Supabash Audit (Readiness) Report

Target: localhost
Assessment Type: Supabash Audit (Readiness)
Run Type: ai-audit
Compliance Profile: PCI-DSS 4.0
Compliance Focus: Cardholder data environment controls with emphasis on strong cryptography and vulnerability management.

Run Info

- started_at: 2026-02-06 21:23:38 UTC
- finished_at: 2026-02-06 21:28:09 UTC

Table of Contents

Summary

The scan of localhost identified multiple open application and database ports but no confirmed vulnerabilities or misconfigurations; all findings are informational and relate to exposed services only.

LLM Usage

- total_tokens=4509
- cost_usd=0.011201
- provider=openai
- model=gpt-5.1

Findings

- **LOW** Multiple application and infrastructure services exposed on localhost
- Evidence: Open TCP ports include: 19090 (HTTP Golang net/http), 3000 (ppp), 33425/3947/42901/9840 (HTTP Node.js Express), 4000 (remoteanything), 5050 (mmcc), 8080 (http-proxy), 9090 (HTTP Golang net/http), 9100 (jetdirect), 5432 (PostgreSQL 9.6.0+), 6379 (Redis 6.2.11), 34403 and 52550 (unknown).
- Recommendation: Restrict network exposure of non-essential services using host-based firewalls or security groups; ensure that PostgreSQL, Redis, and HTTP services are bound only to trusted interfaces, require strong authentication, and are patched regularly. For unknown or unused services (e.g., ports 34403 and 52550), either disable them or document and secure them according to PCI-DSS requirements for system hardening and service minimization.

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: PCI-DSS 4.0
- Compliance focus: Cardholder data environment controls with emphasis on strong cryptography and vulnerability management.

Scope & Assumptions

- In scope: localhost, http://localhost:19090, http://localhost:33425, http://localhost:42901, http://localhost:3947, http://localhost:9840, http://localhost:8080, 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.
- PCI scope caveat: this run does not confirm whether services store/process/transmit CHD or SAD.
- Out of scope: independent attestation/certification decisions and control operation effectiveness testing.

Compliance Coverage Matrix

Control Area	Status	Evidence Source	Notes
CDE Asset & Service Inventory	Covered	nmap, httpx, whatweb	based on successful tool runs
Vulnerability Discovery & Exposure Checks	Partial	nuclei, gobuster	skipped: sqlmap (No parameterized URL provided (include '?' in target URL))
Transport Security 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-pci-20260206-222338`
- manifest: `evidence/ai-audit-pci-20260206-222338/manifest.json`
- artifact_count: 13

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
- `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 21:28:00 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	18

Risk Normalization

- Promoted in summary risk synthesis: LOW+1
- Reduced in summary risk synthesis: INFO-18
- Basis: LLM summary may aggregate multiple low-signal findings into higher-level operational risk statements.

Normalization Details

- LOW Multiple application and infrastructure services 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); rule:unclassified_service_aggregation (ports: 34403, 52550)

Findings (Detailed)

Note: 9 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, UncommonHeaders
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:19090
- Compliance Mapping: Potential Gap: PCI-DSS 4.0 Req 2 (Secure Configurations) (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-yqbpvt2m/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
whatweb	success	`whatweb http://localhost:19090 --log-json -`
wpscan	skipped	
nuclei	success	`nuclei -u http://localhost:19090 -jsonl -rate-limit 100`
gobuster	success	`gobuster dir -u http://localhost:19090 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
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
- **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-yqbpvt2m/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
- **whatweb**: `whatweb http://localhost:19090 --log-json -`
- **nuclei**: `nuclei -u http://localhost:19090 -jsonl -rate-limit 100`
- **gobuster**: `gobuster dir -u http://localhost:19090 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
- **supabase_audit**: `supabase_audit`