CyberSecure-web - Website Security Report

Scanned URL: https://docs.google.com/spreadsheets/d/1n05Wf9hD9KGC_LwmP-rGD5RonmWmF-
KyUukZ1xsjZrY/edit?gid=0#gid=0
Scan Timestamp: 8/8/2025, 12:59:33 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, CMS not detected	Update CMS and use plugins for security.
Missing Security Headers	Yes	x-frame-options, 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]	Audit and clean injected scripts.
DNS Rebinding	Yes	142.250.182.174	Implement DNS hardening (e.g., DNS pinning).