JUSTIN
Jurnal Sistem dan Teknologi Informasi
p-ISSN : 2460-3562 / e-ISSN : 2620-8989
DOI: 10.26418/justin.v12i3.80045
Vol. 12, No. 3, Juli 2024

Rancang Bangun *Firewall* Router Mikrotik Berbasis Data Plugin Wordfence

Arif Wicahyanto[1]
[1]*Fakultas Kedokteran, Universitas Sebelas Maret*
Indonesia
[1]wicahyanto@staff.uns.ac.id

Abstrak

Pengguna CMS (*Content Management System*) Wordpress menghadapi berbagai macam serangan siber. Selain risiko keamanan data, serangan siber yang berulang dan terus menerus menghabiskan sumber daya komputasi. Penambahan *firewall* pada perangkat router menjadi salah satu upaya pengamanan *server* dari serangan siber dengan cara memblokir alamat IP penyerang. Pengelola jaringan atau server memperoleh alamat IP penyerang dengan cara mengakses halaman *plugin* Wordfence yang telah terinstall pada Wordpress. Proses tersebut membutuhkan waktu dan sumber daya manusia. Penelitian ini bertujuan untuk merancang dan membangun sistem pemblokiran otomatis pada *firewall router* Mikrotik dengan menggunakan data alamat IP penyerang dari *plugin* Wordfence.

Kata kunci: Wordpress, Wordfence , *Firewall,* Mikrotik

Mikrotik Router Firewall Design Based on Wordfence Plugin Data

Abstract

Wordpress CMS (Content Management System) users face a wide variety of cyberattacks. In addition to data security risks, repeated and continuous cyberattacks consume computing resources. Adding a firewall to the router device is one of the efforts to secure the server from cyber attacks by blocking the attacker's IP address. Network or server managers obtain the attacker's IP address by accessing the Wordfence plugin page that has been installed on Wordpress. The process requires time and human resources. This research aims to design and build an automatic blocking system on the Mikrotik router firewall using the attacker's IP address data from the Wordfence plugin.

Keywords: Wordpress, Wordfence , *Firewall,* Mikroti

I. PENDAHULUAN

Sebagai CMS dengan pengguna terbanyak, Wordpress banyak berhadapan dengan serangan siber seperti SQL *Injection*, XSS, *file upload*, DDOS, dan lainnya. Serangan pada *website* dapat berakibat kerusakan pada *website* atau *website* tidak dapat diakses karena beban *server* yang sangat berat [1]. Serangan-serangan pada *website* berbasis Wordpress menempati posisi tertinggi jika dibandingan serangan pada CMS lainnya [2].

Penambahan *firewall* pada perangkat *router* menjadi pengamanan *server* dari serangan siber [3]. Serangan akan berhenti pada perangakat *router* sehingga *website-website* pada *server* tidak akan mengalami serangan. Perangkat *router* Mikrotik dapat menjalankan fungsi *firewall*, *router* akan memblokir akses ke *server* dari alamat-alamat IP yang melakukan penyerangan [4].

Pada penelitian sebelumnya, "Sistem Keamanan Jaringan Komputer Bridge *Firewall* Menggunakan Router Board Mikrotik RB750" [5] membuktikan bahwa paket data berhasil disaring sesuai aturan yang telah ditetapkan pada *firewall* dengan cara menentukan alamat-alamat IP yang akan disaring.

Penelitian "Otomatisasi Jaringan Menggunakan Script Python Untuk Penyediaan Konfigurasi Internet Dan Manajemen Mikrotik" [6] perangkat Mikrotik berhasil dikonfigurasi secara otomatis dengan memasukan parameter-parameter yang telah ditentukan. Pengguna menjalankan *script* konfigurasi dan proses konfigurasi akan dijalankan secara otomatis oleh *script* Python.

Penelitian "Pemanfaatan Fitur *Layer* 7 *Protocol* Untuk Filter *Website* dan Management *Bandwidth*" [7] menunjukkan bahwa paket data dapat tersaring sesuai

aturan-aturan (*rule*) *firewall layer* 7 yang telah ditetapkan untuk data yang tidak terenkripsi.

Serangan siber yang terjadi pada website yang menggunakan protokol HTTPS membuat data serangan terenkripsi. Hal ini membuat fitur *firewall layer* 7 tidak digunakan. Oleh karena itu dibutuhkan sebuah sumber data alamat – alamat IP penyerang yang dapat digunakan untuk proses pemblokiran.

Wordfence merupakan salah satu *plugin* keamanan Wordpress yang dengan jumlah instalasi terbanyak ke dua dengan jumlah 4 juta instalasi aktif [8]. Salah satu fitur Wordfence adalah adanya data *log* alamat-alamat IP penyerang serta jenis serangan yang dilakukan [9].

Firewall pada perangkat *router* Mikrotik [10] membutuhkan data alamat – alamat IP yang akan diblokir. Pengelola server dapat mengakses halaman log penyerang pada plugin Wordfence dengan terlebih dahulu melakukan proses *login* pada setiap *website* yang akan diakses. Proses yang dilakukan tersebut memakan waktu dan sumber daya manusia [11]. Proses pemblokiran tersebut membutuhkan peran pengelola *server* atau jaringan. Hal ini memungkinkan terjadinya gangguan pada server saat terjadi serangan yang membuat beban server tinggi dan pemblokiran terlambat dilakukan.

Tujuan yang ingin dicapai dari penelitian ini adalah merancang dan membangun sistem yang melakukan pemblokiran alamat IP pada *router* Mikrotik secara otomatis berdasarkan data alamat IP penyerang dari *plugin* Wordfence. Hal ini diharapkan akan menjaga kinerja server tetap normal saat terjadi serangan siber.

II. METODOLOGI PENELITIAN

Pada penelitian ini menggunakan metode PPDIOO yang merupakan singkatan dari Prepare, Plan, Design, Implement, Operate, dan Optimize. PPDIOO merupakan metodologi perancangan dan pengembangan jaringan yang dikembangkan oleh Cisco, dimana pada metode ini setiap tahapannya mendefinisikan *life-cycle* yang berkelanjutan [9]. Adapun tahapan yang akan dilakukan :

A. Prepare

Pemetaan kebutuhan software dan hardware yang akan digunakan. Sofware yang digunakan berupa *server* database MariaDB, program Python 3.10, dan plugin Wordfence. Hardware berupa virtual server dengan 6 *core* vCPU yang menjalankan 32 website berbasis Wordpress.

B. Plan

Langkah-langkah yang dilakukan pada tahap ini meliputi:

1. Penentuan cara data IP penyerang akan dikumpulkan dari website-website Wordpress
2. Penentuan mekanisme otomatisasi pemblokiran IP pada *firewall* Mikrotik.
3. Penentuan bagaimana program Python akan berinteraksi dengan *database* dan *firewall*
4. Penentuan frekuensi pengambilan data pada website.

C. Design

Pada tahap ini dilakukan beberapa mekanisme yaitu

1. Pengambilan data IP pada tabel khusus plugin Wordfence yang menyimpan data IP penyerang kemudian memasukkan pada tabel khusus IP penyerangan Mendesain database MariaDB untuk menyimpan data IP penyerang, termasuk skema tabel dan struktur data.
2. Mendesain algoritma Python untuk mengambil data IP dari tabel khusus IP penyerang dan mengirimkan data tersebut ke firewall Mikrotik.
3. Mendesain *rule firewall* Mikrotik untuk memblokir paket data dari IP yang terdaftar dalam database dan mengatur akses API di router Mikrotik.
4. Mendesain sistem *cron job* untuk menjalankan program Python secara berkala.

D. Implement

Implementasi desain yang telah dibuat pada *server* website-website berbasis Wordpress serta perangkat *router* Mikrotik. Implementasi yang dilakukan meliputi:

1. Mengatur akses baca tabel IP sehingga program Python dapat membaca data IP penyerang.
2. Mengatur akses *username* dan *password* pada *router* Mikrotik untuk keperluan akses API oleh program Python.
3. Memasang program Python pada sistem cron job *server* pada interval 1 menit.

E. Operate

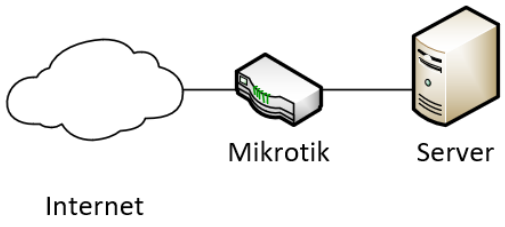
Melakukan pengamatan data rule firewall Mikrotik serta pengamatan pada sistem *cron jo*b *server*, di mana program akan dijalankan setiap 1 menit.

F. Optimize

Mengamati dan menganalisa proses pemblokiran yang dilakukan pada perangkat Mikrotik dengan membadingkan data pada *database* blokir IP.

III. HASIL DAN PEMBAHASAN

Topologi *server* dan *router* Mikrotik yang digunakan pada penelitian sebagai berikut:

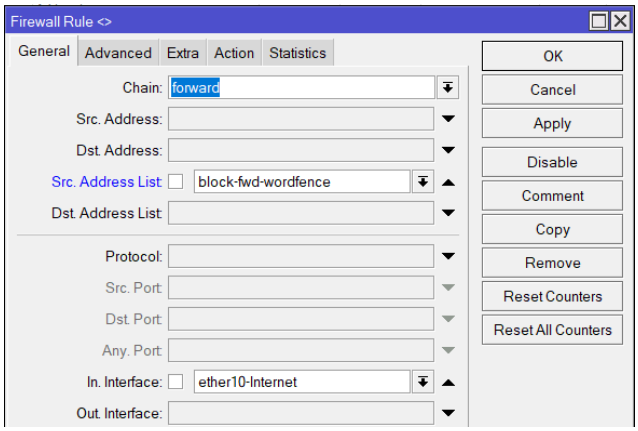


Gambar 1. Topologi jaringan

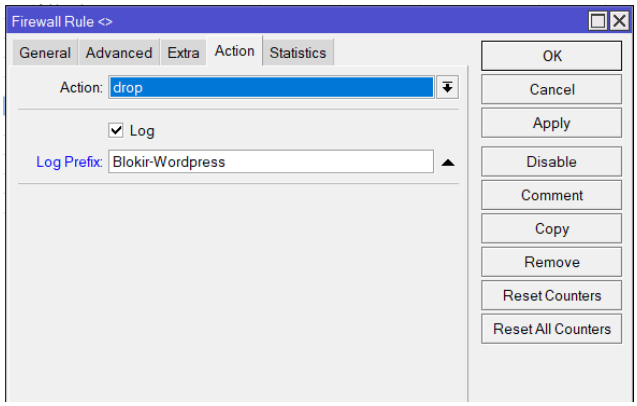
Perangkat *router* Mikrotik memiliki dua buah antar muka jaringan, satu antar muka menuju ke arah internet sedang satu antar muka menuju ke arah *server*. Paket data dengan tujuan *server* akan diteruskan melewati *router* Mikrotik.

Pada *router* Mikrotik dibuat sebuah aturan (*rule*) baru untuk akan memblokir (*drop*) sumber alamat IP yang tercantum dalam daftar IP (Src. Address List) block-fwd-

wordfence. Selanjutnya, daftar alamat IP block-fwd-wordfence akan diisi secara otomatis dengan data IP penyerang oleh program Python.

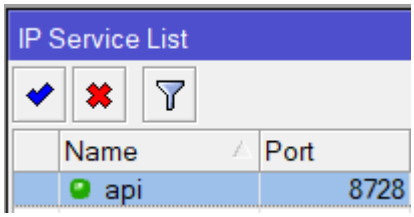


Gambar 2. Aturan blokir *forward src address list* pada *interface* masuk



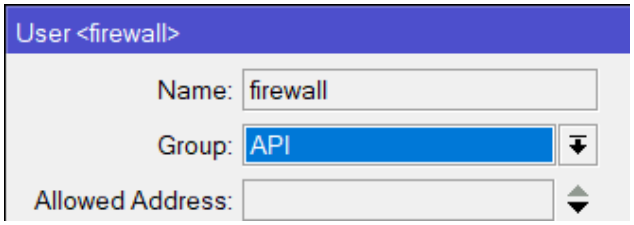
Gambar 3. Aksi blokir *drop* dan *log*

Program Python berkomunikasi dengan perangkat *router* Mikrotik melalui layanan API (*Application Programm Interface*). Layanan API aktif (*listen*) pada *port* 8728.

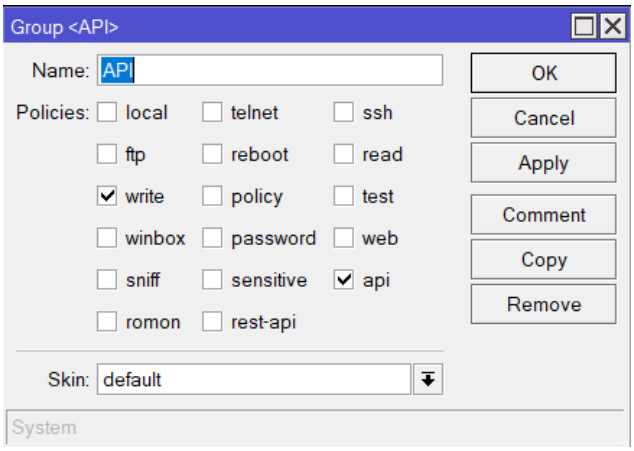


Gambar 4. Layanan API perangkat Mikrotik

Pada perangkat Mikrotik dibuat *user* khusus dengan hak akses *write* dan API. Dengan hak tersebut, user khusus yang dipersiapkan dapat melakukan penambahan data IP pada *Src. Address List* block-fwd-wordfence perangkat Mikrotik dan mengakses fungsi API Mikrotik.

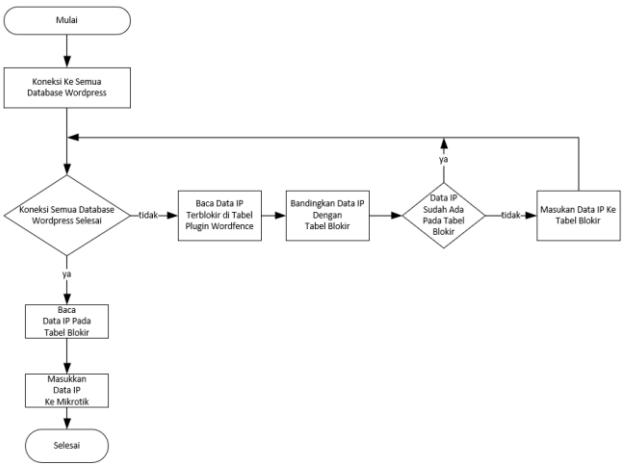


Gambar 5. Grup akses user program Python



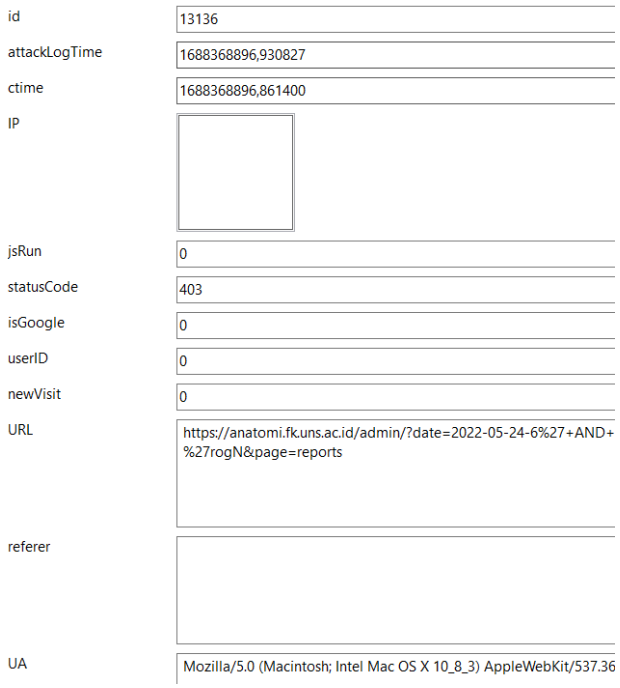
Gambar 6. Hak akses user program Python

Program Python berfungsi untuk untuk melakukan proses otomatisasi pengambilan data alamat IP penyerang, kemudian memasukan data tersebut ke perangkat Mikrotik untuk dilakukan pemblokiran. Adapun alur kerja program Python sebagai berikut:



Gambar 7. *Flowchart* program Python

Program Python melakukan pembacaan *database* MariaDB pada *website-website* yang telah ditentukan. Program Python memilik akses membaca (*read*) pada setiap tabel wp_wfHits atau wp_wfhits. Berikut salah satu contoh data pada tabel Wordfence tersebut:



Gambar 8. Data serangan di sebuah website

Data alamat IP penyerang disimpan pada kolom IP dalam bentuk format *numeric binary string* sehingga untuk memperoleh data IP dalam bentuk *string* digunakan *query* SQL sebagai berikut :

```
1  SELECT SUBSTRING_INDEX(INET6_NTOA(IP),':',-1)
2  as IP FROM `wp_wfhits`
```

Message | Summary | Result 1 | Profile | Status

IP
1.15.141.154
2.58.56.57
2.58.56.57
5.39.23.15
5.39.23.15
5.62.34.17
5.62.34.17
5.62.34.17
5.62.34.17
5.62.34.17
5.62.34.17
5.62.34.17
5.62.34.17

Gambar 9. Data IP dalam tabel log plugin Wordpress

Pada *server* dibuat sebuah *database* khusus untuk penyimpanan data alamat-alamat IP penyerang. Tabel alamat_terblokir dibuat untuk penyimpanan data alamat-alamat IP, adapun desain tabel sebagai berikut :

Fields | Indexes | Foreign Keys | Checks | Triggers | Options | Comment | SQL Preview

Name	Type	Length
id	int	11
website	varchar	255
ip	varchar	255
waktu_terblokir	datetime	
waktu_input	datetime	
kirim_mikrotik	tinyint	4

Gambar 10. *Flowchart* program Python

Kolom *website* digunakan untuk menyimpan sumber *website* yang mengalami serangan, kolom ip digunakan untuk menyimpan data alamat IP penyerang, kolom waktu_terblokir digunakan untuk menyimpan data waktu terblokir, kolom waktu_input digunakan untuk menyimpan data waktu input data ke *database*, dan kolom kirim_mikrotik digunakan untuk menyimpan status pengiriman data ke perangkat Mikrotik. Data bernilai 0 disimpan pada kolom kirim_mikrotik jika data alamat IP belum dikirimkan ke perangkat Mikrotik sedangan data bernilai 1 disimpan pada kolom kirim_mikrotik jika data alamat IP sudah dikirimkan ke perangkat Mikrotik.

Program Python membutuhkan beberapa pustaka (*library*). Pustaka yang digunakan adalah routeros_api [13] yang digunakan untuk berkomunikasi dengan perangkat Mikrotik melalui layanan API. Pustaka strftime dan datetime digunakan untuk operasi yang berhubungan dengan waktu. Agar program Python dapat berkomunikasi dengan *database* MariaDB digunakan pustaka mysql.connector [14].

```
from time import strftime
from datetime import datetime
import mysql.connector
import routeros_api
```

Gambar 11. Pustaka program Python

Program disimpan dalam bentuk file *firewall*.py kemudian dikirim ke *server*. Program diuji untuk mengukur berapa lama waktu yang dibutuhkan untuk menjalankan program tersebut. Pada *server* dijalankan perintah berikut :

```
# time /usr/bin/python3.9  /root/firewall.py
```

Gambar 12. Ujicoba waktu eksekusi program Python

Pada 3 percobaan diperoleh hasil rata – rata eksekusi program 0,316 detik.

TABEL I
WAKTU EKSEKUSI PROGRAM PYTHON

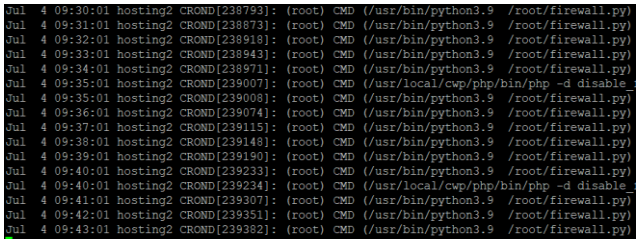
Percobaan	Eksekusi (detik)
1	0,221
2	0,248
3	0,361
4	0,412
5	0,341

Program dipasang dalam sistem cron dan diatur untuk berjalan setiap satu menit.

```
*/1 * * * * root /usr/bin/python3.9  /root/firewall.py
```

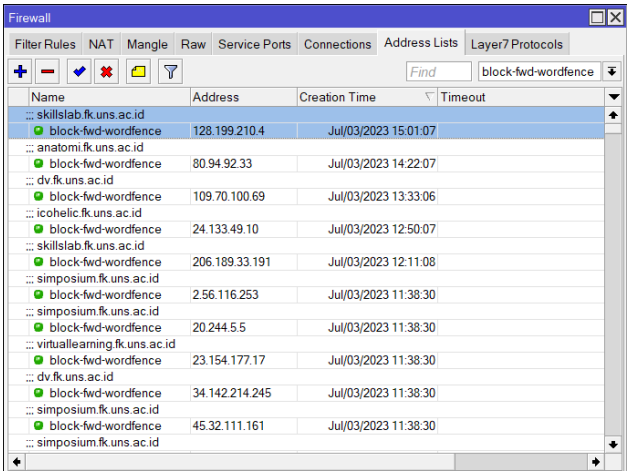
Gambar 13. Pemasangan program Python pada cron *server*

Program Python dipasang pada sistem cron job, dilanjutkan dengan pengamatan proses berjalannya program. Pada *server*, log eksekusi program diamati pada file /var/log/cron. Hasil pengamatan menunjukkan program Python berhasil berjalan setiap menit.



Gambar 14. Log eksekusi program tiap menit

Hasil pengiriman data alamat-alamat IP penyerang ke perangkat Mikrotik oleh program Python diamati pada menu *Address List*.



Gambar 15. Data alamat IP penyerang

Pada data *Address List* block-fwd-wordfence terdapat data alamat – alamat IP penyerang yang secara otomatis ditambahkan oleh program Python. Menu *log* perangkat Mikrotik menampilkan aktivitas pemblokiran alamat-alamat IP oleh *firewall* secara *real time.*

Gambar 16. *Log* blokir alamat IP penyerang

Pada periode waktu Juli 2023 hingga Desember 2024 dilakukan pengamatan jumlah alamat IP penyerang yang berhasil secara otomatis dimasukkan ke dalam data blokir. Hasil pengamatan diperoleh rata-rata 1353 alamat IP per bulan yang berhasil dimasukkan ke dalam daftar blokir *firewall*.

TABEL II
DATA JUMLAH ALAMAT IP PENYERANG

Periode	Jumlah
Juli 2023	1409
Agustus 2023	2614
September 2023	1281
Oktober 2023	784
November 2023	954
Desember 2023	1077

IV. KESIMPULAN

Dari hasil pengujian penelitian rancang bangun *firewall router* Mikrotik berbasis data *plugin* Wordfence dapat di simpulan bahwa data alamat IP penyerang yang bersumber dari *plugin* Wordfence dapat dimasukkan secara otomatis pada daftar blokir IP *firewall router* Mikrotik dengan rata-rata 1353 alamat IP per bulan pada periode Juli 2023 hingga Desember 2023. Penggunaan sumber data IP penyerang lain seperti OWASP ModSecurity dapat dipertimbangkan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.

[2] Securi Inc., “2022 Website Threat Research Report,” Securi Inc., 2023.

[3] P. P. Mukkamala and S. Rajendran, “a Survey on the Different Firewall Technologies,” *Int. J. Eng. Appl. Sci. Technol.*, vol. 5, no. 1, pp. 363–365, 2020, doi: 10.33564/ijeast.2020.v05i01.059.

[4] M. Fakhmi and L. M. Gultom, “Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis),” in *Seminar Nasional Industri dan Teknologi (SNIT)*, 2021, pp. 260–277.

[5] A. Robbahul Barra, R. Sujatmika, and I. Umami, “Sistem Keamanan Jaringan Komputer Bridge Firewall Menggunakan Router Board Mikrotik Rb750,” *J. Teknol. Dan Sist. Inf. Bisnis-JTEKSIS*, vol. 4, no. 1, p. 427, 2022, [Online]. Available: https://doi.org/10.47233/jteksis.v4i2.561

[6] M. Fahmi, M. Maisyaroh, I. Komarudin, S. Faizah, and I. Fadhilah, “Otomatisasi Jaringan Menggunakan Script Python Untuk Penyediaan Konfigurasi Internet Dan Manajemen Mikrotik,” *Bina Insa. Ict J.*, vol. 8, no. 1, p. 53, 2021, doi: 10.51211/biict.v8i1.1517.

[7] B. Kurniawan, F. Panjaitan, P. Studi, T. Informatika, F. I. Komputer, and U. B. Darma, “Pemanfaatan Fitur Layer 7 Protocol Untuk Filter Website Dan Management Bandwidth 1,” *J. Jupiter*, vol. 15, no. 1, pp. 538–548, 2023.

[8] Wordpress, “Wordpress Security Plugin.” Accessed: Apr. 28, 2023. [Online]. Available: https://wordpress.org/plugins/tags/security/
[9] G. Stoyanov, A. Aleksieva-Petrova, and M. Petrov, “Analysis of modern security plugins for wordpress,” 2024, p. 60001. doi: 10.1063/5.0193762.
[10] Mikrotik.com, “RouterOS Filter.” [Online]. Available: https://help.mikrotik.com/docs/display/ROS/Filter
[11] N. Ben-Asher and C. Gonzalez, “Effects of cyber security knowledge on attack detection,” *Comput. Human Behav.*, vol. 48, pp. 51–61, 2015, doi: 10.1016/j.chb.2015.01.039.
[12] S. Susanto, A. Daru, and F. Christanto, “Packet Filtering Gateway and Application Layer Gateway on Mikrotik Router Based Firewalls for Server and Internet Access Restrictions,” 2023, pp. 1–6. doi: 10.1109/ICTECA60133.2023.10490754.
[13] Social WiFi., “RouterOS-api.” [Online]. Available: https://pypi.org/project/RouterOS-api/
[14] MySQL, “MySQL Connector/Python Developer Guide.” [Online]. Available: https://dev.mysql.com/doc/connector-python/en/