Repeater : Publikasi Teknik Informatika dan Jaringan
Volume. 2 No. 4 Oktober 2024
e-ISSN : 3046-7276, dan p-ISSN : 3046-7284, Hal. 16-26
DOI: https://doi.org/10.62951/repeater.v2i4.196
Available online at: https://journal.aptii.or.id/index.php/Repeater

Implementasi dan Analisa Sistem Pencegahan Intrusi pada Aplikasi Web Menggunakan Web Application Firewall

Deski Ari Sandi [1*], Agus Tedyyana [2]
[1,2] Teknik Informatika, Keamanan Sistem Informasi, Politeknik Negeri Bengkalis, Indonesia
deskiarisandi11@gmail.com [1*], agusteddyana@polbeng.ac.id [2]

Alamat: Jl. Bathin Alam, Sungai Alam. Bengkalis Riau - 28711
Korespondensi penulis: deskiarisandi11@email.com

Abstract*. In the era of information technology advancement, web applications have become a means of seeking information. However, with technological progress, they have become increasingly vulnerable to cyber attacks such as SQL Injection and Cross-Site Scripting (XSS). This research aims to implement the Teler-waf Web Application Firewall (WAF) to protect web applications from such attacks. The research methodology includes the implementation of the Teler-waf WAF, analysis of web application security, and testing the speed of attack detection. The results show that Teler-waf is effective in preventing attacks, and its integration with Telegram bots provides real-time notifications to system administrators, enhancing security responsiveness. This research contributes to strengthening web application security and understanding the role of the Teler-waf WAF in addressing cyber threats.*

Keywords*: Web Application Firewall, Teler-waf, SQL Injection, Cross Site Scripting, Telegram*

Abstrak. Dalam era kemajuan teknologi informasi, aplikasi web menjadi sarana dalam pencarian informasi, namun semakin kemajuan teknologi, semakin juga rentan terhadap serangan siber seperti SQL Injection Cross Site Scripting (XSS). Penelitian ini bertujuan untuk mengimplementasikan Web Application Firewall (WAF) Teler-waf dalam melindungi aplikasi web dari serangan tersebut. Metode penelitian meliputi implementasi WAF Teler-waf, analisis keamanan aplikasi web, dan pengujian kecepatan deteksi serangan. Hasil penelitian menunjukkan bahwa Teler-waf efektif dalam mencegah serangan, dengan integrasi bot Telegram memberikan notifikasi real-time kepada administrator sistem, meningkatkan respons keamanan. Penelitian ini berkontribusi dalam memperkuat keamanan aplikasi web dan memahami peran WAF Teler-waf dalam menghadapi ancaman serangan siber

Kata kunci: Web Application Firewall, Teler-waf, SQL Injection, Telegram

1. LATAR BELAKANG

Di era digital saat ini, kemajuan teknologi informasi telah membawa perubahan signifikan dalam cara kita bekerja dan mengakses informasi, dengan aplikasi web menjadi alat vital dalam berbagai aktivitas online. Namun, dengan pertumbuhan pesat aplikasi web, muncul pula risiko keamanan yang serius, seperti serangan Denial of Service (DoS), SQL Injection, Cross-Site Scripting (XSS), dan malware, yang dapat mengancam integritas dan keamanan data. Berdasarkan laporan Badan Sandi Siber Negara (BSSN) pada tahun 2022, total trafik anomali serangan siber di Indonesia mencapai 976.429.996, menunjukkan besarnya ancaman terhadap aplikasi web. Untuk mengatasi masalah ini, penerapan Web Application Firewall (WAF) seperti Teler-waf menjadi solusi penting, karena dirancang khusus untuk melindungi aplikasi web dari berbagai serangan dengan menganalisis dan memblokir ancaman sebelum mencapai aplikasi. Penelitian ini bertujuan untuk mengimplementasikan sistem keamanan Web Application Firewall Teler-waf pada

Received: Juli 02, 2024; Revised: Juli 30, 2024; Accepted: Agustus 26, 2024; ; Online Available : Agustus 28 2024;

aplikasi web, menganalisis tingkat keamanan dan efektivitas deteksi serangan, serta memberikan manfaat berupa peningkatan keamanan, notifikasi real-time tentang serangan, dan informasi tentang implementasi serta peran Teler-waf dalam melindungi aplikasi web.

2. KAJIAN TEORITIS

Beberapa penelitian sebelumnya telah mengeksplorasi implementasi dan analisis sistem pencegahan intrusi menggunakan Web Application Firewall (WAF). Misalnya, Bangkit Wiguna et al. (2020) meneliti penggunaan ModSecurity WAF untuk mencegah serangan SQL Injection, menemukan bahwa meskipun WAF memperpanjang waktu muat situs web, ia efektif dalam melindungi data dari pencurian(Bangkit Wiguna et al., 2020). Alamsyah (2021) juga meneliti ModSecurity, menunjukkan bahwa WAF meningkatkan keamanan web dengan mencegah serangan umum. Randi Rizal dan Yusuf Sumaryana (2021) menggunakan ModSecurity dan OWASP Core Rules Set untuk melindungi aplikasi web kampus dari serangan seperti XSS dan SQL Injection, menunjukkan efektivitas WAF dalam mendeteksi dan memblokir ancaman(Rizal & Sumaryana, 2021). Muhammad Dody Firmansyah (2021) meneliti Modevasive sebagai solusi terhadap serangan DDoS, menemukan bahwa Modevasive efektif dalam mengurangi dampak serangan dan melindungi ketersediaan layanan web(Dody Firmansyah, 2021). Suryayusra dan Muhammad Muharromin (2023) membandingkan ModSecurity dan Shadow Daemon, menemukan bahwa keduanya efektif dalam mencegah serangan, tetapi dengan mekanisme yang berbeda(Muharromin et al., n.d.). Panca Putra Pahlawan dan Faruk Ulum (2021) membandingkan ModSecurity dan ModEvasive terhadap serangan Slow Headers, dengan hasil bahwa ModSecurity lebih efektif dalam mencegah jenis serangan tersebut(Pahlawan, 2021).

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah menggunakan metode keamanan. Metode ini melibatkan serangkaian tahapan mengidentifikasi dan menganalisis serangan dari memonitoring dan mencegah serangan pada aplikasi web.

Pada penelitian ini dilakukan dengan tahapan terstruktur, adapun tahapan penelitian dapat dilihat pada gambar 1.

Gambar 1. Tahapan Penelitian

Berdasarkan gambar 1 dapat dijelaskan tahapan penelitian sebagai berikut:

Identifikasi Masalah

Tahapan ini merupakan langkah awal dari penelitian yang akan dilakukan dimana penulis akan membuat rumusan masalah yang ditemukan pada objek penelitian dan mengidentifikasi batasan-batasan dari masalah yang diteliti untuk memberikan arahan yang lebih jelas.

Studi Literatur

Dalam tahap pengumpulan sumber literatur, Penulis melakukan riset dan mengumpulkan berbagai sumber yang berkaitan dengan Web Application Firewall dan serangan SQL Injection dan Cross Site Scripting (XSS). Tujuan pengumpulan literatur ini adalah untuk mendapatkan informasi yang penting dan mendalam tentang sistem keamanan ini dan serangan SQL Injection dan Cross Site Scripting (XSS), serta membangun landasan teoritis yang kuat untuk penelitian ini.

Menyiapkan Alat dan Bahan

Dalam tahapan selanjutnya adalah menyiapkan alat dan bahan yang dibutuhkan seperti perangkat dan tools yang dibutuhkan untuk melakukan penelitian diantara lainnya yaitu:

Tabel 1. Kebutuhan Hardware

Laptop Lenovo G460
Processor Core i3
Ram 6 GB
SSD 128 GB dan HDD 500 GB
Wi-fi dan Data Seluler

Tabel 2. Kebutuhan Software

Sistem Operasi Windows 10 64Bit
Oracle VM VirtualBox
Sistem Operasi Ubuntu-Server
Sistem Operasi Kali Linux
SQL Injection dan Cross Site Scripting

Implementasi dan Konfigurasi Sistem

Dalam tahap ini, tahapan awal adalah merancang struktur lingkungan penelitian, termasuk pembuatan topologi jaringan, dan diikuti oleh perancangan lingkungan. Selanjutnya, implementasi penelitian dilaksanakan.

Perancangan topologi jaringan adalah fondasi dari pembangunan lingkungan penelitian. Topologi ini terdiri dari tiga elemen, yaitu penyerang (attacker), perangkat Web Aplication Firewall Teler-waf dan bot telegram sebagai penerima notifikasi.

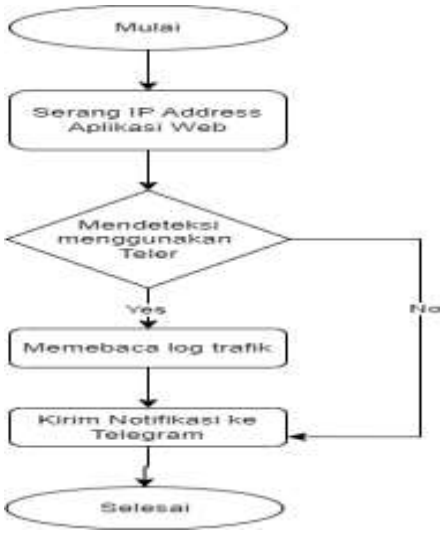
Tahapan berikutnya melibatkan proses instalasi yang mencakup:

a. Instalasi Web Aplication Firewall Teler-waf
b. Konfigurasi Teler-waf
c. Integrasikan ke Bot Telegram

Pengujian dan Analisa

Dalam tahap pengujian sistem keamanan aplikasi web, penulis menjalani serangkaian tindakan yang terstruktur. Awalnya, penulis melakukan perencanaan pengujian dengan menetapkan tujuan, cakupan, skenario, dan pengujian yang akan diterapkan. Ini merupakan tahap kunci dalam memastikan pengujian dilakukan dengan jelas dan efisien.

Berikut serangan yang akan dilakukan oleh penulis dalam penelitian pada gambar 2:



Gambar 2. Pengujian dan Alur Sistem Teler-waf

4. HASIL DAN PEMBAHASAN

Berdasarkan tahapan penelitian, maka dapat diperoleh hasil dari pengujian pada penelitian. Pengujian dilakukan dalam dua tahap, tahap pertama dilakukan saat aplikasi web belum diimplementasikan dengan web application firewall Teler-waf, dan tahap kedua dilakukan setelah web application firewall Teler-waf diimplementasikan. Pengujian serangan dilakukan dengan menggunakan dua teknik serangan yang berbeda, yaitu SQLMap dan Cross Site Scripting.

Tahap Pengujian Tanpa WAF

Serangan pertama yang dilakukan adalah melakukan SQL Injection. Dalam melakukan serangan SQL Injection menggunakan SQLMap, berikut perintah yang digunakan dalam melakukan serangan seperti gambar 1 :

Gambar 3. Serangan SQL Injection

Dari hasil serangan SQL Injection menggunakan SQLMap menampilkan bahwa serangan tersebut berhasil dilakukan. Dapat dilihat padagambar diatas menunjukan bahwa database dari aplikasi web dapat ditemukan.

Serangan kedua yang dilakukan adalah melakukan serangan Cross Site Scripting. Adapun script yang digunakan dalam melakukan serangan Cross Site Scripting terhadap aplikasi web seperti pada gambar 4 :

Gambar 4. Serangan Cross Site Scripting

Setelah melakukan serangan Cross Site Scripting dengan menyisipkan script pada aplikasi web, hasil yang didapatkan seperti gambar :

Gambar 5. Hasil Serangan Cross Site Scripting

Pada gambar diatas menunjukkan bahwa, hasil dari melakukan serangan Cross Site Scripting terhadap aplikasi web berhasil dilakukan.

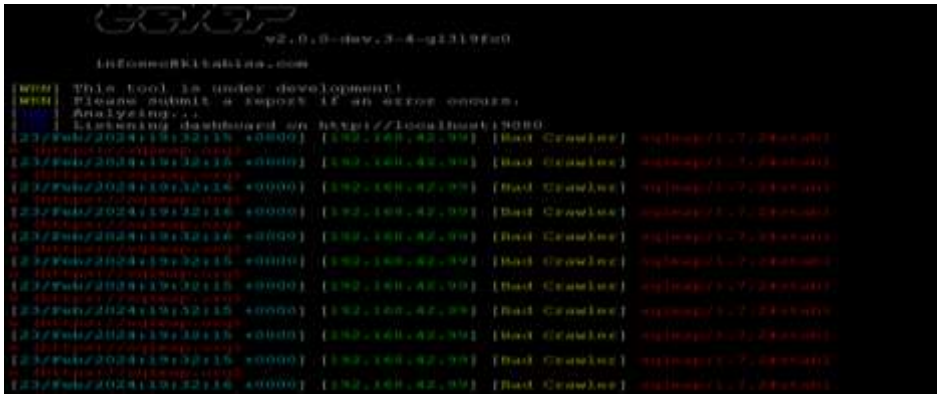
Tahap Pengujian Menggunakan WAF

Serangan SQLMap yang dilakukan pada aplikasi web yang sudah diimplementasikan web application firewall dengan menggunakan script dan payload yang sama pada pengujian sebelumnya. Berikut serangan SQLMap ke aplikasi web seperti gambar 6 :

Gambar 6. Serangan SQL Injection

Gambar 6 Serangan SQL Injection

Jalankan perintah teler-waf untuk mendeteksi SQL Injection menggunakan SQLMap. Perintah yang digunakan untuk menjalankan teler-waf dan hasil yang didapatkan ketika serangan SQLMap terdeteksi. Sepeti gambar 7 :



Gambar 7. Hasil Deteksi

Dari hasil teler-waf mendeteksi serangan SQL Injection, serangan tersebut terdeteksi dalam kategori serangan Common Web Attack dan Bad Crawler. Common Web Attack adalah jenis teknik serangan yang digunakan untuk mengekploitasi atau memanfaatkan kerentanan pada aplikasi web. dan Bad Crawler teknik serangan yang beroperasi dengan niat untuk merusak**.**

Setelah itu serangan SQLMap terblokir secara langsung. Hasil pemblokiran seperti pada gambar 8 :

Gambar 8. Hasil Terblokir

Setelah serangan berhasil terdeteksi dan terblokir, teler-waf akan mengirimkan notifikasi berupa terjadinya serangan ke bot telegram. Seperti pada gambar dibawah 9 :

Gambar 9. Notifikasi Serangan SQL Injection

Serangan selanjutnya yang dilakukan dengan melakukan serangan Cross Site Scripting (XSS). Berikut serangan Cross Site Scripting (XSS) ke aplikasi web aplikasi web seperti pada gambar dibawah 10 :

Gambar 10. Serangan Cross Site Scripting

Gambar 11. Hasil Deteksi

Dari hasil teler-waf mendeteksi serangan XSS, serangan tersebut terdeteksi dalam kategori serangan Common Web Attack.

Hasil pemblokiran serangan Cross Site Scripting seperti pada gambar 12 :

Gambar 12. Hasil Terblokir

Dari gambar diatas menunjukan bahwa serangan tersebut berhasil diblokir. Setelah serangan berhasil terdeteksi dan terblokir.

Gambar 13. Notifikasi Serangan Cross Site Scripting

Pada gambar 13 adalah hasil notifikasi yang dikirimkan dari teler-waf, bahwa terjadi serangan Cross Site Scripting.

Dari hasil proses pengujian serangan dengan menggunakan 2 teknik yang serangan yang sama yaitu SQL Injection menggunakan SQLMap & Cross Site Scripting pada aplikasi web. Adapun untuk hasil pengujian 2 serangan tersebut sebelum dan sesudah diimplementasikan Web Application Firewall. Dapat dilihat pada tabel 1 berikut:

Tabel 3. Hasil Pengujian Serangan

No	Teknik Serangan	Tahap Pertama	Tahap Kedua
1	SQL Injection	Berhasil	Gagal
2	Cross Site Scripting	Berhasil	Gagal

Dari hasil melakukan serangan SQL Injection menggunakan SQLMap dan Cross Site Scripting terhadap aplikasi web yang belum dan sesudah diimplementasikan Web Application Firewall. Mendapatkan hasil seberapa cepat teler-waf dalam mendeteksi serangan yang dilakukan, hasil ditunjukan pada tabel 2 :

Tabel 4. Hasil Serangan SQL Injection

No	Kategori Serangan	Waktu Menyerang	Waktu Terdeteksi	Waktu Terblokir
1	Common Web Attack	19:32:15	19:32:16	19:32:16
2	Common Web Attack	19:32:15	19:32:16	19:32:16
3	Bad Crawler	19:32:15	19:32:16	19:32:16
4	Common Web Attack	19:32:15	19:32:16	19:32:16
5	Bad Crawler	19:32:15	19:32:17	19:32:17
6	Bad Crawler	19:32:15	19:32:17	19:32:17
7	Bad Crawler	19:32:16	19:32:17	19:32:17
8	Common Web Attack	19:32:16	19:32:17	19:32:17

Tabel 5. Hasil Serangan Cross Site Scripting

No	Kategori Serangan	Waktu Menyerang	Waktu Terdeteksi	Waktu Terblokir
1	Common Web Attack	20:00:10	20:00:10	20:00:10
2	Common Web Attack	20:00:10	20:00:10	20:00:10
3	Common Web Attack	20:00:11	20:00:11	20:00:11
4	Common Web Attack	20:00:11	20:00:11	20:00:11
5	Common Web Attack	20:00:11	20:00:11	20:00:11
6	Common Web Attack	20:00:12	20:00:12	20:00:12
7	Common Web Attack	20:00:12	20:00:12	20:00:12
8	Common Web Attack	20:00:12	20:00:12	20:00:12

Pada tabel diatas adalah hasil uji coba serangan, hasil menunjukan bahwa teler-waf cukup cepat dalam mendeteksi serangan SQL Injection dan Cross Site Scripting. Dapat dilihat pada tabel diatas jarak antara waktu serangan dilakukan dan waktu teler-waf mendeteksi serangan hanya jeda 1 detik setelah serangan dilakukan. Dan yang didapatkan

pada tabel hasil diatas dilakukan secara manual dalam menghitung waktu serangan, terdeteksi, dan terblokirnya serangan.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian, penulis menyimpulkan bahwa Teler-WAF memiliki kemampuan mendeteksi dan mencegah serangan SQL Injection menggunakan SQLMap serta Cross Site Scripting (XSS). Penggunaan bot Telegram sebagai penerima notifikasi serangan memudahkan dalam meningkatkan kesadaran keamanan, karena notifikasi dapat diterima secara real-time. Untuk memperkuat keamanan aplikasi web, penerapan Teler-WAF memerlukan konfigurasi yang tepat, pemantauan aktivitas melalui laporan, pembaruan berkala pada aturan untuk mendeteksi pola serangan baru, serta pengembangan fitur-fitur yang ada. Koneksi jaringan yang baik juga diperlukan untuk mengoptimalkan deteksi serangan.

DAFTAR REFERENSI

Bangkit Wiguna, Adi Prabowo, W., & 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. https://doi.org/10.31849/digitalzone.v11i2.4867

Dody Firmansyah, M. (2021). Analisa Keamanan Web Server terhadap Serangan Distributed Denial of Service menggunakan Modevasive. *Telcomatics*, *6*(1), 2541–5867. https://doi.org/10.37253/telcomatics.v6i1.4990

Muharromin, M., Informatika, J. T., & Darma, U. B. (n.d.). *Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache*. 393–402.

Pahlawan, P. P. (2021). Perbandingan Penerapan Metode Pengamanan Mod Security Dan Mod Evasive Pada Web Server Terhadap Serangan Slow Headers. *Journal of Engineering, Computer Science and …*, *1*(1), 93–100. http://jurnal.teknokrat.ac.id/index.php/JECSIT/article/view/12

Rizal, R., & Sumaryana, Y. (2021). Peningkatan Keamanan Aplikasi Web Menggunakan Web Application Firewall (WAF) Pada Sistem Informasi Manajemen Kampus Terintegrasi. *Jurnal ICT : Information Communication & Technology*, *20*(2), 323–330. https://doi.org/10.36054/jict-ikmi.v20i2.416

H. Hardianto and T. Sutabri, “Analisis cyber crime handling pada aplikasi web dengan WAF ModSecurity,” PETIR J. Pengkaj. dan Penerapan Tek. Inform., vol. 16, no. 1, pp. 91–99, 2023, [Online]. Available: https://doi.org/10.33322/petir.v16i1.1910.

H. Alamsyah, “Penerapan Sistem Keamanan WEB Menggunakan Metode WEB Aplication Firewall,” vol. 11, no. 1, 2021.

A. Tedyyana and O. Ghazali, “INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION journal homepage : www.joiv.org/index.php/joiv INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION Teler Real-time HTTP Intrusion Detection at Website with Nginx Web Server,” vol. 5, no. September, pp. 327–332, 2019, [Online]. Available: www.joiv.org/index.php/joiv

A. Aryapranata, “Web Application Firewall pada Situs Web Institut Bisnis Nusantara www.ibn.ac.id,” vol. 4, no. 1, pp. 55–59, 2020.

S. R. Widianto and I. A. Azzam, “Analisis Upaya Peretasan Web Application Firewall Dan Notifikasi Serangan Menggunakan Bot Telegram,” Elektra, vol. 3, no. 2, pp. 19–28, 2018.