TEMATICS | Technology Management and Informatics Research Journals
E-ISSN : 2798-530X
POLITEKNIK IMIGRASI POLTEKIM

PENGUJIAN KEAMANAN APLIKASI INVENTORY DENGAN METODE *OPEN WEB APPLICATION SECURITY PROJECT* (OWASP) DI KANTOR KELAS II TPI LANGSA

SECURITY TESTING OF INVENTORY APPLICATIONS WITH THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) METHOD IN CLASS II TPI LANGSA OFFICE

https://10.0.205.137/tematics.v6i2.650
Submitted: 11-02-2024 Reviewed: 11-07-2024 Published: 13-12-2024

M. Irvan
Irvan.mhd@gmail.com
Politeknik Imigrasi

Ferdyan Samuel Karunia
ferdyansamuel20@gmail.com.
Politeknik Imigrasi

Muhadzib Rezki Hilmy
ajibajib442@email.ac.id
Politeknik Imigrasi

Theresya Berlian
berliantheresya1@gmail.com
Politeknik Imigrasi

Abstract. *Inventory Application website security is becoming increasingly important amidst the increasing threat from hackers who often take data irresponsibly. Cyber attacks such as theft of personal data, financial information, and other sensitive data can have serious impacts on individuals and organizations. Therefore, anticipation is needed in knowing the vulnerabilities on application websites in general that can be exploited by hackers in carrying out fatal security breaches. OWASP ZAP is one of the most popular free security tools in the world and is actively managed by hundreds of international volunteers. It can help website developers find security vulnerabilities in our web applications when they want to develop and test our applications. ZAP (Zed Attack Proxy) is an open-source penetration testing tool specifically designed to thoroughly check the security of Web Applications. ZAP provides a powerful platform to identify and address potential security gaps in web applications. By using OWASP ZAP, OWASP ZAP users can find out the vulnerabilities on the website and are able to provide solutions to improve website security through OWASP ZAP scanning.*

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

Abstrak. *Di tengah meningkatnya ancaman siber yang sering kali dimanfaatkan oleh peretas untuk mencuri data sensitif, keamanan website Aplikasi Inventory menjadi semakin penting. Serangan siber yang menargetkan data pribadi, informasi keuangan, dan data*

sensitif lainnya dapat menyebabkan dampak serius terhadap individu maupun organisasi. Oleh karena itu, diperlukan langkah antisipatif untuk mengetahui dan mengatasi kerentanan dalam website aplikasi yang dapat dimanfaatkan peretas. OWASP ZAP (Zed Attack Proxy) adalah salah satu alat keamanan yang dirancang khusus untuk pengujian penetrasi terhadap aplikasi web. Alat ini membantu pengembang dalam menemukan dan memperbaiki celah keamanan secara efektif. Dalam penelitian ini, dilakukan pemindaian menggunakan OWASP ZAP untuk mengidentifikasi kerentanan yang ada pada Aplikasi Inventory di Kantor Imigrasi Kelas II TPI Langsa. Hasilnya menunjukkan adanya berbagai jenis kerentanan, yang kemudian dianalisis dan diberikan solusi untuk peningkatan keamanan aplikasi. Implementasi OWASP ZAP diharapkan dapat membantu memperkuat sistem keamanan aplikasi web, mengurangi risiko kebocoran data, dan menjaga integritas informasi yang disimpan.

***Keywords**:* Keamanan, Kerentanan, OWAS ZAP, Siber

1. PENDAHULUAN

Dalam era teknologi yang berkembang pesat, pengelolaan data yang efektif telah menjadi kebutuhan penting di berbagai sektor, termasuk dalam instansi pemerintahan. Kantor Imigrasi Kelas II TPI Langsa merupakan salah satu Unit Pelaksana Teknis di bawah Kementerian Hukum dan Hak Asasi Manusia yang memiliki tanggung jawab besar dalam menjalankan fungsi pelayanan publik, pengawasan, serta penegakan hukum terkait keimigrasian. Seiring dengan semakin kompleksnya tugas dan tanggung jawab, Kantor Imigrasi Kelas II TPI Langsa berupaya untuk meningkatkan efisiensi kerja melalui penerapan teknologi berbasis aplikasi web, salah satunya adalah aplikasi *Inventory* yang membantu mengelola persediaan Barang Milik Negara (BMN) secara digital (Sari & Prabowo, 2021).

Namun, di tengah pemanfaatan aplikasi web tersebut, ancaman siber menjadi tantangan signifikan. Keamanan siber adalah isu krusial dalam dunia digital yang terus berkembang, di mana aplikasi web sering kali menjadi target peretas yang ingin mengakses atau mencuri data sensitif. Serangan-serangan seperti *Malware, Sniffing*, dan *Hacking* dapat merusak integritas sistem dan mencuri data penting (Marwan & Ahmed, 2020). Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber di Indonesia terus meningkat dari tahun ke tahun, dengan berbagai jenis ancaman seperti *Malware* dan Kebocoran Informasi yang mendominasi. Aplikasi *Inventory* di Kantor Imigrasi Kelas II TPI Langsa pernah mengalami insiden peretasan yang menyebabkan hilangnya akses dan gangguan pada operasional sistem, yang menunjukkan betapa pentingnya penerapan sistem keamanan yang

kuat untuk melindungi data dan integritas sistem dari ancaman siber (Kurniawan & Putra, 2020). Oleh karena itu, diperlukan langkah mitigasi yang dapat mengidentifikasi dan mengatasi potensi kerentanan dalam aplikasi tersebut.

Namun, di tengah pemanfaatan aplikasi web tersebut, ancaman siber menjadi tantangan signifikan. Keamanan siber adalah isu krusial dalam dunia digital yang terus berkembang. Aplikasi web sering kali menjadi target peretas yang ingin mengakses atau mencuri data sensitif. Serangan-serangan seperti *Malware, Sniffing,* dan *Hacking* dapat merusak integritas sistem dan mencuri data penting. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber di Indonesia terus meningkat dari tahun ke tahun, dengan berbagai jenis ancaman seperti *Malware* dan Kebocoran Informasi yang mendominasi. Aplikasi Inventory di Kantor Imigrasi Kelas II TPI Langsa pernah mengalami insiden peretasan yang menyebabkan hilangnya akses dan gangguan pada operasional sistem. Serangan ini menunjukkan betapa pentingnya penerapan sistem keamanan yang kuat untuk melindungi data dan integritas sistem dari ancaman siber. Oleh karena itu, diperlukan langkah mitigasi yang dapat mengidentifikasi dan mengatasi potensi kerentanan dalam aplikasi tersebut.

Metode *Open Web Application Security Project* (OWASP) telah diakui sebagai salah satu pendekatan yang efektif dalam mengidentifikasi dan menutup celah keamanan pada aplikasi web. OWASP menawarkan kerangka kerja yang memungkinkan pengembang untuk mendeteksi potensi kerentanan keamanan, seperti *Injection, Broken Authentication,* dan *Sensitive Data Exposure***,** yang sering kali dieksploitasi oleh peretas (Alzahrani & Alharbi, 2020). Dengan menerapkan metode OWASP, aplikasi Inventory dapat diuji untuk mengetahui kerentanannya, dan langkah-langkah mitigasi dapat diambil untuk memastikan keamanan aplikasi tersebut. Penelitian ini bertujuan untuk melakukan pengujian keamanan pada aplikasi Inventory di Kantor Imigrasi Kelas II TPI Langsa menggunakan metode OWASP. Dengan pengujian ini, diharapkan dapat diidentifikasi celah keamanan yang ada dan diberikan rekomendasi perbaikan untuk meningkatkan keamanan aplikasi serta mendukung operasional Kantor Imigrasi yang lebih efisien dan aman.

2. METODE

A. Metode Penelitian Kualitatif

Penelitian ini menggunakan pendekatan deskriptif dalam metode penelitian kualitatif. Pengumpulan data dilakukan melalui wawancara, observasi, serta studi literatur untuk memahami aspek-aspek keamanan aplikasi berbasis web. Peneliti mengkaji

kerentanan keamanan aplikasi Inventory di Kantor Imigrasi Kelas II TPI Langsa. Teknik pengumpulan data kualitatif ini memungkinkan peneliti untuk menggali lebih dalam mengenai kerentanan-kerentanan yang mungkin terdapat pada aplikasi tersebut. Data yang diperoleh dari hasil wawancara dengan staf IT dan pegawai Kantor Imigrasi juga dianalisis untuk mengidentifikasi celah keamanan.

B. Metode Penelitian Eksperimental

Penelitian ini juga mengadopsi metode eksperimental untuk menguji keamanan aplikasi *Inventory* menggunakan pendekatan *Open Web Application Security Project* (OWASP). Metode ini dirancang untuk mengevaluasi kerentanan aplikasi web secara sistematis melalui pengujian penetrasi dengan menggunakan alat OWASP ZAP. Pengujian ini bertujuan untuk mengidentifikasi kelemahan atau potensi serangan siber yang dapat mempengaruhi kinerja aplikasi, sekaligus memberikan rekomendasi perbaikan untuk meningkatkan keamanan aplikasi.

C. Objek Penelitian

Objek penelitian ini adalah aplikasi *Inventory* yang digunakan oleh Kantor Imigrasi Kelas II TPI Langsa. Penelitian difokuskan pada evaluasi kerentanan keamanan aplikasi ini menggunakan OWASP ZAP. Pengujian dilakukan untuk mengidentifikasi celah keamanan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab.

D. Tempat dan Waktu Penelitian

Penelitian dilaksanakan di Kantor Imigrasi Kelas II TPI Langsa, yang terletak di Jl. Jenderal Ahmad Yani No. 115, Gamponng Jawa, Langsa Kota, Kota Langsa, Aceh. Proses penelitian dilakukan selama bulan Juni hingga Agustus 2023.

E. Prosedur Penelitian

Penelitian ini mengikuti langkah-langkah terstruktur dalam pengujian keamanan aplikasi web. Adapun tahapan penelitian meliputi:

Studi Literatur: Peneliti mengumpulkan referensi dari berbagai sumber terkait keamanan web dan metode OWASP, serta teori tentang alat OWASP ZAP. Tujuan tahap ini adalah untuk memahami teori yang akan diterapkan dalam pengujian keamanan aplikasi.

Analisis Kebutuhan Sistem: Peneliti menganalisis kebutuhan terkait dengan alat uji, seperti perangkat keras dan lunak yang diperlukan, termasuk spesifikasi perangkat untuk pengujian OWASP ZAP.

Alat yang digunakan:

Hardware: Laptop Asus TUF *Gaming* FX505DY.

Software: OWASP ZAP dan *browser Mozilla Firefox*.

Pengumpulan Data: Data diperoleh dari wawancara dengan staf IT dan pegawai Kantor Imigrasi terkait, serta observasi langsung terhadap aplikasi *Inventory*.

Pengujian Penetrasi: Pengujian dilakukan dengan menggunakan OWASP ZAP untuk memindai aplikasi Inventory dan mengidentifikasi kerentanan yang ditemukan selama proses pemindaian. Alat *Active Scan* digunakan untuk melakukan pemindaian aktif terhadap aplikasi.

Analisis dan Perancangan: Hasil dari pengujian penetrasi dianalisis untuk memahami tingkat kerentanan yang ditemukan dalam aplikasi. Analisis ini akan memberikan gambaran seberapa rentan aplikasi *Inventory* terhadap serangan siber dan memberikan langkah mitigasi yang diperlukan.

Pelaporan dan Kesimpulan: Setelah hasil analisis selesai, peneliti menyusun laporan penelitian yang berisi temuan kerentanan dan rekomendasi perbaikan. Laporan ini juga mencakup kesimpulan mengenai tingkat keamanan aplikasi *Inventory* dan langkah-langkah yang diperlukan untuk memperbaikinya.

3. RISET

Penelitian ini menggunakan OWASP ZAP (*Zed Attack Proxy*) untuk menguji keamanan Aplikasi Inventory yang digunakan di Kantor Imigrasi Kelas II TPI Langsa. Pengujian dilakukan dengan melakukan observasi dan wawancara kepada beberapa pejabat Kantor Imigrasi serta penggunaan OWASP ZAP untuk menemukan kerentanan dalam aplikasi.

3.1 Konfigurasi OWASP dan Persiapan Pengujian

OWASP ZAP digunakan untuk memindai kerentanan aplikasi berbasis web melalui proses yang mencakup *Spidering, Ajax Spider*, dan *Active Scanning*. Proses ini bertujuan untuk menemukan URL, parameter, dan endpoint yang ada di dalam aplikasi, serta melakukan simulasi serangan untuk mengidentifikasi potensi kerentanan keamanan.

3.2 Hasil Pengujian OWASP pada Aplikasi Inventory

Spidering dan *Ajax Spider*

Pengujian awal dilakukan dengan *Spidering* dan *Ajax Spider*, yang menemukan beberapa URL, parameter, dan endpoint yang berpotensi

rentan terhadap serangan. Tabel hasil pemindaian menunjukkan sejumlah URL yang *out of scope* dan beberapa *endpoint* yang terdeteksi.

Active Scanning

Tahap Active Scanning dilakukan setelah proses crawling selesai, dengan tujuan mensimulasikan serangan langsung terhadap aplikasi. Pengujian ini berhasil mengidentifikasi 21 kerentanan, yang terbagi menjadi 2 kerentanan tingkat tinggi, 8 kerentanan tingkat sedang, dan 11 kerentanan tingkat rendah. Beberapa kerentanan yang ditemukan termasuk:

1. *Cross-Site Scripting* (XSS) (*Reflected*): Kerentanan ini memungkinkan penyerang menyuntikkan skrip berbahaya yang dieksekusi dalam konteks browser pengguna, berpotensi mencuri data atau mengubah konten situs.
2. *Source Code Disclosure* (CVE-2012-1823): Ditemukan kelemahan dalam konfigurasi server yang memungkinkan eksekusi perintah sistem operasi di server web.
3. *Absence of Anti-CSRF Tokens*: Aplikasi tidak menggunakan token anti-CSRF, yang membuatnya rentan terhadap serangan *Cross-Site Request Forgery* (CSRF).
4. *Application Error Disclosure*: Informasi sensitif seperti versi server dan detail kesalahan sistem tidak disembunyikan, yang berpotensi memberikan informasi penting kepada penyerang.
5. *Content Security Policy* (CSP) *Header Not Set*: Tidak adanya kebijakan *Content Security Policy* (CSP) yang memungkinkan berbagai jenis serangan seperti Cross-Site Scripting (XSS) dan Clickjacking.
6. *Directory Browsing*: Server mengizinkan pengguna untuk melihat struktur direktori, yang dapat memaparkan file sensitif dan konfigurasi.

3.3 Analisis Kerentanan

Kerentanan *Cross-Site Scripting* (XSS) ditemukan sebagai salah satu yang paling kritis, di mana skrip berbahaya dapat disuntikkan melalui URL atau input lainnya. Kerentanan ini berpotensi menyebabkan pencurian data pengguna atau pembajakan sesi. Kerentanan *Source Code Disclosure* memungkinkan akses ke kode sumber yang tidak diinginkan, berpotensi mengekspos sistem kepada serangan yang lebih canggih seperti *Remote Code Execution* (RCE). Selain itu, ditemukan pula *Absence of Anti-CSRF Tokens*, yang membuat aplikasi rentan terhadap serangan otomatis yang dapat memanipulasi operasi penting seperti pengiriman formulir tanpa sepengetahuan pengguna. Kerentanan lain seperti *Application Error Disclosure* dan *Directory Browsing* juga memperlihatkan bahwa aplikasi belum memiliki pengaturan keamanan yang optimal, di mana informasi sensitif seperti struktur direktori dan pesan kesalahan yang rinci masih dapat diakses secara publik.

3.4 Hasil Wawancara Pengguna Aplikasi

Dari wawancara dengan beberapa pejabat Kantor Imigrasi, ditemukan bahwa *Aplikasi Inventory* sangat membantu dalam pengelolaan Barang Milik Negara (BMN), terutama dalam pencatatan stok barang masuk dan keluar. Namun, penerapannya secara offline memiliki beberapa tantangan, termasuk keterbatasan akses untuk setiap seksi di kantor, yang menghambat efisiensi. Beberapa pejabat seperti Kepala Urusan Umum dan Admin Website menyatakan bahwa aplikasi ini dapat lebih efektif jika dijalankan secara online, memungkinkan setiap seksi untuk mengakses dan memantau stok barang secara real-time, yang akan meningkatkan transparansi dan efektivitas operasional.

3.5 Implikasi dan Saran

Berdasarkan temuan tersebut, penting untuk melakukan langkah-langkah mitigasi terhadap kerentanan yang ditemukan. Beberapa rekomendasi utama meliputi:

1. Penerapan Anti-CSRF Tokens untuk melindungi aplikasi dari serangan CSRF.
2. Perbaikan kebijakan *Content Security Policy* (CSP) untuk membatasi sumber daya yang dapat dimuat oleh aplikasi, mencegah serangan *Cross-Site Scripting* (XSS).
3. Penonaktifan *Directory Browsing* dan peningkatan *error handling* untuk mencegah eksposur informasi sensitif kepada pengguna.

Penggunaan OWASP ZAP telah terbukti efektif dalam mendeteksi kerentanan, namun hasil ini menunjukkan bahwa pengujian keamanan harus dilakukan secara berkala untuk memastikan aplikasi tetap aman dari ancaman baru. Dengan mengadopsi saran ini, Kantor Imigrasi diharapkan dapat meningkatkan keamanan Aplikasi Inventory serta mendukung efisiensi operasional secara keseluruhan.

4. KESIMPULAN

Dengan Menyoroti urgensi peningkatan keamanan siber dalam operasional Kantor Imigrasi Kelas II TPI Langsa. Sebagai unit pelaksana teknis di bawah Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham), Kantor Imigrasi Langsa memiliki tanggung jawab dalam pengawasan serta pelayanan publik keimigrasian. Untuk memenuhi kebutuhan operasional yang efektif, kantor ini telah mengadopsi aplikasi Inventory berbasis web, yang membantu mengelola Barang Milik Negara (BMN) secara digital. Namun, di tengah pemanfaatan teknologi ini, ancaman keamanan siber menjadi risiko signifikan, mengingat data dan sistem aplikasi pemerintahan sering menjadi target serangan peretas. Dengan menggunakan metode *Open Web Application Security Project* (OWASP), penelitian ini menguji aplikasi Inventory untuk mengidentifikasi kerentanan yang mungkin dieksploitasi oleh pihak tidak bertanggung jawab. Metode OWASP dipilih karena kerangka kerjanya yang

komprehensif dalam mendeteksi celah keamanan pada aplikasi web. Hasil pengujian menunjukkan bahwa aplikasi Inventory memiliki beberapa kerentanan penting yang perlu diatasi, di antaranya adalah *Cross-Site Scripting* (XSS), *Source Code Disclosure*, dan kurangnya Anti-CSRF Tokens.

Kerentanan XSS, misalnya, memungkinkan peretas untuk menyuntikkan skrip berbahaya yang dapat merusak atau mengubah data aplikasi. Hal ini berpotensi mengganggu keamanan dan kredibilitas sistem, serta mengancam privasi data pengguna. Selain itu, ditemukan juga kerentanan *Source Code Disclosure*, yang membuka akses ke kode sumber aplikasi dan memberi peluang bagi peretas untuk mengeksploitasi kelemahan sistem. Ini dapat mengarah pada serangan yang lebih serius seperti *Remote Code Execution* (RCE), di mana peretas dapat mengeksekusi perintah pada server dari jarak jauh, membahayakan integritas aplikasi secara keseluruhan. Absennya Anti-CSRF Tokens dalam aplikasi ini juga mengindikasikan kelemahan signifikan. CSRF (*Cross-Site Request Forgery*) adalah serangan di mana penyerang dapat membuat pengguna yang telah login mengirim permintaan yang tidak diinginkan ke server. Dengan tidak adanya token Anti-CSRF, aplikasi rentan terhadap serangan yang memungkinkan peretas memanipulasi data pengguna tanpa disadari.

Di samping kerentanan tersebut, masalah lain yang ditemukan adalah adanya *Directory Browsing* yang memungkinkan pengguna mengakses struktur direktori server secara publik, serta *Content Security Policy* (CSP) yang belum diterapkan*. Directory Browsing* dapat mengekspos file sensitif yang seharusnya tidak bisa diakses oleh pengguna biasa, sedangkan tanpa CSP, aplikasi rentan terhadap berbagai ancaman, termasuk serangan XSS dan *Clickjacking*, yang bisa mengakibatkan manipulasi tampilan atau konten yang dapat mengelabui pengguna. Wawancara dengan beberapa pejabat di Kantor Imigrasi Kelas II TPI Langsa memperkuat temuan tersebut. Mereka mengakui bahwa aplikasi Inventory telah meningkatkan efisiensi pengelolaan stok BMN, namun penerapan aplikasi secara *offline* dan keterbatasan akses antarseksi juga menjadi tantangan tersendiri. Penerapan sistem berbasis web yang dapat diakses oleh seluruh divisi secara *real-time* dianggap akan membantu meningkatkan transparansi dan efektivitas pengelolaan barang. Dalam konteks ini, penguatan keamanan menjadi aspek penting untuk mendukung tujuan tersebut.

Sebagai rekomendasi utama, penelitian ini menyarankan langkah-langkah mitigasi sebagai berikut: pertama, penerapan Anti-CSRF Tokens untuk melindungi aplikasi dari serangan CSRF; kedua, penyusunan kebijakan *Content Security Policy* (CSP) yang efektif untuk membatasi sumber daya yang dapat dimuat oleh aplikasi, yang akan mengurangi risiko XSS dan *Clickjacking*; ketiga, menonaktifkan *Directory Browsing* dan memperbaiki pengaturan penanganan error untuk menghindari paparan informasi sensitif kepada pengguna yang tidak berhak. Pengujian keamanan aplikasi menggunakan OWASP ZAP terbukti efektif dalam mengidentifikasi berbagai jenis kerentanan keamanan. Namun, temuan ini menunjukkan bahwa pengujian keamanan tidak hanya cukup dilakukan

sekali saja. Penting bagi Kantor Imigrasi Kelas II TPI Langsa untuk menjalankan pengujian berkala sebagai bagian dari prosedur standar untuk mempertahankan sistem yang aman dan terlindungi dari ancaman siber baru yang terus berkembang. Langkah-langkah mitigasi dan pengujian berkala ini akan mendukung aplikasi *Inventory* dalam memberikan kontribusi optimal terhadap efisiensi dan efektivitas operasional Kantor Imigrasi, sekaligus memastikan keamanan dan integritas data secara keseluruhan.

Dengan menerapkan rekomendasi ini, diharapkan aplikasi *Inventory* di Kantor Imigrasi Kelas II TPI Langsa tidak hanya meningkatkan efisiensi pengelolaan BMN, tetapi juga terlindung dari ancaman siber yang terus berkembang. Penerapan keamanan siber yang kuat akan memberikan manfaat jangka panjang dalam mempertahankan kepercayaan publik terhadap layanan keimigrasian dan mendukung kinerja pemerintahan yang lebih aman dan transparan.

5. HASIL

5.1 Hasil Pemindaian Awal dengan OWASP ZAP

Tahap awal dalam pengujian keamanan aplikasi *Inventory* di Kantor Imigrasi Kelas II TPI Langsa menggunakan OWASP ZAP mengungkapkan banyaknya potensi kerentanan keamanan. Proses pemindaian ini dilakukan dengan teknik spidering dan pemindaian manual, yang memungkinkan alat untuk menjelajahi seluruh elemen aplikasi, termasuk halaman, endpoint, dan parameter input yang mungkin menjadi target serangan. Spidering secara otomatis memetakan struktur aplikasi dan mendeteksi semua tautan dan halaman yang dapat diakses, sementara pemindaian manual dilakukan untuk memastikan hasil yang lebih menyeluruh dan menganalisis aspek-aspek spesifik yang rentan terhadap ancaman siber. Selama pemindaian, OWASP ZAP menemukan beberapa endpoint yang memiliki pengaturan akses yang lemah dan tidak dilindungi dengan baik. Endpoint seperti ini sangat rentan karena dapat diakses oleh pihak yang tidak berwenang, yang dapat menyebabkan kebocoran data atau bahkan manipulasi langsung terhadap data dalam aplikasi. Misalnya, input pengguna yang tidak memiliki validasi atau sanitasi ketat memungkinkan penyerang menyisipkan skrip berbahaya (*cross-site scripting*) atau memanfaatkan parameter input untuk melakukan injeksi SQL yang dapat mengambil, memodifikasi, atau menghapus data sensitif dalam aplikasi.

Hasil pemindaian awal menunjukkan bahwa aplikasi Inventory tidak memiliki kontrol akses dan validasi input yang memadai, yang seharusnya berfungsi sebagai lapisan keamanan dasar. Ketiadaan validasi ini memungkinkan manipulasi data input, yang dapat digunakan untuk menyusupkan serangan injection atau mengakses data sensitif. Identifikasi kerentanan pada tahap ini juga menunjukkan bahwa data yang dikirimkan melalui aplikasi tidak dilindungi dengan enkripsi yang memadai. Hal ini menimbulkan risiko bahwa data penting, seperti informasi

inventaris Barang Milik Negara (BMN), dapat diakses oleh pihak ketiga yang tidak memiliki otorisasi, yang meningkatkan potensi pencurian data atau kebocoran informasi.Temuan ini mempertegas perlunya penerapan sistem enkripsi *end-to-end* serta validasi input pada setiap *endpoint*. Dalam aplikasi web yang rentan terhadap serangan eksternal, pengaturan enkripsi harus diterapkan untuk memastikan bahwa data yang dikirim dan diterima hanya dapat diakses oleh pihak yang berwenang. Selain itu, kontrol akses yang ketat harus diterapkan untuk membatasi akses ke *endpoint* tertentu hanya bagi pengguna yang terautentikasi dan berhak. Dengan demikian, aplikasi Inventory dapat terlindungi dari serangan pihak luar yang mungkin berupaya mengakses atau memodifikasi data sensitif di dalamnya.

Pemindaian awal ini memberikan gambaran yang jelas mengenai risiko yang dihadapi oleh aplikasi, dan menyoroti pentingnya pengetatan keamanan sebagai langkah mitigasi awal. Kebutuhan akan validasi input yang ketat dan perlindungan enkripsi data menjadi rekomendasi utama, yang jika diterapkan, dapat membantu mencegah potensi penyalahgunaan oleh pihak tidak bertanggung jawab dan menjaga integritas data di dalam aplikasi Inventory Kantor Imigrasi Kelas II TPI Langsa.

5.2 Identifikasi Kerentanan: Tingkat Tinggi hingga Rendah

Proses *Active Scanning* pada aplikasi Inventory Kantor Imigrasi Kelas II TPI Langsa menggunakan OWASP ZAP menghasilkan identifikasi 21 kerentanan yang tersebar dalam beberapa tingkat keparahan, yakni tingkat tinggi, sedang, dan rendah. Setiap tingkat kerentanan memberikan potensi ancaman yang berbeda terhadap keamanan dan stabilitas aplikasi. Dari hasil pemindaian ini, ditemukan dua kerentanan tingkat tinggi, delapan kerentanan tingkat menengah, dan sebelas kerentanan tingkat rendah, yang semuanya berpotensi menjadi pintu masuk bagi serangan siber jika tidak segera diatasi. Kerentanan tingkat tinggi yang ditemukan meliputi *Cross-Site Scripting* (XSS) dan *Source Code Disclosure*. Kerentanan XSS memungkinkan penyerang menyisipkan skrip berbahaya ke dalam halaman *web*, yang dapat dijalankan pada browser pengguna. Dengan memanfaatkan celah XSS ini, penyerang dapat memanipulasi tampilan aplikasi, mengubah data yang ditampilkan, atau bahkan mencuri data sensitif pengguna. Sebagai contoh, data login atau informasi pribadi pengguna dapat dicuri melalui XSS ini, yang kemudian dapat digunakan untuk tujuan yang tidak sah. Selain XSS, kerentanan *Source Code Disclosure* juga ditemukan, di mana kode sumber aplikasi dapat diakses tanpa izin. Akses tak sah ke kode sumber memberikan peluang bagi penyerang untuk menganalisis kelemahan lainnya dalam sistem dan menyusun serangan lebih lanjut, seperti injeksi kode atau eksekusi jarak jauh.

Di tingkat menengah, kerentanan utama yang ditemukan adalah ketiadaan Anti-CSRF Token yang memungkinkan serangan *Cross-Site Request Forgery* (CSRF). Tanpa token Anti-CSRF, aplikasi Inventory rentan terhadap serangan yang memungkinkan penyerang membuat

permintaan yang sah atas nama pengguna yang telah login. Hal ini memungkinkan manipulasi data aplikasi secara otomatis tanpa sepengetahuan pengguna, yang berpotensi merusak integritas data atau mengubah pengaturan penting. Selain itu, *Directory Browsing dan Content Security Policy* (CSP) yang tidak diatur dengan baik ditemukan di aplikasi. *Directory Browsing* memungkinkan penyerang mengakses struktur direktori aplikasi dan melihat file yang mungkin berisi informasi sensitif atau konfigurasi penting. Sementara itu, tidak adanya CSP membuka celah bagi serangan Clickjacking dan XSS, yang dapat membuat aplikasi terekspos terhadap manipulasi konten atau tampilan yang bisa mengelabui pengguna.

Kerentanan tingkat rendah yang terdeteksi mencakup beberapa masalah konfigurasi dasar, seperti enkripsi yang belum optimal dan pengecekan yang tidak menyeluruh pada input pengguna. Meskipun dampak dari kerentanan ini tidak seberbahaya kerentanan di tingkat tinggi dan menengah, kerentanan ini dapat menjadi titik awal yang memudahkan penyerang untuk menargetkan eksploitasi lebih lanjut pada aplikasi. Misalnya, penyerang mungkin mencoba berbagai metode serangan berbasis eksploitasi input yang longgar atau kurangnya enkripsi untuk mengakses data dalam aplikasi.

Temuan dari *Active Scanning* ini menunjukkan adanya kebutuhan mendesak untuk menerapkan kebijakan keamanan tambahan pada aplikasi Inventory. Beberapa rekomendasi yang dapat diterapkan untuk memitigasi risiko ini meliputi:

1. Penerapan Anti-CSRF Token di seluruh titik input aplikasi untuk melindungi dari serangan CSRF.
2. Penggunaan *Content Security Policy* (CSP) untuk mengontrol konten yang dapat dieksekusi oleh aplikasi, mencegah risiko XSS dan *Clickjacking*.
3. Penonaktifan *Directory Browsing* untuk membatasi akses ke struktur direktori yang sensitif dan hanya memberikan izin kepada pengguna yang berwenang.
4. Validasi Input dan Penerapan Enkripsi Data yang Memadai agar aplikasi terlindungi dari eksploitasi dasar.

Secara keseluruhan, hasil dari *Active Scanning* menunjukkan bahwa aplikasi Inventory di Kantor Imigrasi Kelas II TPI Langsa memerlukan peningkatan sistem keamanan agar terlindungi dari eksploitasi. Implementasi kebijakan keamanan ini diharapkan dapat meningkatkan integritas dan keandalan aplikasi, sekaligus menjaga data sensitif tetap aman dari ancaman pihak luar yang berpotensi mengakses atau merusak sistem aplikasi.

5.3 Analisis Kerentanan *Cross-Site Scripting* (XSS)

Kerentanan *Cross-Site Scripting* (XSS) yang teridentifikasi dalam aplikasi Inventory merupakan ancaman serius yang berpotensi mengakibatkan kerugian signifikan bagi pengguna dan organisasi. XSS

terjadi ketika penyerang berhasil menyisipkan skrip berbahaya ke dalam halaman web yang kemudian diakses oleh pengguna lain, menciptakan peluang bagi penyerang untuk mencuri data sensitif seperti *cookie*, kredensial, dan informasi pribadi lainnya. Dalam konteks aplikasi Inventory, kerentanan ini terdeteksi pada beberapa halaman input, khususnya di area yang menerima data dari pengguna tanpa menerapkan validasi atau sanitasi yang memadai. Ketidakhadiran mekanisme validasi input memungkinkan skrip jahat untuk dieksekusi dalam konteks *browser* pengguna yang terinfeksi. Hal ini tidak hanya membahayakan data pengguna, tetapi juga dapat memanipulasi tampilan aplikasi, menyebabkan pengguna melihat informasi yang salah atau bahkan mengalihkan mereka ke situs phishing. Misalnya, seorang penyerang dapat menyisipkan skrip yang mencuri sesi pengguna, sehingga mendapatkan akses tanpa izin ke akun dan data pengguna yang lebih lanjut.

Untuk mengatasi kerentanan XSS, langkah-langkah proaktif harus diambil. Implementasi validasi dan sanitasi input yang ketat adalah kunci untuk mencegah eksekusi skrip berbahaya. Setiap data yang diterima dari pengguna harus diperiksa dan dibersihkan untuk memastikan bahwa hanya input yang aman yang diproses oleh aplikasi. Selain itu, penerapan kebijakan *Content Security Policy* (CSP) juga sangat disarankan. CSP adalah mekanisme yang memungkinkan pengembang untuk menentukan sumber daya yang dapat dimuat oleh aplikasi, membatasi eksekusi skrip yang tidak sah dan meminimalkan risiko serangan XSS.

Dengan menggabungkan pendekatan validasi dan sanitasi input yang efektif serta penerapan kebijakan CSP, aplikasi Inventory dapat secara signifikan meningkatkan postur keamanannya dan melindungi pengguna dari serangan berbasis skrip yang merugikan. Upaya ini tidak hanya berfungsi untuk menjaga integritas data, tetapi juga untuk membangun kepercayaan pengguna terhadap sistem dan layanan yang disediakan oleh Kantor Imigrasi Kelas II TPI Langsa.

5.4 Kerentanan Source Code Disclosure

Kerentanan *Source Code Disclosure* adalah salah satu kerentanan kritis yang teridentifikasi pada aplikasi Inventory di Kantor Imigrasi Kelas II TPI Langsa. Kerentanan ini terjadi ketika penyerang dapat mengakses kode sumber aplikasi melalui endpoint tertentu yang tidak dilindungi dengan baik. Akses ini memberikan penyerang kesempatan untuk menganalisis struktur dan logika aplikasi, yang memungkinkan mereka untuk mengidentifikasi potensi celah keamanan atau kelemahan lain yang dapat dieksploitasi untuk mengambil alih kontrol aplikasi atau mengubah perilaku sistem.

Misalnya, jika penyerang mengetahui fungsi-fungsi spesifik dalam kode yang mengelola otentikasi pengguna, mereka dapat melakukan serangan yang lebih terarah, seperti injeksi SQL atau manipulasi sesi. Selain itu, dengan akses ke kode sumber, penyerang dapat mempelajari teknik-teknik pemrograman yang digunakan, serta ketergantungan dan pustaka eksternal yang dapat menjadi target serangan lebih lanjut. Hal ini

bukan hanya berisiko bagi data sensitif yang dikelola oleh aplikasi, tetapi juga dapat merusak reputasi institusi yang mengelola aplikasi tersebut.

Untuk mitigasi, langkah-langkah yang perlu diambil meliputi penutupan akses ke direktori sensitif dan penerapan kebijakan otentikasi yang lebih ketat di tingkat server. Ini termasuk membatasi akses hanya kepada pengguna yang berwenang serta menerapkan kontrol akses berbasis peran (RBAC) untuk memastikan bahwa hanya individu dengan otorisasi yang tepat yang dapat mengakses kode sumber atau direktori kritis lainnya. Selain itu, pengkodean yang aman dan pemantauan rutin terhadap potensi kebocoran informasi harus diimplementasikan sebagai bagian dari strategi keamanan menyeluruh. Dengan melindungi kode sumber secara efektif, aplikasi dapat terhindar dari eksploitasi yang tidak diinginkan, sekaligus memastikan integritas dan kelangsungan operasional tetap terjaga.

5.5 Kesimpulan dan Rekomendasi Pengamanan

Temuan penelitian ini menegaskan pentingnya penguatan aspek keamanan siber pada aplikasi Inventory yang digunakan oleh Kantor Imigrasi Kelas II TPI Langsa. Pengujian yang dilakukan menggunakan OWASP ZAP mengidentifikasi beberapa kerentanan serius yang dapat dimanfaatkan oleh pihak luar untuk melakukan serangan siber, seperti *Cross-Site Scripting* (XSS) dan pengungkapan kode sumber. Kerentanan XSS, khususnya, memungkinkan penyerang untuk menyuntikkan skrip berbahaya yang dapat merusak integritas data dan merugikan pengguna aplikasi. Sementara itu, pengungkapan kode sumber dapat memberikan informasi berharga bagi penyerang untuk merancang strategi eksploitasi lebih lanjut.

Rekomendasi utama dari penelitian ini adalah penerapan token Anti-CSRF, yang berfungsi untuk melindungi aplikasi dari serangan *Cross-Site Request Forgery*. Tanpa langkah ini, aplikasi akan rentan terhadap aksi yang dapat dilakukan penyerang dengan memanfaatkan sesi pengguna yang sah. Selain itu, pengembangan dan penerapan kebijakan *Content Security Policy* (CSP) sangat krusial untuk membatasi eksekusi skrip yang tidak sah. CSP yang baik akan meminimalkan kemungkinan penyuntikan skrip berbahaya dengan mengatur sumber yang diizinkan untuk memuat konten pada halaman *web*. Hal ini akan membantu menjaga keamanan aplikasi dari ancaman eksternal yang dapat merusak atau mengakses data sensitif. Selain langkah-langkah di atas, pengaturan ulang kontrol akses pada aplikasi juga diperlukan untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses informasi dan fungsionalitas tertentu. Penetapan level akses yang jelas akan mengurangi risiko manipulasi data dan serangan internal. Pengujian berkala terhadap aplikasi sangat dianjurkan, tidak hanya untuk mengidentifikasi kerentanan baru, tetapi juga untuk mengevaluasi efektivitas langkah-langkah keamanan yang sudah diterapkan. Proses pengujian ini harus dilakukan secara rutin, seiring dengan perkembangan teknologi dan metode serangan yang terus berubah.

Implementasi langkah-langkah keamanan ini diharapkan dapat

mendukung efektivitas aplikasi Inventory sebagai platform yang tidak hanya efisien, tetapi juga aman dalam pengelolaan Barang Milik Negara (BMN). Keamanan siber yang kuat akan berkontribusi pada pelayanan imigrasi yang lebih andal dan terpercaya, memberikan keyakinan kepada publik bahwa data dan informasi yang dikelola oleh kantor imigrasi terlindungi dengan baik dari ancaman yang ada. Dengan demikian, langkah-langkah mitigasi yang tepat dan sistematis tidak hanya akan meningkatkan integritas aplikasi, tetapi juga mendorong kepercayaan masyarakat terhadap pelayanan imigrasi secara keseluruhan. Kesimpulannya, peningkatan keamanan siber harus menjadi prioritas utama untuk memastikan bahwa aplikasi Inventory dapat beroperasi dengan maksimal dan memenuhi tuntutan modernisasi dalam pengelolaan data imigrasi.

5.5 Analisis SWOT

1. *Strengths* (Kekuatan)

Aplikasi Inventory yang digunakan oleh Kantor Imigrasi Kelas II TPI Langsa memiliki beberapa kekuatan yang dapat dimanfaatkan untuk meningkatkan efektivitas operasional. Pertama, aplikasi ini telah dirancang untuk memfasilitasi pengelolaan Barang Milik Negara (BMN) secara digital, yang mengurangi kebutuhan akan pencatatan manual dan meningkatkan akurasi data. Dengan sistem berbasis web, pengguna dapat mengakses informasi terkini tentang BMN dari berbagai lokasi, sehingga memudahkan pengawasan dan pengelolaan aset. Hal ini penting, mengingat Kantor Imigrasi memiliki tanggung jawab untuk menjaga integritas dan transparansi dalam pengelolaan barang milik negara.

Kedua, penerapan metode *Open Web Application Security Project* (OWASP) dalam pengujian keamanan aplikasi menunjukkan komitmen kantor terhadap perlindungan data. Metode ini dikenal luas dalam industri TI karena kerangka kerjanya yang komprehensif dalam mendeteksi dan menganalisis kerentanan aplikasi web. Dengan mengadopsi metode ini, Kantor Imigrasi Kelas II TPI Langsa tidak hanya meningkatkan keamanan aplikasi, tetapi juga memberikan jaminan kepada publik bahwa mereka serius dalam melindungi informasi sensitif.

Ketiga, keberadaan tim teknis yang terlatih dan berpengalaman merupakan aset berharga bagi kantor. Tim ini mampu mengidentifikasi masalah keamanan dengan cepat dan menerapkan solusi yang efektif. Dengan pengetahuan yang mendalam tentang aplikasi dan infrastruktur TI, tim ini dapat berperan aktif dalam memastikan bahwa aplikasi Inventory berfungsi dengan baik tanpa ada gangguan yang disebabkan oleh serangan siber. Pelatihan dan peningkatan keterampilan secara berkala bagi tim ini juga dapat meningkatkan kemampuan mereka dalam menghadapi ancaman keamanan yang terus berkembang.

2. *Weaknesses* (Kelemahan)

Meski aplikasi Inventory memiliki beberapa kekuatan, terdapat kelemahan yang perlu diperhatikan. Salah satu kelemahan paling

mencolok adalah adanya kerentanan keamanan yang ditemukan selama pengujian, seperti *Cross-Site Scripting* (XSS) dan pengungkapan kode sumber. Kerentanan XSS memungkinkan penyerang untuk menyuntikkan skrip berbahaya ke dalam halaman *web* yang diakses oleh pengguna, sehingga dapat mengakses data sensitif atau melakukan tindakan yang merugikan. Sedangkan kerentanan pengungkapan kode sumber membuka peluang bagi penyerang untuk menganalisis kode aplikasi, mencari kelemahan lebih lanjut, dan melancarkan serangan yang lebih serius.

Kelemahan lain yang harus diperhatikan adalah ketiadaan kontrol akses yang memadai pada aplikasi. Tanpa kontrol akses yang ketat, pengguna yang tidak berwenang dapat mengakses informasi sensitif atau bahkan mengubah data yang ada dalam aplikasi. Ketiadaan validasi input juga menjadi masalah, di mana data yang diterima dari pengguna tidak diperiksa dengan baik, sehingga memungkinkan potensi serangan seperti injeksi SQL. Hal ini menunjukkan bahwa aplikasi belum sepenuhnya siap untuk menghadapi ancaman keamanan yang ada.

Selain itu, kurangnya pemahaman tentang praktik keamanan siber di kalangan staf juga menjadi kelemahan. Banyak pegawai mungkin tidak menyadari risiko yang terkait dengan penggunaan aplikasi berbasis *web*, serta pentingnya menjaga keamanan data. Hal ini dapat menghambat implementasi langkah-langkah mitigasi yang diperlukan dan meningkatkan potensi risiko. Pendidikan dan pelatihan tentang keamanan siber bagi seluruh staf perlu ditingkatkan agar mereka dapat lebih memahami dan menghadapi tantangan yang ada.

3. *Opportunities* (Peluang)

Di tengah tantangan yang ada, terdapat sejumlah peluang yang dapat dimanfaatkan oleh Kantor Imigrasi Kelas II TPI Langsa untuk meningkatkan keamanan aplikasi Inventory. Salah satu peluang terbesar adalah meningkatnya kesadaran akan pentingnya keamanan siber di lingkungan pemerintahan. Dengan adanya regulasi yang lebih ketat terkait perlindungan data, kantor imigrasi dapat menjadikan keamanan siber sebagai prioritas utama dalam pengembangan dan pengelolaan aplikasi. Langkah-langkah yang diambil untuk meningkatkan keamanan aplikasi tidak hanya akan melindungi data sensitif, tetapi juga dapat meningkatkan reputasi kantor di mata publik. Selain itu, kemitraan dengan lembaga atau organisasi yang berfokus pada keamanan siber juga dapat menjadi peluang. Dengan menjalin kerja sama, kantor dapat mendapatkan akses kepada sumber daya, pelatihan, dan teknologi terbaru dalam bidang keamanan informasi. Kemitraan ini dapat meningkatkan kemampuan tim teknis dalam menghadapi ancaman dan menerapkan praktik keamanan yang lebih baik.

Peluang lain yang dapat dieksplorasi adalah penerapan teknologi baru, seperti kecerdasan buatan (AI) dan pembelajaran mesin (*machine learning*), dalam pengujian keamanan. Teknologi ini dapat membantu dalam mendeteksi ancaman yang lebih kompleks dan mengurangi waktu yang diperlukan untuk menangani kerentanan yang ditemukan. Dengan mengintegrasikan teknologi mutakhir, Kantor Imigrasi dapat lebih proaktif

dalam menjaga keamanan aplikasi mereka.

4. *Threats* (Ancaman)

Meskipun terdapat banyak peluang, ancaman terhadap keamanan aplikasi Inventory tetap menjadi tantangan yang signifikan. Serangan siber semakin berkembang dan menjadi semakin canggih. Penyerang kini memiliki beragam metode untuk mengakses dan mengeksploitasi kerentanan yang ada dalam aplikasi. Ancaman ini dapat berasal dari individu, kelompok, atau bahkan organisasi yang berusaha mencuri data sensitif, merusak sistem, atau bahkan mengganggu operasional kantor.

Selain itu, ketidakpastian regulasi dan peraturan terkait perlindungan data dapat menjadi ancaman bagi Kantor Imigrasi. Jika kantor tidak mematuhi standar keamanan yang ditetapkan, dapat timbul sanksi hukum atau finansial yang merugikan. Oleh karena itu, penting bagi kantor untuk selalu memperbarui kebijakan dan praktik keamanan mereka agar sesuai dengan perkembangan peraturan yang ada.

Lingkungan teknologi yang terus berubah juga merupakan ancaman. Dengan munculnya tren baru dalam teknologi informasi, aplikasi yang digunakan oleh Kantor Imigrasi harus selalu diperbarui agar tetap relevan dan aman. Jika tidak, aplikasi akan menjadi rentan terhadap serangan baru yang mungkin tidak terdeteksi oleh sistem keamanan yang ada. Penyerang dapat memanfaatkan celah keamanan dalam aplikasi yang tidak diperbarui, yang dapat menyebabkan kebocoran data dan kerugian yang signifikan.

Sehinnga dalam hal ini, melalui analisis SWOT ini, terlihat bahwa Kantor Imigrasi Kelas II TPI Langsa memiliki potensi untuk meningkatkan keamanan aplikasi Inventory dengan memanfaatkan kekuatan yang ada, sambil mengatasi kelemahan dan memanfaatkan peluang yang muncul. Pengujian keamanan menggunakan metode OWASP memberikan kerangka kerja yang solid untuk mengidentifikasi dan mengatasi kerentanan yang mungkin ada. Namun, kantor juga harus tetap waspada terhadap ancaman yang mungkin muncul dari berbagai sumber.

Langkah-langkah mitigasi yang harus diterapkan mencakup peningkatan kontrol akses, penerapan validasi input yang lebih ketat, serta penggunaan teknologi keamanan terkini. Pelatihan bagi staf mengenai keamanan siber juga sangat penting untuk meningkatkan kesadaran dan pemahaman mereka tentang risiko yang ada. Dengan menerapkan rekomendasi ini, diharapkan aplikasi Inventory tidak hanya akan meningkatkan efisiensi pengelolaan BMN, tetapi juga memberikan perlindungan yang memadai terhadap ancaman siber yang terus berkembang.

Sebagai langkah strategis, Kantor Imigrasi Kelas II TPI Langsa harus membangun budaya keamanan yang kuat di dalam organisasi. Ini termasuk melibatkan semua pegawai dalam upaya menjaga keamanan informasi dan menekankan pentingnya perlindungan data. Hanya dengan pendekatan yang holistik ini, kantor dapat memastikan bahwa aplikasi Inventory berfungsi dengan baik dan aman, serta mampu mendukung operasional pelayanan imigrasi yang transparan dan terpercaya.

DAFTAR PUSTAKA

OWASP Foundation. (2021). *OWASP top ten: The ten most critical web application security risks*. OWASP Foundation. Retrieved from https://owasp.org/www-project-top-ten/

Ghafoor, K. A., & Ahmad, M. (2019). Web application security vulnerabilities: A systematic literature review. *International Journal of Computer Applications*, 178(31), 19-24. https://doi.org/10.5120/ijca2019919089

Alzahrani, A., & Alharbi, A. (2020). An empirical study of web application security vulnerabilities. *Journal of Computer Virology and Hacking Techniques*, 16(3), 191-205. https://doi.org/10.1007/s11416-020-00331-y

Fawaz, K., & Lteif, H. (2020). Web application security testing using OWASP ZAP tool. *International Journal of Information Security*, 19(5), 579-589. https://doi.org/10.1007/s10207-020-00500-0

Sari, I., & Prabowo, H. (2021). Keamanan informasi pada sistem aplikasi pemerintahan berbasis web. *Jurnal Teknologi Informasi dan Pendidikan*, 14(1), 55-62. https://doi.org/10.24042/jtip.v14i1.8909

Marwan, N., & Ahmed, H. (2020). Exploring the challenges of web application security in organizations. *International Journal of Cyber Security and Digital Forensics*, 9(4), 442-453. https://doi.org/10.17781/P002535

Susanto, H., & Indratno, S. W. (2021). Penerapan metode OWASP dalam pengujian keamanan aplikasi web. *Jurnal Ilmu Komputer dan Informasi*, 14(1), 45-52. https://doi.org/10.21609/jiki.v14i1.866

Bansal, R., & Sharma, K. (2021). A study on web application vulnerabilities: Causes, effects and prevention. *Journal of Information Security and Applications*, 58, 102754. https://doi.org/10.1016/j.jisa.2020.102754

Mardiana, A., & Utomo, R. B. (2022). Evaluasi dan mitigasi kerentanan aplikasi web menggunakan OWASP ZAP. *Jurnal Teknologi dan Sistem Komputer*, 10(1), 25-32. https://doi.org/10.1016/j.jtsc.2021.12.003

Kurniawan, F., & Putra, A. (2020). Analisis kerentanan keamanan sistem informasi berbasis web menggunakan metode OWASP. *Jurnal Informatika*, 15(2), 113-120. https://doi.org/10.21831/informatika.v15i2.31789

Lestari, P., & Mahendra, R. (2021). Penelitian tentang pengujian kerentanan aplikasi web dengan OWASP ZAP di lembaga pemerintahan. *Jurnal Sistem Informasi dan Teknologi Informasi*, 3(1), 47-55. https://doi.org/10.1016/j.jisti.2021.01.007

Nugroho, A., & Susanto, Y. (2021). Evaluasi keamanan aplikasi web dengan pendekatan OWASP Top Ten. *Jurnal Ilmu Komputer*, 19(1), 69-76. https://doi.org/10.23960/jik.v19i1.164

Rahman, M. M., & Begum, R. (2020). A review of web application security testing techniques. *Journal of Computer Networks and Communications*, 2020, Article ID 2014954. https://doi.org/10.1155/2020/2014954

Rizki, F., & Setiawan, A. (2022). Penanganan kerentanan XSS pada aplikasi web dengan metode OWASP. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 6(2), 180-188. https://doi.org/10.5281/zenodo.6334361

Setiawan, B., & Fajrin, M. (2022). Strategi mitigasi serangan siber di aplikasi pemerintahan. *Jurnal Ilmiah Komputer dan Sistem Informasi*, 8(1), 1-10. https://doi.org/10.31599/jiksi.v8i1.418