Analisis Kerentanan Aplikasi Web dengan Pendekatan Uji Penetrasi Menggunakan Kerangka Kerja OWASP WSTG v4.2 = Web Application Vulnerability Analysis with Penetration Testing Approach Using OWASP WSTG v4.2 Framework

Muhammad Rizky Utomo, author

Abstrak

Isu keamanan adalah topik yang sangat penting di dunia komputer dan jaringan internet karena ancaman terhadap sistem keamanan terus-menerus berkembang dan meningkat. Oleh karena itu, sistem keamanan terus diperbarui untuk menghadapi potensi terjadinya peretasan terhadap sistem komputasi, termasuk pada aplikasi web. Dengan diperbaruinya sistem keamanan aplikasi web, pengujian diperlukan untuk memastikan ketahanannya terhadap berbagai ancaman terbaru. Untuk memudahkan rangkaian kegiatan pengujian dengan adanya metode yang dapat direplikasi, penulis merancang Kerangka Uji ID OWASP WSTG Terstruktur, sebuah pendekatan berbasis OWASP Web Security Testing Guide versi v4.2 yang diterapkan pada pengujian aplikasi web. Pengujian yang dilakukan meliputi 21 ID OWASP WSTG berbeda dari segi autentikasi, konfigurasi, ekstraksi informasi, injeksi, hingga manajemen session. Dari ID-ID tersebut, penulis menemukan 6 kerentanan dengan nilai High, 8 kerentanan dengan nilai Medium, 5 kerentanan dengan nilai Low, dan 2 kerentanan dengan nilai Informational. ID OWASP WSTG yang dipilih sebagai poin pengujian juga memiliki kaitan dengan OWASP Top 10 (2021) sebagai referensi kerentanan yang banyak ditemukan dan ISO/IEC 27001:2022 sebagai referensi standar keamanan informasi. Hasil yang didapatkan menunjukkan relevansi dari penggunaan Kerangka Uji ID OWASP WSTG Terstruktur sebagai alur uji penetrasi menggunakan OWASP WSTG.

.....Security issues are a critical concern in the world of computing and the internet, as threats to system security continue to evolve and intensify. Consequently, security systems are constantly updated to defend against potential breaches in computing environments, including web applications. As web application security improves, testing becomes necessary to ensure resilience against emerging threats. To facilitate a replicable testing process, the author designed the Structured OWASP WSTG ID Testing Framework, an approach based on version 4.2 of the OWASP Web Security Testing Guide, applied to web application testing. The assessment covered 21 different OWASP WSTG IDs across authentication, configuration, information extraction, injection, and session management. Among these IDs, the author identified 6 vulnerabilities rated High, 8 rated Medium, 5 rated Low, and 2 rated Informational. The selected WSTG IDs were also mapped to relevant categories in the OWASP Top 10 (2021), a widely used reference for common vulnerabilities, and ISO/IEC 27001:2022, a standard for information security. The results demonstrate the relevance of using the Structured OWASP WSTG ID Testing Framework as a penetration testing workflow aligned with the OWASP WSTG methodology.