Website Security Analysis Report

Analysis Overview

URL Analyzed:	https://www.whitesharkmedia.com/
Analysis Date:	July 29, 2025 at 08:50 PM
Analysis Status:	SUCCESSFUL

MALWARE DETECTED

Severity Level: HIGH

Indicators:

• Found 2 suspicious pattern(s)

Network Information

IP Address:	172.67.75.58
ASN:	13335
ASN Description:	CLOUDFLARENET, US
Country:	US
Description:	Cloudflare, Inc.
CIDR:	172.64.0.0/13

Domain Information

SSL/TLS Security

TLS Version:	TLSv1.3
Certificate Type:	DV
Subject:	whitesharkmedia.com
Certificate Authority (CA):	WE1
	Google Trust Services
	US
Valid From:	Jul 3 20:19:57 2025 GMT
Valid Until:	Oct 1 21:19:50 2025 GMT
Serial Number:	83F4BC914F5F265D0D5AC7A73E2989FE

Content Management System

CMS Detected:	WordPress
Plugins Found:	3 plugins
	• cookie-notice
	• gravityformsrecaptcha
	• gravityforms

Security Headers

Missing Headers:

FAILED: Strict-Transport-Security

FAILED: X-Content-Type-Options

FAILED: X-Frame-Options

FAILED: X-XSS-Protection

FAILED: Referrer-Policy

FAILED: Content-Security-Policy

FAILED: Permissions-Policy

FAILED: Cross-Origin-Embedder-Policy

FAILED: Cross-Origin-Opener-Policy

FAILED: Cross-Origin-Resource-Policy

WordPress Security Analysis

XMLRPC.php Test:	PASSED
	Reason: XMLRPC.php is properly protected (HTTP 403)
	HTTP Status: 403
WP-Login.php Test:	PASSED
	Reason: WP-Login page is not accessible (HTTP 403)
	HTTP Status: 403
User Enumeration Test:	FAILED
	Reason: User enumeration is possible via WordPress REST API

Blocklisting Status

Overall Status: CLEAN

Services Checked: 2

Google Safe Browsing

Status: CLEAN

Message: Domain is not blocklisted by Google Safe Browsing

Details: No threats detected

VirusTotal

Status: CLEAN

Message: Domain is clean according to 0 scanners

Details: No threats detected by any security scanner

DNS Records

A Records (IPv4):	172.67.75.58, 104.26.13.162, 104.26.12.162

HTTP Headers

Header	Value
Date	Tue, 29 Jul 2025 20:49:53 GMT
Content-Type	text/html; charset=UTF-8
Transfer-Encoding	chunked
Connection	keep-alive
Server	cloudflare
Vary	Accept-Encoding, Accept-Encoding
Cache-Control	public, max-age=3600, s-maxage=3600
Expires	Wed, 11 Jan 1984 05:00:00 GMT
Cf-Edge-Cache	cache,platform=wordpress
X-Xss-Protection	1; mode=block
X-Httpd	1
Host-Header	8441280b0c35cbc1147f8ba998a563a7
X-Proxy-Cache	HIT
Report-To	{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=DyklL0kUJHrxY7yu43RCkRvW%2BnzIifM17e
Cf-Cache-Status	DYNAMIC
Nel	{"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Content-Encoding	gzip
CF-RAY	966f7c46eb196bce-DFW