P-ISSN 2654-5438
E-ISSN 2828-4917

ANALISA KERENTANAN KEAMANAN WEBSITE TIKETKAI.COM MENGGUNAKAN OWASP ZAP DENGAN METODE PTES (STUDI KASUS PT.KAI DIVRE 3 PALEMBANG)

[1]Tantri Langgeng Widodo, [2*]Ade Putra
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma
[2]Komputer Akutansi, Fakultas Vokasi, Universitas Bina Darma
*ade.putra@binadarma.ac.id

Abstract *- Web application security has become a major concern in today's digital age, especially in the face of increasingly sophisticated cyber threats. This study aims to analyze security vulnerabilities on the website of PT.KAI Divre 3 Palembang uses OWASP ZAP (Zed Attack Proxy) and PTES (Penetration Testing Execution Standard) approaches as methodological guides. This case study provides insights into how important web applications in the transportation sector can be exposed to diverse cyber threats. This research method involves Intelligence Gathering stage using WHOIS, Vulnerability Analysis with Nikto, and Exploitation using OWASP ZAP to identify vulnerabilities that may exist on the website. Vulnerability findings are then analyzed based on the level of risk and its impact on the system. The results of this analysis provide a deeper understanding of the potential risks faced by PT web applications. KAI Divre 3 Palembang. The results of this study indicate the presence of vulnerabilities that require serious attention. The findings include vulnerabilities such as Cross-Site Scripting (XSS), SQL Injection, as well as several other vulnerabilities that could compromise user data confidentiality and System Integrity. Based on the findings, recommendations for corrective actions are proposed to mitigate risks and ensure that the system remains secure.*

Keywords: Analysis, PTES, OWASP ZAP

Abstrak - Keamanan aplikasi web telah menjadi perhatian utama dalam era digital saat ini, terutama dalam menghadapi ancaman siber yang semakin canggih. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada website PT.KAI Divre 3 Palembang menggunakan alat *OWASP ZAP (Zed Attack Proxy)* dan pendekatan *PTES (Penetration Testing Execution Standard)* sebagai panduan metodologis. Studi kasus ini memberikan pandangan tentang bagaimana aplikasi web yang penting dalam sektor transportasi dapat terpapar terhadap ancaman siber yang beragam. Metode penelitian ini melibatkan tahap *Intelligence Gathering* menggunakan *WHOIS, Vulnerability* Analysis dengan *Nikto*, serta *Exploitation* menggunakan *OWASP ZAP* untuk mengidentifikasi kerentanan yang mungkin ada pada website. Temuan kerentanan kemudian dianalisis berdasarkan tingkat risiko dan dampaknya terhadap sistem. Hasil analisis ini memberikan pemahaman yang lebih mendalam tentang potensi risiko yang dihadapi oleh aplikasi web PT.KAI Divre 3 Palembang. Hasil dari penelitian ini menunjukkan adanya kerentanan yang memerlukan perhatian serius. Penemuan mencakup kerentanan seperti *Cross-Site Scripting (XSS), SQL* Injection, serta beberapa kerentanan lainnya yang dapat membahayakan kerahasiaan data pengguna dan integritas sistem. Berdasarkan temuan tersebut, rekomendasi tindakan perbaikan diusulkan untuk memitigasi risiko dan memastikan bahwa sistem tetap aman.

Kata kunci: Analisis, *PTES, OWASP ZAP*

P-ISSN 2654-5438
E-ISSN 2828-4917

1. Pendahuluan

Di era yang semakin digital, layanan tiket online semakin populer dan menjadi salah satu opsi utama pemesanan tiket transportasi bagi banyak orang. Salah satu *platform* paling terkenal di Indonesia dan menjadi pelopor jasa pemesanan tiket berbasis online adalah tiketkai.com, yaitu sebuah website yang menawarkan layanan pemesanan tiket kereta api secara online. Sebagai *platform* yang mengontrol informasi sensitif seperti informasi pribadi dan informasi pembayaran, tiketkai.com harus mengutamakan keamanan situs web nya untuk menghindari risiko serangan *siber*.

Menurut hasil survei McAfee pada awal januari 2023, 80% responden Indonesia menyatakan khawatir dengan serangan siber. Ironisnya, penelitian McAfee juga menemukan banyak masyarakat Indonesia yang tidak sadar akan bahaya pembobolan keamanan digital. Berikut diantaranya yaitu reputasi perusahaan yang buruk, resiko kehilangan data, konsumen ikut terancam keamananya dan kerugian secara finansial.

Penelitian ini bertujuan untuk menganalisa kerentanan keamanan website tiketkai.com karena penulis memperoleh informasi adanya keluhan dari beberapa pihak bahwa adanya kurang *mobile*nya website pada saat digunakan dan membuat rasa ingin mengetahui celah ataupun kerentanan yang bisa mengganggu *user* pada saat mengaksesnya, dengan menggunakan *Penetration Test Execution Standard (PTES)* yang memberikan petunjuk langkah demi langkah untuk melakukan penetration test secara terstruktur dan sistematis. Pendekatan *PTES* mencakup langkah-langkah mulai dari desain, pemindaian, hingga analisis dan pelaporan hasil untuk memastikan semua potensi kerentanan tiketkai.com teridentifikasi (Thurfah Afifa Rosaliah & Hananto, 2021).

Dengan bantuan analisis keamanan yang dilakukan dengan metode *PTES* dan *tool OWASP ZAP*, diharapkan tiketkai.com dapat meningkatkan keamanannya terhadap serangan siber dan memberikan layanan yang lebih aman dan andal kepada penggunanya. Selain itu, penelitian ini diharapkan dapat berkontribusi pada keamanan siber dan pengujian penetrasi aplikasi web secara umum [1]. Berdasarkan masalah serta referensi di atas maka penulis akan melakukan implementasi dan melakukan analisa untuk mencegah hal-hal yg menyebabkan kerentanan pada *website*. Maka dari itu penulis mengambil judul "**Analisa Kerentanan Keamanan Website *Tiketkai.com* menggunakan *Tools OWASP ZAP* dengan metode *PTES*".**

2. Tinjauan Pustaka

2.1 WHOIS

WHOIS adalah sebuah protokol yang digunakan untuk mengambil informasi tentang domain, seperti informasi kontak pemilik domain, tanggal pendaftaran, server nama *(DNS)*, dan informasi teknis lainnya. Ini membantu untuk memahami siapa yang bertanggung jawab atas situs web dan memungkinkan komunikasi di area tertentu. *WHOIS* umumnya digunakan untuk tujuan bisnis, keamanan *siber*, dan penegakan hukum [2]

2.2 NIKTO

Nikto adalah alat pemindai / tools scanning kerentanan, dibuat dengan bahasa pemrograman Perl dan awalnya dirilis pada akhir 2001, yang menyediakan pemindaian / scanning kerentanan tambahan **khusus untuk server web**, arti nya Nikto termasuk dalam tools / alat *CGI scanner*. *Nikto* adalah *tools* pencari celah keamanan pada website yang bebas digunakan atau gratis, *Nikto* adalah kode Program yang berlisensi GPL (bebas digunakan) [3]

P-ISSN 2654-5438
E-ISSN 2828-4917

2.3 *OWASP ZAP*

*OWASP ZAP (Zed Attack Proxy) a*dalah sebuah aplikasi *open-source* yang digunakan untuk melakukan testing keamanan pada aplikasi web yang memiliki jangkauan analisa kerentanan yang menyeluruh. Aplikasi ini berjalan pada platform Java dan dapat dijalankan pada sistem operasi *Windows, Linux, dan macOS.* [4]

2.4 *WEBSITE*

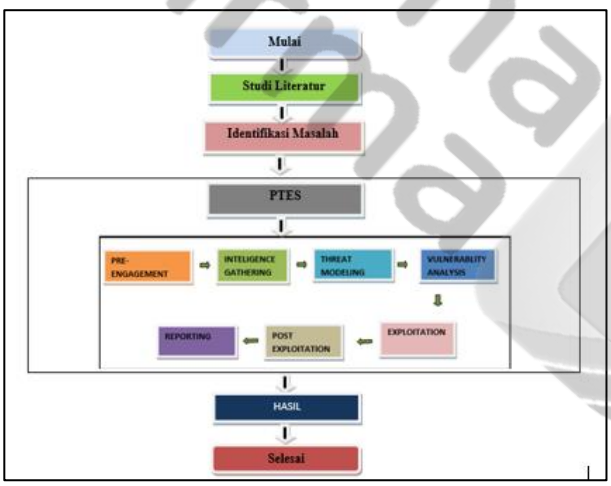
Situs *web* adalah kumpulan halaman *web* terkait yang diakses melalui Internet. Sebuah website biasanya mempunyai alamat unik yang sering disebut *URL (Uniform Resource Locator)* yang dipakai untuk mengetahui lokasi suatu halaman *web* di Internet. [5]

2.5 *PTES (PENETRATION TESTING EXECUTION STANDARD)*

PTES adalah suatu standar yg ditemukan pada tahun 2010 dan bisa melakukan analisa untuk audit keamanan suatu website. Celah keamanan situs web biasanya terjadi pada prosedur keamanan. Saat memperbarui perangkat lunak, kontrol sistem internal, atau penginstalan infrastruktur, Integritas, Kerahasiaan, Akuntabilitas atau Penggunaan Data atau Layanan. [6]

3. Metodologi Penelitian

Berikut dibawah ini kerangka penelitian yang digunakan pada metodologi penelitian adalah sebagai berikut



Gambar 1. Kerangka Penelitian

3.1 Pre-engagement

- Mendefinisikan tujuan dan ruang lingkup pengujian.
- Mempeoleh izin atau sudah ada komunikasi pada pihak perusahaan.
- Mengumpulkan informasi awal tentang target beserta sumber daya yg diperlukan.

3.2 Information Gathering

- Mengumpulkan informasi tentang target dari sumber terbuka.
- Mencari informasi tentang *domain*, *subdomain*, alamat *email*. Dalam hal ini menggunakan *Whois.com*
- Identifikasi alamat domain, dan informasi pendukung lainnya.

3.3 Threat Modelling

- Mengidentifikasi potensi ancaman yang mungkin dihadapi target.

P-ISSN 2654-5438
E-ISSN 2828-4917

- Pemodelan ancaman memfasilitasi deteksi serangan terhadap pemilik layanan dalam penelitian ini.
- Memberi gambaran untuk ke tahapan selanjutnya.

3.4 Vulnerability Analysis

- Melakukan pemindaian kerentanan terhadap target menggunakan *Nikto*.
- Menganalisis hasil pemindaian untuk mengidentifikasi kerentanan.

3.5 Exploitation

- Mencoba memanfaatkan kerentanan yang ditemukan.
- Menguji eksploitasi menggunakan *OWASP ZAP* dan melihat apakah berhasil menemukan celah kerentanan.
- Menjelaskan apa saja maksud dari kerentanan yang ada dan mengurutkannya berdasarkan level

3.6 Post Exploitation

- Menjaga akses ke dalam sistem yang telah dikompromikan.
- Melakukan eksplorasi lebih lanjut untuk mengumpulkan informasi.
- Menganalisa penyebab dari kerentanan yang ada

3.7 Reporting

- Mendokumentasikan semua langkah yang diambil selama pengujian.
- Menyajikan temuan kerentanan dan hasil uji dengan jelas.
- Memberikan rekomendasi perbaikan keamanan sebagai salah upaya melindungi data pengguna pribadi yang memiliki data sensitif seperti NIK.

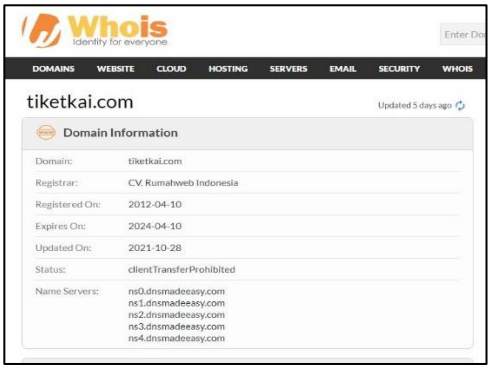
4. Hasil dan Pembahasan

4.1 Pre-engagement

Merupakan tahapan awal sebelum melakukan pengujian yakni mengenalkan dan mengumpulkan informasi terlebih dahulu terhadap obyek yang akan digunakan dalama hal ini tiketkai.com dan mengumpulkan sumberdaya ataupun *software* yang akan dipakai seperti *whois, nikto,* dan *owasp zap* serta berkomunikasi pada pihak perusahaan

4.2 Information Gathering

Tahapan kedua yang berfungsi sebagai pengumpul informasi dalam hal ini menggunakan whois.com dan hasilnya yaitu tiketkai.com bisa dilihat melalui gambar disamping yang menghasilkan informasi nama domain, registar, masa terdaftar, masa expired, masa update dan status.



Gambar 2. Hasil *whois.com*

P-ISSN 2654-5438
E-ISSN 2828-4917

4.3 Threat Modelling

Tahapan ketiga yang merupakan tahapan yang melalukan pemodelan ancaman berdasarkan kerentanan apa saja yang biasa terjadi pada suatu website dan memudahkan nantinya pada saat melakukan *vulnerability Analysis.*

4.4 Vulnerability Analysis

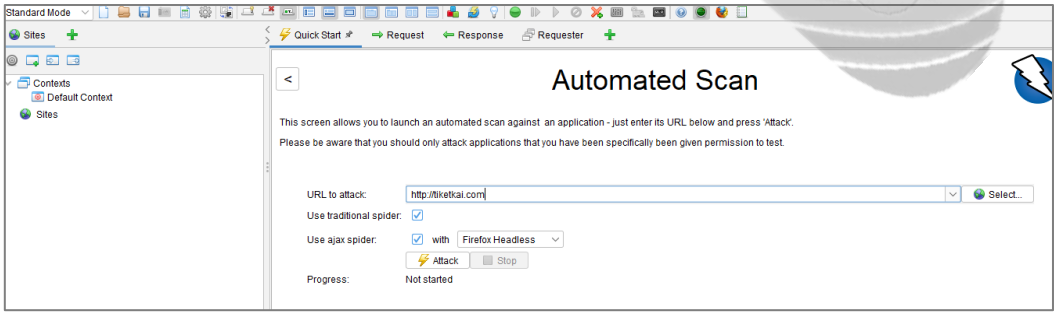
Tahapan keempat yakni melakukan Analisa kerentanan menggunakan nikto yang merupakan alat pemindaian keamanan web yang spesifik, dengan perintah *nikto -h yang* berfungsi melalukan *scanning* secara menyeluruh lalu menghasilkan informasi berupa target *ip, target domain, time access,* dan celah yg muncul kepermukaan seperti *Server: No banner retrieved, the anti-click jacking, the x-xss protection header is not defined.*

Gambar 3. Hasil *scanning Nikto*

4.5 Exploitation

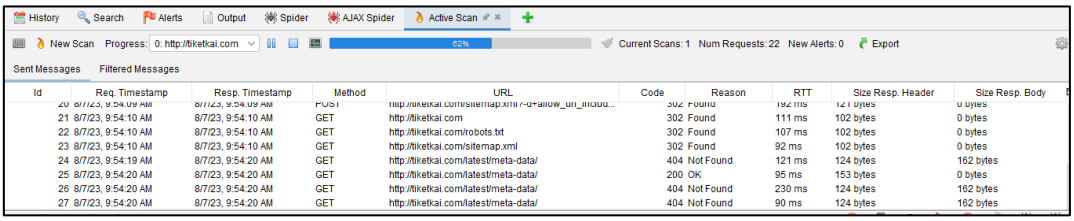
Tahapan kelima, yakni fase *exploitation* yg bertujuan melakukan pengujian terhadap tiketkai.com, *tools* yang digunakan untuk melakukan pengujian yaitu *OWASP ZAP* dengan cara memasukan nama website yang akan diuji lalu pilih opsi dan disamping ini merupakan hasil dari 7 kerentanan yang ada.

1. Pada tahap ini silahkan masukan nama website yang akan dituju serta klik attack pada tombol dibawahnya agar kita bisa melakukan *exploitation*



Gambar 4. Halaman *automated scan*

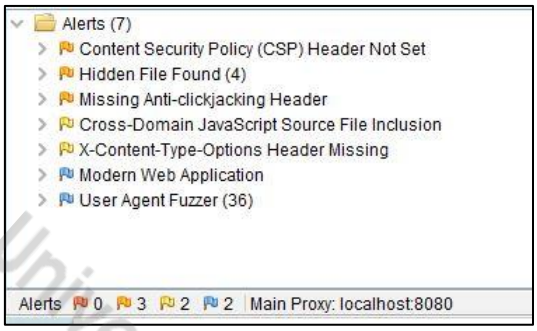
2. Pada tahap ini aplikasi membutuhkan waktu kisaran 10 sampai 20 menit untuk memproses *scanning* dan identifikasi celah apa saja yang bisa jadi kemungkinan kelemahan pada website yang akan dicari.



Gambar 5. Proses *scanning* pada *OWASP ZAP*

P-ISSN 2654-5438
E-ISSN 2828-4917

3. Selanjutnya bisa kita lihat dibawah ini merupakan hasil dari pengujian yangg memberikan peringatan atau kemungkinan kerentanan apa saja yg sudah teridentifikasi, disitu bisa kita lihat ada sekitar 7 kerentanan dengan tingkatan berbeda sesuai dengan hasil scanning yang sudah kita lakukan.



Gambar 6. Hasil *autoscanning OWASP ZAP*

4. Berikut dibawah ini merupakan warna sesuai urutan level kerentanan pada hasil *OWASP-ZAP* yakni kuning itu ***low***, oranye itu ***medium***, biru itu ***informational.***

Gambar 4. Hasil *OWASP ZAP*

4.6 Post Exploitation

Tahapan keenam, yakni fase *Post Exploitation* merupakan tahapan lanjutan dari *Exploitation* yang berfungsi mendefinisikan penyebab-penyebab dari kerentanan yang ada berdasarkan hasil 7 kerentanan tersebut. Ini adalah tahap lanjutan setelah penyerang berhasil memperoleh akses yang dapat digunakan untuk menjelajahi lebih dalam, mengumpulkan informasi, dan bahkan mengambil alih kendali yang lebih besar atas sistem atau jaringan yang telah dikompromikan.

Tabel 1. Penyebab Kerentanan

	KERENTANAN	LEVEL	PENYEBAB
1	Content Security Policy (CSP) Header Not Set	*Medium*	Lapisan keamanan yang harus diatur pada server web untuk mengontrol sumber daya yang dapat dimuat oleh halaman web
2	Hidden file Not Found	*Medium*	Pengelolaan hak akses berkas yang kurang baik. Ini dapat terjadi jika file tersembunyi yang seharusnya tidak dapat diakses oleh pengguna tetap memiliki
3	Missing Anti-clickjacking Header	*Medium*	Konfigurasi yang salah dari header *anti-clickjacking (seperti"x-frame-options")* ketika *header* ini tidak ada atau diatur dengan benar. Situs web dapat menajadi rentan tehadap serangan *clickjacking*
4	Cross Domain Javascript File-Inclusion	*Low*	Kurangnya pengamanan yang memadal terhadap inklusi file *Javascript* dan domain yang berbeda
5	X-Content Type-Options Header Missing	*Low*	Ketiadaan *header X-Content-Type-Options* atau pengaturan yang tidak benar. Tanpa header ini, browser dapat melakukan MIME sniffing yang berpotensi membuka pintu bagi serangan berbasis jenis konten *(MIME)*
6	Modern Web Application	*Informational*	Pengembangan Teknologi modern makin hari makin meluas sehingga penting untuk mengevaluasi kerja website
7	User Agent Fuzzer	*Informational*	Menunujukan potensi resiko manipulasi informasi pengguna yang harus diperhatikan dan diatasi

P-ISSN 2654-5438
E-ISSN 2828-4917

4.7 Reporting

Tahapan Ketujuh, yakni memberikan solusi perbaikan terhadap 7 kerentanan yang ada berdasarkan hasil yang sudah didapat. Berikut dibawah ini penulis tampilkan solusi yang dapat digunakan.

Tabel 2. Solusi Kerentanan

	KERENTANAN	LEVEL	SOLUSI
1	Content Security Policy (CSP) Header Not Set	*Medium*	Atur header csp dalam respons *HTTP* untuk mengontrol sumber daya yang dimuat, untuk membatasi resiko skrip berbahaya
2	Hidden file Not Found	*Medium*	Identifikasi dan review file tersembunyi yg ada dalam server web
3	Missing Anti-clickjacking Header	*Medium*	Aktifkan header anti-clickjacking yang sesuai pada server web anda. Ini biasanya dilakukan untuk mengatur *heoder HTTP"X-Frame-Options"* dengan nilai *"Deny"* atau *"Sameorigin"*
4	Cross Domain Javascript File-Inclusion	*Low*	Gunakan mekanisme pengendalian akses lintas domain yang tepat, seperti *CORS (Cross-Origin-Resource-Sharing*) Untuk membatasi pemanggilan lintas domain
5	X-Content Type-Options Header Missing	*Low*	Aktifkan header X-Content-Type-Options pada server web anda dengan mengatur nilainya menjadi *"nosnifff"*. Ini akan mencegah browser anda untuk melakukan MIME sniffing dan menginterpretsikan tipe konten yg sama
6	Modern Web Application	*Informational*	Menyarankan pihak web developer untuk lebih update lagi terhadap *flow website* tersebut
7	User Agent Fuzzer	*Informational*	Ini adalah peringatan informasi sehingga tidak perlu dilakukan perubahan

5. Kesimpulan

Berdasarkan hasil yang telah diperoleh pada penelitian terbukti bahwasahnya website tiketkai.com memiliki 7 kerentanan berdasarkan level Beberapa kerentanan yang diidentifikasi meliputi *Content Security Policy (CSP) Header Not Set* yakni Aplikasi tidak menerapkan kebijakan keamanan CSP dengan baik, meningkatkan risiko serangan *XSS*, *Hidden File Not Found* berarti Ada keberadaan file tersembunyi yang seharusnya tidak dapat diakses, menunjukkan masalah dalam manajemen hak akses berkas. Kekurangan *header anti-clickjacking* dapat memungkinkan serangan *clickjacking* tanpa pengetahuan pengguna. *Cross-Domain JavaScript Source File Inclusion* berarti Potensi masalah keamanan dalam mencoba memuat *file JavaScript* dari domain berbeda tanpa pengamanan yang tepat. Kekurangan *header X-Content-Type Options* meningkatkan risiko serangan tipe *MIME* dan penyisipan konten berbahaya. *Modern Web Application* memungkin ada aspek-aspek modern dalam aplikasi yang memerlukan pengamanan tambahan untuk mengatasi risiko keamanan. Adanya *User Agent Fuzzer* menunjukkan potensi risiko manipulasi informasi pengguna yang harus diperhatikan dan diatasi.

Referensi

[1] Ary G, Sanjaya S(2022). "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF"

[2] Andriyan W, Septiawan S, Aulya A. PERANCANGAN WEBSITE SEBAGAI MEDIA INFORMASI DAN PENINGKATAN CITRA PADA SMK DEWI SARTIKA TANGERANG**.** *Jurnal Teknologi Terpadu 6 79-88*

[3] Altulaihan E, Alismail A, Frikha M(2023) A Survey on Web Application Penetration Testing

P-ISSN 2654-5438
E-ISSN 2828-4917

[4] Cahyani (2021). ANALISIS KERENTANAN WEBSITE SMP NEGERI 3 SEMARAPURA MENGGUNAKAN METODE PENGUJIAN RATE LIMITING DAN OWASP. *Information System and Emerging Technology Journal*

[5] Cunong D, Saputra M, Puspitasari W *(2020).* ANALYSIS OF OROS MODELER DATA REPORTING PROCESS TO SAP HANA IN ACTIVITY BASED COSTING FOR INDONESIA TELECOMMUNICATION INDUSTRY

[6] Elanda A, Lintang Buana (2022). ANALISIS KEAMANAN SISTEM INFORMASI BERBASIS WEBSITE DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) VERSI 4: SYSTEMATIC REVIEW

[7] Febriana R(2022). Blackbox Testing Sistem Informasi Absensi Pegawai Karawang Dengan Metode Top 10 Owasp Attack**.** *Jurnal Ilmiah Wahana Pendidikan 2022(12) 327-334*