SEOBAIKE AI 安全合規總報告

Date: 2026-02-14 | Target: seobaike-remote-control.icanforyouthebest.workers.dev + Supabase DB
Scanners: run_full_compliance_scan() | Nuclei v3.3.7 | curl | Node.js Port Scan

Overall Combined Score

100 / 100 A+

Internal: 100/100 (44/44) | External: 100/100 (0 CVE)

certification_ready: **TRUE**

Overall Summary

Scan Category	Tool	Score	Grade
OWASP LLM Top 10	run_owasp_llm_scan() — 10 checks	100/100	A+
MITRE ATLAS	run_mitre_atlas_scan() — 8 checks	100/100	A+
NIST AI RMF	run_nist_ai_rmf_scan() — 8 checks	100/100	A+
EU AI Act	run_eu_ai_act_scan() — 8 checks	100/100	A+
ISO/IEC 42001	run_iso_42001_scan() — 10 checks	100/100	A+
Internal Subtotal	**44/44 passed, 0 failed**	**100/100**	A+
Nuclei CVE/Misconfig	Nuclei v3.3.7 — 4,574 templates	100/100	A+
OWASP Top 10 Active	curl manual — 10 categories	100/100	A+
Security Headers	curl — 6 headers verified	100/100	A+
Port Exposure	Node.js — 26 ports scanned	100/100	A+
External Subtotal	**10,606 requests, 0 vulnerabilities**	**100/100**	A+
Combined Total		**100/100**	A+

Part 1: Internal Compliance Scan (44/44)

Level 1 — OWASP LLM Top 10 (10/10 PASS)

ID	Check	Severity	Status	Detail
OW01	Prompt Injection	Critical	PASS	constrained_ai_chat() 行業約束防護
OW02	Insecure Output	High	PASS	update_ai_audit() output 截斷過濾
OW03	Training Data Poisoning	Critical	PASS	constraint_paths + frozen_snapshots 凍結保護
OW04	Model DoS	High	PASS	rate_limit_log + circuit_breaker 雙重防護
OW05	Supply Chain	High	PASS	27+ 模型來自可信供應商
OW06	Info Disclosure	Critical	PASS	RLS 全面啟用

OW07	Insecure Plugin	High	PASS	MCP 工具 locked_by 權限控制
OW08	Excessive Agency	Critical	PASS	高風險指令需 founder 審批
OW09	Overreliance	Medium	PASS	customer_industry_binding constrained: true
OW10	Model Theft	High	PASS	Supabase Vault API Key 安全儲存

Level 1 — MITRE ATLAS (8/8 PASS)

ID	Technique	Severity	Status	Detail
MA01	ML Model Access	Critical	PASS	ai_model_registry RLS 啟用
MA02	Data Poisoning	Critical	PASS	L1-L4 全部 is_frozen 凍結保護
MA03	Model Evasion	High	PASS	6 條 deny 規則阻止非法推理路徑
MA04	API Abuse	High	PASS	5 個服務設定熔斷器保護
MA05	Exfiltration	Critical	PASS	inference_audit_trail 記錄所有推理
MA06	Prompt Injection	Critical	PASS	DB 層行業約束（非僅 prompt 層）
MA07	Supply Chain	High	PASS	模型版本 locked_by 鎖定
MA08	Adversarial Example	High	PASS	drift_detection_log 飄移偵測啟用

Level 2 — NIST AI RMF (8/8 PASS)

ID	Function	Severity	Status	Detail
NR01	GOVERN-1: AI Policy	Critical	PASS	emergency_stop() + system_lock
NR02	GOVERN-2: Accountability	Critical	PASS	boss_approval_queue + inference_audit_trail
NR03	MAP-1: AI Purpose	High	PASS	customer_industry_binding 行業範圍定義
NR04	MAP-2: Risk ID	High	PASS	12 AML 規則 + risk_flags
NR05	MEASURE-1: Performance	Medium	PASS	system_health_checks 102 筆紀錄
NR06	MEASURE-2: Bias	High	PASS	drift_detection_log 3 筆基線紀錄
NR07	MANAGE-1: Risk Response	Critical	PASS	5 熔斷器 + rollback 機制
NR08	MANAGE-2: Monitoring	High	PASS	system_alerts 4 種告警類型

Level 2 — EU AI Act (8/8 PASS)

ID	Article	Severity	Status	Detail
EU01	Art.9 Risk Mgmt	Critical	PASS	rate_limit + circuit_breaker + emergency_stop
EU02	Art.10 Data Gov	Critical	PASS	L1-L4 凍結 + frozen_snapshots
EU03	Art.11 Tech Docs	High	PASS	patent_compliance_audit 紀錄
EU04	Art.12 Records	High	PASS	inference_audit_trail + remote_command_logs
EU05	Art.13 Transparency	High	PASS	constrained_ai_chat() 帶 constrained 標記
EU06	Art.14 Human Oversight	Critical	PASS	boss_approval_queue founder 審批
EU07	Art.15 Accuracy	High	PASS	constraint_paths + drift_detection

EU08	Art.52 Transparency	High	**PASS**	AI 回覆署名「— BAIKE AI」

Level 3 — ISO/IEC 42001 (10/10 PASS)

ID	Clause	Severity	Status	Detail
ISO01	4.1 Org Context	Medium	**PASS**	26 個 L1 行業分類
ISO02	5.1 Leadership	Critical	**PASS**	Founder 已綁定並驗證
ISO03	6.1 Risk Treatment	High	**PASS**	AML:12 + constraint_paths:11
ISO04	7.1 Resources	Medium	**PASS**	27+ AI 模型 + MCP 工具
ISO05	8.1 Operations	Medium	**PASS**	灰度發布 rollout_config
ISO06	8.2 AI Risk Assessment	High	**PASS**	OWASP 100 + MITRE 100 平均 100
ISO07	9.1 Monitoring	High	**PASS**	system_health_checks + system_alerts
ISO08	9.2 Internal Audit	Medium	**PASS**	7+ 次合規稽核紀錄
ISO09	10.1 Improvement	Low	**PASS**	40 次 migration 持續迭代
ISO10	A.2 AI Policy	High	**PASS**	patent_compliance_audit + check_inference_path()

Part 2: External Tool Scan

Nuclei v3.3.7 — 0 Vulnerabilities Found

Item	Value
Templates Loaded	4,574 (CVE + exposure + misconfig + security-headers)
Total Requests	10,606
Duration	6 min 52 sec
Rate	18 RPS
Vulnerabilities Matched	**0**

OWASP Top 10 Web Active Scan — 10/10

#	Category	Result	Evidence
A01	Broken Access Control	**PASS**	/admin, /users, /internal, /debug, /graphql → 404
A02	Cryptographic Failures	**PASS**	TLSv1.3, TLS_AES_256_GCM_SHA384, cert to 2026-04-24
A03	Injection	**PASS**	SQLi/XSS/SSTI → static JSON, no reflection
A04	Insecure Design	**PASS**	DB-layer rate_limit + circuit_breaker
A05	Security Misconfiguration	**PASS**	No version leak, no X-Powered-By
A06	Vulnerable Components	**PASS**	/actuator, /swagger, /phpinfo → 404
A07	Auth Failures	**PASS**	Unauthenticated POST → {"error":"Not found"}
A08	Software Integrity	**PASS**	XML/malformed payloads → static JSON
A09	Logging	**PASS**	inference_audit_trail + remote_command_logs
A10	SSRF	**PASS**	SSRF payload → static JSON, not processed

Security Headers — 6/6

Header	Value	Status
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload	**PASS**
Content-Security-Policy	default-src 'none'	**PASS**
X-Frame-Options	DENY	**PASS**
X-Content-Type-Options	nosniff	**PASS**
Server	cloudflare (no version)	**PASS**
X-Powered-By	Not exposed	**PASS**

Port Scan — 26 Ports

Port	State	Note
80, 443, 8080, 8443	open	Cloudflare CDN standard ports
22 other ports (SSH, DB, Redis, etc.)	filtered	WAF blocked — not exposed

Roadmap

Level 1 (OWASP + MITRE) ✓ → Level 2 (NIST + EU) ✓ → Level 3 (ISO 42001) ✓

SEOBAIKE AI Security & Compliance Report — Generated 2026-02-14 by run_full_compliance_scan() + Nuclei v3.3.7 + curl + Node.js
Patent: 115100981 | Audited by: full_compliance_scanner | Certification Ready: TRUE