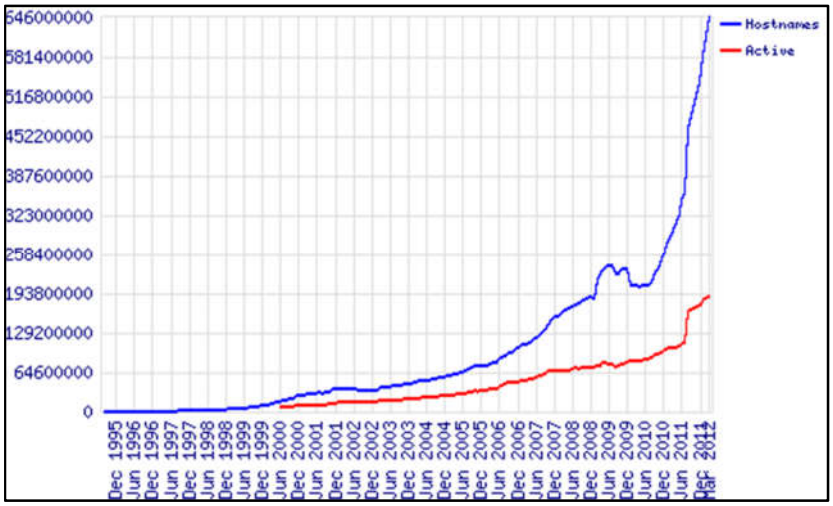
BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

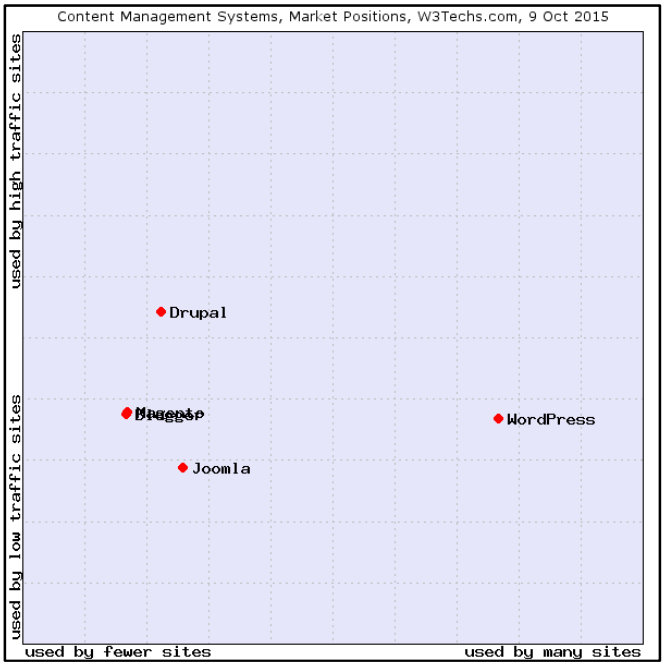
Perkembangan jumlah situs web pada era teknologi informasi saat ini menunjukkan tren peningkatan yang begitu cepat. Menurut survei yang diadakan oleh Netcraft, sebuah perusahaan riset dan keamanan internet, jumlah situs web yang aktif saat ini mencapai 644 juta situs web. Lebih tepatnya 644,275,754 situs web [1] dan angka tersebut akan terus bertambah setiap tahunnya. Semakin mudahnya orang memiliki situs web mendukung meningkatnya jumlah situs web saat ini. Salah satunya adalah penggunaan Content Management System (CMS) yang memungkinkan pengguna membuat situs web hanya dalam beberapa menit saja.



Gambar 1.1 Statistik peningkatan jumlah situs web

Wordpress, merupakan sebuah *Content Management System* (CMS) yang banyak digunakan untuk mengembangkan situs web. Mulai situs web pribadi, blog, toko online, hingga situs web korporasi dan pemerintahan. Berdasarkan survei dari W3techs, sebuah perusahaan survei teknologi web, *marketshare* Wordpress saat ini mencapai 24,5% dari total situs web yang tersedia di internet. Sedangkan dari situs

web yang menggunakan CMS lain seperti Joomla, Drupal, dan sebagainya, Wordpress menempati 58,9% posisi situs web dengan teknologi CMS [2].



Gambar 1.2 Statistik marketshare CMS

Dengan semakin meningkatnya minat pemilik situs web termasuk perusahaan komersial dan pemerintahan terhadap Wordpress karena kemudahan penggunaannya dan sifatnya yang open-source, semakin banyak pula pengembang web yang menciptakan plugin untuk menambah fungsionalitas CMS Wordpress dan berbagai macam tema untuk kustomisasi tampilan situs web berbasis Wordpress. Dampaknya, hal itu semakin membuka banyak celah keamanan terhadap *core* sistem Wordpress itu sendiri. Seperti dari plugin atau tema yang memiliki celah keamanan, atau plugin atau tema premium bajakan yang disusupi *backdoor*.

Menurut survei The Hacker News, sebuah portal keamanan informasi, pada tahun 2009, jumlah situs web berbasis Wordpress yang terkena serangan hacker mencapai 81.00 situs web. Angka ini terus meningkat hingga pada tahun 2012 jumlahnya

mencapai 170.000 situs web [3]. Dibutuhkan setidaknya waktu lima hari untuk mencari kerusakan memperbaiki seluruh kerusakan pada satu situs web dan biaya sekitar 100 US dollar untuk jasa perbaikan [4]. Apabila dalam setahun ada 100.000 situs web yang diretas, maka diperkirakan akan membutuhkan waktu yang banyak untuk membenahi situs web tersebut dan biaya 100.000.000 US Dollar lebih untuk biaya jasa maintenance. Itupun belum termasuk kerugian akibat berhentinya proses bisnis perusahaan saat sistemnya diretas.

1.2 Rumusan Masalah

Berdasarkan kondisi yang terjadi saat ini diketahui bahwa WordPress rentan diserang oleh hacker karena plugin dan temanya memiliki sejumlah celah keamanan. Ulah hacker yang merusak situs-situs web ini mengakibatkan kerugian materi dan non-materi yaitu kerugian berupa besarnya biaya yang harus dikeluarkan untuk jasa maintenance website dan kerugian berupa waktu yang terbuang hanya untuk membenahi situs web yang diretas, apalagi perusahaan yang menangani lebih dari satu situs web seperti provider web hosting.

Dari paparan di atas dirumuskan permasalahan pada penelitian ini adalah bagaimana cara mengamankan situs web berbasis WordPress dengan cepat dan efektif, terutama bagi para pemilik situs web yang mengelola lebih dari satu situs web.

1.3 Batasan Masalah

Pada penelitian ini, fokus penulis adalah situs web yang berbasis CMS WordPress dan permasalahan keamanan yang dijadikan acuan di sini adalah WordPress Codex, sebuah repositori informasi mengenai WordPress. Sedangkan untuk spesifikasi web server yang di gunakan untuk instalasi WordPress adalah sebagai berikut:

1. Web server Apache
2. PHP versi 5.*
3. Basis data MySQL
4. Sistem operasi Windows dan CloudLinux 6.7

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah menciptakan sebuah pendekatan untuk mengamankan situs web yang berbasis Wordpress dari serangan peretas dengan cara yang lebih cepat dan efisien, melalui pengembangan satu portal aplikasi untuk memantau dan melakukan maintenance pada lebih dari satu situs web sekaligus.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah terciptanya sebuah plugin *Wordpress* dan *cloud* SaaS *server* sebagai *back-end* pengguna untuk mengontrol dan menjaga kemanan situs web berbasis *Wordpress* miliknya. Tidak hanya pada *end-user*, tetapi terutama pada penyedia jasa website *development* yang membutuhkan banyak waktu untuk *maintenance* situs web pelanggannya satu-persatu.

Selain itu, produk keluaran berupa layanan SaaS *cloud* ini juga dapat dilakukan *monetizing* dengan menyediakan paket premium untuk pengguna profesional dan jasa *security hardening* server maupun Wordpress.