing Execution Standard (PTES): Studi Kasus pada Sistem Informasi di Universitas Pendidikan Ganesha

Oleh

Nabila Aulia Azizah, NIM 2215091040

Jurusan Teknik Informatika

Program Studi Sistem Informasi

ABSTRAK

Sistem Informasi berbasis web di institusi pendidikan menyimpan dan memproses data sensitif, menjadikannya target utama bagi penjahat siber, khususnya melalui serangan Cross-Site Scripting (XSS). Penelitian ini mengidentifikasi dan mengevaluasi kerentanan XSS di dua belas sistem informasi berbasis web di Universitas Pendidikan Ganesha menggunakan metodologi Penetration Testing Execution Standard (PTES), dikombinasikan dengan teknik grey-box untuk sistem yang dapat diakses oleh mahasiswa dan black-box yang tidak dapat diakses oleh mahasiswa, serta metodologi OWASP Risk Rating untuk menilai tingkat risiko dari kerentanan. Pengujian dilakukan oleh peneliti sebagai penguji internal dengan hak akses mahasiswa. Penggunaan alat otomatis mencakup pengintaian pasif, pengintaian aktif, dan pengujian manual untuk meminimalisir false positive dan memvalidasi hasil temuan kerentanan. Sebelas kerentanan XSS ditemukan pada dua belas sistem yang diuji, lima Reflected XSS ditemukan pada Sistem C, D, dan J, dan enam Stored XSS ditemukan di Sistem I, J, dan K. Tidak ada kerentanan DOM-Based XSS terkonfirmasi pada keseluruhan sistem yang diuji. Semua kerentanan yang teridentifikasi memiliki risiko Medium. Temuan ini menunjukkan bahwa kerentanan XSS masih ditemukan dalam institusi pendidikan, mengindikasikan bahwa penaganan input yang belum diterapkan secara konsisten di seluruh sistem. Hasil penelitian ini menegaskan pentingnya menerapkan remediasi menuju praktik pengembangan yang aman, implementasi sanitasi input yang tepat, output encoding, serta menerapkan Content Security Policy (CSP), sekaligus pentingnya pelaksanaan pengujian keamanan secara berkala guna memperkuat keamanan secara menyeluruh pada sistem informasi pada institusi pendidikan.

Kata Kunci: Cross-Site Scripting**,** Penetration Testing**,** PTES**,** OWASP**,** Risk Rating**.**