jifor-1

by wiharja listrik

Submission date: 19-Apr-2022 11:33AM (UTC-0400)
Submission ID: 1810598380
File name: Template_JIFOR_-_NAUFALARIZQA_RAMADHA_MEISA_PUTRA_1.docx (325.09K)
Word count: 1515
Character count: 9568

Web Application Firewall untuk Meningkatkan Keamanan Informasi

Naufalarizqa Ramadha Meisa Putra

Program Studi Teknik Informatika, Universitas Krisnadwipayana
Jl. Kampus Unkris, Jatiwaringin, Pondok Gede, Jakarta Timur
Email: naufalarizqa@unkris.ac.id

Abstract

Due to the increasing spread of the Internet and information systems, thus causing web applications, the risks and associated threats in this field have also increased. In recent years, several different websites such as government sites and non-government sites have been targeted by penetration attacks and illegal hacking activity. The attacks carried out often result in significant financial and credibility losses along with harming organizational and even national interests. Given the magnitude and complexity of cyberattacks and due to the diversity of web application structures, the need to have comprehensive and effective solutions to prevent or mitigate the negative effects of such attacks is very important. One of the latest tools to prevent infiltration and attacks on websites is a web application firewall (WAF), which allows security policies to be enforced between the user and the web application. In this journal, five simulations of cyberattacks have been carried out to determine how effective the use of WAF is in preventing and minimizing the risk of cyberattacks. In conclusion, WAF can block all five simulated attacks instantly.

***Keywords**: Internet, cyberattack, WAF.*

1. Pendahuluan

Dengan pengembangan metode untuk menembus aplikasi web, serangan SQL injection dan cross-site scripting sangat sering terjadi. Menurut sifat serangan ini, serangan semacam ini tidak mudah diidentifikasi dan dicegah melalui firewall dan IPS. Dari sudut pandang teknis, alasan utama yang mendasari adalah masalah terkait dengan struktur web atau protokol HTTP. Protokol HTTP tidak dirancang untuk struktur aplikasi web yang kompleks saat ini. Misalnya, protokol HTTP stateless, yang artinya setiap permintaan ditangani secara independen. sementara untuk stateful diperlukan untuk menggunakan operasi terpisah.

Dalam organisasi besar, banyak aplikasi web memerlukan kebijakan keamanan yang berbeda untuk melindunginya dari berbagai serangan siber. Terutama dengan memprioritaskannya dan mengklasifikasikannya berdasarkan sensitivitas dan pentingnya aplikasi web, dan kemudian dalam hal kepentingan.

Berbagai metode dan alat digunakan untuk menerapkan kebijakan keamanan untuk mengamankan aplikasi web. Semua cara penetrasi ke aplikasi berbasis web dan akses tidak sah ke program dapat dicegah dengan mematuhi dan menerapkan standar keamanan. Dalam banyak kasus setelah

membuat program operasional dan menjalankan berbagai pengujian, seperti

pengujian penetrasi dan pengujian keamanan, satu atau beberapa masalah keamanan dalam aplikasi web terdeteksi.

Web Application Firewall (WAF) dapat melakukan inspeksi paket yang mendalam (*deep packet inspection*) di lalu lintas jaringan yang terjadi antara klien dan sisi server. Dengan menganalisis data yang ditransfer antara klien dan server, WAF dapat mengidentifikasi segala kemungkinan serangan dari *deep packet inspection*. WAF secara otomatis mempelajari aplikasi web, mempelajari perilaku pengguna (*user behavior*), memperbarui pertahanan web dengan intelijen berbasis riset tentang ancaman terbaru saat ini, serta WAF juga memiliki performa tinggi dan transparan.

2. LANDASAN TEORI

Berikut ini adalah dari sejumlah landasan teori yang akan digunakan dalam penulisan ini :

2.1.Web Application Firewall

Secara umum, WAF dapat didefinisikan sebagai berikut: satu titik kebijakan keamanan ditempatkan antara pengguna akhir dan aplikasi web. Tugas utama WAF adalah melindungi masalah keamanan dalam aplikasi web terhadap serangan dan metode intrusi melalui pemrograman dengan cara untuk mencegah penyalahgunaan dan akses tidak sah ke sistem.

2.2.Standar Keamanan WAF

Standar paling penting di WAF meliputi berikut:

1) *PCI DSS (Payment Card Industry Data Security Standard)*

Standar ini adalah salah satu standar informasi sistem yang paling penting tentang organisasi dan perusahaan yang berurusan dengan transaksi keuangan pelanggan Online.

2) *OWASP Top 10 (Open Web Application Security Project)*

Praktik terbaik yang terkenal dan paling penting yang disediakan oleh OWASP di bidang WAF dikenal sebagai OWASP top 10 dan praktik terbaik WAF didukung oleh hampir semua produsen WAF. OWASP top 10 berisi 10 pendekatan orisinal untuk penetrasi aplikasi web dan cara-cara untuk mencegah serangan semacam itu.

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

Gambar 1. OWASP TOP 10 - 2017

2.3.Karakteristik WAF

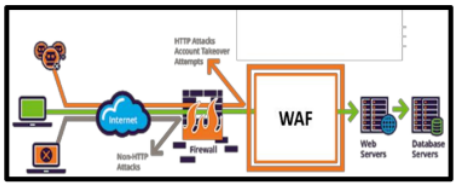
Karakteristik yang dimiliki WAF meliputi berikut:

a. Mendukung standar ancaman utama yang diketahui dan cara menangani ancaman seperti OWASP Top 10 dan PCI DSS.

b. Memeriksa input dan output aplikasi web berdasarkan definisi kebijakan / aturan keamanan dan implementasi operasi yang sesuai seperti Block, Allow, Alert, dan log registrasi, sesuai dengan praktik yang diterima.
c. Menghentikan dan mengungkapkan informasi penting (Pencegahan kebocoran data) - kemampuan untuk memeriksa output dan respons aplikasi web melalui definisi kebijakan dan aturan keamanan dan implementasi operasi yang sesuai seperti *Block, Allow, Alert, Mask*.
d. Implementasi kebijakan keamanan melalui model Positif, Negatif.
    1) Dalam model Positif atau *whitelist* (daftar putih) dengan menetapkan operasi yang dapat diterima, perilaku yang diizinkan, memasukkan rentang data yang dapat diterima yang ditentukan dan hanya operasi ini yang diizinkan dan operasi lainnya yang didiagnosis ilegal, itu akan mencegah tindakan dari melakukan.
    2) Dalam model negatif atau *blacklist* (daftar hitam), daftar semua tindakan tidak sah ditentukan dan semua operasi sisanya di izinkan.
e. Memeriksa konten halaman web seperti HTML, HTML dinamis, CSS, serta protokol transfer halaman web seperti HTTP, HTTPS, TLS.
f. Memeriksa pesan Layanan web, termasuk XML dan SOAP.
g. Mengecek protokol apa pun atau apa yang digunakan konstruk data untuk mentransfer data ke aplikasi web atau menerima data.
h. Mencegah atau mendeteksi cookies yang berbahaya dan bersifat merusak.
i. Memiliki kemampuan untuk *Fail Open* / gagal terbuka (Misalnya, dalam kasus WAF dinonaktifkan karena masalah perangkat keras, semua lalu lintas jaringan yang masuk dan keluar diizinkan untuk ditransfer tanpa melewati WAF) atau mendukung *Fail Closed* / gagal tutup (jika gagal WAF terjadi karena untuk masalah perangkat keras, lalu lintas input dan output, tidak diizinkan untuk ditransfer dari WAF).
j. Dukungan untuk sertifikat klien SSL dan otentikasi klien proxy.
k. Kemampuan untuk menerima pembaruan baru baik otomatis maupun manual.

2. METODE PENELITIAN

Di studi ini, WAF diletakkan sesuai topologi di gambar 2 yaitu diletakan sebelum *web server*.



Gambar 2. Topologi Pengujian

Tahapan yang akan dilakukan untuk melakukan pengujian keamanan WAF yaitu Simulasi serangan peretasan dilakukan pada suatu *web public*. Terdapat 5 tipe pengujian dalam studi ini.

TABEL 1. SIMULASI PENGUJIAN SERANGAN

Tipe Serangan	Tingkatan	Attack Target
SQL Injection	*High*	*Website Server Server Farm*
Cross-site Scripting	*High*	*Website Server Server Farm*
Scrapping Attack	*High*	*Website Server Server Farm*
Automatic Vulnerability Scanning	*High*	*Website Server Server Farm*
Suspicious File Extension Access	*High*	*Website Server Server Farm*

3. HASIL DAN PEMBAHASAN

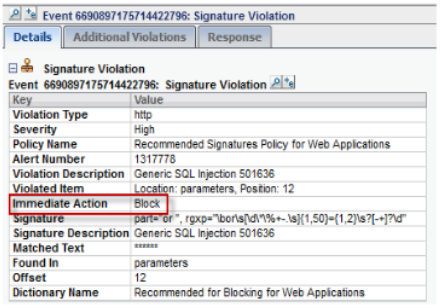
Dari serangkaian simulasi pengujian serangan yang dilakukan pada penelitian ini, dapat disimpulkan bahwa respon dari WAF seperti pada tabel 2 berikut.

TABEL 2. RESPON WAF TERHADAP SIMULASI PENGUJIAN SERANGAN

No	Tipe Serangan	Tingkatan (*Severity*)	Attack Target	Respon WAF	Waktu Mitigasi
1	*SQL Injection*	*High*	*Website Server Server Farm*	*Block*	*Instant*
2	*Cross-site Scripting*	*High*	*Website Server Server Farm*	*Block*	*Instant*
3	*Scrapping Attack*	*High*	*Website Server Server Farm*	*Block*	*Instant*
4	*Automatic Vulnerability Scanning*	*High*	*Website Server Server Farm*	*Block*	*Instant*
5	*Suspicious File Extension Access*	*High*	*Website Server Server Farm*	*Block*	*Instant*

3.1. Hasil Pengujian *SQL Injection*

Setelah dilakukan simulasi serangan dengan *SQL Injection* pada website yang dituju, maka perangkat WAF akan menghentikan serangan/block secara *instant* saat terdeteksi serangan *SQL Injection*.

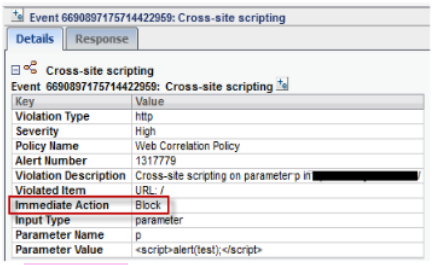


Gambar 3. Perangkat WAF berhasil mengeblok serangan *SQL Injection*

3.2. Hasil Pengujian *Cross-site Scripting (XSS)*

Setelah dilakukan simulasi serangan dengan *Cross-site Scripting* (XSS) pada website yang dituju, maka perangkat WAF akan menghentikan serangan/block secara *instant* saat

terdeteksi serangan *Cross-site Scripting* (XSS).


Event 669089717571442295 9: Cross-site scripting

Details | Response

Cross-site scripting

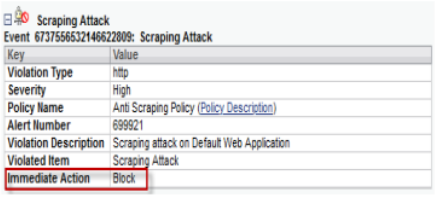
Event 669089717571442295 9: Cross-site scripting

Key	Value
Violation Type	http
Severity	High
Policy Name	Web Correlation Policy
Alert Number	1317779
Violation Description	Cross-site scripting on parameter p in [redacted]
Violated Item	URL: /
Immediate Action	Block
Input Type	parameter
Parameter Name	p
Parameter Value	<script>alert(test);</script>

Gambar 4. Perangkat WAF berhasil mengeblok serangan *Cross-site Scripting (XSS)*

3.3. Hasil Pengujian *Scrapping Attack*

Setelah dilakukan simulasi serangan dengan Scrapping pada website yang dituju, maka perangkat WAF akan menghentikan serangan/block secara *instant* saat terdeteksi serangan *Scrapping Attack* berdasarkan *Anti Scrapping Policy*.


Scraping Attack

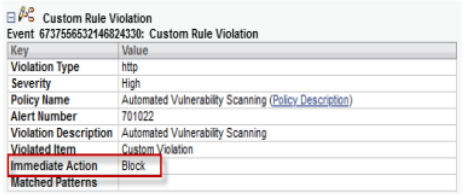
Event 6737556532146622809: Scraping Attack

Key	Value
Violation Type	http
Severity	High
Policy Name	Anti Scraping Policy (Policy Description)
Alert Number	699921
Violation Description	Scraping attack on Default Web Application
Violated Item	Scraping Attack
Immediate Action	Block

Gambar 5. Perangkat WAF berhasil mengeblok serangan *Scrapping Attack*

3.4. Hasil Pengujian *Automatic Vulnerability Scanning*

Setelah dilakukan simulasi serangan dengan *Vulnerability Scanning* pada website yang dituju, maka perangkat WAF akan menghentikan serangan/block secara *instant* saat terdeteksi serangan *Vulnerability Scanning*.


Custom Rule Violation

Event 6737556532146824330: Custom Rule Violation

Key	Value
Violation Type	http
Severity	High
Policy Name	Automated Vulnerability Scanning (Policy Description)
Alert Number	701022
Violation Description	Automated Vulnerability Scanning
Violated Item	Custom Violation
Immediate Action	Block
Matched Patterns	

Gambar 6. Perangkat WAF berhasil mengeblok serangan *Automatic Vulnerability Scanning*

3.5. Hasil Pengujian *Suspicious File Extension Access*

Setelah dilakukan simulasi serangan dengan *Suspicious File Extension Access* pada website yang dituju, maka perangkat WAF akan menghentikan serangan/block secara *instant* saat terdeteksi serangan *Suspicious File Extension Access*.


Event 6737556532150671486: Custom Rule Violation

Key	Value
Violation Type	http
Severity	High
Policy Name	Suspicious File Extension Access (Policy Description)
Alert Number	703030
Violation Description	Suspicious File Extension Access
Violated Item	Custom Violation
Immediate Action	Block
Matched Patterns	

Gambar 7. Perangkat WAF berhasil mengeblok serangan *Suspicious File Extension Access*

4. PENUTUP

4.1. Kesimpulan

Dari hasil penelitian ini dapat ditarik beberapa kesimpulan bahwa Penggunaan Perangkat WAF dapat melindungi aplikasi Web dari serangan-serangan siber. Hal ini terbukti dari dilakukannnya simulasi serangan yang dilakukan yaitu simulasi serangan *SQL Injection*, *Cross-site Scripting (XSS)*, *Scrapping Attack*, *Automatic Vulnerabilty Scanning*, dan *Suspicious File Extension Access*. Kelima serangan tersebut berhasil dihentikan (*block*) oleh perangkat WAF dengan waktu proses *instant*. Dengan demikian, penggunann WAF menjadi sangat efektif dalam

penanganan serangan siber dan meningkatkan keamanan informasi.

Daftar Pustaka

1. Jim McMillan, 2009, *Intrusion Detection FAQ: What is the difference between an IPS and a Web Application Firewall?*
2. Payment Card Industry Security Standards Council. (2020, Agustus). Payment Card Industry (PCI) Data Security Standard.
3. Imperva Inc. (2018). Imperva SecureSphere Appliances Datasheet.
4. Imperva Inc. (2019). Imperva WAF Gateway.
5. OWASP, Open Web Application Security Project, and Global AppSec. (2020) Web application firewall.
6. Singh Aniruddha, Vaish Abhishek & Keserwani, Kumar Pankaj, "*Information Security : Component and Techniques*" International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 4, January, 2014.
7. Kumar Sumit, Dalal Sumit & Dixit Vivex, "*The OSI Model: Overview On The Seven Layers of Computer Networks*" International Journal of Computer Science and Information Technology Research, vol. 2, issue 3, pp. 461-466, September 2014.
8. Miller, Lawrence C., "Next-Generation Firewalls For Dummies®.," Indianapolis: Wiley Publishing, Inc.,201
9. Himanshu Sharma. Kali Linux - an Ethical Hacker's Cookbook. Packt Publishing. 2017.
10. Georgia Weidman. Penetration Testing: A Hands-on Introduction to Hacking. No Starch Press. 2014.

jifor-1

ORIGINALITY REPORT

18%	15%	8%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Benfano Soewito, Charlie Erwin Andhika. "Next Generation Firewall for Improving Security in Company and IoT Network", 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), 2019 Publication	5%
2	dspace.uii.ac.id Internet Source	2%
3	ojs.unik-kediri.ac.id Internet Source	1%
4	docplayer.net Internet Source	1%
5	Submitted to Western Governors University Student Paper	1%
6	jurnal.teknikunkris.ac.id Internet Source	1%
7	msrit-bucket.s3.us-west-2.amazonaws.com Internet Source	1%
8	jurnal.iaii.or.id Internet Source	

		1 %
9	repository.universitasbumigora.ac.id Internet Source	1 %
10	text-id.123dok.com Internet Source	1 %
11	news.publishersglobal.com Internet Source	1 %
12	owasp.org Internet Source	1 %
13	pei.e-journal.id Internet Source	1 %
14	blog.naver.com Internet Source	<1 %
15	repository.uncp.ac.id Internet Source	<1 %
16	widuri.raharja.info Internet Source	<1 %
17	Wiga Ariani. "Efektivitas Bahan Ajar Berbasis Penemuan Terbimbing Untuk Meningkatkan Kemampuan Komunikasi Matematis Peserta Didik Kelas VIII SMP", Journal on Education, 2020 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		