

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Web 2.0 merupakan istilah yang digunakan untuk menunjukkan berbagai layanan di web yang memungkinkan pemakai untuk berkolaborasi dan berbagi informasi secara online. Teknologi Web 2.0 menggunakan teknologi yang sejak lama dikembangkan untuk web, ditambah dengan berbagai teknologi yang memungkinkan kolaborasi serta berbagai informasi. Sehingga secara logis bisa dikatakan bahwa Web 2.0 akan mempunyai masalah keamanan yang sama dengan aplikasi web sebelumnya bahkan lebih. Pembuatan aplikasi *website* dapat dikatakan mudah atau sulit, disatu sisi bahasa pemrogramannya mudah dipelajari namun disisi lain kemudahan tersebut sering membuat *web developer* terlena. Faktor keamanan menjadi syarat mutlak dipenuhi dalam aplikasi Web 2.0. Tetapi tidak semua *developer* menyadari hal tersebut. Bahkan ada yang membangun aplikasi *website* tanpa di-optimasi dan tidak memperhitungkan keamanan data. Akibatnya aplikasi *website* tersebut mudah dirusak oleh pihak-pihak yang tidak bertanggung jawab. Tapi, ada pendekatan baru dalam pemrograman *website* yang bisa meng-handle masalah-masalah tersebut. Salah satunya adalah pemrograman web berbasis *framework*.

Framework merupakan sekumpulan *library* yang diorganisasikan pada sebuah rancangan arsitektur untuk memberikan ketepatan, kecepatan, kemudahan dan konsistensi dalam pengembangan aplikasi. *Framework*

menyediakan berbagai *library* untuk pengembangan aplikasi *website* secara tepat dan mudah dengan tidak mengurangi dari segi keamanan *website* tersebut. Terdapat banyak *framework* untuk aplikasi *website* yang dikembangkan sesuai dengan bahasa pemrograman yang digunakan. Contoh *framework* untuk aplikasi *website* antara lain adalah Ruby on Rails (Ruby), CodeIgniter (PHP), Symphony (PHP), CakePHP (PHP), Zope (Python), DotNetNuke (VB.NET), Apache Struts (Java), Spring (Java), dan lain sebagainya.

Salah satu dari sekian banyaknya *framework* untuk aplikasi *website* tersebut adalah Ruby on Rails (RoR). RoR merupakan *framework* Ruby berbasis open source untuk pengembangan aplikasi web (*web application framework*). RoR versi *beta* pertama dilepaskan kepada publik pada bulan juli 2004. RoR menerapkan secara penuh pola perancangan MVC (Model View Controller) dan juga dilengkapi dengan dukungan Ajax, *internationalization*, *localization*, dan ORM (Object Relational Model). Pengembangan suatu aplikasi web dengan menggunakan *framework* Ruby on Rails dapat dilakukan secara lebih cepat, mudah dan aman dibandingkan dengan *framework* lainnya. Seorang *web developer* dapat menulis program menggunakan RoR dengan sedikit pengkodeaan, dengan menjaga ukuran kode program tetap kecil maka dapat mempercepat pengembangan aplikasi dan memperkecil *bug* yang akan membuat kode program para *developer* mudah dipahami, dipelihara dan ditingkatkan. Kesuksesan RoR ini kemudian menginspirasi para *developer* PHP untuk membangun *framework* serupa dalam bahasa *scripting* PHP.

Kemudian, para *developer* PHP menciptakan *framework* CakePHP dan pertama diluncurkan pada tahun 2006 sebagai adaptasi dari *framework* RoR.

Framework RoR dan CakePHP banyak dikaji secara khusus untuk dibandingkan. Kajian yang dilakukan banyak membandingkan dari segi kinerja (*performance*), metodologi dan keamanan (*security*). Pada penelitian sebelumnya menghasilkan beberapa solusi untuk mengatasi ancaman pada sistem keamanan *framework* RoR semisal, solusi untuk ancaman *SQL Injection* yaitu menghindari mekanisme *generate* SQL berbasis *user-controller variables* (Hendrayana, 2007;5). Tetapi, pada penelitian tersebut mempunyai beberapa kelemahan. Salah satunya, kurangnya solusi untuk ancaman *Cross Site Scripting (XSS)*. Sehingga menimbulkan ketertarikan peneliti untuk melakukan penelitian pada *framework* tersebut. Karena kesuksesan RoR menginspirasi para *developer* PHP membuat *framework* CakePHP. Maka penelitian ini diadakan untuk mengkaji ulang lebih dalam mengenai perbedaan sistem keamanan pengembangan aplikasi website antara *framework* RoR dan CakePHP. Penelitian ini akan dilakukan dengan studi literatur sebagai kegiatan utama dan pembangunan dua buah *prototype* aplikasi website Web 2.0 untuk masing-masing *framework* sebagai penguat dari hasil analisa literatur. Hasil akhir dari penelitian ini diharapkan dapat diketahui mana yang terbaik diantara *framework* RoR dan CakePHP dalam segi sistem keamanan pengembangannya.

1.2 Perumusan Masalah

Berdasarkan uraian latar belakang masalah diatas maka dapat didefinisikan permasalahan-permasalahan yang dihadapi dalam penelitian ini diantaranya adalah :

1. Langkah-langkah analisa apa saja yang diperlukan untuk membandingkan sistem keamanan dalam pengembangan aplikasi *website* Web 2.0 yang dibangun oleh *framework* RoR dan CakePHP?
2. Apa saja kelebihan dan kekurangan dari masing-masing *framework* dilihat dari segi keamanannya ?
3. Ancaman apa saja yang dapat menyerang sistem keamanan *framework* RoR dan CakePHP ?
4. Bagaimana solusi untuk menghadapi ancaman pada sistem keamanan *framework* RoR dan CakePHP ?
5. Dengan cara alternatif apa untuk memilih *framework* terbaik diantara kedua *framework* tersebut ?

1.3 Batasan Masalah

Dari rumusan masalah diatas dan mengingat waktu pengerjaan serta banyaknya kemungkinan masalah serta kendala-kendala yang dihadapi dalam penelitian ini, maka batasan-batasan masalah pada penelitian ini adalah:

1. Penelitian ini hanya dibatasi pada dua *framework* yaitu Ruby on Rails versi 2.3.4 dan CakePHP versi 1.2.5.
2. Berdasarkan pembahasan developer Duane O'brien maka penelitian ini hanya dibatasi pada empat ancaman pada sistem keamanan *framework* RoR dan CakePHP yaitu *SQL injection*, *Cross Site Scripting (XSS)*, *Cross-Site Request Forgery (XSRF)* dan *authentication*.
3. Hal yang akan dibandingkan adalah sistem keamanan dari pengembangan *website* Web 2.0 yang akan dibuat oleh masing-masing *framework*. Keamanan yang dimaksud yaitu, proses yang dilalui dalam membangun sebuah *website*, mulai dari komponen-komponen utama yang disediakan oleh masing-masing *framework* maupun fitur-fitur tambahan yang disediakan.
4. Akan dilakukan pengkajian yang terbaik diantara kedua *framework* tersebut berdasarkan hasil penelitian yang akan dilakukan.

1.4 Tujuan Penelitian

Kegiatan penelitian ini dilakukan dengan tujuan untuk meneliti lebih dalam tentang perbedaan sistem keamanan dalam pengembangan aplikasi web berbasis *framework* antara RoR dan CakePHP. Hasil dari penelitian ini diharapkan dapat digunakan sebagai bahan pertimbangan bagi *developer* yang sudah atau akan menggunakan salah satu dari *framework* RoR dan CakePHP untuk membangun sebuah aplikasi *website* berbasis *framework*.

1.5 Manfaat Penelitian

Dengan diadakannya penelitian ini, maka manfaat bagi para *web developer* dapat digunakan sebagai bahan pertimbangan untuk ikut mengadopsi salah satu dari *framework* RoR dan CakePHP serta sebagai tambahan referensi untuk pengembangan penelitian ini.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyusunan laporan penelitian ini adalah:

1. Bab 1 Pendahuluan

Pada bagian ini dipaparkan latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

2. Bab II Tinjauan Pustaka dan Landasan Teori

Pada bab ini berisi tentang penilaian, kesimpulan, manfaat yang sudah tercapai dan yang belum tercapai dari penelitian terdahulu. Dan pada bab ini juga akan menjelaskan tentang konsep dan prinsip dasar yang diperlukan untuk memecahkan masalah penelitian.

3. Bab III Cara Penelitian

Bab ini menjelaskan tentang alat yang digunakan untuk penelitian dan akan memaparkan jalannya penelitian pada perbandingan system keamanan framework RoR dan CakePHP.

4. Bab IV Hasil Penelitian dan Pembahasan

Pada bab ini akan dilakukan pengujian terhadap penelitian yang sedang dikerjakan kemudian akan menyimpulkan hasil dari pengujian tersebut serta melakukan pembahasan.

5. Bab V Penutup

a. Kesimpulan

Berisi pemaparan singkat berupa kesimpulan mengenai hasil dari penelitian. Pemaparan berisi beberapa kesimpulan apakah kriteria perbandingan dapat menjadi kekuatan atau kelemahan bagi kedua *framework*.

b. Saran

Berisi saran yang direkomendasikan untuk pengembangan penelitian selanjutnya agar hasil yang diperoleh lebih maksimal.