CyberSecure-web - Website Security Report

Scanned URL: https://www.google.com/search?q=logo+images&rlz=1C1CHBF_enIN1103IN1103&oq=logo&gs_lcrp=EgZjaHJvbWUqDAgBEAAYQxiABBiKBTIRCAAQRRg5GEMYsQMYgAQYigUyDAgBEAAYQxiABBiKBTIPCAIQABhDGLEDGIAEGIoFMg8IAxAAGEMYsQMYgAQYigUyDwgEEAAYQxixAxiABBiKBTIMCAUQABhDGIAEGIoFMg8IBhAAGEMYsQMYgAQYigUyCggHEAAYsQMYgAQyCggIEAAYsQMYgAQyBwgJEAAYgATSAQg5MTIwajBqN6gCALACAA&sourceid=chrome&ie=UTF-8
Scan Timestamp: 8/8/2025, 10:28:53 am

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, CMS not detected	Update CMS and use plugins for security.
Missing Security Headers	Yes	strict-transport-security, x-content-type-options, referrer-policy, permissions-policy	Add CSP, HSTS, and X-Frame-Options headers.
Open Ports	Yes	443, 80	Close/secure unused ports with firewall.
Hidden Scripts	Yes	[object Object], [object Object], [object Object]	Audit and clean injected scripts.
DNS Rebinding	Yes	216.58.200.164	Implement DNS hardening (e.g., DNS pinning).

Report generated by CyberSecure-web - Open Source Security Scanner