

Website Security Analysis Report

Analysis Overview

URL Analyzed:	https://cultureally.org
Analysis Date:	January 08, 2026 at 10:52 PM
Analysis Status:	SUCCESSFUL

MALWARE DETECTED

Severity Level: HIGH

Indicators:

- Found 3 suspicious pattern(s)

Network Information

IP Address:	162.159.134.42
ASN:	13335
ASN Description:	CLOUDFLARENET, US
Country:	US
Description:	Cloudflare, Inc.
CIDR:	162.158.0.0/15

Domain Information

Registrar:	TUCOWS DOMAINS, INC.
------------	----------------------

Created:	2020-11-01T23:12:00
Expires:	2026-11-01T23:12:00
Last Updated:	2025-10-23T00:13:27
Status:	['clientTransferProhibited', https://icann.org/epp#clientTransferProhibited', 'clientUpdateProhibited', https://icann.org/epp#clientUpdateProhibited']
Name Servers:	ns-1293.awsdns-33.org, ns-1668.awsdns-16.co.uk, ns-381.awsdns-47.com, ns-549.awsdns-04.net

SSL/TLS Security

TLS Version:	TLSv1.3
Certificate Type:	DV
Subject:	cultureally.org
Certificate Authority (CA):	WE1
	Google Trust Services
	US
Valid From:	Dec 21 10:18:30 2025 GMT
Valid Until:	Mar 21 11:18:27 2026 GMT
Serial Number:	BB901C5EFB58AE8A0EBDAEC2CBC97100

Content Management System

CMS Detected:	WordPress
Active Theme:	edumall
Plugins Found:	22 plugins
	• bdthemes-element-pack-lite

	• beauty-gravity
	• buddypress
	• buttonizer-multifunctional-button
	• cleantalk-spam-protect
	... and 17 more

Security Headers

Present Headers:

PASSED: Referrer-Policy

PASSED: X-Frame-Options

PASSED: X-XSS-Protection

PASSED: Permissions-Policy

PASSED: X-Content-Type-Options

PASSED: Content-Security-Policy

PASSED: Strict-Transport-Security

PASSED: Cross-Origin-Opener-Policy

PASSED: Cross-Origin-Embedder-Policy

PASSED: 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:	FAILED
	Reason: WP-Login page is accessible without CAPTCHA protection
	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):	162.159.134.42
MX Records:	alt3.aspmx.l.google.com. (Priority: 10), alt4.aspmx.l.google.com. (Priority: 10), alt2.aspmx.l.google.com. (Priority: 5), aspmx.l.google.com. (Priority: 1), alt1.aspmx.l.google.com. (Priority: 5)
TXT Records:	"ca3-8f9d50c0eebc4d4f8a253f5e3c0c928b"

Services Detected:

- Google Workspace - Email hosted on Google Workspace
- Google Workspace - Email hosted on Google Workspace
- Google Workspace - Email hosted on Google Workspace
- Google Workspace - Email hosted on Google Workspace
- Google Workspace - Email hosted on Google Workspace

HTTP Headers

Header	Value
nel	{ "success_fraction": 0.01, "report_to": "cf-nel", "max_age": 604800 }
date	Thu, 08 Jan 2026 22:52:48 GMT
link	<https://cultureally.org/wp-json/>; rel="https://api.w.org/", <https://cultureally.org/wp-json/wp/v2/pages/437>; rel="alternate"; title="JSON"; type="application/json", <https://cultureally.org/>; rel=shortlink
vary	Accept-Encoding
cf-ray	9baf446ef9974529-ATL
server	cloudflare
alt-svc	h3=":443"; ma=86400
ki-edge	v=25.0.0;mv=5.0.18
cache-tag	1b4f5638-71a4-4771-902f-6640adea7e92,a6fc88f05f5b8 72c6fbef05b9434f88ed387f4ce4f28ad6300ba4c7ba0c9a129
ki-origin	g1p
report-to	{ "endpoints": [{ "url": "https://a.nel.cloudflare.c om/vreport/v4?s=bkvl7iqF9g8ZQreDK9U6hCzyJv0YNK%2BU1E08FTw2LLHRwh4q mzWJ5
set-cookie	apbct_timestamp=1767910539; path=/; secure; HttpOnly; SameSite=Lax, apbct_site_landing_ts=1767910539; path=/; secure; HttpOnly; SameSite=Lax, apbct_prev_referer=http%3A%2F%2Faio.online; path=/; secure; HttpOnly; SameSite=Lax, apbct_cookies_test=%257B%2522cookies_names%2522%253A%255B%2522apbct_times path=/; secure; HttpOnly; SameSite=Lax, apbct_page_hits=1; path=/; secure; HttpOnly; SameSite=Lax, apbct_site_referer=http%3A%2F%2Faio.online; path=/; secure; HttpOnly; SameSite=Lax, __cf_bm=wyqs_Q9QcF65zxkgly.84V.GwztNFoQxRTEGLq.sKA-1767912768-1.0.1.1-7piW path=/; expires=Thu, 08-Jan-26 23:22:48 GMT; domain=.cultureally.org; HttpOnly; Secure; SameSite=None
content-type	text/html; charset=UTF-8

http_version	HTTP/2
ki-cache-tag	1b4f5638-71a4-4771-902f-6640adea7e92,a6fc88f05f5b872c6fbef05b9434f88ed387f4ce4f28ad6300ba4c7ba0c9a129
cache-control	public, max-age=0, s-maxage=3600
ki-cache-type	Edge
last-modified	Thu, 08 Jan 2026 22:15:40 GMT
x-kinsta-cache	HIT
x-tec-api-root	https://cultureally.org/wp-json/tribe/events/v1/
cf-cache-status	MISS
referrer-policy	strict-origin-when-cross-origin
x-frame-options	SAMEORIGIN
content-encoding	gzip
x-tec-api-origin	https://cultureally.org
x-xss-protection	1; mode=block
x-tec-api-version	v1
ki-cf-cache-status	SAVING
permissions-policy	accelerometer=(), autoplay=(), camera=(), cross-origin-isolated=(), display-capture=(self), encrypted-media=(), fullscreen=*, geolocation=(self), gyroscope=(), keyboard-map=(), magnetometer=(), microphone=(), midi=(), payment=*, picture-in-picture=*, publickey-credentials-get=(), screen-wake-lock=(), sync-xhr=*, usb=(), xr-spatial-tracking=(), gamepad=(), serial=()
x-edge-location-klb	1
x-content-type-options	nosniff
content-security-policy	upgrade-insecure-requests;
strict-transport-security	max-age=63072000
x-content-security-policy	default-src 'self'; img-src *; media-src * data;;
cross-origin-opener-policy	unsafe-none
access-control-allow-headers	Content-Type, Authorization
access-control-allow-methods	GET,POST
cross-origin-embedder-policy	unsafe-none; report-to='default'

cross-origin-resource-policy	cross-origin
x-permitted-cross-domain-policies	none
cross-origin-opener-policy-report-only	unsafe-none; report-to='default'
cross-origin-embedder-policy-report-only	unsafe-none; report-to='default'

Generated by Website Security Analyzer

Report generated on January 09, 2026 at 01:25 PM