

Website Security Analysis Report

Analysis Overview

URL Analyzed:	https://cyber-forensics.pl/
Analysis Date:	October 28, 2025 at 07:20 PM
Analysis Status:	SUCCESSFUL

MALWARE DETECTED

Severity Level: **MEDIUM**

Indicators:

- Found 1 suspicious pattern(s)
- Found 1 SEO spam pattern(s)

Network Information

IP Address:	172.67.165.141
ASN:	13335
ASN Description:	CLOUDFLARENET, US
Country:	US
Description:	Cloudflare, Inc.
CIDR:	172.64.0.0/13

Domain Information

Registrar:	OVH SAS
------------	---------

Created:	2020-05-27T15:03:52
Expires:	2026-05-27T15:03:52
Last Updated:	2025-04-08T21:18:25
Name Servers:	dilbert.ns.cloudflare.com, liv.ns.cloudflare.com

SSL/TLS Security

TLS Version:	TLSv1.3
Certificate Type:	DV
Subject:	cyber-forensics.pl
Certificate Authority (CA):	WE1
	Google Trust Services
	US
Valid From:	Oct 12 15:50:08 2025 GMT
Valid Until:	Jan 10 16:48:44 2026 GMT
Serial Number:	A3767E896BBD1143112BF510B9BE3506

Content Management System

CMS Detected:	WordPress
Active Theme:	forensic_new
Plugins Found:	8 plugins
	• add-to-any
	• contact-form-7
	• cookie-law-info
	• google-analytics-for-wordpress

	• highlighting-code-block
	... and 3 more

Security Headers

Present Headers:

PASSED: Strict-Transport-Security

Missing Headers:

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:	FAILED
	Reason: XMLRPC.php is accessible and vulnerable
	HTTP Status: 200
WP-Login.php Test:	PASSED
	Reason: WP-Login page has CAPTCHA protection: recaptcha, simple_captcha, custom_captcha
	HTTP Status: 200
User Enumeration Test:	PASSED
	Reason: User enumeration is properly protected

Blocklisting Status

Overall Status: CLEAN

Services Checked: 2

VirusTotal

Status: CLEAN

Message: Domain is clean according to 0 scanners

Details: No threats detected by any security scanner

Google Safe Browsing

Status: CLEAN

Message: Domain is not blocklisted by Google Safe Browsing

Details: No threats detected

DNS Records

A Records (IPv4):	104.21.42.195, 172.67.165.141
WWW Records:	www.cyber-forensics.pl (A): 104.21.42.195, www.cyber-forensics.pl (A): 172.67.165.141

HTTP Headers

Header	Value
nel	{"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
date	Tue, 28 Oct 2025 19:20:52 GMT
link	<https://cyber-forensics.pl/wp-json/>; rel="https://api.w.org/", <https://cyber-forensics.pl/wp-json/wp/v2/pages/2>; rel="alternate"; title="JSON"; type="application/json", <https://cyber-forensics.pl/>; rel=shortlink

vary	accept-encoding
cf-ray	995cca2c1eb0c1-ATL
pragma	no-cache
server	cloudflare
alt-svc	h3=":443"; ma=86400
expires	Sat, 26 Jul 1997 05:00:00 GMT
report-to	{ "group": "cf-nel", "max_age": 604800, "endpoints": [{ "url": "https://a.nel.cloudflare.com/report/v4?s=t2ikzuo3o2Oo2utjEqAObvGMloq0Ubakzg9toz" }] }
set-cookie	ip2location_redirection_first_visit=1761679251%3B1665b19714a5f1b36cc3466fbb00199d; HttpOnly; Secure; Path=/; Max-Age=86400; Expires=Wed, 29 Oct 2025 19:20:51 GMT
content-type	text/html; charset=UTF-8
http_version	HTTP/2
cache-control	max-age=0, no-cache, no-store, must-revalidate
last-modified	Tue, 28 Oct 2025 19:20:51 GMT
cf-cache-status	DYNAMIC
content-encoding	gzip
strict-transport-security	max-age=31536000; includeSubDomains; preload

Generated by Website Security Analyzer

Report generated on October 30, 2025 at 06:31 AM