BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

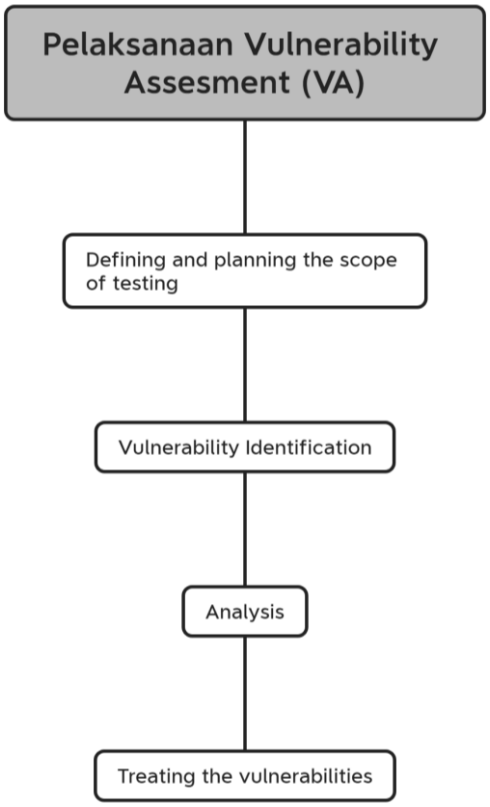
Penelitian ini menggunakan Metode Terapan yang berfokus pada hasil perbandingan, sehingga dapat menghasilkan informasi berdasarkan uji *Vulneravility Assessment (VA) software*. Secara pengujian penelitian ini akan dilaksanakan menggunakan tiga tahapan inti dari proses *vulnerability assessment (VA)* (Priandono, 2006).

Gambar 3.1 Metode Penelitian Terapan (Priandono, 2006)

3.1.1 Penentuan Batasan Proyek

Tahapan ini mengenai batasan proyek, dilakukann agar *vulnerability assessment* tidak melebihi parameter yang di tentukan.

3.1.1 Pelaksanaan Vulnerability Assessment



Gambar 3.2 Alur pelaksanaan *Vulnerability Assessment (VA)*

Tahap ini melakukan pemindaian *Vulnerability Assessment (VA),* tahap *Definising and planning the scope of testing* adalah mengidentifikasi dan merencanakan objek yang akan dilakukang pengetesan, tahap *vulnerability identification* adalah tahap mengidentifikasi kerentanan, tahap *analysys* adalah tahap menganalaisis hasil, tahap *trathing the vulnerabilitie*s adalah tahap hasil *output* yang diberikan dengan menggunakan *software Acunetix WVS* dan *Owasp Zap* dengan parameter *SQL Injection, Cross-site Scripting (XXS), CSRF (Cross-Site Request Forgery*).

3.1.2 Analisa hasil dan Pelaporan Akhir

Tahap ini berisi temuan hasil parameter dari pemindaian menggunakan *Acunetix WVS* dan *Owasp Zap*. Temuan ini dievaluasi untuk melihat gangguan atau kelamahan ini yang akan berdampak terhadap sistem. Selain dievaluasi juga dilakukan pengelompokan terhadap hasil temuannya. Laporan akhir ini akan diberikan kepada tim pelaksana IT atau administrator sistem, untuk memperbaiki kelemahan website

3.1.2.1 Acunetix WVS

Tahap ini melakukan pemindaian kerentanan *vulnerability assessment* dengan menggunakan software *Acunetix WVS* dengan target web kampus. Versi dari *Acunetix WVS* yang digunakan pada penelitian ini adalah versi 13.0.0. Hasil dari pemindaian kerentanan yang didapatkan dari software *Acunetix WVS* kemudian dilakukukan perbandiang hasil dari celah keamanan yang ditemukan.

3.1.2.2 Owasp Zap

Tahap ini melakukan pemindaian kerentanan *vulnerability assessment* dengan menggunakan *Owasp Zap* dengan target web kampus. Versi dari *Owasp Zap* yang digunakan pada penelitian ini adalah versi 2.11.0. Hasil dari pemindaian kerentanan yang didapatkan dari software *Owasp Zap* kemudian dilakukukan perbandiang hasil dari celah keamanan yang ditemukan.