JURNAL PENELITIAN MULTIDISIPLIN BANGSA
e-ISSN : 3048-4251
Volume 2, No. 8, Tahun 2026
https://ejournal.amirulbangunbangsapublishing.com/index.php/jpnmb/index

Pengujian Keamanan Website Menggunakan Metode Black Box dengan OWASP ZAP pada Kali Linux

Tamsir Aryadi[1], M. Ridho[2], Ahmad Hafizh[3], Ilham Dani[4]
[1,2,3,4] *Universitas Bina Darma Palembang, Indonesia*

Received : 11 Januari 2026, Revised : 21 Januari 2026, Published : 27 Januari 2026

Corresponding Author
Nama Penulis: Tamsir Aryadi
E-mail: muhammadridho5229@gmail.com

Abstrak

Keamanan website merupakan aspek penting dalam menjaga keberlangsungan layanan dan perlindungan data pengguna. Penelitian ini bertujuan untuk menguji keamanan sebuah website menggunakan metode Black Box Testing dengan memanfaatkan OWASP Zed Attack Proxy (ZAP) pada sistem operasi Kali Linux. Pengujian dilakukan tanpa mengetahui struktur internal sistem, sehingga dapat merepresentasikan sudut pandang pihak eksternal. Tahapan pengujian meliputi persiapan, konfigurasi OWASP ZAP, pemindaian menggunakan fitur spider, passive scan, dan active scan, serta analisis hasil temuan kerentanan. Hasil pengujian menunjukkan adanya beberapa potensi celah keamanan dengan tingkat risiko yang berbeda, terutama terkait konfigurasi keamanan dan validasi input. Seluruh temuan diklasifikasikan berdasarkan standar OWASP Top 10 sebagai dasar penyusunan rekomendasi perbaikan. Penelitian ini menunjukkan bahwa pengujian keamanan menggunakan metode Black Box dengan OWASP ZAP pada Kali Linux efektif dalam memberikan gambaran kondisi keamanan website secara objektif.

Kata kunci *– Keamanan Website, Black Box Testing, OWASP ZAP, Kali Linux*

Abstract

Website security is a critical aspect of ensuring service reliability and protecting user data. This study aims to evaluate the security of a website using the Black Box Testing method by utilizing the OWASP Zed Attack Proxy (ZAP) tool on the Kali Linux operating system. The testing process is conducted without accessing the internal structure of the system, thereby representing the perspective of an external attacker. The evaluation stages include preparation, OWASP ZAP configuration, website scanning using spider, passive scan, and active scan features, followed by an analysis of the identified vulnerabilities. The results indicate the presence of several potential security weaknesses with varying risk levels, particularly related to security misconfigurations and input validation issues. All identified vulnerabilities are classified based on the OWASP Top 10 standard to support risk assessment and improvement recommendations. This study demonstrates that Black Box security testing using OWASP ZAP on Kali Linux is effective in providing an objective overview of website security conditions.

Keywords *– Website Security, Black Box Testing, OWASP ZAP, Kali Linux*

How To Cite : *Aryadi, T., Ridho, M., Hafizh, A., & Dani, I. (2026). Pengujian Keamanan Website Menggunakan Metode Black Box dengan OWASP ZAP pada Kali Linux. Jurnal Penelitian Multidisiplin Bangsa, 2(8), 1482–1491. https://doi.org/10.59837/jpnmb.v2i8.736*

Copyright *©2026 Tamsir Aryadi, M. Ridho, Ahmad Hafizh, Ilham Dani*

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat mendorong penggunaan website sebagai media utama dalam penyediaan layanan dan pertukaran informasi. Namun, penggunaan website yang semakin luas menuntut perhatian lebih terhadap aspek keamanan sistem. Pengujian keamanan website diperlukan untuk mendeteksi kerentanan sejak dini dan menjaga kestabilan layanan yang disediakan.(Al et al., 2025)

Dalam pelaksanaan pengujian keamanan website, Kali Linux sering dimanfaatkan karena menyediakan berbagai tools *penetration testing* yang mendukung analisis kerentanan sistem (Kali Linux. 2023). Kali Linux sebagai platform utama yang dilengkapi berbagai alat seperti *Nmap, Burp Suite, sqlmap, dan OWASP ZAP*. Salah satu tools yang banyak digunakan adalah OWASP Zed Attack Proxy (ZAP), sebuah perangkat lunak *open-source* yang dirancang untuk mendeteksi celah keamanan pada aplikasi web. OWASP ZAP mampu melakukan pemindaian pasif dan aktif untuk mengidentifikasi berbagai jenis kerentanan, seperti *SQL Injection*, *Cross-Site Scripting* (XSS), serta kesalahan konfigurasi keamanan. Kombinasi OWASP ZAP dengan sistem operasi Kali Linux dinilai efektif dan efisien dalam proses pengujian keamanan website. (Irawan, 2022)

Metode *Black Box* yang dipadukan dengan OWASP ZAP memungkinkan pengujian keamanan dilakukan secara objektif dan sistematis dengan mengacu pada standar OWASP Top 10. Hasil pengujian yang diperoleh dapat digunakan sebagai dasar evaluasi untuk meningkatkan keamanan aplikasi web melalui perbaikan konfigurasi, penerapan kontrol keamanan yang lebih ketat, serta penguatan perlindungan data pengguna. Dengan demikian, pengujian keamanan website secara berkala sangat diperlukan untuk meminimalkan risiko serangan siber dan menjaga kepercayaan pengguna terhadap layanan berbasis web.(Febriana, 2022)

TINJAUAN PUSTAKA

Keamanan Website

Keamanan website merupakan komponen krusial dalam pengelolaan sistem informasi berbasis web karena berfungsi melindungi data serta menjaga kestabilan layanan dari berbagai ancaman siber. Website yang tidak memiliki sistem keamanan yang memadai berpotensi mengalami serangan seperti pencurian informasi, perubahan data tanpa izin, maupun gangguan operasional. Oleh sebab itu, pengujian keamanan perlu dilakukan secara sistematis guna mengidentifikasi kelemahan sistem sejak dini sehingga tindakan pencegahan dapat diterapkan sebelum terjadi eksploitasi oleh pihak yang tidak bertanggung jawab.(Nurelasari et al., 2024)

Metode Black Box Testing

Metode *Black Box* adalah teknik pengujian yang menitikberatkan pada evaluasi fungsi sistem tanpa memerlukan pengetahuan mengenai struktur internal maupun kode sumber aplikasi. Pengujian dilakukan dengan memberikan berbagai skenario input dan mengamati respons yang dihasilkan oleh sistem untuk mendeteksi potensi kerentanan keamanan. Pendekatan ini dinilai efektif karena mampu mensimulasikan serangan dari sudut pandang pengguna eksternal, sehingga memberikan gambaran kondisi keamanan website yang lebih realistis dan objektif.(W et al., 2021)

OWASP Zed Attack Proxy (ZAP)

OWASP Zed Attack Proxy (ZAP) merupakan salah satu tools pengujian keamanan aplikasi web yang dikembangkan oleh Open Web Application Security Project (OWASP) dan bersifat *open-source*. Tools ini dirancang untuk membantu proses identifikasi kerentanan melalui pemindaian pasif dan aktif yang mengacu pada standar OWASP Top 10. Dengan kemampuan mendeteksi berbagai jenis celah keamanan seperti *SQL Injection*, *Cross-Site Scripting* (XSS), dan kesalahan konfigurasi, OWASP ZAP menjadi alat yang banyak digunakan dalam penelitian dan praktik pengujian keamanan website.(Zairina et al., 2025)

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

Kali Linux sebagai Platform Pengujian Keamanan

Kali Linux merupakan sistem operasi berbasis Linux yang dirancang khusus untuk kebutuhan *penetration testing* dan analisis keamanan jaringan maupun aplikasi web. Sistem operasi ini menyediakan berbagai tools pendukung yang terintegrasi, termasuk OWASP ZAP, sehingga memudahkan proses pengujian keamanan secara menyeluruh. Penggunaan Kali Linux sebagai platform pengujian memberikan lingkungan kerja yang stabil dan efisien, serta mendukung penerapan metode *Black Box* dalam mengidentifikasi kerentanan website secara optimal.(Linux et al., 2025)

METODE

Penelitian ini menggunakan pendekatan deskriptif dengan metode pengujian keamanan aplikasi web. Pendekatan deskriptif dipilih untuk menggambarkan kondisi keamanan website berdasarkan hasil pengujian yang dilakukan tanpa melakukan manipulasi terhadap sistem. Metode pengujian yang digunakan adalah *Black Box Testing*, yaitu pengujian yang berfokus pada fungsi dan respons sistem tanpa mengetahui struktur internal atau kode sumber aplikasi. Pendekatan ini bertujuan untuk mensimulasikan serangan dari sudut pandang pengguna eksternal sehingga hasil pengujian mencerminkan kondisi keamanan website yang sesungguhnya.(Hasibuan & Elhanafi, 2022)

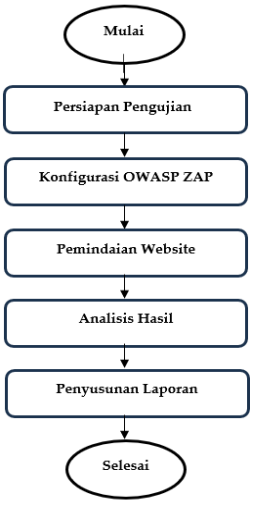
Objek Penelitian

Objek dalam penelitian ini adalah sebuah website yang digunakan sebagai target pengujian keamanan. Website tersebut diuji untuk mengetahui tingkat kerentanan terhadap berbagai jenis serangan siber yang umum terjadi pada aplikasi web. Pengujian dilakukan tanpa mengubah konfigurasi sistem secara langsung, sehingga seluruh proses analisis dilakukan berdasarkan interaksi eksternal melalui antarmuka website. Hal ini sesuai dengan prinsip metode *Black Box* yang menekankan pengujian dari sisi pengguna atau penyerang luar.(Priambodo et al., 2023)

Tools dan Lingkungan Pengujian

Lingkungan pengujian pada penelitian ini menggunakan sistem operasi Kali Linux yang dirancang khusus untuk kebutuhan *penetration testing*. Tools utama yang digunakan adalah OWASP Zed Attack Proxy (ZAP), yang berfungsi untuk melakukan pemindaian kerentanan pada aplikasi web. OWASP ZAP digunakan karena mampu mendeteksi berbagai celah keamanan berdasarkan standar OWASP Top 10, seperti *SQL Injection*, *Cross-Site Scripting* (XSS), dan kesalahan konfigurasi keamanan. Kombinasi Kali Linux dan OWASP ZAP memberikan dukungan yang optimal dalam proses pengujian keamanan website secara terstruktur.(Kerentanan et al., 2025)

Tahap Pengujian Keamanan



Gambar 1.
Alur Penelitian

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

1. Persiapan Pengujian
   Tahap ini mencakup penentuan target website, ruang lingkup pengujian, serta persiapan lingkungan pengujian menggunakan Kali Linux dan OWASP ZAP agar proses pengujian berjalan terarah.
2. Konfigurasi OWASP ZAP
   Pada tahap ini dilakukan pengaturan proxy, browser, dan parameter pemindaian pada OWASP ZAP untuk memastikan seluruh aktivitas akses website dapat direkam dan dianalisis dengan baik.
3. Pemindaian Website
   Pemindaian dilakukan secara menyeluruh dengan memanfaatkan fitur *spider*, pemindaian pasif, dan pemindaian aktif pada OWASP ZAP. Tahap ini bertujuan untuk memetakan struktur website sekaligus mendeteksi berbagai potensi celah keamanan.
4. Analisis hasil Pengujian
   Setelah pemindaian selesai, hasil yang diperoleh diperiksa dan dikelompokkan berdasarkan jenis serta tingkat risiko kerentanannya. Analisis ini membantu menentukan bagian mana dari website yang perlu segera diperbaiki.
5. Penyusunan Laporan Pengujian
   Tahap terakhir adalah menyusun laporan yang berisi hasil pengujian, daftar celah keamanan yang ditemukan, serta saran perbaikan. Laporan ini digunakan sebagai acuan untuk meningkatkan keamanan website agar lebih aman dari serangan siber.

Teknik Analisis Data

Data yang diperoleh dari hasil pemindaian OWASP ZAP dianalisis secara kualitatif dengan mengelompokkan kerentanan berdasarkan kategori dan tingkat risikonya, seperti rendah, sedang, dan tinggi. Analisis ini bertujuan untuk memberikan gambaran menyeluruh mengenai kondisi keamanan website serta menentukan prioritas perbaikan yang perlu dilakukan. Hasil analisis kemudian disajikan dalam bentuk deskripsi dan tabel untuk memudahkan pemahaman serta mendukung pengambilan keputusan terkait peningkatan keamanan system.(Sabariman et al., 2024)

PEMBAHASAN

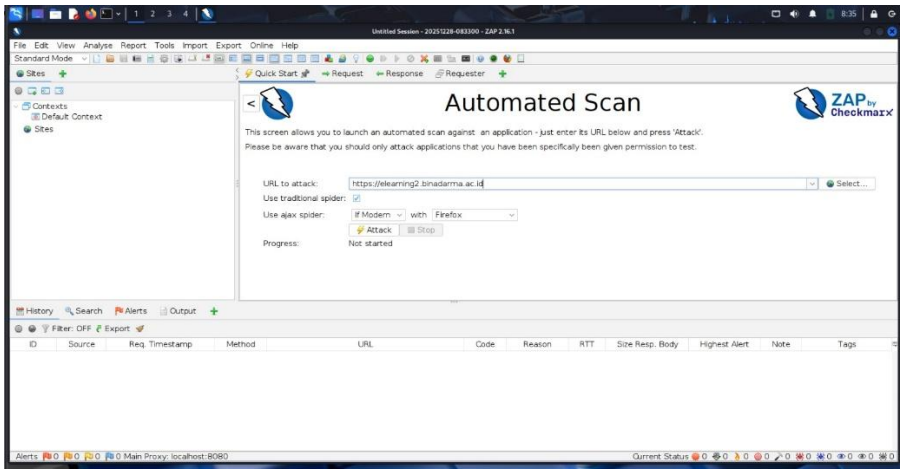
Pada penelitian ini, dilakukan pengujian keamanan website elearning2.binadarma.ac.id menggunakan metode Black Box, yaitu metode pengujian yang dilakukan tanpa mengetahui struktur kode sumber maupun konfigurasi internal sistem. Pengujian dilakukan dari sudut pandang pengguna atau pihak luar, sehingga dapat menggambarkan kondisi keamanan website secara nyata. Alat yang digunakan adalah OWASP Zed Attack Proxy (ZAP) yang dijalankan pada sistem operasi Kali Linux, karena Kali Linux menyediakan lingkungan yang stabil dan lengkap untuk keperluan pengujian keamanan.(W et al., 2021)

Tahapan pengujian keamanan pada penelitian ini dibagi menjadi lima tahap utama, yaitu persiapan pengujian, konfigurasi OWASP ZAP, pemindaian website, analisis hasil pengujian, dan penyusunan laporan pengujian.(Linux et al., 2025)

Tahap Persiapan Pengujian

Tahap persiapan pengujian merupakan langkah awal yang bertujuan untuk memastikan bahwa seluruh kebutuhan pengujian telah siap sebelum proses pengujian dilakukan. Pada tahap ini, peneliti menyiapkan sistem operasi Kali Linux sebagai platform utama pengujian. Kali Linux dipilih karena telah dilengkapi dengan berbagai tools pengujian keamanan, termasuk OWASP ZAP.(Oleh, 2022)

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

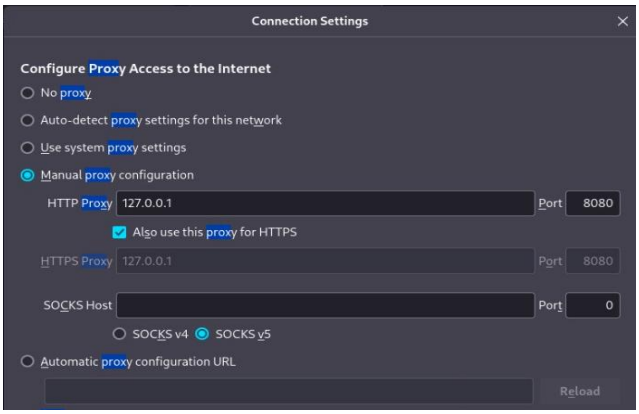


Gambar 2.
Tampilan Awal OWASP ZAP

Selanjutnya, peneliti menentukan target pengujian, yaitu website elearning2.binadarma.ac.id. Pengujian dilakukan dalam konteks akademik dan penelitian, dengan tujuan untuk menganalisis tingkat keamanan website. Oleh karena itu, aspek etika dan legalitas tetap diperhatikan selama proses pengujian.

Pada tahap ini, peneliti juga melakukan pengamatan awal terhadap website, seperti struktur halaman, fitur login, menu navigasi, serta layanan utama yang tersedia. Hal ini dilakukan untuk memahami ruang lingkup website yang akan diuji, sehingga proses pengujian dapat berjalan secara terarah dan menyeluruh.

Konfigurasi OWASP ZAP



Gambar 3.
Konfigurasi Proxy

Setelah tahap persiapan selesai, langkah berikutnya adalah melakukan konfigurasi OWASP ZAP. OWASP ZAP dijalankan pada Kali Linux dan diatur sebagai proxy yang menghubungkan browser dengan website target. Dengan pengaturan ini, seluruh lalu lintas data antara browser dan website elearning2.binadarma.ac.id dapat dipantau dan dianalisis oleh OWASP ZAP.

Browser dikonfigurasi agar menggunakan alamat proxy lokal OWASP ZAP, sehingga setiap permintaan (*request*) dan tanggapan (*response*) HTTP dapat terekam secara otomatis. Selain itu, peneliti

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

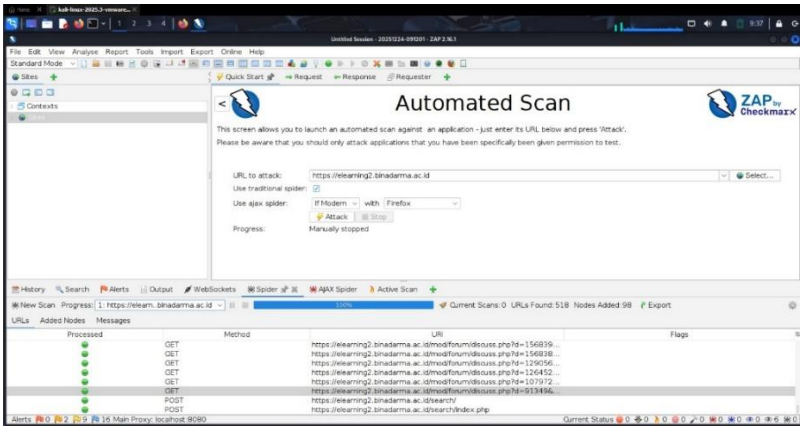
juga mengatur scope target pada OWASP ZAP agar pemindaian hanya difokuskan pada domain elearning2.binadarma.ac.id, sehingga tidak terjadi pemindaian ke domain lain yang tidak terkait.

OWASP ZAP digunakan dalam konteks pengujian Black Box, di mana seluruh pengujian dilakukan tanpa akses ke sistem internal website. Konfigurasi ini mencerminkan kondisi nyata di lapangan, di mana potensi serangan berasal dari pihak luar yang hanya memiliki akses melalui antarmuka website.(Bimandaru et al., 2023)

Pemindaian Website

Tahap pemindaian website merupakan inti dari proses pengujian keamanan. Pada tahap ini, OWASP ZAP digunakan untuk melakukan berbagai jenis pemindaian guna mengidentifikasi potensi kerentanan pada website elearning2.binadarma.ac.id. Pemindaian dilakukan melalui beberapa metode, antara lain *Spider*, *Passive Scan*, dan *Active Scan*.(Priambodo et al., 2023)

a. Spider



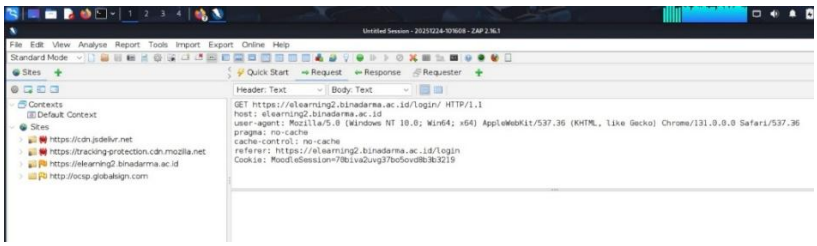
Gambar 4.
Pemindaian Spider

Proses spider digunakan untuk menjelajahi seluruh halaman website secara otomatis. OWASP ZAP mengakses setiap tautan yang tersedia pada website, termasuk halaman login, dashboard, dan fitur lainnya yang dapat diakses. Tujuan dari proses ini adalah untuk memetakan struktur website serta mengidentifikasi halaman dan parameter yang berpotensi memiliki celah keamanan.

Dengan adanya proses spider, OWASP ZAP dapat mengetahui ruang lingkup website secara lebih luas, sehingga pemindaian selanjutnya dapat dilakukan secara lebih menyeluruh.

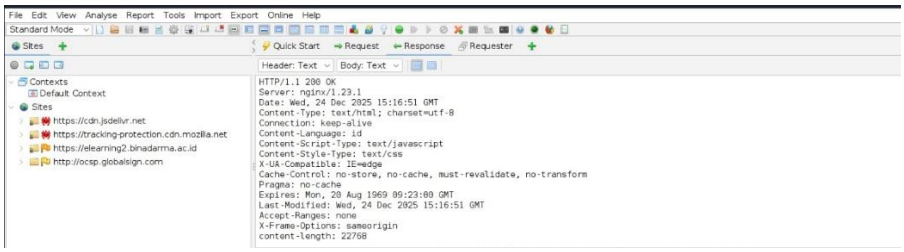
b. Passive Scan

Passive scan dilakukan secara otomatis saat OWASP ZAP memantau lalu lintas data antara browser dan website. Pada metode ini, OWASP ZAP tidak mengirimkan serangan secara langsung, melainkan hanya menganalisis request dan response yang terjadi secara normal.



Gambar 5.
Hasil Analisis Request

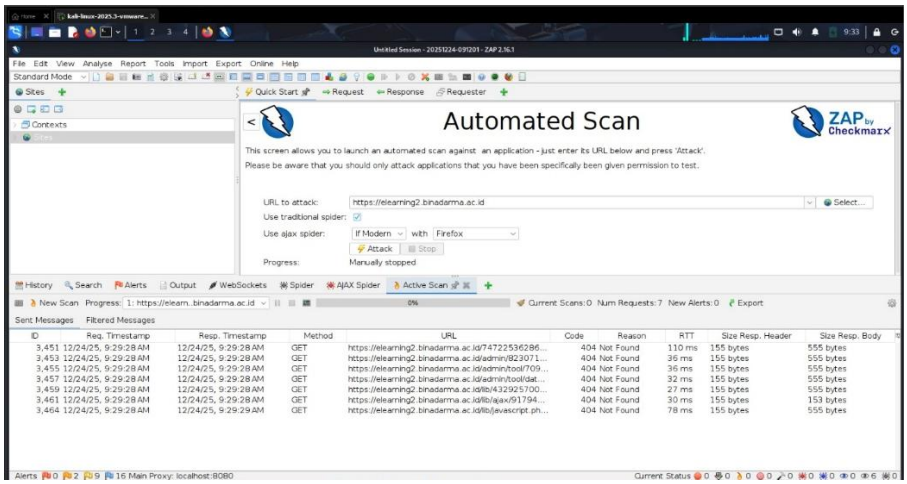
This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license



Gambar 6.
Hasil Analisis Response

Passive scan bertujuan untuk mendeteksi kerentanan yang bersifat ringan hingga sedang, seperti pengungkapan informasi melalui header HTTP, penggunaan cookie yang tidak aman, serta konfigurasi keamanan yang kurang tepat. Karena tidak melakukan interaksi aktif, metode ini relatif aman dan tidak mengganggu kinerja website.

c. Active Scan



Gambar 7.
Pemindaian Aktif

Active scan merupakan metode pemindaian aktif yang dilakukan dengan cara mengirimkan permintaan tertentu ke website untuk menguji adanya potensi kerentanan. Pada tahap ini, OWASP ZAP mencoba mengidentifikasi celah keamanan seperti SQL Injection, Cross-Site Scripting (XSS), dan kerentanan input lainnya.

Pemindaian aktif dilakukan secara terkontrol dan bertujuan untuk mengetahui sejauh mana website mampu menahan serangan dari pihak luar. Hasil dari active scan memberikan gambaran yang lebih jelas mengenai tingkat keamanan website elearning2.binadarma.ac.id.

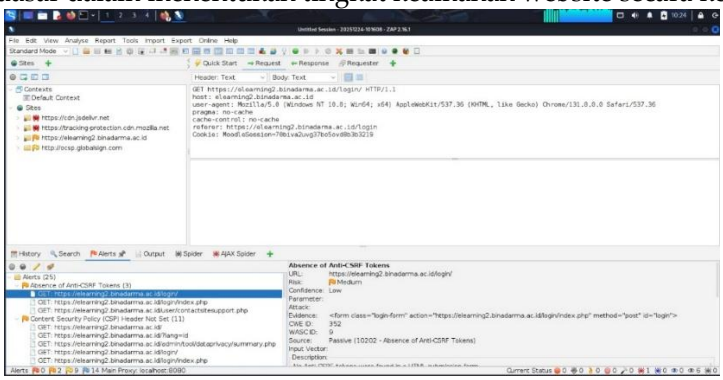
Analisis Hasil Pengujian

Setelah proses pemindaian selesai, tahap selanjutnya adalah melakukan analisis terhadap hasil pengujian yang diperoleh dari OWASP ZAP. Hasil pemindaian ditampilkan dalam bentuk daftar temuan kerentanan yang diklasifikasikan berdasarkan tingkat risiko, seperti rendah, menengah, dan tinggi.

Pada tahap ini, peneliti meninjau setiap temuan untuk memahami jenis kerentanan yang terdeteksi serta potensi dampak yang dapat ditimbulkan terhadap sistem e-learning. Analisis

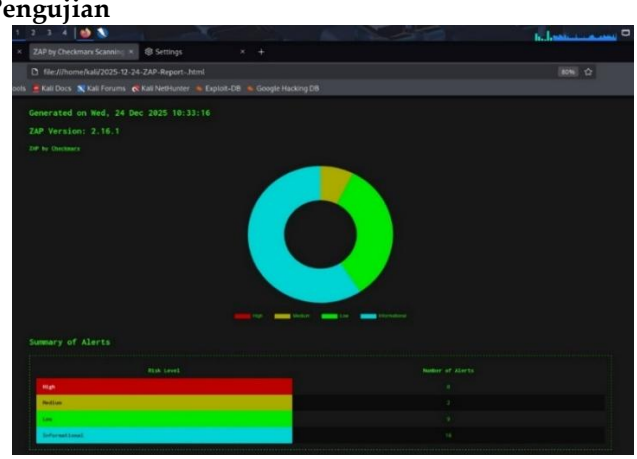
This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

dilakukan dengan mengacu pada standar keamanan aplikasi web, seperti OWASP Top 10, sehingga dapat diketahui apakah kerentanan yang ditemukan termasuk dalam kategori risiko yang serius.
Selain itu, peneliti juga mengevaluasi apakah kerentanan tersebut berpotensi mempengaruhi data pengguna, seperti data akun mahasiswa dan dosen, atau hanya bersifat konfigurasi teknis. Hasil analisis ini menjadi dasar dalam menentukan tingkat keamanan website secara keseluruhan

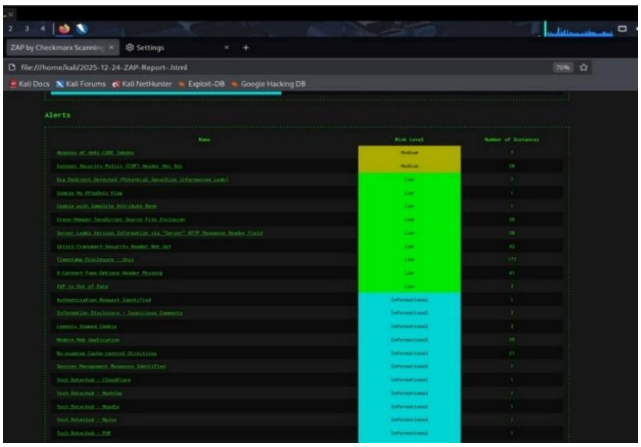


Gambar 8.
Hasil Pengujian (Alerts)

Penyusunan Laporan Pengujian



Gambar 9.
Diagram Laporan Pengujian



Gambar 10.
Laporan Tingkat Resiko

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

Tahap terakhir dari proses pengujian keamanan adalah penyusunan laporan pengujian. Laporan ini disusun secara sistematis agar mudah dipahami oleh pihak pengelola website maupun pihak akademik. Laporan pengujian mencakup informasi mengenai metode pengujian, alat yang digunakan, tahapan pengujian, serta hasil temuan kerentanan.

Selain itu, laporan juga memuat penjelasan singkat mengenai setiap kerentanan yang ditemukan beserta rekomendasi perbaikan yang dapat dilakukan untuk meningkatkan keamanan website elearning2.binadarma.ac.id. Rekomendasi ini diharapkan dapat membantu pengelola sistem dalam memperbaiki celah keamanan yang ada.

Laporan pengujian ini juga dapat dijadikan sebagai dokumentasi dan referensi untuk pengujian keamanan di masa mendatang, sehingga keamanan website e-learning dapat terus ditingkatkan secara berkelanjutan.

KESIMPULAN

Kesimpulan dari penelitian ini menunjukkan bahwa pengujian keamanan website menggunakan metode Black Box dengan bantuan OWASP Zed Attack Proxy (ZAP) pada Kali Linux dapat memberikan gambaran yang objektif mengenai tingkat keamanan aplikasi web. Melalui tahapan persiapan, konfigurasi, pemindaian, hingga laporan hasil pengujian, berbagai potensi celah keamanan berhasil diidentifikasi, baik yang bersifat ringan maupun yang berisiko lebih tinggi. Temuan tersebut dapat dimanfaatkan sebagai bahan evaluasi untuk meningkatkan keamanan website melalui perbaikan konfigurasi, penerapan kontrol keamanan yang lebih baik, serta penguatan perlindungan data pengguna. Oleh karena itu, pengujian keamanan secara berkala menggunakan OWASP ZAP menjadi langkah penting untuk meminimalkan risiko serangan siber dan menjaga keandalan serta kepercayaan pengguna terhadap layanan berbasis web. Selain itu, hasil penelitian ini dapat membantu administrator website dalam mengidentifikasi dan menangani celah keamanan sejak dini sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab, serta memberikan kontribusi dalam memperluas pemahaman mengenai efektivitas penggunaan tools otomatis dalam pengujian keamanan aplikasi web menggunakan metode Black Box.

DAFTAR PUSTAKA

Al, R., Bintang, R., & Widyawan, T. I. (2025). *Pengujian Kerentanan Website Menggunakan Metode Penetration Testing Dengan OWASP (Studi Kasus : Pemerintah Kabupaten Semarang) Website Vulnerability Testing Using the Penetration Testing Method with OWASP (Case Study : Semarang Regency Government)*. *8*(2), 106–115.

Bimandaru, A., Alamsyah, A., & Nugroho, A. (2023). Analisis Pengujian Penetrasi Pada Layanan Hosting Menggunakan Metode Black Box (Studi kasus : Blogspot, Wordpress dan Shared Hosting). *Foristek*, *14*(1). https://doi.org/10.54757/fs.v14i1.238

Febriana, R. (2022). Blackbox Testing Sistem Informasi Absensi Pegawai Karawang Dengan Metode Top 10 Owasp Attack. *Jurnal Ilmiah Wahana Pendidikan*, *8*(12), 327–334. 10.5281/zenodo.6945632

Hasibuan, M., & Elhanafi, A. M. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. *Sudo Jurnal Teknik Informatika*, *1*(4), 171–177. https://doi.org/10.56211/sudo.v1i4.160

Irawan, D. S. (2022). Pengujian Keamanan Sistem Informasi Berbasis Web Berdasarkan Dokumen Owasp Wstg v4. 2 (Studi Kasus: Sistem Informatics Expo Universitas Islam Indonesia). *Universitas Islam Indonesia*, *2*. https://dspace.uii.ac.id/handle/123456789/40200

Kerentanan, A., Pendekatan, M., Kasus, S., & Universitas, S. (2025). *Swadharma (jeis)*. *05*.

Linux, D. K., Bernandra, C., Pura, P., Maulana, T. Y., Februri, A., & Ariyadi, T. (2025). *Analisis Celah Keamanan Website Menggunakan Tools OWASP ZAP*. *4*(1).

Nurelasari, E., Gumilang, D., & Farabi, A. (2024). *Analisis Keamanan Sistem Website Menggunakan Metode*

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

Open Web Application Security Project (OWASP) Pada Simantep . ID. *8*(3), 3049–3054.

Oleh, D. (2022). *Universitas Islam Indonesia) Tugas Akhir*. *2*.

Priambodo, D. F., Rifansyah, A. D., & Hasbi, M. (2023). Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating. *Teknika*, *12*(1), 33–46. https://doi.org/10.34148/teknika.v12i1.571

Sabariman, S., Haeruddin, H., & Lee, D. (2024). Analisis Kerentanan Aplikasi Akademik Berbasis Website Xyz Menggunakan Owasp. *Jurnal Khatulistiwa Informatika*, *11*(2), 92–102. https://doi.org/10.31294/jki.v11i2.20194

W, Y., Anto, R., Teguh Yuwono, D., & Yuliadi, Y. (2021). Deteksi Serangan Vulnerability Pada Open Jurnal System Menggunakan Metode Black-Box. *Jurnal Informatika Dan Rekayasa Elektronik*, *4*(1), 68–77. https://doi.org/10.36595/jire.v4i1.365

Zairina, Z., Huwae, R. B., & Jatmika, A. H. (2025). *Implementasi Owasp Top 10 Dalam Pengujian Penetrasi Website : Mengidentifikasi Celah Keamanan Dalam Sistem Pengelolaan Voting Indonesia (Implementation Of OWASP Top 10 In Website Penetration Testing : Identifying Security Gaps in Indonesia ' s Voting Man*. *7*(1).

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license