Implementasi Plugin Pada Wordpress Untuk MengidetifikasiSerangan Cyber

1st Shendy Setiawan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
shendysetiawann@student.telkomuniversity.ac.id

2nd Nyoman Bogi
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
aditya@telkomuniversity.ac.id

3rd Sofia Naning
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
sofiananing@telkomuniversity.ac.id

***Abstrak* — Seiring dengan perkembangan teknologi informasi yang semakin pesat dan dinamis, tingkat kejahatan siber juga semakin meningkat dewasa ini. Kejahatan siber (*cybercrime*) yang dimaksud ialah percobaan serangan terhadap suatu keamanan sistem informasi. Menurut Ditjen Aptika Kominfo, aktivitas yang dilakukan oleh sekelompok orang yang ingin menembus suatu sistem keamanan bertujuan untuk mendapatkan, mengubah, mencari, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar- benar dibutuhkan. Dirancang sebuah plugin WordPress yang akan menampilkan data dari serangan dan log report yang telah terintegrasi dengan *Security Information and Event Management* (SIEM) dan *Web Application Firewall* (WAF) dari pengujian yang telah dilakukan bahwa plugin sudah berfungsi sesuai dengan fitur yang tersedia dan data yang diambil dengan data yang ditampilkan sudah sesuai.**

Kata kunci*— *Plugin*, SIEM, WAF, *Wordpress

I. PENDAHULUAN

Seiring dengan perkembangan teknologi informasi yang semakin pesat dan dinamis, tingkat kejahatan siber juga semakin meningkat dewasa ini. Kejahatan siber (*cybercrime*) yang dimaksud ialah percobaan serangan terhadap suatu keamanan sistem informasi. Menurut Ditjen Aptika Kominfo, aktivitas yang dilakukan oleh sekelompok orang yang ingin menembus suatu sistem keamanan bertujuan untuk mendapatkan, mengubah, mencari, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan [1].

WordPress adalah sistem manajemen konten (CMS) multifungsi yang dapat diterapkan untuk berbagai tujuan. *WordPress* awalnya digunakan sebagai alat untuk membuat *blog*, tetapi kemudian terus berkembang. Saat ini, Anda dapat menggunakan *WordPress* untuk membuat halaman profil perusahaan untuk toko online [2].

Salah satu keunggulan *WordPress* adalah fitur pluginnya. *Plugin* adalah sekumpulan *script* PHP yang berguna untuk menambah atau mengganti fungsi dasar situs [3]. Dengan menggunakan *plugin*, pengguna dapat menambah fitur *WordPress* yang sebelumnya tidak tersedia, seperti penjadwalan otomatis [4].

Oleh sebab itu, berdasarkan latar belakang yang sudah didapat maka akan dibuat sebuah plugin wordpress untuk menampilkan data dari siem dan waf untuk mengidetifikasi serangan siber.

II. KAJIAN TEORI

A. *Plugin*

Plugin adalah program tambahan yang terintegrasi menyediakan fitur tambahan yang belum tersedia di program utama. Plugin WordPress adalah sekumpulan program aplikasi tambahan berisi fungsi scripting dari bahasa PHP yang menyediakan fungsionalitas atau layanan khusus untuk meningkatkan fungsi yang ada *WordPress* [5].

III. METODE

Adapun metodologi pada penelitian Proyek Akhir ini, sebagai berikut.

A. Studi Literatur

Studi literatur dilakukan dengan mengumpulkan literatur-literatur dan kajian-kajian yang berkaitan dengan permasalahan yang ada pada penelitian proyek akhir ini, baik berupa buku referensi, artikel, maupun *e-journal* yang berhubungan dengan implemntasi plugin pada *wordpress* untuk mengidentifikasi serangan *cyber.*

B. Tahap Perancangan Sistem

Melakukan perancangan implemntasi plugin pada *wordpress* untuk mengidentifikasi serangan *cyber* berbasis PHP dengan membuat diagram alir dan pemodelan sistem lalu dituangkan ke dalam bahasa pemograman PHP menggunakan *software Visual Studio Code*.

C. Tahap Pengujian Sistem

Pengujian implementasi plugin pada *wordpress* untuk mengidentifikasi serangan *cyber* dilakukan dengan menggunakan *blackbox testing* untuk mengetahui plugin berjalan sesuai fitur.

D. Troubleshooting

Apabila terjadi error atau terdapat data yang tidak berjalan dengan baik Ketika mengambil data, maka langkah selanjutnya adalah mencari letak kesalahannya kemudian mencari cara untuk mengatasinya.

E. Tahap Kesimpulan

setelah semua rangkaian metodologi telah dilakukan maka selanjutnya adalah menyimpulkan hasil dari pengujian dan analisis yang telah dilakukan.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan cara kerja plugin yang akan dibuat untuk menampilkan hasil data yang telah di dapat ke dalam plugin. Plugin sebagai komponen tambahan yang diinstal dan diaktifkan pada situs *WordPress* untuk menambahkan fungsional. Ada ribuan plugin yang tersedia, namun pada perancangan ini menggunakan plugin fitur keamanan. Berikut ini adalah contoh perencanaan plugin WordPress yang akan di buat terdiri dari:

1. Tampilan data dari SIEM pada plugin.
2. Tampilan data dari WAF pada plugin.

GAMBAR 1
(Flowchart)

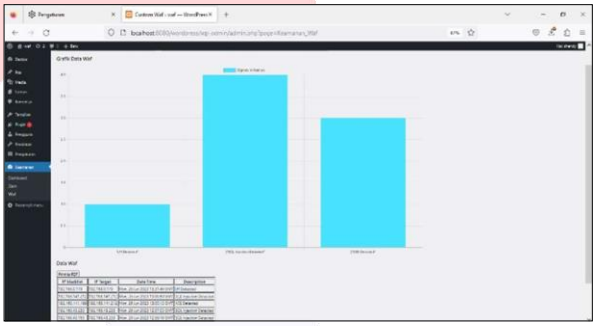
Flowchart yang ditunjukkan pada Gambar 1 menjelaskan sistem akan menerima data SIEM dan data WAF. Plugin menggunakan data JSON untuk menampilkan data yang diperlukan oleh plugin tersebut. Apabila berhasil maka data akan di tampilkan pada tampilan plugin yang telah dibuat dan apabila tidak berhasil maka sistem akan kembali ke pengolahan data JSON.

Pada Blackbox testing dengan metode pengujian keamanan yang dilakukan dengan tujuan mengevaluasi kerentanan atau kelemahan suatu sistem dari sudut pandang pihak luar. Setelah proses pengujian *blackbox*, hasil pengujian perangkat lunak dapat dianalisis untuk mendapatkan pemahaman yang lebih baik tentang kinerja sistem. Dengan menganalisis hasil pengujian dapat mengidetifikasi masalah, kesalahan, dan kekurangan perangkat lunak. Setelah itu, data ini dapat digunakan untuk melakukan perbaikan dan peningkatan yang diperlukan agar sistem beroperasi dengan lebih baik, lebih aman, dan memberikan pengalaman pengguna yang lebih baik. Dalam pengujian skenario *blackbox testing* kesesuaian fungsional pada *plugin* sesuai dengan yang diharapkan.

TABEL 1
(Pengujian Plugin)

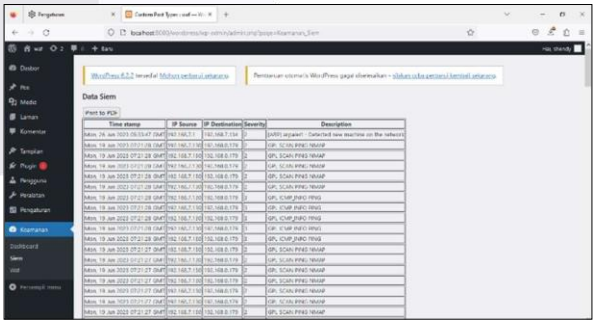
No.	*Scenario*	*Expected Result*	*Output*
1	*Upload plugin* ke W*ordPress.*	Dapat mengupload *plugin* ke *WordPress.*	Berhasil
2	Aktivasi *plugin* yang telah di *upload.*	*Plugin* dapat di aktivasi.	Berhasil
3	Pada menu SIEM menampilkan data SIEM.	Dapat menampilkan data SIEM.	Berhasil
4	Pada menu WAF menampilkan data WAF.	Dapat menampilkan data WAF.	Berhasil
5	Deaktivasi *plugin* yang telah digunakan.	*Plugin* dapat di deaktivasi.	Berhasil
6	Hapus *plugin* dari *WordPress.*	*Plugin* dapat di hapus dari *WordPress.*	Berhasil

Pada Tabel 1 Dapat dilihat bahwa hasil pengujian *blackbox testing* sistem yang di buat berjalan sesuai dengan fitur yang tersedia, hal tersebut dibuktikan dengan adanya *output* dengan keterangan berhasil pada setiap scenario.



GAMBAR 2
(Tampilan WAF)

Pada Gambar 2 dapat dilihat tampilan WAF pada *plugin*, pada grafik terdapat dua sumbu pada sumbu *vertikal* (sumbu y) medeskripsikan banyak nya data pada satu serangan, sedangkan pada sumbu *horizontal* (sumbu x) mendeskripsikan data serangan, kemudian pada tabel terdapat data serangan pada WAF dari database.



GAMBAR 3
(Tampilan SIEM)

Pada Gambar 3 dapat dilihat tampilan SIEM pada plugin, terdapat *time stam*p sebagai waktu aktivitas pada SIEM*, IP source* sebagai IP sumber, *IP destination* sebagai IP tujuan, *severity* sebagai keretanan pada aktivitas dan deskripsi untuk mejelaskan apa yang terjadi.

Dengan menganalisis hasil pengujian dapat mengidetifikasi masalah, kesalahan, dan kekurangan perangkat lunak. Setelah itu, data ini dapat digunakan untuk melakukan perbaikan dan peningkatan yang diperlukan agar sistem beroperasi dengan lebih baik, lebih aman, dan memberikan pengalaman pengguna yang lebih baik. Dalam pengujian skenario *blackbox testing* pada *plugin* sesuai dengan data yang terdapat pada SIEM dan WAF.

V. KESIMPULAN

Dari hasil penelitian yang telah dilakukan dapat disimpulkan bahwa pembuatan plugin telah berhasil dilakukan dan dapat digunakan untuk menampilkan data.

REFERENSI

[1] S. Ali and T. N. Malik, “Intrusion Detection and Prevention against Cyber Attacks for an Energy Management System,” *Mehran Univ. Res. J. Eng. Technol.*, vol. 41, no. 1, pp. 202–219, 2022, doi: https://doi.org/10.22581/muet1982.2201.20.

[2] Surahman, *Buku Sakti SEO WordPress dan Joomla*. Jakarta: PT Elex Media Komputindo, 2018.

[3] Y. Sugiono, *Panduan Membuat Plugin WordPress*. Jakarta: PT Elex Media Komputindo, 2017.

[4] E. Ramadian, A. Hijriani, and R. Prabowo, “Pengembangan Plugin Laporan Penjualan Pada Toko Bibit Bebek Berbobot Berbasis Wordpress,” *J. Perpadun*, vol. 2, no. 3, pp. 344–353, 2021.

[5] Y. Kurniawan, *Menghias WordPress itu Gampang*. Jakarta: PT Elex Media Komputindo, 2008.