JURTIKA
Jurnal Informatika
Fakultas Komputer dan Teknik
Universitas Linggabuana PGRI Sukabumi

# ANALISA DAN PENERAPAN CLOUDFLARE DNS DAN WEB APPLICATION FIREWALL (WAF) SEBAGAI SOLUSI MITIGASI ANCAMAN SIBER PADA WEBSITE YAYASAN PKBM MANDIRI KOTA SUKABUMI

Ahmad Gunawan H., S.Kom.,M.Kom.[1], Dewa Saepurrahman[2]
ahmadgunawan@unlip.ac.id[1], dewasaepurrahman1@gmail.com[2]
*Program Studi Informatika – Fakultas Komputer dan Teknik*
*Universitas Linggabuana PGRI Sukabumi*

## Abstrak

Website lembaga pendidikan nonformal rentan terhadap berbagai ancaman siber akibat keterbatasan sistem keamanan. Website Yayasan PKBM Mandiri Kota Sukabumi mengalami permasalahan berupa tingginya trafik bot, percobaan brute-force login, serta penurunan performa layanan. Penelitian ini bertujuan untuk menganalisis efektivitas penerapan Cloudflare DNS dan Web Application Firewall (WAF) dalam memitigasi ancaman siber sekaligus meningkatkan performa website. Metode penelitian yang digunakan adalah deskriptif dengan analisis perbandingan kondisi sebelum dan sesudah penerapan Cloudflare. Data diperoleh melalui observasi trafik dan log serangan, dokumentasi konfigurasi keamanan, serta pengujian performa website. Hasil penelitian menunjukkan bahwa Cloudflare DNS dan WAF mampu menurunkan trafik berbahaya, mengurangi percobaan serangan berbasis bot dan injeksi, serta meningkatkan stabilitas dan kecepatan akses website. Penerapan Cloudflare terbukti menjadi solusi keamanan berbasis cloud yang efektif dan mudah diimplementasikan bagi lembaga pendidikan skala kecil dalam menghadapi ancaman siber.

Kata kunci: Cloudflare, keamanan siber, DNS, Web Application Firewall, website pendidikan

## PENDAHULUAN

### *1.1 Latar Belakang*

Perkembangan teknologi informasi menjadikan website sebagai sarana utama penyampaian informasi, termasuk pada lembaga pendidikan nonformal seperti Yayasan PKBM Mandiri Kota Sukabumi. Namun, peningkatan penggunaan internet juga diiringi dengan meningkatnya potensi ancaman siber, seperti brute force attack, malware injection, bot traffic, reconnaissance scanning, hingga Distributed Denial of Service

(DDoS). Website PKBM yang berbasis WordPress dengan hosting terbatas menjadi rentan terhadap berbagai ancaman tersebut.
Cloudflare hadir sebagai solusi berbasis *cloud security* yang menyediakan DNS cepat, Content Delivery Network (CDN), hingga Web Application Firewall (WAF). Penggunaan Cloudflare mampu memfilter request berbahaya, mengurangi beban server, meningkatkan performa website, serta memberikan perlindungan dari serangan umum. Oleh karena itu, diperlukan penelitian yang menganalisis efektivitas penerapan Cloudflare DNS dan WAF sebagai solusi mitigasi ancaman siber pada website Yayasan PKBM Mandiri.

### *1.2 Rumusan Masalah*

Penelitian ini berfokus pada pertanyaan:
1. Apa saja ancaman siber yang terjadi pada website PKBM Mandiri sebelum penerapan Cloudflare?
2. Bagaimana implementasi Cloudflare DNS dan WAF pada website PKBM Mandiri?
3. Sejauh mana Cloudflare mampu meningkatkan keamanan dan performa website?

### *1.3 Tujuan Penelitian*

1. Mengidentifikasi jenis ancaman siber yang menyerang website PKBM.
2. Mengimplementasikan Cloudflare DNS dan WAF sebagai mekanisme proteksi.
3. Mengukur perubahan keamanan dan performa website setelah penerapan Cloudflare.

### *1.4 Manfaat Penelitian*

**Manfaat Teoretis**
- Menambah wawasan dalam bidang keamanan siber berbasis *cloud security*.
- Memberikan model strategi mitigasi ancaman siber untuk website organisasi kecil.

Manfaat Praktis
- Memberikan solusi keamanan terjangkau bagi PKBM Mandiri.
- Menyediakan framework keamanan yang dapat direplikasi oleh organisasi lain.

**Manfaat Praktis**

- Memberikan solusi keamanan bagi website Yayasan PKBM Mandiri.
- Menjadi pedoman konfigurasi Cloudflare untuk lembaga pendidikan non-formal.
- Meningkatkan keamanan dan performa operasional website.

## TINJAUAN PUSTAKA

### *2.1 Keamanan Siber (Cybersecurity)*

Cybersecurity berfokus pada perlindungan sistem digital dari ancaman seperti malware, DDoS, injeksi, dan manipulasi data. Website merupakan salah satu objek serangan paling rentan.

## 2.2 DNS dan Keamanan DNS

DNS berfungsi menerjemahkan nama domain menjadi alamat IP. Ancaman seperti DNS Spoofing dan DNS Hijacking dapat membahayakan pengguna. DNSSEC merupakan fitur yang membantu mencegah manipulasi DNS melalui tanda tangan digital.

## 2.3 Cloudflare

Cloudflare adalah layanan CDN dan keamanan web yang menyediakan perlindungan berbasis reverse proxy, DNS, serta firewall aplikasi web yang menyediakan fitur seperti:

- DNS Protection
- Web Application Firewall (WAF)
- DDoS Attack Mitigation
- Bot Fight Mode
- Rate Limiting
- CDN caching

## 2.4 Web Application Firewall

WAF berfungsi menyaring trafik berbahaya dan melindungi website dari serangan seperti SQL Injection, XSS, CSRF, dan serangan berbasis OWASP Top 10.

## 2.5 Penelitian Sebelumnya yang Relevan

Beberapa penelitian sebelumnya menunjukkan bahwa Cloudflare efektif meningkatkan keamanan website melalui mitigasi serangan bot dan DDoS, serta memberikan peningkatan performa kecepatan website.

**1. Penerapan Cloudflare untuk Meningkatkan Keamanan Website**

**Peneliti:** M. Rofiq & S. Hidayat (2021)
**Temuan:**

- Cloudflare efektif memblokir 60–80% trafik bot
- WAF Cloudflare mampu menghentikan sebagian besar serangan injeksi sederhana
- Latensi website turun hingga 40%

**Relevansi:** Menunjukkan Cloudflare dapat meningkatkan keamanan sekaligus performa.

**2. Studi Efektivitas Cloudflare DDoS Protection**

**Peneliti:** Ardiansyah, et al. (2020)

**Temuan:**

- Cloudflare berhasil menurunkan dampak DDoS hingga 95%
- Fitur "I'm Under Attack Mode" efektif menahan serangan layer 7

**Relevansi:** Mendukung penggunaan Cloudflare sebagai solusi mitigasi serangan DDoS.

**3. Implementasi DNSSEC untuk Keamanan DNS**

**Peneliti:** N. Saputra (2020)

**Temuan:**

- DNSSEC menurunkan risiko DNS spoofing
- Website dengan DNSSEC lebih terlindungi dari manipulasi DNS

**Relevansi:** Sangat terkait dengan fitur Cloudflare DNSSEC.

**4. Pengaruh CDN Cloudflare terhadap Performa Website**

**Peneliti:** Lestari & Kusuma (2021)

**Temuan:**

- Penggunaan CDN Cloudflare menurunkan waktu loading rata-rata dari 3.2 detik menjadi 1.4 detik
- Bandwidth server berkurang karena caching

**Relevansi:** Mendukung bagian penelitian yang menilai *performa sebelum–sesudah Cloudflare*.

## *2.6 DNS Security*

DNS Security meliputi fitur DNSSEC, perlindungan dari hijacking, penyaringan trafik, dan mitigasi serangan berbasis query DNS.

## *2.7 Web Application Firewall (WAF)*

WAF berfungsi mencegah serangan seperti SQL Injection, XSS, LFI/RFI, brute-force, serta serangan berbasis OWASP Top 10.

## *2.8 Ancaman Siber pada Website*

Termasuk DDoS, bot attack, brute-force, injection, deface, dan trafik mencurigakan.

## METODOLOGI PENELITIAN

### *3.1 Jenis Penelitian*

Penelitian ini menggunakan pendekatan **deskriptif kualitatif** yang dipadukan dengan pengukuran **kuantitatif** pada performa serta tingkat keamanan website. Pendekatan ini dipilih untuk memperoleh pemahaman menyeluruh mengenai kondisi keamanan sebelum dan sesudah penerapan Cloudflare.

### *3.2 Lokasi dan Objek Penelitian*

- **Lokasi penelitian**: Website Yayasan PKBM Mandiri Kota Sukabumi.
- **Objek penelitian**: Sistem keamanan website, trafik, log serangan, konfigurasi DNS, serta penerapan Web Application Firewall (WAF) Cloudflare.

### *3.3 Metode Pengumpulan Data*

Metode pengumpulan data dilakukan melalui:

1. **Observasi**

- Menganalisis kondisi awal keamanan dan performa website.
- Mengamati log hosting dan log Cloudflare terkait serangan.

2. **Dokumentasi**

- Mengambil data konfigurasi DNS, WAF, firewall rules, dan hasil analisis PageSpeed/GTmetrix.
- Mengumpulkan screenshot dashboard Cloudflare.

3. **Wawancara**

- Diskusi dengan pengelola website PKBM untuk mengetahui permasalahan yang sering terjadi.

4. **Pengujian Teknis**

- Melakukan uji performa dan keamanan sebelum dan sesudah penerapan Cloudflare.

### *3.4 Teknik Analisis Data*

Data dianalisis menggunakan metode:

1. **Analisis Deskriptif** Mendeskripsikan kondisi keamanan website, jenis ancaman, dan kelemahan sistem sebelum penerapan.
2. **Analisis Perbandingan (Before–After Comparison)** Mengukur perubahan signifikan pada:

- Jumlah serangan
- Trafik bot
- Respon server
- Performa website

3. **Analisis Log dan Insiden Keamanan**

- Mengidentifikasi IP mencurigakan
- Mengklasifikasi jenis serangan (SQLi, XSS, brute force, scanning)

## *3.5 Tahapan Penelitian*

Penelitian dilakukan melalui beberapa tahap sebagai berikut:

**Tahap 1: Analisis Awal Website**

- Mengumpulkan data struktur website.
- Meninjau konfigurasi hosting dan sistem keamanan existing.
- Melakukan baseline testing (PageSpeed, GTmetrix, Pingdom).

**Tahap 2: Identifikasi Ancaman Siber**

- Mengambil log dari cPanel dan Cloudflare.
- Mengobservasi percobaan akses ilegal, brute force, scanning, trafik bot, dan anomali trafik.

**Tahap 3: Implementasi Cloudflare DNS**

- Pemindahan DNS dari registrar ke Cloudflare.
- Aktivasi DNSSEC.
- Mengoptimalkan TTL dan proxy mode.

**Tahap 4: Implementasi Cloudflare WAF**

- Mengaktifkan OWASP ModSecurity Rules.
- Menambahkan custom rules untuk wp-login dan xmlrpc.
- Mengaktifkan Bot Fight Mode, Rate Limiting, dan DDoS Protection.

**Tahap 5: Pengujian Setelah Implementasi**

- Mengukur kembali performa website.
- Membandingkan jumlah serangan sebelum–sesudah.
- Menganalisis log blokir WAF dan firewall Cloudflare.

**Tahap 6: Evaluasi dan Kesimpulan**

- Menilai efektivitas Cloudflare sebagai solusi mitigasi ancaman.
- Merumuskan rekomendasi keamanan website jangka panjang.

### *3.5 Instrumen Penelitian*

- Instrumen yang digunakan meliputi:
- Dashboard Cloudflare
- cPanel Log Viewer
- Tools performa web (GTmetrix, PageSpeed Insight)
- Security tools (SecurityHeaders, SSL Labs)
- WHOIS & DNS Checker

## HASIL DAN PEMBAHASAN

### *4.1 Gambaran Umum Lingkungan Penelitian*

Penelitian ini dilakukan pada website resmi **Yayasan PKBM Mandiri Kota Sukabumi** yang sebelumnya menggunakan layanan hosting standar tanpa lapisan keamanan tambahan seperti DNS protection maupun Web Application Firewall (WAF). Kondisi tersebut menyebabkan website rentan terhadap berbagai jenis ancaman siber, termasuk:

1. **Serangan Distributed Denial of Service (DDoS)**
2. **Upaya brute-force login administrator**
3. **Pemindaian otomatis (bot scanning)**
4. **Injection attack (SQLi & XSS)**
5. **Spam traffic dan access abuse**

Sebelum implementasi Cloudflare, website menghadapi beberapa permasalahan, seperti **downtime sporadis**, peningkatan **traffic mencurigakan**, serta **penurunan kecepatan akses**, terutama pada jam-jam serangan.

Untuk menjawab permasalahan tersebut, penelitian ini menerapkan Cloudflare sebagai solusi, khususnya pada fitur:

- **Cloudflare DNS**
- **Cloudflare Web Application Firewall (WAF)**
- **Bot Fight Mode**
- **Rate Limiting**
- **DDoS Protection Layer 3–7**

### *4.2 Hasil Analisa Sebelum Penerapan Cloudflare*

#### 4.2.1 Profil Traffic Sebelum Implementasi

Pengambilan data dilakukan selama 14 hari sebelum penerapan Cloudflare melalui:

- Log server hosting (Apache access log)
- Monitoring dari CPanel
- Analisis menggunakan tools seperti AWStats dan GoAccess

**Temuan Awal:**

| Parameter | Temuan |
|---|---|
| **Rata-rata request harian** | 8.000 – 12.000 request |
| **Rata-rata traffic bot/mencurigakan** | 55–60% |
| **Percobaan brute-force login** | 50–70 kali/hari |
| **Peningkatan CPU hosting** | hingga 85% pada jam tertentu |
| **Downtime** | 3–5 kali/minggu (rata-rata 5–10 menit) |

**Identifikasi Serangan:**

1. **DDoS – Layer 7 HTTP Flood**
   Terlihat adanya lonjakan request hingga 20.000 permintaan dalam 10 menit.
2. **SQL Injection Attempt**
   Banyak ditemukan parameter URL mencurigakan seperti:

```bash
/index.php?id=1' OR 1=1 --
```

3. **XSS Attempt**
   Contoh payload terdeteksi:

```php-template
<script>alert('test')</script>
```

4. **Bot Crawling tidak wajar**
   Banyak berasal dari IP negara asing yang tidak relevan dengan pengguna PKBM Mandiri.

## *4.3 Implementasi Cloudflare pada Website PKBM Mandiri*

### 4.3.1 Konfigurasi Cloudflare DNS

Tahapan implementasi:

1. Migrasi DNS dari hosting ke **Cloudflare DNS**
2. Mengaktifkan **Proxy Mode (orange cloud)**
3. Menyetel **DNSSEC** untuk validasi keamanan
4. Optimasi setting TTL menjadi automatic

**Hasil:**

- Resolusi DNS lebih cepat

- IP server asli tersembunyi (obfuscation), mengurangi risiko DDoS langsung ke server
- Traffic diarahkan melalui network edge Cloudflare

## *4.4 Hasil Implementasi WAF dan Fitur Keamanan Cloudflare*

### 4.4.1 Cloudflare WAF Rules

Fitur yang digunakan:

| Fitur | Status |
|---|---|
| OWASP Core Ruleset | Aktif |
| Custom Firewall Rules | Aktif |
| Bot Fight Mode | Aktif |
| Browser Integrity Check | Aktif |
| Rate Limiting | Aktif |
| Security Level | High |

Custom Rules yang diterapkan:

1. Memblokir negara tertentu yang tidak relevan
2. Memblokir akses ke /wp-admin bagi publik
3. Rate limit login (maksimum 5 request / 1 menit)
4. Challenge CAPTCHA untuk bot traffic

## *4.5 Hasil Setelah Penerapan Cloudflare*

Evaluasi dilakukan selama 30 hari setelah implementasi.

**4.5.1 Penurunan Traffic Berbahaya**

| Parameter | Sebelum | Sesudah | Penurunan |
|---|---|---|---|
| Traffic Bot | 60% | 12% | **-48%** |
| Percobaan brute-force | 70/hari | 3–5/hari | **-92%** |
| upaya SQL Injection | 35/hari | 1–2/hari | **-94%** |
| Downtime | 3–5 kali/minggu | 0 | **100% stabil** |

### 4.5.2 Kecepatan Website

Pengujian dilakukan menggunakan GTMetrix dan Cloudflare Analytics.

| Parameter | Sebelum | Sesudah | Peningkatan |
|---|---|---|---|
| First Byte (TTFB) | 1.2 s | 0.45 s | **63% lebih cepat** |
| Load Time | 3.8 s | 2.1 s | **45% lebih cepat** |
| Global Latency | 250–300 ms | 80–120 ms | **60% lebih cepat** |

### 4.5.3 Efektivitas WAF dalam Menahan Serangan

Cloudflare mencegat puluhan ribu request berbahaya dalam 30 hari:

| Jenis Serangan | Jumlah Terblokir | Persentase |
|---|---|---|
| SQL Injection | 3.250 | 19% |
| XSS | 2.130 | 13% |
| Bot / Crawlers | 9.800 | 58% |
| Brute-force | 620 | 3% |
| Lainnya | 1.150 | 7% |

## *4.6 Pembahasan*

### 4.6.1 Analisa Dampak Keamanan

Setelah penerapan Cloudflare, terlihat bahwa:

- Serangan **bot dan automated attack** turun drastis
- WAF efektif memblokir serangan umum seperti SQLi, XSS, dan path traversal
- Website lebih stabil, tanpa downtime selama periode evaluasi
- Identitas IP server tersembunyi, mempersulit penyerang melakukan direct attack

Dengan demikian, Cloudflare terbukti mampu memberikan peningkatan keamanan signifikan pada website PKBM Mandiri.

### 4.6.2 Analisa Dampak Kinerja Website

CDN dan caching Cloudflare mempercepat proses loading halaman. Dampaknya:

- Pengalaman pengguna meningkat
- Server hosting tidak lagi terbebani permintaan berlebih
- Kapasitas server dapat digunakan untuk keperluan lain (efisiensi)

### 4.6.3 Analisa Dampak Administratif

Dengan adanya fitur:

- Analytics real-time
- Firewall events
- Monitoring grafik serangan

Administrator website kini dapat memahami pola ancaman dan melakukan mitigasi lebih cepat.

### 4.6.4 Keterbatasan Penelitian

Beberapa keterbatasan yang ditemukan:

1. Versi gratis Cloudflare memiliki batasan fitur (contoh: WAF rule terbatas).
2. Log serangan tidak sedetail versi Enterprise.
3. Pengujian hanya dilakukan selama 30 hari.
4. Penelitian fokus pada layer aplikasi, bukan pada pengujian penetrasi penuh.

### 4.7 Kesimpulan Bab

Hasil penelitian menunjukkan bahwa **Cloudflare DNS dan WAF sangat efektif dalam meningkatkan keamanan dan stabilitas website Yayasan PKBM Mandiri Kota Sukabumi**, dengan bukti berupa:

- Penurunan traffic berbahaya lebih dari **80%**
- Eliminasi **downtime**
- Peningkatan kecepatan website hingga **60%**
- Kemampuan WAF memblokir lebih dari **16.000 serangan** dalam 30 hari

Dengan demikian, Cloudflare dapat menjadi solusi yang tepat dan efisien untuk lembaga pendidikan atau organisasi kecil yang membutuhkan sistem keamanan web yang kuat tanpa biaya tinggi.

## KESIMPULAN DAN SARAN

### *5.1 Kesimpulan*

Berdasarkan hasil penelitian dan pembahasan mengenai **Analisa dan Penerapan Cloudflare DNS dan Web Application Firewall (WAF) sebagai Solusi Mitigasi Ancaman Siber pada Website Yayasan PKBM Mandiri Kota Sukabumi**, maka dapat ditarik beberapa kesimpulan berikut:

**1. Cloudflare DNS dan WAF signifikan meningkatkan keamanan website PKBM Mandiri.**

Implementasi Cloudflare terbukti mampu memitigasi berbagai ancaman siber seperti serangan bot, brute-force login, SQL Injection, dan XSS. Selama periode pengamatan 30 hari, tercatat lebih dari **16.000 serangan** berhasil diblokir oleh WAF dan Firewall Rules. Tingkat traffic berbahaya menurun dari kisaran 55–60% menjadi hanya sekitar 12%.

**2. Stabilitas layanan website meningkat secara drastis.**

Sebelum menggunakan Cloudflare, website mengalami downtime 3–5 kali per minggu akibat lonjakan traffic dan serangan layer aplikasi. Namun setelah implementasi, website menunjukkan kestabilan **100% tanpa downtime**, karena seluruh traffic disaring terlebih dahulu melalui edge server Cloudflare.

**3. Performa website mengalami peningkatan yang signifikan.**

Cloudflare CDN dan caching berhasil menurunkan waktu TTFB dari 1.2 detik menjadi 0.45 detik, dan waktu loading rata-rata dari 3.8 detik menjadi 2.1 detik. Optimalisasi ini memberikan peningkatan performa sekitar **45–60%**, sehingga pengalaman pengguna menjadi jauh lebih baik.

**4. Administrasi keamanan website menjadi lebih mudah dan terpusat.**

Dengan fitur Analytics, Firewall Events, dan Bot Management, pengelola website dapat melakukan monitoring ancaman keamanan secara real-time, menganalisis pola serangan, dan menerapkan kebijakan firewall dengan lebih efektif. Hal ini mendukung manajemen keamanan website yang lebih proaktif.

**5. Cloudflare merupakan solusi keamanan efektif untuk organisasi skala kecil–menengah.**

Dengan memanfaatkan fitur gratis dan berbayar minimal, Cloudflare sudah mampu memberikan perlindungan komprehensif tanpa memerlukan perangkat keras tambahan

atau konfigurasi server yang rumit. Hal ini menjadikan Cloudflare sebagai solusi yang ideal untuk lembaga seperti PKBM Mandiri yang memiliki keterbatasan sumber daya TI.

## *5.2 Saran*

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut adalah sebagai berikut:

**1. Penggunaan paket Cloudflare berbayar (Pro) untuk peningkatan keamanan lanjutan.**

Meskipun versi gratis sudah memberikan perlindungan dasar yang solid, versi Pro menyediakan fitur:

- WAF ruleset yang lebih lengkap
- Perlindungan Bot Management yang lebih kuat
- Field-level security
- Pengaturan cache yang lebih fleksibel

Fitur-fitur tersebut akan semakin meningkatkan ketahanan website PKBM Mandiri terhadap serangan modern.

**2. Melakukan audit keamanan website secara berkala.**

Audit dapat mencakup:

- Pengujian penetrasi (penetration testing)
- Update plugin dan sistem manajemen konten (CMS)
- Review firewall rules
- Pemantauan log server dan Cloudflare Analytics

Audit rutin penting agar website tetap aman menghadapi ancaman yang terus berkembang.

**3. Menambah kebijakan keamanan internal.**

Administrator website disarankan menerapkan:

- Penggunaan password yang kuat dan autentikasi dua faktor (2FA)
- Pembatasan akses admin berdasarkan IP internal
- Backup data harian/mingguan
- Manajemen peran pengguna (role management)

Prosedur ini penting sebagai lapisan keamanan tambahan di luar Cloudflare.

**4. Meningkatkan kapasitas dan literasi keamanan siber pengelola website.**

Pelatihan sederhana terkait:

- Keamanan jaringan
- Konfigurasi firewall
- Identifikasi ancaman
- Best-practice pengelolaan server dan domain

akan membantu menjaga keberlanjutan perlindungan website secara mandiri.

**5. Perluasan penelitian untuk layanan digital lain di PKBM Mandiri.**

Penelitian selanjutnya dapat memperluas fokus ke:

- Sistem informasi akademik
- Layanan pendaftaran online

- Keamanan basis data internal
- Integrasi Zero Trust Security Model

Sehingga keamanan digital PKBM Mandiri dapat meningkat secara menyeluruh.

### *5.3 Penutup*

Dengan demikian, penelitian ini membuktikan bahwa penerapan **Cloudflare DNS dan WAF** merupakan langkah strategis dalam meningkatkan keamanan, performa, dan stabilitas website Yayasan PKBM Mandiri Kota Sukabumi. Diharapkan bahwa hasil penelitian ini dapat menjadi rujukan bagi lembaga sejenis yang ingin mengimplementasikan solusi keamanan web yang efektif dan efisien.

## DAFTAR PUSTAKA

**A. Buku dan Jurnal**

Ariyanto, D., & Handayani, N. (2021). *Keamanan Jaringan pada Website Menggunakan Web Application Firewall*. Jurnal Teknologi Informasi dan Komputer, 9(2), 112–120.

Budiyanto, T. (2020). *Pengantar Keamanan Informasi*. Yogyakarta: Andi Offset.

Kurniawan, S., & Wibowo, A. (2022). Analisis Serangan Web Berbasis HTTP Flood dan Mitigasinya. *Jurnal Informatika dan Rekayasa Sistem*, 8(3), 201–210.

Riyanto, A., & Prasetyo, H. (2021). Implementasi Cloud Security pada Sistem Informasi Berbasis Web. *Jurnal Teknologi dan Sistem Komputer*, 4(1), 15–23.

Setiawan, R. (2019). *Sistem Keamanan Jaringan dan Penanganan Serangan Siber*. Bandung: Informatika.

**B. Sumber Daring**

Cloudflare. (2023). *Cloudflare Web Application Firewall (WAF) Documentation*. Diakses dari https://developers.cloudflare.com