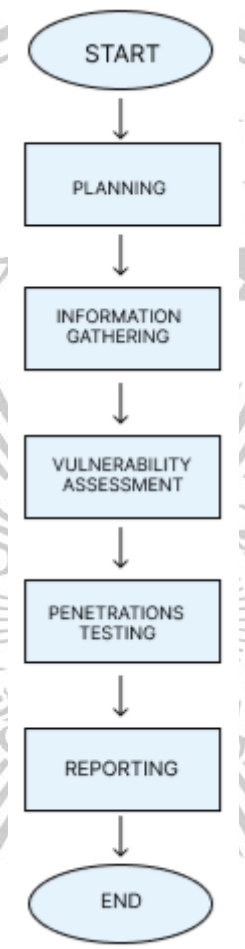
BAB III
METODE PENELITIAN

3.1 Alur Penelitian

Metodologi dalam penelitihan ini menggunakan beberapa tahapan dari penetrations testing sampai reporting. Alur dari penelitihan ini adalah sebagai berikut:



Gambar 3. 1 Alur Penelitian

3.2 *Planning*

Pada fase *Planning*, akan dibuat perencanaan mengenai lingkup dari penelitian *Penetration Testing*. Ini meliputi menentukan ruang lingkup dan tujuan pengujian, termasuk sistem yang akan diuji serta metode pengujian yang akan digunakan[6]. Ini juga mencakup identifikasi sistem yang akan diuji dan teknik pengujian yang akan digunakan. Pengumpulan data seperti nama jaringan, *domain server*, dan *server email* dilakukan untuk memahami lebih dalam cara kerja target serta potensi kerentanan yang mungkin ada. [13]. Proses *penetration testing* pada *website*, langkah awal yang diperlukan adalah

dilakukan perencanaan. Perencanaan yang dimaksud mencakup identifikasi hal untuk di tes, waktu yang dibutuhkan, alat atau tools yang diperlukan. Pada penelitian ini standart kerentanan keamanan yang digunakan yaitu OWASP Top 10 2021. Dalam standart OWASP Top 10 terdapat 10 kerentanan keamanan *website*. Perlu adanya perencanaan untuk dilakukan 10 kerentanan ini, tergantung kerentanan yang didapat pada tahap *information gathering* dan *vulnerability assessment*.

3.3 *Information Gathering*

Setelah perencanaan telah dibuat, selanjutnya adalah melakukan tahapan pengumpulan informasi dan melakukan analisis terhadap informasi-informasi yang diperoleh dari target. fase *Gathering-Information*. Pada fase ini, *pentester* melakukan analisis terhadap informasi yang tersedia secara publik, proses yang dikenal sebagai *Open Source Intelligence (OSINT) gathering* [14]. Informasi yang dikumpulkan adalah informasi mengenai website yang akan diuji, seperti alamat IP, struktur jaringan, versi perangkat lunak, serta sumber daya dan layanan yang mungkin rentan. Pada tahap *information gathering* menggunakan beberapa *tools* yaitu nmap, wapplyzer dan recon-ng.

3.4 *Vulnerability Assessment* (scanning secara otomatis)

Penelitian ini menggunakan *vulnerability assessment* yang dilakukan dengan *automated testing*. *Vulnerability assessments* yaitu strategi yang mengikuti pendekatan sistematis dan proaktif untuk menemukan sebuah kerentanan [8]. dengan pemilihan teknik tersebut secara sistematis akan mendapatkan akurasi yang baik dalam menemukan kerentanan dan mempercepat waktu penelitian. Pada vulnerability Assessment ini menggunakan tools OWASP ZAP dan Nessus.

3.4.1 OWASP ZAP

OWASP ZAP adalah alat pemindai kerentanan yang dikembangkan oleh organisasi OWASP. Alat ini merupakan salah satu proyek paling aktif dari OWASP karena terus dikembangkan dan bersifat *open-source*, memungkinkan kontribusi dari siapa pun dalam pengembangannya.[9]**.** Pada penelitian ini menggunakan OWASP ZAP dengan fitur proxy spidering(pemindaian secara otomatis). Hasil dari OWASP ZAP yaitu memberikan laporan kerentanan yang didalamnya berisi ringaksan

kerentanan dan resiko dari kerentanan tersebut.

3.4.2 Nessus

Nessus adalah software yang dikelola oleh Tenable.sc. yang bisa kita gunakan dengan cara berlangganan dan atau bisa gunakan versi gratis.[10] Hasil dari Nessus yaitu ringakasan kerentanan yang mencakup tingkat keparahan(Critical, High, Medium dan Low) dan Rekomendasi perbaikan mencakup saran spesifik untuk memperbaiki atau mengatasi, seperti pembaruan perangkat lunak, perubahan konfigurasi, atau penerapan patch keamanan.

3.5 Penetrations Testing

Penetration Testing adalah sebuah metode pengujian terhadap sebuah sistem atau jaringan komputer yang bertujuan untuk mengevaluasi keamanan sistem atau jaringan komputer[4]. Pengujian kerentanan menggunakan tools OWASP ZAP dengan berdasarkan parameter keamanan OWASP TOP 10 2021. OWASP Top 10, atau sering disebut sebagai OWASP 10, adalah sebuah metodologi yang dikeluarkan oleh komunitas OWASP. Metodologi ini mencakup 10 daftar utama celah keamanan yang berpotensi mengancam keamanan sebuah website. Daftar ini terus diperbarui dan berkembang seiring dengan perkembangan teknologi *website* yang terus berubah[11]. Pada *penetration testing* Dilakukan beberapa pengujian dari informasi yang sudah di analisis dan perencanaan yang sudah dibuat pada tahap sebelumnya tergantung pada kerentanan yang ditemukan pada tahapan vulnerability assessment dan information gathering. Penetration ini akan memakai hasil yang didapat dari pencarian kerentanan dan hasil dari beberapa informasi yang sudah didapatkan pada proses sebelumnya. Acuan untuk melakukan sebuah tes penetrasi ini adalah berdasarkan pada framework OWASP Top 10 Web Application Security Risks.

3.6 Reporting (analisis dari tahapan pentest)

Setelah melakukan empat tahapan uji kerentanan, langkah terakhir yang perlu dilakukan adalah membuat laporan yang komprehensif, dan disusun untuk menjelaskan temuan, kerentanan yang ditemukan, tingkat keparahan, serta rekomendasi perbaikan atas kegiatan penetration testing yang dilakukan. Pelaporan merupakan tahap penelitian menganalisis hasil penyerangan. Pada tahap pelaporan, selain menganalisis hasil, juga memberikan kontrol atas rekomendasi untuk membuat website PT SekarLaut TBK lebih aman[15].