BAB I
PENDAHULUAN

1.1 Latar Belakang

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 (Cunong et al., 2020). 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*".**

1.2 Rumusan Masalah

Adapun permasalahan dari analisis kerentanan website tiketkai.com menggunakan *OWASP ZAP* dengan metode *PTES* pada studi kasus PT KAI Divre 3 Palembang adalah sebagai berikut:

1. Celah keamanan apa yang mungkin ada di tiketkai.com?
2. Seberapa parah risiko dari setiap kerentanan ditentukan?
3. Bagaimana cara memperbaiki dan mereduksi kerentanan yang terdapat pada website tiketkai.com?
4. Bagaimana hasil scan kerentanan ini dapat membantu PT KAI Divre 3 Palembang meningkatkan keamanan dan melindungi data pengguna di tiketkai.com?

1.3 Batasan Masalah

Batasan masalah dari pemindaian kerentanan website tiketkai.com menggunakan metode *OWASP ZAP* dengan *PTES* pada studi kasus PT KAI Divre 3 Palembang yaitu bisa dilihat dibawah ini:

1. Ruang lingkup penelitian yakni kajian akan fokus pada website milik tiketkai.com milik PT KAI Divre 3 Palembang sebagai obyek analisis. Riset akan fokus pada pengujian keamanan aplikasi web terkait dengan tiketkai.com.

2. Jenis kerentanan yang dianalisis yakni penelitian akan fokus pada identifikasi kerentanan keamanan yang terkait dengan kerentanan web yang paling parah dan sering terjadi secara umum, contohnya *SQL Injection*, *Cross-Site Scripting (XSS)*, *Cross-Site Request Forgery (CSRF)*, dan lain-lain. Analisis lainnya, seperti kerentanan pada sistem operasi atau infrastruktur jaringan, bukan pada lingkup penelitian ini.
3. Alat Pindai Keamanan Studi akan menggunakan *OWASP ZAP (Open Web Application Security Project Zed Attack Proxy)* sebagai alat pemindaian keamanan utama untuk mengidentifikasi kerentanan di situs tiketkai.com. Penggunaan alat analisis keamanan lainnya tidak termasuk dalam ruang lingkup penelitian ini.
4. Sumber daya yang digunakan dalam penelitian ini akan dipeloeh dari website tiketkai.com milik PT KAI Divre 3 Palembang.Sumber informasi lain yang tidak terkait langsung dengan situs web tidak termasuk dalam cakupan topik penelitian.

1.4 Tujuan Penelitian

Tujuan penelitian dari analisis kerentanan website tiketkai.com menggunakan *OWASP ZAP* dengan metode *PTES (Penetration Test Execution Standard)* pada studi kasus PT KAI Divre 3 Palembang adalah sebagai berikut:

1. Identifikasi berbagai celah keamanan yakni yang ada pada website tiketkai.com. Dengan menggunakan alat analisis keamanan *OWASP ZAP* dan metode *PTES* yang sistematis, berbagai kerentanan keamanan seperti injeksi *SQL*, *XSS*, *CSRF*, dan lainnya akan diidentifikasi dan dicatat.

2. Penilaian risiko keamanan yakni setelah mengidentifikasi kerentanan, penelitian ini akan menilai tingkat risiko keamanan untuk setiap kerentanan yang ditemukan. Ini membantu untuk memahami keparahan kerentanan dan urgensi perbaikan yang perlu dilakukan untuk mengatasi risiko keamanan ini.

3. Membuat rekomendasi untuk perbaikan yaitu penelitian ini bertujuan untuk memberikan rekomendasi perbaikan yang spesifik dan efektif untuk mengatasi kerentanan keamanan yang ditemukan. Rekomendasi ini akan membantu PT KAI Divre 3 Palembang mengambil tindakan perbaikan dan meningkatkan keamanan tiketkai.com.

4. Tingkatkan keamanan situs web yaitu bertujuan untuk meningkatkan keamanan tiketkai.com secara keseluruhan. Dengan mengidentifikasi dan memperbaiki kerentanan keamanan yang ada, diharapkan website akan lebih tahan terhadap potensi serangan dan ancaman keamanan siber.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diberikan pada penelitian analisa kerentanan keamanan website tiketkai.com menggunakan *OWASP ZAP* dengan metode *PTES* pada studi kasus PT KAI Divre 3 Palembang adalah sebagai berikut:

1. Identifikasi dan perbaiki celah keamanan, Penelitian ini membantu PT KAI Divre 3 Palembang untuk mengidentifikasi berbagai celah keamanan yang mungkin ada pada website tiketkai.com dengan mengetahui kerentanan ini, tindakan korektif dan peningkatan keamanan dapat dilakukan untuk memperbaiki kelemahan keamanan yang ada.
2. Peningkatan keamanan situs web, Menerapkan saran perbaikan dari analisis kerentanan ini akan meningkatkan keamanan tiketkai.

   Dengan menambal celah keamanan, situs web menjadi lebih tahan terhadap potensi serangan dan ancaman keamanan siber.

3. Kepercayaan pengguna, dengan menunjukkan komitmen PT KAI Divre 3 Palembang dalam memperbaiki celah keamanan dan melindungi data pengguna, kepercayaan pengguna terhadap situs tiketkai.com.
4. Manajemen Risiko Keamanan yang Lebih Baik, melalui analisis kerentanan, PT KAI Divre 3 Palembang mampu mengetahui tingkat risiko keamanan yang ada pada website tiketkai.com dengan pengetahuan ini, perusahaan dapat mengambil tindakan pencegahan yang tepat dan mengelola risiko keamanan dengan lebih baik.
5. Kesadaran dan Pemahaman Tim *TI*, studi ini juga dapat meningkatkan kesadaran dan pemahaman tim *IT* di PT KAI Divre 3 Palembang tentang keamanan siber dan pentingnya melakukan pemantauan dan analisis keamanan secara berkala.

1.6 Penelitian Terdahulu

Berikut dibawah ini merupakan beberapa ulasan dari penelitian terdahulu yang dapat memberikan referensi dalam penulisan penelitian yakni sebagai berikut:

Menurut pendapat Rahmad Ashar pada jurnal yang berjudul "Analisis Keamanan Open Website Menggunakan Metode *OWASP* dan *ISSAF*". Jurnal ini diterbitkan pada tanggal 31 Desember 2022. Artikel ini membahas analisis keamanan website Diskominfo Kerinci yang terbuka menggunakan metode *OWASP* dan *ISSAF*. Metodologi penelitian mencakup langkah-langkah seperti identifikasi, pemindaian,

penggunaan, pemeliharaan akses dan pelaporan. Metodologi *ISSAF* mencakup langkah-langkah seperti pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, penyebaran, eskalasi hak istimewa, dan pelaporan. Sumber yang digunakan dalam penelitian ini meliputi berbagai sumber yang berkaitan dengan keamanan informasi dan keamanan *website*. (Rahmad Ashar, 2022).

Menurut pendapat dari Penulis Jurnal ini adalah Muhammamd Faturachzi. Pada jurnal yang berjudul "Analisa Keamanan Website Menggunakan Metode *Footprinting* dan *Vulnerability Scanning* pada Website Kampus diterbitkan pada tanggal 2 tahun 2021. Jurnal ini membahas analisis keamanan situs web menggunakan metode *footprinting* dan pemindaian kerentanan. Studi ini berfokus pada *website* Kampus Muhammad Fatkhurozzi dengan tujuan mengidentifikasi potensi kerentanan dan merekomendasikan perbaikan untuk meminimalkan risiko keamanan. Studi ini menggunakan teknik dan alat peretasan etis seperti domain *CMD, Zenmap* dan *Whois* untuk mengumpulkan informasi tentang situs web target. Pemindaian *footprint* dan kerentanan menemukan banyak kerentanan termasuk kelemahan aplikasi, serangan *header host*, dan kurangnya perlindungan *CSRF*. Di akhir dokumen, disarankan untuk menerapkan langkah-langkah keamanan untuk mengatasi kerentanan ini dan melindungi situs web dari kemungkinan serangan. (fatkhurozzi, 2022).