**Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika**
**Volume 3, Nomor 1, Tahun 2025**
e-ISSN: 3031-8912; p-ISSN: 3031-8904; Hal 66-76
DOI : https://doi.org/10.61132/merkurius.v3i1.585
*Available online at:* https://journal.arteii.or.id/index.php/Merkurius

# Deteksi Kerentanan Keamanan Dan Mitigasi Situs Web Crowdo.Co.Id Berbasis OWASP Zed Attack Proxy (ZAP )

**Mochammad Fadilah [1*], Nur Nawaningtyas [2]**
[1.2] Program Studi Teknik Informatik, STMIK Widuri, Jakarta Selatan, Indonesia

Alamat: 3, Jl. Palmerah Barat No.353, RT.3/RW.5, Grogol Utara, Kec. Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 11480
*Correspondence email: dbrantakanz82@gmail.com*

***ABSTRACT:*** *This study aims to analyze security vulnerabilities and mitigation on the crowdo.co.id website using the OWASP Zed Attack Proxy (ZAP) tool, which is a web application security testing tool. High-level security attacks have increasingly risen alongside the advancement of information technology, making vulnerability testing crucial to ensure the integrity and security of information systems. This research involved scanning the crowdo.co.id website to identify various vulnerabilities, including those listed in the OWASP Top 10. The research process encompassed active and passive scanning, data analysis from the scans, and the formulation of mitigation strategies for each identified vulnerability. The findings revealed that the website had 14 detected vulnerabilities, consisting of 1 high-priority vulnerability, 3 medium-priority vulnerabilities, 7 low-priority vulnerabilities, and 3 additional informational alerts. The security dimensions tested included potential XSS attacks, SQL Injection, and other deficiencies that could jeopardize user data. Based on these results, recommended mitigations include code improvements, enhanced security configurations, and the implementation of additional preventive measures. This study concludes that while the website's security is in the medium category, further improvements are necessary to reduce vulnerability risks. Through this approach, the study provides significant contributions to enhancing web application security.*

***Keywords:*** *Vulnerability, Security, OWASP, ZAP*

**ABSTRAK**: Penelitian ini bertujuan untuk menganalisis kerentanan keamanan dan mitigasi pada situs web crowdo.co.id menggunakan alat OWASP Zed Attack Proxy (ZAP), yang merupakan alat pengujian keamanan aplikasi web. Serangan keamanan tingkat tinggi semakin meningkat seiring perkembangan teknologi informasi, sehingga pengujian kerentanan menjadi penting untuk memastikan integritas dan keamanan sistem informasi. Penelitian ini dilakukan dengan memindai situs web crowdo.co.id untuk mengidentifikasi berbagai kerentanan, termasuk kerentanan yang sesuai dengan OWASP Top 10. Proses penelitian mencakup pemindaian aktif dan pasif, analisis data hasil pemindaian, serta penyusunan strategi mitigasi untuk setiap kerentanan yang ditemukan. Hasil penelitian menunjukkan bahwa situs web ini memiliki 14 kerentanan yang terdeteksi, terdiri dari 1 kerentanan prioritas tinggi, 3 kerentanan prioritas sedang, 7 kerentanan prioritas rendah, dan 3 informasi tambahan. Dimensi keamanan yang diuji mencakup potensi serangan XSS, SQL Injection, dan kekurangan lainnya yang dapat mengancam data pengguna. Berdasarkan hasil tersebut, mitigasi yang direkomendasikan meliputi perbaikan kode, peningkatan konfigurasi keamanan, dan penerapan langkah-langkah preventif tambahan. Penelitian ini menyimpulkan bahwa meskipun keamanan situs berada dalam kategori sedang, perbaikan lebih lanjut sangat diperlukan untuk mengurangi risiko kerentanan. Dengan pendekatan ini, penelitian memberikan kontribusi penting dalam meningkatkan keamanan aplikasi web. owasp zap, audit keamanan, keamanan website, crowdo.co.id

**Kata Kunci:** Kerentanan, Keamanan, OWASP, ZAP

## 1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa berbagai kemajuan di berbagai bidang kehidupan. Teknologi tidak hanya membawa manfaat berupa kemudahan akses informasi, peningkatan efisiensi kerja, dan konektivitas global, namun juga membawa tantangan baru, terutama terkait keamanan siber. Dalam beberapa tahun terakhir, jumlah dan kompleksitas serangan keamanan terhadap sistem informasi telah meningkat. Serangan-

*Received November 23, 2024; Revised Desember 08, 2024; Accepted Desember 22, 2024;*
*Online Available Desember 24, 2024*

serangan ini sering mengeksploitasi celah dan kerentanan dalam sistem dan dapat membahayakan integritas, kerahasiaan, dan ketersediaan data (Novianto et al., 2016). Dalam konteks ini, pengujian kerentanan menjadi elemen kunci dalam mendeteksi dan memitigasi risiko keamanan yang dapat berdampak negatif pada sistem informasi. Metode yang banyak digunakan adalah menggunakan alat pengujian otomatis seperti OWASP Zed Attack Proxy (ZAP). Alat ini dirancang untuk mendeteksi berbagai jenis kerentanan dalam aplikasi web melalui analisis lalu lintas dan pengujian kerentanan aktif. Penelitian ini didasarkan pada studi kasus situs web "crowdo.co.id", sebuah platform layanan aplikasi pinjaman bisnis yang mengutamakan keamanan dalam bertransaksi keuangan. Studi ini bertujuan menggunakan OWASP ZAP untuk mengidentifikasi kerentanan keamanan, memprioritaskan kerentanan, dan memberikan tindakan mitigasi untuk meningkatkan keamanan situs web (Al-matarneh, 2020). Berdasarkan teori keamanan sistem informasi (Anderson et al., 2021) yang bertujuan untuk melindungi data dan layanan dari akses tidak sah, intrusi, dan kerusakan, penelitian ini menggunakan deteksi kerentanan dan memanfaatkan prinsip-prinsip mitigasi (Anderson et al., 2022) untuk menyelidiki kode yang dapat dieksploitasi, desain, dan kelemahan konfigurasi. OWASP ZAP digunakan sebagai alat sumber terbuka oleh Open Web Application Security Project (OWASP) untuk menyusun OWASP Top 10 (daftar kerentanan aplikasi web yang paling umum, termasuk injeksi, otentikasi palsu, dan cross-site scripting (XSS) ). Mendeteksi kerentanan berdasarkan: (Kapoyos dan kawan-kawan, 2023). Oleh karena itu, penelitian ini tidak hanya mengidentifikasi risiko tetapi juga memberikan strategi perbaikan seperti: Hal ini termasuk memperkuat konfigurasi, menyempurnakan kode, dan menambahkan lapisan perlindungan (O'Neill et al., 2022) untuk memastikan bahwa kerentanan yang ditemukan tidak dieksploitasi lagi. Penelitian ini secara khusus akan berkontribusi dalam meningkatkan keandalan dan keamanan situs web crowdo.co.id dan memberikan lebih banyak informasi kepada pengembang aplikasi web di Indonesia tentang pentingnya keamanan siber dalam menghadapi tantangan era digital. Milano dkk., 2020).

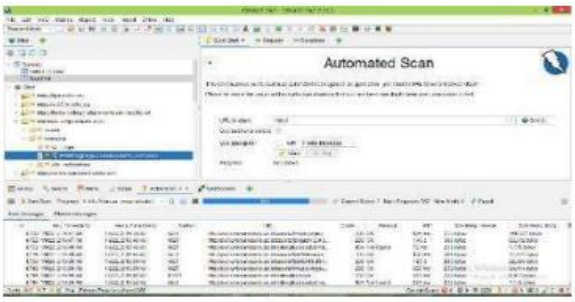
## 2. METODE PENELITIAN

Penelitian ini bertujuan untuk mendeteksi dan mengatasi kerentanan keamanan yang ada pada situs web crowdo.co.id dengan menggunakan metode OWASP Zed Attack Proxy (ZAP). Metode ini dipilih karena kemampuannya dalam melakukan pemindaian keamanan secara mendalam dan terstruktur, yang dapat membantu mengidentifikasi potensi celah atau kelemahan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Dengan

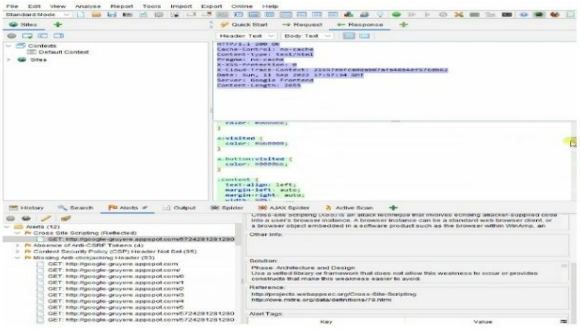
menggunakan teknik pemindaian aktif dan pasif, penelitian ini akan mengungkap berbagai jenis kerentanan yang dapat mempengaruhi integritas dan kerahasiaan data yang ada di situs tersebut, seperti SQL injection, cross-site scripting (XSS), dan kerentanan lainnya yang termasuk dalam kategori OWASP Top 10 (Charly et al., 2022).

Dalam penelitian ini, pendekatan yang digunakan adalah pendekatan kualitatif dengan fokus pada analisis mendalam terhadap hasil pemindaian yang dilakukan oleh OWASP ZAP. Selain itu, penelitian ini juga akan memberikan rekomendasi terkait tindakan mitigasi yang perlu diambil untuk memperbaiki dan memperkuat sistem keamanan pada situs **crowdo.co.id**. Pendekatan ini diharapkan dapat memberikan gambaran yang jelas tentang bagaimana situs web dapat memitigasi potensi ancaman, serta memberikan solusi berbasis standar terbaik dalam pengamanan aplikasi web (Musa Shuaibu et al., 2015).

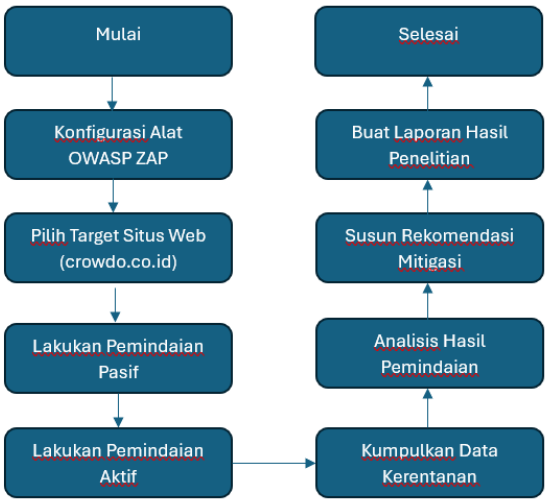
Hasil dari penelitian ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan keamanan situs web, serta memberikan wawasan bagi pengembang dan pemilik situs untuk mengurangi risiko serangan yang dapat merugikan baik pengguna maupun pengelola situs. Dengan demikian, penelitian ini tidak hanya akan mengidentifikasi masalah, tetapi juga menawarkan solusi praktis yang dapat diterapkan untuk meningkatkan ketahanan keamanan situs web terhadap berbagai ancaman yang terus berkembang (Longueira-Romero et al., 2022).




**Gambar 1.** Tampilan  pada aplikasi oswasp zap
*Sumber: Mochammad Fadilah, 2024*



**Gambar 2.** Proses scanning pada aplikasi oswasp zap
*Sumber: Mochammad Fadilah, 2024*




**Gambar 3.** Gambar tahapan penelitian untuk mendeteksi kerentanan menggunakan OWASP ZAP

Bagian - bagian ini menjelaskan langkah-langkah penelitian untuk mengidentifikasi kerentanan keamanan pada situs *crowdo.co.id* menggunakan OWASP ZAP.

a. **Mulai**: Langkah awal dimulai dengan persiapan untuk penelitian.
b. **Konfigurasi Alat OWASP ZAP**: Sebelum pemindaian dilakukan, OWASP ZAP harus dikonfigurasi sesuai dengan kebutuhan penelitian. Ini meliputi pengaturan proxy, target, dan parameter yang relevan untuk pemindaian.
c. **Pilih Target Situs Web (crowdo.co.id)**: Menentukan situs web yang akan menjadi objek penelitian, dalam hal ini situs **crowdo.co.id**.
d. **Lakukan Pemindaian Pasif**: Pemindaian pasif dilakukan untuk mengumpulkan informasi tentang target tanpa mengirimkan permintaan berbahaya. Tahapan ini bertujuan untuk mengidentifikasi kerentanan dasar seperti kebijakan keamanan header HTTP.
e. **Lakukan Pemindaian Aktif**: Setelah pemindaian pasif selesai, dilakukan pemindaian aktif. Tahapan ini melibatkan pengiriman permintaan eksploitasi untuk mengidentifikasi kerentanan lebih dalam, seperti SQL Injection atau XSS (Babate et al., 2015).
f. **Kumpulkan Data Kerentanan**: Semua hasil pemindaian, baik pasif maupun aktif, dikumpulkan untuk dianalisis. Data ini mencakup detail kerentanan yang ditemukan, seperti jenis kerentanan dan lokasinya pada situs web (*Copyright*, 2016).
g. **Analisis Hasil Pemindaian**: Data yang terkumpul dianalisis untuk memahami penyebab dan potensi dampak dari kerentanan yang ditemukan. Ini melibatkan evaluasi tingkat keparahan dan prioritas mitigasi.

h. **Susun Rekomendasi Mitigasi**: Berdasarkan analisis, dibuat rekomendasi langkah-langkah mitigasi untuk mengatasi kerentanan yang ditemukan. Rekomendasi ini dirancang untuk meningkatkan keamanan situs web (*Subject Index*, 2016).

i. **Buat Laporan Hasil Penelitian**: Tahap akhir adalah menyusun laporan yang merangkum seluruh proses, **temuan**, dan rekomendasi mitigasi. Laporan ini berfungsi sebagai dokumentasi hasil penelitian.

j. **Selesai**: **Penelitian** selesai setelah laporan selesai dibuat.

Proses penelitian ini dikembangkan menggunakan pendekatan deskriptif untuk mengidentifikasi kerentanan keamanan pada website cloud.co.id menggunakan OWASP ZAP. Tahap penelitian diawali dengan persiapan, dimana OWASP ZAP dikonfigurasi sesuai kebutuhan penelitian dengan menetapkan proxy, target, dan parameter pemindaian. Setelah selesai melakukan setup, peneliti menetapkan website sasaran yaitu crowdo.co.id sebagai subjek penelitian. Tingkat berikutnya adalah pemindaian pasif, yang bertujuan untuk mengumpulkan informasi awal tanpa mengirimkan permintaan jahat seperti: B. Kebijakan keamanan tajuk HTTP. Pemindaian aktif kemudian dilakukan dengan mengirimkan permintaan eksploitasi untuk mendeteksi kerentanan yang lebih kompleks seperti injeksi SQL dan skrip lintas situs (XSS) (Babate et al., 2015). Data kerentanan yang diperoleh melalui kedua jenis pemindaian mencakup rincian seperti jenis kerentanan dan lokasi. Kami kemudian menganalisisnya untuk menilai tingkat keparahan dan dampaknya terhadap keamanan situs dan data pengguna. Berdasarkan hasil analisis, dibuat rekomendasi mitigasi berupa perbaikan kode, penambahan enkripsi, dan pembaruan konfigurasi keamanan agar situs lebih tahan terhadap ancaman. Langkah terakhir adalah membuat laporan yang merangkum proses, hasil, dan rekomendasi mitigasi. Proses investigasi ini dirancang secara sistematis untuk memastikan efektivitas deteksi dan penghapusan kerentanan yang ditemukan.

## 3. HASIL DAN PEMBAHASAN

Pencarian literatur yang relevan dilakukan untuk mendukung analisis keamanan situs web berbasis OWASP ZAP. Kami memulai dengan pencarian di database digital yang tersedia di Perpustakaan Nasional Indonesia dan beberapa perpustakaan online lainnya, yang menghasilkan 150 sitasi awal. Proses penyaringan pertama dilakukan dengan membaca judul dan abstrak setiap sitasi, untuk memastikan literatur yang terpilih memiliki kesesuaian topik dengan penelitian ini. Hasilnya, terdapat 20 literatur awal yang dianggap relevan.

Selanjutnya, dari 20 literatur tersebut dilakukan penyaringan lebih lanjut dengan mempertimbangkan kesesuaian metodologi dan spesifikasi penelitian, terutama yang mengarah pada keamanan aplikasi web dengan metode OWASP ZAP. Pada tahap akhir ini, kami mengidentifikasi 3 literatur utama yang sesuai dengan tujuan dan cakupan penelitian ini. Literatur tersebut menjadi dasar dalam melakukan *systematic review* serta mendukung pemahaman lebih mendalam mengenai potensi kerentanan dan metode mitigasi yang efektif pada sistem informasi web berbasis OWASP.

Tabel-tabel ini memuat informasi penting tentang jenis pengujian, alat yang digunakan, dan hasil uji keamanan. Berikut adalah rincian tabel-tabel yang disusun:

**Tabel 1.** Identifikasi Sistem Informasi yang Diuji dan Hasil Pengujian OWASP Versi 4 (Authentication Testing)

| Literatur | Sistem Informasi / Web Server | Menggunakan Acunetix | Acunetix Threat Level |
|---|---|---|---|
| 1 | Aplikasi Pinjaman Online | Ya | Tinggi (Level 3) |
| 2 | Website www.crowdo.co.id | Tidak | - |
| 3 | Web Server | Ya | Medium (Level 2) |
| | | | |

*Sumber: Mochammad Fadilah, 2024*

Tabel ini mencakup tiga kolom yang mengidentifikasi sistem informasi atau web server yang diuji, penggunaan alat keamanan seperti Acunetix Web Vulnerability Scanner, dan hasil pengujian pada lima tahap otentikasi dari OTG-AUTHN-001 hingga OTG-AUTHN-003.

Berdasarkan Tabel 1, dapat dilihat bahwa **Aplikasi Pinjaman Online** (Elanda & Lintang Buana, 2020)menunjukkan kelemahan dalam pengujian tahap OTG-AUTHN-001, di mana data pengguna tidak sepenuhnya dienkripsi antara klien dan server. **Website www.crowdo.co.id** (Arenas et al., 2013)memiliki hasil yang lebih baik dalam tahap ini karena menggunakan koneksi HTTPS, sedangkan **Web Server** (Ullrich, 2017)memiliki ancaman menengah pada tahap OTG-AUTHN-003.

Dalam pengujian OTG-AUTHN-002 yang memeriksa kredensial default, ketiga sistem informasi lolos uji, menunjukkan bahwa pengaturan kata sandi default telah diubah. Namun, untuk tahap OTG-AUTHN-003, yang menguji mekanisme penguncian terhadap percobaan login yang salah, hanya Literatur [2] yang lolos pengujian, menandakan perlunya

pengembangan sistem yang lebih kuat untuk melindungi pengguna dari risiko *brute force attack.*

**Tabel 2.** Hasil Pengujian OWASP Versi 4 (Authentication Testing dan Authorization Testing)

| Literatur | OTG-AUTHN-006 | OTG-AUTHN-007 | OTG-AUTHN-008 | OTG-AUTHN-009 |
|---|---|---|---|---|
| [1] | Tidak Lolos | Lolos | Lolos | Lolos |
| [2] | Tidak Lolos | Lolos | - | - |
| [3] | Tidak Lolos | Lolos | Tidak Lolos | Lolos |
| | | | | |

*Sumber: Mochammad Fadilah, 2024*

Tabel ini memiliki empat kolom yang memuat hasil pengujian untuk tahap-tahap otentikasi (OTG-AUTHN-006 hingga OTG-AUTHN-09) serta tahap otorisasi (OTG-AUTHZ-001 hingga OTG-AUTHZ-004).

**Tabel 3.** Hasil Pengujian OWASP Versi 4 (Authentication Testing dan Authorization Testing)

| Literatur | OTG-AUTHZ-001 | OTG-AUTHZ-002 | OTG-AUTHZ-003 | OTG-AUTHZ-004 |
|---|---|---|---|---|
| [1] | Lolos | Tidak Lolos | Lolos | Tidak Lolos |
| [2] | Lolos | Lolos | Lolos | - |
| [3] | Lolos | Tidak Lolos | Lolos | Tidak Lolos |
| | | | | |

*Sumber: Mochammad Fadilah, 2024*

Tabel II menunjukkan bahwa pada tahap OTG-AUTHZ-001, yang menguji akses tidak sah pada root direktori, seluruh literatur menunjukkan hasil yang positif, dengan alat WFuzz dan Netsparker yang efektif mendeteksi kelemahan ini. Namun, Literatur [1] dan [3] gagal dalam tahap OTG-AUTHZ-002, yang menguji bypassing authorization schema, menunjukkan bahwa sistem mereka rentan terhadap eksploitasi.

**Tabel 4.** Hasil Pengujian OWASP Versi 4 (Session Testing)

| Literatur | OTG-SESS-001 | OTG-SESS-002 | OTG-SESS-003 | OTG-SESS-004 | OTG-SESS-005 |
|---|---|---|---|---|---|
| [1] | Tidak Lolos | Lolos | Lolos | Lolos | Tidak Lolos |
| [2] | Lolos | Lolos | Lolos | Lolos | Lolos |
| [3] | Tidak Lolos | Lolos | Lolos | Lolos | Tidak Lolos |
| | | | | | |

*Sumber: (Mochammad Fadilah, 2024)*

Tabel ini terdiri dari lima kolom yang mencakup tahap pengujian sesi dari OTG-SESS-001 hingga OTG-SESS-005, termasuk aspek pengujian manajemen sesi, atribut cookies, serta perlindungan terhadap *Cross Site Request Forgery* (CSRF).

Keterangan:

a. OTG-SESS-001: Testing for Bypassing Session Management Schema
b. OTG-SESS-002: Testing for Cookies Attributes
c. OTG-SESS-003: Testing for Session Fixation
d. OTG-SESS-004: Testing for Exposed Session Variables
e. OTG-SESS-005: Testing for Cross-Site Request Forgery (CSRF)

**Tabel 5.** Tools Pengujian OWASP Versi 4 (Authentication Testing)

| **Literatur** | **Tools OTG-AUTHN-001** | **Tools OTG-AUTHN-002** | **Tools OTG-AUTHN-003** | **Tools OTG-AUTHN-004** | **Tools OTG-AUTHN-005** |
|---|---|---|---|---|---|
| [1] | WebScarab | Brutus | Firefox | WebScarab | WebScarab |
| [2] | Firefox | Netsparker | OWASP ZAP | Netsparker | OWASP ZAP |
| [3] | WebScarab | Brutus | Firefox | WebScarab | WebScarab |

*Sumber: Mochammad Fadilah, 2024*

Tabel ini merinci alat-alat yang digunakan dalam setiap tahap uji otentikasi. Beberapa alat yang tercantum antara lain adalah WebScarab, Brutus, Mozilla Firefox, dan OWASP ZAP.

Keterangan:

a. OTG-AUTHN-001: Testing for Credentials Transported over an Encrypted Channel
b. OTG-AUTHN-002: Testing for Default Credentials
c. OTG-AUTHN-003: Testing for Weak Lockout Mechanisms
d. OTG-AUTHN-004: Testing for Bypassing Authentication Schema
e. OTG-AUTHN-005: Testing "Remember Me" Functionality

**Tabel 6.** Tools Pengujian OWASP Versi 4 (Authentication Testing, Authorization Testing, dan Session Testing)

| Literatur | Tools OTG-AUTHN-009 | Tools OTG-AUTHN-010 | Tools OTG-AUTHZ-001 | Tools OTG-AUTHZ-002 | Tols OTG-AUTHZ-003 |
|---|---|---|---|---|---|
| [1] | - | - | WFuzz | Dirb | WebScarab |
| [2] | - | - | ZAP, Netsparker | Netsparker, Firefox | ZAP, Netsparker |
| [3] | - | - | WFuzz | Dirb | WebScarab |

*Sumber: Mochammad Fadilah, 2024*

Tabel ini mencakup alat yang digunakan dalam pengujian otentikasi, otorisasi, dan sesi, termasuk Netsparker, Dirb, Google Chrome (Plugin), dan WFuzz.

Keterangan:

a. OTG-AUTHN-009: Testing for Weak Password Change/Reset Functionalities
b. OTG-AUTHN-010: Testing for Weaker Authentication in Alternative Channels
c. OTG-AUTHZ-001: Testing Directory Traversal/File Include
d. OTG-AUTHZ-002: Testing for Bypassing Authorization Schema
e. OTG-AUTHZ-003: Testing for Privilege Escalation

**Tabel 7.** Tools Pengujian OWASP Versi 4 (Session Testing)

| Literatur | Tools OTG-SESS-003 | Tools OTG-SESS-004 | Tools OTG-SESS-005 | Tools OTG-SESS-006 | Tools OTG-SESS-007 |
|---|---|---|---|---|---|
| [1] | ZAP | ZAP | OWASP CSRF Tester | Firefox | Firefox |
| [2] | ZAP, Chrome Plugin | ZAP, Chrome Plugin | Netsparker, Firefox | Firefox | Firefox |
| [3] | ZAP | ZAP | OWASP CSRF Tester | Firefox | Firefox |

*Sumber: Mochammad Fadilah, 2024*

Tabel ini menunjukkan alat yang digunakan dalam pengujian sesi, meliputi Zed Attack Proxy, OWASP CSRF Tester, dan Mozilla Firefox. Bagian ini menyajikan hasil pemindaian OWASP ZAP dan analisis kerentanan yang ditemukan.

**Tabel 8.** Atribut Prediksi Keamanan Situs

| No | Atribut | Nilai | Keterangan |
|---|---|---|---|
| [1] | Kerentanan Tinggi | 1 | Ancaman serius, berisiko tinggi untuk dieksploitasi |
| [2] | Kerentanan Sedang | 3 | Ancaman dengan dampak sedang, berpotensi mempengaruhi privasi |
| [3] | Kerentanan Rendah | 7 | Ancaman minimal namun tetap perlu diatasi |
| [4] | Informasi | 3 | Informasi tambahan untuk penguatan keamanan |

*Sumber: Mochammad Fadilah, 2024*

Berdasarkan hasil analisa, website crowdo.co.id memiliki 14 kerentanan, diantaranya satu kerentanan tingkat tinggi berupa risiko XSS dan tiga kerentanan sedang seperti kelemahan injeksi SQL dan otentikasi, 7 kerentanan tingkat rendah, dan 7 kerentanan tingkat rendah. dan 3 informasi tambahan. Risiko XSS yang teridentifikasi memungkinkan penyerang memasukkan skrip berbahaya dan mencuri data pengguna, sementara injeksi SQL dapat menyebabkan pencurian data jika tidak segera ditangani. Selain itu, terdapat kerentanan dalam manajemen sesi pengguna yang dapat dimanfaatkan oleh peretas untuk membajak sesi. Analisis ini menyoroti pentingnya terus menjaga keamanan aplikasi web, termasuk penggunaan enkripsi data sensitif, penerapan otentikasi dua faktor, Memberikan rekomendasi perbaikan seperti pembersihan kode untuk potensi kerentanan injeksi.

## 4. KESIMPULAN

Berdasarkan pemindaian menggunakan OWASP ZAP versi 2.15.0, ditemukan bahwa situs *crowdo.co.id* memiliki 14 kerentanan yang mencakup berbagai tingkat prioritas. Kerentanan tingkat tinggi menunjukkan adanya risiko yang signifikan bagi keamanan data dan privasi pengguna situs. Diperlukan langkah mitigasi oleh pengembang untuk mengatasi kerentanan ini, yang dapat berupa perbaikan kode, penambahan lapisan keamanan, atau penerapan enkripsi yang lebih kuat. Penelitian ini bertujuan memberikan pemahaman yang lebih mendalam mengenai kerentanan yang ada pada situs *crowdo.co.id* dan menawarkan solusi mitigasi yang praktis untuk mengurangi risiko serangan siber di masa depan

## DAFTAR PUSTAKA

Arenas, A. E., Podar, M., & Dalvi, P. (2013). Managing risks in crowd-funding platforms. *AIS Electronic Library (AISeL)*. http://aisel.aisnet.org/wisp2012/32

Babate, I., Musa, A., Kida, M., & Saidu, K. (2015). State of cyber security: Emerging threats landscape. *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)*, *3*(1), 113–119.

Charly, P., Diatmika, K. E., Prayoga, I. M. P., & Listartha, I. M. E. (2022). Pendeteksian keamanan website SMA Greenschool menggunakan metode OWASP dengan pengujian XSS. *Format: Jurnal Ilmiah Teknik Informatika*, *11*(1), 77. https://doi.org/10.22441/10.22441/format.2022.v11.i1.008

Copyright. (2016). iv. https://doi.org/10.1016/s0065-2458(16)30017-1

Elanda, A., & Lintang Buana, R. (2020). Analisis keamanan sistem informasi berbasis website dengan metode Open Web Application Security Project (OWASP) versi 4: Systematic review (Vol. 5, Issue 2). www.xyz.com

Longueira-Romero, Á., Engineering, A., & Program, P. (2022). Cybersecurity evaluation methodology based on metrics for industrial embedded systems.

Musa Shuaibu, B., Md Norwawi, N., Selamat, M. H., & Al-Alwani, A. (2015). Systematic review of web application security development model. *Artificial Intelligence Review*, *43*(2), 259–276. https://doi.org/10.1007/s10462-012-9375-6

Subject Index. (2016). 5, 251–257. https://doi.org/10.1016/s0065-2458(16)30021-3

Ullrich, P. (2017). The risk to breach vote privacy by unanimous voting. *Journal of Information Security and Applications*, *35*, 168–174. https://doi.org/10.1016/j.jisa.2017.07.001