CyberSecure-web - Website Security Report

Scanned URL: https://www.linkedin.com/checkpoint/challenge/AgFh-1hRrtSXRAAAAZiInfhiSwGDJn7nHL3U59ZU807zmxi6ts8Ltm69R9H70zyuh9nhvLleSH1qKuyXFLKer8V1zfy-Gg?ut=29N65L0ZlaeHU1
Scan Timestamp: 8/8/2025, 1:08:45 pm

Scan Summary

Vulnerability	Status	Details	Suggestion
Malware Links	No	None	Use malware scanners, remove infected links.
Phishing Pages	No	No additional information	Avoid mimicking login pages; secure forms.
Open Redirects	No	No additional information	Validate redirect URLs server-side.
CMS Vulnerabilities	No	CMS: None, No information available	Update CMS and use plugins for security.
Missing Security Headers	No	None missing	Add CSP, HSTS, and X-Frame-Options headers.
Open Ports	Yes	443, 80	Close/secure unused ports with firewall.
Hidden Scripts	No	None	Audit and clean injected scripts.
DNS Rebinding	Yes	150.171.22.12	Implement DNS hardening (e.g., DNS pinning).

Report generated by CyberSecure-web - Open Source Security Scanner