BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran Magang

Kerja Praktek (KP) merupakan salah satu kegiatan akademik yang memberikan kesempatan kepada mahasiswa untuk mengintegrasikan teori dan konsep keilmuan yang telah dipelajari selama perkuliahan dengan praktik secara langsung di dunia industri, dunia usaha, dan dunia kerja (IDUKA). Melalui kegiatan ini, mahasiswa diharapkan dapat meningkatkan pengetahuan, keterampilan, serta pengalaman profesional sesuai dengan bidang keahliannya sehingga memiliki kesiapan yang lebih baik dalam menghadapi dunia kerja setelah menyelesaikan pendidikan (Politeknik Negeri Bengkalis 2025).

Seiring berkembangnya transformasi digital, penggunaan internet dan aplikasi berbasis *website* terus mengalami peningkatan pada berbagai sektor, termasuk pemerintahan, pendidikan, kesehatan, maupun industri (Samsudiat et al. 2024). *Website* tidak lagi hanya dimanfaatkan sebagai media penyampaian informasi, tetapi juga sebagai sarana pelayanan, komunikasi, dan pendukung proses bisnis organisasi. Di balik kemudahan tersebut, aplikasi web juga menjadi salah satu target utama serangan siber karena menyimpan berbagai informasi penting dan dapat diakses melalui jaringan internet. Keamanan dan perlindungan data merupakan aspek penting dalam proses pembangunan *website* guna menjaga kerahasiaan informasi pribadi pengguna serta mencegah terjadinya akses atau penyalahgunaan data oleh pihak yang tidak memiliki hak (Widyaningrum et al. 2024).

Salah satu pendekatan yang banyak digunakan untuk mengevaluasi tingkat keamanan aplikasi web adalah *Vulnerability Assessment* (VA). VA merupakan proses untuk mengidentifikasi kerentanan atau kelemahan yang terdapat pada suatu sistem yang berpotensi dimanfaatkan oleh pihak yang tidak berwenang dalam melakukan serangan. Kerentanan tersebut dapat memengaruhi aspek kerahasiaan

(*confidentiality*), integritas (*integrity*), maupun ketersediaan (*availability*) sistem. Selain membantu mengidentifikasi kelemahan keamanan, *Vulnerability Assessment* juga berperan dalam meningkatkan kesadaran terhadap pentingnya keamanan informasi melalui identifikasi berbagai celah keamanan yang mungkin terdapat pada suatu sistem. Salah satu perangkat lunak yang banyak digunakan dalam proses *Vulnerability Assessment* adalah *OWASP ZAP (Open Web Application Security Project)* (Hasibuan et al. 2023).

OWASP merupakan organisasi nirlaba yang menyediakan panduan keamanan perangkat lunak khususnya *website* yang memberikan keamanan sistem melalui proyek open-source bersama dengan tools dari OWASP sebagai pendukung dalam pengujian sistem (Zahra et al. 2023). Sebagai panduan kerangka kerja yang dirilis oleh OWASP, *Web Security Testing Guide* (WSTG) merupakan panduan pengujian keamanan aplikasi web yang dikembangkan oleh *OWASP Foundation*. WSTG menyediakan kerangka kerja (*framework*) serta praktik terbaik (*best practices*) yang digunakan dalam proses pengujian keamanan aplikasi dan layanan berbasis web. Selain menjelaskan metodologi pengujian, WSTG juga memuat berbagai teknik pengujian yang dapat digunakan untuk mengidentifikasi kerentanan pada aplikasi web sehingga menjadi salah satu acuan yang banyak digunakan dalam kegiatan *security testing* dan *penetration testing* ("WSTG - v4.2 | OWASP Foundation," n.d.-a).

PT. Bumi Siak Pusako Zapin dipilih sebagai lokasi Kerja Praktek karena perusahaan yang bergerak di sektor hilir minyak dan gas bumi ini menerapkan pemanfaatan teknologi informasi untuk mendukung operasional, ketertiban administrasi, serta tata kelola perusahaan yang transparan. Sejalan dengan upaya peningkatan keamanan informasi dari infrastruktur lama perusahaan telah melakukan pengembangan *website* baru dengan menerapkan mekanisme autentikasi yang lebih modern melalui *Single Sign-On* (SSO) *Google dan One-Time Password* (OTP) berbasis email sebagai bentuk penguatan keamanan proses autentikasi. Halaman autentikasi merupakan salah satu komponen yang memiliki tingkat risiko tinggi karena menjadi target berbagai serangan, seperti *brute force*,

pencurian kredensial, eksploitasi sesi (*session hijacking*), maupun manipulasi parameter autentikasi (Buana et al. 2025).

Berdasarkan hasil pemeriksaan keamanan secara terbatas terhadap *website* perusahaan selama pelaksanaan Kerja Praktek, *website* perusahaan sebelumnya pernah ditemukan adanya indikasi penyisipan tautan (*link injection*) yang mengarah ke situs tidak sah, seperti situs perjudian daring maupun phishing. Temuan tersebut menunjukkan bahwa *website* pernah menjadi sasaran penyalahgunaan oleh pihak yang tidak bertanggung jawab sehingga berpotensi menurunkan kredibilitas perusahaan serta membahayakan pengunjung *website*. Meskipun permasalahan tersebut telah ditangani melalui evaluasi internal dan perusahaan telah melakukan pengembangan *website* baru, evaluasi yang dilakukan sebelumnya masih bersifat terbatas dan belum mengkaji kondisi keamanan *website* secara menyeluruh menggunakan metode *Vulnerability Assessment*. Kondisi ini menyebabkan tingkat keamanan *website* baru belum dapat diketahui secara komprehensif sehingga masih diperlukan proses identifikasi terhadap kemungkinan adanya kerentanan yang belum terdeteksi

Terlepas dari penerapan mekanisme autentikasi menggunakan SSO Google dan OTP, setiap perubahan arsitektur aplikasi web tetap membawa potensi risiko celah keamanan baru jika tidak dikonfigurasi dengan tepat. Metode *login* yang mengintegrasikan pihak ketiga dan pengiriman token digital rentan terhadap ancaman taktis seperti eksploitasi sesi (*session hijacking*), kerentanan penanganan API, hingga manipulasi logika *bypass login* (Halil and Mansur 2026). Oleh karena itu, diperlukan sebuah tindakan evaluasi berkala keamanan *website* BSP Zapin dan melindunginya dari serangan dimasa yang akan datang.

Berdasarkan permasalahan tersebut, penulis mengusulkan pelaksanaan pengujian keamanan menggunakan metode *Vulnerability Assessment* dengan memanfaatkan OWASP ZAP sebagai alat utama dalam proses identifikasi kerentanan. Serta analisis respons sistem secara terarah pada *website* baru PT. Bumi Siak Pusako Zapin. Melalui proses *information gathering*, *vulnerability scanning*, dan verifikasi teknis, selanjutnya, setiap temuan yang diperoleh diverifikasi melalui pengujian manual menggunakan Burp Suite serta teknik pengujian langsung

terhadap aplikasi untuk memastikan tingkat validitas kerentanan yang teridentifikasi. Hasil pengujian tersebut digunakan sebagai dasar dalam mengevaluasi efektivitas mekanisme keamanan yang telah diterapkan serta menyusun rekomendasi penguatan konfigurasi keamanan (*security hardening*), khususnya pada mekanisme autentikasi *Single Sign-On* (SSO) Google dan One-Time Password (OTP) berbasis email. Diharapkan melalui laporan Kerja Praktek yang berjudul "Analisis Keamanan *Website Company Profile* terhadap Potensi Serangan Siber Menggunakan Metode *Vulnerability Assessment* " ini, penulis dapat memberikan kontribusi nyata dalam menjamin integritas pertahanan perimeter sistem autentikasi pada PT. Bumi Siak Pusako Zapin.

1.2 Tujuan Dan Manfaat Magang

Tujuan dari pelaksanaan Kerja Praktek ini adalah sebagai berikut:

1. Menerapkan pengetahuan dan keterampilan teoritis yang telah diperoleh selama perkuliahan pada situasi nyata di dunia kerja, khususnya dalam bidang tata kelola dan keamanan sistem informasi.
2. Membantu PT. Bumi Siak Pusako Zapin dalam mengevaluasi tingkat keamanan pada *website* baru *company profile* melalui metode pemindaian kerentanan (*Vulnerability Assessment*) secara terarah.
3. Mengidentifikasi potensi celah keamanan (*vulnerability identification*) yang terdapat pada *website* berdasarkan hasil *information gathering*, *vulnerability scanning*, serta verifikasi teknis.
4. Untuk menguji efektivitas serta memberikan rekomendasi penguatan konfigurasi (*security hardening*) konkret terhadap implementasi *Single Sign-On* (*SSO*) Google dan *Multi-Factor Authentication* berbasis *OTP* Email yang telah diterapkan perusahaan.
5. Melakukan validasi terhadap temuan kerentanan menggunakan pengujian manual dengan Burp Suite dan teknik pengujian langsung untuk memastikan tingkat validitas hasil pemindaian.
6. Memperoleh pengalaman kerja secara langsung di lingkungan perusahaan serta meningkatkan pemahaman terhadap penerapan

standar keamanan informasi dalam dunia industri energi dan migas.

Adapun manfaat dari pelaksanaan Kerja Praktek ini adalah sebagai berikut:

1. Mendapatkan pengalaman langsung dalam dunia kerja profesional, khususnya pada pemeliharaan dan pengujian keamanan teknologi informasi di lingkungan perusahaan minyak dan gas bumi.
2. Meningkatkan kemampuan analisis dalam mengidentifikasi, mengukur tingkat risiko, serta mengevaluasi kerentanan pada aplikasi web berbasis publik.
3. Menambah pemahaman mengenai proses validasi arsitektur pertahanan perimeter serta ketahanan sistem autentikasi modern yang mengintegrasikan teknologi *SSO* Google dan *OTP* berbasis email.
4. Mengasah kemampuan berpikir kritis dalam mengevaluasi keandalan fitur *login* baru terhadap potensi ancaman taktis seperti eksploitasi sesi, *brute force*, atau manipulasi logika *bypass* autentikasi.
5. Membantu perusahaan dalam memetakan kondisi keamanan terkini pada aset layanan digital terbaru serta memberikan panduan teknis penguatan sistem untuk mencegah insiden pengambilalihan hak akses secara ilegal.
6. Meningkatkan kesiapan memasuki dunia kerja melalui penerapan ilmu keamanan sistem informasi secara langsung di lingkungan industri.
7. Menumbuhkan sikap profesional, tanggung jawab, kedisiplinan, ketelitian tinggi, dan etika kerja yang baik dalam berinteraksi di lingkungan industri.

1.3 Luaran Proyek Magang

Adapun luaran proyek magang yang dihasilkan adalah sebagai berikut:

1. Laporan Hasil Pemindaian Otomatis (Automated Vulnerability Scan Report)

   Dokumen teknis hasil pemindaian menggunakan OWASP ZAP terhadap website *company profile* PT. Bumi Siak Pusako Zapin (bspz.co.id), memuat daftar temuan celah keamanan, evaluasi konfigurasi *header* keamanan, dan status kerentanan pada sisi perimeter

sistem.

2. Dokumen Bukti Pengujian Manual (*Proof of Concept - PoC* via Burp Suite)

   Kumpulan bukti visual, riwayat *intercept request*, dan manipulasi parameter lalu lintas data menggunakan Burp Suite untuk memvalidasi ketahanan logika *login*, aliran data *SSO* Google, serta pengiriman token *OTP* Email.

3. Bukti Validasi Manual (Manual Verification via Burp Suite)
   Dokumentasi pendukung berupa hasil *intercept request* dan pengujian manual menggunakan Burp Suite, untuk memvalidasi temuan OWASP ZAP terkait ketahanan autentikasi *login*, integrasi SSO Google, serta pengiriman token OTP Email.

4. Panduan Penguatan Konfigurasi Keamanan (Security Hardening Guidance)

   Rekomendasi teknis berbasis temuan dan referensi OWASP ZAP bagi tim IT perusahaan untuk memperketat kebijakan keamanan, meliputi pembatasan domain pada fitur SSO Google serta penerapan *rate-limiting* dan kedaluwarsa token OTP Email.

5. Alur Kerja Pengujian Keamanan Sistem Autentikasi
   Dokumentasi tahapan metodologi *vulnerability assessment* yang diterapkan selama Kerja Praktek, mulai dari *information gathering*, pemindaian dengan OWASP ZAP, hingga verifikasi manual pada area kontrol akses perusahaan.

6. Dokumentasi Analisis Respons Server

   Catatan teknis mengenai perilaku halaman autentikasi baru dalam menangani berbagai variasi input pengguna, sebagai bagian dari analisis untuk memastikan tidak terjadi kebocoran informasi konfigurasi internal sistem.

7. Log Lalu Lintas Data (HTTP History Log)

   Rekaman log *request* dan *response* HTTP/HTTPS dari OWASP ZAP dan Burp Suite sebagai bukti pendukung proses pengujian.