Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache

Suryayusra[1)], Muhammad Muharromin[2)]
[1,2]Jurusan Teknik Informatika, Universitas Bina Darma
e-mail: Suryayusra@binadarma.ac.id, muhammadmuharromin@gmail.com

Abstrak

Penerapan sistem keamanan pada web server harus dilakukan karena web server dapat dengan mudah diserang oleh orang yang tidak bertanggung jawab. Penelitian ini akan menerapkan dan menganalisis kinerja keamanan dari aplikasi web firewall berbasis web server menggunakan ModSecurity dan Shadow Daemon, dimana tujuan dari penelitian sistem keamanan web server ini adalah untuk menganalisis kinerja ModSecurity dan Shadow Daemon dalam menjaga keamanan pada web server. Metode eksperimental, dalam penelitian ini akan mengumpulkan data dan mengimplementasikan firewall aplikasi web menggunakan ModSecurity dan Shadow Daemon sebagai sistem keamanan server web dan akan dilakukan analisis lebih lanjut. sebagai server keamanan web. Hasil dari penelitian ini akan menunjukkan bahwa dengan menggunakan Modsecurity dan Web Application Firewall berbasis Shadow Daemon pada sistem keamanan web server dapat memblokir serangan SQL injection, Cross Site Scripting (XSS), menampilkan tampilan pesan terlarang dan dengan menyembunyikan data dari pengguna yang mengeksekusinya.

Kata kunci *— Web Server, Firewall, WAF, ModSecurity, Shadow Daemon.*

Abstract

The application of a security system on the web server must be done because the web server can be easily attacked by irresponsible people. This study will implement and analyze the security performance of a web server-based firewall web application using ModSecurity and Shadow Daemon, where the purpose of this web server security system research is to analyze the performance of ModSecurity and Shadow Daemon in maintaining security on the web server. Experimental method, in this study will collect data and implement a web application firewall using ModSecurity and Shadow Daemon as a web server security system and further analysis will be carried out. as a web security server. The results of this study will show that using Modsecurity and a Shadow Daemon-based Web Application Firewall on a web server security system can block SQL injection attacks, Cross Site Scripting (XSS), display forbidden messages and hide data from users who execute them.

Keywords — *Web Server, Firewall, WAF, ModSecurity, Shadow Daemon.*

1. PENDAHULUAN

Seiring dengan kemajuan teknologi , Terdapat macam-macam web server yang digunakan dalam mempermudah dalam mengelola data. Web Server sekarang ini

telah menjadi bagian yang pasti di lakukan dalam kegiatan sehari-hari, Hal tersebut tentunya dapat mempermudah aktivitas manusia untuk memperoleh sumber informasi. Namun, dalam dunia teknologi tidak ada yang sempurna, berbagai kelebihan di dunia internet pasti adal kekurangan, dalam hal seperti inilah yang rentan terhadap serangan dari pihak yang tidak bertanggung jawab.

Keamanan server web adalah bagian penting dari perlindungan terhadap serangan. Keamanan server web dapat dicapai dengan menginstal firewall, program anti-virus, atau dengan perangkat lunak open source yang sama dengan komputer yang digunakan. Keamanan pada server web dapat dicapai dengan memasang web application firewall (WAF) untuk mencegah serangan pada layanan web [1].

Firewall aplikasi web adalah metode untuk melindungi server web yang mencegah ancaman dari penyerang. Web application firewall dapat bekerja dengan melakukan konfigurasi pada web terlebih dahulu dan memasukkan script crs pengembangan aplikasi, sehingga dapat diterapkan pada aplikasi yang akan di uji coba. Seperti firewall seperti biasanya, ia menyaring data yang masuk dan keluar sehingga dapat menghentikan lalu lintas berbahaya menurut aturan yang ditentukan.

Firewall aplikasi web memiliki beberapa fungsi dalam mengimplementasikan keamanan aplikasi web, mulai dari pemantauan lalu lintas, direktori aman, penyaringan string dan proteksi serangan injeksi SQL, Cross-Site Scripting. Firewall Aplikasi Web membuat lapisan keamanan yang mampu mendeteksi dan mencegah serangan pada web. Adapun tindakan yang bisa dilakukan, seperti memblokir serangan dengan menampilkan status 403. Dimana yang nantinya virtual patching akan memblokir permintaan jahat.

2. METODE PENELITIAN

Metode penelitian ini akan menggunakan metode eksperimen. Penelitian ini akan mencoba mengimplementasikan dan menganalisis web application firewall dalam sistem keamanan web server. Hasil pengujian dianalisis guna membuat rekomendasi yang sesuai untuk firewall sebagai sistem keamanan server web. Dari hasil analisis maka akan disimpulkan tentang manfaat, fungsionalitas dan kinerja dari Web Application Firewall yang telah dibuat [2].

2.1 Metode Pengumpulan Data

Berikut teknik pengumpulan data dalam penelitian ini :

1. Mencari Informasi

Belajar dari buku web, jurnal penelitian, dan artikel tentang firewall aplikasi web, jaringan komputer, sistem keamanan web, dan informasi pendukung penelitian sehingga dapat membantu peneliti memecahkan masalah topik penelitian.

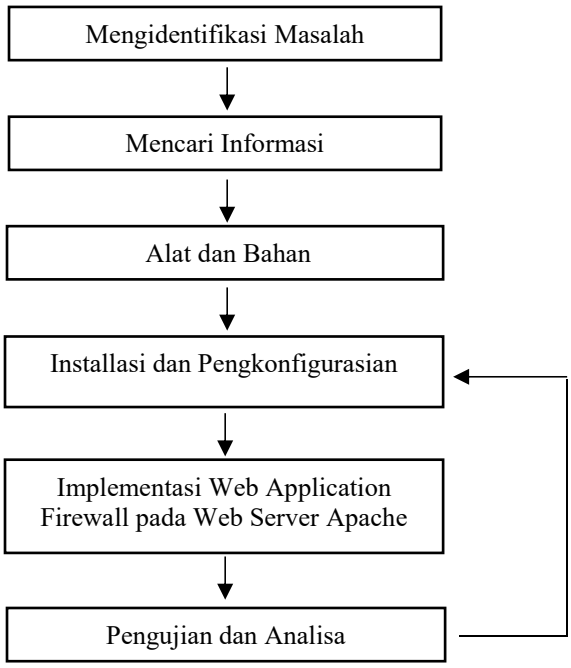
2. Studi Laboratorium

Hasil data akan diuji coba dengan melakukan testing di Kampus Bina Darma tepatnya di ruan DSTI, perihal uji coba sistem keamanan web menggunakan Web Application Firewall.

2.2 Rencana Kerja Sistem

Berikut ini proses implementasi web application firewall sebgai sistem kemanan web adalah sebagai berikut :

1. Mengidentifikasi Masalah
2. Mencari Informasi
3. Alat dan Bahan
4. Installasi dan Pengkonfigurasian
5. Implementasi Web Application Firewall pada Web Server Apache



Gambar 1. Rencana Sistem Kerja

3.HASIL DAN PEMBAHASAN

3.1 Desain Sistem

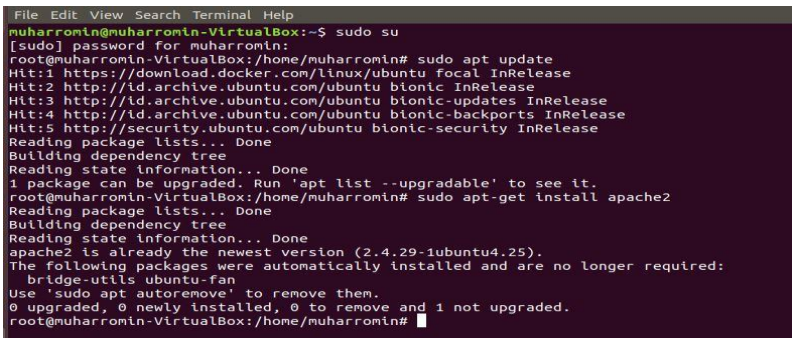
Sebelum melakukan penelitian ini ada beberapa sistem yang akan disiapkan terlebih dahulu untuk memulai uji coba yang akan dilakukan terhadap ModSecurity dan Shadow Daemon.

1.Desain Aplikasi Web

Dalam penelitian ini akan medesain web server, web server yang akan digunakan ialah web apache yang berbasis MySQL

a. Instalasi Apache

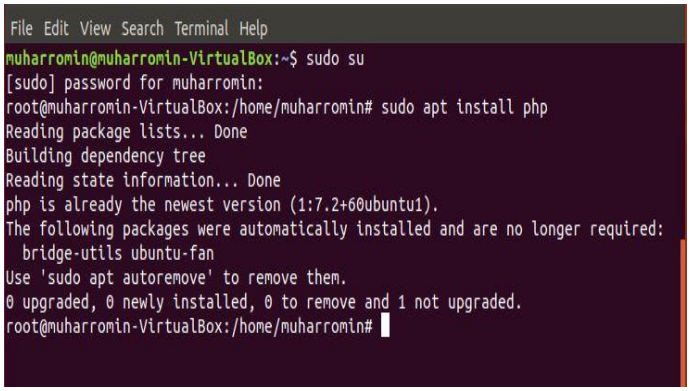
Apache Web Server adalah program untuk menjalankan Web pada komputer [3]. Apache ini akan digunakan sebagai host utama untuk menjalankan website yang akan digunakan untuk penelitian ini. Untuk mengetahui cara menginstal apache Anda akan menggunakan Ubuntu dengan mengetik ”sudo apt update” lalu ketika sudah selesai maka ketikkan perintah berikutnya yaitu “sudo apt-get install apache2”. Setelah selesai melakukan penginstallan, untuk melihat hasilnya akan ada direktori /var/www/html/ di linux Ubuntu.



Gambar 2. installasi Apache2

b. Installasi PHP

PHP merupakan bahasa pemrograman yang dipakai dalam pengembangan suatu web. Installasi PHP ini dilakukan agar bahasa pemrograman yang digunakan pada aplikasi web yang akan digunakan di penelitian ini. Berikut cara untuk menginstallasi PHP ini dengan cara menegtikkan perintah “sudo apt install php"



Gambar 3. Installasi PHP

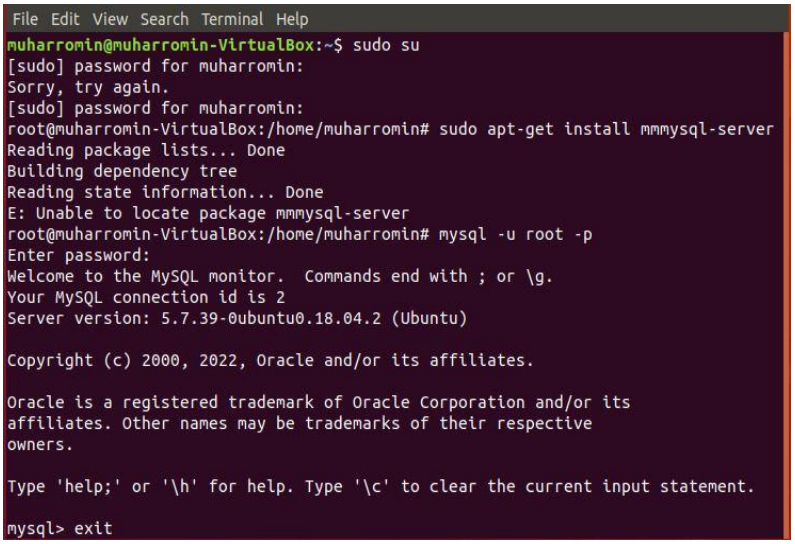
c. Installasi PHPMyAdmin

PHP MyAdmin adalah program berbasis PHP yang digunakan untuk mendukung manajemen grafis database MySQL [3]. Langkah-langkah yang diperlukan untuk menginstal phpmyadmin, dengan menegtik “sudo apt-get install phpmyadmin” saat proses installasi berlangsung , akan diarahkan untuk memilih web , lalu pilih saja apache, ketika selesai nanti akan disuruh buat password untuk login ke phpmyadmin, dan tunggu proses hingga selesai. Lalu buka coba buka php myadmin di web dengan mengetikkan “http:IP-Server-anda/phpmyadmin”.

Gambar 4. Tampilan PHP MyAdmin

d. Installasi MySQL

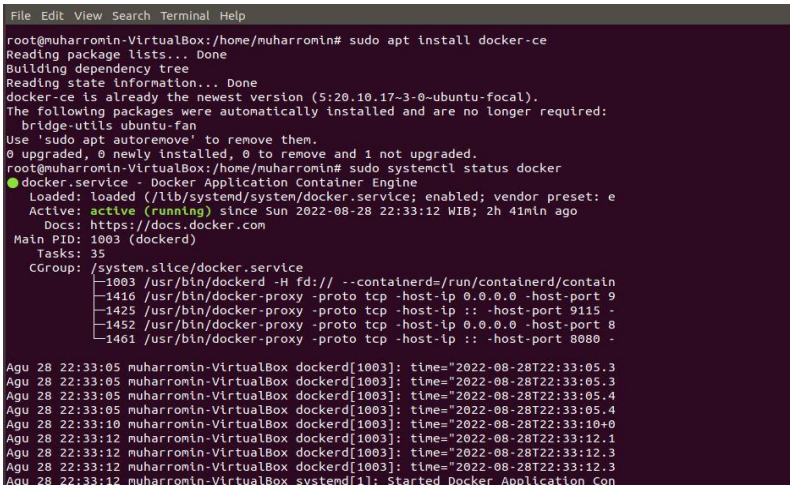
MySQL adalah program yang digunakan untuk menyimpan data yang akan digunakan oleh sebuah website atau data yang akan digunakan oleh sebuah website atau data lain yang akan digunakan oleh sebuah program di komputer [3]. Server MySQL digunakan untuk media menyimpan data website yang akan diinstal pada web server. Untuk mempelajari cara menginstal MySQL dengan mengetik “ sudo apt-get install mysql-server” lalu setelah proses installasis selesai, nanti bisa mengecek keberhasilan installasinya dengan cara masuk ke MySQL menggunakan perintah “mysql -u root -p”.



Gambar 5. Installasi MySQL

e. Installasi Docker

Docker merupakan aplikasi yang menyederhanakan expositions pengelolaan compositions aplikasi di dalam kontainer[4]. Untuk melakukan isntallasi docker ini dapat memasukkan perintah" sudo apt update " lalu perintah berikutnya " sudo apt install apt-transport-https ca-certificates curl software-properties-common " lalu tambahkan kunci GPG untuk repositori docker " curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add – " dan juga tambahkan repositori docker ke sumber APT " sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable" " selanjutnya perbarui basis data " sudo apt update " pastikan akan menginstall dari repo docker " apt-cache policy docker-ce " dan yang terakhir install deocker dengan masukkan perintah " sudo apt install docker-ce "



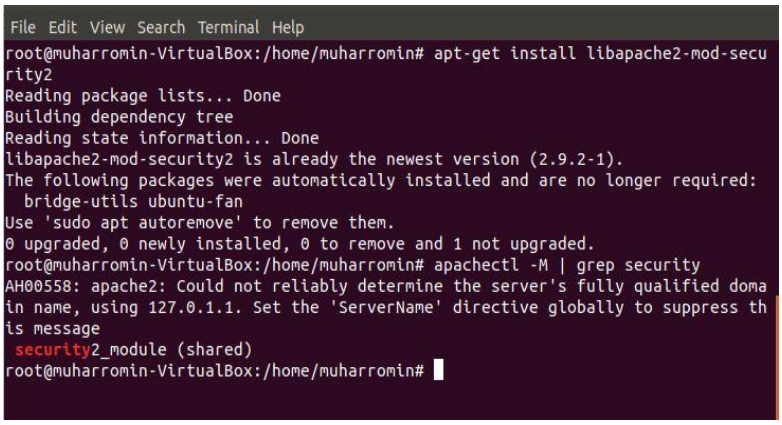
Gambar 6. Installasi Docker

2. Implementasi Web Application Firewall

a. ModSecurity

Dalam melakukan penginstallan web application firewall untuk menjaga web agar terlindungi, Langkah pertama harus menginstall module modsecurity, cara untuk menginstall

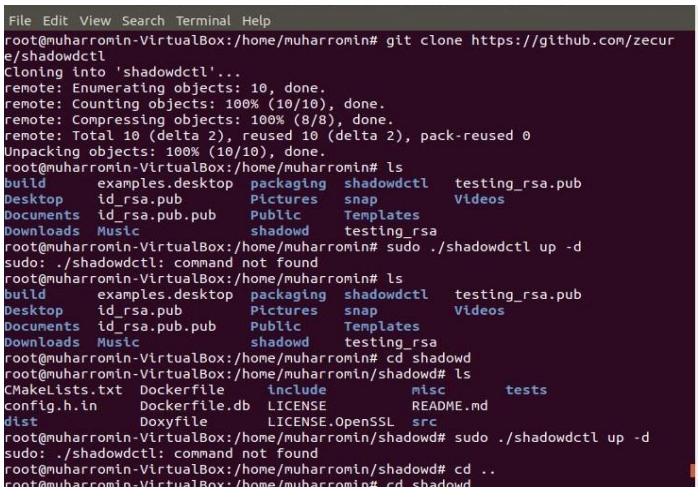
module modsecurity dengan cara mengetikkan “apt-get install libapache2-mod-security2“. Untuk melihat apakah modsecurity sudah terinstall kita masukkan “ apachectl -M | grep –color security “ dan “ is -l /var/log/apache2/modsec_audit.log ”. Ketika telah berhasil install maka tampilanya akan seperti gambar dibawah ini.



Gambar 7. Installasi ModSecurity

b. Shadow Daemon

Langkah untuk menginstall shadow daemon cukup mudah, yang pertama harus menginstall docker terlebih dahulu dan juga harus mempunyai akun github, jika sudah langsung saja masukkan perintah yang pertama “ git clone https://github.com/zecure/shadowctl.git “ kemudian “ cd shadowctl “ lalu “ sudo ./shadowctl up -d “ tunggu hingga wadah shadowd_ui benar-benar dimulai. Setelah installasi selesai, lalu tambahkan akun pengguna untuk antarmuka web.



Gambar 8. Installasi Shadow Daemon

Lalu untuk mengatur konfigurasi shadow daemon dapat memasukkan perintah “ sudo nano /etc/php/7.2/apache2/php.ini “ maka akan tampil seperti gambar dibwah ini.

3.2 Hasil Pengujian

1. Pengujian dengan Firewall Mod Security

a. Uji coba XSS (Cross Site Scripting)

Percobaan menggunakan Cross Site Scripting (XSS) ini memakai module crs dengan index “hellow”

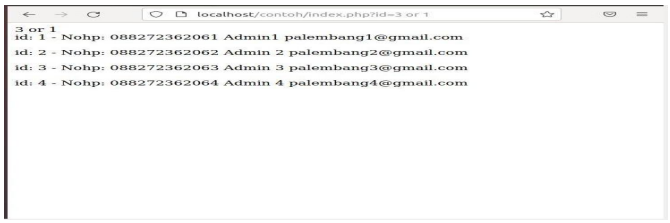
Gambar 9. Percobaan XSS Tanpa ModSecurity

Lalu akan diuji coba ketika web application firewall sedang posisi aktif maka hasil yang didapatkan akan muncuk kata *Forbidden.*

Gambar 10. XSS berhasil di block dengan ModSecurity

b. Pengujian SQL Injection

Pengujian serangn SQL Injection ini menggunakan crs index php seperti ambar dibawah ini :



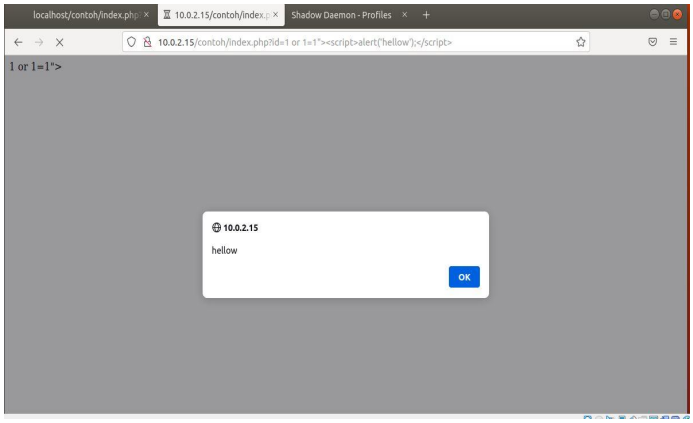
Gambar 11. Pengujian SQL Injection tanpa Mod Security

Gambar 12. Pengujia SQL Injection dengan ModSecurity

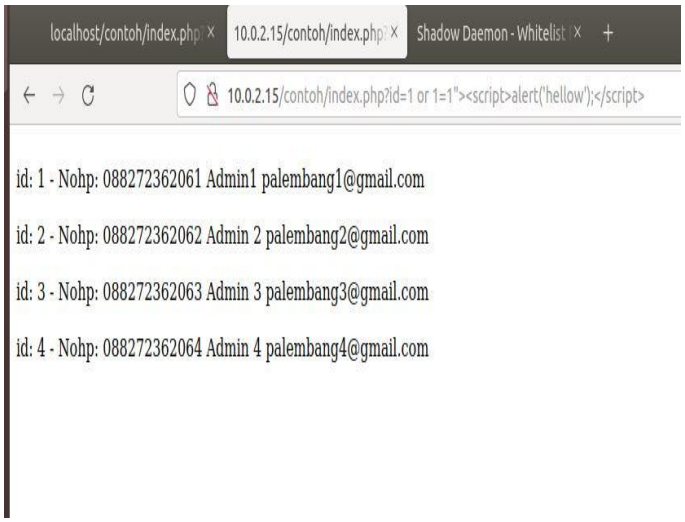
2. Pengujian dengan Firewall Shadow Daemon

a. Uji coba XSS (Cross Site Scripting)

Percobaan menggunakan Cross Site Scripting (XSS) ini memakai module crs dengan index “hellow”



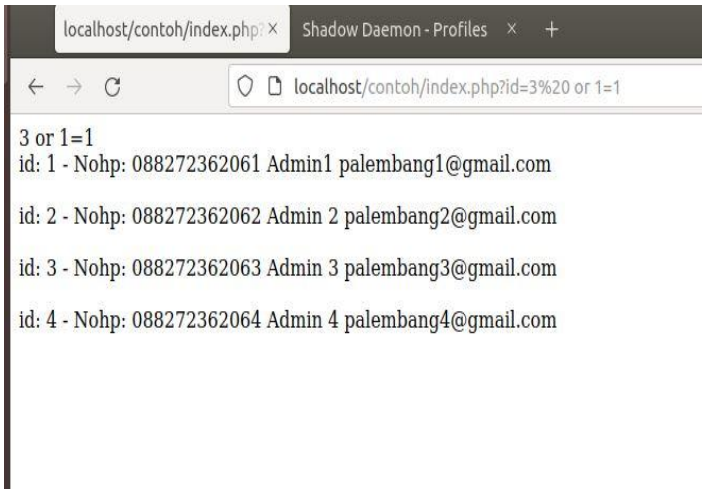
Gambar 13. Serangan XSS Tanpa Shadow Daemon



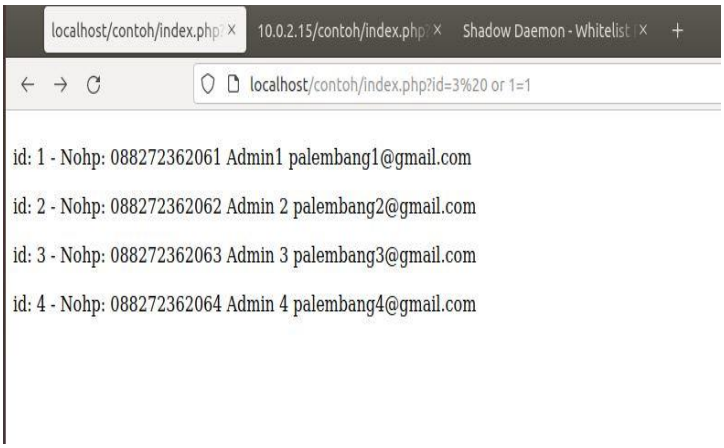
Gambar 14. Serangan XSS dengan Shadow Daemon

b. Pengujian SQL Injection

Pengujian serangn SQL Injection ini menggunakan crs index php seperti ambar dibawah ini :



Gambar 15. Serangan SQL Injection tanpa Shadow Daemon



Gambar 16. Serangan SQL Injection dengan Shadow Daemon

4. KESIMPULAN

Dari penelitian yang telah dilaksanakan dapat kita simpulkan bahwa web application firewall dapat melindungi web server agar lebih aman, tapi ada perbedaan antara ModSecurity dan Shadow Daemon, ModSecurity langsung memblock serangan terhadap web server sehingga web tidak bisa di akses sama sekali sedangkan Shadow Daemon web masih dapat di akses tapi tapi serangan yang masuk disaring dan di block.

5.SARAN

Dalam kesimpulan dari penelitian ini penulis akan memberikan saran terhadap web application firewall. Web Application Firewall sangat mutakhir dalam melindungi web secara real time, dan juga web application firewall ini adalah gen terbaru dari firewall yang biasanya, Untuk hasil yang maksimal, coba terapkan beberapa aturan dan modul keamanan lain pada website.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada pembimbing saya atas dukungan dan dorongan dalam melakukan penelitian ini.

DAFTAR PUSTAKA

[1] Widianti, S. R., & Azzam, I. A. (2018). Analisis Upaya Peretasan Web Application Firewall Dan Notifikasi Serangan Menggunakan Bot Telegram Pada Layanan Web Server. *Elektra*, 19-28.

[2] Riska, & Alamsyah, H. (2021). Penerapan Sistem Keamanan WEB Menggunakan Metode WEB Aplication Firewall. *Jurnal Amplifier*, Vol 11 No 1.

[3] Emanuel, A. W. (2006). Instalasi Apache Web Server, Mysql Database, Dan PHP Pada Sistem Operasi Fedora Core 5. *Jurnal Informatika UKM*, 23 - 35.

[4] Bik, M. F. (2017). Implementasi Docker Untuk Pengelolaan Banyak Aplikasi Web (Studi Kasus : Jurusan Teknik Informatika UNESA). *Jurnal Manajemen Informatika*, 46-50.

[5] Akhriana, A., & Irmayana, A. (2019). Web App Pendeteksi Jenis Serangan Jaringan Komputer Dengan Memanfaatkan Snort Dan Log Honeypot. 87-98.

[6] Anggraena, J. K. (2013). Simulasi Keamanan Pada Aplikasi Web Dengan Web Application Firewall. *Jurnal Ilmiah Komputer Dan Informatika (KOMPUTA)*, 45-50.

[7] Laitupa, D. R., Ismail, S. J., & Rizal, M. F. (2015). Implementasi Modsecurity Sebagai Sistem Monitoring Keamanan Aplikasi Web Secara Real Time. *E-Proceeding Of Applied Science*, 2132 - 2134.

[8] Ridho, F. (2015). Kinerja Modsecurity Technical Report (Studi Kasus: Pencegahan Terhadap Serangan Sql Injection). *Jurnal Aplikasi Statistika Dan Komputasi Statistik*, 75-101.

[9] Wiguna, B., Prabowo, W. A., & Ananda, R. (2020). Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, 245-256.

[10] Putra, N. R. (2021). Web Application Firewall Untuk Meningkatkan Keamanan Informasi . *Jurnal Jiifor*, 21-26.