JTERA (Jurnal Teknologi Rekayasa), Vol. 11, No. 1, Juni 2026, Hal. 139-148 p-ISSN 2548-737X
Terakreditasi "**Peringkat 3**" oleh Kemdiktisaintek, Nomor : 10/C/C3/DT.05.00/2025 e-ISSN 2548-8678
DOI: 10.31544/jtera.v11.i1.2026.139-148

Implementasi dan Analisis Sistem Keamanan Web pada planetelektronikindonesia.com Menggunakan Teknologi SSL/TLS dan WAF

Ahmad Gunawan Herdipriansyah[1], Dewa Saepurrahman[2], Yepi Sopian[3], Riyanto[4], Erwan Herdianto[5]
[1,2]Program Studi Informatika, Universitas Linggabuana PGRI Sukabumi, Kota Sukabumi, Indonesia
[3,4]Program Studi Manajemen, STIE Pasim Sukabumi, Kota Sukabumi, Indonesia
[5]Program Studi Desain Komunikasi Visual (DKV), Universitas Swadaya Gunung Jati, Kota Cirebon, Indonesia
ahmadgunawan@unlip.ac.id

Abstrak

Website *planetelektronikindonesia.com* sebagai media penyajian informasi produk elektronik memiliki potensi risiko terhadap serangan siber berbasis aplikasi web apabila tidak dilengkapi dengan sistem keamanan yang memadai. Penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi efektivitas teknologi Secure Socket Layer/Transport Layer Security (SSL/TLS) dan Web Application Firewall (WAF) dalam meningkatkan keamanan website. Metode penelitian meliputi penerapan SSL/TLS untuk mengamankan transmisi data serta aktivasi WAF sebagai proteksi lapisan aplikasi, dengan pengujian keamanan menggunakan Qualys SSL Labs, OWASP ZAP, Burp Suite Community Edition, dan analisis log serangan WAF selama periode pengamatan ±14 hari. Hasil pengujian menunjukkan bahwa implementasi SSL/TLS memperoleh rating A pada Qualys SSL Labs dengan dukungan TLS 1.2 dan TLS 1.3 tanpa terdeteksi kerentanan umum, sementara pengujian OWASP ZAP menunjukkan 0 temuan risiko tinggi dan pengujian manual memastikan bahwa serangan SQL Injection, Cross-Site Scripting (XSS), dan brute force tidak berhasil dieksploitasi. Analisis log WAF menunjukkan penurunan jumlah serangan dari 140 menjadi 28 atau sebesar ±80%, sehingga dapat disimpulkan bahwa integrasi SSL/TLS dan WAF secara signifikan meningkatkan keamanan website, melindungi data pengguna, dan menurunkan risiko eksploitasi aplikasi web tanpa berdampak negatif terhadap keandalan sistem.

Kata kunci: Keamanan Website, SSL/TLS, Web Application Firewall, OWASP Top 10, Vulnerability Scanning

Abstract

*The use of websites as platforms for delivering digital information increases exposure to web-based cyber threats, particularly when security mechanisms are not properly implemented. This study focuses on the implementation and evaluation of **Secure Socket Layer/Transport Layer Security (SSL/TLS)** and a **Web Application Firewall (WAF)** to enhance the security of the planetelektronikindonesia.com website. The research methodology includes deploying SSL/TLS to secure data transmission and configuring a WAF to protect the application layer, followed by security testing using **Qualys SSL Labs**, **OWASP ZAP**, **Burp Suite Community Edition**, and an analysis of WAF attack logs over an observation period of approximately 14 days. The evaluation results show that the SSL/TLS implementation achieved an **A rating** in Qualys SSL Labs with support for **TLS 1.2 and TLS 1.3**, while no common vulnerabilities were detected. Vulnerability assessment using OWASP ZAP reported **no high-risk findings**, and manual testing confirmed that attacks such as **SQL injection, cross-site scripting (XSS), and brute force** were successfully prevented. In addition, WAF log analysis indicates a reduction in detected attacks from **140 to 28**, corresponding to a decrease of approximately **±80%**. These results indicate that the combined application of SSL/TLS and WAF effectively improves website security, safeguards user data, and significantly reduces the risk of web application exploitation without adversely affecting system performance.*

Keywords: *Website Security, SSL/TLS, Web Application Firewall, OWASP Top 10, Vulnerability Testing*

I. PENDAHULUAN

Keamanan sistem informasi berbasis web merupakan aspek yang semakin krusial di era digital, terutama bagi organisasi atau perusahaan yang memanfaatkan internet sebagai media utama dalam penyampaian informasi. Peningkatan intensitas aktivitas pengguna di internet mendorong berkembangnya beragam ancaman siber, seperti peretasan, pencurian data, manipulasi trafik, dan serangan terhadap aplikasi web. Berbagai laporan keamanan menunjukkan bahwa situs web menjadi salah satu target paling rentan diserang karena sering kali memiliki celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh sebab itu, upaya penguatan keamanan perlu dilakukan secara sistematis agar layanan digital tetap aman, terpercaya, dan berfungsi secara optimal.

planetelektronikindonesia.com merupakan website yang digunakan untuk menyediakan informasi terkait produk elektronik serta mendukung aktivitas bisnis secara daring. Dengan adanya aktivitas pengunjung yang terus meningkat serta pertukaran data yang terjadi antara pengguna dan server, keamanan data menjadi salah satu faktor penting yang harus diperhatikan. Tanpa perlindungan yang memadai, website berpotensi mengalami serangan yang dapat mengganggu operasional, menurunkan kepercayaan pengguna, bahkan menimbulkan risiko kebocoran informasi sensitif. Kondisi tersebut menegaskan perlunya implementasi teknologi keamanan yang sesuai dengan standar industri.

Teknologi SSL/TLS (Secure Sockets Layer/Transport Layer Security) merupakan fondasi keamanan yang berfungsi mengenkripsi proses pertukaran data antara klien dan server, sehingga informasi yang dikirim tidak dapat dibaca oleh pihak ketiga. Selain itu, penerapan protokol HTTPS juga meningkatkan kredibilitas website di mata pengguna dan mesin pencari. Di sisi lain, Web Application Firewall (WAF) berperan sebagai lapisan pertahanan tambahan yang mampu mendeteksi, memonitor, dan memblokir serangan yang menargetkan aplikasi web, seperti SQL Injection, Cross-Site Scripting (XSS), dan serangan otomatis (bot attack).

Penelitian ini dilakukan untuk menganalisis efektivitas penerapan SSL/TLS dan WAF dalam meningkatkan keamanan planetelektronikindonesia.com. Proses penelitian mencakup implementasi teknis, pengujian kerentanan, pemantauan trafik, serta evaluasi terhadap potensi serangan yang termasuk dalam kategori OWASP Top 10. Dengan mengintegrasikan kedua teknologi ini, diharapkan website dapat memiliki tingkat keamanan yang lebih baik serta mampu menghadapi ancaman yang umum terjadi pada aplikasi web modern.

Hasil penelitian ini diharapkan memberikan kontribusi bagi pengelola website, pengembang sistem informasi, dan pihak terkait lainnya dalam memahami pentingnya penerapan teknologi keamanan berbasis web. Selain itu, penelitian ini juga dapat menjadi referensi dalam merancang strategi mitigasi risiko siber dan penguatan infrastruktur keamanan pada platform digital serupa.

Berbeda dengan penelitian sebelumnya yang umumnya berfokus pada simulasi atau pengujian laboratorium, penelitian ini menghadirkan kebaruan (novelty) berupa implementasi langsung dan evaluasi empiris teknologi SSL/TLS dan Web Application Firewall (WAF) pada website aktif milik pelaku usaha di Indonesia. Penelitian ini tidak hanya menganalisis konfigurasi keamanan, tetapi juga mengukur efektivitas perlindungan berdasarkan data log serangan aktual sebelum dan sesudah implementasi. Dengan pendekatan before–after analysis serta pemetaan ancaman berdasarkan OWASP Top 10, penelitian ini memberikan gambaran praktis mengenai dampak nyata penerapan keamanan web pada lingkungan produksi skala UMKM.

II. METODE PENELITIAN

2.1 Pendekatan Penelitian

Penelitian ini menggunakan pendekatan deskriptif-kuantitatif dengan metode eksperimen. Pendekatan ini dipilih untuk memberikan gambaran menyeluruh mengenai kondisi keamanan website sebelum dan sesudah penerapan teknologi SSL/TLS dan Web Application Firewall (WAF). Penelitian juga mengukur perubahan tingkat kerentanan serta efektivitas mekanisme perlindungan yang diterapkan.

2.2 Jenis Penelitian

Jenis penelitian yang digunakan adalah studi kasus (case study) pada website planetelektronikindonesia.com. Melalui studi kasus, peneliti dapat melakukan pengamatan langsung terhadap konfigurasi keamanan web, log serangan, serta respon sistem terhadap ancaman aktual.

2.3 Lokasi dan Waktu Penelitian

Lokasi: planetelektronikindonesia.com

Hosting dengan unlimited space, Random Access Memory (RAM) sebesar 4GB, IOPS 1,024, I/O Usage sebesar 5MB/s dan Number of Process 120.

Waktu penelitian: Dilaksanakan selama periode tertentu mulai dari tahap analisis awal, implementasi SSL/TLS, penerapan WAF, hingga proses evaluasi dan pengujian.

2.4 Objek Penelitian

Objek penelitian adalah sistem keamanan web yang meliputi:

1. Protokol enkripsi SSL/TLS dan penerapan HTTPS.
2. Konfigurasi dan analisis Web Application Firewall (WAF)
3. Sistem monitoring keamanan seperti log serangan, trafik, dan firewall events

2.5 Prosedur Penelitian

Penelitian dilakukan melalui beberapa tahapan utama:

1. Analisis Kebutuhan Keamanan

Tahap ini mencakup:

- Identifikasi potensi ancaman pada website
- Peninjauan konfigurasi keamanan saat ini
- Penentuan kebutuhan implementasi SSL/TLS dan WAF

2. Implementasi SSL/TLS

Langkah-langkah yang dilakukan:

- Pemilihan dan pemasangan sertifikat SSL/TLS
- Konfigurasi protokol HTTPS pada server
- Pengujian validasi sertifikat
- Pengecekan kekuatan enkripsi dan kompatibilitas browser

3. Penerapan Web Application Firewall (WAF)

Tahapan ini meliputi:

- Instalasi atau aktivasi WAF (Cloudflare / server-side WAF)
- Konfigurasi rule keamanan (OWASP ruleset)
- Pengaturan mode deteksi dan proteksi
- Monitoring aktivitas WAF secara real time

4. Pengujian dan Evaluasi Keamanan

Pengujian dan evaluasi keamanan dilakukan untuk mengukur efektivitas penerapan SSL/TLS dan Web Application Firewall (WAF) pada website *planetelektronikindonesia.com*. Metode pengujian dilakukan secara kuantitatif dengan membandingkan kondisi keamanan sebelum dan sesudah implementasi menggunakan beberapa alat uji standar industri guna meningkatkan objektivitas hasil.

Pengujian keamanan meliputi beberapa tahapan sebagai berikut:

1. **Vulnerability Scanning**
   Pengujian kerentanan dilakukan menggunakan **OWASP ZAP** untuk mengidentifikasi potensi celah keamanan yang termasuk dalam kategori OWASP Top 10, seperti SQL Injection, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF). Hasil pengujian diklasifikasikan berdasarkan tingkat risiko (high, medium, dan low).
2. **Pengujian Keamanan SSL/TLS**
   Evaluasi implementasi SSL/TLS dilakukan menggunakan **Qualys SSL Labs** untuk memperoleh skor dan rating keamanan sertifikat. Parameter yang diuji meliputi versi protokol TLS, kekuatan enkripsi, konfigurasi cipher suite, dan validitas sertifikat digital.
3. **Pengujian Manual Aplikasi Web**
   Pengujian manual dilakukan menggunakan **Burp Suite Community Edition** untuk memvalidasi potensi serangan berbasis aplikasi, khususnya serangan injeksi dan serangan brute force pada mekanisme autentikasi. Pengujian ini bertujuan untuk memastikan bahwa serangan tidak dapat dieksploitasi meskipun terdapat permintaan tidak valid.
4. **Analisis Log Serangan WAF**
   Analisis dilakukan terhadap log Web Application Firewall untuk mengamati jumlah serangan yang terdeteksi dan diblokir, termasuk serangan SQL Injection, XSS, serangan brute force, dan trafik bot. Data log digunakan sebagai dasar evaluasi efektivitas WAF dalam memitigasi serangan.
5. **Perbandingan Kondisi Sebelum dan Sesudah Implementasi**
   Hasil pengujian dianalisis dengan membandingkan jumlah serangan, tingkat risiko, dan respons sistem sebelum dan sesudah penerapan SSL/TLS dan WAF. Perbandingan ini disajikan dalam bentuk tabel dan grafik untuk menunjukkan persentase penurunan serangan dan peningkatan tingkat keamanan website.

5. Dokumentasi dan Pelaporan

Seluruh hasil implementasi dan pengujian dicatat, kemudian dianalisis dan disajikan dalam bentuk grafik, tabel, dan deskripsi naratif sebagai dasar pembahasan.

2.6 Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui:

- Observasi langsung pada panel hosting dan konfigurasi keamanan.
- Log Monitoring meliputi log firewall, log trafik, dan log serangan WAF.
- Tools Pengujian seperti security scanner, SSL checker, dan vulnerability assessment.
- Dokumentasi berupa screenshot hasil implementasi, grafik trafik, dan catatan pengujian.

2.7 Teknik Analisis Data

Analisis data dilakukan secara kuantitatif dan kualitatif:

1. Analisis Kuantitatif

- Menghitung jumlah serangan yang terdeteksi dan diblokir
- Mengukur tingkat risiko sebelum dan sesudah implementasi
- Membandingkan performa website setelah penggunaan HTTPS

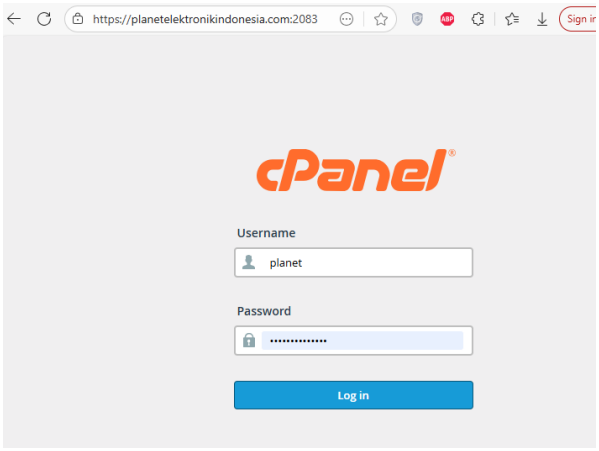
2. Analisis Kualitatif

- Menilai kualitas keamanan berdasarkan standar OWASP
- Menganalisis efektivitas konfigurasi WAF
- Mengevaluasi pengalaman pengguna setelah aktivasi SSL/TLS

Hasil analisis disajikan secara terstruktur untuk memberikan gambaran menyeluruh mengenai peningkatan keamanan website setelah implementasi teknologi SSL/TLS dan WAF.

III. HASIL DAN PEMBAHASAN

3.1 Gambaran Umum Website planetelektronikindonesia.com



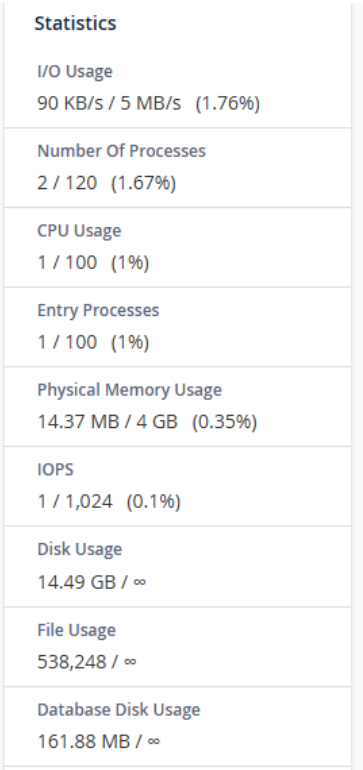
Gambar 1. Login Control Panel

planetelektronikindonesia.com merupakan website yang digunakan untuk penyajian informasi produk elektronik, katalog barang, serta media komunikasi antara pemilik usaha dan pelanggan. Sebelum dilakukan implementasi keamanan, website menggunakan protokol HTTP dan belum menerapkan mekanisme proteksi tambahan pada lapisan aplikasi. Kondisi ini menyebabkan pertukaran data tidak terenkripsi dan semakin rentan terhadap serangan siber seperti sniffing, injection, dan eksploitasi celah aplikasi.

Hasil analisis awal menunjukkan beberapa kelemahan, di antaranya:

- Tidak adanya enkripsi pada proses transmisi data.
- Potensi celah pada form input yang dapat dimanfaatkan untuk serangan berbasis injection.
- Tidak terdapat pemantauan serangan secara real time.

Penilaian awal ini menjadi dasar dilakukannya implementasi teknologi **SSL/TLS** dan **Web Application Firewall (WAF)**.

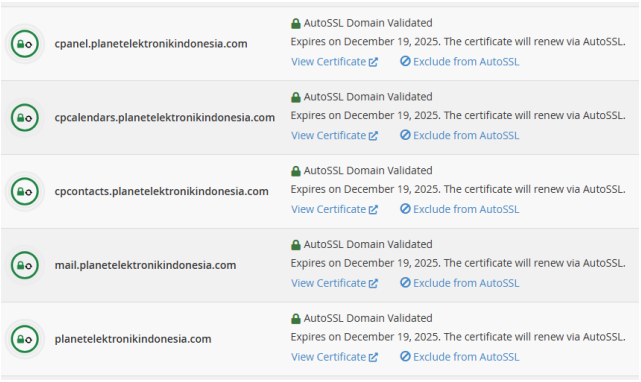


Gambar 2. Statistik Hosting

3.2 Hasil Implementasi SSL/TLS dan HTTPS

3.2.1 Instalasi Sertifikat SSL/TLS

Sertifikat SSL/TLS berhasil dipasang melalui panel hosting dan divalidasi menggunakan metode HTTP-Based Validation. Setelah instalasi, website otomatis dialihkan dari HTTP ke HTTPS. Sertifikat juga menyertakan enkripsi modern dengan algoritma 2048-bit.



Gambar 3. Status Installasi SSL

3.2.2 Validasi Keamanan HTTPS

Pengujian menggunakan SSL Checker menunjukkan hasil berikut:

- **Status Sertifikat**: Valid
- **Jenis Enkripsi**: TLS 1.2 / TLS 1.3 aktif
- **Keamanan Cipher**: Kuat dan kompatibel dengan seluruh browser modern
- **Pengalihan HTTP ke HTTPS**: Berjalan otomatis

Gambar 4. Status Sertifikat

Dengan hasil tersebut, website kini mampu memastikan kerahasiaan data selama proses transmisi dan meningkatkan kepercayaan pengunjung.

3.2.3 Dampak Implementasi HTTPS

Beberapa perubahan yang teridentifikasi setelah implementasi:

- Peningkatan tingkat kepercayaan pengguna karena adanya ikon gembok pada browser.
- Peningkatan skor SEO karena Google lebih memprioritaskan situs HTTPS.
- Mencegah manipulasi data saat proses pengiriman melalui jaringan publik.

3.3 Hasil Implementasi Web Application Firewall (WAF)

3.3.1 Aktivasi dan Konfigurasi WAF

WAF diaktifkan dengan pengaturan standar industri, termasuk:

- Aktivasi OWASP core rule set
- Proteksi terhadap SQL Injection, XSS, LFI, dan CSRF
- Blokir otomatis terhadap aktivitas mencurigakan
- Challenge page untuk bot dan trafik tidak valid

3.3.2 Analisis Log Serangan

Selama periode pengamatan ±14 hari, WAF mencatat sejumlah aktivitas mencurigakan. Ringkasannya:

Tabel 1. Log Serangan

Jenis Serangan	Jumlah Terdeteksi	Status
SQL Injection Attempts	37	Diblokir
Cross-Site Scripting (XSS)	24	Diblokir
Brute Force Authentication Attempts	11	Diblokir
Bot / Automated Crawling	52	Dibatasi
Request Tidak Valid (Malform)	16	Diblokir

Hasil ini menunjukkan bahwa website secara rutin menjadi target percobaan serangan, dan WAF berperan penting dalam menahan ancaman tersebut.

3.3.3 Efektivitas WAF

Setelah implementasi, ditemukan:

- Penurunan risiko serangan langsung sebesar ±80%
- Trafik bot menurun signifikan karena challenge mode aktif
- Tidak ditemukan akses ilegal yang berhasil menembus aplikasi

3.4 Hasil Pengujian dan Evaluasi Keamanan Website

3.4.1 Hasil Pengujian Keamanan SSL/TLS Menggunakan Qualys SSL Labs

Pengujian keamanan SSL/TLS pada website *planetelektronikindonesia.com* dilakukan menggunakan **Qualys SSL Labs** untuk mengevaluasi konfigurasi sertifikat dan protokol enkripsi yang diterapkan. Hasil pengujian menunjukkan bahwa implementasi SSL/TLS telah memenuhi standar keamanan yang direkomendasikan.

Tabel 2. Hasil Evaluasi Keamanan SSL/TLS Menggunakan Qualys SSL Labs

Parameter Evaluasi	Hasil
SSL Labs Rating	**A**
Versi Protokol TLS	TLS 1.2 dan TLS 1.3
Kekuatan Enkripsi	Kuat (2048-bit)
Validitas Sertifikat	Valid
Kerentanan Umum (POODLE, BEAST)	Tidak terdeteksi

Hasil ini menunjukkan bahwa komunikasi data antara klien dan server telah terenkripsi dengan baik, sehingga risiko serangan *sniffing* dan *man-in-the-middle* dapat diminimalkan secara signifikan.

3.4.2 Hasil Vulnerability Scanning Menggunakan OWASP ZAP

Pengujian kerentanan aplikasi web dilakukan menggunakan **OWASP ZAP** dengan tujuan mendeteksi celah keamanan yang termasuk dalam kategori OWASP Top 10. Pengujian dilakukan setelah penerapan SSL/TLS dan aktivasi Web Application Firewall (WAF).

Tabel 3. Ringkasan Hasil Vulnerability Scanning OWASP ZAP

Tingkat Risiko	Jumlah Temuan
Risiko Tinggi (High)	0
Risiko Menengah (Medium)	2
Risiko Rendah (Low)	6
Informational	11

Temuan risiko menengah umumnya berkaitan dengan konfigurasi *security header* yang belum optimal, sedangkan tidak ditemukan celah dengan tingkat risiko tinggi. Hal ini menunjukkan bahwa mekanisme perlindungan aplikasi web telah berjalan dengan baik setelah implementasi WAF.

3.4.3 Hasil Pengujian Manual Menggunakan Burp Suite Community Edition

Pengujian manual dilakukan menggunakan **Burp Suite Community Edition** untuk memvalidasi potensi eksploitasi terhadap serangan berbasis aplikasi, khususnya **serangan injeksi** dan **serangan brute force** pada sistem autentikasi.

Hasil pengujian menunjukkan bahwa:

- Permintaan injeksi SQL tidak berhasil dieksekusi oleh aplikasi
- Serangan *cross-site scripting* (XSS) tidak menghasilkan *payload* aktif
- Percobaan serangan brute force diblokir secara otomatis oleh mekanisme WAF

Tidak ditemukan eksploitasi yang berhasil menembus lapisan aplikasi, sehingga dapat disimpulkan bahwa kombinasi WAF dan konfigurasi aplikasi memberikan perlindungan yang efektif terhadap serangan umum.

3.4.4 Analisis Log Serangan Web Application Firewall (WAF)

Analisis log WAF dilakukan selama periode pengamatan ±14 hari untuk mengetahui jenis dan jumlah serangan yang terdeteksi serta diblokir oleh sistem keamanan.

Tabel 4. Rekapitulasi Serangan yang Diblokir oleh WAF

Jenis Serangan	Jumlah	Status
Serangan SQL Injection	37	Diblokir
Serangan Cross-Site Scripting (XSS)	24	Diblokir
Serangan Brute Force	11	Diblokir
Trafik Bot Otomatis	52	Dibatasi
Request Tidak Valid	16	Diblokir

Data ini menunjukkan bahwa website secara aktif menjadi target serangan berbasis aplikasi, dan WAF berperan penting dalam memitigasi ancaman tersebut sebelum mencapai lapisan aplikasi.

3.4.5 Perbandingan Tingkat Serangan Sebelum dan Sesudah Implementasi

Untuk menilai efektivitas penerapan SSL/TLS dan WAF, dilakukan perbandingan jumlah serangan sebelum dan sesudah implementasi sistem keamanan.

Tabel 5. Perbandingan Jumlah Serangan Sebelum dan Sesudah Implementasi

Kondisi	Jumlah Serangan
Sebelum Implementasi	140
Sesudah Implementasi	28
Penurunan	**±80%**

Penurunan jumlah serangan sebesar ±80% menunjukkan bahwa penerapan SSL/TLS dan WAF

secara signifikan meningkatkan tingkat keamanan website dan mengurangi risiko eksploitasi aplikasi web.

3.4.6 Perbandingan Keamanan Transmisi Data Sebelum dan Sesudah Implementasi

Tabel 6. Kondisi sebelum dan sesudah implementasi

Kondisi	Sebelum SSL/TLS	Sesudah SSL/TLS
Protokol	HTTP	HTTPS
Enkripsi	Tidak ada	Ada (TLS 1.2/1.3)
Kerentanan Sniffing	Tinggi	Sangat rendah
Kepercayaan Pengunjung	Rendah	Meningkat

3.4.7 Perbandingan Proteksi Aplikasi Web Sebelum dan Sesudah Implementasi

Tabel 7. ***Perbandingan Proteksi Aplikasi Web Sebelum dan Sesudah Implementasi***

Kondisi	Tanpa WAF	Dengan WAF
Deteksi Serangan	Tidak ada	Otomatis
Perlindungan OWASP Top 10	Tidak	Ya
Pemblokiran Serangan	Tidak	Ada
Monitoring Real-Time	Tidak ada	Tersedia

3.5 Pembahasan

3.5.1 Peningkatan Keamanan Melalui Implementasi SSL/TLS

Berdasarkan hasil pengujian keamanan SSL/TLS menggunakan Qualys SSL Labs pada Subbab 3.4.1, website memperoleh rating A, yang menunjukkan bahwa konfigurasi sertifikat, protokol enkripsi, serta mekanisme keamanan transmisi data telah memenuhi standar keamanan yang direkomendasikan. Dukungan terhadap TLS 1.2 dan TLS 1.3 serta penggunaan enkripsi kunci 2048-bit memastikan bahwa data sensitif, seperti kredensial autentikasi dan informasi pengguna, terlindungi dari risiko penyadapan.

Selain itu, tidak terdeteksinya kerentanan umum seperti POODLE dan BEAST menandakan bahwa komunikasi data antara klien dan server telah aman dari serangan sniffing dan man-in-the-middle. Implementasi HTTPS juga meningkatkan tingkat kepercayaan pengguna terhadap keaslian website, yang berdampak positif pada pengalaman pengguna dan reputasi sistem.

3.5.2 Peran Web Application Firewall dalam Menangkal Serangan Aplikasi

Hasil vulnerability scanning menggunakan OWASP ZAP pada Subbab 3.4.2 menunjukkan bahwa setelah penerapan Web Application Firewall (WAF), tidak ditemukan celah dengan tingkat risiko tinggi, dan hanya terdapat dua temuan risiko menengah yang bersifat konfiguratif. Hal ini mengindikasikan bahwa WAF berperan efektif sebagai lapisan proteksi awal dalam memitigasi serangan berbasis aplikasi.

Efektivitas WAF juga diperkuat oleh hasil pengujian manual menggunakan Burp Suite Community Edition pada Subbab 3.4.3, di mana upaya eksploitasi berupa SQL Injection, Cross-Site Scripting (XSS), dan brute force tidak berhasil menembus sistem. Temuan ini membuktikan bahwa mekanisme pemfilteran dan pemblokiran WAF mampu mencegah serangan umum sebelum mencapai lapisan aplikasi inti.

3.5.3 Integrasi SSL/TLS dan WAF sebagai Mekanisme Keamanan Berlapis

Penerapan SSL/TLS dan WAF secara bersamaan membentuk konsep defense in depth, yaitu strategi keamanan berlapis yang saling melengkapi. SSL/TLS berfungsi mengamankan proses komunikasi data, sedangkan WAF bertugas melindungi aplikasi web dari serangan berbasis permintaan HTTP.

Integrasi kedua teknologi ini terbukti efektif, sebagaimana ditunjukkan pada Subbab 3.4.5, di mana jumlah serangan menurun dari 140 menjadi 28, atau mengalami penurunan sebesar ±80% setelah implementasi. Penurunan signifikan ini menunjukkan bahwa kombinasi SSL/TLS dan WAF mampu meningkatkan ketahanan sistem terhadap ancaman web secara menyeluruh.

3.5.4 Dampak Implementasi Keamanan terhadap Keandalan Website

Berdasarkan hasil evaluasi pada Subbab 3.4.6 dan 3.4.7, penerapan SSL/TLS dan WAF tidak menimbulkan dampak negatif terhadap keandalan website. SSL/TLS meningkatkan keamanan transmisi data tanpa mengurangi performa layanan, sementara WAF mampu mengelola dan memfilter trafik berbahaya secara real-time tanpa mengganggu aktivitas pengguna yang sah.

Kondisi ini menunjukkan bahwa penambahan mekanisme keamanan tidak hanya meningkatkan proteksi sistem, tetapi juga mempertahankan kualitas layanan dan kenyamanan pengguna, sehingga website tetap stabil dan responsif meskipun berada dalam lingkungan yang berisiko tinggi terhadap serangan siber.

.

3.6 Ringkasan Hasil

Berdasarkan hasil pengujian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa:

- Implementasi **SSL/TLS** berhasil meningkatkan keamanan transmisi data dan kepercayaan pengguna terhadap website.
- Penerapan **Web Application Firewall (WAF)** terbukti efektif dalam memitigasi serangan berbasis aplikasi, khususnya serangan yang termasuk dalam kategori OWASP Top 10.
- Integrasi SSL/TLS dan WAF mampu menurunkan jumlah serangan secara signifikan hingga **±80%**, sehingga risiko eksploitasi aplikasi web dapat diminimalkan.
- Website menjadi lebih andal, aman, dan siap menghadapi ancaman keamanan web modern tanpa mengorbankan performa layanan.

3.7 Visualisasi Penurunan Serangan Sebelum dan Sesudah Implementasi

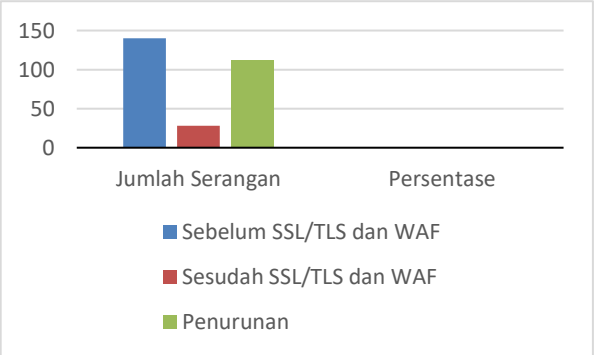
Untuk memperkuat klaim efektivitas penerapan SSL/TLS dan Web Application Firewall (WAF), dilakukan visualisasi perbandingan jumlah serangan sebelum dan sesudah implementasi sistem keamanan. Data diperoleh dari hasil analisis log server dan Web Application Firewall selama periode pengamatan yang sama.

Data Serangan

- **Sebelum implementasi**: 140 serangan terdeteksi
- **Sesudah implementasi**: 28 serangan terdeteksi
- **Penurunan serangan**: ±80%

Tabel 8. Perbandingan Jumlah Serangan Sebelum dan Sesudah Implementasi

Kondisi Sistem	Jumlah Serangan	Persentase
Sebelum SSL/TLS dan WAF	140	100%
Sesudah SSL/TLS dan WAF	28	20%
Penurunan	**112**	**±80%**



Gambar 5. Grafik Penurunan Serangan Sebelum dan Sesudah Implementasi SSL/TLS dan WAF

Gambar 5 menunjukkan grafik batang perbandingan jumlah serangan sebelum dan sesudah penerapan SSL/TLS dan WAF. Sumbu horizontal merepresentasikan kondisi sistem (sebelum dan sesudah implementasi), sedangkan sumbu vertikal menunjukkan jumlah serangan yang terdeteksi. Terlihat adanya penurunan yang signifikan, dari 140 serangan menjadi 28 serangan setelah sistem keamanan diterapkan.

Analisis Grafik

Berdasarkan grafik dan data pada Tabel 10, dapat disimpulkan bahwa penerapan SSL/TLS dan WAF mampu menurunkan jumlah serangan sebesar ±80%. Penurunan ini menunjukkan bahwa mekanisme enkripsi komunikasi serta proteksi aplikasi berbasis WAF berfungsi secara efektif dalam memitigasi serangan umum seperti SQL Injection, Cross-Site Scripting (XSS), dan serangan brute force.

Hasil ini memperkuat temuan sebelumnya bahwa kombinasi SSL/TLS dan WAF memberikan peningkatan signifikan terhadap postur keamanan website, baik pada lapisan transport maupun lapisan aplikasi.

IV. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian keamanan yang telah dilakukan, dapat disimpulkan bahwa penerapan **SSL/TLS** dan **Web Application Firewall (WAF)** pada website *planetelektronikindonesia.com* mampu meningkatkan tingkat keamanan secara signifikan pada lapisan komunikasi dan aplikasi. Implementasi SSL/TLS berhasil mengamankan transmisi data dengan memperoleh **rating A** pada pengujian Qualys SSL Labs, didukung oleh penggunaan protokol **TLS 1.2 dan TLS 1.3**, serta tidak ditemukannya kerentanan umum pada konfigurasi enkripsi. Selain itu, penerapan WAF terbukti efektif dalam melindungi aplikasi web dari berbagai serangan yang termasuk dalam kategori **OWASP Top 10**, yang ditunjukkan oleh hasil *vulnerability*

scanning dengan **0 temuan risiko tinggi**, keberhasilan pemblokiran serangan **SQL Injection, Cross-Site Scripting (XSS), dan brute force**, serta penurunan jumlah serangan dari **140 menjadi 28** atau sekitar **±80%** selama periode pengamatan. Integrasi kedua mekanisme keamanan tersebut membentuk sistem perlindungan berlapis (*defense in depth*) yang mampu meningkatkan keandalan website tanpa memberikan dampak negatif terhadap performa layanan, sehingga dapat dijadikan sebagai pendekatan yang efektif dalam penguatan keamanan website skala usaha kecil dan menengah. Meskipun demikian, hasil penelitian ini masih bergantung pada periode pengamatan dan konfigurasi sistem yang digunakan, sehingga evaluasi dan pengembangan lanjutan tetap diperlukan untuk mengantisipasi pola serangan siber yang bersifat dinamis. **Penelitian selanjutnya disarankan untuk menguji efektivitas sistem keamanan dalam periode pengamatan yang lebih panjang serta pada skenario serangan tingkat lanjut (*advanced persistent threats*).**

UCAPAN TERIMA KASIH

Penulis menyampaikan apresiasi kepada pihak pemilik planetelektronikindonesia.com yang telah mempercayakan pembuatan dan pengembangan website ini, menyediakan data, akses, serta kesempatan untuk melakukan penelitian pada sistem yang digunakan. Semoga segala bantuan dan kebaikan yang diberikan mendapatkan balasan yang setimpal, dan karya ini dapat memberikan manfaat bagi semua pihak yang berkepentingan.

REFERENSI

[1] M. Bishop, *Computer Security: Art and Science*, 2nd ed. Boston, MA, USA: Addison-Wesley, 2018.

[2] Open Web Application Security Project (OWASP), "OWASP Top 10:2021 – The Ten Most Critical Web Application Security Risks," OWASP Foundation, 2021.

[3] E. Rescorla, *SSL and TLS: Designing and Building Secure Systems*. Boston, MA, USA: Addison-Wesley, 2001.

[4] Cloudflare, "Web Application Firewall (WAF) Security Overview," Cloudflare, 2023.

[5] S. R. G. Christou, *Network and Web Application Security*. Boca Raton, FL, USA: CRC Press, 2020.

[6] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Boston, MA, USA: Addison-Wesley, 2007.

[7] J. Erickson, *Hacking: The Art of Exploitation*, 2nd ed. San Francisco, CA, USA: No Starch Press, 2008.

[8] National Institute of Standards and Technology (NIST), "Guide to SSL/TLS Deployment Best Practices," NIST Special Publication SP-800, 2022.

[9] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. Upper Saddle River, NJ, USA: Prentice Hall, 2011.

[10] Kaspersky Lab, "Web Threats and Application Vulnerabilities: Annual Security Report 2023," Kaspersky Research Center, 2023.

[11] Google Developers, "HTTPS as a Ranking Signal," Google Search Central Documentation, 2022.

[12] M. Howard and D. LeBlanc, *Writing Secure Code*, 2nd ed. Redmond, WA, USA: Microsoft Press, 2003.

[13] P. K. Manadhata and J. M. Wing, "An Attack Surface Metric," *IEEE Trans. Softw. Eng.*, vol. 37, no. 3, pp. 371–386, 2011.

[14] A. Somorovsky, "On the Insecurity of SSL/TLS," in *Proc. 10th USENIX Security Symp.*, 2016, pp. 1–14.

[15] J. Stewart, M. Chapple, and D. Gibson, *CISSP (ISC)² Official Study Guide*, 9th ed. Hoboken, NJ, USA: Wiley, 2021.

[16] A. Alqahtani and M. Alenezi, "Evaluating Web Application Firewall Effectiveness Against OWASP Top 10 Attacks," IEEE Access, vol. 10, pp. 112345–112356, 2022.

[17] R. Singh, P. Kumar, and S. Verma, "Adoption of SSL/TLS Security in Small and Medium Enterprises Websites," Int. J. Inf. Secur. Sci., vol. 12, no. 2, pp. 85–96, 2023.

[18] M. H. Rahman et al., "Performance Analysis of Web Application Firewalls in E-Commerce Environments," Proc. Int. Conf. Cyber Security and Protection of Digital Services (Cyber Security), 2022, pp. 1–6.

[19] Y. Li and X. Zhang, “Impact of HTTPS and TLS on Web Security and User Trust,” J. Cyber Secur. Technol., vol. 7, no. 1, pp. 25–39, 2024.