JUSTER*: Jurnal Sains dan Terapan*
Vol. 4, No. 1, Januari 2025
p-ISSN: 2809-7661, e-ISSN: 2809-7750

Analisis Celah Keamanan Website Menggunakan Tools OWASP ZAP Di Kali Linux

Calvin Bernandra Putra Pura[1*], Try Yudha Maulana[2], Aldi Februri[3], Tamsir Ariyadi[4]
[1,2,3,4]Universitas Bina Darma, Jln.Jendral Ahmadyani No.3,9/10 Ulu, Kecamatan Seberang Ulu 1, Kota Palembang Sumatra Selatan 30111
Email Corespondent[*]: calvinbernandraputrapura@gmail.com

Abstract

As the use of the internet for various activities increases, website security becomes a very important issue. Conducting audits and testing for security holes is one way to ensure that a website is secure. The OWASP Zed Attack Proxy (ZAP) tool, an open-source tool used to identify attacks, is used in this study. OWASP ZAP is enabled on Kali Linux to identify potential web security issues. This study aims to analyze security vulnerabilities on websites using the OWASP Zed Attack Proxy (ZAP) tool in the Kali Linux environment. OWASP ZAP is one of the open-source tools that is widely used to identify vulnerabilities in web applications. This study uses an experimental approach by utilizing OWASP ZAP to scan the target website. This process includes identifying security vulnerabilities, analyzing risks, and providing recommendations for mitigation of the vulnerabilities found. The results of the study show some of its vulnerabilities, such as Cross-Site Scripting (XSS) attacks, SQL Injection, and security misconfigurations that can be fixed to improve website security.
***Keywords**: Kali linux, OWASP ZAP, Website security, Security holes, Security audite*

Abstrak

Seiring dengan meningkatnya penggunaan internet untuk berbagai macam aktivitas, keamanan website menjadi salah satu masalah yang sangat penting. Melakukan audit dan pengujian celah keamanan adalah salah satu cara untuk memastikan situs web aman. Alat OWASP Zed Attack Proxy (ZAP), sebuah alat sumber terbuka yang digunakan untuk mengidentifikasi serangan, digunakan dalam penelitian ini. OWASP ZAP diaktifkan di Kali Linux untuk mengidentifikasi potensi masalah keamanan web. Penelitian ini bertujuan untuk menganalisis celah keamanan pada website dengan menggunakan tools OWASP Zed Attack Proxy (ZAP) di lingkungan Kali Linux. OWASP ZAP merupakan salah satu tools open-source yang banyak digunakan untuk mengidentifikasi kerentanan pada aplikasi web. Penelitian ini menggunakan pendekatan eksperimen dengan memanfaatkan OWASP ZAP untuk melakukan scanning terhadap website target. Proses ini mencakup identifikasi celah keamanan, analisis risiko, dan pemberian rekomendasi mitigasi terhadap kerentanan yang ditemukan. Hasil penelitian menunjukkan beberapa kerentanannya, seperti serangan Cross-Site Scripting (XSS), SQL Injection, dan kesalahan konfigurasi keamanan yang dapat diperbaiki untuk meningkatkan keamanan website.
***Kata Kunci:** Audit keamanan, Celah keamanan, Kali linux, Keamanan website, OWASP ZAP*

PENDAHULUAN

Di era digital saat ini, keamanan website menjadi sangat penting. Ada sejumlah besar serangan siber yang dapat mengancam integritas, kerahasiaan, dan ketersediaan data yang ada di sebuah website. Oleh karena itu, pengujian keamanan secara berkala diperlukan untuk mengidentifikasi kemungkinan kerusakan. OWASP ZAP (*Zed Attack Proxy*) adalah salah satu alat yang banyak digunakan oleh profesional keamanan untuk menemukan celah keamanan di aplikasi web. Berbagai pengujian keamanan terhadap aplikasi web dan pemindaian otomatis dan manual adalah beberapa fitur yang ditawarkan oleh alat ini untuk melakukan analisis.

Tujuan penelitian ini adalah untuk mengevaluasi masalah keamanan pada sebuah website yang menggunakan OWASP ZAP yang dioperasikan di Kali Linux. Kali Linux dipilih karena merupakan distribusi

Linux yang sangat populer di dunia keamanan siber.

Salah satu alat open-source adalah OWASP Zed Attack Proxy (ZAP), yang digunakan untuk melakukan pengujian keamanan pada aplikasi web. Dengan bantuan program ini, penguji dapat mendeteksi berbagai jenis serangan, termasuk Cross-Site Scripting (XSS), SQL Injection, dan misconfigurations. Karena Kali Linux adalah sistem operasi yang dirancang khusus untuk pengujian penetrasi dan forensik, penggunaan OWASP ZAP di dalamnya memberikan keunggulan khusus.

Tujuan dari penelitian ini adalah untuk mengevaluasi masalah keamanan yang terjadi pada situs web yang menggunakan OWASP ZAP. Dengan menggunakan fitur-fitur yang tersedia di OWASP ZAP, penelitian ini diharapkan dapat memberikan gambaran yang jelas tentang celah keamanan yang mungkin dieksploitasi oleh penyerang. Hasil penelitian ini juga diharapkan dapat memberikan saran untuk meningkatkan keamanan situs web.

OWASP ZAP diaktifkan di Kali Linux dalam penelitian ini untuk mengidentifikasi dan menganalisis berbagai potensi masalah keamanan web. Pemindaian aktif mencari kerentanan dengan mengirimkan permintaan yang meniru perilaku penyerang, dan pemindaian pasif mengumpulkan informasi tentang target tanpa mengirimkan permintaan yang dapat mengubah status server. Serangan Cross-Site Scripting (XSS), SQL Injection, dan banyak kerentanan lainnya ditunjukkan dalam temuan penelitian.

Pengujian keamanan OWASP ZAP di Kali Linux menunjukkan kerentanan dan solusi untuk memperkuat keamanan website. Oleh karena itu, penelitian ini membantu upaya terus-menerus untuk meningkatkan standar keamanan web dan melindungi data pribadi dari ancaman yang

Selain itu, dengan kemajuan teknologi, tren ancaman keamanan cyber terus berkembang. Serangan-serangan yang lebih canggih mulai muncul dibandingkan dengan sebelumnya. Serangan yang semakin sering terjadi, seperti serangan Distributed Denial of Service (DDoS), ransomware, dan Advanced Persistent Threats (APT), adalah beberapa contoh yang memerlukan penanganan yang serius. Oleh karena itu, pengembangan dan penelitian alat keamanan seperti OWASP ZAP sangat penting untuk menjaga infrastruktur digital aman.

Banyak organisasi kini mulai menerapkan strategi keamanan berlapis karena kesadaran akan pentingnya keamanan web telah meningkat. Strategi ini mencakup penerapan alat pengujian seperti OWASP ZAP, penerapan praktik terbaik dalam pengembangan aplikasi, dan meningkatkan kesadaran karyawan tentang risiko keamanan. Metode ini mengurangi risiko serangan cyber dan melindungi aset digital yang berharga. Namun, masih ada masalah, terutama dalam memastikan bahwa setiap lapisan keamanan bekerja dengan baik dan memastikan sistem tetap up-to-date dengan ancaman terbaru.

Banyak organisasi kini mulai menerapkan strategi keamanan berlapis karena kesadaran akan pentingnya keamanan web telah meningkat. Strategi ini mencakup penerapan alat pengujian seperti OWASP ZAP, penerapan praktik terbaik dalam pengembangan aplikasi, dan meningkatkan kesadaran karyawan tentang risiko keamanan. Metode ini mengurangi risiko serangan cyber dan melindungi aset digital yang berharga. Namun, masih ada masalah, terutama dalam memastikan bahwa setiap lapisan keamanan bekerja dengan baik dan memastikan sistem tetap up-to-date dengan ancaman terbaru

METODE

OWASP ZAP adalah aplikasi yang digunakan untuk mendeteksi kerentanan dalam aplikasi web. OWASP ZAP menyediakan pemindai otomatis. Dalam penggunaannya, pemindai OWASP ZAP dapat digunakan untuk menguji server, jaringan, perangkat, dan endpoint. Proses

pemindaian mencakup beberapa tahapan, yaitu eksplorasi, serangan, dan pelaporan**.**

Berikut adalah kerangka kerja penelitian yang dilakukan untuk menganalisis kerentanan sebuah website menggunakan aplikasi OWASP ZAP.

Gambar 1. Alur penelitian

Pengumpulan Data

Tahapan pertama adalah pengumpulan data untuk mendapatkan informasi yang diperlukan guna mencapai tujuan penelitian.

Analisis Kerentanan Website

Selanjutnya, dilakukan studi literatur dari berbagai sumber seperti jurnal dan buku untuk memperolehinformasi terkait metode penyerangan dan kerentanan website.

Menentukan Solusi

Tahap berikutnya adalah menganalisis kerentanan website menggunakan OWASP ZAP dan mencarisolusi yang sesuai

Kesimpulan

Langkah terakhir adalah menyimpulkan hasil penelitian berdasarkan analisis yang telah dilakukan.Harap mengirimkan naskah anda secara elektronik untuk direview sebagaiattachmentse-mail. Ketika anda mengirimkan dokumen naskah versi awal dalam format Word.docx.

HASIL DAN PEMBAHASAN

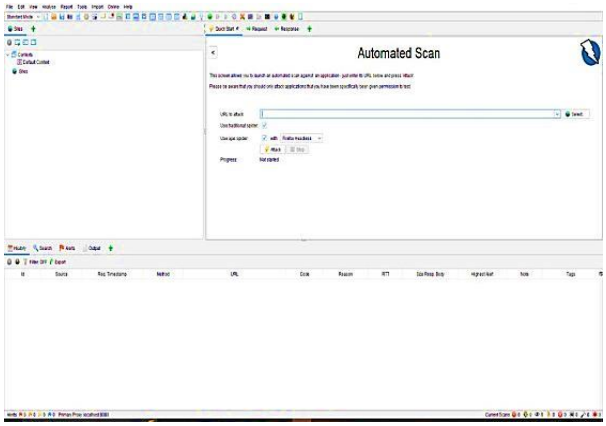
Langkah-langkah berikut menjelaskan proses penggunaan OWASP ZAP untuk menganalisis kerentanan sebuah website secara sistematis:

Tampilan Awal OWASP ZAP

Saat pertama kali membuka program OWASP ZAP, pengguna akan melihat tampilan awal. Pada halaman ini, klik opsi Automated Scan yaggditandaidenganikon

Gambar 2. Tampilan halaman utama aplikasi Owasp Zap.

Sebuah sumber daya yang dimaksudkan untuk melakukan pengujian keamanan aplikasi web. Terdapat Menu Bar di bagian atas jendela yang memberikan akses ke berbagai fungsi dan fitur aplikasi, seperti File, Edit, View, Tools, dan Help. Menu Bar juga memungkinkan pengguna untuk menyesuaikan dan mengkonfigurasi pengaturan ZAP OWASP. Di bawahnya, terdapat Toolbar yang berisi ikon-ikon untuk tindakan cepat, seperti menambahkan permintaan atau respons baru, dan mengakses preferensi aplikasi.



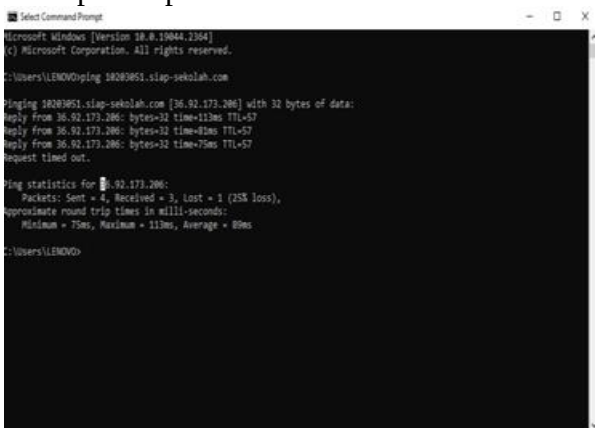
Gambar 3. Tampilan halaman automated scan aplikasi Owasp Zap

Pengguna dapat menemukan form di tengah layar yang memungkinkan mereka untuk memulai pemindaian otomatis terhadap aplikasi web. Dalam bidang teks yang disediakan, pengguna dapat

memasukkan URL aplikasi web yang ingin diuji dan, jika diperlukan, memilih konteks atau seting khusus lainnya. Selain itu, ada tombol Mode Aksi dan Use Context File yang dapat diaktifkan untuk mengubah pengaturan pemindaian lebih lanjut. Di bagian bawah form terdapat indikator Progress yang menunjukkan kemajuan pemindaian. Panel bawah tetap menampilkan keluaran proses atau log, yang mencakup informasi seperti waktu, metode, URL, kode status, dan tipe permintaan atau respons.

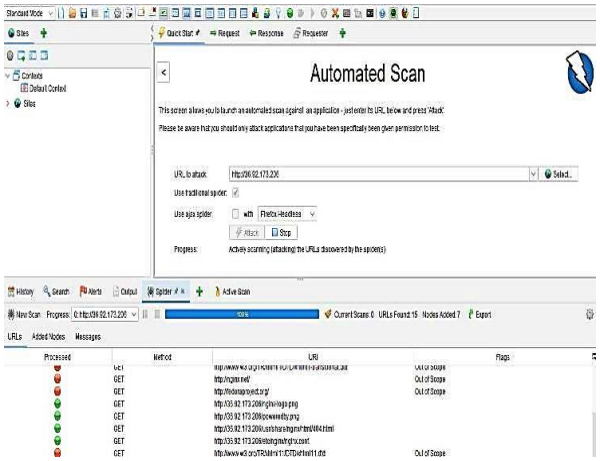
Memasukkan URL Website

Pada langkah ini, masukkan URL website yang telah diperoleh. Cara mendapatkannya adalah dengan mencari URL di Google, menyalin tautan teratas, lalu membuka aplikasi Command Prompt. Ketik perintah ping diikuti dengan URL yang telah disalin, namun tanpa menyertakan http atau https. Tekan Enter, dan nomor atau kode yang muncul Gambar 4dapat dimasukkan ke dalam OWASP ZAP. Setelah itu, tekan Attack untuk memulai proses, seperti yang ditampilkan pada Gambar 4



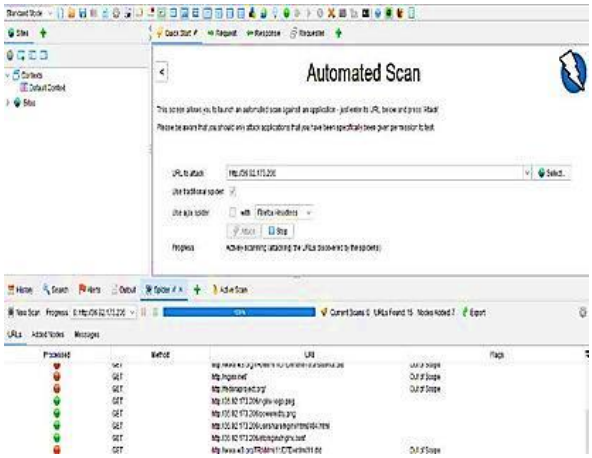
Gambar 4.Tampilan *command prompt*

Proses yang dilakukan untuk mengakses domain 103020515.siap-sekolah.com ditunjukkan pada gambar. Ini dilakukan untuk memastikan bahwa perangkat pengguna terhubung ke server yang dimaksud. Hasil ping menunjukkan bahwa dari empat permintaan yang dikirimkan, satu paket hilang. Ini dapat menunjukkan bahwa ada gangguan kecil pada jaringan. Proses ini relevan selama tahap awal analisis keamanan OWASP ZAP karena diperlukan konektivitas yang stabil untuk memastikan ZAP dapat memindai (scanning) targe dengan baik.



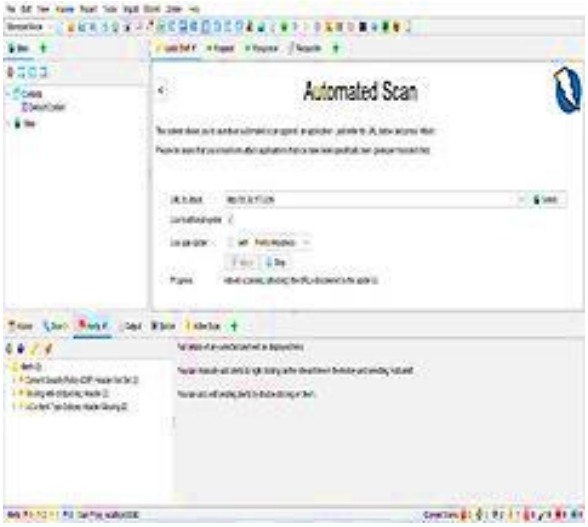
Gambar 5. Tampilan proses scanning Owasp Zap

Terlihat konfigurasi untuk memilih target URL dan tipe pemindaian (spider atau scan aktiva). Proses scan aktiva ditandai dengan progres di bar biru. Di bagian bawah terdapat log aktivitas HTTP yang mencatat berbagai permintaan (requests), metode (GET), URL yang diakses, status respons, dan indikasi kemungkinan kerentanan, seperti peringatan merah atau oranye. Ini menunjukkan bahwa ZAP OWASP memeriksa aplikasi untuk kelemahan seperti XSS, SQL Injection, dan konfigurasi server yang tidak aman, dan memberikan detail hasil pemindaian untuk analisis tambahan.



Gambar 6. Tampilan proses *scanning* Owaszap

OWASP ZAP (Zed Attack Proxy), alat pengujian keamanan aplikasi web sumber terbuka. OWASP ZAP memungkinkan pengguna memindai aplikasi secara otomatis dengan memasukkan URL tujuan, seperti yang terlihat pada fitur Autoscan. Alat ini mendeteksi berbagai kerentanan keamanan, termasuk skrip lintas situs (XSS) dan injeksi SQL, dengan menampilkan URL yang diproses, metode HTTP yang digunakan, dan daftar potensi kerentanan yang terdeteksi. OWASP ZAP juga menawarkan fitur seperti spidering untuk memeriksa struktur aplikasi web dan pemindaian aktif untuk mengidentifikasi kerentanan keamanan dengan lebih baik, menjadikannya pilihan populer di kalangan penguji penetrasi dan tim keamanan aplikasi.



Gambar 7. Tampilan hasil akhir scanning Owaszap

OWASP ZAP (Zed Attack Proxy) dengan fitur "auto scan" untuk menguji keamanan aplikasi web. Di bagian atas terdapat kolom untuk memasukkan URL target yang akan diurai, dan opsi tambahan seperti ``Gunakan laba-laba klasik'' untuk menjelajahi struktur aplikasi. Kemajuan pemindaian juga ditampilkan dan memberikan informasi tentang proses pemindaian saat ini. Tab seperti Peringatan dan Situs muncul di bagian bawah layar dan menampilkan hasil analisis, sepertirincian potensi kerentanan yang terdeteksi dan struktur situs yang sedang dianalisis. OWASP ZAP membantu pengembang dan penguji penetrasi secara efisien mengidentifikasi dan memulihkan kerentanan dalam aplikasi web.

KESIMPULAN

Pengujian menggunakan OWASP ZAP di Kali Linux berhasil mendeteksi beberapa kerentanannya pada website yang dianalisis. Pemindaian ini penting untuk mengidentifikasi dan memperbaiki masalah keamanan sebelum dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Penggunaan alat seperti OWASP ZAP sangat dianjurkan bagi pengembang dan administrator website untuk memastikan bahwa aplikasi mereka aman dari potensi ancaman siber. Untuk meningkatkan keamanan lebih lanjut, sangat disarankan untuk melakukan audit keamanan secara rutin dan memperbaiki setiap celah yang ditemukan.

DAFTAR PUSTAKA

Agus, S. (2020). Penggunaan OWASP ZAP untuk Mengidentifikasi Kerentanan pada Aplikasi Web. Jurnal Keamanan Siber, 5(2), 45-56.

Aydin, M., & Yüksel, M. (2017). Web application security: Threats andcountermeasures. International Journal of Information Security Science, 6(1), 27-37. Christy, M., & Shah, S. (2016). Proactive web application security: Using OWASP ZAP. Proceedings of the 2016 IEEE International Conference on Cybercrime and Computer Forensics (ICCCF), 1-5

Gupta, R., & Bhardwaj, A. (2017). Security Testing Of Web Applications Using OWASP tools. International Journal of Advanced Research in Computer Science, 8(5), 1234-1241.

Jang-Jaccard, J., & Nepal, S. (2014). A Survey Of Emerging Threats In Cybersecurity. Journal Of Computer And System Sciences, 80(5), 973-993.

Kaur, P., & Singh, M. (2018). Vulnerability Analysis And Security Assessment Of Web Applications Using OWASP ZAP. International Journal of Engineering and Advanced Technology, 7(6), 25-30.

Harma, S., & Yadav, A. (2019). A study of Web Application Security Vulnerabilities Using OWASP ZAP. Journal of Information Security Research, 10(4), 177-183.

Verma, P., & Arora, A. (2017). Application of OWASP ZAP In Web Application Security Testing. International Journal Of Engineering Research and Technology,6(9),31-36.

Harahap, A. M., & Nasution, S. (2020). Analisis keamanan web aplikasi menggunakan OWASP ZAP pada Universitas XYZ. Jurnal Teknik Informatika, 8(2), 45-54.

Putra, D. A., & Ramdhani, M. A (2018). Implementasi Dan Analisis Keamanan Aplikasi Web Menggunakan OWASP ZAP Di Lingkungan Perguruan Tinggi. Jurnal Teknologi Informasi dan Komunikasi, 6(3), 23-30.