SCANALA
AUTOMATED WEBSITE SECURITY ASSESSMENT

Security Assessment Report

Website Vulnerability Assessment

Prepared for
agmo.ai

Report date: 19 November 2026
Assessment type: Essentials scan (automated, read-only)

CONFIDENTIAL — This report is intended only for the owner of the assessed domain. It documents an automated, outside-in assessment; it is not a substitute for a manual penetration test and cannot determine whether the site has already been compromised.

Document control

VERSION	DATE	DETAIL	AUTHOR
1.0	19 November 2026	Automated assessment generated and released	Scanala

Prepared by	Scanala automated scanner
Assessment method	Automated, read-only (HTTP GET, DNS, TCP connect); CISA KEV cross-reference
Target	agmo.ai

Contents

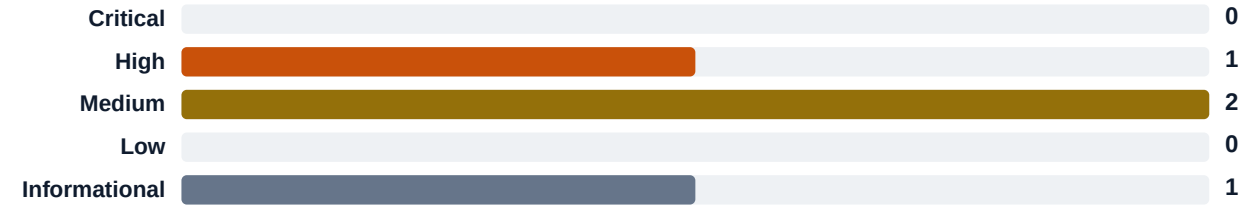
Section I — Executive summary
Section II — Introduction
Section III — Scope & methodology
Section IV — Information gathering
Section V — Findings
Section VI — Checks that passed
Section VII — Appendix: findings by area

Section I — Executive summary

This report documents an automated security assessment of agmo.ai, carried out on 19 November 2026. Several weaknesses were found. Work through the findings from the top.

A total of 4 issue(s) were identified: 0 critical, 1 high, 2 medium, 0 low and 1 informational. The site scored 73/100 (grade C).

NUMBER OF FINDINGS BY RISK LEVEL



SUMMARY OF FINDINGS

SEVERITY	FINDING	STATUS
High	No DMARC record — spoofed emails are not blocked	Open
Medium	HSTS header is missing	Open
Medium	No Content-Security-Policy	Open
Informational	No CAA record	Open

This assessment is a point-in-time snapshot. Security posture changes constantly; monitoring and re-assessment should be an ongoing process.

Section II — Introduction

The owner of agmo.ai proved control of the domain and requested an automated security self-test by Scanala. The objective of this assessment is to detect potential vulnerabilities and weaknesses that are visible from outside the application, and to provide practical remediation guidance.

Section III — Scope & methodology

Only agmo.ai (and its www/non-www twin) was assessed, after ownership was verified. All checks are read-only — HTTP GET requests, DNS lookups and TCP connects. No passwords were tried, no forms were submitted, and no vulnerability was exploited. Detected software is cross-referenced against the CISA Known Exploited Vulnerabilities catalogue. Social engineering, denial-of-service and testing of systems outside the named target are out of scope.

RISK LEVEL RATINGS

LEVEL	DESCRIPTION
Critical	Direct, immediate risk of compromise or data loss. Remediate today.
High	Significant impact to confidentiality, integrity or availability. Remediate this week.
Medium	Substantial weakness that should be fixed promptly.
Low	Noticeable weakness; fix as part of normal maintenance.
Informational	For awareness; no direct risk on its own.

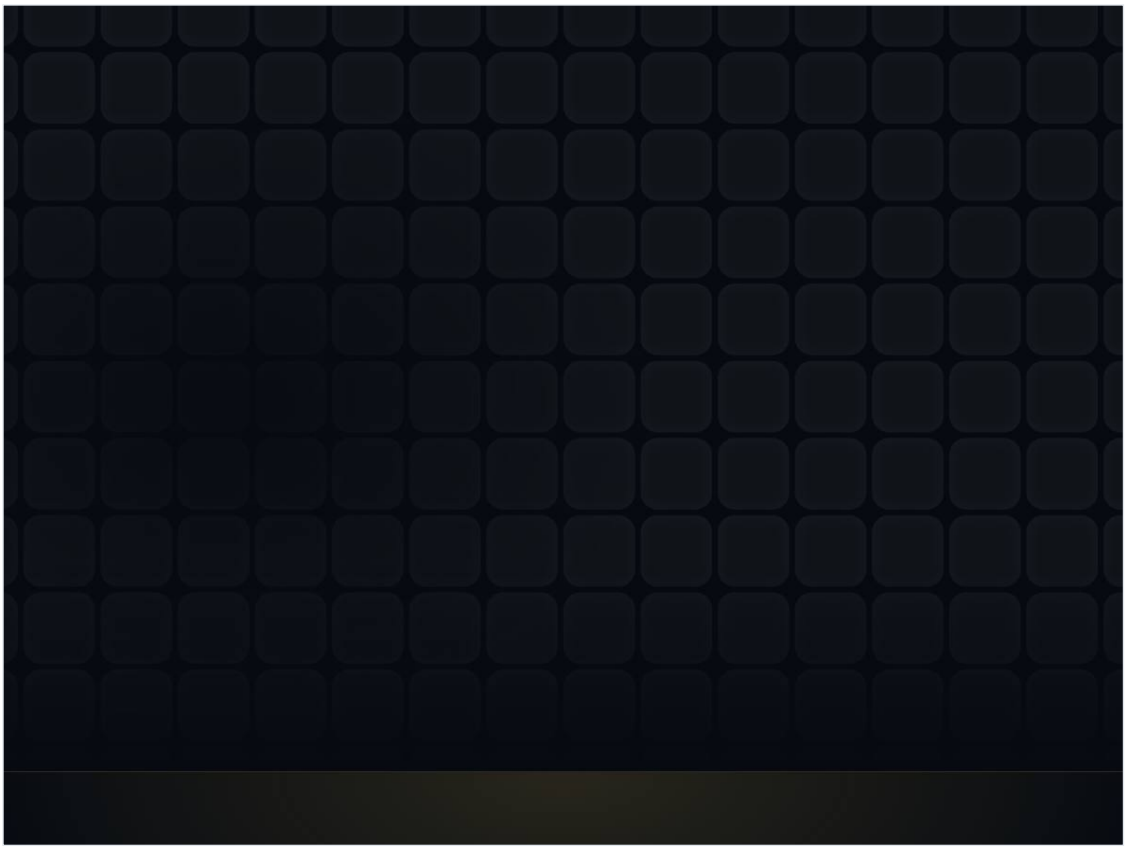
OWASP TOP 10 REFERENCE

CATEGORY	DESCRIPTION
A01 Broken Access Control	Users can act outside their intended permissions.
A02 Cryptographic Failures	Sensitive data exposed through weak or missing encryption.
A03 Injection	Untrusted input is run as a command or query (SQLi, XSS).
A05 Security Misconfiguration	Insecure defaults, exposed files, missing hardening.
A06 Vulnerable & Outdated Components	Known-vulnerable software, libraries or plugins in use.
A07 Identification & Authentication Failures	Weaknesses in login, sessions or account handling.

Section IV — Information gathering

Target	agmo.ai
IP address(es)	172.67.134.139, 104.21.6.60
Server / CDN	cloudflare
Protocol	HTTPS
Page title	Agmo AI | Malaysia's Premier AI Software Powerhouse
Technologies	None fingerprinted

HOMEPAGE AT TIME OF SCAN



Section V — Findings (4)

HIGH

I. No DMARC record — spoofed emails are not blocked

DNS & email spoofing · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION

Fake emails that appear to come from your own domain are the main tool for invoice and bank-transfer fraud against SMEs. DMARC tells Gmail, Outlook and others to reject messages that fail SPF/DKIM checks, and sends you reports of who is abusing your domain.

OBSERVATIONS

No TXT record at _dmarc.agmo.ai

IMPLICATION

Email spoofing enabling phishing and invoice/payment fraud.

RECOMMENDATION

Add a TXT record at _dmarc.agmo.ai: "v=DMARC1; p=quarantine; rua=mailto:dmarc@agmo.ai". Start with p=none for two weeks if unsure, then tighten to quarantine and reject.

MEDIUM

II. HSTS header is missing

HTTPS & certificates · OWASP A02 Cryptographic Failures · Status: Open

DESCRIPTION

Without HSTS, an attacker on public Wi-Fi can silently downgrade a visitor to the unencrypted site on their first request.

IMPLICATION

Information disclosure; traffic interception or tampering.

RECOMMENDATION

Send the header: Strict-Transport-Security: max-age=31536000; includeSubDomains

MEDIUM

III. No Content-Security-Policy

Browser security headers · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION

A Content-Security-Policy limits which scripts the browser will run. Without one, any injected script (for example card-skimming code added after a hack) runs with no restriction.

IMPLICATION

Client-side attack exposure (cross-site scripting, clickjacking, session theft).

RECOMMENDATION

Start with a report-only policy to see what would break, then enforce it. A reasonable start: default-src 'self'; plus the specific script/CDN hosts the site uses.

INFORMATIONAL

IV. No CAA record

DNS & email spoofing · OWASP A05 Security Misconfiguration · Status: Open

DESCRIPTION

A CAA record limits which certificate authorities may issue certificates for your domain.

IMPLICATION

Email spoofing enabling phishing and invoice/payment fraud.

RECOMMENDATION

Optional hardening: add a CAA record naming your certificate provider, e.g. 0 issue "letsencrypt.org".

Section VI — Checks that passed (10)

- **Site is reachable over HTTPS**
  Traffic between visitors and your site is encrypted.
- **HTTP redirects to HTTPS**
  Visitors who type the plain http:// address are sent to the secure version.
- **Clickjacking protection is set**
  Other websites cannot load your pages in a hidden frame to trick your users into clicking.
- **MIME sniffing is disabled**
  Browsers will not second-guess file types, so an uploaded file cannot be treated as a script.
- **CORS does not trust arbitrary websites**
  Other websites cannot read your site's responses on behalf of your logged-in users.
- **Certificate is valid (issued by Google Trust Services)**
  The TLS certificate is trusted by browsers and has not expired.

' **Only modern TLS is accepted (TLSv1.3)**
Obsolete TLS 1.0/1.1 are refused; only current, secure protocols are allowed.

' **SPF record is published**
Receiving mail servers can check which servers are allowed to send email as your domain.

' **No dangling subdomains among common names**
No common subdomain points to a deleted service that someone could take over.

' **No database or remote-desktop ports exposed**
Databases and remote-access services are not reachable from the internet.

Section VII — Appendix: findings by area

DNS & email spoofing

- High — No DMARC record — spoofed emails are not blocked
- Informational — No CAA record

HTTPS & certificates

- Medium — HSTS header is missing

Browser security headers

- Medium — No Content-Security-Policy

UPGRADE

Get the full picture with a Full Scan

This report is a free Essentials scan of agmo.ai. It covers the outside-facing basics, but the issues that most often lead to a breach — downloadable config files, outdated software and vulnerable components — are only checked on a Full Scan.

A FULL SCAN ADDS

- Exposed .env, config & app-settings files
- Backups, database dumps & .git folders
- Directory listing & debug pages
- WordPress / Joomla core & plugin versions
- End-of-life PHP, server & JS libraries
- Risky components (file managers, Telerik…)

$9.99

per scan · no subscription

Log in to Scanala, open this domain and choose “Run Full Scan”.