1. Pendahuluan

Latar Belakang

Berikut versi paragrafnya setelah digabung:

Meningkatnya prevalensi dan kecanggihan ancaman dunia maya menimbulkan tantangan yang signifikan terhadap keamanan aplikasi web. Kerentanan pada aplikasi web sering kali berasal dari kelemahan yang melekat pada kode, konfigurasi, atau desain, membuat sistem ini rentan terhadap eksploitasi. Pengujian penetrasi, metode simulasi serangan dunia nyata, sangat penting untuk mengidentifikasi dan mengatasi kerentanan ini. Namun, pendekatan tradisional sering kali mengandalkan alat tunggal dengan cakupan terbatas, gagal mengatasi sifat multifaset dari ancaman siber modern. [1] [2]

Untuk mengatasi keterbatasan tersebut, penelitian ini memperkenalkan kerangka kerja pengujian penetrasi multi-agen kolaboratif yang mengintegrasikan beberapa alat untuk mengevaluasi kerentanan aplikasi web secara komprehensif. Kerangka kerja tersebut menggunakan alat seperti OWASP ZAP, Nikto, dan Wapiti untuk mensimulasikan skenario serangan canggih yang mencakup berbagai teknik, mulai dari analisis statis hingga pengujian aplikasi dinamis. Dengan memanfaatkan kekuatan unik dari alat-alat ini, kerangka kerja ini menawarkan pendekatan yang lebih kuat dan holistik untuk pengujian penetrasi. [3]

Studi ini dibangun berdasarkan literatur yang ada, menunjukkan efektivitas sistem multi-agen dalam mengatasi tantangan keamanan siber yang kompleks. Penelitian sebelumnya telah menunjukkan potensi alat kolaboratif untuk meningkatkan deteksi dan pelaporan kerentanan. Namun, masih ada kesenjangan dalam mengintegrasikan teknik canggih seperti pembelajaran penguatan mendalam untuk pengujian adaptif. Penelitian ini membahas kesenjangan tersebut dengan menerapkan kerangka kerja yang dinamis dan berorientasi pada tujuan yang menggabungkan kekuatan alat individu dengan pembelajaran mesin tingkat lanjut. [5] [6]

Selain itu, kerangka kerja yang diusulkan menyoroti pentingnya pelaporan yang efektif, yang sering diabaikan dalam pengujian penetrasi. Pelaporan yang transparan dan terstruktur memungkinkan pemangku kepentingan untuk memahami temuan, memprioritaskan upaya remediasi, dan membuat keputusan yang tepat. Untuk itu, penelitian ini mengintegrasikan pemrosesan data menggunakan ELK Stack dan visualisasi. Filebeat mengirimkan temuan ke Elasticsearch, sementara Kibana menyediakan dasbor intuitif yang menjembatani kesenjangan antara audiens teknis dan non-teknis. [7]

Penelitian ini menawarkan beberapa keunggulan dibandingkan pendekatan tradisional. Sistem multi-agen meningkatkan akurasi dan cakupan dengan mengoordinasikan beragam alat, sementara pembelajaran penguatan mendalam memungkinkan adaptasi terhadap ancaman yang terus berkembang. Integrasi ELK Stack memastikan pelaporan yang dapat ditindaklanjuti, memfasilitasi respons yang tepat waktu dan efektif. Dengan mengatasi keterbatasan pendekatan sebelumnya, penelitian ini bertujuan untuk memperkuat keamanan aplikasi web dan memberikan kontribusi pada perkembangan bidang keamanan siber secara lebih luas.