INTISARI

Keamanan siber menjadi isu kritis di era digital saat ini, seiring dengan meningkatnya jumlah dan kompleksitas serangan terhadap sistem informasi. Apache HTTP *Server*, sebagai salah satu perangkat lunak *server* yang paling banyak digunakan di dunia, tidak terlepas dari berbagai kerentanan yang dapat dieksploitasi. Salah satu kerentanan kritis yang ditemukan pada tahun 2021 adalah CVE-2021-42013, yang mencakup *Path traversal* dan *Remote code execution*. Kerentanan ini memungkinkan penyerang untuk mengakses *file* sistem yang seharusnya tidak dapat diakses dan mengeksekusi kode arbitrer di *server*, dengan skor CVSS 9.8 yang menunjukkan tingkat ancaman yang sangat tinggi. Penelitian ini bertujuan untuk mengembangkan aplikasi otomatisasi *penetration testing* berbasis *web* untuk mengidentifikasi dan mengeksploitasi kerentanan CVE-2021-42013 pada Apache HTTP *Server*. Aplikasi ini dirancang agar pengguna dapat dengan mudah mengunduh laporan hasil uji penetrasi hanya dengan sekali klik, serta mempercepat proses pembuatan laporan yang selama ini memakan waktu lama jika dilakukan secara manual. Metode otomatisasi ini diharapkan dapat meningkatkan efisiensi dan efektivitas dalam proses pengujian penetrasi. Hasil penelitian menunjukkan bahwa aplikasi yang dikembangkan mampu mengurangi waktu yang dibutuhkan untuk melakukan *penetration testing* secara signifikan dibandingkan dengan metode manual. Proses pemindaian Nmap otomatis menunjukkan pengurangan waktu sebesar 15.08%, eksploitasi kerentanan sebesar 14.11%, dan pembuatan laporan sebesar 99.65%. Aplikasi ini tidak hanya mempermudah akses dan pengunduhan laporan hasil uji penetrasi, tetapi juga meningkatkan efisiensi dan konsistensi proses pengujian. Penggunaan teknologi *web* terbukti efektif dalam menyediakan lingkungan pengembangan yang cepat dan responsif, serta mampu menangani beban kerja yang stabil. Penelitian ini diharapkan dapat berkontribusi dalam pengembangan aplikasi berbasis *web* untuk uji penetrasi, serta meningkatkan pengetahuan dan keterampilan dalam bidang keamanan siber dan pengembangan perangkat lunak.

Kata kunci: *penetration testing*, otomatisasi, Flask, Apache *webserver*, CVE-2021-42013

ABSTRACT

Cybersecurity has become a critical issue in today's digital era, with the increasing number and complexity of attacks on information systems. Apache HTTP Server, as one of the most widely used server software in the world, is not immune to various vulnerabilities that can be exploited. One critical vulnerability discovered in 2021 is CVE-2021-42013, which includes Path traversal and Remote code execution. This vulnerability allows attackers to access system files that should not be accessible and execute arbitrary code on the server, with a CVSS score of 9.8, indicating a very high threat level. This research aims to develop a web-based automated penetration testing application to identify and exploit the CVE-2021-42013 vulnerability in Apache HTTP Server. The application is designed to allow users to easily download penetration test reports with a single click and speed up the report generation process, which has traditionally been time-consuming when done manually. This automation method is expected to enhance the efficiency and effectiveness of the penetration testing process. The research results show that the developed application significantly reduces the time required to conduct penetration testing compared to manual methods. The automatic Nmap scanning process shows a time reduction of 15.08%, vulnerability exploitation by 14.11%, and report generation by 99.65%. This application not only simplifies access and downloading of penetration test reports but also improves the efficiency and consistency of the testing process. The use of web technology has proven effective in providing a fast and responsive development environment, capable of handling stable workloads. This research is expected to contribute to the development of web-based applications for penetration testing and enhance knowledge and skills in the field of cybersecurity and software development.

Keywords: penetration testing, automation, Flask*,* Apache *webserver, CVE-2021-42013*