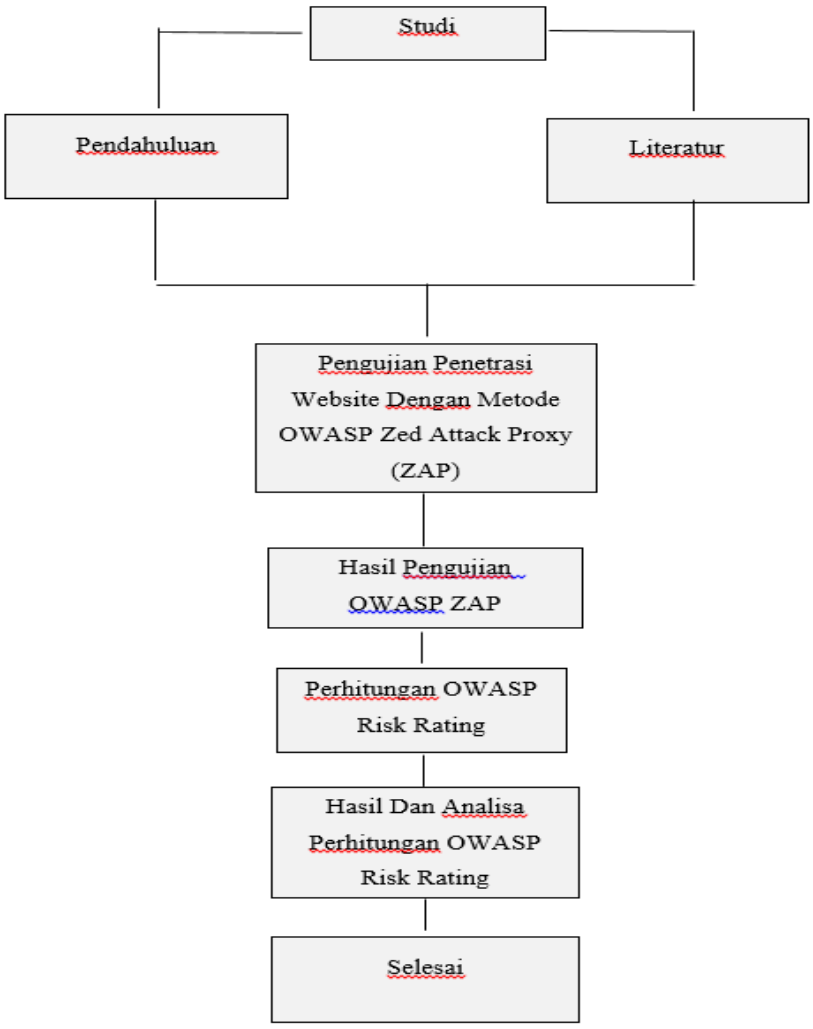
BAB III

METODOLOGI PENELITIAN

Pada penelitian ini diusulkan beberapa skenario penyusunan untuk mendeteksi, mengklasifikasikan, dan memahami serangan. Berikut tahapan yang dilakukan untuk menyelesaikan penelitian diantaranya studi yang terdiri dari pendahuluan dan observasi [4], Teknik pengumpulan data atau informasi ini dilakukan dengan tujuan pengamatan masalah apa yang terjadi dan pendalaman permasalahan yang telah terjadi pada Website SIMPKN Informatika.

Struktur tahapan yang dilakukan penelitian ini dengan rancangan sebagai berikut:

Gambar 3



Gambar 3 Alur Penelitian

3.1 Studi Pendahuluan

Tahapan Studi Pendahuluan bertujuan untuk mendapatkan informasi terkait Website SIMPKN Informatika. Wawancara dilakukan berguna untuk mengecek kebenaran Informasi mengenai website tersebut.

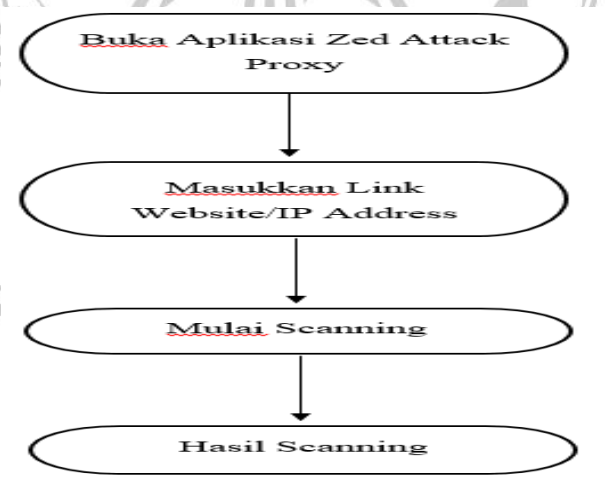
3.2 Studi Literatur

Tahapan Studi Literatur didapatkan melalui membaca jurnal, artikel maupun Sumber lain dari internet. Tahapan ini bertujuan untuk mendapatkan informasi dari sumber-Sumber lainnya yang nanti nya dapat dijadikan acuan dan penjelasan terkait kasus penelitian.

3.3 Pengujian Penetrasi Website Dengan Metode OWASP Zed Attack Proxy (ZAP)

Tahapan pengujian penetration test menggunakan perangkat lunak OWASP Zed Attack Proxy (ZAP). OWASP Zed Attack Proxy (ZAP) adalah metode scanning website untuk menemukan kerentanan-kerentanan yang ada pada website, nantinya kerentanan tersebut akan dianalisa seberapa berdampaknya terhadap kinerja website. Website yang diuji adalah Website SIMPKN Informatika yang merupakan sistem pendaftaran PKN (Program Kerja Nyata) dan MBKM (Merdeka Belajar Kampus Merdeka) yang ada pada Prodi Informatika. Untuk langkah-langkah penetration ditunjukkan pada skema dibawah ini:

Gambar 3.3



Gambar 3.3 Alur Penggunaan Tools ZAP (Zed Attack Proxy)

Hasil scanning diperoleh Setelah proses pengujian selesai dilakukan, beberapa hasil uji inilah yang merupakan kerentanan-kerentanan yang ada pada website.

3.4 Hasil Pengujian OWASP ZAP

Tahapan ini berisi penjelasan mengenai hasil yang didapatkan dari pengujian keamanan Website SIMPKN Informatika. Analisa diperoleh Setelah mendapatkan hasil pengujian keamanan website menggunakan OWASP Zed Attack Proxy (ZAP).

3.5 Perhitungan OWASP Risk Rating

Tahapan perhitungan Risk Rating ini dilakukan guna mengidentifikasi resiko, Faktor untuk memperkirakan dampak, menentukan tingkat keparahan resiko, dan memutuskan apa yang harus diperbaiki.

3.6 Hasil Dan Analisa Perhitungan OWASP Risk Rating

Tahapan berisi analisa hasil yang diperoleh dari perhitungan resiko kerentanan pada website menggunakan OWASP Risk Rating. Tabel tingkat kemungkinan seperti tabel dibawah ini dapat dilihat Pada **Tabel 3.6.1**:

Tabel 3.6.1 Tabel Tingkat Kemungkinan (Likelihood Factors)

Likelihood factors	
Threat Agent Factors	
Skills required	Some technical skills [3]
Motive	Possible reward [4]
Opportunity	Special access or resources required [4]
Population Size	Partners [5]
Vulnerability Factors	
Easy of Discovery	Automated tools available [9]
Ease of Exploit	Automated tools available [9]
Awareness	Hidden [4]
Intrusion Detection	Logged without review [8]

Tabel Tingkat kemungkinan didapatkan yang merupakan tingkat keamanan website lalu selanjutnya menentukan nilai tingkat dampak resiko keamanan secara keseluruhan yang dapat dilihat Pada **Tabel 3.6.2** dibawah ini:

Tabel 3.6.2 Tabel Tingkat Dampak Resiko (Impact Factors)

Impact factors	
Technical Impact Factors	
Loss of confidentiality	Extensive non-sensitive data disclosed [6]
Loss of Integrity	Minimal slightly corrupt data [1]
Loss of Availability	Minimal secondary services interrupted [1]
Loss of Accountability	Attack fully traceable to individual [1]

Business Impact Factors	
Financial damage	Minor effect on annual profit [3]
Reputation damage	Loss of major accounts [4]
Non-Compliance	Not Applicable [0]
Privacy violation	One individual [3]

3.7 Selesai

Hasil yang didapatkan dari analisa pengujian keamanan website menggunakan perangkat lunak OWASP Zed Attack Proxy (ZAP) dan pengujian OWASP Risk Rating kalkulator. Hasil Analisa ditampilkan berdasarkan hasil yang telah diperoleh dengan tujuan untuk menambah keamanan website. Pada bagian ini juga terdapat Mitigation atau upaya pencegahan apabila terjadi penyerangan yang nantinya dapat meningkatkan keamananan pada website. Mitigation juga diklasifikasi berdasarkan tingkat kerentanan dari Kerentanan Sedang, Kerentanan Rendah dan Kerentanan Tidak berdampak (Informatif).