BAB 3
METODE PENELITIAN

Proses penelitian ini secara umum meliputi inisiasi, pengembangan model, dan pengembangan produk aplikasi. Pada tahap inisiasi dilakukan identifikasi permasalahan dan kajian pendukungnya. Tahap selanjutnya, adalah pemilihan metode-metode dalam security hardening. Pada tahapan akhir dikembangkan sebuah produk berupa aplikasi untuk memudahkan pengguna menggunakan layanan cloud untuk security hardening dengan rincian penjelasan tiap-tiap tahapnya sebagai berikut:

3.1 Metode Pengumpulan Data

Metode pengumpulan data dalam penelitian ini antara lain melalui :

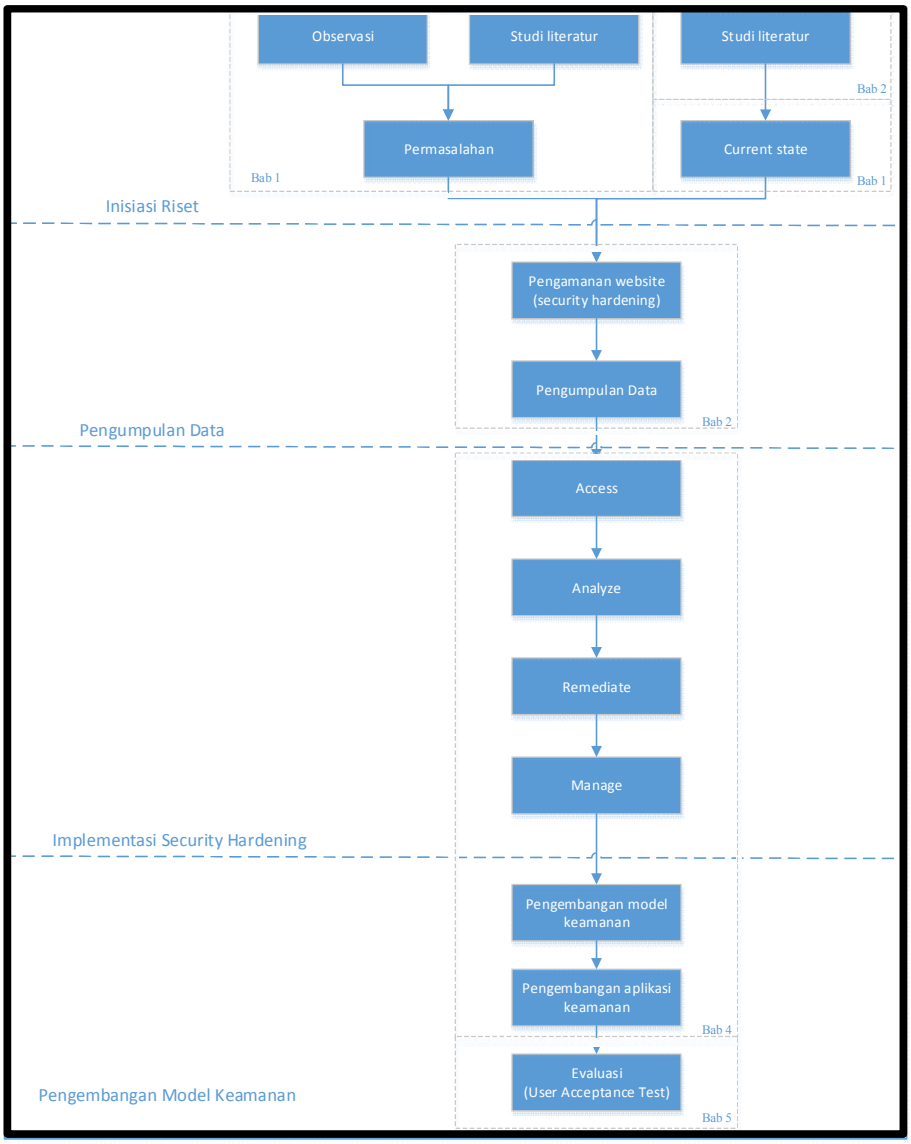
3.1.1 Kajian Literatur

Kajian literatur yang diperlukan dalam penelitian ini untuk mendukung teori-teori yang mendasari masalah dan informasi yang berkaitan dengan penelitian ini antara lain yang bersumber dari Wordpress Codex sebagai manual book online para developer Wordpress sedunia dan Wordpress Security White Paper yang dirilis oleh Automattic Inc sendiri selaku perusahaan pengembang Wordpress. [9]

3.1.2 Kuesioner

Kuesioner dilakukan guna mendapatkan informasi dan pemahaman mengenai penelitian ini. Informasi dalam penelitian ini bersumber dari beberapa webmaster dan web developer, yaitu tentang masalah keamanan pada situs web. Diantaranya seorang founder dan CEO dari sebuah software house di Semarang, seorang praktisi e-government Jawa Tengah, dan beberapa orang pengelola web hosting. Dari kuesioner secara non-formal pada mereka melalui beberapa pertanyaan terlampir, permasalahan yang timbul dalam penelitian ini adalah sulitnya seorang webmaster

mengatasi serangan keamanan pada situs web, terlebih bagi webmaster yang bekerja mengelola lebih dari satu situs web. Selain itu, menurut pengalaman pribadi penulis, membenahi satu situs web yang diretas membutuhkan waktu yang tidak sedikit karena bisa lebih dari satu hari hanya untuk membenahi satu situs web.



Gambar 3.4 Metode Penelitian

3.2 Jenis Data

Dalam penelitian ini jenis data yang digunakan adalah data sekunder yang diperoleh dari kajian literatur. Data tersebut berupa data kualitatif statistik penyebab diretasnya situs web berbasis Wordpress selama tahun 2009 sampai dengan 2012.

Tabel 3.4 Statistik Situs Wordpress yang Diretas Periode 2009-2012

Tahun	Jumlah Situs WordPress yang Diretas
2009	81.000
2010	98.000
2011	144.000
2012	170.000

Menurut StartBloggingOnline.com, sebuah perusahaan konsultan internet dan startup, sebesar 41% dari situs Wordpress yang diretas, penyebab utamanya adalah kesalahan konfigurasi pada web server. 8% penyebab lainnya, dikarenakan penggunaan password adminstrator yang terlalu mudah ditebak dan diserang secara brute-force. Sedangkan penyebab terbesar, yaitu 51% kerusakan, diakibatkan oleh plugin dan themes Wordpress yang disusupi backdoors ataupun memiliki celah keamanan pada plugin atau theme itu sendiri. [3]

3.3 Implementasi Security Hardening

Dari studi literature yang dilakukan dalam bab sebelumnya, penerapan security hardening berpotensi meningkatkan keamanan pada situs web, tidak terkecuali situs web berbasis CMS Wordpress. Berikut ini merupakan langkah penerapan security hardening:

3.3.1 Access

Mengidentifikasi celah-celah keamanan yang masih terdapat dalam sistem dan mengeksploitasi sistem untuk mengetahui lubang keamanan pada sistem tersebut.

3.3.2 Analyze

Memperkirakan tingkat keamanan dan menganalisis dampak yang terjadi pada celah keamanan tersebut, kemudian mengklasifikasikan tingkat kerusakan yang diakibatkan oleh celah keamanan tersebut.

3.3.3 Remediate

Menemukan celah keamanan pada sistem yang diuji dan mencari cara untuk menutup celah keamanan tersebut untuk mengamankan sistem.

3.3.4 Manage

Mengintegrasikan patch pada celah keamanan untuk menutup lubang keamanan dan mencegah serangan masuk, serta mencegah terbukanya celah keamanan lain.