LAPORAN AUDIT KEAMANAN WEBSITE

Target Website:

https://kotimkab.go.id

Tanggal Scan:	11 July 2025, 13:30 WIB
Response Code:	200
Response Time:	5.50 detik
Total Vulnerabilities:	2

KAMPANYE KEAMANAN SIBER INDONESIA

Laporan ini merupakan bagian dari Kampanye Keamanan Siber untuk meningkatkan awareness dan implementasi keamanan website pemerintah daerah.

RINGKASAN EKSEKUTIF

Audit keamanan website telah dilakukan terhadap https://kotimkab.go.id pada tanggal 11 July 2025. **Hasil Keseluruhan:** • Total vulnerabilities ditemukan: 2 • Tingkat keamanan: Good (84/100) • SSL/TLS Status: Aktif • Security Headers: 6/7 diimplementasikan **Distribusi Severity:** • High Risk: 0 item • Medium Risk: 2 item • Low Risk: 0 item

Prioritas Tindakan: Disarankan untuk mengatasi vulnerabilities dengan tingkat risiko menengah dalam waktu dekat.

DETAIL VULNERABILITIES

■ MEDIUM RISK VULNERABILITIES

1. **Missing Security Header**
Missing Content-Security-Policy header - Prevents various injection attacks

2. **Exposed File**
Sensitive file accessible: /wp-config.php

TEMUAN TEKNIS

■ SSL/TLS Configuration

SSL Status:	■ Aktif
Certificate Issuer:	GlobalSign nv-sa
Valid Until:	Feb 15 11:21:42 2026 GMT
Cipher Suite:	TLS_AES_256_GCM_SHA384

■■ Security Headers

X-Frame-Options	■ Implemented	SAMEORIGIN
X-Content-Type-Options	■ Implemented	nosniff
X-XSS-Protection	■ Implemented	1; mode=block
Strict-Transport-Security	■ Implemented	max-age=63072000; includeSubDomains; preload
Content-Security-Policy	■ Missing	Not Set
Referrer-Policy	■ Implemented	strict-origin-when-cross-origin
Permissions-Policy	■ Implemented	accelerometer=(), camera=(), gyroscope=(), magneto

■■ Server Information

Server:	nginx
Powered By:	Unknown
Technology Stack:	Nginx

REKOMENDASI PERBAIKAN

■ PRIORITAS MEDIUM

1. **Server Configuration**
Hide server version information to prevent information disclosure

■ PRIORITAS LOW

1. **Content Security**
Implement Content Security Policy (CSP) headers

2. **Monitoring**
Set up security monitoring and logging for suspicious activities

■ TIMELINE IMPLEMENTASI

Prioritas Tinggi: 1-2 minggu • Implementasi SSL/TLS jika belum ada • Perbaikan vulnerability dengan risiko tinggi **Prioritas Menengah:** 1-2 bulan • Implementasi security headers • Perbaikan konfigurasi server **Prioritas Rendah:** 2-6 bulan • Optimisasi tambahan • Monitoring dan maintenance rutin

LAMPIRAN

■ External Links Found

Total external links: 115
1. http://tumbangmujam-kotim.desa.id
2. http://rasautumbuh-kotim.desa.id/
3. http://regeilestari-kotim.desa.id
4. http://pundu-kotim.desa.id
5. https://play.google.com/store/apps/details?id=com.gismarttax
6. http://simpur-kotim.desa.id/
7. http://soren-kotim.desa.id/
8. http://tanjungharapan-kotim.desa.id
9. http://parit-kotim.desa.id/
10. http://tehang-kotim.desa.id
... dan 105 link lainnya

TENTANG SCAN INI

Scan keamanan ini menggunakan Website Security Scanner yang dikembangkan khusus untuk Kampanye Keamanan Siber Indonesia. Scanner ini melakukan pemeriksaan otomatis terhadap: • Konfigurasi SSL/TLS • Security headers HTTP • Informasi server yang terekspos • Vulnerability umum (directory traversal, SQL injection) • Analisis form dan CSRF protection • Directory listing dan file backup yang terekspos **Disclaimer:** Hasil scan ini bersifat informatif dan tidak menggantikan audit keamanan profesional yang komprehensif. Disarankan untuk melakukan penetration testing oleh ahli keamanan siber untuk analisis yang lebih mendalam.