EVALUASI KINERJA KEAMANAN WORLD WIDE WEB DENGAN PENERAPAN WEB APPLICATION FIREWALL PADA DINAS KOMUNIKASI DAN INFORMATIKA BARITO TIMUR BERBASIS LINUX

TUGAS AKHIR

Disusun Oleh:

RESTU UNTUNG BERKATNI

NIM. 1910817310006

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS TEKNIK

UNIVERSITAS LAMBUNG MANGKURAT

BANJARMASIN, JUNI 2025

EVALUASI KINERJA KEAMANAN WORLD WIDE WEB DENGAN PENERAPAN WEB APPLICATION FIREWALL PADA DINAS KOMUNIKASI DAN INFORMATIKA BARITO TIMUR BERBASIS LINUX

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Sarjana Strata-1 Teknologi Informasi

Disusun Oleh:

RESTU UNTUNG BERKATNI

NIM. 1910817310006

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS TEKNIK

UNIVERSITAS LAMBUNG MANGKURAT

BANJARMASIN, JUNI 2025

LEMBAR PENGESAHAN

SKRIPSI PROGRAM STUIDI S-1 TEKNOLOGI INFORMASI

EVALUASI KINERJA KEAMANAN WORLD WIDE WEB DENGAN PENERAPAN WEB APPLICATION FIREWALL PADA DINAS KOMUNIKASI DAN INFORMATIKA BARITO TIMUR BERBASIS LINUX

OLEH

RESTU UNTUNG BERKATNI

Telah dipertahankan di depan Tim penguji pada 10 Juni 2025 dan dinyatakan

LULUS

Komite Penguji :

Ketua	**: Dr.Ir.Yuslena Sari, S.Kom., M.Kom** **NIP 198411202015042002**	.....
Anggota 1	**: Helda Yunita, S.Kom., M.Kom** **NIP 199106192024062001**	.....
Anggota 2	**: Irham Maulani Abdul Gani, S.Kom., M.Kom** **NIP 199710312025061009**	Irham .....
Pembimbing Utama	**: Eka Setya Wijaya, S.T., M.Kom** **NIP 198205082008011010**	.....
Pembimbing Pendamping	**: Andreyan Rizky Baskara, S.Kom., M.Kom** **NIP 199307032019031011**	.....

Banjarmasin, 10 JUL 2025

Diketahui dan disahkan oleh:

Wakil Dekan Bidang Akademik,
Fakultas Teknik ULM,

Dr. Mahmud, S.T., M.T.
NIP. 197401071998021001

Koordinator Program Studi
S-1 Teknologi Informasi,

Andreyan Rizky Baskara, S.Kom., M.Kom
NIP. 199307032019031011

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini,

Nama	: Restu Untung Berkatni
NIM	: 1910187310006
Fakultas	: Teknik
Program Studi	: Teknologi Informasi
Judul Tugas Akhir	: Evaluasi Kinerja Keamanan World Wide Web dengan Penerapan Web Application Firewall pada Dinas Komunikasi dan Informatika Barito Timur Berbasis Linux
Pembimbing Utama	: Eka Setya Wijaya, S.T., M.Kom.
Pembimbing Pendamping	: Andreyan Rizky Baskara, S.Kom., M.Kom.

Dengan ini saya menyatakan bahwa Tugas Akhir ini telah disusun ntuk memenuhi salah satu syarat memperoleh gelar akademik pada Program Studi Teknologi Informasi. Sepanjang pengetahuan saya, tidak terdapat karya atau pendapat orang lain yang saya gunakan tanpa mencantumkan sumber secara tertulis dalam naskah ini, baik yang berasal dari terbitan ilmiah, laporan, dan seluruh referensi telah dicantumkan dengan benar dalam daftar pustaka sesuai ketentuan penulisan ilmiah yang berlaku.

Banjarmasin, Juni 2025

Restu Untung Berkatni

NIM.1910817310006

LEMBAR PERSETUJUAN

EVALUASI KINERJA KEAMANAN WEB DENGAN PENERAPAN WAF PADA DISKOMINFO BARITO TIMUR BERBASIS LINUX

OLEH

RESTU UNTUNG BERKATNI

NIM. 1910817310006

Telah diperiksa dan terpenuhi semua persyaratan akademik, administrasi

Banjarmasin, 14 Mei 2025

Pembimbing Utama,

Eka Setya Wijaya, S.T., M.Kom.
NIP. 198205082008011010

EVALUASI KINERJA KEAMANAN WEB DENGAN PENERAPAN WAF PADA DISKOMINFO BARITO TIMUR BERBASIS LINUX

OLEH

RESTU UNTUNG BERKATNI

NIM. 1910817310006

Telah diperiksa dan terpenuhi semua persyaratan akademik, administrasi

Banjarmasin, 14 Mei 2025

Pembimbing Pendamping,

Andreyan Rizky Baskara, S.Kom., M.Kom.
NIP. 199307032019031011

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi kinerja keamanan Web Application *Firewall* (WAF) berbasis Linux yang diterapkan pada sistem web Diskominfo Kabupaten Barito Timur. Peningkatan serangan siber seperti SQL Injection dan Cross-Site Scripting (XSS) mendorong perlunya perlindungan sistem informasi yang lebih kuat di lingkungan pemerintahan. Evaluasi dilakukan dengan simulasi serangan menggunakan OWASP ZAP, SQLmap, dan XSStrike untuk menguji efektivitas WAF dalam mendeteksi dan memblokir ancaman. Hasil pemindaian awal menunjukkan sejumlah kerentanan yang signifikan, terutama pada pustaka JavaScript yang rentan dan konfigurasi header keamanan yang kurang optimal. Setelah perbaikan dan penguatan aturan WAF, dilakukan pemindaian ulang yang menunjukkan penurunan drastis jumlah kerentanan. Pengujian penetrasi juga membuktikan bahwa WAF berhasil mencegah serangan SQLi dan XSS secara efektif. Dengan demikian, penerapan WAF berbasis Linux terbukti mampu meningkatkan keamanan aplikasi web pemerintah dan memberikan perlindungan tambahan terhadap berbagai ancaman siber.

Kata kunci: *Cross-Site Scripting*, Keamanan Web, Linux, *SQL Injection*, *Web Application Firewall*

ABSTRACT

This study aims to evaluate the performance of a Linux-based Web Application Firewall (WAF) implemented on the web system of the Communication and Information Office of East Barito Regency. The rise of cyberattacks such as SQL Injection and Cross-Site Scripting (XSS) High lights the urgent need for stronger information system security in government environments. The evaluation was conducted through simulated attacks using OWASP ZAP, SQLmap, and XSStrike to assess the WAF's effectiveness in detecting and blocking threats. Initial scans revealed significant vulnerabilities, particularly outdated JavaScript libraries and suboptimal security header configurations. FolLowing the implementation of improved WAF rules and configurations, subsequent scans showed a substantial reduction in vulnerabilities. Penetration tests further confirmed that the WAF successfully blocked both SQLi and XSS attacks. Therefore, the implementation of a Linux-based WAF has proven effective in enhancing government web application security and provides additional protection against various cyber threats.

Keywords: Cross-Site Scripting, Linux, OWASP Zed Attack Proxy, SQL Injection, Web Application Firewall

HALAMAN PERSEMBAHAN

Penulis mempersembahkan Tugas Akhir kepada :

1. Ibu, Ayah, Kakak dan keluarga tercinta yang telah memberikan motivasi, dukungan moral dan materi, dan senantiasa mendoakan penulis akan keberlangsungan penyelesaiaan Tugas Akhir ini.
2. Ibu Dr. Ir. Yuslena Sari, S.Kom, M.kom., selaku Koordinator Program Studi Teknologi Informasi yang selalu menyempatkan waktunya untuk memberikan bimbingan dan arahan kepada kami mahasiswa teknologi informasi untuk segera menyelesaikan Tugas Akhir ini.
3. Bapak Eka Setya Wijaya, S.T., M.Kom., selaku Dosen Pembimbing Utama yang selalu menyempatkan waktu untuk memberikan bimbingan, arahan, dan dukungan kepada penulis dari awal sampai akhir penyelesaian.
4. Bapak Andreyan Rizky Baskara, S.Kom., M.Kom., selaku Dosen Pembimbing pendamping dan Dosen Pembimbing Akademik yang senantiasa memberikan bimbingan, arahan, dan dukungan kepada penulis untuk segera menyelesaikan Tugas Akhir ini.
5. Seluruh Dosen beserta Staf Program Studi Teknologi Informasi yang turut membantu dan mengarahkan dalam penyelesaian Laporan Tugas Akhir.
6. Seluruh mahasiswa Program Studi Teknologi Informasi yang telah membantu penulis dalam membentuk lingkungan perkuliahan yang memberi semangat bagi penulis dalam menyelesaikan Tugas Akhir ini.

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kepada Tuhan atas penyertaan, kasih karunia, dan hikmat yang telah diberikan selama proses penyusunan hingga terselesaikannya Tugas Akhir ini. Tanpa pertolongan dan penyertaan-Nya, penulis tidak akan mampu melewati seluruh proses, mulai dari perencanaan, pengumpulan data, analisis, hingga penulisan akhir. Tugas Akhir yang berjudul *"Evaluasi Kinerja Keamanan World Wide Web dengan Penerapan Web Application Firewall pada Dinas Komunikasi dan Informatika Barito Timur Berbasis Linux"* ini disusun sebagai salah satu syarat akademik untuk memperoleh gelar Sarjana Strata-1 pada Program Studi Teknologi Informasi di Fakultas Teknik Universitas Lambung Mangkurat, Banjarmasin.

Penulis menyadari bahwa dalam proses penyusunan Tugas Akhir ini terdapat berbagai tantangan dan hambatan, baik dari segi teknis, waktu, maupun mental. Namun, semua itu dapat dilalui berkat dukungan moral, spiritual, dan intelektual dari berbagai pihak yang telah dengan tulus membantu dan mendorong penulis untuk terus maju dan menyelesaikan karya ilmiah ini dengan sebaik mungkin. Oleh karena itu, dengan penuh rasa hormat, tulus, dan ucapan terima kasih yang mendalam, penulis ingin menyampaikan apresiasi setinggi-tingginya kepada:

1. Ibu, Ayah, Kakak dan keluarga tercinta yang telah memberikan motivasi, dukungan moral dan materi, dan senantiasa mendoakan penulis akan keberlangsungan penyelesaiaan Tugas Akhir ini.
2. Koordinator Program Studi Teknologi Informasi, Bapak Andreyan Rizky Baskara, S.Kom., M.Kom., yang telah memberikan saran dan Solusi dalam penyelesaian Tugas Akhir.
3. Bapak Eka Setya Wijaya, S.Kom., M.Kom., selaku Dosen Pembimbing Utama yang selalu menyempatkan waktu untuk memberikan bimbingan, arahan, dan dukungan kepada penulis dari awal sampai akhir penyelesaian.
4. Bapak Andreyan Rizky Baskara, S.Kom., M.Kom., selaku Dosen Pembimbing pendamping dan Dosen Pembimbing Akademik yang senantiasa memberikan

bimbingan, arahan, dan dukungan kepada penulis untuk segera menyelesaikan Tugas Akhir ini.

5. Seluruh Dosen beserta Staf Program Studi Teknologi Informasi yang turut membantu dan mengarahkan dalam penyelesaian Laporan Tugas Akhir.
6. Seluruh mahasiswa Program Studi Teknologi Informasi yang telah membantu penulis dalam membentuk lingkungan perkuliahan yang memberi semangat bagi penulis dalam menyelesaikan Tugas Akhir ini.

Penulis menyampaikan terimakasih juga kepada semua pihak yang turut membantu dalam penyelesaian laporan Tugas Akhir ini. Tugas Akhir ini telah disusun dengan optimal dan masihlah jauh dari kesempurnaan. Penulis menerima saran dan kritik yang membangun agar Tugas Akhir ini dapat memberikan banyak manfaat bagi semua orang.

Banjarmasin, Juni 2025

Penulis,

Restu Untung Berkanti

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR RIWAYAT HIDUP

Nama Lengkap : Restu Untung Berkatni

TTL : Jaar, 19 April 2001

Alamat : Jaar, Rt. 10 No. 117 Kec. Dusun Timur Kab. Barito Timur

Agama : Kristen

Kewarganegaraan : Indonesia

Anak Ke- : 2 dari 2 bersaudara

Riwayat Pendidikan : SDN 2 Jaar

SMPN 1 Tamiang Layang

SMAN 1 Tamiang Layang

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi (TIK) di Kabupaten Barito Timur telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan masyarakat. Namun, perkembangan teknologi informasi yang pesat juga meningkatkan risiko keamanan data. Terdapat beberapa contoh kasus peretasan, salah satunya adalah kejadian *cybercrime* yang terjadi pada PT Bank Syariah Indonesia (BSI) Tbk di tahun 2023, yang melibatkan peretasan data nasabah oleh kelompok hacker LockBit 3.0. Insiden tersebut mengakibatkan terganggunya layanan mobile banking dan ATM BSI selama satu minggu, serta terjadinya pencurian data pribadi dan finansial nasabah, termasuk nama, alamat, nomor kartu, dan riwayat transaksi mereka. Peretas mengklaim mencuri data sebesar 1,5 TB dan mengancam akan merilisnya jika tuntutan mereka tidak dipenuhi [1]. Kasus cybercrime yang semakin meningkat pada 2022 meliputi serangan terhadap aplikasi e-HAC dari Kementerian Kesehatan, situs media sosial seperti Instagram dan Facebook, serta layanan digital lain seperti Tokopedia dan IndiHome [2].

Insiden peretasan Pusat Data Nasional (PDN) pada 20 Juni 2024 menimbulkan dampak signifikan terhadap layanan publik, di mana pelaku berhasil mengunci data penting yang tersimpan di dalamnya dan menuntut tebusan sebagai syarat pemulihan akses. Insiden tersebut menimbulkan kekhawatiran publik mengenai keamanan data pribadi, mengingat Pusat Data Nasional (PDN) menyimpan berbagai informasi penting milik masyarakat Indonesia, seperti data KTP dan informasi layanan penerbangan. Beberapa layanan publik mengalami gangguan total atau parsial, termasuk layanan e-KTP, BPJS Kesehatan, sistem perpajakan, layanan keimigrasian, layanan pendidikan, serta layanan perbankan dan keuangan, yang menyebabkan kesulitan masyarakat dalam mengakses layanan-layanan tersebut. Layanan imigrasi lumpuh, menyebabkan penumpukan penumpang

di bandara, yang menunjukkan gangguan besar pada sistem perjalanan internasional. Proses investigasi oleh Badan Siber dan Sandi Negara (BSSN) menghadapi tantangan akibat data yang terenkripsi, sehingga memperlambat pemulihan, meningkatkan biaya operasional, dan memperbesar potensi kerugian finansial jika tebusan dibayarkan [3].

Diskominfo Barito Timur merupakan sebuah organisasi yang bertanggung jawab dalam mengelola informasi dan teknologi di wilayah Barito Timur. Dalam menjalankan tugasnya, Diskominfo Barito Timur harus memastikan bahwa sistem keamanan informasi yang digunakan dapat melindungi data dan informasi yang dimiliki dari penyalahgunaan Informasi Elektronik [4]. Sistem pengamanan merupakan sistem yang membatasi akses komputer atau melarang akses ke dalam komputer [5]. Sebuah pernyataan dari Diskominfo Barito Timur mengungkapkan bahwa masalah ketahanan keamanan web mereka menjadi perhatian yang serius, Keamanan situs web Diskominfo yang rapuh akibat jarang diperbaruinya, membuka celah bagi peretas untuk melancarkan serangan SQL injection, sehingga menampilkan situs judi online. Hal ini menggarisbawahi pentingnya evaluasi rutin dan pemeliharaan sistem keamanan untuk mencegah serangan siber. Kelemahan ini menunjukkan bahwa tanpa pembaruan dan penilaian yang konsisten, situs web pemerintah menjadi lebih rentan terhadap serangan, menekankan perlunya peningkatan berkelanjutan dalam protokol keamanan dan pemantauan aktif untuk melindungi data sensitif.

Berdasarkan wawancara dengan Ari Opu Pahandrian Migang, ST sebagai Kepala Bidang Persandian dan Statistik bahwa belum pernah ada penelitian terkait evaluasi sistem keamanan WAF yang dilakukan di Diskominfo Barito Timur. Kantor Kominfo Barito Timur telah mengambil langkah strategis dalam memperkuat keamanan web mereka dengan menerapkan Web Application Firewall (WAF) berbasis Linux. WAF menjadi solusi penting untuk melindungi aplikasi web dari berbagai serangan siber, seperti SQL injection, cross-site scripting (XSS), dan serangan DDoS. WAF bekerja dengan memantau, menyaring, dan mengendalikan

lalu lintas HTTP menuju dan dari aplikasi web, memberikan lapisan keamanan tambahan yang tidak dapat diatasi oleh *firewall* tradisional. Hal ini menjadi langkah krusial, mengingat Kominfo memiliki tanggung jawab untuk melindungi data pribadi seperti nama, NIP, jenis kelamin, agama dan lain-lain [6].

WAF Diskominfo Barito Timur telah dirancang dengan arsitektur yang melibatkan beberapa komponen seperti internet, gateway, WAF, cPanel, reverse *proxy*, dan *server* web untuk melindungi aplikasi web. OWASP ZAP dapat menjadi alat yang sangat berharga dalam meningkatkan efektivitas WAF ini. Dengan demikian, kombinasi OWASP ZAP dan *ModSecurity* dapat menciptakan lapisan pertahanan yang lebih kuat, memastikan bahwa WAF Diskominfo Barito Timur mampu memberikan perlindungan yang optimal terhadap berbagai jenis serangan siber [6].

Penelitian ini bertujuan untuk mengevaluasi kinerja keamanan web WAF berbasis Linux di Diskominfo Barito Timur sehingga diharapkan dapat memberikan gambaran mengenai kemampuan WAF dalam menangkal serangan siber dan meningkatkan keamanan aplikasi web pemerintah. Dengan demikian, tujuan dari penelitian ini dapat terpenuhi yaitu untuk mengevaluasi kinerja keamanan web WAF berbasis Linux di Diskominfo Barito Timur yang dimana Diskominfo bartim bertugas untuk melindungi semua sub-domain dan domain *diskominfo.baritotimurkab.go.id*.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas, maka rumusan masalah yang menjadi fokus penelitian ini sebagai berikut:

1. Konfigurasi apa sajakah yang dapat diterapkan pada aturan WAF Berbasis Linux agar efektif dalam menjaga gangguan sql injection dan XSS di Kantor Kominfo Barito Timur?
2. Faktor-faktor apa sajakah yang mempengaruhi kinerja dari web WAF Diskominfo Tamiang Layang?

1.3 Batasan Masalah

Dalam pengerjaan penelitian ini, batasan masalah yang perlu diperhatikan adalah sebagai berikut:

1. Evaluasi hanya akan berfokus pada sistem keamanan dengan penerapan web WAF di Diskominfo Tamiang Layang untuk menguji ketahanan terhadap XSS dan SQL injection
2. Pengujian dilakukan langsung pada *server* web *diskominfo.baritotimurkab.go.id* di Diskominfo Tamiang Layang menggunakan jaringan lokal

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Menganalisis konfigurasi pada aturan WAF Berbasis Linux agar efektif dalam menjaga gangguan sql injection dan XSS di Kantor Kominfo Barito Timur
2. Menganalisis faktor-faktor yang mempengaruhi kinerja dari web WAF Diskominfo Tamiang Layang

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Memberikan pemahaman mendalam tentang sistem keamanan informasi Diskominfo Tamiang Layang.
2. Membantu Diskominfo Tamiang Layang dalam memilih dan mengimplementasikan WAF yang tepat
3. Memberikan masukan kepada pemerintah dalam menyusun kebijakan keamanan

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terkait

Penelitian terkait memberikan landasan teori yang kuat dalam memahami efektivitas sistem keamanan berbasis Web Application *Firewall* (WAF), khususnya untuk menangkal ancaman siber pada aplikasi web. Penelitian ini mencakup evaluasi efektivitas WAF dalam mendeteksi kerentanan seperti SQL Injection dan XSS, menunjukkan bahwa pengaturan aturan khusus pada WAF dapat meningkatkan perlindungan sistem secara signifikan. Selain itu, studi lain menyoroti keunggulan integrasi teknologi seperti OWASP ZAP dalam mengidentifikasi dan mengatasi potensi kelemahan WAF. Temuan ini memberikan perspektif penting dalam upaya merancang dan mengevaluasi sistem keamanan yang andal berbasis Linux di lingkungan Diskominfo Barito Timur.

2.1.1 *Analytic Approach to Improve Security Features of Web Application using Freeware WAF*

Penelitian yang dilakuan oleh Akshay Jadhav mengkaji efektivitas *firewall* aplikasi web (WAF) dan pemindai aplikasi web sumber terbuka dalam mendeteksi dan mencegah berbagai jenis serangan terhadap aplikasi web. Penelitian menggunakan beberapa alat seperti OWASP ZAP, Nessus Essentials, dan Arachni untuk mengevaluasi kerentanan pada aplikasi web yang berbeda, dengan fokus utama pada sistem perbankan online yang rentan sebagai subjek uji utama [7].

Metode penelitian ini terdiri dari beberapa tahap yang dirancang untuk mengevaluasi efektivitas WAF dan pemindai aplikasi web. Tahapan metode tersebut meliputi pemilihan aplikasi web yang rentan seperti Global Online Banking System, Damn Vulnerable Web Application (DVWA), dan OWASP Mutillidae II untuk pengujian, pengujian manual pada aplikasi perbankan

menggunakan Burp Suite untuk memahami dan memverifikasi hasil pemindai otomatis serta menemukan parameter khusus untuk aturan baru, implementasi WAF daemon bayangan dengan proxy terbalik dan pemindai aplikasi web sumber terbuka untuk mendeteksi dan mencegah serangan pada setiap tahap pengaturan eksperimental, serta analisis hasil pemindaian dari berbagai pemindai pada setiap pengaturan eksperimental untuk menyimpulkan efektivitas WAF sumber terbuka dan pentingnya aturan khusus dalam mencegah serangan. Hasilnya menunjukkan bahwa penggunaan WAF dan *proxy* terbalik dengan aturan khusus secara signifikan meningkatkan keamanan aplikasi web [7].

2.1.2 *Methodology for Malware Analysis in Linux Environments*

Metodologi analisis malware untuk Linux mencakup tindakan awal, analisis biner, analisis statis, analisis dinamis, analisis memori, dan pengumpulan informasi. Setiap tahap melibatkan langkah-langkah khusus untuk mengumpulkan informasi tentang perilaku dan struktur malware. Metodologi ini menekankan perbedaan antara OS Windows dan Linux serta kebutuhan akan prosedur khusus untuk masing-masing. Tindakan awal melibatkan hashing file, mengambil snapshot sistem korban, dan memeriksa lalu lintas keluar. Analisis biner berfokus pada pengumpulan informasi dari file biner, seperti string teks dan format file. Analisis statis melibatkan membedah kode malware tanpa menjalankannya untuk memahami strukturnya. Analisis dinamis mencakup menjalankan malware dalam lingkungan aman dan meninjau perubahan yang terjadi pada sistem korban. Metodologi ini bertujuan untuk memberikan pendekatan sistematis terhadap analisis malware di Linux [8].

2.1.3 *Performance Evaluation of Penetration Testing Tools in Diverse Computer System Security Scenarios*

Penelitian ini bertujuan untuk mengevaluasi kinerja berbagai alat dan teknik yang digunakan dalam penilaian kerentanan, dengan fokus pada efikasi

alat uji penetrasi sistem komputer. Penelitian ini berupaya melakukan analisis mendalam terhadap berbagai alat dan teknik yang digunakan dalam penilaian kerentanan sistem komputer, dengan menekankan pada pentingnya pemilihan alat uji penetrasi yang efisien dalam mendeteksi kerentanan dan memberikan solusi mitigasi. Penelitian ini juga mengusulkan pendekatan analisis pasca-eksploitasi sebagai bagian integral dari proses evaluasi, untuk memberikan wawasan mendalam tentang dampak potensial dari serangan dan menawarkan rekomendasi strategi mitigasi yang efektif [9].

Metode yang digunakan dalam penelitian ini mencakup analisis statis dan manual, dengan teknik seperti *fingerprinting*, pemindaian kerentanan, fuzzing, pemindaian Nmap, dan penggunaan alat pencarian basis data bernama search-sploit. Penelitian ini memberikan analisis komprehensif tentang berbagai alat dan teknik yang digunakan dalam penilaian kerentanan dan pengujian penetrasi, serta menyoroti pentingnya penilaian kerentanan dalam mengamankan sistem komputer. Hasil penelitian menunjukkan bahwa alat dan teknik yang digunakan dapat membantu dalam mengidentifikasi dan mengurangi kerentanan dalam sistem komputer. Namun, penelitian ini juga mencatat bahwa ada beberapa keterbatasan yang membatasi penerapan hasil penelitian ini dalam berbagai skenario. Dengan demikian, di masa depan penelitian dapat difokuskan pada sistem yang lebih kompleks dengan langkah-langkah keamanan tambahan [9].

2.1.4 *Comparative Assessment of Static Analysis Tools for Software Vulnerability*

Penelitian ini bertujuan untuk mengevaluasi dan membandingkan tiga alat analisis statis untuk kerentanan perangkat lunak menggunakan perangkat lunak sumber terbuka yang ditulis dalam bahasa C. Tujuannya adalah untuk membantu pengembang perangkat lunak memilih alat yang sesuai untuk kebutuhan mereka dalam mengidentifikasi dan memperbaiki kerentanan perangkat lunak. Penelitian ini menggunakan tiga alat analisis statis, yaitu

ITS4, *Flawfinder*, dan RATS, yang diterapkan pada aplikasi PuTTY, Wireshark, dan Nmap [10].

Metode penelitian melibatkan pengujian ketiga alat analisis statis pada aplikasi yang dipilih, dengan fokus pada jenis kerentanan seperti buffer overf*Low*, format string, dan random number generation. Analisis data dilakukan dengan membandingkan jumlah dan jenis kerentanan yang ditemukan oleh setiap alat, serta mengevaluasi efektivitas masing-masing alat dalam mendeteksi kerentanan dan menangani hasil positif palsu. Hasil pengujian menunjukkan bahwa *Flawfinder* mendeteksi jumlah kerentanan terbanyak, sementara ITS4 dan RATS memiliki kekuatan dan kelemahan masing-masing dalam mendeteksi jenis kerentanan tertentu [10].

2.1.5 *Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall*

Penelitian terkait membahas tentang implementasi Web Application *Firewall* (WAF) menggunakan *ModSecurity* dan metode Reverse *Proxy* untuk meningkatkan keamanan aplikasi web. Penelitian ini fokus pada pengujian tiga jenis serangan siber: Cross-Site Scripting (XSS), SQL Injection, dan Unauthorized Vulnerability Web Scanning, baik pada kondisi aplikasi web yang dilindungi maupun yang tidak dilindungi oleh WAF tersebut. Hasil penelitian menunjukkan bahwa penerapan *ModSecurity* dan Reverse *Proxy* secara signifikan mampu mencegah serangan-serangan tersebut, yang menunjukkan peningkatan dalam keamanan aplikasi web yang diuji [11].

Metode penelitian ini melibatkan pengujian terhadap aplikasi web menggunakan dua kondisi: dengan dan tanpa penerapan *ModSecurity* dan Reverse *Proxy*. Variabel bebasnya adalah kondisi penerapan *ModSecurity* dan Reverse *Proxy*, sementara variabel terikatnya adalah tingkat keamanan aplikasi web setelah dilakukan pengujian serangan. Pengujian dilakukan dengan tiga jenis serangan yang berbeda, yaitu XSS, SQL Injection, dan Unauthorized Vulnerability Web Scanning. Analisis dilakukan dengan membandingkan hasil

serangan pada kedua kondisi untuk menilai efektivitas implementasi WAF dalam meningkatkan keamanan aplikasi web [11].

2.1.6 *Penerapan Sistem Keamanan Website Menggunakan Web Application Firewall Dengan Framework Open Web Application Security Project*

Penelitian ini berfokus pada penggunaan Web Application *Firewall* (WAF) untuk meningkatkan keamanan aplikasi web, dengan menyaring, memantau, dan memblokir lalu lintas HTTP untuk mencegah serangan seperti injeksi SQL, cross site scripting (XSS), dan lainnya. Framework OWASP digunakan sebagai panduan utama dalam konfigurasi WAF serta identifikasi kerentanan aplikasi web. Penelitian ini menggunakan metode eksperimen dengan mengimplementasikan WAF sebagai sistem proteksi berbasis web melalui empat tahapan utama. observasi pada web *server* Boom Store, penggunaan alat dan bahan seperti *modsecurity* untuk *server* Apache atau NAXSI untuk *server* Nginx, implementasi dan uji penetrasi dengan perangkat lunak seperti Burp Suite dan OWASP ZAP, serta analisis dan uji coba hasil pengujian penetrasi untuk memberikan saran perbaikan pada sistem keamanan web [12].

Hasil penelitian menunjukkan bahwa *ModSecurity* sebagai WAF efektif dalam mencegah serangan umum dan meningkatkan keamanan aplikasi web. Uji penetrasi menggunakan OWASP ZAP mengonfirmasi bahwa WAF berhasil melindungi web dari serangan seperti Cross Site Scripting (XSS) dan memperbaiki masalah seperti Application Error Disclosure dan Directory Browsing. Observasi dan implementasi yang dilakukan memastikan bahwa WAF dapat diterapkan dengan baik pada *server* aplikasi web, dan analisis hasil pengujian menunjukkan peningkatan signifikan dalam keamanan aplikasi web setelah penerapan WAF sesuai dengan panduan Framework OWASP [12].

Berikut adalah tabel ringkasan penelitian terkait yang diurutkan dalam Tabel 2.1.

Tabel 2. 1 Ringkasan Penelitian

No	Judul	Penulis (Tahun)	Masalah	Hasil	Keterkaitan penelitian
1	Analytic Approach to Improve *Security* Features of Web Application using Freeware WAF	Akshay Jadhav (2023)	tingginya jumlah kerentanan dalam aplikasi yang tidak memiliki mekanisme keamanan, seperti injeksi SQL, serangan XSS (cross-site scripting), serangan brute force terhadap kata sandi, injeksi HTML, dan serangan pengelabuan klik (clickjacking).	penggunaan aturan default pada WAF tidak cukup untuk mencegah sebagian besar serangan. Meskipun demikian, aturan khusus WAF terbukti efektif dalam mengurangi jumlah kerentanan kritis, termasuk transmisi kata sandi dalam teks biasa dan kebijakan kata sandi yang lemah.	Keamanan web Berbasis Linux, Peningkatan Perlindungan Terhadap Ancaman Malware, Relevansi dengan IoT Malware, Penyempurnaan Metode Evaluasi Kinerja WAF
2	Methodology for Malware	Juan Antonio Sicilia	Keterbatasan alat uji penetrasi dalam mendeteksi dan	Metodologi analisis malware Linux efektif mengidentifikasi dan	Penelitian ini mengevaluasi WAF berbasis Linux untuk

No	Judul	Penulis (Tahun)	Masalah	Hasil	Keterkaitan penelitian
	Analysis in Linux Environments	Montalvo (2020)	mengurangi kerentanan sistem, serta masalah ketidakakuratan hasil.	memahami perilaku Linux.Encoder.1. Studi kasus menyoroti kekuatan serta keterbatasan analisis statis dan dinamis.	melindungi aplikasi web, dengan menganalisis WAF untuk mengidentifikasi pola serangan dan menguji efektivitas keamanan
3	Performance Evaluation of Penetration Testing Tools in Diverse Computer System *Security* Scenarios	Joseph Teguh Santoso, Budi Raharjo (2022)	evaluasi alat uji penetrasi komputer mengenai keterbatasan deteksi dan keakuratan hasil.	alat uji penetrasi terbukti efektif dalam mendeteksi kerentanan dan memberikan rekomendasi mitigasi yang efektif	identifikasi dan mitigasi kerentanan dalam sistem keamanan
4	Comparative Assessment of	Peter Miele, Mohammed	membandingkan alat analisis statis untuk	*Flawfinder* unggul dalam mendeteksi	Evaluasi keamanan web

No	Judul	Penulis (Tahun)	Masalah	Hasil	Keterkaitan penelitian
	Static Analysis Tools for Software Vulnerability	Alquwaisem, Dae-Kyoo Kim (2018)	mengidentifikasi kerentanan perangkat lunak C open source, fokus pada efektivitas dan penanganan hasil palsu.	kerentanan di aplikasi PuTTY, Wireshark, dan Nmap dibandingkan ITS4 dan RATS.	
5	Improving *Security* of Web-Based Application Using *ModSecurity* and Reverse Proxy in Web Application *Firewall*	Rizki Agung Muzaki, Obrina Candra Briliyant, Maulana Andika Hasditama, Hamzah Ritchi (2020)	Efektivitas WAF *ModSecurity* & Reverse Proxy dalam menanggulangi XSS, gangguan SQL Injection, dan serangan web tanpa izin.	Penerapan WAF menggunakan *ModSecurity* & Reverse Proxy signifikan meningkatkan keamanan aplikasi web dengan mencegah XSS, SQL Injection, & serangan web scanning.	Evaluasi efektivitas WAF
6	Penerapan Sistem Keamanan	Muhammad Dandi Permana,	keamanan aplikasi web yang rentan terhadap serangan	Hasil penelitian menunjukkan bahwa penggunaan	Metode eksperimen WAF berbasis Linux

No	Judul	Penulis (Tahun)	Masalah	Hasil	Keterkaitan penelitian
	Website Menggunakan Web Application *Firewall* Dengan Framework Open Web Application *Security* Project	Syahril Rizal, Suryayusra, Febriyanti Panjaitan (2023)	dari pihak yang tidak bertanggung jawab selama pandemi Covid-19	*ModSecurity* sebagai Web Application *Firewall* (WAF) efektif dalam meningkatkan keamanan aplikasi web juga Pengujian penetrasi menggunakan OWASP ZAP mengonfirmasi bahwa serangan tersebut berhasil dicegah setelah implementasi WAF	

2.2 Dasar Teori

2.2.1 *Keamanan Web*

Keamanan Keamanan web merupakan serangkaian langkah yang diterapkan untuk melindungi aplikasi web dari serangan eksternal seperti SQL Injection, Cross Site Scripting (XSS), dan lain-lain. Salah satu metode yang efektif dalam menjaga keamanan web adalah penggunaan Web Application *Firewall* (WAF), seperti *ModSecurity*, yang berfungsi memonitor, menyaring, dan memblokir lalu lintas berbahaya berdasarkan aturan yang telah ditetapkan. WAF dapat mencegah akses yang tidak sah dengan menghentikan permintaan yang mencurigakan, memberikan lapisan perlindungan tambahan terhadap berbagai ancaman keamanan web [13] [14].

Manajemen risiko keamanan informasi sendiri merupakan suatu proses mengidentifikasi, mengevaluasi, dan mengendalikan risiko keamanan informasi. Risiko keamanan informasi adalah potensi kerugian yang dapat terjadi akibat pelanggaran keamanan informasi. Manajemen risiko keamanan informasi penting untuk dilakukan agar organisasi dapat melindungi data dan informasinya dari ancaman dan serangan [15].

Organisasi perlu mengadopsi pendekatan holistik dalam manajemen risiko keamanan informasi, termasuk penerapan kebijakan keamanan, pelatihan karyawan, dan penggunaan teknologi canggih untuk deteksi dan respons terhadap ancaman. Selain itu, pemantauan berkelanjutan dan penilaian rutin terhadap sistem keamanan sangat penting untuk menyesuaikan strategi dengan ancaman baru yang muncul. Dengan langkah-langkah yang komprehensif ini, organisasi dapat membangun sistem keamanan informasi yang kuat dan beradaptasi dengan perubahan lanskap ancaman siber [16].

Salah satu langkah kunci dalam memastikan keamanan web adalah menerapkan kebijakan keamanan yang jelas dan tegas. Kebijakan ini harus mencakup berbagai aspek, seperti protokol enkripsi data, autentikasi pengguna yang kuat, dan pengawasan aktivitas yang mencurigakan. Tanpa kebijakan yang

efektif, perusahaan berisiko mengalami kebocoran data, serangan malware, dan ancaman keamanan lainnya. Kesadaran akan pentingnya kebijakan ini juga harus diinternalisasi oleh seluruh elemen perusahaan [16].

Selain kebijakan yang kuat, pelatihan bagi karyawan menjadi komponen penting dalam manajemen keamanan web. Karyawan harus dibekali dengan pengetahuan yang cukup mengenai praktik keamanan yang baik, seperti mengenali email phishing, menggunakan kata sandi yang kuat, dan menjaga privasi informasi sensitif. Pelatihan ini penting karena serangan siber sering kali berhasil akibat kesalahan manusia, seperti menggunakan perangkat yang tidak aman atau mengabaikan protokol keamanan yang telah ditetapkan [16].

Pemanfaatan teknologi canggih untuk deteksi dini dan respons terhadap ancaman menjadi keharusan dalam menjaga keamanan sistem informasi. Teknologi seperti *firewall* dan fitur *ModSecurity* pada Nginx memainkan peran penting, di mana *ModSecurity* berfungsi sebagai penjaga gerbang antara Nginx web *server* dan lalu lintas jaringan. Selain itu, pemantauan berkelanjutan terhadap sistem keamanan sangat penting agar organisasi dapat merespons ancaman baru yang muncul dengan cepat dan efektif. Pemantauan ini perlu dilakukan secara real-time untuk mengidentifikasi aktivitas mencurigakan dan segera mengambil tindakan pencegahan guna meminimalkan risiko yang mungkin terjadi. Dengan langkah-langkah ini, organisasi dapat meningkatkan ketahanan terhadap ancaman keamanan yang semakin kompleks [16].

Manajemen risiko yang efektif dalam keamanan web juga memerlukan kolaborasi antara departemen teknologi informasi dan tim manajemen. Keputusan mengenai alokasi anggaran untuk keamanan, pembelian teknologi baru, atau pelatihan karyawan harus melibatkan berbagai pemangku kepentingan. Kolaborasi ini memastikan bahwa setiap keputusan yang diambil mendukung upaya organisasi dalam menciptakan ekosistem keamanan yang solid [16].

Dengan adopsi langkah-langkah ini, organisasi dapat membangun sistem keamanan informasi yang lebih adaptif dan tangguh terhadap ancaman yang terus

berubah. Meskipun ancaman siber semakin kompleks, penerapan kebijakan yang kuat, pelatihan karyawan, serta pemanfaatan teknologi akan memberikan perlindungan yang memadai bagi keamanan web organisasi [16].

2.2.2 *Linux*

Linux merupakan sistem operasi yang bisa bekerja sendiri sebagai standalone PC, atau pun sebagai workstation yang bisa bekerja sama dalam jaringan [17]. Sistem Operasi merupakan program utama yang menghubungkan Software Aplikasi yang digunakan oleh user dengan hardware. Pengertian sistem operasi secara umum ialah pengelola seluruh sumber-daya yang terdapat pada sistem komputer dan menyediakan sekumpulan layanan (system calls) yang sering disebut “tools atau utility” berupa aplikasi ke pemakai sehingga memudahkan dan menyamankan penggunaan ketika memanfaatan sumber-daya sistem komputer tersebut [18].

Salah satu kekuatan utama Linux adalah keberagaman distribusinya. Ada banyak "distro" Linux, seperti Ubuntu, Fedora, Debian, dan banyak lainnya, yang masing-masing menawarkan fitur dan kegunaan yang berbeda untuk berbagai jenis pengguna dan kebutuhan. Distribusi ini mencakup berbagai alat dan aplikasi yang memungkinkan pengguna untuk menyesuaikan dan mengoptimalkan sistem mereka sesuai kebutuhan spesifik mereka [19].

Selain itu, Linux dikenal dengan stabilitas dan keamanannya, menjadikannya pilihan populer untuk *server*, superkomputer, dan perangkat embedded, serta desktop dan laptop pribadi. Fleksibilitas dan efisiensinya juga membuat Linux sangat cocok untuk berbagai lingkungan komputasi, dari perangkat kecil hingga sistem berskala besar [19].

Sistem operasi Linux menggunakan sistem file berbasis hierarki. Setiap file dan direktori di Linux dapat diakses melalui root directory yang dilambangkan dengan "/". Semua file penting, termasuk konfigurasi sistem dan perangkat lunak, tersimpan di direktori ini atau subdirektorinya. Setiap file dan folder diidentifikasi berdasarkan nama yang peka terhadap huruf besar dan kecil,

yang menjadikannya berbeda dari beberapa sistem operasi lain seperti Windows [19].

Selain itu, Linux terkenal karena fleksibilitas dan portabilitasnya. Kernel Linux ditulis dalam bahasa pemrograman C, yang memungkinkan untuk porting atau diterjemahkan ke berbagai jenis perangkat keras. Hal ini membuat Linux dapat berjalan di banyak platform, mulai dari komputer pribadi hingga perangkat mobile atau sistem embedded. Bahkan, Linux juga dapat digunakan pada superkomputer hingga perangkat kecil seperti router dan sistem rumah pintar [19].

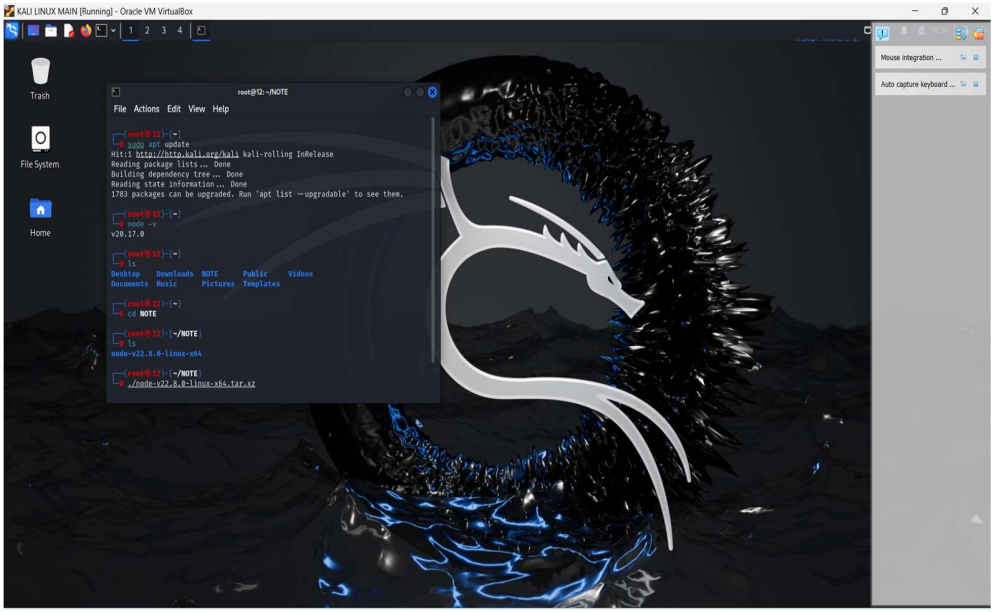
Keamanan merupakan salah satu aspek penting dari Linux. Dengan menggunakan model izin berbasis pengguna dan grup, Linux memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses file atau menjalankan proses tertentu. File sistem Linux juga mendukung jurnal, yang berarti setiap perubahan pada sistem file dicatat sebelum diterapkan, sehingga sistem dapat pulih dengan cepat dari kegagalan sistem atau shutdown yang tidak terduga [19].

Linux juga menawarkan model open-source, di mana kode sumber sistem operasi tersedia bagi siapa saja untuk dipelajari, dimodifikasi, dan didistribusikan ulang. Ini mendorong inovasi dan kolaborasi komunitas global, dengan pengembang dari berbagai latar belakang yang berkontribusi dalam pengembangan dan pemeliharaan Linux. Sistem lisensi GNU General Public License (GPL) menjamin bahwa perubahan atau perbaikan yang dilakukan pada Linux tetap dapat diakses secara bebas oleh publik [19].

Kesederhanaan arsitektur Linux menjadikannya salah satu sistem operasi yang sangat stabil dan efisien. Sistem operasi ini dapat berjalan dengan baik bahkan pada perangkat keras lama yang memiliki sumber daya terbatas. Dengan desain modular, pengguna dapat mengkonfigurasi sistem hanya dengan memuat komponen yang dibutuhkan, sehingga meningkatkan efisiensi penggunaan memori dan CPU [19].

Linux memiliki versi lain yang digunakan untuk menguji dan mengeksploitasi kelemahan WAF yaitu Kali Linux, Kali Linux sendiri

merupakan distribusi Linux berbasis Debian yang dirancang khusus untuk keamanan informasi dan uji penetrasi. Dikembangkan oleh *Offensive Security*, Kali Linux dilengkapi dengan berbagai alat keamanan, termasuk Nmap, Metasploit, dan Wireshark, yang berguna untuk menganalisis, menguji, dan mengeksploitasi celah keamanan di sistem jaringan. Distribusi ini banyak digunakan oleh profesional keamanan siber untuk mengevaluasi keamanan jaringan dan mendeteksi kelemahan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab [20]. Berikut Homepage kali linux dapat dilihat pada gambar 2. 1.



Gambar 2. 1 Homepage Kali Linux

Kali Linux menekankan pada etika hacking atau "ethical hacking," yang berarti penggunaannya dilakukan dengan tujuan legal, seperti mengidentifikasi kelemahan keamanan untuk memperbaikinya, bukan untuk mengeksploitasi. Dengan antarmuka yang ramah pengguna, Kali Linux juga menawarkan fleksibilitas untuk dioperasikan di berbagai platform, mulai dari desktop hingga perangkat mobile. Pengguna dapat mengkonfigurasi sistemnya dengan mudah untuk menyesuaikan dengan kebutuhan pengujian mereka [20].