BAB III
METODOLOGI PENELITIAN

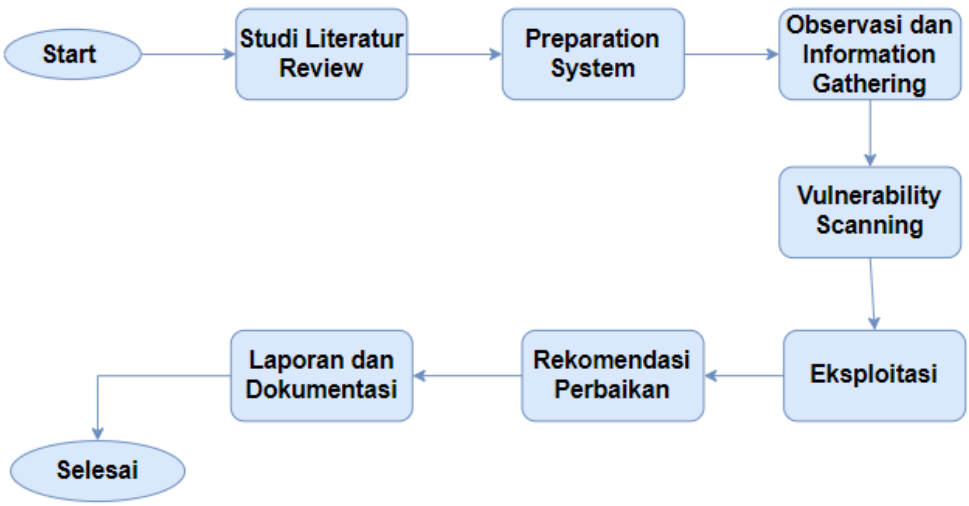
3.1 Pendekatan Penelitian

Metode penetrasi digunakan pada web sihebat.tasikmalayakota.go.id yang memilki kerentanan terhadap serangan *SQL Injection* dengan menggunakan pendekatan eksperimen. Pengujian dilakukan menggunakan dua teknik *inferensial SQL Injection*, yaitu *Boolean-based Blind dan time-based blind,* untuk mengetahui dampaknya terhadap sistem target.

Penelitian ini dilakukan pada website sihebat.tasikmalaykota.go.id yang dikelola oleh Dinas Sosial Kota Tasikmalaya, selama jangka waktu dari Desember 2024 hingga mei 2025.

3.2 Diagram Alur Penelitian

Diagram alur penelitian terdapat pada gambar 3.1



Gambar 3. 1 Diagram Alur Penelitian

3.3 Studi Literatur

Studi literatur digunakan untuk bahan rujukan diskusi dari hasil penelitian, *studi literatur* juga bertujuan untuk mengetahui berbagai teori yang relevan dengan masalah ruang dihadapi. Teori yang terkait dengan masalah penelitian yang digunakan ialah *penetration testing, SQl Injection*, serta penggunaan *tools* seperti SQLMap, OWASP ZAP, Nikto, Nslookup dan Nmap. Literatur dikumpulkan dari jurnal ilmiah, artikel teknis, dan dokumen stanar keamanan informasi.

Kemudian, data dari sumber tersebut dikumpulkan dengan menggunakan teknik pencarian database akademik seperti *Google Scholar, Publish Or Perish, IEEE Xplore*, dan lainnya. Selanjutnya, jurnal tersebut di analisis untuk menemukan materi penting yang diperlukan untuk selanjutnya disusun dalam bentuk tulisan yang sistematis.

3.4 Persiapan Sistem

Menyiapkan sistem yang akan digunakan dalam penelitian termasuk dalam persiapan sistem. Tujuan dari tahapan ini ialah untuk memastikan bahwa sistem siap untuk pengujian dan analisis. Langkah awal sebelum pengujian mempersiapkan sitem dan lingkungan pengujian:

1. Menentukan target website berbasis web dengan potensi celah keamanan (menggunakan *Google dorking).*
2. Menyiapkan *tools* pengujian diantaranya Kali Linux, SQLMap, Nikto, Nmap, Nslookup, OWASP ZAP dan lainnya.
3. Melakukan konfigurasi jaringan dan koneksi ke domain target.

Karena linux memiliki berbagai alat keamanan yang diperlukan untuk pengujian SQL *Injection*, maka kali linux digunakan sebagai sistem operasi utama dalam pengujian penetrasi. Pada aplikasi berbasis web, dan SQLMap digunakan untuk menemukan dan mengeksploitasi kerentanan *SQL Injection.*

3.5 Observasi dan *Information Gathering*

Menentukan tujuan penelitian dan metode yang akan digunakan, data yang dikumpulkan selama observasi disesuaikan dengan desain yang telah ditetapkan, dapat berupa catatan, foto, atau rekaman video, dan lainnya. Setelah itu, data disusun dan dikategorikan untuk memudahkan analisis lebih lanjut.

Pengujian menggunakan alamat domain website untuk mencari informasi tentang alamat IP target. Melakukan ping ke domain sistem dan menggunakan Nmap dan Nslookup port *scanning* dapat mengumpulkan data dan versi database target, dan alat lainnya yang digunakan untuk mengetahui informasi target. Proses ini meliputi:

1. Mengetahui alamat IP dan port target menggunakan Nslookup dan Nmap.
2. Menguji konektivitas dengan melakukan ping pada website target.

3.6 Vulnerability Scanning

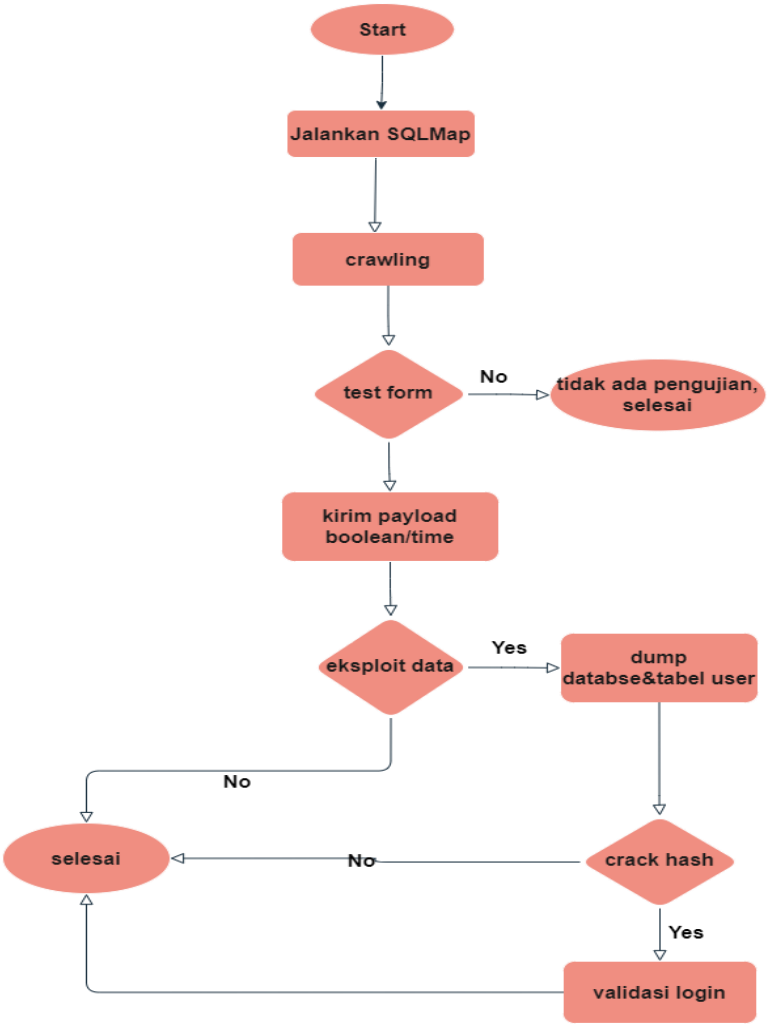
Dilakukan dengan *tools* berikut:

1. Nikto digunakan untuk memindai kerentanan server, file tersembunyi dan konfigurasi yang tidak aman.
2. OWASP ZAP digunakan untuk melakukan *scanning* aktif, crawling dan analisis header keamanan digunakan untuk pemindaian kerentanan pada aplikasi berbasis web. Menggunakan spider dan ajax spider. ZAP

mampu memindai beberapa kerentanan dengan melakukan crawling direktori. Hasil *scanning* digunakan untuk mengidentifiaksi potensi celah yang bisa dieksploitasi lebih lanjut.

3.7 Eksploitasi Kerentanan

Eksplotasi dilakukan menggunakan SQLMap, dengan pengujian pada *form login* dan parameter yang ditemukan rentan, alur eksploitasi terdapat pada gambar 3.2



Gambar 3. 2 Alur Pengujian menggunakan SQLMap

Parameter utama yang digunakan dalam eksekusi SQLMap adalah:

1. --u: Url target.
2. --forms: Menguji form HTML.
3. --batch: Otomatisasi proses.
4. --level=5 dan --risk=3: Meningkatkan intensitas eksploitasi
5. --crawl=2: Mengeksplorasi kedalaman direktori.

Menggunakan parameter pada proses eksploitasi, untuk meningkatkan intensitas proses pada SQLMap, sehingga penelitian ini memberikan metodologi sekploitasi yang sistematis dan efektif untuk menemukan kerentanan tersembunyi yang tidak ditemukan dengan metode biasa.

Eksploitasi dilakukan dengan dua pendekatan:

1. *Boolean-based blind SQL Injection* yaitu mengamati perubahan respon berdasarkan kondisi logika.
2. *Time-based blind SQL Injection* yaitu mengamati waktu respon berdasarkan perintah *delay.*

SQLMap juga digunakan untuk:

1. Mengambil daftar database dan tabel.
2. Mengekstrak data sensitif (seperti username dan password dalam bentuk hash).
3. Mengidentifiaksi *hash* dan mendeskripsi dengan *tools online*.

3.8 Dokumentasi Dan Laporan

Tahapan terkahir pada penelitian ini yaitu laporan dan dokumentasi. Tujuan dari tahapan ini ialah untuk mencatat seluruh proses penelitian dan membuat

laporan yang lengkap tentang seluruh proses penelitian. Seluruh proses dan hasil pengujian didokumentasikan, termasuk:

1. Hasil *scanning* dan eksploitasi.
2. Tangkapan layar proses eksploitasi.
3. Rekomendasi mitigasi berdasarkan hasil *scanning.*

Laporan disusun secara sistematis dan digunakan sebagai bahan evaluasi keamanan aplikasi web, serta sebagai dasar saran pengamanan ke depan. Terakhir, laporan penelitian dipublikasikan dalam format yang sesuai, seperti jurnal ilmiah, konferensi, atau repositori universitas.