Ainex Preliminary Security Report

AI-assisted external security posture assessment

Risk 100 • critical

TARGET	GENERATED	SCAN TYPE	ESTIMATED DURATION
https://gmolx.com/	26 Mar 2026, 00:58	AI-assisted preliminary external assessment	38s

EXECUTIVE SUMMARY

Preliminary external signals indicate a mixed security posture with several hardening opportunities. Prioritize high-impact control gaps and validate fixes with a full technical assessment.

PRIORITY ACTION PLAN

RANK	FINDING	WHY NOW	EXPECTED RISK REDUCTION
#1	HSTS header	Address hsts header to reduce exploitable exposure and improve defensive posture.	Reduced attack surface and improved audit readiness.
#2	Content Security Policy	Address content security policy to reduce exploitable exposure and improve defensive posture.	Reduced attack surface and improved audit readiness.
#3	X-Content-Type-Options	Address x-content-type-options to reduce exploitable exposure and improve defensive posture.	Reduced attack surface and improved audit readiness.
#4	Clickjacking protections (X-Frame-Options / frame-ancestors)	Address clickjacking protections (x-frame-options / frame-ancestors) to reduce exploitable exposure and improve defensive posture.	Reduced attack surface and improved audit readiness.
#5	Referrer-Policy	Address referrer-policy to reduce exploitable exposure and improve defensive posture.	Reduced attack surface and improved audit readiness.

FINDINGS REGISTER

SEVERITY	FINDING	BUSINESS IMPACT	QUICK REMEDIATION
MEDIUM	**HSTS header** Surface: Headers • CVSS-like 5.5	May weaken baseline hardening and increase exploitability over time.	Set Strict-Transport-Security with max-age >= 15552000 (180 days) and includeSubDomains where applicable.
MEDIUM	**Content Security Policy** Surface: Headers • CVSS-like 5.5	May weaken baseline hardening and increase exploitability over time.	Implement a strict Content-Security-Policy, minimize unsafe-inline/unsafe-eval, and define least-privilege sources.
LOW	**X-Content-Type-Options** Surface: Headers • CVSS-like 3.2	May weaken baseline hardening and increase exploitability over time.	Add X-Content-Type-Options: nosniff to reduce MIME confusion attacks.

SEVERITY	FINDING	BUSINESS IMPACT	QUICK REMEDIATION
MEDIUM	**Clickjacking protections (X-Frame-Options / frame-ancestors)** Surface: Headers • CVSS-like 5.5	May weaken baseline hardening and increase exploitability over time.	Use CSP frame-ancestors and/or X-Frame-Options DENY/SAMEORIGIN.
LOW	**Referrer-Policy** Surface: Headers • CVSS-like 3.2	May weaken baseline hardening and increase exploitability over time.	Set Referrer-Policy (e.g. strict-origin-when-cross-origin).
LOW	**Permissions-Policy** Surface: Headers • CVSS-like 3.2	May weaken baseline hardening and increase exploitability over time.	Declare Permissions-Policy to limit unnecessary browser capabilities.
MEDIUM	**Server/framework fingerprint leakage** Surface: Exposure • CVSS-like 5.5	May weaken baseline hardening and increase exploitability over time.	Reduce version and framework fingerprint leakage in response headers.
MEDIUM	**Cookie security flags** Surface: Session • CVSS-like 5.5	May weaken baseline hardening and increase exploitability over time.	Ensure session cookies use Secure, HttpOnly, and SameSite attributes with shortest feasible lifetime.

CONTROL SNAPSHOT (NON-PASS)

CATEGORY	CHECK	STATUS	EVIDENCE
Headers	HSTS header	WARN	Header not observed
Headers	Content Security Policy	WARN	Header not observed
Headers	X-Content-Type-Options	WARN	Header not observed
Headers	Clickjacking protections (X-Frame-Options / frame-ancestors)	WARN	No clickjacking control header observed
Headers	Referrer-Policy	WARN	Header not observed
Headers	Permissions-Policy	WARN	Header not observed
Exposure	Server/framework fingerprint leakage	WARN	server=nginx, x-powered-by=n/a
Session	Cookie security flags	WARN	Secure=false, HttpOnly=true, SameSite=true
Browser isolation	Cross-origin isolation policies (COOP/CORP)	WARN	COOP=n/a, CORP=n/a
Security operations	security.txt disclosure channel	WARN	No security.txt found at /.well-known/security.txt

COMPLIANCE MAPPING

FRAMEWORK	MAPPED CONTROLS
SOC2	CC6.1 Logical and access controls • CC7.1 Vulnerability identification and response
ISO27001	A.8 Asset and configuration controls • A.8.23 Web filtering / network protections
PCI_DSS	Req 2 Secure configurations • Req 6 Secure systems and software
GDPR	Art. 32 Security of processing

LIMITATIONS

- Assessment is based on externally observable responses only.
- No authenticated, source-code, or internal network testing was performed.

NEXT STEPS

- Prioritize and remediate critical/high findings within the next sprint.
- Run a full authenticated application and infrastructure assessment.
- Map remediation evidence to compliance controls for audit readiness.