BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan sistem *website* merupakan aspek kritis dalam pengembangan dan operasionalitas suatu *platform online*. Dengan kemajuan teknologi informasi, *website* tidak hanya menjadi sarana untuk menyajikan informasi, tetapi juga menjadi target potensial bagi serangan siber. Ancaman keamanan terus berkembang seiring waktu, memerlukan upaya yang terus-menerus untuk mengidentifikasi dan mengatasi potensi kerentanan.

Berdasarkan *Global Cybersecurity Index* (GCI) 2020 yang diterbitkan oleh *International Telecommunication Union* (ITU), Keadaan keamanan siber di Indonesia menempati peringkat ke-24 dari 194 negara. Hal ini menunjukkan adanya peningkatan dibandingkan tahun 2018, di mana Indonesia berada di peringkat 41 [1].

Pada tahun 2022, BSSN mencatat bahwa Indonesia mengalami 370,02 juta serangan siber, yang menandai peningkatan sebesar 38,72% dibandingkan dengan tahun sebelumnya di mana jumlah serangan mencapai 266,74 juta di tanah air [2]. Menurut lanskap keamanan siber Indonesia tahun 2023, sektor administrasi pemerintahan menjadi yang tertinggi dan paling banyak terkena insiden siber. Insiden tersebut meliputi kebocoran data, serangan *ransomware*, *web defacement*, indikasi potensi serangan DDoS, dan upaya pemantauan proaktif terhadap dugaan insiden siber[3].

Sebagai contoh dari data tersebut, penelitian terkait keamanan siber pada *website* Pemerintah Kabupaten Kediri menggunakan Teknik *penetration testing*, ditemukan beberapa celah keamanan yang memungkinkan pengungkapan data sensitif seperti *username* dan *password* untuk akses *login* ke halaman cp panel admin [4].

Dalam Konteks ini, organisasi atau lembaga pemerintah, seperti Dinas Sosial Surabaya, yang menyediakan layanan melalui *website* resmi, harus memastikan bahwa sistem informasi mereka aman dan dapat diandalkan. *Penetration testing*, sebagai salah satu pendekatan uji keamanan yang efektif, memungkinkan untuk mengidentifikasi potensi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Penetration Testing atau *pentest* adalah serangan terhadapat sebuah sistem

yang dilakukan seseorang untuk membantu mengidentifikasi kerentanan terhadap aplikasi atau jaringan guna memberikan pengukuran untuk perbaikan berkelanjutan [5]. Untuk memastikan keamanan *website* Dinas Sosial Surabaya, diperlukan pendekatan yang komprehensif dan sistematis dalam mengidentifikasi dan mengelola risiko keamanan. Dua metode yang dapat digunakan untuk tujuan ini adalah OWASP Top 10 dan MITRE ATT&CK.

Open Web Application Security Project (OWASP) Top 10 2021 adalah panduan yang terkemuka dalam mengidentifikasi dan mengatasi kelemahan keamanan pada aplikasi web [6]. Metode ini memberikan pandangan tentang ancaman keamanan yang paling relevan dan signifikan yang dihadapi oleh aplikasi web saat ini.Sementara itu, MITRE ATT&CK adalah basis pengetahuan yang dapat diakses secara global mengenai taktik dan teknik musuh berdasarkan observasi dunia nyata. MITRE ATT&CK digunakan sebagai dasar untuk pengembangan model ancaman spesifik dan metodologi di sektor swasta, pemerintah, dan komunitas produk dan layanan keamanan cyber [7]. Kombinasi dari OWASP Top 10 dan MITRE ATT&CK dapat memberikan pendekatan yang holistik untuk pengujian keamanan, dengan fokus pada identifikasi kerentanan spesifik serta pemahaman tentang taktik serangan yang lebih luas.

Metode lain yang dapat digunakan yaitu NIST Cybersecurity Framework (National Institute of Standards and Technology) juga relevan dalam konteks keamanan siber. NIST Cybersecurity Framework menyediakan panduan komprehensif untuk meningkatkan dan mengelola keamanan siber suatu organisasi atau lembaga. Kerangka ini terdiri dari lima fungsi inti, yaitu Identifikasi, Perlindungan, Deteksi, Respons, dan Pemulihan [8]. Setiap fungsi ini dirancang untuk memberikan pendekatan yang terstruktur dalam memahami risiko keamanan siber, melindungi aset kritis, mendeteksi ancaman, merespons insiden, dan memulihkan operasional secara efektif. Dengan menggunakan kerangka tersebut, lembaga maupun organisasi dapat menilai tingkat kepatuhan mereka terhadap praktik terbaik keamanan siber, mengalokasikan sumber daya secara efisien, dan mengoptimalkan strategi untuk mengatasi tantangan siber yang terus berkembang [9]. Namun, metode ini kurang cocok untuk melengkapi metode *penetration testing* pada *website* karena lebih berfokus pada manajemen risiko dan kebijakan keamanan dibandingkan dengan pengujian teknis untuk menemukan celah keamanan secara langsung. Selain itu,

cakupannya yang luas menjadikan metode ini lebih sesuai untuk strategi keamanan siber secara menyeluruh daripada hanya digunakan dalam pengujian penetrasi pada sebuah *website*.

Selain itu, metode lain yang masih relevan dalam konteks keamanan informasi adalah ISO/IEC 27001. ISO/IEC 27001 adalah standar internasional yang menyediakan kerangka kerja untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) [10]. Standar ini berfokus pada pengelolaan risiko keamanan informasi melalui serangkaian kontrol keamanan yang mencakup kebijakan, proses, dan teknologi [11]. Melalui pendekatan berbasis risiko, ISO/IEC 27001 membantu organisasi dalam memastikan kerahasiaan, integritas, dan ketersediaan informasi yang dikelola. Dengan begitu, metode ini lebih berfokus pada strategi manajemen keamanan informasi secara menyeluruh daripada pengujian teknis terhadap kerentanan spesifik pada sebuah website, sehingga kurang cocok digunakan untuk melengkapi penetration testing pada web.

Studi kasus pada *website* Dinassosial.Surabaya.go.id dianggap penting karena lembaga ini menyediakan layanan publik melalui *platform online* dan memilik peran penting dalam memberikan akses informasi. Dengan menganalisis celah keamanan *website* Dinassosial.Surabaya.go.id menggunakan teknik penetration testing dengan pendekatan OWASP Top 10 2021 dan MITRE ATT&CK. Dengan pendekatan ini, diharapkan dapat diidentifikasi berbagai kerentanan dan ancaman keamanan yang ada, serta memberikan rekomendasi untuk meningkatkan keamanan *website* tersebut. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan keamanan informasi dan layanan yang disediakan oleh Dinas Sosial Surabaya, serta dapat menjadi referensi bagi instansi pemerintah lainnya dalam mengelola keamanan aplikasi web mereka.

1.2. Rumusan Masalah

Berdasarkan latar belakang permasalahan tersebut maka penulis mengidentifikasikan permasalahan sebagai berikut:

a. Apa saja kerentanan keamanan yang ada pada *website* Dinas Sosial Surabaya?
b. Bagaimana metode OWASP Top 10 dan MITRE ATT&CK dapat digunakan untuk mengidentifikasi dan mengatasi kerentanan tersebut?

c. Bagaimana solusi pencegahan terhadap celah keamanan *website* yang ditemukan?

1.3. Tujuan Penelitian

Tujuan penelitian merupakan jawaban atau sasaran yang ingin dicapai dalam sebuah penelitian. Oleh sebab itu, tujuan penelitian ini adalah sebagai berikut:

a. Mengidentifikasi kerentanan pada *website* Dinas Sosial Surabaya.
b. Menganalisis kerentanan tersebut menggunakan metode OWASP Top 10 dan MITRE ATT&CK.
c. Memberikan rekomendasi untuk mencegah kerentanan kemanan pada *website* berdasarkan hasil analisis.

1.4. Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

a. Meningkatkan keamanan *website* Dinas Sosial Surabaya.
b. Memberikan panduan praktis untuk pengujian keamanan aplikasi web menggunakan Metode Penetration Testing OWASP Top 10 dan MITRE ATT&CK.
c. Dapat menemukan celah keamanan yang dimiliki oleh *website*.
d. Mendapatkan rekomendasi yang sesuai dengan hasil analisis.

1.5. Batasan Masalah

Pada penelitian ini penulis membutuhkan batasan agar tidak terjadi pelebaran masalah. Adapun batasan masalah dalam penelitian ini sebagai berikut:

a. Penelitian yang dilakukan menggunakan metode Grey-Box karena penulis hanya mempunyai akses sebagai user
b. Tidak mencakup sistem backend yang tidak terhubung langsung ke aplikasi web
c. Penelitian ini hanya membahas sampai tahap rekomendasi pencegahan pada celah keamanan *website*.