Analisis Perbandingan Performa Aplikasi Web Ticketing pada PT Aplikanusa Lintasarta dengan Implementasi ModSecurity dan Shadow Daemon

Alvi Rahmatullah Akbar
Teknik Multimedia dan Jaringan, Teknik Informatika dan Komunikasi, Politeknik Negeri Jakarta
Universitas Indonesia, Jl. Prof. DR. G.A. Siwabessy Kampus, Kukusan, Beji, Depok City, West Java 16425t,
(021) 7270036/ (021) 7270034
humas@pnj.ac.id

Abstract - In carrying out monitoring and ticketing activities, the ITS CC department of PT Aplikanusa Lintasarta uses a web application that still does not have a SQL Injection and XSS attack prevention system. Both are types of attacks that often occur on web applications. This makes ITS CC web applications vulnerable to such attacks. To prevent this can be used WAF (Web Application Firewall). In this study, WAF ModSecurity and Shadow Daemon were used. To determine which of the two is better implemented in the ITS CC web application, it will be based on the success of both preventing SQL injection and XSS attacks and the performance of the ITS CC web application in protection. The results of the analysis show that WAF ModSecurity and Shadow Daemon both managed to prevent SQL Injection attacks and cross-site scripting attacks. The QoS parameter of the web application with the implementation of ModSecurity shows a throughput value of 15.45 kb/s, a packet loss of 0.9%, and an average delay of 32.59 ms. Meanwhile, the Shadow Daemon implementation shows a throughput value of 423.95 kb/s, a packet loss of 2.2%, and an average delay of 38.5 ms. ModSecurity has QoS parameters that are more suitable for the needs of using web ticketing applications in the ITS CC department, so it can be concluded that ModSecurity is better to be implemented in the ITS CC web application.

Keywords: web application, SQL injection, XSS, WAF, QoS

Abstrak*-- Dalam melakukan aktivitas pemantauan dan ticketing, departemen ITS CC PT Aplikanusa Lintasarta menggunakan sebuah aplikasi web yang masih belum memiliki sistem pencegahan serangan SQL Injection dan XSS. Keduanya merupakan jenis serangan yang sering terjadi pada aplikasi web. Ini membuat aplikasi web ITS CC menjadi rentan terhadap serangan tersebut. Untuk mencegahnya dapat digunakan WAF (Web Application Firewall). Pada penelitian ini digunakan WAF ModSecurity dan Shadow Daemon. Untuk menentukan antara keduanya mana yang lebih baik diimplementasikan di aplikasi web ITS CC, akan didasarkan pada keberhasilan keduanya mencegah serangan SQL injection dan XSS serta performa aplikasi web ITS CC dalam proteksinya. Hasil analisis menunjukkan, WAF ModSecurity dan Shadow Daemon keduanya berhasil mencegah serangan SQL Injection dan serangan cross-site scripting. Parameter QoS aplikasi web dengan implementasi ModSecurity menunjukkan nilai throughput sebesar 15,45 kb/s, packet loss sebesar 0,9%, dan delay rata-rata sebesar 32,59 ms. Sementara dengan implementasi Shadow Daemon menunjukkan nilai throughput sebesar 423,95 kb/s, packet loss sebesar 2,2%, dan delay rata-rata sebesar 38,5 ms. ModSecurity memiliki parameter QoS yang lebih cocok dengan kebutuhan penggunaan aplikasi web ticketing di departemen ITS CC, maka dapat disimpulkan bahwa ModSecurity lebih baik untuk diimplementasikan seterusnya di aplikasi web ITS CC.

Kata kunci: aplikasi web, injeksi SQL, XSS, WAF, QoS

I. PENDAHULUAN

PT Aplikanusa Lintasarta adalah sebuah perusahaan yang bergerak di bidang penyediaan layanan komputasi awan. Dalam menjalankan bisnis penyediaan layanan komputasi awan, PT Aplikanusa Lintasarta menjamin ketersediaan sumber daya serta kinerja komputasi awan yang sesuai dengan kebutuhan serta permintaan dari pelanggan atau pengguna layanan tersebut. Di PT Aplikanusa Lintasarta, infrastruktur jaringan yang digunakan untuk penyediaan layanan tersebut adalah berupa data center. Data center berupa sebuah ruangan atau bangunan yang berisi berbagai macam perangkat

keras jaringan yang tersimpan aman dan kondisinya dikontrol sedemikian rupa untuk memastikan performa perangkat keras jaringan tersebut berjalan dengan optimal. Untuk memastikan hal tersebut, PT Aplikanusa Lintasarta memiliki suatu departemen yang memantau aktifitas perangkat keras jaringan di data center dan melakukan pelaporan apabila ada masalah yang terjadi, seluruh kegiatan ini disebut juga ticketing dan departemen yang bertanggungjawab akan kegiatan tersebut adalah departemen Information Technology Services Cloud Center (ITS CC).

Untuk efektivitas kegiatan ticketing di ITS CC, sebuah aplikasi web digunakan untuk melakukan pelaporan kegiatan dan jurnal aktivitas data center untuk shift yang dibagi dua menjadi shift malam dan shift pagi. Namun, pada aplikasi web tersebut masih belum memiliki sistem keamanan sehingga sangat rentan dengan serangan cross-site scripting (XSS) dan SQL injection yang sering terjadi (Putra, 2018). Namun, walaupun dengan sistem keamanan yang diterapkan, performa aplikasi tetap harus optimal untuk kepentingan kelancaran kegiatan tersebut.

Dengan demikian, diperlukan sebuah metode untuk mencegah serangan terhadap aplikasi web yang digunakan di ITS CC dan tetap dengan performa aplikasi web yang optimal, salah satu solusinya adalah dengan menggunakan Web Application Firewall (WAF). Secara khusus pada penelitian ini WAF yang akan digunakan adalah aplikasi ModSecurity dan Shadow Daemon, dua WAF yang digunakan karena termasuk yang cukup populer digunakan, tidak berbayar, dan sumber terbuka (Agarwal, 2018). Kedua WAF tersebut akan diuji dalam menanggulangi serangan cross-site scripting dan SQL injection dan diuji pula performa aplikasi web dengan proteksi keduanya agar dapat ditentukan mana yang lebih baik untuk diimplementasikan seterusnya di aplikasi web ITS CC. Uji performa tersebut didasarkan pada parameter QoS (Quality of Services) yaitu throughput, packet loss, dan delay (Utami, 2020).

II. METODE PENELITIAN

Pendekatan yang dilakukan pada penelitian ini adalah dengan pendekatan kuantitatif atau berdasarkan pada angka. Data berupa angka didapatkan dari Web Server Stress Tool 8 yang akan diolah menjadi parameter QoS yang akan menjadi tolak ukur bagaimana performa aplikasi web dengan implementasi WAF ModSecurity danb Shadow Daemon yang melakukan pencegahan serangan.

Jenis penelitian yang dilakukan berupa komparatif antara WAF ModSecurity dan Shadow Daemon yang mana akan dilakukan perbandingan performa keduanya dalam mencegah serangan pada aplikasi web ITS CC dan bagaimana hasil parameter QoS dari keduanya.

III. HASIL DAN PEMBAHASAN

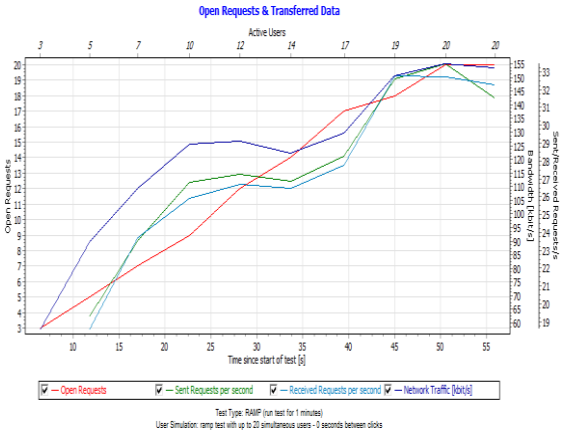
Pada penelitian ini menggunakan software yang tidak berbayar, di antaranya ModSecurity, Shadow Daemon, XAMPP, Webserver Stress Tool 8 dan VirtualBox. XAMPP menjalankan aplikasi web di Apache agar dapat diakses oleh WAF baik yang berada di Windows (ModSecurity) maupun yang berada di sistem operasi virtual (Shadow Daemon). Sementara untuk uji serangan dan performa akan dilakukan dengan SQL Map dan Webserver Stress Tool 8.

Pada hasil WebServer Stress Tool 8 akan didapatkan nilai yang akan digunakan untuk menentukan parameter QoS yaitu throughput, packet loss, dan delay. Pertimbangan ketiganya berdasarkan kebutuhan departemen ITS CC berdasarkan jumlah pengguna yang aktif dan aktivitas di aplikasi web. Karena aplikasi web ini hanya digunakan oleh karyawan departemen ITS CC terutama yang berperan dalam melakukan ticketing, maka pengguna aktif tidak banyak. Puncak aktivitas akan terjadi pada saat handover yaitu saat pergantian shift. Dengan demikian dibutuhkan sebuah sistem dengan parameter QoS yang memiliki nilai delay dan packet loss yang rendah. Dengan nilai throughput yang mempengaruhi bagaimana besarnya data yang dapat dikirim, hal ini hanya akan dibutuhkan pada saat ada pengiriman gambar yang hanya terjadi satu kali setiap pergantian shift untuk mengirimkan foto kondisi ruangan kantor, dan hal tersebut pun hanya jika diperlukan saja.

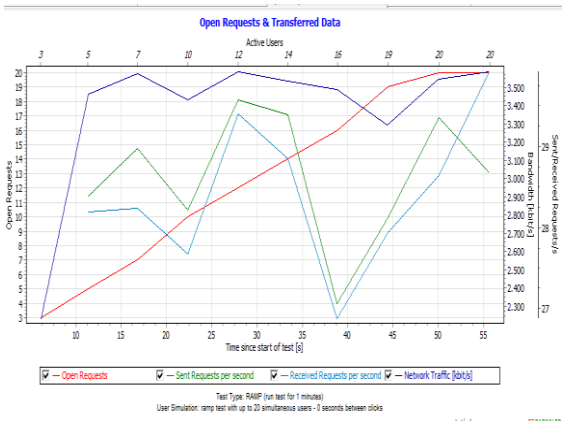
Pengujian dilakukan dengan cara melakukan serangan menggunakan SQL Map untuk SQL injection dan script XSS untuk cross-site scripting. WAF akan bertindak sebagai perantara antara request yang dibuat oleh serangan dan akan ditentukan apakah serangan merupakan request yang diizinkan atau dikategorikan sebagai berbahaya dan diblokir. Hal tersebut akan menampilkan histori aktivitas dalam log WAF yang sedang digunakan. Webserver Stress Tool 8 akan melakukan simulasi traffic dengan penggunaan aplikasi web yang semakin lama semakin ramai yang mana keluaran datanya akan didokumentasikan dan diolah menjadi parameter QoS.

Berdasarkan hasil pengujian, didapatkan hasil bahwa ModSecurity dan Shadow Daemon berhasil dalam mencegah serangan SQL injection dan cross-site scripting yang dilakukan pada aplikasi web ITS CC.

Perbandingan performa aplikasi web dalam proteksi keduanya dapat terlihat sebagai berikut:



Gambar 1. Grafik Performa request dan traffic dengan ModSecurity



Gambar 2. Grafik Performa request dan traffic dengan Shadow Daemon

Berdasarkan hasil penelitian, didapatkan tabel yang menunjukkan delay (click time) dan data yang dikirim (Bytes). Berdasarkan gambar 1 dan 2 yang diambil dari Webserver Stress Tool 8, didapatkan pula nilai paket data dikirim (sent request) dan paket data diterima (received request). Dengan nilai-nilai yang sudah didapat, maka parameter QoS dapat ditentukan dengan menggunakan persamaan sebagai berikut:

Throughput = (jumlah data yang dikirim(kb))/(waktu pengiriman data (s))

Packet loss = ((paket data dikirim-paket data diterima))/(paket data yang dikirim) x 100%

Delay rata-rata = (total delay (ms))/(total paket yang diterima)

Dengan demikian, didapatkan nilai penghitungan parameter QoS ModSecurity dan Shadow Daemon sebagai berikut:

Tabel 1. Parameter QoS aplikasi web dengan ModSecurity dan Shadow Daemon

Parameter QoS	ModSecurity	Shadow Daemon
Throughput	15,45 kb/s	423,95 kb/s
Packet Loss	0,9%	2,2%
Delay rata-rata	32,59 ms	38,5 ms

Berdasarkan tabel 1, dari parameter QoS antara aplikasi web dengan implementasi ModSecurity dan Shadow Daemon terlihat bahwa Shadow Daemon hanya memiliki kelebihan di throughput dengan nilai 423,95 kb/s apabila dibandingkan dengan ModSecurity dengan nilai 15,45 kb/s. Nilai packet loss dan delay rata-rata pada ModSecurity yang masing-masing sebesar 0,9% dan 32,59 ms lebih kecil apabila dibandingkan dengan Shadow Daemon dengan nilai packet loss dan delay masing-masing 2,2% dan 38,5 ms.

Berdasarkan dengan pertimbangan kebutuhan pada analisis kebutuhan, aplikasi web ITS CC memiliki pengguna aktif yang sedikit dan puncak aktivitas pada saat pergantian shift. Walaupun Shadow Daemon memiliki nilai throughput yang lebih tinggi, ModSecurity memiliki parameter QoS yang lebih cocok dengan kebutuhan di departemen ITS CC dengan nilai packet loss dan delay yang lebih rendah. Dengan demikian didapatkan hasil bahwa ModSecurity lebih baik diimplementasikan di departemen ITS CC dibandingkan dengan Shadow Daemon.

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis penelitian ini, maka dapat disimpulkan:

1. ModSecurity dan Shadow Daemon keduanya berhasil mencegah serangan SQL Injection dan serangan cross-site scripting.
2. Performa aplikasi web yang didasarkan pada parameter QoS dengan implementasi ModSecurity menunjukkan nilai throughput sebesar 15,45 kb/s, packet loss

sebesar 0,9%, dan delay rata-rata sebesar 32,59 ms. Sementara dengan implementasi Shadow Daemon menunjukkan nilai throughput sebesar 423,95 kb/s, packet loss sebesar 2,2%, dan delay rata-rata sebesar 38,5 ms.

3. ModSecurity memiliki parameter QoS yang lebih cocok dengan kebutuhan penggunaan aplikasi web ticketing di departemen ITS CC, maka ModSecurity lebih baik untuk diimplementasikan seterusnya di aplikasi web ITS CC.

Untuk penelitian selanjutnya disarankan menggunakan OS yang sama untuk hosting aplikasi web. Menggunakan RAMP walaupun mensimulasikan bagaimana sebuah aplikasi web diakses semakin ramai dari waktu ke waktu, ada baiknya pula apabila tes performa menggunakan mode lainnya. Menggunakan mode deteksi tanpa blokir pada semua WAF yang akan dibandingkan juga dapat dilakukan.

V. REFERENSI

[1] Abdurrahman, Soni, dan Hafid, A.2019. "Optimalisasi Sumber Daya Komputer dengan Virtualisasi Server Menggunakan Proxmox VE". Jurnal FASILKOM, 9(2), 369–376.

[2] Adhi, P.F., Purwanto, A., dan Darmandi E.A. 2018. "Optimalisasi Jaringan Menggunakan Firewall". IKRA-ITH Informatika, 2(3), 17–23.

[3] Agarwal, N., dan Hussain, S.Z. 2018. "A closer look on Intrusion Detection System for web applications". Hindawi. 1-32. dapat dilakukan

[4] Anam, J.K., Sudyana, D., Noviciatie, A., Lizarti, N., dan Agustin. 2020. "Optimalisasi Penggunaan VirtualBox Sebagai Virtual Computer Laboratory untuk Simulasi Jaringan dan Praktikum pada SMK Taruna Mandiri Pekanbaru". J-PEMAS STMIK Amik Riau, 1(2), 37-44.

[5] Arunawati, A.P. 2020. "Optimasi Apache Web Server Menggunakan Varnish Web Cache dan Reverse Proxy Nginx". Repositori UNS, 1-64.

[6] Ayeni, B.K., Sahalu, J.B., dan Adeyanju, K.R. 2018. "Detecting Cross-Site Scripting in Web Application Using Fuzzy Interference System". Hindawi, 1–10.

[7] Ayunda, Dhiatama K., Widjajarto, A., dan Budiono A. 2021. "Implementation and Analysis ModSecurity on Web-Based Application with OWASP Standards". Jurnal Teknik Informatika dan Sistem Informasi, 8(3), 1638-1650.

[8] Dwiyatno, S., Rakhmat, E., dan Gustiawan, O. 2020. "Implementasi Virtualisasi Server Berbasis Docker Container". Prosisko, 7(2), 165-175.

[9] Hariani. 2021. "Eksplorasi Web Browser dalam Pencarian Bukti Digital Menggunakan SQLite". Jurnal Instek, 6(1), 66-74.

[10] Hasugian. 2018. "Perancangan Website Sebagai Sarana Promosi dan Informasi". Journal of Informatic Pelita Nusantara (JIPN), 3(1), 82-85.

[11] Jiwandono, A. 2020. "Analisa Perbandingan Kinerja Web Server Apache, Nginx, dan Litespeed Dengan Menggunakan Metode Stress Test", Repositori UIR, 1-68.

[12] Putra, N.R.M. 2021. "Web Application Firewall untuk Meningkatkan Keamanan Informasi". JIIFOR. 5(2), 21–26.

[13] Rahmatika, Pauziah, U., dan Mursito, H. 2021. "HTML-Based Website Learning Training (Hypertext Markup Languange)". REKA ELKOMIKA: Jurnal Pengabdian kepada Masyarakat, 2(1), 19-25.

[14] Riska dan Alamsyah, H. 2021. "Penerapan Sistem Keamanan Web Menggunakan Metode Web Application Firewall". Jurnal Amplifier, 11(1), 37–42.

[15] Ristijana, D.K., Dirgantoro, B., dan Ruriawan, M.F. (2021). "Implementasi Metode Proteksi Situs Web dari Web Scraping". e-Proceeding of Engineering, 6258-6265.

[16] Utami, P.R. 2020. "Analisis Perbandingan Quality of Service Jaringan Internet Berbasis Wireless pada Layanan Internet Service Provider (ISP) Indihome dan First Media". Jurnal Ilmiah Teknologi dan Rekayasa, 25(2), 125-137. doi:10.35760/tr.2020.v25i2.2723.

[17] Wiguna, B., Prabowo W.A., dan Ananda, R. 2020. "Implementasi Web Application Firewall dalam Mencegah Serangan SQL Injection pada Website". Digital Zone: Jurnal Teknologi Informasi dan Komunikasi, 11(2), 245-256.

[18] Wirawan, R., Bachri, S., Dwi, A., Wibowo, A.A., Wardhani P.I. 2021. "Performa dan Stress Testing dalam Upaya Mengoptimalkan Webgis Open Source (Studi Kasus WebGIS Ekowisata Sungai Mudal KulonProgo)". GEOMATKA, 27(1), 19–26.

[19] Sahi, A. 2020. "Aplikasi Test Potensi Akademik Seleksi Saringan Masuk LP3I Berbasis Web Online Menggunakn Framework CodeIgniter". TEMATIK, 7(1), 120-129.

[20] Sari. 2021. "Penerapan Github sebagai Media E-Learning untuk Mengetahui Keefektifan Kolaborasi Project pada Mata Pelajaran Pemrograman Web dan Perangkat Bergerak di SMK Negeri 2 Surabaya". Jurnal IT-EDU, 6(2), 14-22.

[21] Setyowati dan Siswanti, S. 2021. Perancangan Basis Data dan Pengenalan Server Management Studio. Lembaga Penelitian dan Pengabdian Masyarakat Universitas Dian Nuswantoro Semarang.

[22] Siallagan, T.F.P, dan Wisnu D. 2020. "Rancang Bangun Sistem Pengidentifikasi Travel Bag pada Kelompok Biro Perjalanan Umroh/Haji Berbasis Web". Jurnal Teknologi

Informasi dan Komunikasi STMIK Subang, 15(1).

[23] Wardhani, R.N., Utami, M.C., dan Saputra, I.Y. 2020. “Sistem Informasi Helpdesk Ticketing pada PT Bank Mega Tbk”. Jurnal Ilmiah MATRIK, 22(2), 201-207.

[24] Yunianto, I. dan Adhiyarta, K. 2020. “Jurnal Review: Perbandingan Sistem Operasi Linux dengan Sistem Operasi Windows”. Jurnal IBM. 1-8.

[25] Yusuf, D.K., Aryadi, P., dan Masya, F. 2020. “Aplikasi Politeknik Berbasis Web (APIK)”. Jurnal Swabumi. 127-133.