Supabash Audit (Readiness) Report

Target: localhost
Assessment Type: Supabash Audit (Readiness)
Run Type: ai-audit
Compliance Profile: SOC 2 Type II
Compliance Focus: Security and availability controls with evidence of exposure management and vulnerability assessment.

Run Info

- started_at: 2026-02-06 20:55:33 UTC
- finished_at: 2026-02-06 20:59:56 UTC

Table of Contents

Summary

Automated scanning of localhost identified multiple open application and database ports but no exploitable vulnerabilities or misconfigurations based on the tools and scope used. All recorded items are informational exposure of services rather than confirmed security issues.

Notes

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

LLM Usage

- total_tokens=4337
- cost_usd=0.007906
- provider=openai
- model=gpt-5.1

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: SOC 2 Type II
- Compliance focus: Security and availability controls with evidence of exposure management and vulnerability assessment.

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
Security Surface Inventory	Covered	nmap, httpx, whatweb	based on successful tool runs
Vulnerability & Misconfiguration Checks	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))
Encryption/Transport Control Review	Partial	nmap	skipped: sslscan (No TLS candidate ports detected from discovery)
Access Control 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-soc2-20260206-215533`
- manifest: `evidence/ai-audit-soc2-20260206-215533/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 20:59:49 UTC
- max_actions: 10
- notes: Planner proposed only baseline-completed web actions; stopping agentic loop.
- planner: tool_calling

Findings Overview

Severity	Count
CRITICAL	0
HIGH	0
MEDIUM	0

Severity	Count
LOW	0
INFO	19

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: SOC 2 CC8.1 (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-64h7f2x9/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	

Tool	Status	Command
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	
sslscan	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:33425/1a0c17c9-f966-4f8a-8c3d-300f9ebdbb86 => 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)
- **sslscan**: 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-64h7f2x9/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`