IMPLEMENTASI MODSECURITY SEBAGAI SISTEM MONITORING KEAMANAN APLIKASI WEB SECARA REAL TIME

IMPLEMENTATION OF MODSECURTIY AS A WEB APPLICATION SECURITY MONITORING SYSTEM IN REAL TIME

Dyah Rizky Huzayrha Laitupa[1], Setia Juli Irzal ismail[2], Mochammad Fahru Rizal[3]

[1]qq_12694@yahoo.co.id, [2]jul@tass.telkomuniversity.ac.id, [3]mfrizal@tass.telkomuniversity.ac.id

Abstrak

Penggunaan aplikasi web dalam kehidupan manusia saat ini sangat berkembang. Segala informasi yang ada pada aplikasi web tersebar luas dalam dunia internet maka dari itu aplikasi web sangat rentan terhadap serangan hacker. Hal tersebut membuat keamanan menjadi aspek penting dalam melindungi informasi yang tersebar di dunia internet. Karena adanya kebutuhan akan suatu sistem keamanan maka dibuat suatu sistem yang dapat mendeteksi dan mencegah serangan sehingga dapat dijadikan alat untuk memonitoring keamanan pada sebuah aplikasi web. Untuk membangun sistem ini, akan digunakan Modsecurity yang merupakan web application firewall, seperti firewall pada umumnya yang memiliki tugas yaitu melakukan pemfilteran terhadap apa yang melaluinya dan melakukan blocking terhadap apa yang dianggap berbahaya sesuai dengan rule yang ditetapkan. Sama dengan cara kerja sistem ini yaitu melakukan pencocokan antar request HTTP dengan pola-pola serangan menggunakan rule yang ditetapkan. Kemudian segala bentuk serangan yang telah terdeteksi akan disimpan.

Kata kunci: Keamanan Aplikasi Web, Web Application Firewall, Modsecurity

Abstract

The use of web applications in human life today is highly developed. Information on web applications are spread in the Internet and therefore web applications very vulnerable to hacker attacks. This makes security a key aspect of protecting the information spread in the internet. In this the final project, the writer wants to create a system that can detect and prevent attacks, and can be a tool for monitoring security in a web application. We hope the system will be able to reduce the chances of hackers to hack a web application. To build this system, Mod Security will be used as a web application firewall. Like firewalls in general, modsecurity have the task to do filtering on data package and do the blocking of what is considered to be dangerous in accordance with the rule set. Similar to the way the system works is to do the matching between an HTTP request with the patterns of attacks using the rule set. Then all forms of attacks that have been detected will be saved.

Keywords: Web Application Security, Web Application Firewall, Mod Security

1. Pendahuluan

Di seluruh dunia, saat ini ada lebih dari satu miliar pengguna internet. Penggunaan aplikasi web dalam dunia internet mengalami perkembangan yang sangat pesat. Faktor- faktor yang membuat pengguna internet tertarik menggunakan aplikasi web yaitu kesederhanaan yang terdapat dalam fitur- fitur aplikasi web. Selain itu internet juga memberikan kemudahan kepada penggunanya agar dapat mengakses aplikasi web dimana saja. Hal ini tentu saja mempermudah kegiatan manusia yang memanfaatkan aplikasi web. Namun, tidak ada yang sempurna di dunia ini, berbagai kelebihan aplikasi web dalam dunia internet juga memiliki kelemahan yang berhubungan dengan aspek keamanan yaitu sangat rentan terhadap serangan hacker.

Keamanan pada sebuah aplikasi web merupakan aspek penting yang harus dimiliki. Mengamankan aplikasi web dapat dilakukan dengan memasang firewall, anti virus, atau software sejenis pada server. Namun langkah yang lebih penting untuk mengamankan aplikasi web adalah dengan membuat kode program yang bebas dari bugs, karena jika hanya dengan melakukan pemasangan firewall akan memberikan celah untuk diserang apabila kode yang dibuat tidak bebas dari kesalahan logika pemrograman.

Modsecurity merupakan web application firewall, seperti firewall pada umumnya memiliki tugas untuk melakukan pemfilteran pada data yang masuk maupun keluar, dan melakukan blocking traffic yang dianggap berbahaya sesuai dengan rule yang ditetapkan. Setelah itu segala bentuk serangan yang telah terdeteksi akan disimpan pada suatu database. Dengan metode ini, diharapkan dapat memonitoring keamanan aplikasi web secara real- time sehingga dapat dilakukan suatu pencegahan melalui pemfilteran terhadap request HTTP dengan pola-pola yang berindikasi sebagai serangan dari hacker ke aplikasi web. Maka proyek akhir yang mengambil topik monitoring keamanan aplikasi web ini diberi judul "Implementasi Modsecurity Pada Aplikasi Web Sebagai Sistem Monitoring Keamanan Aplikasi Web Secara Real Time".

2. Dasar Teori dan Metodologi

Keamanan aplikasi web adalah suatu proses untuk mengamankan suatu web. Proses ini berupa suatu mekanisme yang bekerja untuk mencegah akses dan modifikasi oleh user yang tidak dikenal, terhadap data-data dari web yang tersimpan secara online.

SQL Injection merupakan cara mengeksploitasi celah keamanan yang muncul pada level atau "layer" database dan aplikasinya. Celah keamanan tersebut ditunjukkan pada saat penyerang memasukkan nilai "string" dan karakter-karakter contoh lainnya yang ada dalam instruksi SQL; dimana perintah tersebut hanya diketahui oleh sejumlah kecil individu (hacker maupun cracker) yang berusaha untuk mengeksploitasinya.

Cross-Site Script atau kependekannya XSS merupakan salah satu serangan injeksi kode (code injection attack). XSS dilakukan oleh penyerang dengan cara memasukan kode HTML (HyperText Markup Language) atau client script code lainnya kesuatu situs.

Remote file inclusion adalah penyisipan sebuah file dari luar suatu file dalam sebuah webserver dengan tujuan script didalam akan dieksekusi pada saat file yang disisipi diolah. Dampak dari File Inclusion bisa dikatakan "High Risk" karena File Inclusion bisa digunakan untuk mendapatkan akses shell, dan pada akhirnya dilakukan sebuah local explotation untuk mendapatkan hak akses penuh terhadap sistem.

Web Application Firewall (WAF) adalah suatu metode untuk pengamanan pada aplikasi web, yang berupaya mencegah adanya ancaman dari attacker.

Modsecurity merupakan salah satu module apache sebagai WAF (Web Application Firewall). Modsecurity berfungsi melakukan pemfilteran pada data yang masuk maupun keluar, dapat memonitoring traffic serta memblok traffic yang dianggap

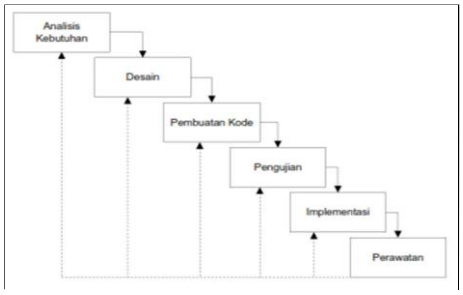
berbahaya dengan menyesuaikan rule yang sudah di tetapkan, secure directory, dan melakukan keamanan terhadap serangan hacker.

PHP merupakan kependekan dari kata Hypertext Preprocessor. PHP adalah bahasa skrip yang dapat ditanamkan atau disisipkan ke dalam HTML. Pemrograman PHP sangat cocok dikembangkan dalam lingkungan web, karena PHP bisa dilekatkan pada script HTML atau sebaliknya.

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL (bahasa Inggris: database management system) atau DBMS yang multithread, multi-user dengan sekitar 6 juta instalasi di seluruh dunia.

Server web dapat merujuk baik pada perangkat keras ataupun perangkat lunak yang menyediakan layanan akses kepada pengguna melalui protokol komunikasi HTTP atau HTTPS atas berkas-berkas yang terdapat pada suatu situs web dalam layanan ke pengguna dengan menggunakan aplikasi tertentu seperti browser web.

Metode yang digunakan dalam pengerjaan proyek akhir ini adalah metode waterfall, dapat dilihat pada gambar berikut :



Gambar 1. 1 Metode Waterfall
Sumber : Workbook Analisis Perancangan Sistem

Berikut adalah penjelasan dari tahap-tahap yang dilakukan dalam model metodelogi waterfall.

1. Analisis Kebutuhan
   Melakukan analisis terhadap kebutuhan sistem dimulai dari pengumpulan data sampai analisis data. Pengumpulan data dalam tahap ini dilakukan dengan studi literatur pada beberapa website maupun buku untuk mendapatkan informasi yang dibutuhkan mengenai konsep WAF, Web Server, Database, SQL Injection, Cross-Site Scripting, File Inclusion.

2. Desain
   Membuat perancangan dari hasil analisis yang telah dilakukan sebelumnya, mulai dari kebutuhan perangkat, kebutuhan perangkat lunak, WAF, serta serangan yang akan digunakan untuk menguji.

3. Implementasi.
   Tahap ini dilakukan implementasi perangkat keras, perangkat lunak, WAF sesuai dengan apa yang telah di spesifikasikan dan di desain pada tahapan desain sebelumnya.

4. Pengujian
   Metode pengujian dilakukan dengan cara melakukan percobaan serangan SQL Injection, Cross-Site Scripting, File Inclusion dengan pengujian yang sudah dirancang terhadap aplikasi web yang telah diimplementasikan modsecurity untuk membuktikan apakah modul aplikasi tambahan tersebut mampu mencegah atau mengurangi dampak dari serangan tersebut.

5. Penyusunan Laporan

3. Pembahasan

3.1 Gambaran Umum Sistem

Sistem ini akan dibangun dengan menggunakan modsecurity, sebuah web aplikasi firewall opensource yang akan di implementasikan pada Ubuntu 12.04, dimana pada modsecurity akan dikofigurasikan basic rule sebagai parameter pengidentifikasi serangan. Modsecurity akan melakukan penyaringan terhadap setiap request HTTP yang akan menuju server. Sehingga bila pada request HTTP mengandung serangan maka request tersebut akan di block atau di hentikan.

3.2 Kebutuhan Sistem

3.2.1 Kebutuhan Hardware

Dalam pengerjaan proyek akhir ini diperlukan komputer server yang akan di implementasikan modsecurity. Pada pengujian sistem dibutuhkan komputer lain yang digunakan sebagai client/ komputer hacker. Spesifikasi minimum perangkat keras yang di perlukan sebagai berikut adalah spesifikasi minimum perangkat keras komputer yang dibutuhkan untuk membangun sistem rancangan.

Tabel 3. 1
Spesifikasi minimum perangkat keras komputer

Hardware	Komputer Server	Komputer Penyerang
RAM	1GB	512MB
Hard	20GB	250GB
Processor	Single core	Pentium IV

Berikut spesifikasi komputer yang digunakan untuk implementasi sistem pada proyek akhir ini, yaitu:

Tabel 3. 2
Spesifikasi perangkat keras komputer yang digunakan

Hardware	Komputer Server	Komputer Penyerang
RAM	1GB	2GB
Hard	20GB	500GB
Processor	Single core VCPU	AMD A8

3.2.1 Kebutuhan Perangkat Lunak

Dalam pengerjaan proyek akhir ini spesifikasi perangkat lunak yang digunakan untuk membangun sistem adalah :

Tabel 3. 3 Spesifikasi perangkat lunak

No	Spesifikasi Software	Komponen
1	Windows 7, Ubuntu 12.04	Sistem Operasi
2	PHP	Bahasa Pemrograman website
3	MySQL	Database
4	Apache	Web Server
5	Mozila Firefox	Browser
6	Modsecurity	Web Aplication Firewall
7	Notepad++ dan Macromedia Dreamweaver	Editor
8	DVWA	Web Aplication Vulnarable

Daftar Pustaka

Clarke, SQL Injection Attacks and Defense. Burlington: Syngress Publishin, Inc, 2009. [2] M.R. Chandraratne, *Comparison of Three Statistical Texture Measures for Lamb Grading*, First International Conference on Industrial and Information System, ICIIS 2006, Sri Lanka, Agustus 2006.

Robert Hansen, Petko D. Petkov, Anton Rager, Seth Fogie J. Grossman, XSS Attacks: Cross Site Scripting Exploits and Defense. Burlington: Syngress Publishing, Inc, 2007.

OWASP Foundation, Unrestricted File Upload. Dipetik November 21, 2012 , Website: http://www.owasp.org/index.php/Unrestricted_File_Upload, 2013.

Lowe Scot, Mastering VMware Vsphere 5 (Menguasai VMware Vsphere 5).: John Wiley & Sons, Inc, 2011