IMPLEMENTASI WEB APPLICATION FIREWALL BERBASIS CORAZA PADA INFRASTRUKTUR SERVER WEB

TUGAS AKHIR

Untuk Memenuhi sebagai persyaratan Mencapai derajat Sarjana
S-1 Program Studi Informatika

Disusun Oleh:
Muhammad Alkautsar Fathur Rohim

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

PROGRAM STUDI INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA
2026

LEMBAR PENGESAHAN TUGAS AKHIR

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1218/Un.02/DST/PP.00.9/06/2026

Tugas Akhir dengan judul : Implementasi Web Application Firewall Berbasis Coraza Pada Infrastruktur Server Web

yang dipersiapkan dan disusun oleh:

Nama : MUHAMMAD ALKAUTSAR FATHUR ROHIM
Nomor Induk Mahasiswa : 22106050022
Telah diujikan pada : Kamis, 04 Juni 2026
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D.
SIGNED

Valid ID: 6a22706146b8e

Penguji I

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 6a22462f18aa1

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 6a226d647b569

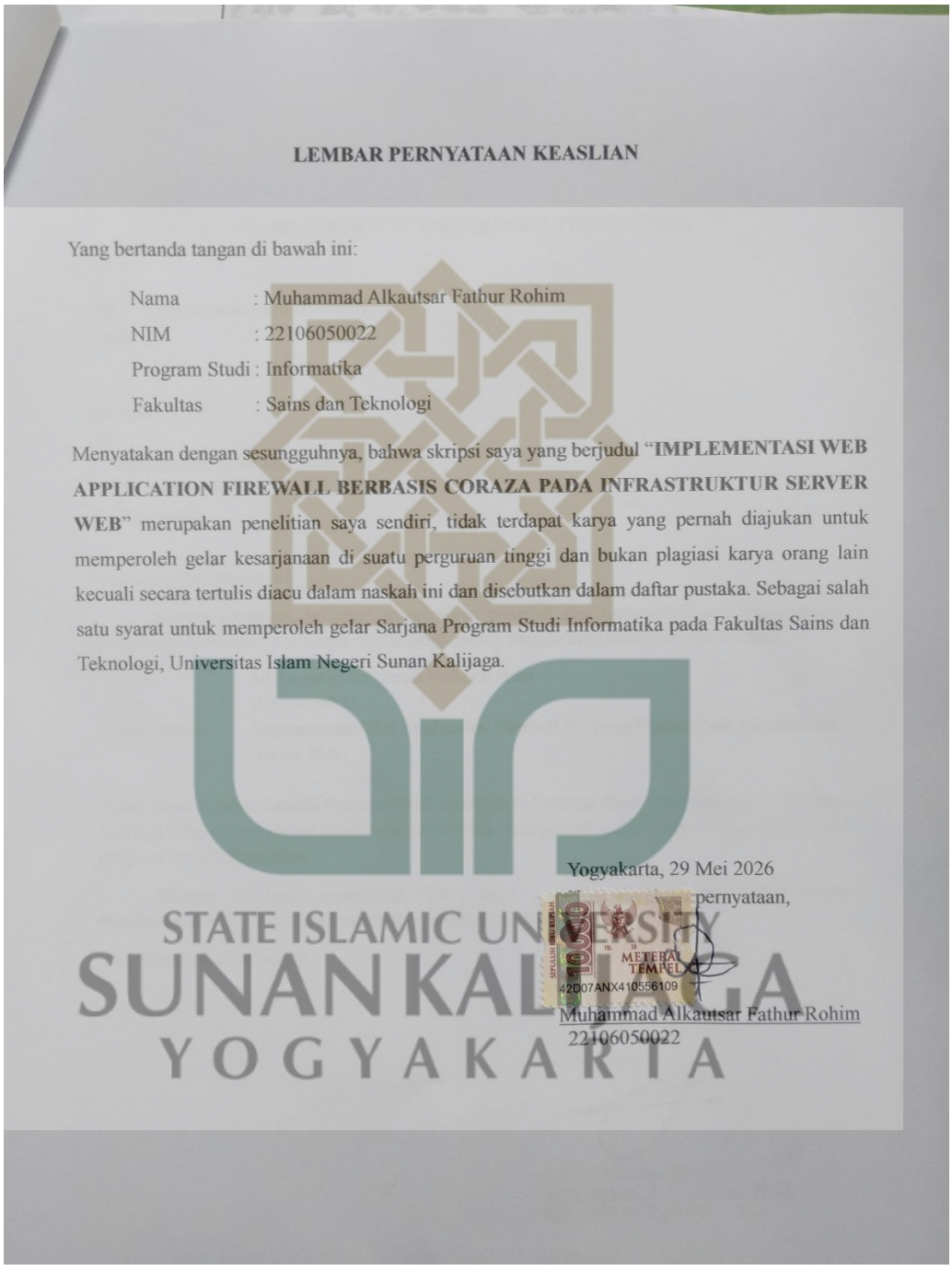
Yogyakarta, 04 Juni 2026
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6a227e6b3e529

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

LEMBAR PERNYATAAN TUGAS AKHIR



LEMBAR PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Muhammad Alkautsar Fathur Rohim
NIM : 22106050022
Program Studi : Informatika
Fakultas : Sains dan Teknologi

Menyatakan dengan sesungguhnya, bahwa skripsi saya yang berjudul "**IMPLEMENTASI WEB APPLICATION FIREWALL BERBASIS CORAZA PADA INFRASTRUKTUR SERVER WEB**" merupakan penelitian saya sendiri, tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi dan bukan plagiasi karya orang lain kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka. Sebagai salah satu syarat untuk memperoleh gelar Sarjana Program Studi Informatika pada Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga.

Yogyakarta, 29 Mei 2026
pernyataan,

Muhammad Alkautsar Fathur Rohim
22106050022

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

LEMBAR PERSETUJUAN TUGAS AKHIR

LEMBAR PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp : -

Kepada
Yth.
Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga
DI Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	:	Muhammad Alkautsar Fathur Rohim
NIM	:	22106050022
Judul Skripsi	:	Implementasi Web Application Firewall Berbasis Coraza Pada Infrastruktur Server Web

Sudah dapat diajukan kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Dengan ini kami mengharap agar skripsi / tugas akhir Saudara dapat segera dimunaqosyahkan. Atas perhatiannya saya ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 29 Mei 2026
Pembimbing,

Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D.
NIP. 19791118 200501 1 003

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

INTISARI

Institusi pendidikan tinggi saat ini menghadapi ancaman siber Layer 7 yang rentan, seperti SQL Injection (SQLi) dan Cross-Site Scripting (XSS). Mahalnya lisensi WAF komersial mendorong kebutuhan akan solusi open-source yang andal. Penelitian ini mengimplementasikan Coraza Web Application Firewall (WAF) dan ELK Stack (Elasticsearch, Logstash, Kibana) pada peladen UIN Sunan Kalijaga menggunakan metode Network Development Life Cycle (NDLC). Infrastruktur sistem ini dibangun di atas lingkungan Docker dengan Caddy Server yang berperan sebagai reverse proxy.

Hasil pengujian menggunakan OWASP ZAP menunjukkan bahwa Coraza WAF dalam mode blokir secara efektif memutus trafik serangan SQLi dan XSS sebelum mencapai peladen backend. Di sisi lain, integrasi ELK Stack terbukti mempermudah analisis forensik digital melalui pemantauan dasbor log yang komprehensif secara real-time. Kendala operasional pada akses pengguna sah akibat keamanan yang ketat (False Positive dan masalah Mixed Content) juga berhasil diatasi melalui penyesuaian aturan (Rule Tuning) dan penerapan Content Security Policy. Sistem ini berhasil membuktikan keseimbangan yang optimal antara keamanan infrastruktur dan ketersediaan layanan.

Kata Kunci: *Web Application Firewall, Coraza, ELK Stack, Keamanan Siber, SQL Injection, Cross-Site Scripting.*

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

ABSTRACT

Higher education institutions currently face vulnerable Layer 7 cyber threats, such as SQL Injection (SQLi) and Cross-Site Scripting (XSS). The high cost of commercial WAF licenses drives the need for a reliable open-source solution. This research implements the Coraza Web Application Firewall (WAF) and ELK Stack (Elasticsearch, Logstash, Kibana) on UIN Sunan Kalijaga's servers using the Network Development Life Cycle (NDLC) framework. The system infrastructure is built within a Docker environment with Caddy Server acting as a reverse proxy.

Penetration testing using OWASP ZAP demonstrates that Coraza WAF in enforcement mode effectively intercepts SQLi and XSS attack traffic before it reaches the backend servers. Furthermore, the ELK Stack integration is proven to streamline digital forensic analysis through comprehensive real-time log dashboard monitoring. Operational issues affecting legitimate user access due to strict security (False Positives and Mixed Content issues) were successfully resolved through Rule Tuning and the application of Content Security Policy. This system successfully achieves an optimal balance between infrastructure security and service availability.

Keywords: *Web Application Firewall*, *Coraza*, *ELK Stack*, *Cybersecurity*, *SQL Injection*, *Cross-Site Scripting*.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

HALAMAN PERSEMBAHAN

Dengan rasa syukur yang mendalam kepada Allah SWT atas segala rahmat, hidayah, dan kekuatan yang telah diberikan selama proses penyelesaian tugas akhir ini, penulis mempersembahkan tugas akhir ini untuk:

1. Kedua orang tua saya Bapak Kasiadi dan Ibu Eva Indaryuni atas cinta, doa, dukungan, serta pengorbanan tanpa batas yang selalu menjadi semangat dan motivasi terbesar dalam setiap langkah hidup saya.
2. Kakak saya Inka Ani Ainul Fitri dan Henrico Suantoro yang senantiasa memberikan dorongan, semangat, dan kasih sayang.
3. Kakak bimbing saya Fajrul Ali Fikri Misbah, M. Bahrul Ulum dan Maftuh Al Fikri Rosyadi yang senantiasa sabar dalam membimbing saya.
4. Dosen pembimbing saya Bapak Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D. yang telah dengan sabar memberikan bimbingan, ilmu, serta motivasi selama proses penyusunan tugas akhir ini.
5. Seluruh bapak dan ibu dosen Informatika yang telah memberikan saya ilmu perkuliahan selama saya menuntut ilmu di UIN Sunan Kalijaga Yogyakarta.
6. Teman-teman seperjuangan saya khususnya seluruh mahasiswa program studi Informatika Angkatan 2022 yang selalu mendukung, menginspirasi, dan menemani dalam suka maupun duka sepanjang perjalanan akademik ini.
7. Kepada diri saya yang diri saya yang selalu bersyukur, selalu bekerja keras, pantang menyerah dan memberikan yang terbaik sampai saat ini. Terima kasih

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala rahmat, karunia, dan hidayah-Nya, sehingga penulis dapat menyelesaikan Laporan Tugas Akhir ini yang berjudul " Implementasi Web Application Firewall Berbasis Coraza Pada Infrastruktur Server Situs Web". Laporan ini disusun sebagai salah satu syarat untuk menyelesaikan program S1 di Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Penulis menyadari bahwa laporan ini tidak akan terselesaikan tanpa bantuan, dukungan, dan bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada:

1. Allah SWT yang selalu memberikan kelancaran kepada penulis untuk menyelesaikan penulisan tugas akhir ini.
2. Bapak Kasiadi dan Ibu Eva Indaryuni, selaku kedua orang tua saya yang selalu memberikan doa dan dukungan.
3. Bapak Prof. Noorhaidi, M.A., M.Phil., Ph.D., selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
4. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi.
5. Bapak Dr. Muhammad Mustakim, S.T., M.T., selaku Ketua Program Studi Informatika.
7. Bapak Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D. selaku Dosen Pembimbing Tugas Akhir yang selalu membantu dan memberikan arahan dalam menyelesaikan penulisan tugas akhir ini.
8. Bapak dan Ibu Dosen Program Studi Informatika yang telah memberikan dan mengajarkan ilmu perkuliahan yang bermanfaat

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

MOTTO

وَاِذْ تَاَذَّنَ رَبُّكُمْ لَىِٕنْ شَكَرْتُمْ لَاَزِيْدَنَّكُمْ وَلَىِٕنْ كَفَرْتُمْ اِنَّ عَذَابِيْ لَشَدِيْدٌ ۝٧

“ **(**Ingatlah) ketika Tuhanmu memaklumkan, Sesungguhnya jika kamu bersyukur, niscaya Aku akan menambah (nikmat) kepadamu, tetapi jika kamu mengingkari (nikmat-Ku), sesungguhnya azab-Ku benar-benar sangat keras.”

(QS. Ibrahim Ayat 7)

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR ISI

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR GAMBAR

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR TABEL

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

BAB I
PENDAHULUAN

1.1. Latar Belakang

Kebutuhan terhadap layanan berbasis web kini menjadi prioritas utama bagi institusi pendidikan tinggi, termasuk di lingkungan Universitas Islam Negeri (UIN) Sunan Kalijaga Yogyakarta. Digitalisasi ini memang mempercepat alur akademik dan administratif. Akan tetapi, ketergantungan yang makin besar terhadap sistem ini justru membuka celah keamanan baru. Berdasarkan temuan Badan Siber dan Sandi Negara (BSSN) dalam Laporan Lanskap Keamanan Siber Indonesia 2024, tercatat lonjakan anomali lalu lintas data yang melampaui angka 330 juta kasus. Dari keseluruhan insiden tersebut, eksploitasi pada kelemahan aplikasi web tercatat sebagai salah satu ancaman yang perlu diwaspadai pada sektor pendidikan dan pemerintahan [1].

Ancaman siber kini menunjukkan pergeseran taktik menuju lapisan aplikasi (*Application Layer / Layer 7*). Hasil pemetaan OWASP Top 10 menunjukkan bahwa kelemahan aplikasi web seperti kegagalan kontrol akses, kegagalan kriptografi, *injection*, dan kelemahan konfigurasi masih menjadi risiko utama pada aplikasi web modern [2]. Titik rentan inilah yang kemudian dijadikan pintu masuk awal oleh peretas untuk melakukan berbagai serangan. Berbekal akses ilegal dari pencurian data kredensial via SQLi atau pembajakan sesi administrator melalui XSS, peretas dapat mengambil alih kendali sistem secara penuh. Rantai eksploitasi tersebut berimplikasi langsung pada insiden yang marak terjadi belakangan ini. Sering kali ditemui kasus peretasan pada situs web lembaga resmi (berdomain go.id atau ac.id) yang secara sepihak dialihkan menjadi halaman promosi judi online. Modifikasi antarmuka secara paksa (*web defacement*) serta penanaman akses tersembunyi (*backdoor injection*) semacam itu tidak hanya merusak integritas arsitektur sistem, melainkan turut menghancurkan kredibilitas institusi.

Meninjau kondisi di lapangan, Upaya perlindungan lapisan aplikasi di PTIPD UIN Sunan Kalijaga saat ini bertumpu pada satu solusi, yakni WAF

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

komersial *F5 Networks*. Perangkat berbayar ini memang terbukti tangguh di lapangan. Mekanisme filternya sanggup mencegat berbagai injeksi kode berbahaya, seperti SQLi dan XSS, secara akurat. Namun persoalan yang sebenarnya baru muncul ketika menyinggung urusan lisensi. Skema lisensi berlangganan yang diterapkan pihak vendor memaksa institusi untuk terus menyediakan dana perpanjangan secara rutin. Jika alokasi dana ini tersendat, konsekuensi teknisnya sangat fatal. Sinkronisasi basis aturan keamanan (*rule set*) akan langsung terputus. Tanpa adanya pembaruan tersebut, peladen otomatis kehilangan tameng utamanya sehingga rentan menjadi sasaran eksploitasi siber varian baru. Memecahkan kebuntuan antara kebutuhan pengamanan dan keterbatasan lisensi ini jelas menuntut adanya perombakan infrastruktur. PTIPD memerlukan rancangan arsitektur WAF alternatif yang sepenuhnya digerakkan oleh sistem sumber terbuka. Keputusan beralih ke jalur sumber terbuka ini didorong oleh target yang spesifik. Selain mencari mesin inspeksi paket yang ketajamannya mampu menyamai layanan komersial, langkah ini akan membebaskan kampus dari ketergantungan vendor sekaligus mengembalikan kontrol pengelolaan keamanan ke tangan institusi itu sendiri.

Implementasi Web Application Firewall seperti ModSecurity memang sudah lama memegang peranan krusial sebagai standar mitigasi utama dalam mengamankan perimeter jaringan. Penelitian terdahulu menunjukkan bahwa ModSecurity berbasis WAF mampu memblokir serangan seperti SQL Injection, Cross-Site Scripting, dan Command Execution [3]. Berangkat dari kebutuhan terhadap engine WAF yang lebih adaptif, Coraza WAF diusulkan dalam penelitian ini sebagai alternatif solusi berbasis sumber terbuka. Coraza dikembangkan menggunakan bahasa Go dan kompatibel dengan aturan OWASP CRS serta mampu meningkatkan pemrosesan inspeksi sekitar 700 hingga 70.000 events per-detik pada scenario benchmark tertentu [4]. Dengan karakteristik tersebut, Coraza menjadi opsi yang relevan untuk diimplementasikan pada lingkungan infrastruktur yang memiliki kepadatan lalu lintas data tinggi.

Keberadaan WAF memang krusial untuk menahan laju serangan, namun postur keamanan jaringan belumlah sempurna tanpa didukung oleh komponen

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

visibilitas data. Sejumlah penelitian terdahulu telah membuktikan tingginya tingkat keberhasilan WAF dalam mereduksi eksploitasi celah web. Kendati demikian, mayoritas studi tersebut mengabaikan aspek pemantauan jaringan yang berkesinambungan [5]. Parameter keberhasilan sering kali hanya dievaluasi secara statis bersandar pada hasil akhir pemindaian menggunakan perangkat lunak pihak ketiga, seperti OWASP ZAP. Keterbatasan ruang pantau ini menyulitkan tugas administrator jaringan saat mencoba melacak waktu presisi terjadinya intrusi, mengidentifikasi titik asal serangan, serta menganalisis pola muatan yang kerap diarahkan ke peladen.

Ketiadaan panel pemantauan terpusat memaksa administrator melakukan audit mandiri terhadap ribuan baris log mentah pascaledakan insiden. Prosedur manual tersebut sangat tidak efisien dan memperlambat langkah penanganan ancaman. Mempertimbangkan kesenjangan ini, fokus penelitian diarahkan pada integrasi antara teknologi Coraza WAF dengan platform analitik ELK Stack (Elasticsearch, Logstash, Kibana). Mekanisme kerjanya menempatkan ELK Stack sebagai pengumpul, penerjemah (*parser*), dan penyaji data log Coraza menjadi visualisasi dashboard yang dinamis. Melalui integrasi ini, infrastruktur PTIPD tidak sekadar memiliki "tembok pertahanan" yang aktif memblokir ancaman, melainkan juga dibekali dengan “visualisasi” data atau log. Kombinasi ini diharapkan mampu meningkatkan proses identifikasi anomali, klasifikasi serangan, hingga pengambilan keputusan mitigasi dengan jauh lebih presisi.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang ada, rumusan masalah yang sesuai di dalam tugas akhir ini adalah:

1. Bagaimana mengimplementasikan Coraza WAF dan menguji efektivitasnya dalam menangani skenario serangan siber pada server website UIN Sunan Kalijaga?
2. Bagaimana mengintegrasikan ELK Stack untuk memvisualisasikan log deteksi serangan dari Coraza WAF secara *real-time* guna mendukung pemantauan keamanan?

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1.3. Batasan Masalah

Untuk menjaga agar ruang lingkup pembahasan lebih terarah dan dapat diselesaikan dalam waktu yang sudah ditentukan, maka tugas akhir ini memiliki batasan masalah sebagai berikut:

1. Penelitian ini dilaksanakan pada lingkungan simulasi sebagai tahap awal pengujian keamanan, yang akan digunakan untuk mengevaluasi kesiapan sistem sebelum diterapkan pada infrastruktur produksi peladen web PTIPD.
2. Menggunakan tiga situs *stagging* yang merepresentasikan layanan situs Banding UKT, KKN, dan Kehadiran sebagai objek implementasi WAF.
3. Sistem operasi yang digunakan adalah *Ubuntu Server* dan *docker* sebagai platform utama untuk implementasi dan pengujian.
4. Menggunakan Platform Coraza sebagai Web Application Firewall untuk melakukan deteksi serta *blocking* dan *Caddy Server* sebagai peladen dari Coraza WAF.
5. Menggunakan *OWASP Core Rule Set* versi terbaru sebagai kumpulan aturan keamanan yang diterapkan pada *Web Application Firewall*.
6. Menggunakan pendekatan *Reverse proxy* sebagai penghubung antara peladen *website* dengan *Caddy Server*.
7. Analisis dan visualisasi data serangan dilakukan menggunakan infrastruktur ELK Stack, yang terdiri dari Filebeat sebagai pengumpul log, Logstash sebagai pengolah data, Elasticsearch sebagai media penyimpanan dan indeks data, serta Kibana sebagai antarmuka visualisasi dan analisis data.
8. Menggunakan ZAP OWASP sebagai alat untuk menjalankan skenario serangan secara otomatis dan dibatasi pada dua jenis serangan aplikasi web, meliputi SQL Injection dan Cross-Site Scripting.
9. Menggunakan perangkat lunak Certbot untuk menghasilkan sertifikat SSL/TLS.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

10. Data yang ditampilkan dalam *dashboard* Kibana dibatasi pada parameter tertentu, yaitu alamat IP penyerang, jenis serangan, *rule WAF* yang terpicu, waktu terjadinya serangan, serta status *response*.
11. Penelitian ini hanya difokuskan pada lalu lintas protokol HTTP dan HTTPS dan tidak membahas sistem *Intrusion Detection System non-web* serta tidak mencakup analisis serangan Distributed Denial of Service (DDoS) pada lapisan jaringan.

1.4. Tujuan Penelitian

Berdasarkan permasalahan yang di ajukan, tujuan dari pelaksanaan Capstone Design Project ini adalah:

1. Merancang dan mengimplementasikan Web Application Firewall berbasis Coraza pada infrastruktur server website UIN Sunan Kalijaga.
2. Mengintegrasikan ELK stack untuk visualisasikan deteksi serangan dari log Coraza WAF secara realtime guna mendukung pemantauan keamanan.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian tugas akhir ini mencakup tiga aspek utama yang saling berkesinambungan.

1. Bagi pengelola infrastruktur (PTIPD UIN Sunan Kalijaga), implementasi ini diharapkan tidak sekadar menambal celah keamanan aplikasi web kampus melalui sistem blokade pertahanan Coraza WAF, tetapi juga menyediakan fasilitas pemantauan historis terpusat menggunakan ELK Stack yang sangat meringankan beban tim teknis dalam mengusut dan menganalisis insiden siber.
2. Bagi peneliti, proyek ini bertindak sebagai media pengujian praktis yang mengubah teori jaringan komputer menjadi pengalaman nyata dalam merancang dan mengkonfigurasi arsitektur Web Application Firewall

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

dengan integrasi sistem visualisasi, sekaligus menjadi bekal portofolio berharga untuk terjun ke industri keamanan teknologi informasi.

3. Bagi Akademisi, dokumentasi proyek ini diharapkan dapat menyumbang literatur yang dapat dijadikan pedoman serta studi kasus mengenai praktik integrasi Web Application Firewall dengan sistem analitik log terpusat di lingkungan institusi pendidikan.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari implementasi, pengujian dan evaluasi yang telah dilakukan, maka penelitian ini menghasilkan beberapa poin kesimpulan sebagai berikut:

1. Implementasi Coraza WAF pada infrastruktur server web berhasil dilakukan dengan menempatkan Caddy Server sebagai *reverse proxy*, *TLS termination*, dan peladen dari Web Application Firewall. Coraza WAF digunakan sebagai mesin inspeksi dengan integrasi OWASP Core Rule Set yang diterapkan pada ketiga domain *stagging* UIN Sunan kalijaga yaitu BandingUKT, EKKN, dan Kehadiran. Hasil pengujian menggunakan OWASP ZAP menunjukkan bahwa Coraza WAF mampu mendeteksi dan memblokir skenario serangan SQL Injection dan Cross-Site Scripting secara akurat. Hal ini ditunjukkan melalui perubahan status respons terhadap permintaan berbahaya menjadi *403 Forbidden* saat Web Application Firewaall dalam mode blokir aktif, sehingga permintaan berbahaya tidak akan diteruskan ke aplikasi *backend.*
2. Integrasi ELK Stack berhasil diterapkan guna mendukung pemantauan keamanan dari hasil deteksi Coraza WAF. Filebeat digunakan untuk membaca dan mengirimkan log Coraza WAF, Logstash memproses serta memisahkan data berdasarkan aplikasi, Elasticsearch sebagai penyimpanan dan *indexing* data, dan Kibana menampilkan hasil dalam bentuk dashboard visualisasi. Melalui integrasi ini informasi waktu kejadian, alamat IP, jenis serangan, Rule Id, dan status respons dapat ditampilkan secara lebih terstruktur. Dengan demikian, pihak pengelola dapat memantau aktivitas serangan secara lebih mudah dibandingkan membaca log mentah secara manual.
3. Evaluasi hasil uji menunjukkan bahwa penerapan WAF dengan aturan

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

keamanan yang ketat tidak hanya berdampak pada peningkatan perlindungan, namun juga dapat memunculkan kendala. Pada aplikasi web EKKN ditemukan kendala *Mixed Content* akibat ketidak kesesuaian protokol antara akses klien berbasih HTTPS dan sebagian komunikasi masih mengarah pada HTTP. Kendala ini dimitigasi melalui penambahan header *Content Security Policy* dengan instruksi *upgrade-insecure-requests* pada konfigurasi Caddy. Selain itu, pada aplikasi web BandingUKT ditemukan kondisi False Positive yang menyebabkan akses pengguna sah ikut terblokir. Masalah tersebut dimitigasi melalui penyesuaian aturan WAF agar aktivitas normal tetap dapat berjalan tanpa menghilangkan fungsi perlindungan terhadap serangan.

Secara keseluruhan, penelitian ini menunjukkan bahwa kombinasi Coraza WAF dan ELK Stack dapat digunakan sebagai alternatif pengamanan aplikasi web berbasis sumber terbuka pada lingkungan simulasi infrastruktur PTIPD. Coraza WAF berperan sebagai lapisan perlindungan yang melakukan deteksi dan pemblokiran terhadap permintaan berbahaya, sedangkan ELK Stack berperan sebagai sistem pemantauan yang mempermudah analisis log keamanan. Namun, hasil penelitian juga menunjukkan bahwa implementasi WAF tidak cukup hanya dilakukan dengan memasang aturan keamanan, tetapi perlu disertai proses evaluasi, penyesuaian aturan, dan pemantauan berkelanjutan agar perlindungan sistem tetap seimbang dengan ketersediaan layanan bagi pengguna sah.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

5.2 Saran

Berdasarkan hasil implementasi dan evaluasi sistem, terdapat beberapa saran yang dapat diberikan kepada pihak-pihat terkait terutama terhadap penelitian selanjutnya, yaitu sebagai berikut:

1. **Tim Pengembang Aplikasi PTIPD**

   Pelonggaran aturan WAF (Rule Tuning) yang dilakukan pada fungsi login saat ini pada dasarnya hanyalah solusi sementara agar user tetap bisa

mengakses aplikasi. Untuk solusi jangka panjang, tim pengembang aplikasi PTIPD disarankan untuk menutup celah keamanan langsung dari dalam kode programnya (*source code*). Perbaikan ini bisa dilakukan dengan cara menggunakan prepared statements agar aman dari injeksi database, menyaring data yang dimasukkan pengguna secara ketat, serta menyembunyikan pesan error PHP agar tidak tampil di layar. Jika kode aplikasi sudah diperbaiki, sistem WAF bisa diatur kembali ke tingkat pengamanan paling ketat tanpa takut salah memblokir pengguna asli (*False Positive).*

2. Administrator Pengelola keamanan PTIPD

Sistem pemantauan log yang dibangun dalam penelitian ini masih mengharuskan administrator untuk memantau layar dasbor secara manual. Untuk pengembangan selanjutnya, sangat disarankan untuk menambahkan fitur notifikasi peringatan dini yang berjalan otomatis, misalnya menggunakan *Kibana Alerting*. Dengan fitur ini, apabila sistem mendeteksi adanya lonjakan serangan yang berbahaya secara tiba-tiba, pemberitahuan akan langsung dikirimkan ke ponsel tim keamanan melalui Telegram atau surel, sehingga penanganan bisa dilakukan lebih cepat.

3. Penelitian Selanjutnya

Penelitian selanjutnya dapat mengembangkan sistem ini dengan mengintegrasikan *machine learning* sebagai lapisan analisis tambahan untuk memperkuat kinerja Coraza WAF. Integrasi ini diperlukan karena pola serangan aplikasi web terus berkembang, termasuk adanya potensi pemanfaatan teknologi berbasis kecerdasan buatan oleh penyerang untuk menghasilkan varian *payload* berbahaya serta bersifat lebih dinamis sehingga sulit dikenali oleh aturan status. Pada aspek analisis terhadap log Coraza WAF yang dikelola melalui ELK Stack, machine learning dapat digunakan untuk mempelajari pola trafik normal dan mencurigakan, mendeteksi anomali, mengklasifikasikan jenis serangan, serta memberikan

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

rekomendasi rule tuning. Dengan demikian, Coraza WAF dan ELK Stack tetap berperan sebagai mesin pertahanan dan pengelola log, sedangkan machine learning berfungsi sebagai mekanisme pendukung untuk meningkatkan adaptivitas sistem terhadap pola serangan baru.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR PUSTAKA

[1] L. Tni and H. Siburian, “LANSKAP KEAMANAN SIBER 2024,” no. 70, 2024.

[2] “OWASP Top 10:2021.” Accessed: May 27, 2026. [Online]. Available: https://owasp.org/Top10/2021/?utm_source=chatgpt.com

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

[4] J. P. Tosso, “How OWASP Coraza Improved Performance by 100x,” Medium. Accessed: Jun. 04, 2026. [Online]. Available: https://medium.com/@jptosso/how-owasp-coraza-improved-performance-by-100x-38d982371ea9

[5] M. D. Mahardika, “Implementasi Mod Security sebagai Web Application Firewall (WAF) pada Learning Management System (LMS) Moodle dengan Metode Open Web Application Security Project (OWASP),” Universitas Islam Negeri Sunan Kalijaga Yogyakarta, Yogyakarta, 2024. [Online]. Available: https://digilib.uin-suka.ac.id/id/eprint/69588/

[6] M. R. Faisal, E. S. Pramukantoro, and M. Data, “IMPLEMENTASI SISTEM DETEKSI SERANGAN PADA WEBSITE BERBASIS WORDPRESS SECARA REALTIME MENGGUNAKAN APACHE KAFKA”.

[7] A. Yudhistira and Y. Fitrisia, “MONITORING LOG SERVER DENGAN ELASTICSEARCH, LOGSTASH DAN KIBANA (ELK),” *Rabit J. Teknol. Dan Sist. Inf. Univrab*, vol. 8, no. 1, pp. 124–134, Apr. 2023, doi: 10.36341/rabit.v8i1.2975.

[8] H. H. Muhammad, A. I. Hadiana, and H. Ashaury, “PENGAMANAN APLIKASI WEB DARI SERANGAN SQL INJECTION DAN CROSS SITE SCRIPTING MENGGUNAKAN WEB APPLICATION FIREWALL,” vol. 7, no. 5, 2023.

[9] S. E. Prasetyo, H. Haeruddin, and K. Ariesryo, “Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall,” *Antivirus J. Ilm. Tek. Inform.*, vol. 18, no. 1, pp. 27–36, May 2024, doi: 10.35457/antivirus.v18i1.3339.

[10] P. S. Saputra and P. A. Pratama, “PERANCANGAN DAN KOMPARASI WEB SERVER NGINX DENGAN WEB SERVER APACHE SERTA PEMANFAATAN REVERSE PROXY SERVER PADA NGINX”.

[11] R. Irianto, M. A. Nugroho, E. Sahputra, R. Maulidi, and L. Isyriyah, “Evaluating Load-Balancing Performance of NGINX and Caddy in Containerized WordPress Deployments”.

[12] M. Zaedil, I. Syamsuddin, and M. N. Y. Utomo, “Coraza-Based WAF with OWASP CRS for SQL Injection in Multi-Domain Web System,” *J. Inf. Syst. Inform.*, vol. 8, no. 2, pp. 2337–2362, Apr. 2026, doi: 10.63158/journalisi.v8i2.1475.

[13] A. Mk, K. S. S. Bala, S. S. T. Sonti, and J. Kp, “An empirical study on the evaluation and enhancement of OWASP CRS (Core Rule Set) in

STATE ISLAMIC UNIVERSITY SUNAN KALIJAGA YOGYAKARTA

ModSecurity," *Comput. Secur.*, vol. 160, p. 104714, Jan. 2026, doi: 10.1016/j.cose.2025.104714.
[14] C. Scano *et al.*, "ModSec-Learn: Boosting ModSecurity with Machine Learning," vol. 1198, 2025, pp. 23–33. doi: 10.1007/978-3-031-76459-2_3.
[15] P. N. K. Bayu, "Implementasi Server Log Monitoring System menggunakan Elastic Stack".
[16] I. G. Adnyana, A. M. Dirgayusari, and K. J. Atmaja, "Data Visualization for Building a Cyber Attack Monitoring Dashboard Based on Honeypot," *sinkron*, vol. 8, no. 4, pp. 2510–2518, Oct. 2024, doi: 10.33395/sinkron.v8i4.14144.
[17] D. U. Khabibah, Y. Nurrohman, K. Dewandaru, S. J. D. H. Balian, and A. Setiawan, "Strategi Mitigasi SQL Injection dengan Implementasi SQLMap dan Web Application Firewall," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 12, Jun. 2024, doi: 10.47134/jtsi.v1i4.2656.
[18] D. Ending Narhudin, B. Irawan, and A. Bahtiar, "EVALUASI KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP: PENILAIAN TERHADAP SERANGAN INJEKSI SQL DAN CROSS-SITE SCRIPTING (XSS)," *JATI J. Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 675–680, Feb. 2024, doi: 10.36040/jati.v8i1.8700.
[19] N. Nelmiawati and K. Dealova, "Analysis of Polyglot Obfuscation Techniques against ModSecurity in Preventing Cross-Site Scripting (XSS) and SQL Injection Attacks with Experimental Method," *J. Tek. Inform. Jutif*, vol. 6, no. 4, pp. 2540–2549, Sep. 2025, doi: 10.52436/1.jutif.2025.6.4.5000.
[20] Ade Gustiyonoo, E. Irawadi Alwi, and S. Mubarak Abdullah, "Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing," *Cyber Secur. Dan Forensik Digit.*, vol. 7, no. 1, pp. 25–33, Nov. 2024, doi: 10.14421/csecurity.2024.7.1.4432.
[21] "The ZAP Homepage," ZAP. Accessed: Jun. 05, 2026. [Online]. Available: https://www.zaproxy.org/
[22] "ZAP – Getting Started." Accessed: Jun. 05, 2026. [Online]. Available: https://www.zaproxy.org/getting-started/

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA