BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada setiap organisasi memiliki ketua maupun wakil ketua yang dipilih langsung oleh mahasiswa melalui pemilu. Saat kegiatan pemilu dilaksanakan, seluruh mahasiswa yang memiliki hak pilih dapat melakukan pemilihan wakil dengan cara menghadiri tempat yang telah disediakan oleh panitia pemilwa. Terdapat beberapa permasalahan yang muncul saat pemilwa dilakukan secara luring, yaitu mahasiswa yang sedang melakukan ko-ass akan kesulitan untuk mengikuti Pemilwa karena mereka harus melaksanakan ko-ass di puskesmas maupun rumah sakit. Setiap kali pemilwa ini dilakukan, menyebabkan suatu kondisi yang kurang kondusif sehingga memakan waktu yang cukup lama. Selama ini, voting secara mencontreng di atas kertas suara menjadi opsi dalam melaksanakan Pemilwa. Persoalan data yang tidak teratur berpengaruh pada validasi data para pemilih, kebutuhan logistik pemungutan suara yang boros secara anggaran, rekapitulasi penghitungan suara yang tidak efisien dalam segi waktu, sampai rentannya manipulasi hasil pemungutan suara oleh oknum yang tidak bertanggung jawab [1]. Untuk menangani permasalahan pemilihan saat ini yang disebabkan oleh kurangnya sistem dalam melakukan pemilihan daring, diperlukan sistem informasi terkait e-voting. E-voting adalah suatu sistem pemilihan dimana data dicatat, disimpan dan diproses dalam bentuk informasi digital. E-voting dapat diartikan sebagai proses pemungutan suara yang dilakukan secara elektronik, meliputi pendaftaran pemilih, pelaksanaan pemilihan, perhitungan suara, dan pengiriman hasil suara [2]. Aplikasi e-voting dianggap lebih efektif dan lebih efisien karena semua proses dapat terkomputerisasi, memberikan kemudahan bagi pengguna untuk memilih calon, mempermudah dalam proses penghitungan suara dan hasil pemilihan bisa langsung diketahui secara cepat dan akurat dalam merealisasikan pemilu, sistem tersebut dapat membantu dalam melakukan perhitungan suara dan dapat mengurangi terjadinya suara tidak sah.

Penelitian ini menggunakan arsitektur MVC (*Model View Controller*) dengan pendekatan PXP (*Personal Extreme Programming*). PXP merupakan metode pengembangan dari *Extreme Programming* yang disesuaikan agar dapat dikerjakan oleh pengembang tunggal [3]. Pengembang memilih metode PXP dalam pengembangan aplikasi karena proses iteratifnya memungkinkan pengembang secara progresif mendalami pemahaman di bidang pengkodean. Fokus khusus pada praktik refactor kode yang baik dan efisien memungkinkan pengembang mengembangkan keahlian secara menyeluruh, memahami cara meningkatkan kualitas dan maintainability kode, serta menanggapi perubahan kebutuhan dengan lebih adaptif. Sistem yang akan dibangun dalam penelitian ini merupakan e-voting pemilihan wakil mahasiswa. Kebutuhan sistem didapat pada fase requirements. Tahap pengembangan akan dilanjutkan dengan perencanaan iterasi dengan menentukan prioritas kebutuhan dan diskusi bersama. Pengembangan sistem akan dilakukan secara iteratif berdasarkan perencanaan yang telah dilakukan. Apabila terdapat perubahan atau penambahan kebutuhan, maka akan dilakukan perencanaan ulang [4]. Terdapat tantangan dalam proses pengembangan aplikasi menggunakan metode PXP, di mana komunikasi yang intens dengan klien dapat menjadi suatu masalah di waktu pengembangan jika terjadi terlalu banyak perubahan. Dalam penelitian yang berjudul "Rancang Bangun Sistem Try Out Berbasis Paperless untuk Evaluasi Hasil Belajar Siswa dengan MVC" penggunaan arsitektur MVC dapat mengurangi kompleksitas program dan membuatnya lebih mudah dikelola serta disesuaikan dengan perubahan yang terjadi. [5]. Bagian *model* dan controller dapat dikerjakan oleh *back-end developer*, sementara bagian view dapat dilakukan oleh *front-end developer* dan tim UI/UX. Penggunaan MVC dapat memungkinkan pengembang untuk fokus pada bagian-bagian tertentu dari website, yang memungkinkan mereka untuk lebih efektif dan efisien dalam pengembangan. Memisahkan tugas-tugas antara *back-end developer* dan *front-end developer* memungkinkan identifikasi dan perbaikan kesalahan atau masalah dalam pengembangan menjadi lebih mudah [6]. Beberapa sumber [7][8][9] juga telah menunjukkan bahwa penggunaan arsitektur MVC

dapat meningkatkan kualitas dan keandalan website. Dalam arsitektur MVC, setiap bagian terpisah dan memiliki tugas yang jelas, sehingga meminimalkan kemungkinan kesalahan dalam pengembangan. Selain itu, penggunaan MVC juga memudahkan pengembangan dan pengujian karena setiap bagian dapat diuji secara terpisah.

Metode PXP memiliki kelebihan pada tahap dari SDLC (*Software Development Life Cycle*) menerapkan unit test dan refactor sehingga kita bisa lebih fleksibel untuk mengatur *pass rate* sebelum aplikasi di *deploy* yang dapat berfungsi untuk mengurasi malfungsi dari sebuah aplikasi. [10].

Keamanan dalam sebuah aplikasi sangat perlu diperhatikan karena ada kemungkinan aplikasi kita diretas atau dibobol oleh orang yang tidak bertanggung jawab. Dalam *framework* laravel ini sebenarnya sudah dilengkapi oleh beberapa fitur yang dapat membuat aplikasi kita menjadi aman atau terproteksi oleh berbagai macam serangan. Contoh salah satu jenis serangan yang sering ditujukan kepada web aplikasi adalah *Cross-Site Scripting,* XSS (*Cross-Site Scripting*) adalah jenis serangan pada aplikasi web yang memungkinkan penyerang menyisipkan skrip berbahaya ke dalam halaman web yang ditampilkan oleh browser pengguna akhir. Serangan ini dapat memungkinkan penyerang untuk mencuri data pengguna, menjalankan tindakan yang tidak diinginkan di situs web, dan bahkan memasukkan konten yang tidak pantas ke dalam halaman web. Serangan XSS dapat terjadi ketika input pengguna tidak divalidasi atau tidak disaring dengan benar sebelum ditampilkan pada halaman web, sehingga memungkinkan penyerang untuk menyisipkan skrip berbahaya ke dalam halaman tersebut [11]. Penggunaan *purifying* (pembersihan) sangat dianjurkan untuk membersihkan data yang disimpan kedalam *database* oleh pengguna sebelum menampilkannya pada halaman web, terutama jika data tersebut bersifat sensitif atau penting.

Penelitian ini tidak hanya bertujuan untuk membuat aplikasi e-voting dengan menggunakan arsitektur MVC dengan pendekatan PXP, tetapi juga untuk memperhatikan aspek keamanan dalam pengembangan aplikasi e-voting. Keamanan menjadi hal yang sangat penting dalam pengembangan

aplikasi e-voting untuk mencegah terjadinya serangan dan manipulasi data oleh pihak yang tidak bertanggung jawab. Oleh karena itu, dalam penelitian ini akan digunakan purifier dalam laravel untuk meningkatkan aspek keamanan dari aplikasi e-voting. Purifier merupakan salah satu plugin dalam laravel yang berfungsi untuk memproses inputan yang masuk ke dalam aplikasi, sehingga menghindari terjadinya serangan injeksi kode atau *SQL injection*. Meningkatkan kepercayaan pengguna terhadap sistem e-voting yang dikembangkan diharapkan dapat tercapai dengan memperhatikan aspek keamanan dalam pengembangan aplikasi e-voting.

1.2 Rumusan Masalah

1. Bagaimana penerapan modul purifier pada *framework* Laravel dapat meningkatkan keamanan aplikasi web dan melindungi aplikasi dari serangan oleh pihak yang tidak bertanggung jawab ?
2. Bagaimana Repository Pattern dapat memengaruhi fleksibilitas dan pemeliharaan perangkat lunak dalam jangka panjang?

1.3 Tujuan Penelitian

1. Membangun aplikasi e-voting dengan menggunakan metode pengembangan PXP dan arsitektur MVC dengan menambahkan fitur keamanan.
2. Dapat meningkatkan partisipasi mahasiswa dalam proses pemilihan karena dapat diakses secara daring, mengatasi kendala geografis dan jadwal yang padat.
3. Mempercepat proses pemilihan dan dapat mengoptimalkan waktu yang diperlukan untuk menghitung suara dan mengumumkan hasil.

1.4 Batasan Penelitian

Dalam penelitian ini penulis melakukan batasan dalam melakukan penelitian terhadap satu variabel.

1. Bahasa pemrograman yang digunakan adalah PHP dan Javascript dengan menggunakan *framework* Laravel dan Bootstrap untuk css
2. *Database Management System* (DMBS) yang digunakan adalah MySql

3. Lingkup e-voting hanya ditujukan kepada mahasiswa kedokteran dan ilmu kesehatan Universitas Brawijaya
4. Metode pengembangan aplikasi menggunakan *Personal Extreme Programming*
5. Modul eksternal yang digunakan untuk melindungi keamanan aplikasi dari serangan *Cross Site Scripting* (XSS) adalah Purifier.