BAB III
TAHAP PELAKSANAAN

3.1 Objek Penelitian

3.1.1 Metode Penelitian

Metode penelitian yang penulis gunakan adalah metode deskriptif kualitatif, yang telah dipertimbangkan bahwa metode ini yang paling sesuai diantara lain untuk digunakan di penelitian ini, karena pada penelitian ini penulis ingin mengolah informasi yang telah didapatkan secara kualitatif khususnya dari studi pustaka di media internet.

Metode yang digunakan sesuai dengan penulisan penulis untuk mengumpulkan dan mengelola informasi mengenai penggunaan Nuclei yang berbasis *command line interface*, yang saat ini penggunaannya hanya dapat dioperasikan oleh orang yang mempunyai keahlian khususnya seorang *Security Engineer*, agar diolah untuk dapat dikembangkan mengurangi segmentasi penggunaan (*End-User Friendly*) dari *hardware* maupun *brainware* oleh penulis secara keseluruhan.

3.1.2 Pengumpulan Data

Metode penelitian terhadap pengumpulan data yang akan penulis lakukan yaitu dengan menggunakan metode Studi literatur melalui sumber terbuka internet.

Data yang dikumpulkan sepenuhnya diperoleh melalui internet yang didalamnya terdapat dokumentasi, jurnal/buku elektronik, dan artikelyang berkaitan dengan mengenai fundamental kerentanan keamanan yang sehingga dapat membantu penulis dalam merancang aplikasi pemindaian kerentanan keamanan website ini dibantu dengan utilitas bernama Nuclei.

3.1.3 Metode Pengembangan Sistem

Penelitian ini menggunakan pendekatan pengembangan SDLC Agile yang saat ini ramai diimplementasikan oleh perusahaan rintisan/*startup* yang banyak terdapat di Indonesia.

3.1.4 Sekilas Tentang Objek Penelitian

Berdasarkan dari referensi yang penulis baca dari salah satunya dokumentasi Nuclei, Nuclei singkatnya merupakan sebuah alat (*tools*) pemindai kerentanan keamanan website berbasis *Command Line Interface* (CLI) pada desktop yang biasa digunakan oleh Security Engineer untuk memudahkan pekerjaan dalam mendeteksi celah keamanan pada suatu website yang ditarget.

Dikutip dari *repository* Nuclei di Github, "Nuclei is f*ast and customizable vulnerability scanner based on simple YAML based DSL*", Nuclei digunakan untuk

mengirim permintaan lintas target berdasarkan template, yang mengarah ke *zero false positive* dan menyediakan pemindaian cepat pada sejumlah besar host. Nuclei menawarkan pemindaian untuk berbagai protokol, termasuk TCP, DNS, HTTP, SSL, File, Whois, Websocket, Headless, dll. Dengan templating yang kuat dan fleksibel, Nuclei dapat digunakan untuk memodelkan semua jenis pemeriksaan keamanan.

3.1.5 Latar Belakang dan Tujuan Objek Penelitian

Nuclei sebuah *tools open source* pemindaian kerentanan website yang dapat diandalkan. Namun, Nuclei ini hanya dapat dioperasikan, dicerna hasil keluaran informasi hanya oleh orang yang mempunyai keahlian dibidangnya dan hanya tersedia didalam sistem operasi desktop.

Oleh karena itu tujuan dari objek penelitian yang penulis lakukan ini adalah untuk memanfaatkan Nuclei semaksimal mungkin yang digunakan di dalam rancangan penelitian ini agar pemindaian kerentanan keamanan website dapat digunakan dengan sangat mudah oleh orang awam sekalipun tanpa membutuhkan keahlian apapun dimanapun berbasis aplikasi website.

3.1.6 Target Dari Objek Penelitian

Target dari objek penelitian ini adalah memfasilitasi kemudahan terhadap individu/kelompok dalam meningkatan kesadaran kerentanan keamanan website yang dimilikinya sehingga dapat melakukan pencegahan dari ancaman peretas(*hacker*) berdasarkan hasil audit berupa dokumen yang dari rancangan pengembangan aplikasi ini berikan.

3.1.7 Deskripsi Tugas

Pengembangan rancangan aplikasi ini dikerjakan oleh 2 orang, Muhammad Dary Azhari sebagai perancang *Front-end* dari pengerjaan antar muka landing page, aplikasi web, desain hingga CMS manajemen user.

Dan Abdul Arfan sebagai perancang *Back-end* atau otaknya dari fitur utama yang dikembangkan ini, yaitu merespon permintaan dari Front-end melalui Restful API lalu menjalankan (*trigger*) service agar Nuclei berjalan di latar belakang dan setelah selesai, maka menyediakan laporan hasil audit berupa dokumen Excel.

3.2 Analisis Sistem Yang Berjalan

3.2.1 Prosedur Sistem Berjalan

Sistem yang berjalan dalam meninjau kerentanan keamanan web, saat ini masih didominasi oleh pengerjaan manual dengan membaca dokumentasi/*guidelines*.

Dokumen yang paling terkenal dan banyak dijadikan standar sebagai referensi pengujian kerentanan aplikasi web yaitu dokumen-dokumen dari organisasi nirlaba OWASP (*Open Web Application Security Project*), yaitu sebuah

proyek keamanan aplikasi web terbuka, sebuah komunitas online yang menghasilkan artikel, metodologi, dokumentasi, alat, dan teknologi yang tersedia secara bebas di bidang keamanan aplikasi web.

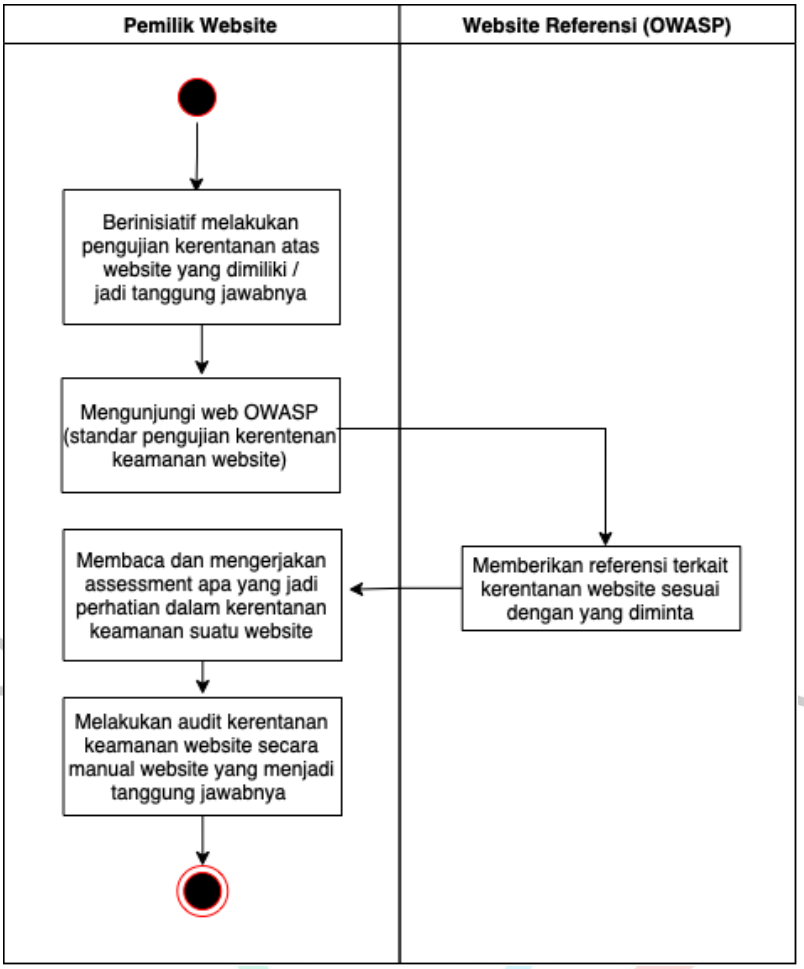
Prosedur sistem berjalan yang dilakukan untuk mencapai itu semua, antara lain:

1. Pemilik website/orang yang bertanggung jawab atas pengembangan suatu website berinisiatif untuk melakukan pengujian kerentanan keamanan website yang jadi tanggung jawabnya.
2. Kemudian membaca referensi yang saat ini menjadi standar pengujian kerentanan keamanan web dari OWASP (*Open Web Application Security Project*).
3. Dan dapat juga mengerjakan *assessment OWASP Web Application Security Testing Checklist* yang berisi tentang daftar-daftar kerentanan web yang harus diwaspadai.

3.2.2 Analisis Permasalahan

Berdasarkan analisis sistem berjalan diatas, dapat disimpulkan bahwa masih terdapat beberapa permasalahan yang ada pada sistem tersebut. Adapun permasalahannya adalah sebagai berikut:

1. Kurangnya kesadaran akan pentingnya aspek keamanan dalam membangun *website* dikarenakan dibutuhkan dedikasi ilmu (keahlian khusus) *web security engineering* dalam mengerti dan memahami referensi kerentanan keamanan *website* dan mengetahui & mengatasi celah-celah *website* yang rentan diretas.
2. Jika telah memahami *web security engineering*, diperlukan pengecekan keseluruhan secara manual mengenai apa saja yang menjadi resiko-resiko kerentanan aplikasi *website* dengan membaca dokumentasi standarisasi yang ada seperti dokumen *OWASP Top 10 Web Application Security Risks*, *OWASP Web Application Security Testing Checklist* dan lain-lain.
3. Pengecekan kerentanan keamanan web keseluruhan secara manual, akan memakan banyak waktu dikarenakan membaca dokumen/*guidelines* yang sudah ada, termasuk mengecek ulang resiko kerentanan keamanan web aplikasi yang sudah diantisipasi/dikerjakan/ditambal.
4. Tidak bisa menghasilkan/mendapatkan laporan resiko-resiko kerentanan apa saja (*action list*) yang memang harus dibenahi.



Gambar 3.1 *Activity Diagram* Sistem Berjalan

3.2.3 Pemecahan Masalah

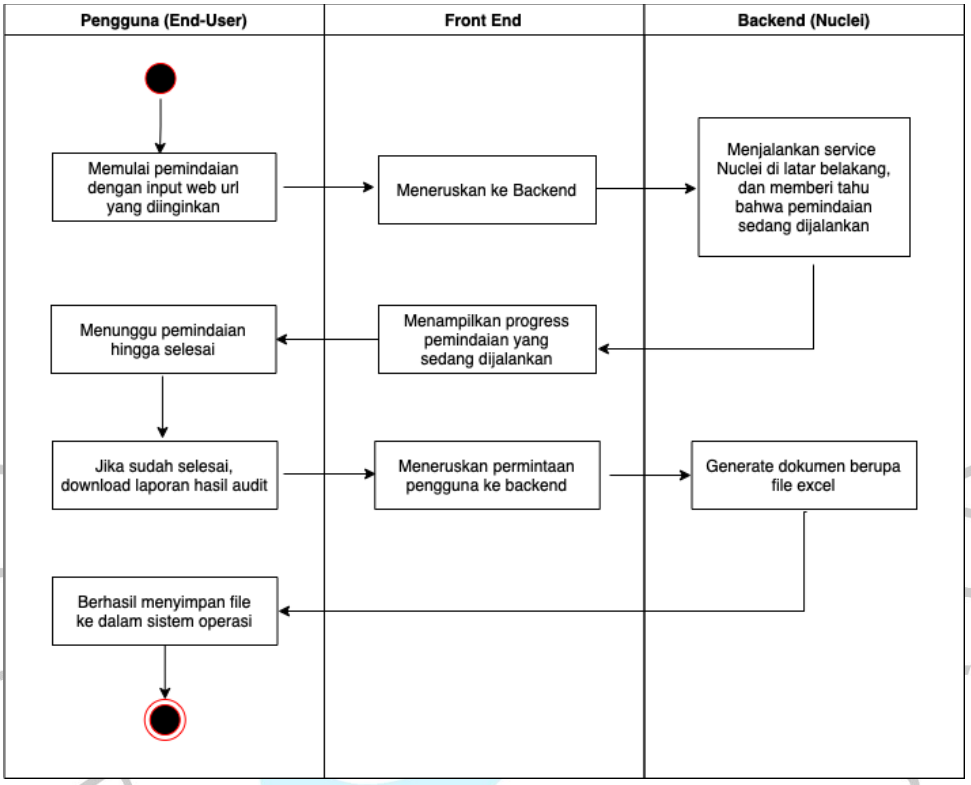
Melihat dari masalah yang ada dan yang sedang dihadapi tersebut, maka diusulkan pemecahan masalah sebagai berikut:

1. Dalam mengatasi masalah kesadaran akan pentingnya keamanan website, dibutuhkan sebuah perancangan sistem informasi berbasis aplikasi web yang mudah dimengerti, mudah digunakan oleh siapapun tanpa adanya *skills barrier* dan dapat diakses dimanapun.
2. Dibutuhkan perancangan sistem informasi yang dapat mengotomasi langkah-langkah mengatasi kerentanan keamanan web yang biasa dilakukan manual seperti membaca referensi, melakukan assesmen dari OWASP dengan fitur otomasi pemindaian kerentanan keamanan website.
3. Dibuatkan sistem otomasi pemindaian kerentanan keaman web terkomputerisasi yang dapat diakses dimanapun, mudah digunakan oleh siapapun dan dimanapun untuk melakukan audit/pemindaian terhadap resiko-resiko kerentanan keamanan *website* tersebut.

4. Menyediakan laporan dokumen hasil audit mengenai hal-hal apa saja resiko kerentanan keamanan *website* yang harus diperbaiki dari kerentanan keamanan *website* yang diputuskan untuk diaudit oleh pengguna.

3.2.4 Usulan Sistem

Secara umum usulan sistem dalam proses perancangan sistem yaitu akan membuat aplikasi berbasis web pemindaian kerentanan keamanan web dengan harapan mampu menangani permasalahan yang ada. Berikut *workflow* sistem yang diusulkan.



Gambar 3.2 *Activity Diagram* Usulan Sistem

3.3 Analisis Kebutuhan

Penulis menemukan bahwa ada 2 kebutuhan dalam rancangan sistem informasi ini antara lain, kebutuhan pengguna (*End-User)* dan kebutuhan sistem administrator (Admin).

3.3.1. Kebutuhan Pengguna

Berdasarkan analisa dari penulisan ini, kami melihat kebutuhan penggunaan seminimal-minimalnya (*Minimum Viable Product*) atas rancangan pengembangan sistem informasi ini, antara lain:

1. Pengguna dapat melakukan registrasi ke dalam aplikasi.
2. Pengguna dapat melakukan masuk (*sign in*) kedalam aplikasi.
3. Pengguna dapat melakukan keluar (*sign out*) keluar aplikasi.

4. Pengguna dapat melakukan pemindaian terhadap website yang diinginkan dengan memasukkan (*input*) url website.
5. Pengguna dapat melihat daftar website yang sudah pernah dipindai
6. Pengguna dapat melihat perkembangan (progress) pemindaian website yang sedang berjalan.
7. Pengguna dapat mengunduh dokumen laporan hasil audit dari pemindaian yang sudah sukses selesai berupa *file* Excel.

3.3.2. Kebutuhan Sistem Administrator

Admin dapat mengakses CMS untuk menunjang berbagai kebutuhan administrasi khususnya dalam manajemen pengguna sederhana CRUD (*Create, Read, Update, Delete*).

CRUD merupakan singkatan dari *Create*, *Read*, *Update* dan *Delete*. Yang merupakaan keempat istilah ini sebuahperintah atau *query* yang digunakan programmer dalam melakukan aksi melalui database.