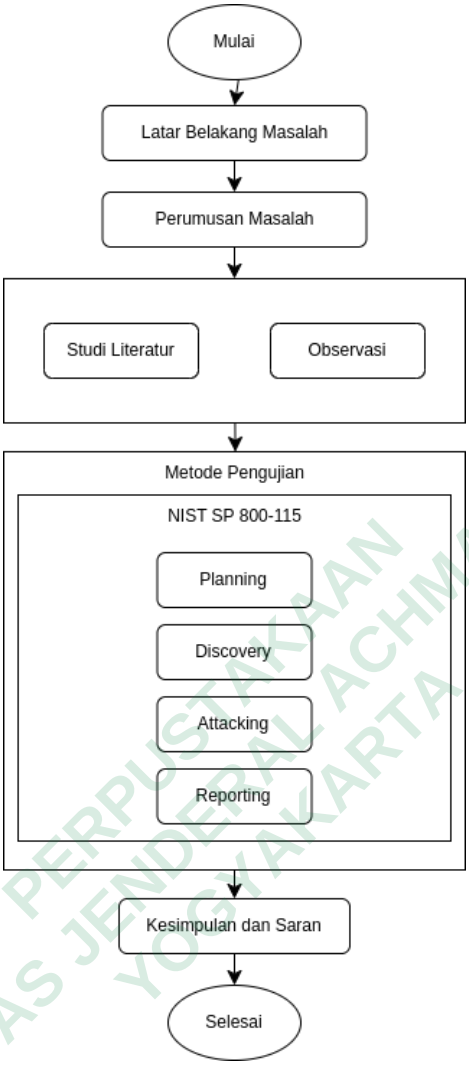
# BAB 3
# METODE PENELITIAN

Penelitian ini mengimplementasikan metode NIST 800-115 untuk mengidentifikasi kerentanan yang terdapat pada aplikasi web layanan Sistem Informasi Calon Mahasiswa Baru (SICAMA) Universitas Jenderal Achmad Yani Yogyakarta yaitu *https://sicama.unjaya.ac.id*. Fokus utama penelitian ini terletak pada tahap identifikasi kerentanan, yang merupakan bagian penting dalam proses *assessment*. Dalam tahap *assessment* ini, peneliti memanfaatkan sejumlah *tools* yang dirancang khusus untuk analisis keamanan pada *website*. Antara lain, digunakan *Nikto Scanner, ZAP, Nmap*, serta *Helium Security*. Penggunaan alat-alat ini memungkinkan peneliti untuk mengidentifikasi celah keamanan potensial dalam struktur dan fungsionalitas aplikasi web layanan SICAMA Universitas Jenderal Achmad Yani Yogyakarta. Berikut alur penelitian yang digunakan.






**Gambar 3.1** Alur Penelitian

Gambar 3.1 menunjukkan serangkaian langkah yang akan dilakukan dalam proses penelitian ini. Mulai dari langkah awal persiapan sampai tahap pelaporan, setiap prosedur dijelaskan secara rinci. Langkah pertama melibatkan perumusan masalah yang terdiri dari studi literatur dan observasi, dilanjutkan dengan metode pengujian dengan menggunakan metode NIST SP-800-115 yang terdiri dari perencanaan (*planning*), penemuan (*discovery*), penyerangan (*attacking*) dan pelaporan (*reporting*).

## 3.1 BAHAN DAN ALAT PENELITIAN

Penelitian ini menggunakan SICAMA Universitas Jenderal Achmad Yani Yogyakarta sebagai objek untuk penilaian kerentanan, khususnya dalam konteks penyediaan informasi bagi calon mahasiswa baru. Dalam menjalankan penelitian ini, metodologi yang digunakan mengacu pada NIST SP 800-115 (*National Institute of Standards and Technology Special Publication 800-115*), yang memberikan panduan komprehensif untuk teknik pengujian dan penilaian keamanan. Selain itu, penelitian ini juga menggunakan OWASP Top 10 sebagai acuan pelaporan, yang merupakan daftar sepuluh ancaman keamanan aplikasi web paling kritis yang diidentifikasi oleh Open Web Application Security Project (OWASP).

Penelitian ini menggunakan laptop dengan spesifikasi yang cukup untuk menjalankan *Operating System* dan *software* dalam menguji dan melakukan penilaian kerentanan pada SICAMA Universitas Jenderal Achmad Yani Yogyakarta serta menggunakan *software* pengujian kerentanan untuk menguji kerentanan pada *website*. Spesifikasi laptop yang dipergunakan untuk menjalankan *software* penelitian adalah sebagai berikut:

*Operating System* : *Ubuntu 22.04.4 LTS Jammy*
*Processor* : *10th Gen Intel Core i3 -1005G1*
*Memory* : 8 GB
*Storage* : 256GB (SSD)

Berikut merupakan *software* yang akan digunakan untuk menganalisis kerentanan pada *website* SICAMA Universitas Jenderal Achmad Yani Yogyakarta:

**Tabel 3.1** *Software* yang digunakan berserta fungsinya

| No | *Software* | Fungsi |
|---|---|---|
| 1 | *Netcraft* | Digunakan untuk mencari informasi tentang *website*, layanan web, dan infrastruktur yang digunakan pada web. |

| | | |
|---|---|---|
| 2 | *Network Mapper* (Nmap) 7.80 | Digunakan untuk memindai, memetakan jaringan komputer dan mendeteksi sistem operasi. |
| 3 | *Nikto Scanner* 2.1.5 | Digunakan untuk memindai dan menguji keamanan *website* secara umum seperti konfigurasi, layanan menggunakan *command line interface*. |
| 4 | ZAP (*Zed Attack Proxy*) 2.14.0 | Digunakan dalam menguji keamanan web meliputi pemindaian kerentanan, *proxy* intersepsi, eksploitasi, *penetration testing* dan dokumentasi. |
| 6 | *Web Helium Security* | Digunakan untuk mengidentifikasi kerentanan dan melakukan pengujian secara *automation vulnerability assessment* melalui *web based vulnerability assessment.* |



## 3.2 JALAN PENELITIAN

Pengujian pada penelitian ini menggunakan metodologi NIST SP 800-115 yang memiliki empat tahapan diantaranya perencanaan (*planning*), Penemuan (*discovery*), penyerangan (*attacking*), dan pelaporan (*reporting*) (Peter, 2023). Adapun tujuan menggunakan metodologi tersebut untuk memudahkan ketika ingin melakukan analisis dan pengujian pada uji penetrasi *website*, dengan melalui beberapa tahapan yang dilakukan sesuai dengan mekanisme dari batasan informasi serta tujuan dilakukannya pengujian. Berdasarkan uraian dari metodologi dan metode yang digunakan pada penelitian ini, untuk lebih detailnya terkait dari yang dilakukan pada setiap proses tahapan pengujiannya dijelaskan pada poin-poin dibawah ini:

1. Perencanaan (*Planning*)

   Tahap awal dalam penelitian ini adalah perencanaan (planning) dan persiapan (preparation), yang melibatkan pertukaran informasi, perencanaan, dan persiapan yang matang. Langkah pertama adalah

mengurus surat izin penelitian kepada pihak pengelola aplikasi web *sicama.unjaya.ac.id* untuk mendapatkan akses dan persetujuan. Setelah izin diperoleh, peneliti melakukan observasi awal terhadap platform untuk memahami konteks dan operasionalnya. Selain itu, peneliti juga melakukan studi literatur yang relevan untuk mengumpulkan informasi dan teori yang mendukung penelitian. Studi literatur ini penting untuk memahami penelitian sebelumnya terkait sistem informasi akademik dan metode evaluasi yang digunakan, sehingga dapat merancang metodologi yang tepat.

2. Penemuan (*Discovery*)

   Pada tahap *discovery* ini, yang merupakan tahapan dalam proses *information gathering* atau pengumpulan informasi terkait *website* target pengujian, bertujuan untuk mengumpulkan informasi yang berkaitan dengan *website* target, mencari *port* yang terbuka, dan lainnya. Tahapan ini terdiri dari dua tahap, yaitu *information gathering* dan *vulnerability scanning*. Pada tahap *information gathering*, dilakukan pengumpulan informasi mengenai informasi umum mengenai infrastruktur *website* yang telah dijabarkan pada bagian hasil dan pembahasan, khususnya sub bagian struktur dan fungsi website menggunakan website *sitereport.netcraft.com* dan *Network Mapper* (Nmap). Kemudian, pada tahap *vulnerability scanning*, dilakukan pemindaian kerentanan pada website tersebut, dengan penjelasannya terdapat pada sub bagian pemindaian *website* menggunakan Nikto Scanner.

3. Pengujian (*Attacking*)

   Tahap *attacking* merupakan tahapan yang dilakukan untuk menguji kerentanan *website* yang telah didapatkan dari proses sebelumnya dari mulai pengumpulan data dan informasi dari *website* target kemudian pemindaian kerentanan yang kemudian ditindaklanjuti pada proses pengujian *attacking* ini. Pada proses ini menggunakan, ZAP *(Zed Attack Proxy)*, dan *Helium Security* menguji kerentanan pada keamanan *website* target.

4. Pelaporan (*Reporting*)

Pada tahap *reporting* ini ialah berfokus pada melaporkan hasil pengujian kerentanan serta menyajikan daftar kerentanan OWASP TOP 10 tahun 2021 untuk kemudian diberikan keterangan atas hasil dan temuan dari pengujian yang telah dilakukan.