JEMSI: Jurnal Ekonomi Manajemen Sistem Informasi
E-ISSN: 2686-5238
P-ISSN: 2686-4916
https://dinastirev.org/JEMSI dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jemsi.v6i3
https://creativecommons.org/licenses/by/4.0/
Received: 12 Desember 2024 | **Revised:** 23 Desember 2024 | **Accepted:** 15 Januari 2025

Analisis Kerentanan Perlindungan Data Pribadi pada Aplikasi Sistem Informasi Berbasis Web Gudang IT Inventory: Case Study PT Ecotech Resource Development

Daniel Lo[1], Muhamad Dodi Firmansyah[2]
[1]Universitas Internasional Batam, Batam, Indonesia, 2131046.daniel@uib.edu
[2]Universitas Internasional Batam, Batam, Indonesia, dodyfirmasnsyah@uib.edu

Corresponding Author: 2131046.daniel@uib.edu[1]

Abstract: *PT Ecotech Resource Development has a website-based information system application known as Web Gudang IT Inventory. This application is designed to control and manage the company's warehouse operations efficiently. This system supports company activities by utilizing information technology to provide convenience in managing inventory and logistics data. In many deeds, this digital-based management reflects the company's commitment to adapting to technological developments while increasing data security, accuracy, and transparency in supporting dynamic operational activities.*

Keyword: *IT Inventory Warehouse Web, SSL CHECKER, OWASP ZAP*

Abstrak: Perusahaan PT Ecotech Resource Development memiliki aplikasi sistem informasi berbasis website yang dikenal sebagai Web Gudang IT Inventory. Aplikasi ini dirancang untuk mengontrol dan mengelola operasional gudang perusahaan secara efisien. Sistem ini mendukung kegiatan perusahaan dengan memanfaatkan teknologi informasi untuk memberikan kemudahan dalam pengelolaan data inventarisasi dan logistik. Dalam banyak akta, pengelolaan berbasis digital ini mencerminkan komitmen perusahaan untuk beradaptasi dengan perkembangan teknologi sekaligus meningkatkan keamanan, akurasi, dan transparansi data dalam mendukung aktivitas operasional yang dinamis.

Kata Kunci: Web Gudang IT Inventory, SSL CHECKER, OWASP ZAP

PENDAHULUAN

Seiring perkembangan Teknologi Sistem Informasi, perusahaan menjadi salah satu bagian yang terkena dampaknya. Dengan ada dukungan dari Sistem Informasi dalam sistem kerja, praktikal sistem kerja dapat menjadi lebih efektif dan efisien, seperti pekerjaan yang harusnya di kerjakan 1 minggu dengan adanya Sistem Informasi dapat selesai dalam 1 hari. Dalam artian hubungan yang kuat antara Sistem Informasi dengan suatu perusahaan dapat

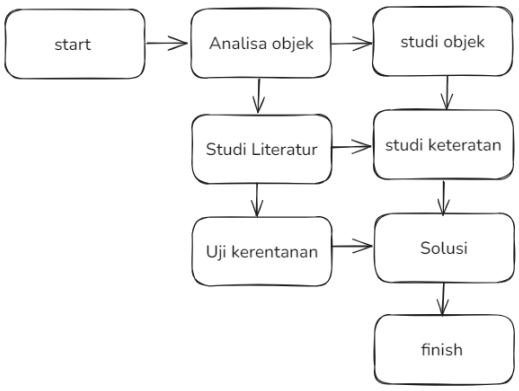
menghasilkan sistem kerja yang sangat efektif dan efisien. Web Gudang IT Inventory menjadi salah satu pengaplikasian Sistem Informasi dalam sistem kerja perusahaan.

Penerapan Web Gudang IT Inventory dalam sebuah perusahaan menggunakan media aplikasi yang berbasis web sistem informasi yang berguna untuk mengontrol sistem penyimpanan perusahaan, dari keluar dan masuknya barang, stok ketersediaan barang dalam penyimpanan, dan lainnya yang berhubungan dengan sistem kerja gudang. Dengan adanya aplikasi ini, pekerja tidak harus bekerja secara keseluruhan dengan manual. setelah pemasukan dan pengeluaran barang, pekerja hanya harus mengupdate aplikasi untuk menjadi pacuan informasi stok barang dan perusahaan PT Ecotech Resource Development telah menerapkan perkembangan teknologi sistem informasi dalam sistem kerja. PT Ecotech Resource development memiliki aplikasi berbasis web sebagai pengatur penyimpanan gudang perusahaan. Dan pada saat ini tercatat bahwa aplikasi tersebut sudah mulai jalan 30 persen dalam penerapan sistem kerja.

Keamanan terhadap data pribadi menjadi salah satu permasalahan dalam penggunaan aplikasi berbasis web dalam sistem kerja perusahaan. Penelitian ini bertujuan untuk menganalisa kerentanan perlindungan data pribadi dalam aplikasi Web Inventory IT PT Ecotech Resource Development untuk meningkatkan layanan aplikasi terhadap perusahaan menggunakan OWASP ZAP. Framework yang berguna untuk mencari kelemahan dari suatu aplikasi. Informasi dari penelitian ini akan menjadi bahan diskusi dan analisis berdasarkan Framework yang digunakan yang akan menjadi literatur yang menjadi hasil usulan keamanan terhadap data pribadi.

METODE

Dalam penelitian ini penulis menggunakan *OWASP ZAP* dan *SSL CHECKER* sebagai tools dalam melengkapi penelitian ini. *OWASP ZAP* merupakan salah satu open source application yang digunakan untuk pengujian keamanan aplikasi web secara otomatis dan manual. Penulis menggunakan aplikasi ini untuk melakukan penelitian terhadap keamanan aplikasi Web Gudang Inventory PT Ecotech. Selain aplikasi ini tidak berbayar, aplikasi ini juga sangat mudah untuk digunakan dan sudah memenuhi standar penilaian keamanan suatu aplikasi. Penulis juga menggunakan *SSL CHECKER* untuk menilai keamanan ssl aplikasi, *SSL CHECKER* merupakan alat yang digunakan untuk memeriksa sertifikat ssl suatu aplikasi sudah terpasang dengan benar. SSL merupakan protokol internet standar yang digunakan untuk server dan browser. Penggunaan *SSL CHECKER* membantu penulis untuk menganalisa salah satu keamanan pada aplikasi Web Gudang Inventory PT Ecotech. untuk penulisan dari penelitian ini, penulis menggunakan beberapa langkah atau metode untuk mengarahkan penelitian hingga sesuai dengan perumusan masalah dan tujuan dari penelitian. Berikut Langkah-langkahnya



Gambar 1. Langkah-langkah penelitian

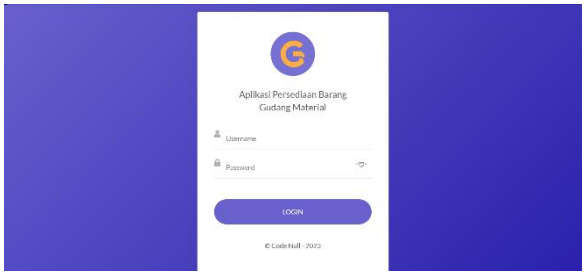
OWASP (Open Web Application Security Project) adalah organisasi nirlaba yang berfokus pada meningkatkan keamanan perangkat lunak. Dalam konteks pengujian kerentanan aplikasi, OWASP menyediakan berbagai pedoman, alat, dan sumber daya untuk membantu pengembang dan penguji aplikasi mengidentifikasi dan memperbaiki potensi masalah keamanan. Berikut adalah pemahaman terkait pengujian kerentanan aplikasi berdasarkan OWASP:

1. Keamanan Data: Melindungi data sensitif dari ancaman seperti pencurian, manipulasi, atau akses tidak sah.
2. Kepatuhan Regulasi: Memenuhi persyaratan keamanan yang diatur oleh hukum atau standar industri (misalnya, GDPR, PCI DSS).
3. Mencegah Kerugian: Menghindari kerugian finansial dan reputasi akibat serangan siber.

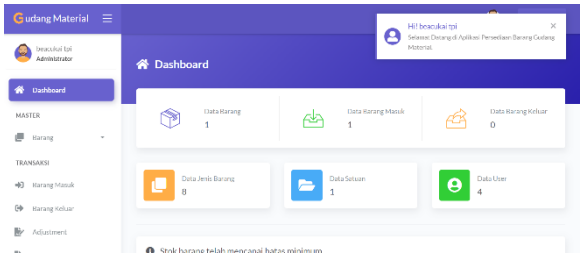
SSL Checker adalah alat yang digunakan untuk memeriksa validitas, keamanan, dan konfigurasi sertifikat SSL/TLS pada sebuah situs web. Alat ini membantu memastikan bahwa sertifikat SSL yang digunakan telah terpasang dengan benar, masih berlaku, dan menggunakan protokol serta enkripsi yang sesuai untuk melindungi data pengguna. Dengan SSL Checker, kita dapat mengidentifikasi masalah seperti sertifikat yang sudah kedaluwarsa, kesalahan rantai sertifikat, atau konfigurasi server yang tidak aman. Selain itu, alat ini juga memberikan informasi tentang detail sertifikat, seperti penerbit, algoritma enkripsi, dan masa berlaku, yang sangat penting untuk menjaga kredibilitas dan keamanan situs web Anda. Menggunakan SSL Checker secara rutin membantu memastikan situs tetap aman dan dipercaya oleh pengunjung.

Analisa objek

Dalam tahapan ini akan terdapat penjelasan yang lebih jelas. Dari aktifitas web, aplikasi, dan infrastuktur web.



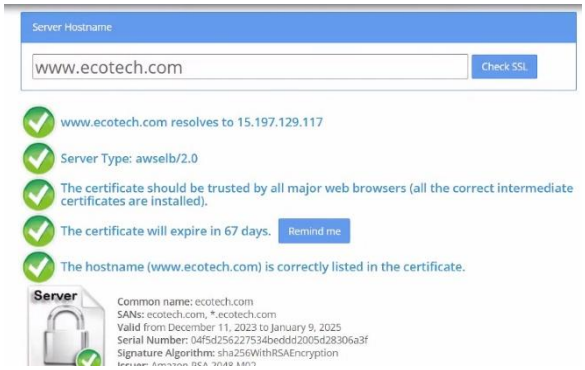
Gambar 2. Tampilan login



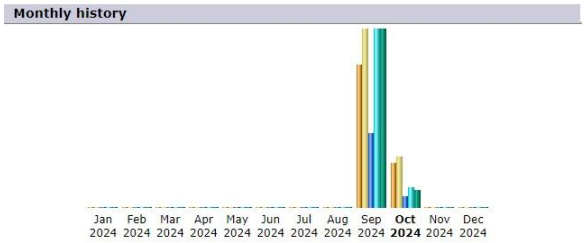
Gambar 3. Tampilan interface website

Untuk mengetahui keamanan web, penulis meninjau terlebih web yang akan dianalisis. Berdasarkan gambar 2 dan 3 ditunjukkan tampilan login dan interface dari website. Selanjutnya penulis akan mengetes keamanan web.

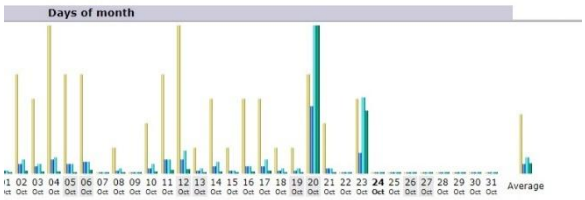
Untuk mendapatkan hasil dari tes ini, penulis menggunakan *Tools* yaitu Sslshopper untuk mendapatkan hasul tesnya.



Gambar 4. Hasil SSLSHOPPER



Gambar 5. Data grafik aktifitas perbulan



Gambar 6. Data grafik aktifitas perhari

Berdasarkan hasil analisis tercatat bahwa website Gudang Inventory IT aktif pada bulan September dan Oktober, dan intensitas yang sangat aktif pada perengahan bulan September.

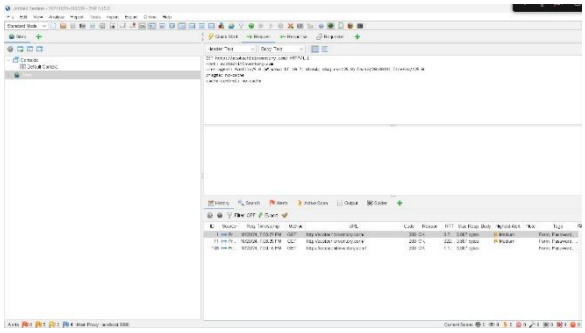
Studi literatur

Untuk memperlancar kelanjutan analisa, penulis menggunakan beberapa artikel yang bertemakan website gudang, OWASP ZAP, dan kerentanan perlindungan data pribadi. Penulis mengumpulkan 15 hingga 20 artikel yang didapati melalui google scholar (https://scholar.google.com).

Uji kerentanan

Pada tahapan ini penulis melakukan pengetesan terhadap website untuk mencari indikasi kerentanan pada website. Untuk melakukan pengetesan penulis menggunakan metode *Open Web Application Secutity Project* (OWASP).

Untuk *Tools scanning* yang digunakan, penulis menggunakan OWASP ZAP untuk melakukan pengetesan kerentanan website.



Gambar 7. Hasil scanning OWASP ZAP

Dari hasil scanning menggunakan OWASP ZAP, penulis mendapatkan bahwa website terdeteksi 11 indikasi kerentanan yang terbagi menjadi 5 level medium dan 2 level low dan 4 level internasional. level medium yang dapat menjadi perhatian adalah absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header not set, Hidden file found, Missing Anti-clickjacking Header, dan Vulnerable JS Library. Berikut terlampir detail kerentanannya:



Gambar 8. Absence of Anti-CSRF Tokens

Pada gambar 6 ditunjukan bahwa tidak terdapatnya Anti-CSRF Tokens di formulir pengiriman HTML. Sehingga kerentanan ini dapat menyebabkan pengiriman permintaan HTTP ke Lokasi target tanpa diketahui oleh pengguna.



Gambar 9. Content Security Policy (CSP) Header not set

Pada gambar 7 ditunjukan kerentanan CSP Header not set. Content Security Policy (CSP) merupakan lapisan tambahan keamanan yang berfungsi mendeteksi dan memisahkan penyerangan terhadap website, termasuk XSS dan data injection attacks. Dan pada gambar 7 menunjukan kalau bagian header untuk CSP belum di buat. Sehingga dapat menyebabkan CSP tidak aktif.



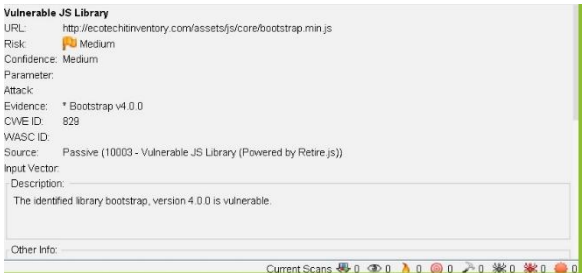
Gambar 10. Hidden file found

Pada gambar 8 terindikasi masalah Hidden File Found, yang berarti ada data yang terdeteksi yang tidak digunakan atau tersembunyi di dalam website. Yang dapat mengancam bocornya administrasi, konfigurasi, atau identifikasi dalam website.



Gambar 11. Missing Anti-clickjacking Header

Pada gambar 9 menunjukkan kerentanan yang menyebabkan respon tidak termasuk yang menunjukan ke arah fitur yang bertujuan untuk melindungi ‘ClickingJacking’ dari serangan.



Gambar 12. Vulnerable JS Library

Pada gambar 10 mengidentifikasi versi bootstrap yang digunakan pada website sangat rentan.

HASIL DAN PEMBAHASAN

Setelah menguji kerentanan dari website, penulis mencari solusi dari setiap ma-salah yang teridentifikasi dan dituangkan ke dalam jurnal untuk menjadi saran atau perubahan yang dapat dilakukan author website Setelah menguji kerentanan dari website, penulis mencari solusi dari setiap masalah yang teridentifikasi dan dituangkan ke dalam jurnal untuk menjadi saran atau perubahan yang dapat dilakukan author website.

1. Input Validation and Escape

Setiap input dari pengguna perlu divalidasi dan di-escape dengan benar sebelum ditampilkan di halaman web. Pastikan hanya karakter yang diizinkan yang dapat di-input, terutama pada input HTML, JavaScript, atau URL. Teknik ini bisa menggunakan HTML-encoding atau escape khusus seperti <, >, &, dan lainnya untuk menghindari interpretasi kode.

2. Content Security Policy (CSP)

Menggunakan Content Security Policy adalah langkah yang efektif untuk mem-batasi sumber daya mana saja yang diizinkan dimuat oleh browser. CSP memungkinkan Anda menentukan asal sumber yang diperbolehkan untuk skrip, gambar, dan konten lainnya, sehingga mengurangi risiko serangan XSS

3. Avoid Using eval and innerHTML

Sanitasi data di sisi server penting dilakukan agar data yang dikirimkan ke klien sudah bersih dari kode berbahaya. Meskipun banyak mekanisme di sisi klien, seperti JavaScript, hal ini tidak bisa diandalkan karena bisa di-bypass. Server-side validation memberikan perlindungan tambahan dari serangan XSS.

4. Server-Side Data Sanitization

Mengaktifkan SameSite Attribute pada cookie membantu mencegah serangan berbasis XSS yang mengeksploitasi cookie, terutama untuk mencegah permintaan lintas situs yang tidak sah.

5. Menggunakan Library for Input Sanitization

Library seperti DOMPurify atau Sanitize.js dapat membantu membersihkan kon-ten HTML dari karakter atau tag yang berpotensi berbahaya. Ini terutama bermanfaat jika aplikasi Anda mengizinkan pengguna memasukkan konten HTML yang lebih kompleks (frahan 2019).

6. Implement the SameSite Cookie Attribute

Mengaktifkan SameSite Attribute pada cookie membantu mencegah serangan berbasis XSS yang mengeksploitasi cookie, terutama untuk mencegah permintaan lintas situs yang tidak sah.

7. Update and Patch Frameworks dan Libraries

KESIMPULAN

Hasil dari Analisa untuk melindungi aplikasi dari kerentanan Cross-Site Scripting (XSS), diperlukan pendekatan berlapis yang mencakup validasi input, escape output, dan pembatasan sumber daya yang diizinkan. Mengimplementasikan mekanisme keamanan seperti Content Security Policy (CSP), sanitasi input baik di sisi server maupun klien, dan memilih framework yang memiliki perlindungan XSS bawaan adalah langkah penting untuk mencegah eksekusi kode berbahaya di browser pengguna. Dengan menjaga aplikasi selalu ter-update serta menerapkan praktik terbaik dalam penanganan data pengguna, risiko serangan XSS dapat diminimalisir secara signifikan, menjaga keamanan dan integritas aplikasi

Penulis yang ingin mengucapkan terima kasih atas bantuan atau dorongan dari rekan kerja, pekerjaan khusus oleh staf teknis atau dukungan keuangan dari suatu organisasi harus menyebutkannya di bagian Ucapan Terima Kasih.

REFERENSI

A. P. Kehista *et al.*, “Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review),” *J. Ilmu Manaj. Terap.*, vol. 4, no. 5, pp. 625–632, 2023, doi: https://dinastirev.org/JIMT/article/view/1541.

A. Septian *et al.*, “Analisis Tingkat Keamanan Data Pada Salah Satu Kantor Perpajakan Di Bekasi Yang Rentan Terhadap Serangan Cyber Dalam Sistem Keuangan,” *Humanit. J. Homaniora, Sos. dan Bisnis*, vol. 2, no. 7, pp. 711–718, 2024, doi: http://humanisa.my.id/index.php/hms/article/view/191.

A. W. Wardhana and H. B. Seta, “Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ,” *Inform. J. Ilmu Komput.*, vol. 17, no. 3, pp. 226–237, 2021, doi: 10.52958/iftk.v17i3.3653.

C. Vania, M. Markoni, H. Saragih, and J. Widarto, “Tinjauan yuridis terhadap perlindungan

data pribadi dari aspek pengamanan data dan keamanan siber," *J. Multidisiplin Indones.*, vol. 2, no. 3, pp. 654–666, 2023, doi: https://doi.org/10.58344/jmi.v2i3.157.

D. Wijayanto, "Analisis Tingkat Resiko Pada Website Xyz Menggunakan Metode Owasp," *Digit. Transform. Technol.*, vol. 4, no. 1, pp. 644–651, 2024, doi: 10.47709/digitech.v4i1.4485.

E. Nurelasari and D. G. Al Farabi, "ANALISIS KEAMANAN SISTEM WEBSITE MENGGUNAKAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA SIMANTEP. ID," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 3, pp. 3049–3054, 2024, doi: https://doi.org/10.36040/jati.v8i3.9314.

G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *JIPI (Jurnal Ilm. Penelit. Dan Pembelajaran Inform.*, vol. 5, no. 1, pp. 45–55, 2020, doi: https://doi.org/10.29100/jipi.v5i1.1565.

I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, pp. 160–165, 2022, doi: https://doi.org/10.37034/jidt.v4i3.236.

I. Pratama and A. A. B. A. Wiradarma, "Open source intelligence testing using the owasp version 4 framework at the information gathering stage (case study: X company)," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 7, pp. 8–12, 2019, doi: 10.5815/ijcnis.2019.07.02.

M. Yunus, "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4," *J. Ilm. Inform. Komput.*, vol. 24, no. 1, pp. 37–48, 2019, doi: http://dx.doi.org/10.35760/ik.2019.v24i1.1988.

R. Farismana and D. Pramadhana, "Perbandingan Vulnerability Assesment Menggunakan Owasp Zap dan Acunetix Pada Sistem Informasi Repositori Politeknik Negeri Indramayu," *J. Tek. Inform. dan Teknol. Inf.*, vol. 3, no. 2, pp. 26–32, 2023, doi: 10.55606/jutiti.v3i2.2853.

R. M. Fauzi, R. Hermawan, D. R. Adhy, and S. Maesaroh, "Analisis Kerentanan Keamanan Web Menggunakan Metode OWASP Dan PTES di Web Pemerintahan Desa XYZ," *Power Elektron. J. Orang Elektro*, vol. 13, no. 2, pp. 225–231, 2024, doi: http://ejournal.poltekharber.ac.id/index.php/powerelektro/article/view/6711.

S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: https://doi.org/10.33364/algoritma/v.18-1.827.

T. Ariyadi, T. L. Widodo, N. Apriyanti, and F. S. Kirana, "Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP.," *Techno. com*, vol. 22, no. 2, 2023, doi: 10.33633/tc.v22i2.7562.