DI - ASH AI Pentest Platform

CONFIDENTIAL - FEBRUARY 11, 2026

AI-Assisted Pentesting Platform for Ali & Sons

Executive overview: current architecture, security readiness, posture/compliance reporting, and 90-day path to production-grade maturity.

Prepared for Senior Management & CISO

WHY THIS PLATFORM

Business Value

Faster

Automates scan execution, report creation, and evidence capture.

Clearer

Converts technical findings into management-readable risk narratives.

Local

Runs AI analysis engine locally for better data sovereignty posture.

> "From scan output to decision-ready risk report in one platform, with consistent governance language."

Strategic objective: accelerate security assurance lifecycle

CURRENT ARCHITECTURE

How It Works Today

Core Components

- Frontend dashboard (search, new scan, history, reports, AI chat)
- FastAPI backend (authentication, orchestration, reporting)
- Scanner engines: Nuclei, Nikto, SQLMap, Katana
- Local AI engine: llama.cpp + GGUF model
- SQLite persistence and HTML report artifacts

Delivery Outputs

- Combined report for full stakeholder alignment
- Executive report for business-level risk view
- Technical report with evidence and remediation
- Compliance summary report with framework mapping and remediation appendix
- Chat-based explanation of findings by scan ID and security topic

Operational model: internal deployment with local toolchain

SECURITY POSTURE

Strengths in Current Build

Engine Depth

Multiple scanners provide broader coverage than single-tool workflow.

Risk Translation

Findings include business impact and remediation guidance.

Operational Resilience

Timeout controls, stop actions, and AI fallback responses implemented.

Implemented Controls

- Role-aware authentication + bcrypt password hashing
- Security headers: CSP, X-Frame-Options, nosniff, HSTS on HTTPS
- Step-up password verification for sensitive scan/report actions
- Per-tool subprocess controls with progress tracking
- Structured reporting outputs aligned for leadership, technical, and compliance stakeholders

Recent Delivered Improvements

- SQLMap reliability hardening with preflight and multi-variant discovery (http/https + apex/www).
- System-wide SQLMap heuristic false-positive suppression and cleaner Nikto warning handling.
- Executive high-level findings table now aligns to full finding counts for consistency.
- Dashboard posture heat map and dedicated compliance report card with framework mapping.
- Light-mode login/loading/dragon and report-selection UX polish for professional presentation quality.

Current risk posture: suitable for controlled internal operation

GAPS TO CLOSE

Pre-Production Hardening Priorities

Priority 1 (Immediate)

- Remove bootstrap/default admin credential behavior
- Restrict CORS to trusted origins only
- Run backend in production profile (disable reload)
- Enforce TLS reverse proxy and internal network controls

Priority 2 (30-60 days)

- RBAC (analyst/lead/admin)
- Login rate limit and lockout controls
- Enhanced immutable audit trail
- Backup and restore drill for reports/data/logs

Security confidence increases significantly after these controls

COMPLIANCE ALIGNMENT

Applicable Standards for Ali & Sons

- **ISO 27001:** Risk treatment, controls governance, evidence readiness
- **SOC 2:** Security monitoring and assurance evidence mapping
- **NIST:** Testing methodology and control-centric remediation alignment

- **OWASP + CIS Controls:** Application and baseline hardening alignment
- **UAE IAS:** Regional governance and expected security controls
- Platform reports can be positioned as evidence support artifacts

Alignment is practical and audit-friendly when governance process is enforced

OPERATING MODEL

Recommended Governance Rhythm

Daily

- Health checks
- Scan failure triage
- Report QA spot checks

Weekly

- Template and tool updates
- Risk trend review
- Backlog remediation sync

Monthly

- Control review with leadership
- KPI presentation
- Retest evidence validation

Objective: predictable security assurance cycle

ROADMAP

90-Day Execution Plan

0-30 Days

- Hardening baseline controls
- CISO sign-off criteria definition
- Operational playbook finalization

31-60 Days

- RBAC and audit model rollout
- Management KPI dashboard version 1
- Compliance evidence review cadence

61-90 Days

- Production readiness review
- Disaster recovery simulation
- Formal handover to steady-state operations

Outcome: scalable, governable, leadership-trusted security platform

DECISION SLIDE

Decision Request to Leadership

> Approve phased productionization of the AI Pentest Platform with a security-hardening sprint first, followed by governance and scale controls.

Investment

Low-to-moderate incremental effort (hardening + governance)

Return

Improved risk visibility, faster remediation, stronger audit readiness

Risk if delayed

Slower detection-to-action cycle and weaker executive visibility

Thank you. Q&A ready.