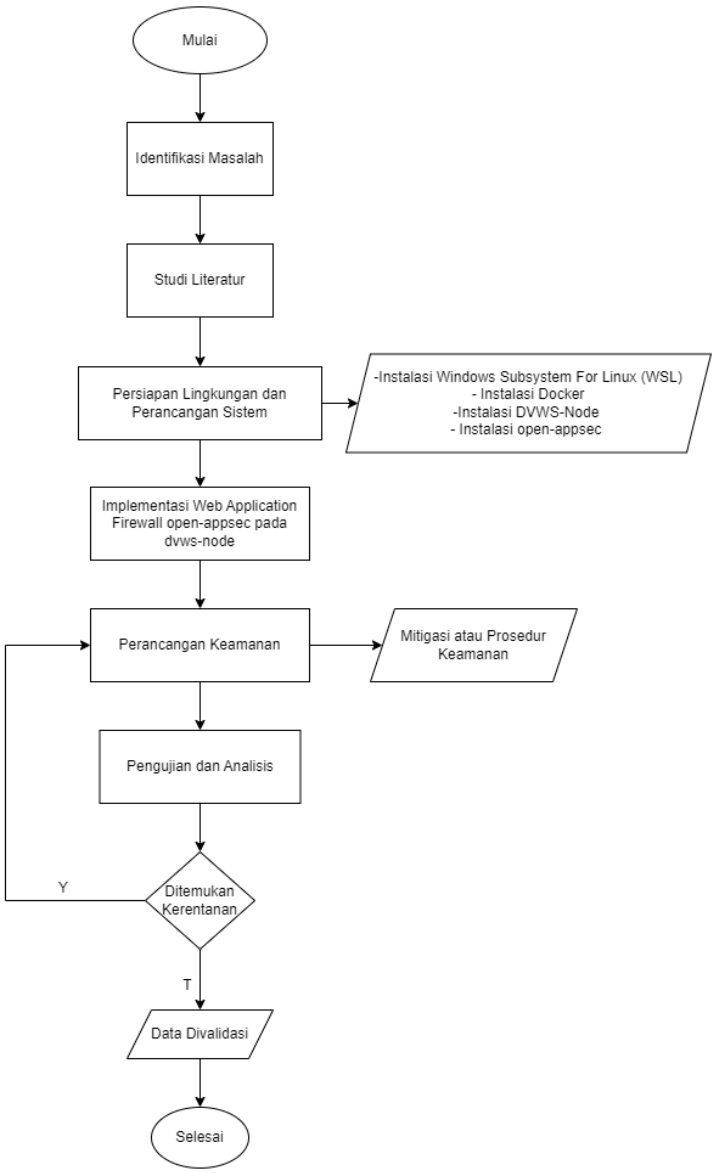
BAB III
METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Tahapan Penelitian merupakan gambaran langkah-langkah yang dilakukan dalam penelitian atau pengembangan untuk mencapai tujuan tertentu. Ini adalah langkah-langkah dan prosedur yang dirancang untuk mengumpulkan data, menganalisis informasi, dan mencapai kesimpulan dalam sebuah studi atau proyek.



Gambar 3.1 Tahapan Penelitian

3.1.1 Identifikasi Masalah

Pada tahap awal ini, langkah yang diambil adalah mengidentifikasi masalah yang ada terkait dengan kerentanan Web API, khususnya pada aplikasi Damn Vulnerable Web Services-Node (DVWS-Node). Identifikasi ini bertujuan untuk memahami sejauh mana sistem tersebut rentan terhadap serangan dan potensi ancaman yang dapat dihadapi. Dengan mengidentifikasi masalah ini, penelitian ini dapat fokus pada aspek-aspek yang perlu diperbaiki atau diperkuat untuk meningkatkan keamanan sistem.

3.1.2 Studi Literatur

Setelah masalah diidentifikasi, langkah selanjutnya adalah melakukan studi literatur. Tahap ini melibatkan pencarian dan pengumpulan informasi dari berbagai sumber yang relevan seperti buku yaitu Research and implementation of WEB application firewall based on feature matching artikel atau jurnal ilmiah seperti; Analisis Kerentanan Web DVWA Yang Menggunakan Web Application Firewall Dengan Menggunakan Standar OWASP, Implementasi Web Application Firewall (WAF) Mod Security dan Pengujian Menggunakan SQL *Injection*, Penerapan Sistem Keamanan Web Menggunakan Metode Web Aplication Firewall, Analisis Performance Web Application Firewall ModSecurity, Development of Vulnerable Web Application Based on OWASP API Security Risks, serta informasi lainnya yang berkaitan dengan penelitian ini.

3.1.3 Persiapan lingkungan dan Perancangan sistem

Pada tahap ini, dilakukan persiapan lingkungan dan perancangan perangkat lunak atau alat yang dibutuhkan untuk penelitian. Fokus utama adalah menginstal dan mengkonfigurasi Web Application Firewall (WAF) dari Open-appsec pada sistem DVWS-Node. Langkah-langkah instalasi dan perancangan ini untuk memastikan bahwa WAF dapat berfungsi dengan baik dan dapat mengidentifikasi serta memitigasi ancaman yang terdeteksi. Proses ini juga mencakup pengaturan aturan-aturan keamanan yang sesuai dengan kebutuhan aplikasi dan lingkungan operasionalnya.

3.1.4 Melakukan Uji Kerentanan

Setelah instalasi dan perancangan selesai, langkah berikutnya adalah Uji kerentanan dilakukan pada DVWS-Node untuk mengidentifikasi celah keamanan yang ada. Uji ini melibatkan penggunaan berbagai alat dan teknik pengujian seperti pemindaian kerentanan, penetrasi, dan analisis statis. Tujuannya adalah untuk menemukan celah keamanan yang bisa dimanfaatkan oleh penyerang.

3.1.5 Analisis Kerentanan

Setelah uji kerentanan dilakukan, langkah berikutnya adalah menentukan apakah serangan yang terdeteksi bersifat tidak normal. Jika serangan tersebut tidak normal, maka perlu dilakukan perancangan tambahan pada WAF untuk menangkal serangan tersebut.

3.1.6 Melakukan Perancangan Keamanan

Jika dari analisis serangan ditemukan bahwa ada serangan yang bersifat tidak normal, langkah berikutnya adalah melakukan perancangan keamanan tambahan pada WAF. Perancangan ini bertujuan untuk memperkuat pertahanan DVWS-Node terhadap serangan yang telah teridentifikasi. Proses perancangan ini mencakup pengaturan aturan-aturan baru pada WAF untuk memblokir jenis serangan tertentu, menyesuaikan parameter-parameter keamanan, dan melakukan pengujian ulang untuk memastikan bahwa perancangan baru efektif dalam menangkal serangan. Dengan demikian, sistem keamanan dapat terus ditingkatkan berdasarkan temuan dari uji kerentanan dan analisis serangan.

3.1.7 Alat Bantu Penelitian

Alat bantu penelitian merupakan alat bantu yang dipilih atau digunakan oleh peneliti dalam melakukan kegiatannya untuk mengumpulkan data agar kegiatan tersebut menjadi sistematis dan mempermudah peneliti.

3.1.7.1 Perangkat Keras

Spesifikasi dari perangkat keras (hardware) yang digunakan dalam penelitian ini berupa laptop dengan spesifikasi sebagai berikut :

a) Model : Lenovo V14
b) *Processor* : 12th Gen Intel(R) Core(TM) i3-1215U 1.20 GHz
c) *Memory* : 8 GB RAM
d) *Hard Disk* : 102 GB

3.1.7.2 Perangkat Lunak

Penelitian ini menggunakan perangkat lunak (software) yang digunakan dalam penelitian sebagai berikut :

a) Sistem Operasi : Windows 11
b) Tools yang digunakan : Windows Subsystem for Linux, Burp Suite, Damn Vulnerable Web Services-Node , Open-appsec

3.2 Jadwal Kegiatan

Tabel 3.2 Jadwal Kegiatan

No	Nama Kegiatan	Bulan																			
		I				II				III				IV				V			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Identifikasi Masalah																				
2	Studi Literatur																				
3	Pemasangan ,perancangan dan melakukan uji kerentanan																				
4	Analisis Serangan																				
5	Melakukan Perancangan Keamanan																				
7	Kesimpulan dan Saran																				