

BAB I

PENDAHULUAN

1.1 Latar Belakang Pemikiran KP

Kerja Praktik (KP) merupakan salah satu kegiatan akademik yang wajib diikuti oleh mahasiswa Politeknik Negeri Bengkalis sebagai bagian dari proses pembelajaran. Kegiatan ini bertujuan untuk memberikan pengalaman nyata kepada mahasiswa dalam memahami dunia kerja secara langsung, khususnya relevan dengan bidang keilmuan yang ditempuh. Melalui Kerja Praktik, mahasiswa diharapkan mampu mengimplementasikan pengetahuan teoritis yang telah diperoleh selama perkuliahan ke dalam praktik kerja di lingkungan industri.

Kerja Praktik (KP) juga berperan sebagai sarana pengembangan kompetensi bagi mahasiswa, baik dalam aspek keterampilan teknis (*hard skill*) maupun keterampilan non-teknis (*soft skill*). Keterampilan tersebut sangat dibutuhkan untuk menghadapi tuntutan dunia kerja yang semakin kompetitif. Setiawan et al. (2022) menyatakan bahwa kerja praktik bermanfaat untuk meningkatkan kepercayaan diri dalam mempersiapkan masa depan dalam karir.

PT Whello Indonesia Prima cabang Pekanbaru dipilih sebagai lokasi pelaksanaan Kerja Praktik karena memiliki keterkaitan dengan bidang keilmuan pada Jurusan Teknik Informatika, khususnya Program Studi Keamanan Sistem Informasi. PT Whello Indonesia Prima merupakan perusahaan yang bergerak dibidang digital marketing dan pengembangan teknologi informasi, dengan layanan meliputi, *Search Engine Optimization* (SEO), pembuatan website serta periklanan digital.

Seiring dengan meningkatnya penggunaan website sebagai media utama dalam kegiatan bisnis, aspek keamanan menjadi hal yang sangat penting untuk diperhatikan. Website memiliki potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab apabila tidak dikelola dengan baik.

Oleh karena itu, diperlukan suatu analisis keamanan untuk mengidentifikasi dan mengevaluasi potensi kerentanan yang terdapat pada website tersebut.

Berdasarkan hal tersebut, dalam pelaksanaan Kerja Praktik ini dilakukan analisis keamanan pada website menggunakan metode *Vulnerability Assessment* untuk mengetahui tingkat keamanan sistem serta memberikan rekomendasi perbaikan yang diperlukan.

1.2 Tujuan dan Manfaat KP

Tujuan dari pelaksanaan Kerja Praktik ini adalah sebagai berikut:

1. Mengimplementasikan pengetahuan yang telah diperoleh selama perkuliahan ke dalam praktik kerja nyata sesuai dengan bidang keilmuan.
2. Melakukan analisis kerentanan keamanan pada website menggunakan metode *Vulnerability Assessment*.
3. Memenuhi salah satu persyaratan akademik dalam menyelesaikan pendidikan Sarjana Terapan Keamanan Sistem Informasi di Politeknik Negeri Bengkalis.

Adapun manfaat dari pelaksanaan Kerja Praktik ini adalah sebagai berikut:

1. Meningkatkan pengetahuan, keterampilan dan pengalaman mahasiswa melalui keterlibatan langsung dalam kegiatan kerja di industri.
2. Melatih kemampuan analisis dalam mengidentifikasi dan mengevaluasi kerentanan keamanan sistem.
3. Mengembangkan kemampuan bekerja sama dalam tim serta memahami standar kerja di bidang teknologi informasi.

1.3 Luaran Proyek Kerja Praktik

Luaran utama dari pelaksanaan Kerja Praktik ini adalah laporan hasil analisis kerentanan keamanan pada website dengan menggunakan *Vulnerability Assessment*. Laporan ini disusun secara sistematis dan berisi hasil pengujian

keamanan yang telah dilakukan terhadap website yang menjadi objek pengujian. Selain laporan utama, luaran dari Kerja Praktik ini meliputi:

1. Dokumen hasil pengujian kerentanan (*Vulnerability Report*)

Dokumen ini berisi daftar kerentanan yang ditemukan disertai dengan tingkat risiko seperti *low*, *medium*, *high* dan *critical* untuk menunjukkan tingkat keparahan dari masing-masing temuan.

2. Dokumentasi proses pengujian

Dokumentasi ini memuat tahapan-tahapan pengujian yang dilakukan secara sistematis, mulai dari proses identifikasi target, pengumpulan informasi (*information gathering*), pemindaian (*scanning*), hingga analisis hasil.

3. Bukti pengujian (*Proof of Concept*)

Luaran ini berupa bukti pendukung atas kerentanan yang di temukan, seperti tangkapan layar (*screenshot*) atau hasil keluaran sistem yang menunjukkan bahwa kerentanan tersebut dapat diuji atau dieksploitasi dalam batasan yang telah ditentukan.