Methotika : Jurnal Ilmiah Teknik Informatika
ISSN :2776 - 5792
Vol. 4, No. 2, Oktober 2024, pp. 53 - 62
https://ejurnal.methodist.ac.id/index.php/methotika

ANALISIS DAN IMPLEMENTASI KEAMANAN WEB SERVER (STUDI KASUS FIKOM UMI)

[1]Lamria Novita Sibarani, [2]Naikson Fandier Saragih, [3]Fati G.N Larosa
[123] Fakultas Ilmu Komputer, Universitas Methodist Indonesia

Info Artikel

History Artikel:
Received, Agus 9, 2024
Revised, Sep 20, 2024
Accepted, Sep 11, 2024

Keywords:
Keamanan,
Web Server,
DDoS,
SQL Injection

ABSTRAK

Masalah keamanan server web merupakan faktor yang sangat penting untuk dipertimbangkan dan dikelola untuk mencegah kerugian akibat berbagai serangan eksternal. Serangan CSRF sekali klik ditemukan di server web Departemen Ilmu Komputer UMI. Semua kerentanan ini telah diatasi (ditambal),Dari gambaran serangan yang terjadi, terlihat adanya ancaman serius terhadap keamanan web server VPS Fikom UMI. Oleh karena itu, perlu adanya upaya untuk terus berupaya melawan berbagai jenis serangan yang biasa terjadi pada server dan website, yakni Serangan DDoS dan injeksi SQL. Jika kerentanan disebabkan oleh serangan DDoS atau injeksi SQL, keamanan server web ditingkatkan oleh firewall aplikasi web. Berdasarkan analisis pengujian serangan DDoS dan SQL injection, terdeteksi adanya kerentanan pada web server Fikom UMI atas serangan DDoS, namun framework CodeIgniter yang digunakan pada web server Fikom UMI telah dikompilasi, sehingga terjadi serangan SQL injection. tidak ada kerentanan yang terdeteksi. Berdasarkan Objek Data PHP (PDO). Implementasi keamanan WAF *(Web Application Firewall)* menggunakan Mod Security berhasil mengalahkan serangan DDoS dalam 10 pengujian dengan rata-rata kesehatan CPU VPS Fikom UMI sebesar 1,45%. Jadi sebelum *WAF (Web Application Firewall)* Mod Security ada, server web Fikom UMI jauh lebih aman.

Penulis Koresponden :
Naikson Fandier Saragih,
Fakultas Ilmu Komputer,
Universitas Methodist Indonesia,
Jl. Hang Tuah no.8, Medan-Sumatera Utara.
Email: Saragihnaikson@gmail.com

1. PENDAHULUAN

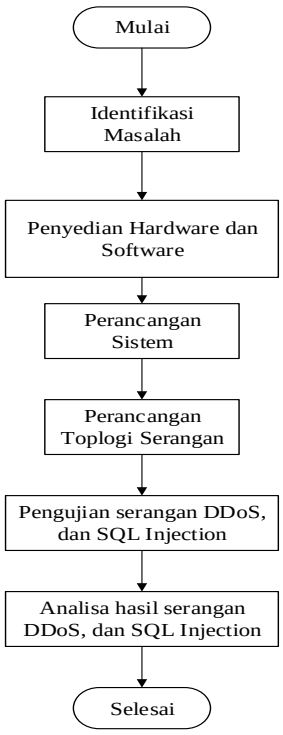
Seiring dengan adanya perkembangan teknologi informasi, masih ada aneka macam sistem keterangan berbasis web yg dipakai buat mempermudah pada pengolahan data juga transaksi, sistem yg berada dalam server memungkinkan client bisa mengakses sistem melalui web. Untuk itu server perlu diamankan berdasarkan akses pihak yg nir bertanggung jawab. Server web adalah komputer yang terdiri dari perangkat keras dan perangkat lunak. [1] Website Fakultas Ilmu Komputer UMI berada pada VPS. Penggunaan VPS dalam membentuk web server tentu menciptakan web server

Fakultas Ilmu Komputer lebih aman. Pada kenyataanya masih poly web server yg terletak dalam VPS kurang memperhatikan baku keamanan yg menyebabkan server acak berkali-kali mengalami permasalah seperti server acak berkali-kali down [2]. Sedangkan data dalam web server yg sangat krusial tentu perlu pada jaga & keterangan tadi perlu dilindungi lantaran poly yg sanggup dilakukan sang hacker buat menerima keterangan suatu perusahaan. Masalah keamanan sebuah web server adalah faktor yg sangat krusial diperhatikan & dikelola supaya nir mengakibatkan kerugian berdasarkan aneka macam agresi pihak luar. Mekanisme dan proses kolektif yang melindungi informasi dan layanan sensitif dan berharga dari pengungkapan, kompromi, atau penghancuran oleh aktivitas tidak sah, orang yang tidak dipercaya, atau kejadian tak terduga. [3] Untuk seluruh kerentanan tadi sudah ditutup (patch). WAF dapat dipandang sebagai proksi terbalik. WAF berbentuk alat, plugin server, atau filter yang dapat disesuaikan dengan aplikasi Anda. Pekerjaan penyesuaian bisa sangat ekstensif dan harus dipertahankan seiring perubahan yang dilakukan pada aplikasi [4].

Tujuan penelitian ini buat melihat celah celah keamanan web server menggunakan analisa agresi DDoS & SQL Injection. Jika masih terdapat celah dari serangan DdoS maupun juga SQL Injection, maka akan ditambahkan keamanan web server menggunakan *Web Application Firewall(WAF). Web Application Firewall(WAF*) adalah sebuah aplikasi pelaksanaan yg bertujuan untuk mengamankan dan mencegah sebuah web berdasarkan upaya penyerangan berdasarkan peretas buat menerima data dan keterangan maaupun pendayagunaan pada jumlah yg akbar yg bisa menghipnotis kestabilan sebuah web sampai mengakibatkan web nir bisa diakses(down)[5].

2. METODE PENELITIAN

Desain penelitian merupakan karangka kerja yang menjelaskan tahap ke tahap bagaimana peneliti ini akan melakukan penelitian nya. Desain penelitian juga berisi prosedur-prosedur untuk peneliti menyelesaikan sebuah permasalahan dalam saat penelitian. Rencana penelitian ini menerapkan analisis keamanan server web Fikom UMI. Kerangka penelitian ini dapat dijelaskan seperti terlihat pada diagram di bawah ini.

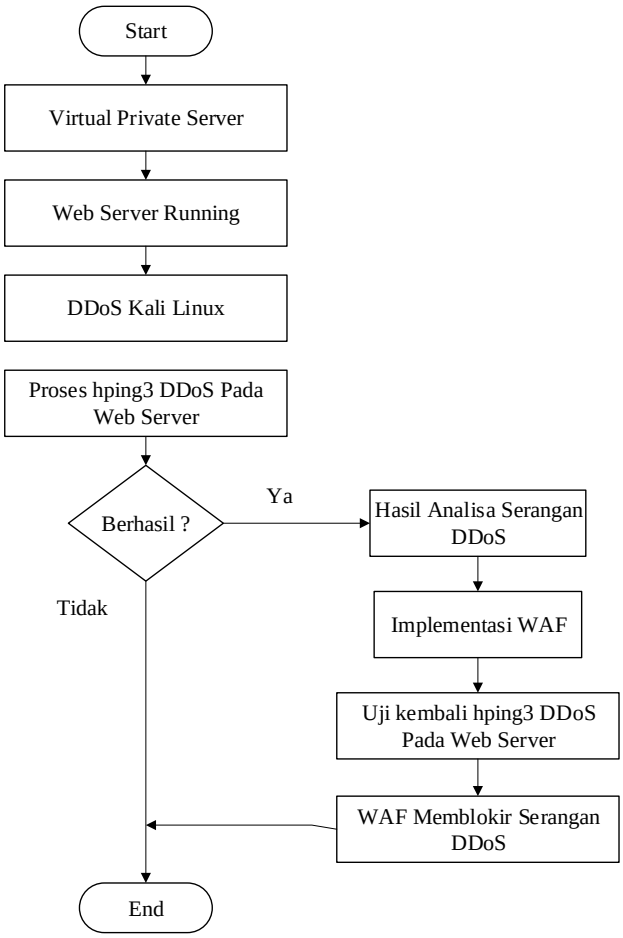


Gambar 1. Tahapan Penelitian

2.1 Perancangan Sistem

Perancangan sistem dalam penelitian ini menandakan cara kerja sistem analisis keamanan web server Fikom UMI. Perancangan sistem ini terdiri menurut perancangan skenario agresi DDoS & SQL Ijection dalam web server.

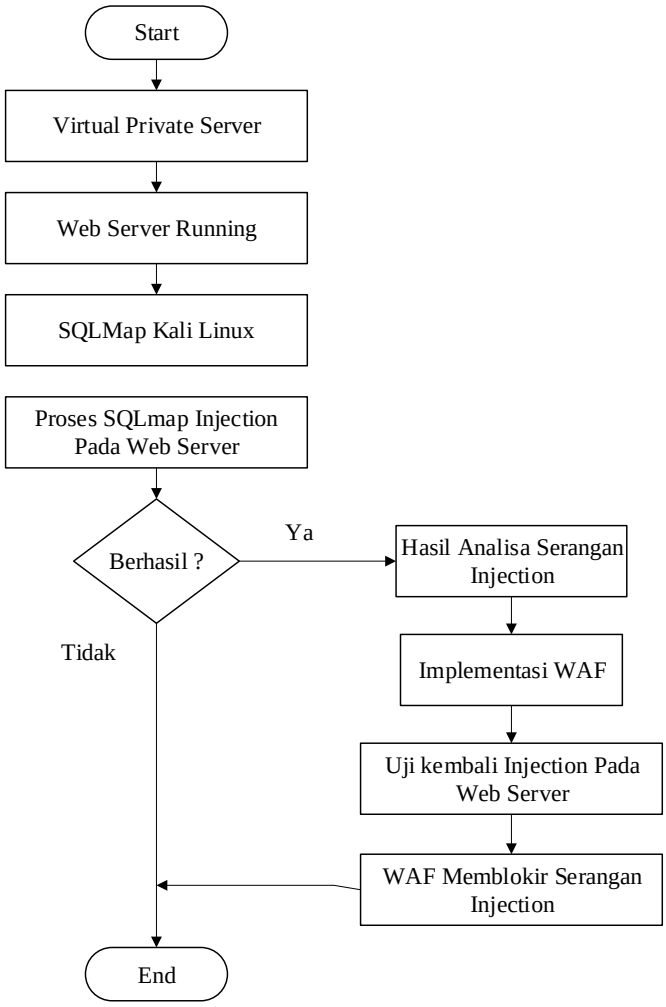
1. Skenario Serangan DDoS Berikut merupakan skenario agresi DDoS buat analisis keamanan web serber Fikom UMI misalnya dalam Gambar 2.



Gambar 2. Skenario Serangan DdoS

Berdasarkan dalam gambar 2. DDoS dipakai buat menyerangan web server menggunakan tujuan melumpuhkan web server Fikom UMI. DDoS yg dipakai dalam kali linux merupakan hping3. Jika agresi DDoS berhasil, maka dilanjutkan menggunakan implemnetasi WAF menggunakan mod security ditujukan buat memblokir data agresi DDoS.

2. Skenario Serangan SQL Ijection Berikut merupakan skenario agresi SQL Ijection buat analisis keamanan web serber Fikom UMI misalnya dalam Gambar 3.

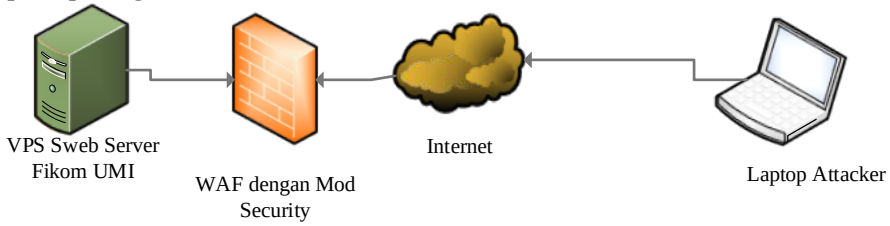


Gambar 3. Skenario Serangan *SQL Ijection*

Berdasarkan dalam gambar 3. SQL Ijection dipakai buat menyerangan web server menggunakan tujuan membuka akses database menurut web Fikom UMI. SQL Ijection menyerangan menggunakan menginjeksi website yg mempunyai celah login. Jika masih ada celah keamanan web server, maka penelitian ini mengimplentasikan WAF menggunakan mod security ditujukan buat memblokir data agresi SQL Ijection [6].

Topologi Jaringan Pada Penelitian

Adapun rancangan topologi jaringan serangan akan diterapkan untuk penelitian ini, dimana terdapat seperti pada gambar 4.



Gambar 4. Rancangan Topologi Jaringan Pengujian

Desain topologi jaringan serangan akan diterapkan pada penelitian ini seperti yang ditunjukkan pada gambar 4. Pada diagram di atas, topologi jaringan terlihat pada saat pengujian yang diteliti dalam

proses serangan DDoS dan SQL injection [7]. Detail penomoran alamat IP dapat dilihat pada tabel berikut.
Tabel 1 dapat dijelaskan sebagai berikut.

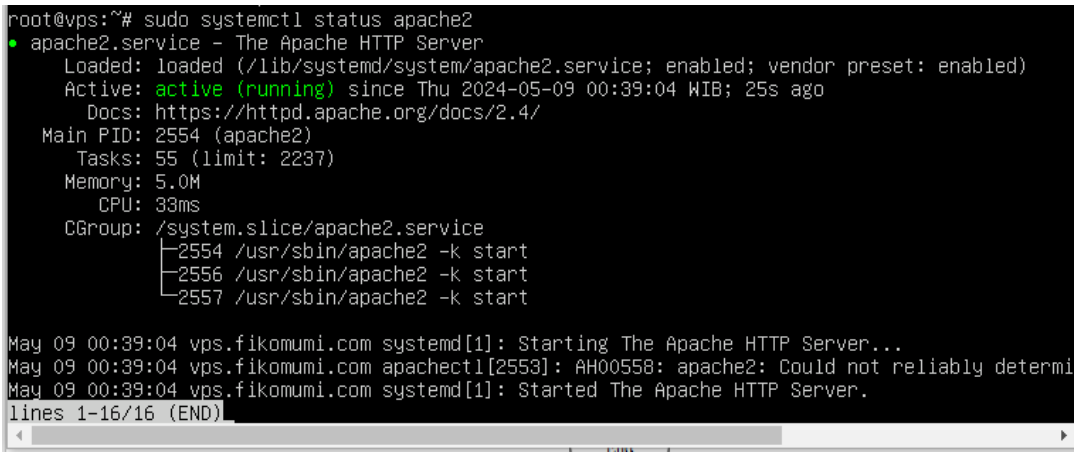
Tabel 1 Penomoran Alamat IP

No	*Hardware/software Network*	*Ket*	Alamat IP / IP *Address*
1	Internet	-	Adress 192.168.3.1
2	*Virtual Private Server* dengan Ubuntu Server	*Web Server*	203.194.114.149
3	*Client* / *Attacker*	*Kali Linux*	*Address* 192.168.3.3 *Gateway* 192.168.3.1

3. HASIL DAN PEMBAHASAN

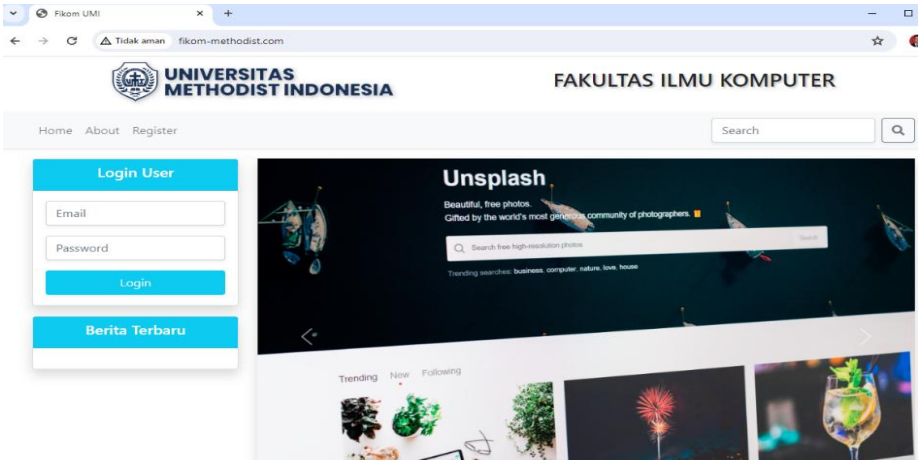
1. Pengamatan Web Server Fikom UMI

Mengamati Web Server Fikom UMI Web Server UMI pada VPS merupakan server yang menyimpan seluruh konten website Fikom UMI dan berkomunikasi dengan komputer klien melalui HTTP.[8] padagamabr yang terlihat dibawah ini merupakan informasi mengenai web server Fikom UMI di VPS.



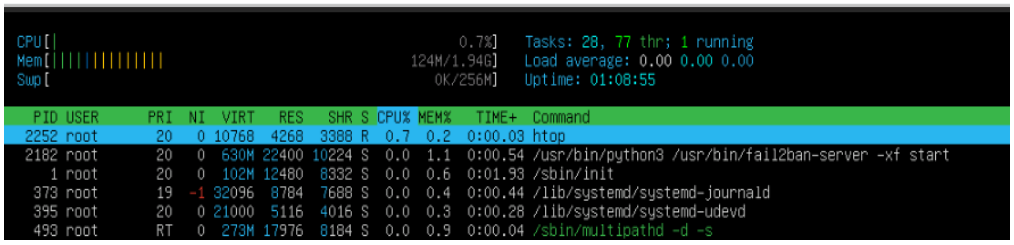
Gambar 5. Informasi Web Server Fikom UMI

Informasi Web Server Fikom UMI Berdasarkan Gambar 5. Web Server Fikom UMI pada VPS sedang aktif dengan nama vps.fikomumi.com. Web server menyimpan informasi pada website Fikom UMI



Gambar 6. *Website* Fikom UMI Didalam VPS

Keamanan server web situs web ini diuji menggunakan serangan DDoS dan injeksi SQL. Selanjutnya kita mengamati keadaan web server VPS Fikom UMI. Berikut tampilan status CPU VPS Fikom UMI ditunjukkan pada Gambar 7.



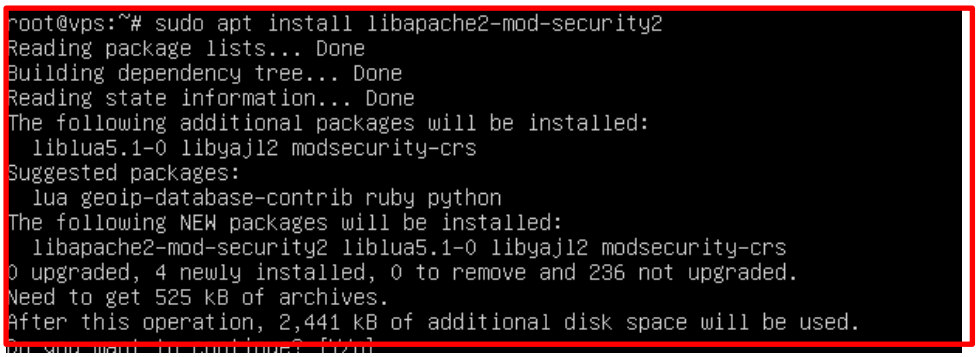
Gambar 7. Kondisi Awal CPU Pada VPS

2. Keamanan WAF Mod Security

Setelah dilakukan analisa, maka didapatkan celah keamanan dari serangan DDoS. Oleh sebab itu maka penelitian ini akan menyertakan WAF *Mod Security* pada web server VPS Fikom UMI [9]. Adapun prosesnya seperti pada *script* di bawah:

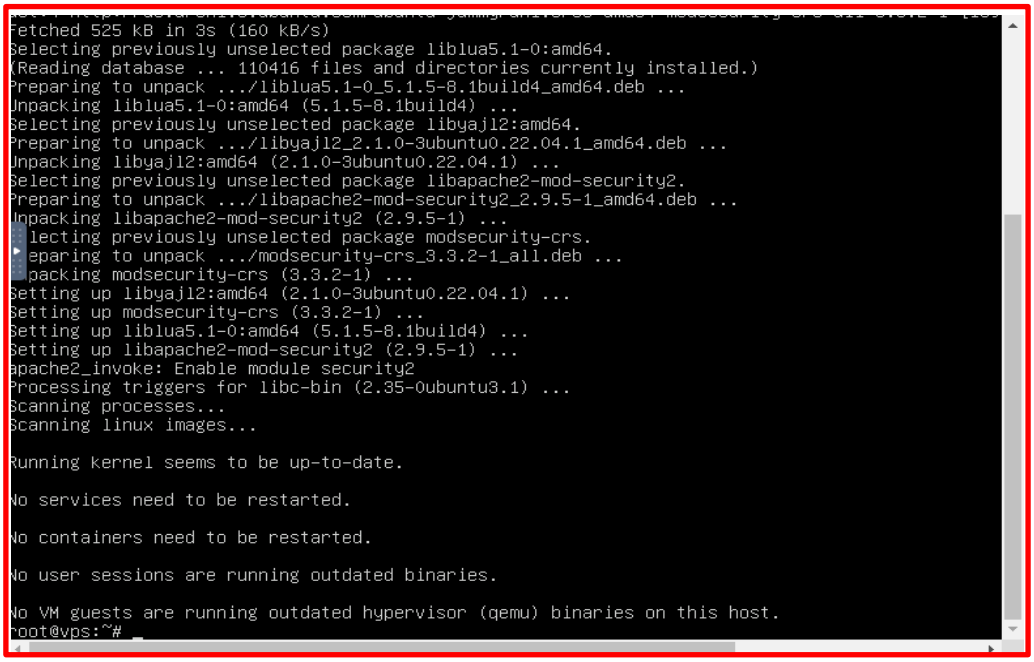
=> Implementasi Keamanan WAF *Mod Security*
sudo apt install libapache2-mod-security2
Script bertujuan untuk melakukan installasi paket WAF dengan *Mod Security*.

Berdasarkan *script* installasi, berikut adalah proses installasi keamanan WAF dengan *Mod Security* yang terlihat seperti Gambar 8.



Gambar 8 Installasi WAF *Mod Security*

Berdasarkan pada Gambar 9, adapun hasil installasi WAF *Mod Security* pada web sever VPS Fikom UMK seperti pada Gambar 9.

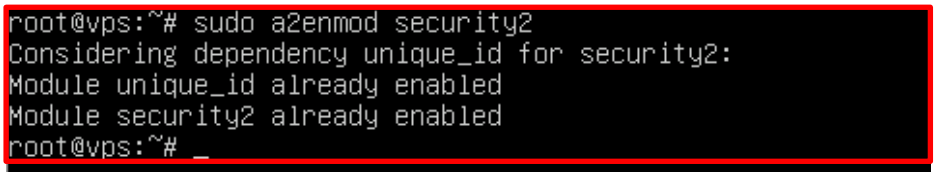


Gambar 9 Installasi WAF *Mod Security* Selesai

Berdasarkan pada Gambar 9, selanjutkan aktifkan WAF Mod Security dengan perintah seperti di bawah:

=> Aktifasi WAF *Mod Security* *sudo a2enmod security2* *Script* bertujuan untuk melakukan aktivasi WAF dengan *Mod Security*.

Berdasarkan *script* aktivasi, berikut adalah proses aktivasi keamanan WAF dengan *Mod Security* yang terlihat seperti Gambar 10.



Gambar 10 WAF *Mod Security* Aktif

3. Pengujian Serangan DDoS Dengan Keamanan WAF Mod Security

Setelah dilakukan penambahkan keamanan WAF, selanjutnya menguji keamanan WAF dengan serangan DDoS. Berikut adalah hasil serangan DDoS Setelah adanya WAF *Mod Security* seperti pada Gambar 11.

Gambar 11 Pengujian Serangan DDoS Setelah Adanya WAF

Berdasarkan pada Gambar 11, pengujian serangan DDoS tidak berhasil dilakukan, sehingga kondisi CPU VPS Fikom UMI seperti pada Gambar 13.

Gambar 12 Kondisi CPU VPS Setelah Adanya WAF

Berdasarkan pada Gambar 12, kondisi CPU VPS dari serangan DDoS dengan mengirimkan paket data adalah 1.4%, kondisi CPU tidak mengalami kenaikan yang signitifikan, sehingga pada kondisi ini terjadi disebabkan adanya keamanan web server dengan WAF *Mod Security* yang dapat menolak seluruh kiriman atau banjiran paker dari serangan DDoS.

4. Hasil Pengujian DDoS Sebelum Adanya Keamanan

Pengujian DDoS dilakukan sebanyak 10 kali pengujian dengan pengiriman besaran paket yang berbeda pada web server VPS Fikom UMI. Adapun hasilnya dapat terlihat sepertiTabel 2.

Tbel 2 Lapora Hasil Pengujian DDoS

No	Pengujian	*Besaran Paket*	*Kondisi CPU*	Keterangan
1	Pengujian DDoS 1	100	3.3.%	Berhasil
2	Pengujian DDoS 2	300	4.2%	Berhasil
3	Pengujian DDoS 3	500	5.3%	Berhasil
4	Pengujian DDoS 4	1000	5.8%	Berhasil
5	Pengujian DDoS 5	5000	7.5%	Berhasil
6	Pengujian DDoS 6	10000	15.4%	Berhasil
7	Pengujian DDoS 7	20000	20.1%	Berhasil
8	Pengujian DDoS 8	50000	32.4%	Berhasil
9	Pengujian DDoS 9	80000	35.2%	Berhasil
10	Pengujian DDoS 10	100000	40.3%	Berhasil

Berdasarkan laporan penyerangan Tabel 2, diketahui bahwa serangan DDoS berhasil dilakukan dengan 10 kali percobaan pengiriman data. Hal ini dikarenakan belum ada keamanan web server dari serangan DDoS.

5. Hasil Pengujian DDoS Setelah Adanya Keamanan

Pengujian DDoS dilakukan sebanyak 10 kali pengujian dengan pengiriman besaran paket yang berbeda pada web server VPS Fikom UMI setelah adanya keamanan WAF *Mod Security*. Adapun hasilnya dapat terlihat seperti tabel 3.

Tabel 3 Laporan Hasil Pengujian DDoS Setelah Adanya WAF

No	Pengujian	*Besaran Paket*	*Kondisi CPU*	Keterangan
1	Pengujian DDoS 1	100	1.4%	Tidak Berhasil
2	Pengujian DDoS 2	300	1.3%	Tidak Berhasil
3	Pengujian DDoS 3	500	1.6%	Tidak Berhasil
4	Pengujian DDoS 4	1000	1.4%	Tidak Berhasil
5	Pengujian DDoS 5	5000	1.3%	Tidak Berhasil

No	Pengujian	*Besaran Paket*	*Kondisi CPU*	Keterangan
6	Pengujian DDoS 6	10000	1.3%	Tidak Berhasil
7	Pengujian DDoS 7	20000	1.2%	Tidak Berhasil
8	Pengujian DDoS 8	50000	1.5%	Tidak Berhasil
9	Pengujian DDoS 9	80000	1.6%	Tidak Berhasil
10	Pengujian DDoS 10	100000	1.9%	Tidak Berhasil

Dapat dilihat pada laporan penyerangan Tabel 3. diketahui bahwa serangan DDoS tidak berhasil dilakukan dengan 10 kali percobaan pengiriman data. Hal ini dikarenakan adanya keamanan WAF web server dari serangan DDoS.

6. Hasil Pengujian SQLMap

Pengujian *SQLmap* dilakukan sebanyak 10 kali pengujian pada web server VPS Fikom UMI. Adapun hasilnya terlihat pada tabel 4.

Tabel 4 Laporan Hasil Pengujian *SQLmap*

No	Pengujian	*Comment* (ID)	*Output SQLmap*	Hasil Pengujian
1	Pengujian SQL 1	' or '='--	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
2	Pengujian SQL 2	' or TRUE--	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
3	Pengujian SQL 3	' or 1=1--	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
4	Pengujian SQL 4	' or 'a'='a'--	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
5	Pengujian SQL 5	' or 1=1#	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
6	Pengujian SQL 6	' or 1=1/*	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
7	Pengujian SQL 7	) or '1'='1--	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
8	Pengujian SQL 8	') or ('1'='1--	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
9	Pengujian SQL 9	1' or 1=1 -- -	*GET parameter 'id' not seem to be injectable*	Tidak Terinjeksi
10	Pengujian SQL 10	' or '1'='1	*GET parameter 'id' not seem to be injactable*	Tidak Terinjeksi

Berdasarkan laporan penyerangan Tabel 4, diketahui bahwa *SQLmap* tidak mampu melakukan *injection* terhadap web server VPS Fikom UMI sehingga web server VPS Fikom UMI aman dari serangan SQL injection.

4. KESIMPULAN

Berdasarkan bab pembahasan sebelumnya mengenai konfigurasi dan proses implementasi, dapat diambil beberapa kesimpulan. Dengan kata lain:

1. Analisis keamanan server web Fikom UMI pada VPS dilakukan menggunakan alat serangan DDoS HPing3 dan injeksi SQL. Alat SQLMap di Kali Linux
2. Berdasarkan analisis pengujian serangan DDoS dan injeksi SQL, ditemukan bahwa serangan DDoS mendeteksi kerentanan di server web Fikom UMI, namun serangan injeksi SQL tidak.
3. Keamanan WAF menggunakan Mod Security terhadap serangan DDoS telah berhasil di implementasikan.

4. Berdasarkan 10 pengujian serangan DDoS setelah WAF Mod Security, VPS Fikom UMI memiliki rata-rata CPU sebesar 1,45%. Jadi sebelum WAF Mod Security ada, server web Fikom UMI jauh lebih aman.

REFERENSI

[1] T. Rahmawati, "Optimalisasi Manajemen Bandwidth Berbasis Mikrotik dengan Metode Queue Tree pada Jaringan Wireless Sekolah Menengah Kejuruan Negeri 11 Luwu," *Fak. Tek. Komput. Univ. Cokrominoto Palopo*, 2020.

[2] N. Fandier Saragih, Reinhard Tamalawe, and Indra M Sarkis, "Analisis Dan Implementasi Secure Code Pada Pengembangan Sistem Keamanan Website Fikom-Methodist.Com Menggunakan Penetration Testing Dan Owasp Zap," *J. TIMES*, vol. 12, no. 1, pp. 28–39, 2023, doi: 10.51351/jtm.12.1.2023690.

[3] F. Dali, "Sistem Keamanan Jaringan Menggunakan Cisco AnyConnect Dengan Metode Network Access Manager," *J. Ilmu Tek. dan Komput.*, vol. Vol.X, no. No. X, pp. 1–7, 2017.

[4] R. Riska and H. Alamsyah, "Penerapan Sistem Keamanan Web Menggunakan Metode Web Aplication Firewall," *J. Amplif. J. Ilm. Bid. Tek. Elektro Dan Komput.*, vol. 11, no. 1, pp. 37–42, 2021, doi: 10.33369/jamplifier.v11i1.16683.

[5] A. Aryapranata, "Web Application Firewall pada Situs Web Institut Bisnis Nusantara www.ibn.ac.id," *J. Esensi Infokom J. Esensi Sist. Inf. dan Sist. Komput.*, vol. 4, no. 1, pp. 55–59, 2020, doi: 10.55886/infokom.v4i1.321.

[6] A. D. A. N. Pemrograman, "Pseudocode," *Definitions*, 2020, doi: 10.32388/tf77dy.

[7] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *Aiti*, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[8] W. Andriyan, S. S. Septiawan, and A. Aulya, "Perancangan Website sebagai Media Informasi dan Peningkatan Citra Pada SMK Dewi Sartika Tangerang," *J. Teknol. Terpadu*, vol. 6, no. 2, pp. 79–88, 2020, doi: 10.54914/jtt.v6i2.289.

[9] A. Mutedi and B. Tjahjono, "Systematic Literature Review: Preventing SQL Injection Attacks Using Tools OWASP CSR Web Application Firewall," *J. Inform. Univ. Pamulang*, vol. 7, no. 1, pp. 151–156, 2022, [Online]. Available: http://openjournal.unpam.ac.id/index.php/informatika