Menerapkan Teknik Firewall Aplikasi Web (WAF) Pada Aplikasi SINTEL Untuk Mengatasi Serangan Siber

Robertus Laipaka
STMIK Pontianak; Jl. Merdeka Barat No. 372, (0561) 735555
E-mail: robertus.laipaka@stmikpontianak.ac.id

ABSTRAK

Seiring dengan meningkatnya pertumbuhan aplikasi web, ancaman keamanan juga merupakan faktor utama yang perlu diperhatikan oleh pengembang aplikasi website. Pengembang web sudah menyadari bahwa salah satu kelemahan paling signifikan dari PHP adalah tidak adanya mekanisme penguatan keamanan default. Sehingga rentan terhadap serangan injeksi SQL, XSS, CSRF, malware, dan brute force. Penelitian ini bertujuan membangun aplikasi SINTEL yang aman sebagai upaya menjaga keakuratan informasi yang dimuat pada aplikasi tersebut. Web Application Firewall (WAF) diterapkan berbasis kode atau diintegrasikan langsung dalam aplikasi SINTEL. Dengan integrasi mendalam dalam aplikasi, pengembang dapat memastikan bahwa aplikasi terlindungi secara efektif dari berbagai ancaman keamanan, sambil tetap mempertahankan performa optimal dan kepatuhan terhadap regulasi. Setelah dilakukan melalui pengujian serangan injeksi SQL, XSS, CSRF, malware, dan brute force, aplikasi SINTEL mampu mengatasi serangan dengan baik. Kondisi ini membuktikan menerapkan WAF berbasis kode pada aplikasi web masih dianggap sangat efektif dalam mengatasi ancaman serangan siber.

Kata kunci: *WAF*, *SQL, XSS, CSRF, SINTEL*

ABSTRACT

Along with the increasing growth of web applications, security threats are also a major factor that website application developers need to pay attention to. Web developers are already aware that one of the most significant weaknesses of PHP is the lack of a default security hardening mechanism. So it is vulnerable to SQL injection, XSS, CSRF, malware and brute force attacks. This research aims to build a safe SINTEL application as an effort to maintain the accuracy of the information contained in the application. Web Application Firewall (WAF) is implemented code-based or integrated directly in the SINTEL application. With deep integration within applications, developers can ensure that applications are effectively protected from a variety of security threats, while maintaining optimal performance and regulatory compliance. After testing SQL injection, XSS, CSRF, malware and brute force attacks, the SINTEL application was able to overcome the attacks well. This condition proves that implementing code-based WAF on web applications is still considered very effective in overcoming the threat of cyber attacks.

***Key words**: WAF, SQL, XSS, CSRF, SINTEL*

1. Pendahuluan

Diera lanskap digital saat ini, keamanan sistem informasi adalah hal yang sangat penting dalam pengembangan aplikasi web(Mahendra Ardiansyah, 2023). Seiringan adanya peningkatan pertumbuhan web, ancaman keamanan juga merupakan faktor utama yang diperhatikan oleh pemilik website. Serangan siber, pembobolan data, dan insiden keamanan lainnya sudah menjadi hal yang biasa, sehingga membuat bisnis dan pengguna rentan terhadap eksploitasi (Herdiana et al., 2021) Sebagai pengembang web yang menggunakan PHP, penting untuk memahami potensi risiko dan menerapkan praktik terbaik. Sebab salah satu kelemahan paling signifikan dari PHP adalah tidak adanya mekanisme penguatan keamanan default. Jadi aplikasi web yang dibuat dengan PHP rentan terhadap beberapa ancaman keamanan (Alamsyah, 2021). Ancaman ini termasuk injeksi SQL, serangan XSS, serangan CSRF, malware dan serangan brute force (Madani et al., 2024). Mengembangkan aplikasi web yang aman dengan PHP bukanlah suatu pilihan, namun sebuah kewajiban. Begitu juga dengan pengembangan aplikasi web SINTEL (sistem informasi intelijen), perlu menerapkan keamanan yang sangat ketat, hal ini dikarenakan aplikasi tersebut memuat informasi yang sensitif seperti, penyelenggaran pemerintahan daerah, pelaksanaan program pembangunan, pelayanan publik, ideologi, politik, ekonomi, sosial budaya dan hankam. Kesalahan informasi yang diterima sebagai akibat dari adanya gangguan atau upaya modifikasi dari pihak luar, akan berdampak pada ketidaktepatan dalam memberikan respon dari suatu kejadian. Peluang terjadinya gangguan terhadap aplikasi SINTEL cukup tinggi, hal ini dikarenakan operator aplikasi tersebut berasal dari 14 (empat belas) kabupaten/kota Provinsi Kalimantan Barat.

Beranjak dari kebutuhan akan pentingnya memastikan keamanan terhadap aplikasi SINTEL, maka perlu menerapkan teknik keamanan Web Application Firewall (WAF). Menerapkan WAF adalah langkah proaktif yang sangat penting untuk melindungi aplikasi web dari berbagai ancaman keamanan, memastikan keamanan data pengguna, dan menjaga kepercayaan serta reputasi organisasi. WAF melindungi dari serangan jenis SQL Injection, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF) dengan memeriksa dan memfilter trafik web yang mencurigakan (Burhani & Priyawati, 2024). WAF pada aplikasi web adalah komponen keamanan yang bertujuan untuk melindungi aplikasi web dari berbagai ancaman dan serangan siber. WAF mampu melakukan analisis perilaku untuk mengenali pola aktivitas yang tidak biasa yang mungkin menunjukkan adanya serangan (Burhani & Priyawati, 2024; Haikal Muhammad et al., 2023). Dengan kemampuan untuk memeriksa, menyaring, dan memblokir lalu lintas yang mencurigakan atau berbahaya, WAF memberikan lapisan perlindungan tambahan yang esensial dalam menjaga keamanan, keandalan, dan kepatuhan aplikasi web (Khabibah et al., 2024).

E-ISSN : 2809-7165

Pada penelitian ini, WAF diterapkan pada aplikasi SINTEL dalam bentuk code. Menerapkan WAF dalam bentuk coding memiliki beberapa keuntungan yang signifikan (Ardiansyah et al., 2023). WAF berbasis kode atau yang diintegrasikan langsung dalam aplikasi memberikan fleksibilitas dan kontrol yang lebih besar atas keamanan aplikasi web. Aturan dan logika keamanan dapat disesuaikan secara spesifik untuk kebutuhan aplikasi tertentu, mengatasi kelemahan yang unik pada aplikasi tersebut. Pengembang dapat segera merespons dan mengimplementasikan perlindungan terhadap ancaman baru atau zero-day vulnerabilities. Menerapkan WAF dalam bentuk coding memberikan fleksibilitas, kontrol, dan efisiensi yang lebih besar dibandingkan dengan solusi WAF tradisional yang berbasis perangkat keras atau cloud.

2. Metode Penelitian

Metode penelitian yang digunakan adalah metode Design Science Research (DSR) dan ini dikarenakan DSR berfokus pada penciptaan dan evaluasi artefak (seperti model, metode, dan sistem) yang bertujuan untuk menyelesaikan masalah praktis dan menghasilkan kontribusi teoretis **(Hevner & Brocke, 2023)**. DSR juga merupakan metode penelitian yang digunakan untuk mengembangkan solusi inovatif terhadap masalah kompleks dalam bidang teknologi informasi, sistem informasi, dan rekayasa. Metode perancangan sistem menggunakan User-Centered Design (UCD). Pendekatan UCD adalah perancangan sebuah desain interface yang memusatkan pengguna sebagai peran utama dalam menentukan kebutuhan sistem. Konsep dari UCD adalah pengguna sebagai pusat dari proses pengembangan sistem (Priyatna et al., n.d.). Pendekatan User-Centered Design (UCD) melibatkan pengguna sejak tahap analisa, desain, testing, build/redesign. Terdapat 4 (empat) tahap dalam pendekatan UCD yaitu *understand context of use, specify user requirements, design olutions and evaluation against requirements* (Rahmawati, 2020). Pemodelan sistem menggunakan Unified Modeling Language (UML).

3. Hasil dan Pembahasan

1. Understand context of use

Pengguna aplikasi ini adalah Pusat Komunikasi dan Informasi Daerah Kabupaten dan Kota untuk wilayah Kalimantan Barat. Melalui aplikasi ini, pemerintah daerah dapat melaporkan situasi Daerah Kabupaten dan Provinsi Kalimantan Barat secara real-time. Manajemen kegiatan intelijen dirasa sangat penting dan bertujuan untuk meningkatkan kecepatan dalam memberikan respon terhadap kejadian. Hak akses terhadap aplikasi dibedakan berdasarkan kategori akun yang terdiri dari operator, admin dan pimpinan. Setiap Daerah wajib memberikan laporan situasi harian Daerah masing-masing yang mencakup

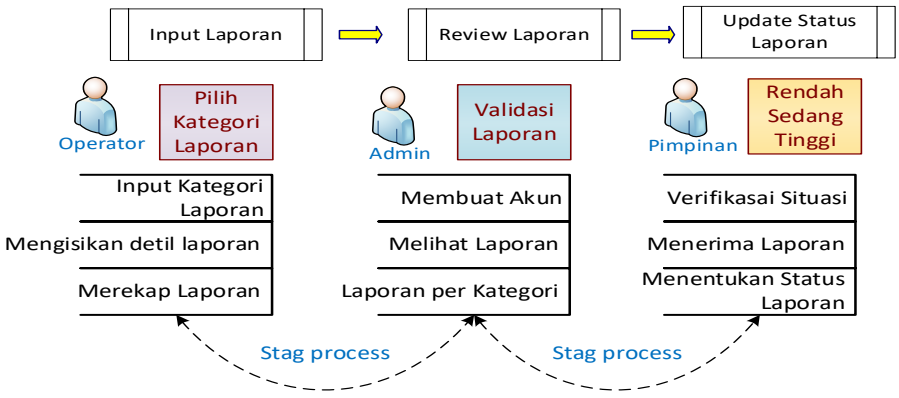
laporan penyelenggaran pemerintahan daerah, pelaksanaan program pembangunan, pelayanan publik, ideologi, politik, ekonomi, sosial budaya dan hankam. Pihak penerima laporan dapat memberikan status (rendah, sedang dan tinggi) terhadap setiap laporan yang disampaikan.

2. Specify user requirements

Langkah pertama dalam memahami kebutuhan pengguna dengan menggunakan teknik brainstorming yaitu mengembangkan solusi kreatif untuk mengatasi masalah tersebut. Brainstorming berupaya menganalisis kebutuhan pengguna dan menemukan hasil seperti desain antarmuka yang menarik dan mudah digunakan serta analisis aplikasi terhadap fitur-fitur yang dapat digunakan oleh pengguna, baik penjual produk maupun pembeli. Berdasarkan hasil identifikasi dari pemangku kepentingan, dapat diketahui bahwa pengguna akhir dari sistem ini adalah semua Daerah Kabupaten dan Kota yang ada di Kalimantan Barat.

3. Design solutions

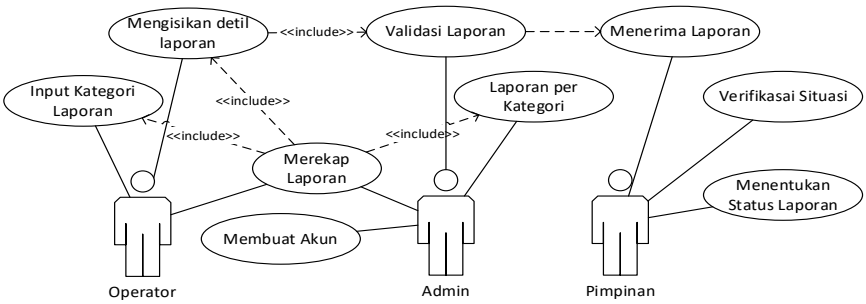
Saat merancang solusi terhadap kebutuhan pengguna yang dijelaskan pada proses sebelumnya, proses desain ini melewati beberapa tahapan desain arsitektur aplikasi, desain diagram, dan desain antarmuka aplikasi. Desain arsitektur yang ideal harus memenuhi kebutuhan pengguna, kompatibel/independen secara teknis, tersedia dengan mudah dan andal kapan saja, mudah dikembangkan, dan tersedia bagi sebanyak mungkin pengguna. Berikut ini adalah rancangan arsitektur aplikasi SINTEL (lihat gambar 1):



Gambar 1. Arsitektur Aplikasi SINTEL

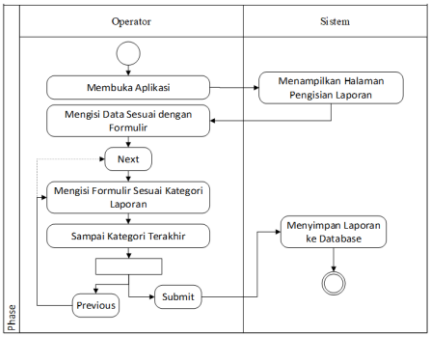
Pada gambar 1 diatas dapat dijelaskan bahwa pengguna aplikasi memiliki tugas masing-masing dan saling berhubungan sesuai dengan stag process. Admin memiliki peran dalam menyediakan akun dan juga melakukan review dari setiap laporan yang telah diinputkan oleh operator. Laporan yang dinyatakan valid dapat dilihat dan diverifikasi oleh Pimpinan untuk mengetahui level penangan dari setiap laporan. Pimpinan akan menentukan status laporan berdasarkan tingkat urjensinya yaitu Rendah, Sedang dan Tinggi. Antarmuka pengguna harus

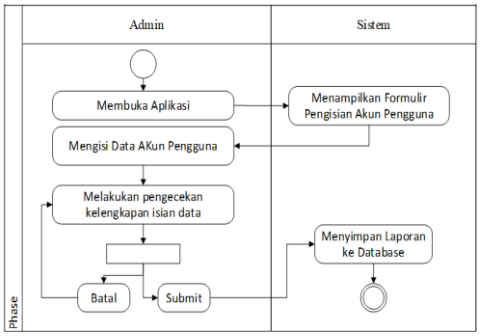
dimodelkan secara visual menggunakan UML (Unified Modeling Language) untuk menggambarkan perilaku sistem selama interaksi pengguna. Diagram use case digunakan sebagai titik awal untuk desain antarmuka pengguna dan biasanya digunakan untuk menangkap persyaratan sistem, yaitu apa yang harus dilakukan oleh sistem. Berikut ini adalah use case diagram SINTEL (lihat gambar 2):



Gambar 2. Use Case Diagram SINTEL

Pada gambar 2 di atas dapat dijelaskan bahwa terdapat 9 use case yang menjadi titik penghubung komunikasi antara actor operator, admin dan pimpinan. Actor Operator melakukan aktivitas pengisian data laporan, mengisikan laporan secara detil berdasarkan kategori dan merakap laporan berdasarkan kategori. Actor Admin melakukan aktivitas pembuatan akun pengguna aplikasi, melihat laporan sambil melakukan validasi dan melihat laporan berdasarkan kategori. Sedangkan actor Pimpinan menerima laporan valid, melakukan verifikasi situasi dari laporan, kemudian menentukan status dari laporan yang telah diverifikasi. Untuk memahami dengan jelas aktivitas setiap use case, diperlukan diagram aktivitas yang mewakili alur aktivitas pada aplikasi SINTEL yang diterapkan. Dapat dlihat pada gambar 3 (a) dan gambar 3(b)):

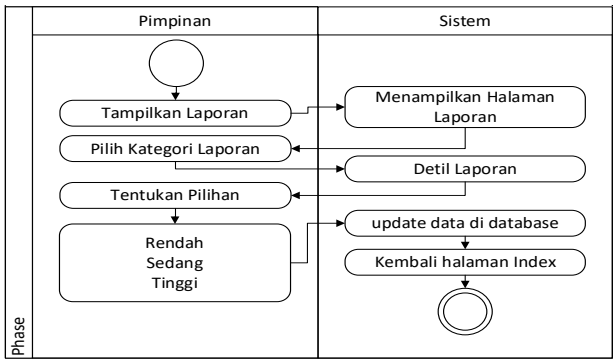




Gambar 3 (a). Diagram Pengisian Laporan Gambar 3 (b). Diagram Pembuatan Akun Pengguna

Gambar 3(a) di atas merupakan Activity Diagram dari pengisian laporan. Seperti terlihat pada gambar tersebut, terdapat 2 swimlane, yaitu Operator dan Sistem. Operator melakukan pengisian aplikasi secara berurutan berdasarkan kategori laporan. Setelah semua kategori laporan diisikan, maka operator dapat menyimpan data laporan. Gambar 3(b) di atas

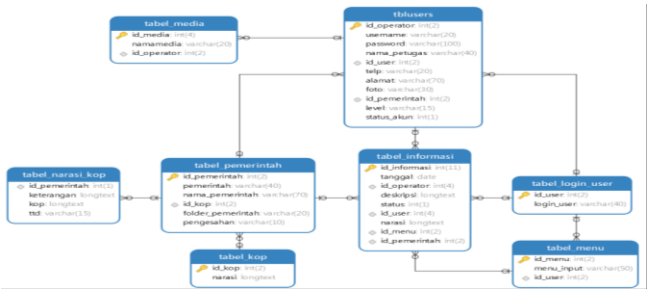
merupakan Activity Diagram dari fungsi pembuatan akun penggguna. Seperti terlihat pada gambar tersebut, terdapat 2 swimlane, yaitu admin dan Sistem. Activity Diagram Pembuatan Akun Pengguna dimaksud untuk menambahkan data pengguna pada sistem SINTEL. Dengan gambaran tersebut, admin dapat melakukan pekerjaan dengan baik dan bisa meminimalkan kesalahan. Berikutnya adalah activity diagram Penentuan Status Laporan (lihat gambar 4):



Gambar 4. Activity Diagram Penentuan Status Laporan

Seperti terlihat pada gambar 4 di atas, terdapat 2 swimlane, yaitu Pimpinan dan Sistem. Pimpinan akan menimbulkan reaksi dari aplikasi itu sendiri. Pimpinan dapat menampilkan laporan situasi daerah tertentu, membaca detil laporan dan menentukan pilihan status laporan situasi tersebut. Pemberian label status Rendah, Sedang dan Tinggi sangat penting sebagai dasar untuk mengambil tindakan yang diperlu untuk mengatasi laporan yang telah disampaikan.

Suatu informasi yang ditampilkan pada sistem bisa bersumber dari beberapa tabel database dan secara khusus sistem SINTEL terdiri dari beberapa tabel yang saling terhubung dalam model Relational Database Management System. Berikut ini adalah Gambar 5 Diagram Hubungan Entitas aplikasi SINTEL.

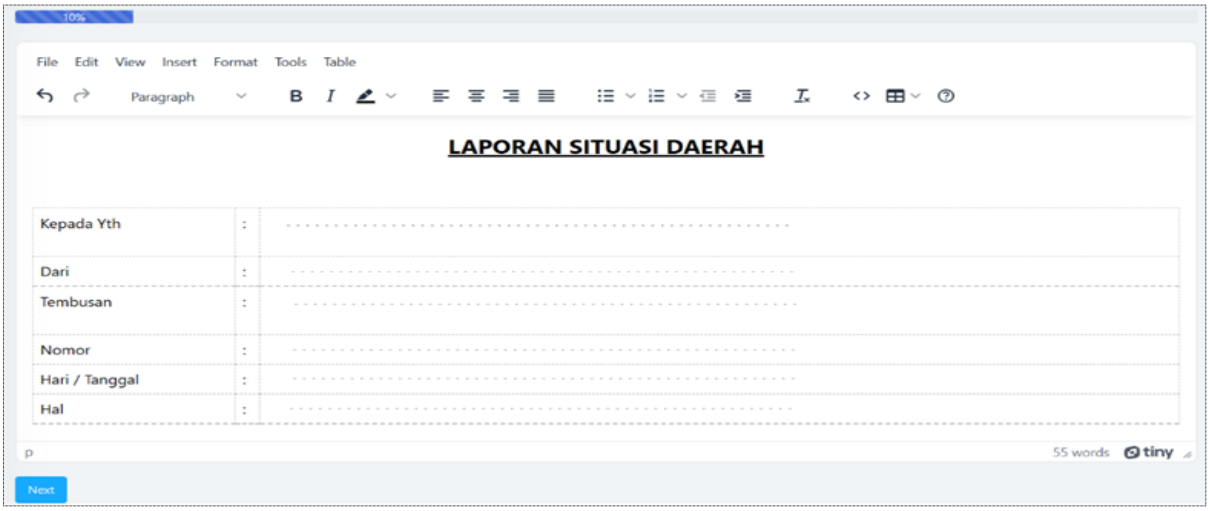


Gambar 5. Diagram Hubungan Entitas

Pada gambar 5 diatas, dapat dipahami bahwa dalam menghasilkan aplikasi SINTEL, memerlukan 9 tabel database yang saling berhubungan antara yang satu dengan yang lainnya. Keterhubungan ini membuktikan adanya integrasi data pada setiap entitas. Ketersediaan data pada master tabel sangat penting bagi transaction tabel. Entitas yang selalu melakukan update terhadap data adalah entitas informasi (tabel_informasi). Langkah

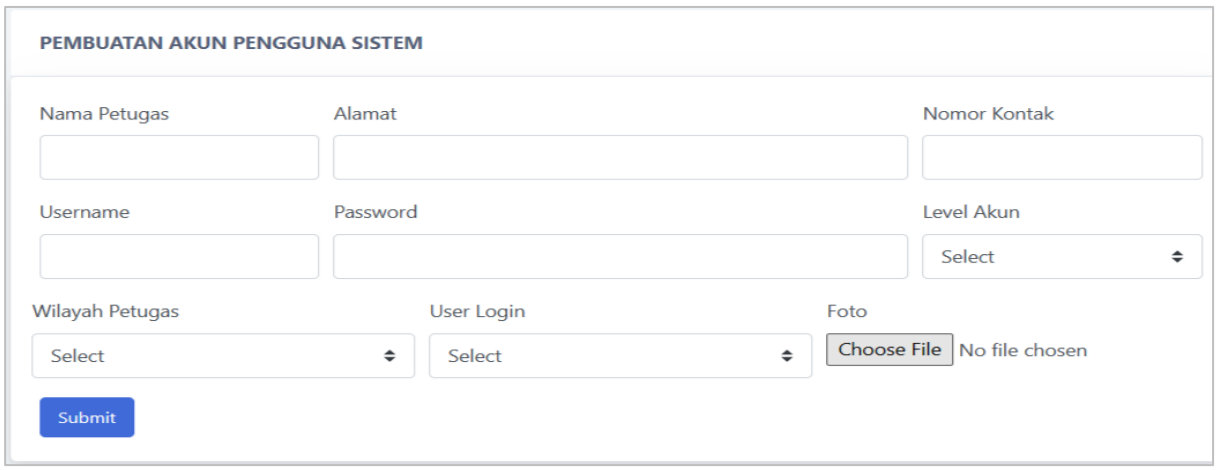
E-ISSN : 2809-7165

selanjutnya yang perlu dipenuhi pada aplikasi SINTEL adalah menyediakan desain fitur yang dapat dipergunakan oleh operator untuk mengisikan laporan situasi daerah (lihat gambar 6).



Gambar 6. Form Pengisian Laporan

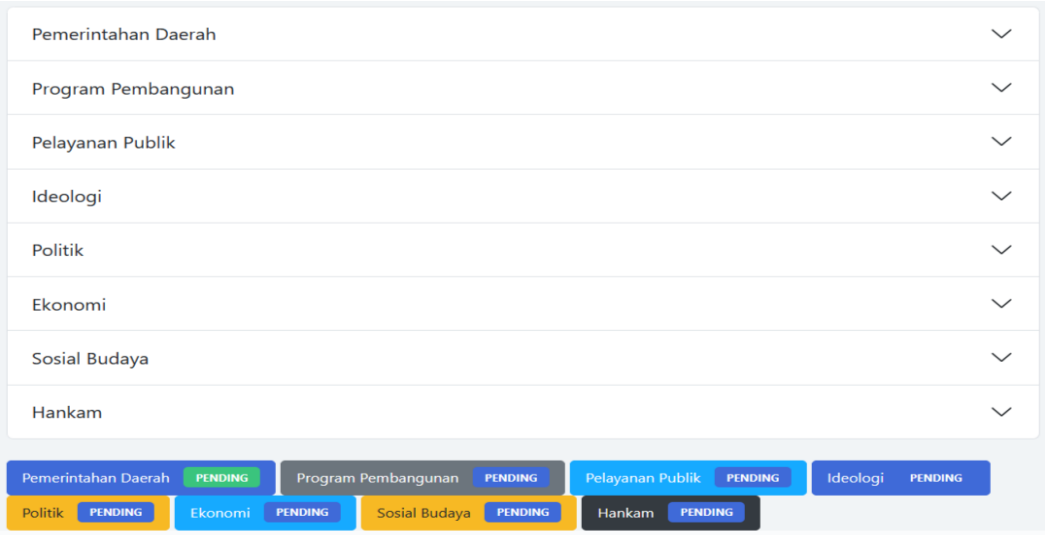
Pada gambar 6 di atas, form pengisian laporan ini situasi daerah ini menjadi hal yang utama pada aplikasi SINTEL. Setiap operator dari masing-masing daerah melaporkan situasi daerahnya melalui form ini. Pada form ini ada bagian utama yang harus diisi yaitu pada bagian header. Bagian ini merujuk kepada laporan ini disampaikan, kemudian melanjutkan pengisian dengan menekan tombol next. Setelah mengisikan bagian pertama dari katergori laporan, operator menekan tombol next kembali sampai semua kategori diisikan jika laporannya tidak nihil. Berikut ini adalah fitur pembuatan akun pengguna aplikasi SINTEL (lihat gambar 7).



Gambar 7. Pembuatan Akun Pengguna

Fitur pembuatan akun pengguna dipergunakan oleh admin untuk meregistrasi akun pengguna dari aplikasi SINTEL. Setiap Daerah masing-masing memiliki 3 akun dengan level yang berbeda yaitu, level operator, admin dan pimpinan. Penggunaan level ini untuk membedakan hak akses pada aplikasi. Setiap level memiliki peran masing-masing, namun

peran utama dimulai dari operator. Berikut ini adalah fitur menentukan status laporan (lihat gambar 8).



Gambar 8. Menentukan Status Laporan

Fitur menentukan status laporan merupakan fitur yang secara khusus dipergunakan oleh pimpinan untuk membaca dan memahami setiap laporan situasi daerah yang telah disampaikan oleh operator. Status dengan level tinggi perlu ditangani secara perioritas karena memiliki urjensi yang tinggi dan berbahaya jika tidak dilakukan penangan dengan segera.

a. Penerapan WAF untuk validasi Input

WAF dapat mendeteksi pola serangan umum seperti SQL injection, XSS, dan buffer overflow melalui pre-defined rules atau signatures. Ketika ada input yang mencurigakan, WAF akan memblokirnya sebelum mencapai server aplikasi.

b. Penerapan WAF untuk Log dan Monitoring pada login dan URL

WAF akan berada di antara pengguna dan aplikasi web, memeriksa setiap permintaan HTTP yang masuk. Setiap permintaan yang masuk akan dicatat ke dalam log, termasuk detail seperti alamat IP, timestamp, URL yang diakses, dan status permintaan. WAF akan terus memonitor log untuk mendeteksi pola yang mencurigakan atau aktivitas berulang yang mungkin mengindikasikan serangan.

Function log_event untuk mencatat kejadian ke dalam file log. function monitor_log untuk memonitor log dan mendeteksi kejadian tertentu. Jika ditemukan kejadian percobaan login gagal, kirim notifikasi atau lakukan tindakan yang sesuai. Function log_login untuk memeriksa dan mencatat kejadian login. function log_url_access untuk memeriksa dan mencatat kejadian akses URL.

c. Penerapan WAF untuk mengatasi serangan SQL Injection

Menggunakan metode validasi server-side dan client-side untuk memastikan bahwa input tidak mengandung karakter yang mencurigakan atau kode SQL. Menggunakan parameterized queries atau prepared statements saat berinteraksi dengan database. PDO secara otomatis menyandi nilai input sesuai dengan jenis data yang diharapkan (seperti integer, string, dll.), sehingga mencegah eksekusi perintah SQL tambahan yang tidak diinginkan.

d. Penerapan WAF untuk mengatasi serangan Brute Force

Membatasi jumlah permintaan yang dapat dilakukan dari alamat IP tertentu dalam interval waktu tertentu. Mengimplementasikan CAPTCHA pada formulir login atau area yang menerima input sensitif. menggunakan daftar putih (whitelist) untuk IP yang dikenal aman dan daftar hitam (blacklist) untuk IP yang dicurigai melakukan serangan. Menggunakan session PHP untuk melacak jumlah percobaan login yang telah dilakukan oleh pengguna. Ketika pengguna mencoba login, akan menambahkan jumlah percobaan login dalam session. Jika jumlah percobaan login melebihi batas yang ditentukan fungsi akan mengembalikan nilai true.

e. Penerapan WAF untuk memblokir serangan XSS (Cross-Site Scripting)

Memvalidasi semua input yang diterima dari pengguna, baik di sisi klien maupun sisi server. Pastikan input tidak mengandung karakter khusus seperti <, >, ", ', dan & yang bisa dieksekusi sebagai skrip oleh browser. Mengcode (mengubah karakter khusus menjadi entitas HTML) data yang berasal dari pengguna sebelum ditampilkan kembali di halaman web.

Menggunakan pendekatan sederhana dengan regex untuk mendeteksi tag <script> dalam input pengguna. Jika serangan XSS terdeteksi, kita memblokir akses dengan memanggil fungsi blockAccess(). Pengguna dapat menyesuaikan dan memperluas kode ini sesuai dengan kebutuhan, seperti menambahkan aturan-aturan tambahan untuk mendeteksi serangan lainnya atau menyesuaikan tindakan yang diambil ketika serangan terdeteksi.

4. Kesimpulan

Web Application Firewall (WAF) diterapkan berbasis kode atau diintegrasikan langsung dalam aplikasi SINTEL. Dengan integrasi mendalam dalam aplikasi, pengembang dapat memastikan bahwa aplikasi terlindungi secara efektif dari berbagai ancaman keamanan, sambil tetap mempertahankan performa optimal dan kepatuhan terhadap regulasi. Setelah dilakukan melalui pengujian serangan injeksi SQL, XSS, CSRF, malware, dan brute force, aplikasi SINTEL mampu mengatasi serangan dengan baik. Kondisi ini membuktikan menerapkan WAF berbasis kode pada aplikasi web masih dianggap sangat efektif dalam mengatasi ancaman serangan siber. Aplikasi ini perlu dilakukan penambahan keamanan agar memiliki keamanan yang cukup untuk mengatasi serangan siber yang sudah semakin canggih.

E-ISSN : 2809-7165

Daftar Pustaka

Alamsyah, H. (2021). Penerapan Sistem Keamanan WEB Menggunakan Metode WEB Aplication Firewall. *Jurnal Amplifier Mei*, *11*.

Ardiansyah, Y., Agus Sunandar, M., & Muhyidin, Y. (2023). Implementasi Keamanan Website Dengan Metode Firewall Aplikasi Web (Waf) Studi Kasus: Web Desa Wantilan. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Issue 3).

Burhani, L. F., & Priyawati, D. (2024). Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (PTES). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *9*(1), 307–319. https://doi.org/10.29100/jipi.v9i1.4455

Haikal Muhammad, H., Id Hadiana, A., Ashaury Informatika, H., Jenderal Achmad Yani Cimahi Jl Terusan Jend Sudirman, U., Cimahi Sel, K., Cimahi, K., & Barat, J. (2023). Pengamanan Aplikasi Web Dari Serangan Sql Injection Dan Cross Site Scripting Menggunakan Web Application Firewall. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Issue 5).

Herdiana, Y., Munawar, Z., Putri, N. I., & Kunci, K. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT : Information Communication & Technology*, *21*(1), 42–52.

Hevner, A. R., & Brocke, J. (2023). A Proficiency Model for Design Science Research Education. *Print) Journal of Information Systems Education*, *34*(3), 264.

Khabibah, D. U., Nurrohman, Y., Dewandaru, K., Balian, S. J. D. H., & Setiawan, A. (2024). Strategi Mitigasi SQL Injection dengan Implementasi SQLMap dan Web Application Firewall. *Journal of Technology and System Information*, *1*(4), 12. https://doi.org/10.47134/jtsi.v1i4.2656

Madani, M. A., Syamsul, L. A., & Akbar, I. (2024). *Penetration Testing untuk Menguji Sistem Keamanan pada Website dengan Metode Black-Box ARTICLE INFO ABSTRACT* (Vol. 2, Issue 1).

Mahendra Ardiansyah, W. (2023). *Peran Teknologi dalam Transformasi Ekonomi dan Bisnis di Era Digital*. https://journal.sabajayapublisher.com/index.php/jmeb

Priyatna, B., Buana, U., & Karawang, P. (n.d.). *Penerapan Metode User Centered Design (Ucd) Pada Sistem Pemesanan Menu Kuliner Nusantara Berbasis Mobile Android*.

Rahmawati, E. (2020). Implementation of the user-centered design (Ucd) method for designing web marketplace of qurban cattle sales in Indonesia. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, *6*(2), 96–108. https://doi.org/10.26594/register.v6i2.1845