INTISARI

PENGEMBANGAN ANTARMUKA WEB UNTUK AUTOMASI UJI PENETRASI KEAMANAN BERBASIS CVE

Sofiyanatul Munawaroh
21/474781/SV/19035

Keamanan siber menjadi aspek krusial di era digital, di mana serangan siber terus meningkat dari tahun ke tahun. Uji penetrasi (*penetration testing*) berperan penting untuk mendeteksi dan mengeksploitasi kerentanan sebelum dimanfaatkan oleh pihak tidak bertanggung jawab. Namun, praktik uji penetrasi umumnya masih dilakukan secara manual atau berbasis *Command Line Interface* (CLI) sehingga kurang efisien, tidak ramah pengguna, dan sulit dalam hal dokumentasi hasil.

Proyek akhir ini bertujuan mengembangkan antarmuka *web* untuk otomatisasi uji penetrasi berbasis *Common Vulnerabilities and Exposures* (CVE) yang terintegrasi dengan basis data. Sistem dirancang agar mampu mencatat hasil setiap tahapan pengujian, mulai dari pemindaian, enumerasi, analisis kerentanan, hingga eksploitasi secara otomatis dan terstruktur. Implementasi dilakukan menggunakan *framework* Flask pada sisi *backend*, ReactJS untuk *frontend* interaktif, serta MySQL sebagai basis data. Terdapat dua kerentanan yang dijadikan studi kasus, yaitu CVE-2012-2122 (MySQL/MariaDB *Authentication Bypass*) dan CVE-2018-10933 (libssh *Authentication Bypass*).

Metode pengembangan meliputi perancangan arsitektur sistem, implementasi modul otomatisasi CVE, serta pengujian fungsional menggunakan pendekatan *black box testing*. Hasil penelitian menunjukkan bahwa sistem mampu menjalankan pengujian multi-CVE secara berurutan, menampilkan progres secara *real-time*, serta menghasilkan laporan individual maupun gabungan dalam format PDF secara otomatis. Dengan demikian, sistem ini meningkatkan efisiensi, akurasi dokumentasi, serta kemudahan pemantauan hasil uji penetrasi.

Kata kunci : uji penetrasi, CVE, Flask, ReactJS, otomatisasi

ABSTRACT

DEVELOPMENT OF A WEB INTERFACE FOR CVE-BASED AUTOMATED PENETRATION TESTING

Sofiyanatul Munawaroh
21/474781/SV/19035

Cybersecurity has become a crucial aspect in the digital era, where cyberattacks continue to increase every year. Penetration testing plays an important role in detecting and exploiting vulnerabilities before they are exploited by irresponsible parties. However, penetration testing practices are generally still carried out manually or through Command Line Interface (CLI), which tends to be inefficient, less user-friendly, and difficult in terms of documenting results.

This final project aims to develop a web-based interface for automated penetration testing based on Common Vulnerabilities and Exposures (CVE), integrated with a database. The system is designed to record the results of each testing stage, from scanning, enumeration, vulnerability analysis, to exploitation automatically and structurally. The implementation uses Flask as the backend framework, ReactJS for an interactive frontend, and MySQL as the database. There are two vulnerabilities used as case studies, namely CVE-2012-2122 (MySQL/MariaDB Authentication Bypass) and CVE-2018-10933 (libssh Authentication Bypass).

The development method involves system architecture design, implementation of automated CVE modules, and functional testing using the black box testing approach. The results of the study show that the system can perform multi-CVE testing sequentially, display real-time progress, and generate both individual and combined reports in PDF format automatically. Therefore, the system improves efficiency, accuracy of documentation, and ease of monitoring penetration testing results.

Keyword: penetration testing, CVE, Flask, ReactJS, automation