BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi terus terjadi di seluruh dunia yang sejalan dengan perkembangan zaman. Seiring dengan perkembangan internet saat ini, penggunanya terus meningkat. Dengan demikian, kemungkinan ancaman siber pun akan meningkat[1]. *Cyber threats* merupakan tindakan ilegal yang mencuri dan merusak data yang berharga dari aplikasi atau *website*, dan dapat mengancam keamanan jaringan, *database* serta sistem komputer. Berdasarkan Table 1.1 di Indonesia, pada Januari hingga Juli 2019, terdapat 33.451.230 ancaman siber yang terjadi. Kemudian, pada Januari hingga Juli 2020, ancaman siber meningkat sebesar 9.35% menjadi 126.882.845. Selanjutnya, pada tahun 2021 ancaman siber meningkat hingga 1.637.973.022, menurut data yang dikumpulkan oleh Badan Siber Nasional [2]. Kemudian kejahatan siber mengalami penurunan pada tahun 2022, jumlah ancaman siber turun dari tahun sebelumnya sebanyak 976.429.996[3]. Pada tahun berikutnya yaitu 2023 ancaman siber di Indonesia mengalami penurunan sebanyak 403.990.813. Hal ini membuktikan bahwa pada tahun 2023 Indonesia telah mengalami penurunan ancaman siber yang cukup baik dari tahun sebelumnya[4].

Table 1 1 Data Ancaman Siber Indonesia

Tahun	Ancaman Siber
2019 (Jan - Jul)	33.451.230
2020 (Jan - Jul)	126.882.845
2021 (Jan - Jul)	741.441.648
2021 (Jul - Des)	1.637.973.022
2022 (Jan – Des)	976.429.996
2023 (Jan – Des)	403.990.813

Teknologi informasi memiliki dampak pada masyarakat secara keseluruhan, baik positif maupun negatif. Salah satu manfaatnya adalah kemampuan untuk mengakses berbagai informasi melalui transaksi dalam dan antar negara. Sebaliknya, dapat memberi kesempatan untuk melakukan berbagai jenis pelanggaran, yang meliputi sabotase, penipuan, perusakan nama baik, perjudian dan pencurian yang juga dapat disebut *cybercrime*. Sebuah *website* harus dilindungi agar data tetap aman karena berfungsi sebagai media penyampaian informasi. Seorang *hacker* dapat membuat program untuk kepentingan dirinya sendiri dan merusak data apabila pemilik situs web mengabaikan keamanan. *Virus*, peretasan rekening bank, pencurian data pengguna dan pencurian *password e-mail/web server* adalah beberapa contoh kasus yang dilakukan oleh *hacker*. Selain mengumpulkan data penting dari situs web, *hacker* bahkan dapat mengubah tampilan situs web organisasi, instansi, dan sekolah[5]

Website resmi Pemerintah Daerah ABC dikembangkan dan dikelola oleh Dinas Komunikasi dan Informatika (Diskominfo) daerah ABC. *Website* ini menyajikan informasi publik seperti profil, visi-misi, struktur organisasi, produk hukum, berita, galeri, dan fasilitas pengaduan masyarakat. Terdapat fitur-fitur seperti profil lembaga, fraksi, dan alat kelengkapan dewan, serta menyediakan akses ke dokumen hukum. Selain itu, terdapat berita dan video kegiatan, galeri foto, serta formulir pengaduan masyarakat yang berisi nama, *email*, nomor *handphone* dan pesan. *Website* pemerintah daerah ABC memiliki tingkat kunjungan yang relatif rendah sekitar 20-50 pengunjung perhari. Hal ini dapat disebabkan oleh kurangnya optimalisasi konten dan promosi digital yang belum maksimal. Hal ini membuktikan bahwa *website* pemerintah daerah ABC umumnya masih perlu ditingkatkan dari sisi visibilitas dan keterlibatan pengunjung.

Pada *website* pemerintah daerah ABC terdapat fitur formulir pertanyaan atau pengaduan yang memungkinkan pengunjung untuk mengirimkan pesan kepada pihak pengelola. Disini pengunjung mengisi data pribadi berupa nama, nomor *handphone*, dan pesan. Sifat informasi tersebut tergolong sensitif dan

termasuk dalam kategori data pribadi, sehingga perlu dijaga kerahasiaannya supaya tidak dimanfaatkan secara tidak sah oleh pihak yang tidak berwenang.

Browser memungkinkan aplikasi web diakses dan dijalankan pada berbagai *platform* sistem operasi. *Platform* aplikasi berbasis *website* cukup rentan terhadap serangan *hacker* dan biasanya terjadi ketika situs web diserang untuk mendapatkan data penting. Serangan siber umumnya dipicu oleh keberadaan *malware*, *ransomware*, serangan rantai pasokan (*supply chain attack*). Serangan yang dapat menyerang aplikasi berbasis web antara lain *Cross-Site Scripting (XSS), Phishing dan SQL Injection.* Penelitian ini dilakukan untuk mengidentifikasi celah keamanan pada situs web dengan menerapkan metode *Penetration Testing Execution Standard (PTES)*. Tahap pengujian keamanan aplikasi berbasis web dilakukan dengan menguji metode serangan yang mungkin terhadap aplikasi target[5].

Website Pemerintah Daerah ABC digunakan sebagai objek pengujian dalam penelitian ini. Pengujian *penetration testing* dilakukan terhadap *website* tersebut karena sebelumnya pernah mengalami serangan yang menyebabkan perubahan pada tampilan *font* di halaman. Dari hasil analisis, serangan ini kemungkinan besar merupakan jenis serangan *XSS (Cross-Site Scripting),* yaitu ketika kode berbahaya disisipkan oleh penyerang ke dalam *website* dan secara otomatis dijalankan oleh *browser* pengguna saat halaman diakses. Hal ini biasanya terjadi karena *website* tidak memfilter *input* dari pengguna dengan baik. Pengujian ini dilakukan untuk menemukan kerentanan serupa, mengevaluasi tingkat keamanan *website*, dan memberikan saran perbaikan guna mencegah terulangnya serangan di masa mendatang.

Terjadinya perubahan tampilan *font* pada *website* Pemerintah daerah ABC dapat berdampak cukup serius. Meskipun terlihat sederhana, serangan ini menunjukkan adanya kerentanan yang dapat dimanfaatkan untuk tujuan berbahaya. Dampaknya antara lain kerusakan tampilan *website* yang menurunkan kredibilitas, pencurian data pengguna seperti *cookie* atau informasi pribadi, hingga potensi pengalihan pengguna ke situs berbahaya. Jika tidak segera ditangani, serangan semacam ini dapat dimanfaatkan sebagai titik

awal untuk melancarkan serangan lain yang berdampak lebih besar. Untuk mengevaluasi masalah keamanan dan kerentanan, peneliti akan menggunakan *Penetration Testing Execution Standard (PTES).*

Pemilihan metode *PTES (Penetration Testing Execution Standard)* didasarkan pada struktur tahapan yang terdefinisi dengan jelas dan mudah diterapkan untuk pengujian keamanan secara umum, mulai dari *Pre-engagement Interaction, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation,* hingga *Reporting*. Dibandingkan dengan metode atau *framework* lain seperti *OSSTMM* atau *ISSAF* yang lebih kompleks dan teknis, *PTES* lebih sederhana dan mudah dipahami, terutama dalam pengujian keamanan sistem milik instansi pemerintah, dan jika dibandingkan dengan *OWASP*, yang lebih fokus pada pengujian aplikasi web saja, *PTES* lebih fleksibel karena bisa digunakan untuk menguji berbagai jenis sistem, termasuk jaringan dan server. Meskipun *NIST* juga memiliki panduan yang rapi dan resmi, *PTES* dinilai lebih praktis dan mudah dipahami karena menggunakan bahasa yang lebih sederhana dan langsung ke teknisnya serta alurnya terstruktur dan tidak membingungkan. Dengan metode ini, proses pengujian bisa dilakukan secara menyeluruh namun tetap efisien dan mudah dipahami hasilnya.

Kajian terkait keamanan sistem telah banyak dikembangkan oleh peneliti terdahulu melalui penerapan metode dan *framework* yang beragam. Metode adalah pendekatan teknis atau langkah-langkah spesifik yang digunakan untuk melakukan pengujian keamanan, seperti *black-box, grey-box*, atau *white-box testing*. Penggunaan metode fokus pada bagaimana proses pengujian dilakukan secara teknis. Metode pengujian *black box* hanya meminta informasi seperti identitas organisasi dan domain *website* disamarkan sehingga pengujian menyerupai serangan nyata, mengingat penguji perlu waktu lebih untuk mengumpulkan informasi tambahan mengenai sistem yang diuji. Pengujian *black box* juga difokuskan pada aspek kualitas perangkat lunak serta berfungsi untuk mengidentifikasi berbagai kerentanan perangkat lunak, termasuk kesalahan antarmuka, fungsi sistem yang tidak sesuai, dan struktur data yang

tidak benar. Dan pada metode *grey box*, penguji hanya memiliki sebagian informasi sistem (misalnya login pengguna biasa). Sementara itu, white box merupakan bentuk pengujian yang dilakukan dengan memberikan seluruh informasi sistem secara lengkap sebelum proses pengujian dimulai [6].

Sementara itu, *framework* adalah kerangka kerja menyeluruh yang mencakup metode, standar, struktur pelaporan, serta panduan teknis dan etika, seperti yang terdapat pada *PTES, OSSTMM, OWASP, ISSAF* dan *NIST SP 800-115*. *Framework* digunakan untuk menstandarkan seluruh proses *penetration testing*, mulai dari perencanaan hingga dokumentasi hasil. Dengan kata lain, metode adalah bagian dari *framework*, sedangkan *framework* mencakup seluruh sistem kerja pengujian keamanan[7]. Metode *OWASP (Open Web Application Security Project) Top 10* mencakup 10 kerentanan utama yang dapat mengancam keamanan website. *OWASP Top 10* berperan dalam memberikan panduan untuk mengurangi risiko kerentanan, serta pemahaman terhadap jenis-jenis kerentanan umum pada aplikasi web membantu organisasi mempersiapkan diri lebih baik dalam melindungi data dari potensi serangan[8]. *ISSAF* adalah *framework* pengujian keamanan yang komprehensif yang fokus pada penilaian dan peningkatan keamanan sistem informasi. *ISSAF* menekankan pengujian keamanan dari perspektif implementasi, *framework* ini menyediakan pendekatan terstruktur untuk pengujian keamanan dan mencakup berbagai aspek evaluasi dan pelaporan sistem. Metodologi pengujian penetrasi *ISSAF* dikembangkan sebagai *framework* untuk melakukan evaluasi terhadap pengendalian keamanan jaringan, aplikasi, dan sistem serta untuk menemukan kerentanan dan menilai posisi keamanan sistem informasi secara keseluruhan[9]. Metodologi *OSSTMM (Open Source Security Testing Methodology Manual)* mencakup pengujian di berbagai saluran, seperti manusia, fisik, nirkabel, telekomunikasi, dan jaringan data. Ini sangat tepat untuk melakukan pengujian keamanan di berbagai lingkungan seperti komputasi awan, infrastruktur virtual, *middleware* pesan, infrastruktur komunikasi seluler, lokasi dengan keamanan tinggi, sumber daya manusia, komputasi tepercaya, dan sumber daya informasi lainnya. *Framework* ini

menekankan pendekatan holistik terhadap pengujian keamanan dengan mempertimbangkan faktor manusia dan kontrol keamanan fisik, serta risiko teknis[9]. *PTES (Penetration Testing Execution Standard)* merupakan standar atau kerangka kerja yang dirancang untuk memberikan pedoman menyeluruh untuk melakukan uji penetrasi pada sistem, aplikasi, atau jaringan. Ini adalah metode uji penetrasi yang mudah digunakan dan memiliki deskripsi yang rinci untuk setiap tahap pengujian. Metode *PTES* berfungsi sebagai acuan yang merinci langkah-langkah penting dalam melakukan pengujian penetrasi secara optimal dan mencakup berbagai tahapan mulai dari perencanaan awal hingga pelaporan hasil uji. Standar ini bertujuan untuk memastikan bahwa pengujian penetrasi dilakukan secara sistematis, terstruktur, dan sesuai dengan kebutuhan keamanan sistem yang diuji[10]. *NIST* berisi panduan resmi untuk uji keamanan teknis termasuk *scanning*, *testing*, dan pelaporan. *NIST SP 800-115* yang terbagi menjadi 4 tipe dalam melakukan pengujian terdiri dari *planning* (persetujuan kepada klien dan penjelasan ruang lingkup dalam penelitian dengan melakukan *scanning*), *discovery* (berisikan *information gathering* dan *vulnerability scanning*), *attack* (evaluasi dari pemindaian yang diperoleh melalui pengujian terhadap keamanan *website*) dan *reporting* (hasil dari setiap tahapan yang dilakukan)[11].

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut maka rumusan masalah telah ditemukan dalam penelitian ini, yaitu tingkat keamanan *website* yang masih rendah, yang mengacu pada kejadian-kejadian yang ditemukan di sejumlah daerah dan adanya serangan *XSS* yang terjadi di masa lalu pada *website* pemerintah daerah ABC, maka dari itu perlu dilakukan pengujian kerentanan *website* yang akan dilakukan oleh peneliti dari data yang relevan.

1.3 Tujuan dan Manfaat

Merujuk pada rumusan masalah yang telah dirumuskan, penelitian ini bertujuan untuk mengidentifikasi kelemahan sistem keamanan pada *website* Pemerintah Daerah ABC melalui proses pengujian penetrasi. Uji coba ini

dilaksanakan melalui percobaan serangan yang telah dikendalikan sebelumnya untuk mengidentifikasi celah keamanan yang ada, serta menyusun saran perbaikan yang sesuai agar sistem menjadi lebih aman. Penelitian ini juga bertujuan untuk menerapkan *Penetration Testing Execution Standard (PTES)* secara menyeluruh, yang terdiri dari tujuh tahapan utama. Melalui penerapan metode ini, dilakukan analisis dan penilaian terhadap hasil dari tiap tahapan untuk mendapatkan gambaran kondisi keamanan sistem secara menyeluruh. Hasil pengujian ini kemudian digunakan sebagai dasar dalam menyusun saran perbaikan yang terarah dan sesuai untuk memperkuat keamanan *website* dalam menghadapi serangan siber yang mungkin terjadi.

Manfaat dari penelitian ini diharapkan dapat menunjukkan tingkat keamanan situs web pemerintah daerah ABC saat ini dan membantu dalam mengidentifikasi kerentanan yang ada pada *website*. Setelah mengidentifikasi kerentanan, upaya mitigasi dapat dilakukan untuk memperbaiki kelemahan sebelum dimanfaatkan oleh pihak yang tidak berwenang seperti yang telah terjadi sebelumnya. Diharapkan juga penelitian ini dapat meningkatkan kesadaran seluruh organisasi tentang pentingnya keamanan siber dan ancaman siber.

1.4 Batasan Masalah

Mengacu pada rumusan masalah dan tujuan penelitian, agar pembahasan tetap terfokus dan sesuai dengan permasalahan yang diangkat, maka ditetapkan batasan penelitian sebagai berikut:

1. Hasil penelitian yang bersifat rahasia tidak dipublikasikan.
2. Peneliti melakukan analisis dan memberikan rekomendasi perbaikan.

1.5 Metode Penelitian

Metode yang diterapkan dalam penelitian ini adalah *Penetration Testing Execution Standard (PTES),* yaitu sebuah *framework* standar dalam pengujian keamanan sistem informasi. *PTES* dipilih karena memiliki struktur yang sistematis dan mudah diterapkan dalam pengujian keamanan *website*, serta

mencakup tujuh tahapan, yaitu *Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation,* dan *Reporting*. Penelitian ini dimulai dengan pengumpulan teori dan referensi yang relevan (studi literatur), kemudian dilanjutkan dengan pengujian langsung terhadap *website* Pemerintah Daerah ABC secara terstruktur menggunakan alat bantu seperti *Nmap, ZAP, Xray,* dan *SQLMap.* Melalui pendekatan ini, peneliti dapat menganalisis kelemahan sistem, mengevaluasi tingkat kerentanannya, serta menyusun rekomendasi perbaikan keamanan secara menyeluruh dan berbasis data hasil eksperimen.