BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran Kerja Praktek

Kerja Praktek (Magang) merupakan salah satu kegiatan akademik yang wajib dilaksanakan oleh mahasiswa sebagai bagian dari proses pembelajaran di perguruan tinggi. Kegiatan ini merupakan sarana bagi mahasiswa untuk mengaplikasikan teori dan keterampilan yang telah dipelajari selama perkuliahan ke dalam dunia kerja serta memperoleh pengalaman praktis sesuai dengan bidang keilmuannya (Politeknik Negeri Bengkalis 2025). Selain itu, Ufia et al. (2024) menyatakan bahwa melalui kegiatan magang mahasiswa tidak hanya memperoleh pengalaman praktis yang relevan dengan bidang keahliannya, tetapi juga mampu memahami berbagai permasalahan yang dihadapi oleh instansi serta memberikan kontribusi dalam penyelesaiannya.

Dalam pelaksanaan magang ini, penulis ditempatkan di Dinas Komunikasi, Informatika, Statistik dan Persandian (Diskominfotiksan) Kota Dumai, khususnya pada Bidang Statistik dan Persandian. Pemilihan instansi ini didasarkan pada kesesuaiannya dengan bidang keilmuan Keamanan Sistem Informasi serta peran instansi dalam pengelolaan berbagai layanan teknologi informasi dan *website* pemerintah daerah. Instansi ini berperan dalam pengelolaan website pemerintah daerah serta berbagai layanan teknologi informasi yang mendukung penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) (Diskominfotiksan Kota Dumai 2026).

Perkembangan teknologi informasi telah mendorong pemanfaatan *website* sebagai sarana penyampaian informasi dan pelayanan publik. Pemanfaatan *website* memberikan berbagai kemudahan dalam penyebaran informasi serta peningkatan kualitas layanan kepada masyarakat. Namun, meningkatnya penggunaan *website* juga diikuti dengan meningkatnya ancaman keamanan siber. Moharir et al. (2025) menjelaskan bahwa *SQL Injection* dan *Cross-Site Scripting (XSS)* merupakan dua

jenis serangan yang umum mengancam keamanan aplikasi web. Sejalan dengan itu, Bakır (2025) menunjukkan bahwa kedua jenis serangan tersebut terus berkembang sehingga diperlukan mekanisme deteksi yang lebih adaptif. Selain itu, Tadhani et al. (2024) menyatakan bahwa penerapan mekanisme pengamanan terhadap serangan *SQL Injection* dan *Cross-Site Scripting (XSS)* menjadi langkah penting untuk menjaga keamanan aplikasi web. Di samping itu, Rustianto et al. (2025) menunjukkan bahwa *brute force attack* juga menjadi ancaman serius apabila mekanisme *autentikasi* tidak dilengkapi pembatasan percobaan login. Neef dan Oudeh (2024) juga menjelaskan bahwa kerentanan *unrestricted file upload (malicious file upload)* dapat dimanfaatkan oleh penyerang untuk mengunggah berkas berbahaya yang berpotensi mengompromikan aplikasi web. Berbagai serangan tersebut dapat menyebabkan kebocoran data, gangguan layanan, perubahan tampilan *website* (*defacement*), penanaman file berbahaya (*backdoor*), hingga pengambilalihan sistem oleh pihak yang tidak berwenang.

Berdasarkan hasil observasi selama pelaksanaan magang, ditemukan bahwa keamanan *website* masih menjadi salah satu tantangan yang dihadapi oleh instansi. Meskipun beberapa *website* telah menerapkan mekanisme keamanan tertentu, hasil pengujian keamanan menunjukkan masih adanya kerentanan aplikasi web yang berpotensi dimanfaatkan oleh penyerang, seperti *Cross-Site Scripting (XSS)* dan berbagai celah keamanan lainnya. Selain itu, beberapa insiden keamanan yang pernah terjadi menunjukkan adanya penyalahgunaan *website* dan perubahan tampilan website (*defacement*) yang mengindikasikan adanya celah keamanan pada sistem yang dikelola. Dalam beberapa kasus, eksploitasi terhadap kerentanan aplikasi web tersebut bahkan dapat berdampak lebih lanjut hingga menyebabkan akses tidak sah pada *server*.

Permasalahan tersebut berpotensi menyebabkan gangguan layanan, kebocoran data, kerusakan integritas sistem, serta menurunkan kepercayaan masyarakat terhadap layanan digital yang disediakan. Kondisi ini menunjukkan bahwa penerapan keamanan *website* perlu terus ditingkatkan untuk meminimalkan risiko serangan serta menjaga keberlangsungan layanan digital yang dikelola oleh instansi.

Berdasarkan permasalahan yang ditemukan, penulis mengimplementasikan sistem keamanan *website* berbasis *Secure Authentication* dan *Input Validation* dengan menerapkan konsep *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) pada lapisan aplikasi *(application layer)* untuk meningkatkan keamanan *autentikasi* pengguna, memperkuat validasi data masukan, mendeteksi aktivitas serangan, serta mencegah ancaman keamanan yang dapat mengganggu *website* dan layanan yang dikelola.

1.2 Tujuan Dan Manfaat Kerja Praktek

Adapun tujuan pelaksanaan Kerja Praktek adalah sebagai berikut:

1. Menerapkan ilmu pengetahuan dan keterampilan yang telah diperoleh selama perkuliahan ke dalam lingkungan kerja nyata.
2. Memahami proses kerja serta penerapan teknologi informasi dan keamanan sistem informasi pada instansi pemerintahan.
3. Menambah wawasan dan pengalaman mengenai dunia kerja profesional, serta mengembangkan kemampuan dalam menganalisis dan menyelesaikan permasalahan yang ditemui selama pelaksanaan Kerja Praktek.
4. Memperoleh pengalaman praktis dalam membangun dan menguji sistem keamanan *website* berbasis IDS dan IPS pada lapisan aplikasi.

Adapun manfaat yang diperoleh dari pelaksanaan Kerja Praktek adalah sebagai berikut:

1. Memperoleh pengalaman kerja dan pemahaman mengenai lingkungan kerja profesional.
2. Meningkatkan pengetahuan dan keterampilan dalam bidang teknologi informasi dan keamanan sistem informasi.
3. Mengembangkan kemampuan analisis, komunikasi, kerja sama tim, serta pemecahan masalah dalam lingkungan kerja.
4. Memperluas wawasan dan relasi profesional yang dapat mendukung pengembangan karier di masa mendatang.

1.3 Luaran Proyek Kerja Praktek

Luaran proyek yang dihasilkan berupa implementasi sistem keamanan *website* berbasis *Secure Authentication* dan *Input Validation* dengan menerapkan konsep *Intrusion Detection System (*IDS*)* dan *Intrusion Prevention System (*IPS*)* pada lapisan aplikasi *(application layer)*. Sistem tersebut dilengkapi dengan mekanisme autentikasi yang aman, validasi data masukan, fitur deteksi dan pencegahan serangan, *dashboard* monitoring keamanan, serta notifikasi serangan secara *real-time* melalui *Telegram*. Selain implementasi sistem, luaran yang dihasilkan juga mencakup lingkungan simulasi keamanan siber menggunakan konsep *Red Team* dan *Blue Team* yang terdiri atas website target dalam kondisi *vulnerable* dan *secure*, *roadmap* simulasi serangan dan pertahanan sistem. Luaran lainnya meliputi laporan hasil *penetration testing website*, serta presentasi dan demonstrasi hasil proyek kepada Bidang Statistik dan Persandian serta Bidang Layanan Aplikasi *E-Government* Diskominfotiksan Kota Dumai sebagai bentuk penyampaian hasil Kerja Praktek.