Penerapan Sistem Keamanan WEB Menggunakan Metode WEB Aplication *Firewall*

Riska[1*,] Hendri Alamsyah[2]
[1,2]Universitas Dehasen Bengkulu, Indonesia
E-mail: [1]*riska.iskandar@unived.ac.id;* [2]*hendri.alamsyah@unived.ac.id*

ABSTRACT

The application of a security system on the web needs to be done considering that the web itself can be accessed through a public network. In this study, a Web Application Firewall (WAF)-based security system will be implemented using modsecurity, in which the purpose of implementing this web security system is to understand the concept of a security system on the web and pay attention to the results before the application of the firewall and after the application of the firewall on the web. This research uses experimental research methods, in this study the implementation of a web application firewall (WAF) using modsecurity as a web security system is carried out, then an analysis is carried out to get the right recommendations for a firewall as a web security system. The results of this study indicate that a firewall using the modSecurity module and rule based on the Web Application Firewall (WAF) on a web security system can block SQL Injection, Cross Site Scripting (XSS), and Command Execution by displaying an error message to the user who performs the command.
Keywords: Security System, Web, firewall, WAF, modsecurity

ABSTRAK

Penerapan sistem keamanan pada web perlu dilakukan mengingat web itu sendiri dapat diakses melalui jaringan publik. Dalam penelitian ini akan diterapkan sistem keamanan berbasis *Web Aplication Firewall* (WAF) menggunakan modsecurity, yang mana tujuan dari penerapan sistem keamanan web ini adalah untuk memahami konsep sistem keamanan pada web dan memperhatikan hasil sebelum penerapan *firewall* dan sesudah penerapan *firewall* pada web. Penelitian ini menggunakan metode penelitian eksprimen, pada penelitian ini dilakukan implementasi *web aplication firewall* (WAF) menggunakan modsecurity sebagai sistem keamanan web, selanjutnya dilakukan analisa untuk mendapatkan rekomendasi yang tepat untuk *firewall* sebagai sistem keamanan web. Hasil penelitian ini menunjukkan bahwa *firewall* dengan menggunakan module dan rule modSecurity berbasis *Web Aplication Firewall* (WAF) pada sistem keamanan web dapat memblokir SQL *Injection*, *Cross Site Scripting* (XSS), dan *Command Execution* dengan menampilkan pesan *error* kepada *user* yang melakukan perintah tersebut.
Kata Kunci : Sistem Keamanan, Web, *firewall*, WAF, modsecurity

1. PENDAHULUAN

Aplikasi web saat ini sudah menjadi bagian yang tidak bisa dipisahkan dalam kehidupan sehari – hari, sebab untuk memperoleh informasi dalam keadaan seperti saat ini semuanya didapatkan melalui aplikasi berbasis web dan juga aplikasi mobile. Hal ini tentu saja mempermudah kegiatan manusia untuk mendapatkan informasi dari pemanfaatan aplikasi web ini. 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 dari pihak yang tidak bertanggung jawab.

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 komputer ataupun *router* yang terhubung langsung atau berada dalam satu jaringan dengan *server* aplikasi web tersebut. Keamanan pada aplikasi web dapat dilakukan dengan menggunakan *web application firewall* (WAF) yang dipasangkan pada layanan web *server*[1]. *Web application firewall* adalah suatu metode untuk pengamanan pada aplikasi web, yang berupaya mencegah adanya ancaman dari *attacker* ataupun *hacker*[2][3]. *Web application firewall* sudah dapat bekerja terlebih dahulu tanpa melakukan konfigurasi tambahan pada *server web* sehingga tidak perlu lagi dilakukan perubahan atas *script default* aplikasi, sehingga dapat diterapkan pada aplikasi yang sudah berjalan walaupun *script* tersebut belum sesuai dengan keinginan[4].

Beberapa fungsi yang dimiliki *Web application firewall* (WAF) seperti, monitoring trafik, secure directory, filtering string dan proteksi dari serangan seperti SQL *Injections*, *Cross-Site Scripting* (XSS), dan *Unrestricted File Upload*. *Web application firewall* membuat suatu lapisan keamanan yang dapat mendeteksi serta mencegah serangan terhadap aplikasi web. Adapun tindakan yang dapat dilakukan seperti menghentikan

request dengan status 403 *forbidden* dan juga dapat melakukan *virtual patching*[4]. *Virtual patching* ini merupakan rule yang dapat diterapkan untuk melakukan *patch* tanpa menyentuh aplikasi guna memblokir *request* yang berbahaya[5].

Dari uraian diatas, penulis akan menerapkan firewall untuk sistem keamanan, dimana salah satu metode pengamanan yang dapat diterapkan yaitu dengan menggunakan web aplication firewall. Dimana metode tersebut akan diterapkan pada website yang akan penulis buat. Untuk bentuk pengujian pertahanan, akan dicoba disimulasikan dengan teknik serangan yang paling sering terjadi. Dengan sistem pertahanan ini, diharapkan dapat memberikan rekomendasi untuk meningkatkan segi keamanan, sehingga aplikasi web yang dibangun tidak hanya mempunyai desain yang baik namun juga terjaga integritas datanya.

2. TINJAUAN PUSTAKA

A. Sistem Kemanan

Sistem keamanan jaringan merupakan suatu proses untuk melakukan identifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer. Tujuan dari pengamanan sistem jaringan ini adalah untuk mengantisipasi resiko ancaman berupa perusakan bagian fisik komputer maupun pencurian data seseorang[6]. Yang dimaksud ancaman fisik itu adalah yang merusak bagian fisik komputer atau hardware komputer sedangkan ancaman logik yaitu berupa pencurian data atau penyusup yang membobol akun seseorang.

B. Web

World Wide Web (biasa disingkat WWW) atau web merupakan salah satu aplikasi internet yang paling popular. Web adalah sebuah sistem dimana informasi dalam bentuk teks, gambar, suara dan lainnya yang tersimpan dalam sebuah internet web *server* ditampilkan dalam bentuk HTML (*hypertext Markup language*)[7].

C. Web Aplication Firewall (WAF)

WAF adalah aplikasi yang menyaring, memantau, dan memblokir ancaman-ancaman pada website. Salah satu aplikasi WAF yang ada adalah ModSecurity. Beberapa serangan yang dapat diatasi oleh ModSecurity adalah SQL Injection dan DDoS Attack.[3]

Web Application Firewall (WAF) sangat mirip dengan bagaimana *firewall* tradisional bekerja. *Firewall* bekerja berdasarkan suatu set aturan yang dikonfigurasi pada *firewall* atau yang disebut dengan *rule*. Aturan ini yang selektif mengizinkan atau menolak lalu lintas jaringan. Aturan pada WAF secara khusus dirancang untuk menyaring lalu lintas jaringan dengan menggunakan protokol HTTP. Aturan ini juga mampu mendeteksi serangan umum, seperti *probe* (upaya mendapatkan informasi awal sebelum melakukan serangan) dari serangan SQL *Injection* dan upaya XSS. *Firewall* bisa berupa perangkat lunak yang di-*instal* pada *host*, atau sebagai perangkat keras khusus. WAF adalah salah satu mekanisme pertahanan awal pada sistem[2].

D. ModSecurity

ModSecurity adalah WAF yang bersifat open source yang merupakan modul tambahan pada Apache. Beberapa fitur mod_security adalah pemeriksaan log, akses ke setiap bagian dari request yang ditujukan ke server (termasuk isi request atau body) dan memberikan respon terhadap hasil pemeriksaan, memiliki rule yang berdasarkan aturan regular expression yang fleksibel, pemeriksaan berkas yang diunggah, validasi real-time dan juga perlindungan buffer-overflow[2].

3. METODE PENELITIAN

Metode penelitian yang digunakan adalah metode eksprimen. Pada penelitian ini dilakukan Implementasi *firewall* sebagai sistem keamanan web. Hasil eksprimen selanjutnya didokumentasikan untuk melakukan analisa sehingga dihasilkan rekomendasi yang tepat untuk *firewall* sebagai sistem keamanan web. Dari hasil analisa tersebut nantinya akan mendapatkan kesimpulan mengenai manfaat, fungsi serta kelebihan dari sistem yang sudah dibangun.

A. Metode Pengumpulan Data

Adapun teknik pengumpulan data yang digunakan dalam penyusunan laporan penelitian ini adalah sebagai berikut:

1. Studi Pustaka

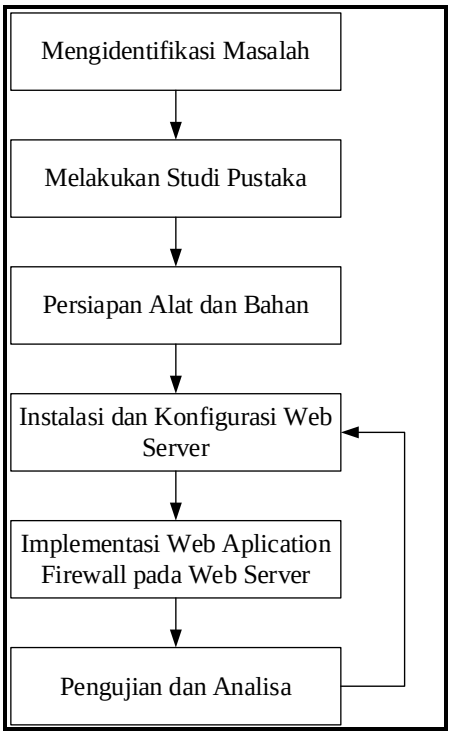
Mempelajari buku-buku, e-book, Jurnal dan artikel tentang komputer, jaringan komputer, sistem keamanan, web dan materi-materi pendukung lainnya, sehingga dapat membantu penulis menyelesaikan penelitian ini.

2. Studi Laboratorium

Data penelitian dikumpulkan dengan melakukan percobaan di Universitas Dehasen Bengkulu tepatnya di laboratorium jaringan, mengenai cara merancang sistem keamanan web menggunakan *firewall*.

B. Rencana Kerja Sistem

Rencana kerja dari implementasi *web aplication firewall* (WAF) sebagai sistem keamanan pada web adalah sebagai berikut.



Gambar 1. Rencana Kerja Sistem

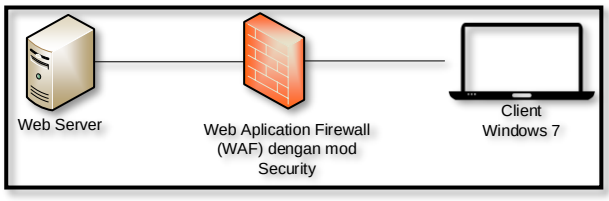
4. HASIL DAN PEMBAHASAN

A. Desain Sistem

Sebelum melakukan penelitian terkait dengan sistem keamanan web menggunakan metode web aplication firewall (WAF), terlebih dahulu akan dilakukan desain dari sistem yang akan diteliti. Adapun beberapa desain sistem yang dibutuhkan adalah sebagai berikut.

1. Infrastruktur Jaringan

Infrastruktur jaringan atau yang lebih sering disebut dengan topologi jaringan yang akan digunakan dalam penelitian ini adalah sebagai berikut.



Gambar 2. Infrastruktur Jaringan yang digunakan

Dari Gambar 2 diatas, dapat dilihat sebuah infrastruktur atau topologi dari jaringan yang akan digunakan dalam penelitian, dimana terdapat sebuah web *server* yang akan dilindungi oleh *web aplication firewall* (WAF) dari serangan client.

2. Desain Aplikasi Web

Aplikasi web yang akan digunakan dalam penelitian ini hanya sebuah aplikasi web sederhana yang menggunakan bahasa pemrograman PHP denga basis data menggunakan MySQL.

a. Instalasi Apache

Web *server* apache ini digunakan sebagai media untuk menjalankan website yang akan digunakan dalam penelitian ini. Dalam penelitian ini webserver apache akan diinstall pada web *server*. Untuk menginstall apache web *server* ini dapat dilakukan dengan cara mengetikkan perintah “apt-get install –y apache2”. Setelah instalasi selesai dilakukan, untuk melihat hasilnya akan ada direktori /var/www/html di linux ubuntu.

b. Instalasi PHP

Instalasi php dilakukan untuk mendukung bahasa pemrograman yang digunakan pada aplikasi website yang digunakan dalam penelitian ini, sehingga perlu juga di-install beberapa module php yang dibutuhkan seperti php-mbstring, php-pear, php-mysql, dan php-pdo. Untuk kebutuhan tersebut, dapat dilakukan dengan cara mengintal php server . Adapun cara yang dapat digunakan adalah dengan mengetikkan perintah “apt-get -y install php php-mbstring php-pear php-mysql php-pdo php-gd libssh-php”.

c. Instalasi PHPMyAdmin

Untuk melakukan instalasi phpmyadmin, dapat dilakukan dengan cara mengetikkkan perintah “apt-get install phpmyadmin” pada terminal di linux ubuntu server . Saat instalasi berlansung, akan ada permintaan pemilihan web server yang digunakan, pilih apache sesuai yang sudah di install sebelumnya dan masukkan password yang dibutuhkan dan tunggu hingga proses instalasi selesai dilakukan.

d. Instalasi MySQL

MySQL server ini digunakan sebagai media untuk menyimpan data website yang akan digunakan dalam penelitian ini. Dalam penelitian ini MySQL server akan diinstall pada webserver . Untuk menginstall MySQL server ini dapat dilakukan dengan cara mengetikkan perintah “apt-get install –y mysql-server mysql-client”, Selama proses instalasi, akan diminta untuk mengisi password pada root user, masukkan password yang akan digunakan dan mudah untuk diingat.

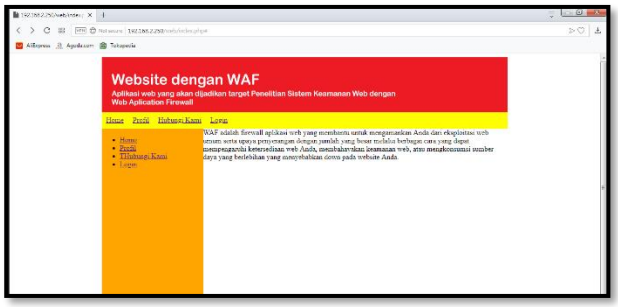
Selanjutnya akan dilakukan konfigurasi untuk menambahkan database pada web server , untuk menambahkan database ke dalam mysql server dapat dilakukan dengan mengetikkan berintah berikut.

a) Mysql –u root –p, lalu enter
b) Kemudian masukkan password yang sudah di inputkan sebelumnya.
c) Kemudian ketikkan “create database sample, lalu enter

d) Selanjutnya ketikkan “GRANT ALL PRIVILEGES sample.* to root@localhost; lalu enter.
e) Dan terakhir ketikkan “FLUSH PRIVILEGES” dan enter.
f) Ketik exit untuk mengakhiri konfigurasi.

e. Instalasi dan Konfigurasi Aplikasi Web

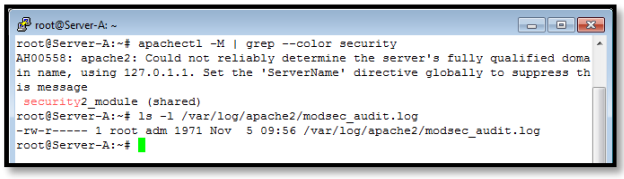
Website yang akan menggulis terapkan dalam penelitian ini dalah website sederhana yang digunakan untuk pengujian keamanan web server dengan menggunakan firewall berbasis web aplication firewall (WAF) yang dalam hal ini akan menggunakan modsecurity. Adapun hasil dari desain aplikasi web yang sudah dibuat dapat dilihat seperti Gambar berikut.



Gambar 3. Tampilan Aplikasi Web

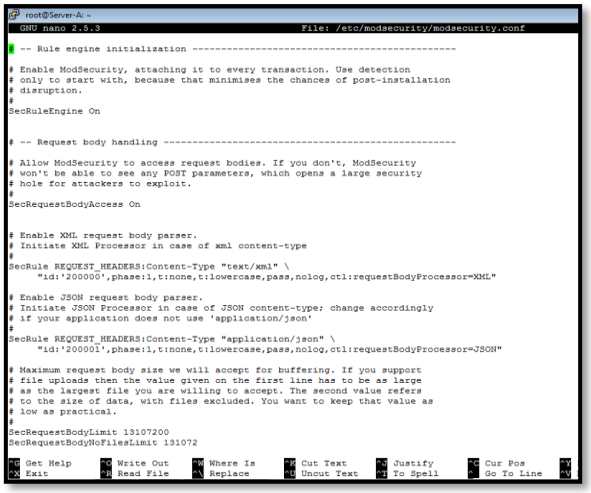
3. Implementasi WAF

Untuk melakukan implementasi *firewall* dalam sistem keamanan web *server* , langkah pertama yang harus dilakukan adalah menambahkan module modSecurity terlebih dahulu. Adapun untuk menambahkan *module* tersebut adalah dengan mengetikkan perintah “apt-get install libapache2-modsecurity modsecurity-crs” sehingga *server* akan dapat menerima file modSecurity dari internet. Untuk memastikan *module firewall* modSecurity sudah terpasang dengan benar dapat dilakukan dengan mengetikkan perintah “apachectl -M | grep --color security” dan “ls -l /var/log/apache2/modsec_audit.log”. Adapun hasil dari instalasi tersebut dapat dilihat seperti berikut ini.



Gambar 4. Hasil Instalasi Module ModSecurity

Setelah berhasil menambahkan module modsecurity kedalam web server, berikut tampilan dari rule modsecurity.



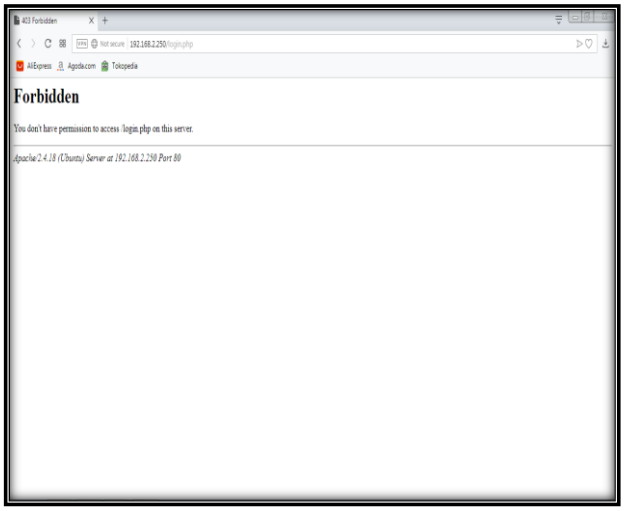
Gambar 5. Rule WAF Modsecurity

Untuk melakukan konfigurasi terhadap rule *firewall* yang sudah di implementasikan seperti Gambar 5, dapat dilakukan dengan mengetikkan perintah “nano /etc/modsecurity/modsecurity.conf” sehingga dapat melakukan konfigurasi terhadap file *firewall* yang sudah diterapkan.

B. Hasil Pengujian

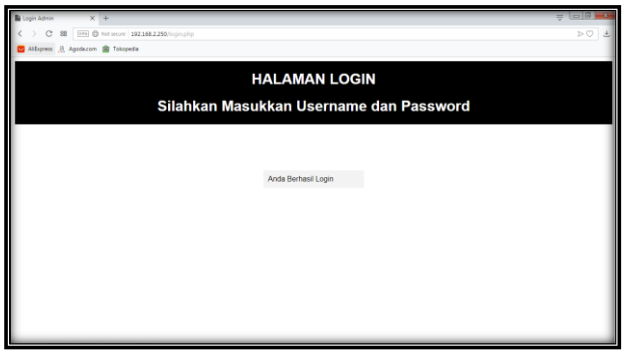
1. Pengujian Pengujian SQL Injection

Pengujian ini dilakukan dengan dua skenario pengujian yaitu melakukan SQL *injection* saat WAF di aktifkan dan WAF di non-aktifkan. Adapun hasil pengujian SQL *injection* saat WAF diaktifkan dapat dilihat seperti Gambar berikut.



Gambar 6. Login SQL Injection di Blok

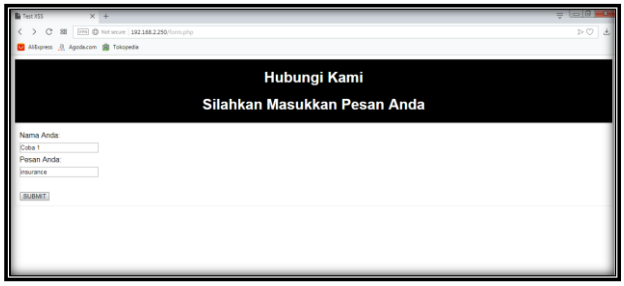
Hasil dari pengujian ini adalah penulis tidak berhasil login dengan menggunakan kode SQL *Injection* dan menampilkan pesan 404 Forbiden. Selanjutnya pengujian kedua dilakukan saat WAF di non-aktifkan. Adapun hasilnya dapat dilihat pada gambar berikut.



Gambar 7. Login SQL Injection Berhasil

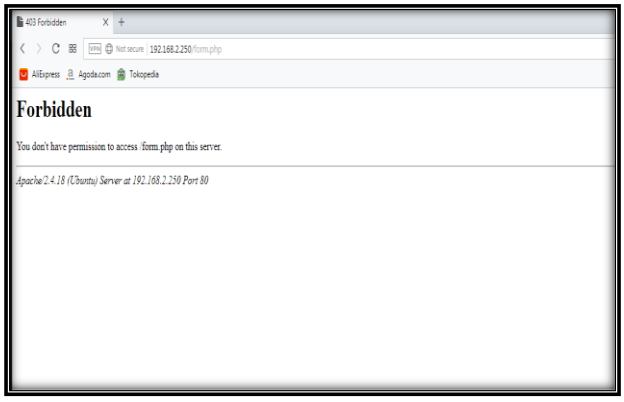
2. Pengujian *Cross Site Scripting* (XSS)

Pengujian ini dilakukan dengan cara mengklik tombol hubungi kami dan memasukkan kode unik yang sering digunakan pada script *Cross Site Scripting* (XSS). Untuk lebih jelasnya dapat dilihat seperti berikut ini.



Gambar 8. Percobaan XSS

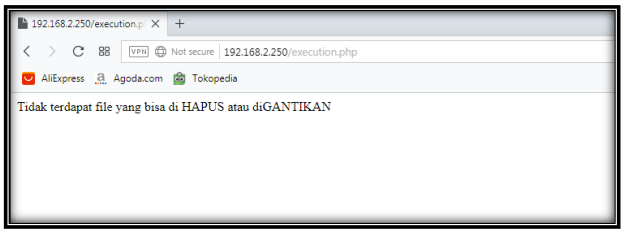
Dari pengujian yang penulis lakukan seperti pda Gambar 8 diatas dengan posisi *firewall* yang sudah aktif dan berjalan pada web *server*, hasil yang didapatkan adalah *firewall* melakukan pemblokiran terhadap pengujian tersebut dan memberikan informasi 404 *forbiden*. Untuk lebih jelasnya dapat dilihat pada gambar berikut.



Gambar 9. XSS Berhasil di Blok

3. Pengujian *Command Execution*

Pengujian ini dilakukan dengan memasukkan file *script command execution* kedalam direktori website yang sudah penulis terapkan diatas tadi. Hasil yang didapatkan dari pengujian ini, *script command execution* tersebut tidak berhasil menemukan file didalam direktori tersebut. Untuk lebih jelasnya dapat dilihat seperti berikut ini.



Gambar 10. Command Execution Berhasil di Blok

Dari hasil pengujian sudah dilakukan, dapat dilihat bahwah *firewall* dengan menggunakan module dan rule modSecurity berbasis *web aplication firewall* (WAF) pada sistem keamanan web dapat memblokir SQL *Injection*, *Cross Site Scripting* (XSS), dan *Command Execution* dengan menampilkan pesan eror kepada *user* yang melakukan perintah tersebut.

5. PENUTUP

A. Kesimpulan

Dari hasil penelitian yang dilakukan, dapat disimpulkan bahwa :

1. Firewall dapat melindungi web server dari serngan SQL Injection, Cross Site Scripting (XSS), dan Command Execution.
2. Firewall dengan module dan rule modSecurity dapat diterapkan pada web server dan berjalan sesuai dengan yang diharapkan.
3. Website yang sudah diterapkan pada web server dapat dilindungi.

B. Saran

Berdasarkan pada hasil kesimpulan di atas, maka penulis memberikan saran sebagai berikut:

1. Guanakan website yang lebih interaktif lagi sehingga dapat dilakukan analisa yang lebih dalam lagi terhadap web server.
2. Untuk memperoleh hasil yang maksimal coba terapkan beberapa module security dan rule yang lebih banyak lagi untuk diterapkan terhadap website berbasis content management system (CMS).

6. REFERENSI

[1] S. Rheno Widianto and I. Abdullah Azzam, "Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server," *Elektra*, vol. 3, no. 2, pp. 19–28, 2018.

[2] I. M. Suartana, H. Endah Wahanani, and A. Noor Sandy, "Sistem Pengaman Web Server Dengan Application Firewall (WAF)," *Scan*, vol. X, no. 1, pp. 3–8, 2015.

[3] A. Hamzah, S. Juli, I. Ismail, L. Meisaroh, S. Si, and M. Si, "Implementasi Sistem Monitoring Jaringan

Menggunakan Zabbix dan Web Web Application Firewall di PT PLN (Persero) Transmisi Jawa Bagian Tengah," *e-Proceeding Appl. Sci.*, vol. 5, no. 3, pp. 2378–2384, 2019.

[4] J. Karisma Anggreana, "Simulasi keamanan pada aplikasi web dengan web aplication firewall." Universitas Komputer Indonesia, 2014.

[5] R. Yanti Jamain, Periyadi, and S. Juli Irza Ismail, "Implementasi Keamanan Aplikasi Web Dengan Web Application Firewall," *e-Proceeding Appl. Sci.*, vol. 1, no. 3, pp. 2191–2195, 2015.

[6] Batikkominfo, "MENGETAHUI TENTANG SISTEM KEAMANAN JARINGAN UNTUK PROTEKSI PERANGKAT KOMPUTER ANDA," *https://www.baktikominfo.id/*, 2018. [Online]. Available: https://www.baktikominfo.id/id/informasi/pengetahuan/mengetahui_tentang_sistem_keamanan_jaringan_untuk_proteksi_perangkat_komputer_anda-677.

[7] A. Prasetyo and R. Susanti, "Sistem Informasi Penjualan Berbasis Web Pada PT. Cahaya Sejahtera Sentosa Blitar," *J. Ilm. Teknol. Inf. Asia*, vol. 10, no. 2, pp. 1–16, 2016.