

# Supabash Audit (Readiness) Report

**Target:** localhost

**Assessment Type:** Supabash Audit (Readiness)

**Run Type:** ai-audit

**Compliance Profile:** ISO/IEC 27001

**Compliance Focus:** Information security controls with structured evidence of vulnerability management and secure configuration.

## Run Info

- started\_at: 2026-02-06 21:28:28 UTC
- finished\_at: 2026-02-06 21:32:59 UTC

## Table of Contents

- [Summary](#)
- [Methodology](#)
- [Scope & Assumptions](#)
- [Compliance Coverage Matrix](#)
- [Evidence Pack](#)
- [Agentic Expansion](#)
- [Findings Overview](#)
- [Findings \(Detailed\)](#)
- [Tools Run](#)
- [Commands Executed](#)

## Summary

The assessment of localhost identified multiple open application and database ports but no confirmed exploitable vulnerabilities or misconfigurations based on the automated tooling executed.

## Notes

- ffuf fallback (after gobuster failure) ran and found 0 paths across 1 target(s): http://localhost:33425 (0).

## LLM Usage

- total\_tokens=4605
- cost\_usd=0.010656
- provider=openai
- model=gpt-5.1

## Findings

- **LOW** Multiple application and service ports exposed on localhost
- Evidence: Nmap detected open ports including 3000 (ppp), 4000 (remoteanything), 5050 (mmcc), 5432 (PostgreSQL 9.6.0+), 6379 (Redis 6.2.11), 8080 (http-proxy), 9090/19090 (Golang net/http), 33425/3947/42901/9840 (Node.js Express), 9100 (jetdirect), and others (34403, 52550).
- Recommendation: Review which services must be reachable and restrict unnecessary ports using host-based firewall rules; ensure all exposed services are authenticated, patched, and bound to appropriate interfaces (e.g., localhost-only for development) in line with ISO/IEC 27001 access control and network security controls.

## Methodology

- Baseline: deterministic evidence collection with scope controls and safe defaults.
- Agentic expansion: tool-calling planner proposes additional evidence collection within allowed scope.
- Compliance profile: ISO/IEC 27001
- Compliance focus: Information security controls with structured evidence of vulnerability management and secure configuration.

## Scope & Assumptions

- In scope: localhost, http://localhost:33425, http://localhost:19090, http://localhost:3947, http://localhost:9840, http://localhost:8080, http://localhost:42901, http://localhost:9090
- Authentication context: unauthenticated network/web checks unless explicitly configured otherwise.
- Control mapping note: mapped controls indicate potential relevance and require manual validation.
- Localhost limitation: this run cannot validate external exposure paths or network segmentation boundaries.
- Out of scope: independent attestation/certification decisions and control operation effectiveness testing.

## Compliance Coverage Matrix

Control Area	Status	Evidence Source	Notes
Asset Discovery & Service Mapping	Covered	nmap, httpx, whatweb	based on successful tool runs
Technical Vulnerability Management	Partial	nuclei, ffuf	failed: gobuster (Error: the server returns a status code that matches the provided opt...); skipped: sqlmap (No parameterized URL provided (include '?' in target URL))
Cryptographic Safeguard Review	Partial	nmap	skipped: sslscan (No TLS candidate ports detected from discovery)
Access Management Exposure Review	Partial	supabase_audit	based on successful tool runs

- Status legend: Covered = all mapped checks succeeded, Partial = some succeeded, Not Assessed = no successful mapped checks.

## Evidence Pack

- directory: evidence/ai-audit-iso-20260206-222828
- manifest: evidence/ai-audit-iso-20260206-222828/manifest.json
- artifact\_count: 14

## Runtime Metadata

- python\_version: 3.14.2
- platform: Linux-5.15.153.1-microsoft-standard-WSL2-x86\_64-with-glibc2.39
- llm\_providers: openai
- llm\_models: gpt-5.1

## Tool Versions

- dnsenum: 1.2.6
- ffuf: 2.1.0-dev
- gobuster: 3.6
- httpx: v1.8.1
- katana: v1.3.0
- nmap: 7.94SVN
- nuclei: v2.9.8
- sqlmap: 1.8.4#stable
- sslscan: 2.1.2
- whatweb: 0.5.5
- wpscan: 3.8.28

## Agentic Expansion

- phase: baseline+agentic
- baseline\_finished\_at: 2026-02-06 21:32:51 UTC
- max\_actions: 10
- notes: Planner proposed only baseline-completed web actions; stopping agentic loop.
- planner: tool\_calling

# Findings Overview

## Summary (LLM)

Severity	Count
CRITICAL	0
HIGH	0
MEDIUM	0
LOW	1
INFO	0

## Detailed (Tools)

Severity	Count
CRITICAL	0
HIGH	0
MEDIUM	0
LOW	0
INFO	19

## Risk Normalization

- Promoted in summary risk synthesis: LOW+1
- Reduced in summary risk synthesis: INFO-19
- Basis: LLM summary may aggregate multiple low-signal findings into higher-level operational risk statements.

## Normalization Details

- LOW Multiple application and service ports exposed on localhost
- Derived via: rule:data\_store\_exposure\_aggregation (ports: 5432, 6379); rule:web\_surface\_aggregation (ports: 3947, 8080, 9090, 9840, 19090, 33425, 42901)

# Findings (Detailed)

Note: 10 repeated INFO findings were deduplicated for readability.

- **INFO** Open port 3000/tcp (nmap)
- Evidence: ppp
- **INFO** Open port 3947/tcp (nmap)
- Evidence: http Node.js Express framework
- **INFO** Open port 4000/tcp (nmap)
- Evidence: remoteanything
- **INFO** Open port 5050/tcp (nmap)
- Evidence: mmcc
- **INFO** Open port 5432/tcp (nmap)
- Evidence: postgresql PostgreSQL DB 9.6.0 or later
- **INFO** Open port 6379/tcp (nmap)
- Evidence: redis Redis key-value store 6.2.11
- **INFO** Open port 8080/tcp (nmap)
- Evidence: http-proxy
- **INFO** Open port 9090/tcp (nmap)
- Evidence: http Golang net/http server
- **INFO** Open port 9100/tcp (nmap)
- Evidence: jetdirect
- **INFO** Open port 9840/tcp (nmap)
- Evidence: http Node.js Express framework

- **INFO** Open port 19090/tcp (nmap)
- Evidence: http Golang net/http server
- **INFO** Open port 33425/tcp (nmap)
- Evidence: http Node.js Express framework
- **INFO** Open port 34403/tcp (nmap)
- Evidence: unknown
- **INFO** Open port 42901/tcp (nmap)
- Evidence: http Node.js Express framework
- **INFO** Open port 52550/tcp (nmap)
- Evidence: unknown
- **INFO** Tech stack detected (whatweb)
- Evidence: Country, IP, X-Powered-By
- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:33425
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:33425
- Compliance Mapping: Potential Gap: ISO/IEC 27001 A.8.9 (Configuration Management) (mapping confidence: medium)
- **INFO** CAA Record (nuclei)
- Evidence: localhost

## Tools Run

Tool	Status	Command
nmap	success	nmap localhost -oX - -sV --script ssl-enum-ciphers -p-
httpx	success	/usr/local/bin/httpx -silent -json -l /tmp/supabash-httpx-scf_i72v/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects
whatweb	success	whatweb http://localhost:33425 --log-json -
wpscan	skipped	
nuclei	success	nuclei -u http://localhost:33425 -jsonl -rate-limit 100
gobuster	failed	gobuster dir -u http://localhost:33425 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error
ffuf	success	ffuf -u http://localhost:33425/FUZZ -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -of json -o - -mc 200,204,301,302,307,401,403 -ac
katana	skipped	
dnsenum	skipped	
ssllscan	skipped	
enum4linux-ng	skipped	
sqlmap	skipped	
searchsploit	skipped	
supabase_audit	success	supabase_audit

## Tool Notes

- **wpscan**: SKIPPED - WordPress not detected by whatweb
- **gobuster**: FAILED - Error: the server returns a status code that matches the provided options for non existing urls. http://localhost:33425/29148848-c6cb-4c6e-bf5a-39dad65755b5 => 401 (Length: 12). To continue please exclude the status code or the length
- **katana**: SKIPPED - Disabled by config (tools.enabled=false)
- **dnsenum**: SKIPPED - Localhost/loopback target (DNS enumeration N/A)
- **ssllscan**: SKIPPED - No TLS candidate ports detected from discovery

- **enum4linux-ng**: SKIPPED - No SMB ports detected (139/445)
- **sqlmap**: SKIPPED - No parameterized URL provided (include '?' in target URL)
- **searchsploit**: SKIPPED - Disabled by config (tools..enabled=false)

## Commands Executed

- **nmap**: nmap localhost -oX - -sV --script ssl-enum-ciphers -p-
- **httpx**: /usr/local/bin/httpx -silent -json -l /tmp/supabash-httpx-scf\_i72v/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects
- **whatweb**: whatweb http://localhost:33425 --log-json -
- **nuclei**: nuclei -u http://localhost:33425 -jsonl -rate-limit 100
- **gobuster**: gobuster dir -u http://localhost:33425 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error
- **ffuf**: ffuf -u http://localhost:33425/FUZZ -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -of json -o - -mc 200,204,301,302,307,401,403 -ac
- **supabase\_audit**: supabase\_audit