Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 8, No. 2, Juni 2023 (341-348) **10.32493/informatika.v8i2.33691**

Implementasi Web Application Firewall untuk Melindungi Aplikasi Web dari Serangan Malware

Muhamad Fahrizal Rizqi[1], Rohmat Tulloh[2], Nazel Djibran[3]

[1,2]Program Studi Teknik Telekomunikasi, Telkom University, Jalan Telekomunikasi, bojongsoang, Bandung, 40257
e-mail: [1]fahrrzz@student.telkomuniversity.ac.id, [2]rohmatth@telkomuniversity.ac.id

[3]IT Security Implementation, PT Datacomm Diangraha, Jalan Kapten Tendean, Mampang Prapatan, Jakarta Selatan, DKI Jakarta, 12790
e-mail: [3]nazel.djibran@datacomm.co.id

Submitted Date: June 16th, 2023 Reviewed Date: June 22nd, 2023
Revised Date: June 27th, 2023 Accepted Date: June 30th, 2023

Abstract

At this time Internet services have become a necessity no longer to provide information services, but have become important so there are many cases of websites being hacked by attackers, for that network security is very important to avoid theft of important data Security in a web application is a important aspect to have. Securing a web application can be done by installing a firewall that is connected directly to the server network. Security for a web application usually uses a web application firewall installed on a web server. To overcome a security problem in Web Applications and minimize losses caused by SQL Injection and XSS attacks, we need a way to overcome these attacks. Several security measures have been used, such as the use of fortiweb to set the traffic destination for a web application. In this study, we will use a Web Application Firewall (WAF) device. Because it can protect Web applications from existing malware attacks and zero day malware. This final project will implement a Web Application Firewall (WAF). By way of device configuration and will use DVWA for malware testing. The technology that will be used to monitor malware logs will use VMware. From the results of testing a web application firewall, it is hoped that it can implement and prevent various malware attacks that attack web applications and can monitor the logs of an attacking malware.

Keywords: Internet; Web Application firewall; Malware; VMware; Traffic

Abstrak

Pada saat ini Layanan Internet sudah menjadi suatu kebutuhan bukan lagi untuk menyediakan layanan informasi, melainkan sudah menjadi hal penting maka banyak terjadi beberapa kasus website diretas oleh attacker, untuk itu keamanan jaringan sudah sangat penting untuk menghidari pencurian data penting Keamanan pada suatu aplikasi web merupakan suatu aspek penting yang harus dimiliki. Mengamankan suatu aplikasi web dapat dilakukan dengan pemasangan firewall yang terhubung langsung dengan jaringan server. Keamanan pada suatu web aplikasi biasanya menggunakan web application firewall yang dipasangkan pada suatu web server. Untuk mengatasi suatu permasalahan keamanan pada Aplikasi Web dan meminimalisir kerugian yang ditimbulkan akibat dari serangan *SQL Injection* dan *XSS*, maka diperlukan suatu cara untuk mengatasi serangan tersebut. Beberapa cara keamanan sudah digunakan, seperti penggunaan fortiweb untuk mengatur traffic destination pada suatu aplikasi web. Pada penelitian ini akan menggunakan perangkat Web Application Firewall (WAF). Karena bisa melindu ngi Web aplikasi dari serangan malware.yang sudah ada maupun malware *zero day*. Pada proyek akhir ini akan mengimplementasikan Web Application Firewall (WAF). Dengan cara konfigurasi perangkat dan akan menggunakan DVWA untuk pengujian malware. Teknologi yang akan digunakan untuk

memonitoring log malware akan menggunakan VMware. Dari hasil pengujian web application firewall diharapkan dapat mengimplementasikan dan mencegah berbagai serangan malware yang menyerang web aplikasi dan dapat memonitoring log suatu malware yang menyerang.

Kata Kunci: Internet; Web Application firewall; Malware; VMware; Traffic

1 Pendahuluan

Pada saat ini Layanan Internet sudah menjadi suatu kebutuhan bukan lagi untuk menyediakan layanan informasi, melainkan sudah menjadi hal penting maka banyak terjadi beberapa kasus website diretas oleh attacker, untuk itu keamanan jaringan sudah sangat penting untuk menghidari pencurian data penting (Perdana, 2022).

Aspek keamanan dalam konteks aplikasi web memiliki pengaruh signifikansi. Dalam artian untuk memitigasi potensi ancaman, penerapan firewall yang terintegrasi secara langsung dengan infrastruktur server menjadi solusi yang alternatif. Dalam aplikasi web, perlindungan keamanan dapat menggunakan Web Application Firewall (WAF) yang terpasang pada lapisan server (Riska & Alamsyah, 2021).

Firewall yang diadopsi dalam lingkup aplikasi web berperan sebagai barikade proaktif untuk mencegah penetrasi oleh pihak yang tidak berwenang. Web Application Firewall berperan dalam melakukan konfigurasi serta pengembangan aplikasi web, sehingga potensi celah keamanan dapat ditekan seoptimal mungkin. Firewall juga dapat menyaring data yang masuk maupun keluar sehingga dapat menghentikan suatu ancaman pada server (Muharromin, 2023).

Bahkan keamanan suatu yang berbasis web memiliki kriminal lebih tinggi sehingga jaringan keamanan tidak bisa menjamin.Karena bukti kejahatan seorang peretas jaringan sulit ditemukan dan dilacak keberadaan nya (Munawar et al., 2020).

Untuk mengatasi suatu permasalahan fasilitas keamanan pada Aplikasi Web dan meminimalisir kerugian yang ditimbulkan akibat dari serangan *SQL Injection* dan *XSS*, maka diperlukan firewall. Firewall yang dimaksud adalah mekanisme keamanan jaringan yang digunakan untuk mengamankan baik bersifat hardware maupun software (Sahren, 2021).

Web Application Firewall memiliki suatu keunggulan nya sendiri dibandingkan firewall tradisional biasa karena menawarkan suatu *visibilitas* yang lebih besar ke dalam aplikasi web sensitif yang dikomunikasikan dengan menggunakan lapisan aplikasi HTTP. Dan dapat mencegah serangan di lapisan aplikasi atau layer 7 (Aryapranata, 2020).

Selain itu menurut sebuah laporan dari Imperva padatahun 2018, kerentanan serangan pada web yang paling tinggi didominasi oleh serangan *SQL injection* yaitu sebanyak 19% atau sebanyak 3.294 kasus di seluruh dunia, hal ini menjadikan serangan SQL injection mengalami peningkatan daripada tahun sebelumnya yang hanya tercatat sebanyak 896 kasus (Wiguna, 2020)

SQL injection dan *cross-site scripting (XSS)* adalah bentuk serangan siber yang mengarah pada eksploitasi kerentanan dalam struktur database aplikasi web. Dua model serangan ini memiliki potensi untuk memungkinkan penyerang dengan niat jahat untuk meretas server basis data aplikasi web, menciptakan dampak yang merugikan seperti kebocoran data, pencurian informasi sensitif, serta ketidaksesuaian integritas data. Biasanya, administrator menggunakan database sekunder untuk menyimpan data atau informasi dari database utama. Ketika ada serangan, administrator akan memulihkan database dengan mengembalikannya menggunakan backup. Tetapi jenis rencana ini tidak dapat mencegah hilangnya data atau pencurian informasi. Salah satu contoh pencurian informasi adalah ketika penyerang mendapatkan nama pengguna dan kata sandi dari database dan menggunakannya untuk masuk ke situs web sebagai administrator. Ini akan memberi penyerang hak istimewa administrator untuk mengendalikan aplikasi web (Robinson, 2018).

Web server berperan sebagai elemen penting dalam konteks pengelolaan jaringan yang menitikberatkan pada aspek keamanan. Dalam struktur ini, web server berfungsi menggabungkan data yang berasal dari berbagai klien dalam suatu rangkaian jaringan induk.

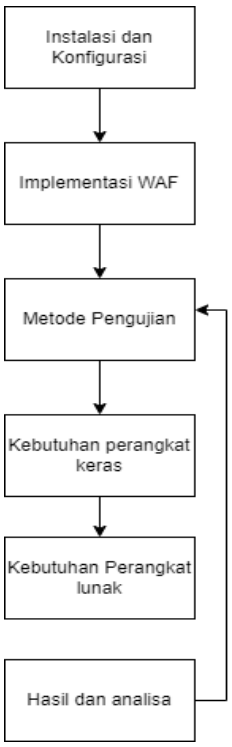
Proses ini memungkinkan klien untuk mengirim permintaan (request) guna memperoleh informasi yang diakses melalui konektivitas web server. Penting untuk dicatat bahwa penggunaan sistem perantara dalam lingkungan ini memungkinkan akuisisi informasi, termasuk data yang bersifat pribadi dan sangat rahasia. Pengaturan ini tidak hanya memastikan akses terhadap data yang terlindungi, tetapi juga mengamankan infrastruktur dari potensi serangan malware pada tahap awal (Firmansyah, 2021).

Bedasarkan kasus tersebut maka perlu meningkatkan kualitas pengamanan pada aplikasi web dengan metode yang diterapkan yaitu menggunakan web application firewall (dapat berupa perangkat keras maupun lunak) perangkat yang diujikan adalah FORTIWEB. Berbeda dengan beberapa penelitian yang sudah ada sebelumnya penelitian kali ini menggunakan perangkat keras untuk implementasi web application firewall.

2 Metode Penelitian

2.1 Perancangan Kerja Sistem

Implemetasi *web application firewall* sebagai sistem pertahan web aplikasi.



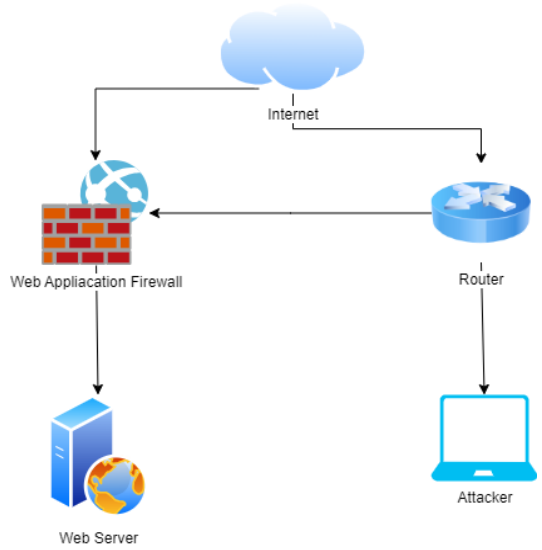
Gambar 1. Perancangan Kerja Sistem

Pada gambar 1 merupakan flowchart perancangan kerja sistem yang digunakan dalam penelitian kali ini menggunakan DVWA sebagai web server dan My SQL sebagai database-nya.

1. Instalasi Apache
   Apache ini digunakan untuk menjalankan web server DVWA dalam penelitian ini Apache akan diinstalasi di Ubuntu server. Untuk menginstal Apache dapat dilakukan dengan cara mengetikan perintahan "apt-get-install apache2 di Ubuntu server.
2. Instalasi MySQL
   MySQL ini adalah sebuah database untuk web server pada penelitian. MySQL akan diinstalasi di Ubuntu server.
   Untuk menginstall MySQL dapat dilakukan dengan cara mengetikan perintah "apt-get-install-y mysql-server.
3. Instalasi DVWA
   DVWA ini digunakan untuk menjadi web server yang akan digunakan untuk simulasi penyerangan. DVWA akan diinstalasi di ubuntu server. Untuk menginstall DVWA dapat dilakukan dengan cara mengetikan perintah sebagai berikut:
   a) Sudo apt-get install git
   b) Sudo git clone berikan link download DVWA nya
   c) Ketikan /var/www/html
   d) Sudo mv DVWA dvwa
4. Konfigurasi DVWA
   a) Cd /var/ww/html
   b) Chmod –R 777 dvwa/
   c) Cd dvwa/config
   d) Sudo cp config.inc.php.dist config.inc.php
   e) Sudo nano config.inc.php
   f) Lalu muncul ip basic dari DVWA kiata bisa ubah sesuai dengan segment jaringan yang kita gunakan
   g) Lalu save file yang sudah kita buat di direktori

ISSN: 2541-1004
e-ISSN: 2622-4615
10.32493/informatika.v8i2.33691

2.2 Implementasi Web Application Firewall



Gambar 2. Implementasi Web Application Firewall

Pada gambar 2 merupakan topologi untuk pengimplementasian web application firewall di mana ada laptop 1 yang berfungsi untuk menjadi *attacker* yang terhubung dengan router.laptop 2 berfungsi sebagai web server yang telah penguji install os ubuntu server, DVWA .Dan perangkat web application firewall peneliti menggunakan perangkat fortiweb.

Web application firewall adalah sebuah sistem pengamanan untuk melindungi website dari attacker. WAF merupakan firewall yang mengamankan layer 7 yang dirancang untuk memantau, mendeteksi dan menyaring.

DVWA adalah sebuah web server yang memang sudah dirancang memiliki banyak celah keamanan untuk dieksplorasi.

2.3 Metode Pengujian

Pengujian yang dilakukan dalam penyerangan kali ini dilakukan dengan beberapa metode yaitu dengan memberikan serangan dan tidak memberikan serangan tanpa dilindungi web application firewall metode serangan dengan tidak memberikan serangan terhadap web application firewall untuk melihat lalu lintas jaringan berjalan normal atau tidak.Ada beberapa jenis malware yang digunakan seperti *SQL Injection*, *XSS* dan *DoS*.

2.4 Spesifikasi Kebutuhan Perangkat Keras

Pada tahapan ini perangkat hardware yang dibutuhkan seperti laptop, perangkat web application firewall di mana spesifikasi hardware yang ditentukan sesuai dengan permintaan user.

Table 1. Spesifikasi Perangkat Keras

Fortiweb	Laptop
250 Throughput	Intel® Core™ i3-3220 Processor 3M Cache, 3.30 GHz
Form Factor 1U	RAM 8 GB
SSD 480 GB	Hardisk 512 GB

2.5 Kebutuhan Perangkat lunak

Peneliti menggunakan perangkat lunak untuk membantu peneliti melakukan pengujian web application firewall. Kebutuhan yang digunakan oleh peneliti bedasarkan kenyamanan.Perangkat lunak yang akan digunakan peneliti adalah sebagai berikut:

Table 2. Perangkat Lunak

Perangkat Lunak	Version
Linux Ubuntu	22.04.03
Apache	2.4
MySQL	8.0
DVWA	1.0.7
VMware ESXi	8.0
Grafana	9.0.0

3 Hasil dan pembahasan

Pengujian ini dilakukan dengan menggunakan dua cara yaitu dengan menyalakan web application firewall dan mematikan web application firewall dengan menggunakan malware seperi *SQL Injection*, *XSS* dan *DoS* yang menyerang ke dalam server.

3.1 Pengujian SQL Injection

12	2023/07/06 21:06:19	policy_dvwa	10.20.10.2	20.30.30.2		Signature Detection	Cross Site Scripting	30.30.2.5	/DVWA/vulnerabi
13	2023/07/06 21:02:02	policy_dvwa	10.20.10.2	20.30.30.2		Signature Detection	SQL Injection	30.30.2.5	/DVWA/vulnerabi
14	2023/07/06 21:00:41	policy_dvwa	10.20.10.2	20.30.30.2		Signature Detection	SQL Injection	30.30.2.5	/DVWA/vulnerabi

Gambar 3. Log Attack SQL Injection

Pada gambar pengujian *SQL Injection* Berikut peneliti akan menguji beberapa serangan *SQL Injection* yang telah diinjeksi ke dalam web server dan akan muncul respon code seperti berikut:

Table 3. Script SQL Injection

Script *SQL Injection*	Respon Code
%' or 0=0 union select null, user(kaliserver) #	403
=fkm=<script>alert(3331)</script>	403
“<script>alert(33)</script>	403

Hasil yang akan didapat dari serangan tersebut membuat akses ke dalam web menjadi 403 *forbidden*. Dan aja juga perbedaan *traffic* yang ada di web server ketika menggunakan web application dan tidak sebagai berikut:

Gambar 4. Traffic Web Server Saat Menggunakan Perangkat

Berikut adalah gambar traffic yang ada di web server dan berjalan normal dibwah 50 b/s saat perangkat web application firewall dinyalakan.

Gambar 5. Traffic Web Server Saat Tidak Menggunakan Perangkat

Berikut adalah gambar *traffic* yang ada di web server dan tidak berjalan normal dikarenakan perangkat web application firewall dimatikan buat traffic sangat tinggi karna berada di atas 50 b/s.

3.2 Pengujian XSS (Cross Site Scripting)

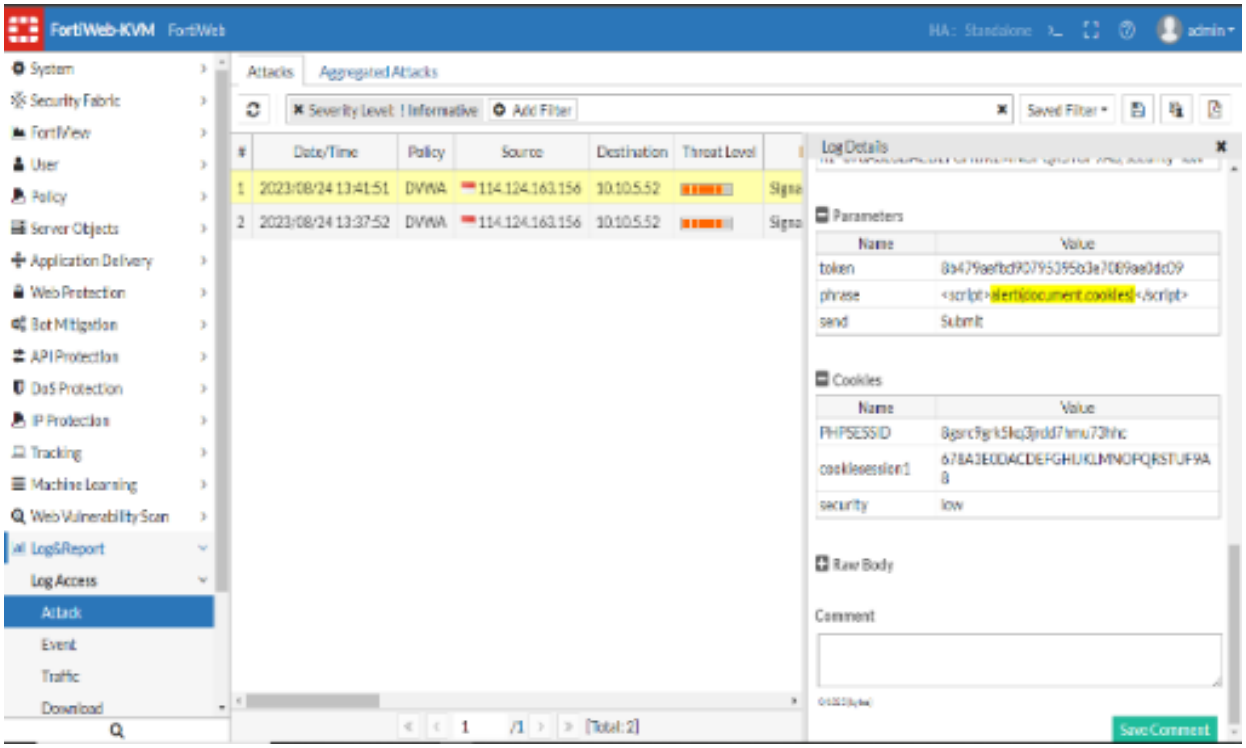
Pada gambar 6, pengujian *XSS*, peneliti akan menguji beberapa script serangan *XSS* yang diinjeksikan ke dalam web server dan akan mucul respon code seperti pada tabel 4.

Table 4. Script XSS

Script *XSS(Cross Site Scripting)*	Respon Code
<img src=x onerror=alert(“tester”)>	403
<script>alert(document.cookies)</script	403
p=</TITLE><SCRIPT>alert("XSS ");</SCRIPT>	403

Hasil yang akan didapat dari serangan tersebut membuat akses ke dalam web menjadi 403 *forbidden* dan membuat *traffic* web server itu sendiri terganggu.

Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 8, No. 2, Juni 2023 (341-348) **10.32493/informatika.v8i2.33691**



Gambar 6. Log Attack XSS

Gambar 7. Web DVWA

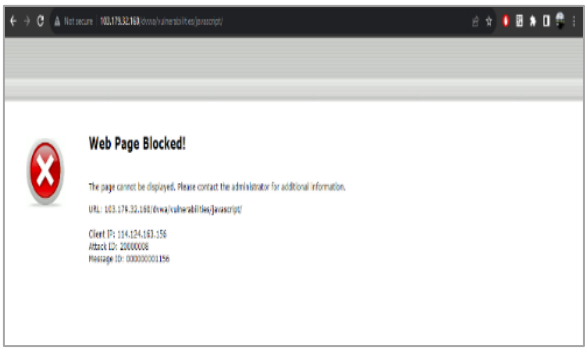
Berikut adalah gambar ketika web server tidak dilindungi perangkat WAF. Ketika script diinjeksikan tidak terjadi apa apa ketika dicek traffic server tidak stabil seperti gambar berikut:

Gambar 8. Traffic Web server Saat Tidak Menggunakan Perangkat

Pada gambar tersebut *traffic* tidak stabil dikarenakan diinjeksikan script *XSS* dan trafficnya akan terus naik. Berbeda apabila web server dilindungi oleh perangkat WAF *traffic* akan stabil dan tidak ada kenaikan yang melonjak seperti gambar berikut:

Gambar 9. Traffic Web Server Saat Menggunakan Perangkat

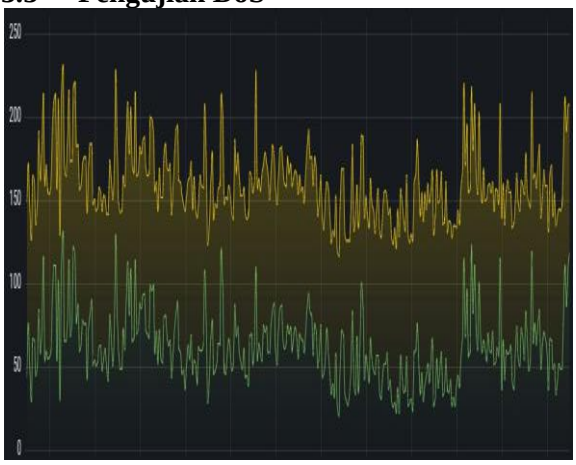
Pada gambar tersebut terlihat *traffic* stabil dan mulai turun ketika web server mulai terlindungi oleh WAF dan akan langsung terkena block script yang diinjeksikan ke dalam web seperti gambar berikut:



Gambar 10. Web Tidak Dapat Diakses

Berikut gambar setelah diaktifkan kembali perangkat WAF script yang kita injek akan di-block oleh perangkat WAF dan akan langsung masuk log ke dalam perangkat WAF yang kita implementasikan.

3.3 Pengujian DoS



Gambar 11. Traffic Serangan DoS

Berikut gambar *traffic*. *Traffic* yang berwarna hijau menandakan traffic yang belum terkena serangan *DoS* sedangkan yang berwarna kuning menunjukkan server yang terkena *DoS* terlihat perbedaan traffic diantara server yang terkena *DoS* dan tidak terkena *DoS*.

4 Kesimpulan

Bedasarkan penelitian yang sudah dilakukan dapat disimpulkan bahwa web application firewall mampu melindungi web server dari serangan malware yang menyerang web aplikasi seperti *SQL Injection, XSS (Cross Site Scripting)* bahkan malware *seperti Dos (Denial Of Service)* dapat bisa teratasi oleh web application firewall yang dimiliki oleh Fortiweb.

Berdasarkan penelitian yang sudah dilakukan mengunakan apache dan DVWA sebagai web server peneliti juga menggunakan fortiweb sebagai web aplikasi firewall menunjukkan hasil yang efektif ditunjukkan dengan pengujian penyerangan menggunakan *SQL Injection, XSS (Cross Site Scripting)* bahkan malware *seperti Dos (Denial Of Service*.berhasil dideteksi dan tidak ada satu malware yang gagal di-block oleh web application firewall. Web server tetap terjaga dari serangan malware yang menyerang. Bedasarkan penelitian ini mampu memonitoring traffic server saat diserang malware maupun tidak terserang oleh malware.

References

Aryapranata, A. (2020). Web Application Firewall pada Situs Web Institut Bisnis Nusantara www.ibn.ac.id. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, *4*(1), 55–59. https://doi.org/10.55886/infokom.v4i1.321

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. (2023). *Analisis Performance Web Application Firewall ModSecuritydan Shadow Daemon Dalam Keamanan Web Server Apache*. *393*, 393–402.

Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, *02*, 14–20.

Perdana Putranto, D., Hananto, B., Ilmu Komputer, F., Pembangunan Nasional Veteran Jakarta, U., Fatmawati Raya, J. R., & Labu, P. (2022). Analisis Keamanan Website Leads UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack. *JURNAL INFORMATIK*, *18*.

Riska, R., & Alamsyah, H. (2021). Penerapan Sistem Keamanan Web Menggunakan Metode Web Aplication Firewall. *Jurnal Amplifier : Jurnal Ilmiah Bidang Teknik Elektro Dan Komputer*, *11*(1), 37–42. https://doi.org/10.33369/jamplifier.v11i1.16683

Robinson, Akbar, M., & Ridha, M. A. F. (2018). SQL injection and cross site scripting prevention using OWASP web application firewall. *International Journal on Informatics Visualization*, *2*(4), 286–292. https://doi.org/10.30630/joiv.2.4.107

Sahren, S. (2021). Implementasi Teknologi Firewall Sebagai Keamanan Server Dari Syn Flood Attack. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *7*(2), 159–164. https://doi.org/10.33330/jurteksi.v7i2.933