INTISARI

Bug hunter, pentester, dan praktisi keamanan seringkali mengandalkan alat-alat seperti nuclei, httpx, dnsx, naabu, dan subfinder. Namun, bagi pengguna hasil pemindaian kerentanan dari nuclei secara default kurang informatif, dengan keterbatasan dalam manajemen dan ketergantungan pada pencarian internet untuk mendapatkan informasi lebih rinci. Dalam survei terhadap 37 responden (48.6% bug hunter, 29.7% pentester), ditemukan bahwa mereka menyatakan kurang efisien dalam memeriksa URL terdampak (73%), mengelola hasil nuclei di platform seperti Telegram dan Discord (67.6%), dan membuat laporan kerentanan secara manual (75.7%) karena melibatkan beberapa alat eksternal. Dari permasalahan tersebut penelitian ini merancang sebuah aplikasi web manajemen kerentanan output nuclei dengan kemampuan mengubah output nuclei menjadi lebih rinci. Aplikasi tersebut menerapkan metode webhook untuk memproses dan sebagai aliran data kerentanan output nuclei ke sistem. Dalam proses pengembangannya, menggunakan metode waterfall, dengan pengujian menggunakan metode Blackbox dan User Acceptance Testing (UAT). Hasil pengujian Blackbox menunjukkan ketidaktemuan masalah pada fungsi yang dapat diakses melalui antarmuka maupun API sebagai webhook, dan hasil uji User Acceptance Testing (UAT) bahwa aplikasi layak digunakan yang didasarkan pada kesesuaian sistem terhadap kebutuhan pengguna, kelancaran fungsi, dan mudah digunakan. Sehingga dapat disimpulkan bahwa sistem dapat efektif digunakan dalam tahapan analisis informasi, perencanaan, analisis hasil, dan pelaporan setelah melakukan deteksi kerentanan menggunakan nuclei.

Kata kunci: Nuclei, Manajemen kerentanan, Webhook, Waterfall, Website

ABSTRACT

Bug hunters, pentesters, and security practitioners often rely on tools such as nuclei, httpx, dnsx, naabu, and subfinder. However, for users the vulnerability scan results from nuclei are by default less informative, with limitations in management and reliance on internet searches for more detailed information. In a survey of 37 respondents (48.6% bug hunters, 29.7% pentesters), it was found that they were less efficient in checking affected URLs (73%), managing nuclei results on platforms such as Telegram and Discord (67.6%), and manually creating vulnerability reports (75.7%) due to the involvement of several external tools. From these problems, this research designed a nuclei output vulnerability management web application with the ability to change the nuclei output into more detail. The application applies the webhook method to process and flow nuclei output vulnerability data to the system. In the development process, it uses the waterfall method, with testing using the Blackbox method and User Acceptance Testing (UAT). The results of Blackbox testing show no problems with functions that can be accessed through the interface or API as a webhook, and the results of User Acceptance Testing (UAT) test that the application is feasible to use based on the suitability of the system to user needs, smooth functioning, and easy to use. So it can be concluded that the system can be effectively used in the stages of information analysis, planning, results analysis, and reporting after conducting vulnerability detection using nuclei.

Keywords: Nuclei, Vulnerability management, Webhook, Waterfall, Website