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: 2026-02-08 14:15:11 UTC
- finished_at: 2026-02-08 14:23:02 UTC

Table of Contents

Summary

The localhost environment exposes multiple monitoring and data services without authentication on network-accessible interfaces, creating a risk of configuration disclosure, data access, and lateral movement that is misaligned with SOC 2 expectations for access control and system monitoring. Hardening should focus on restricting network exposure and enforcing authentication on Prometheus, Redis, metrics, and debug endpoints.

Notes

- ffuf fallback (after gobuster failure) ran and found 0 paths across 1 target(s): http://localhost:8080 (0).

LLM Usage

- total_tokens=6273
- cost_usd=0.016915
- provider=openai
- model=gpt-5.1

Findings

- **HIGH** Prometheus configuration API exposed without authentication
- Evidence: Prometheus status/config endpoint is accessible without authentication: http://localhost:9090/api/v1/status/config (HTTP 200, detected by nuclei and readiness_probe).
- Recommendation: Restrict access to the Prometheus UI and API to trusted networks (e.g., bind to localhost or internal subnet, or place behind a reverse proxy/VPN) and enforce authentication/authorization for the web UI and /api/v1/* endpoints. Review the exposed configuration for embedded secrets or internal endpoints and rotate any sensitive values if present.
- **MEDIUM** Prometheus metrics endpoints exposed without authentication
- Evidence: Metrics endpoints are publicly accessible: http://localhost:8080/metrics and http://localhost:9090/metrics (HTTP 200, detected by nuclei and readiness_probe).
- Recommendation: Limit exposure of /metrics endpoints to internal monitoring components only (IP allowlisting, network policies, or service mesh). Where exposure is required, place metrics behind an authenticated proxy or use mTLS between scrapers and targets to prevent unauthorized access and reconnaissance.
- **MEDIUM** Redis service reachable without authentication

- Evidence: redis-cli PING returned PONG for localhost:6379 without providing a password (readiness_probe).
- Recommendation: Enable Redis authentication (requirepass or ACLs) and configure Redis to bind only to localhost or a private network interface. Disable dangerous commands where possible (e.g., CONFIG, FLUSHALL, KEYS) and ensure firewall rules prevent untrusted hosts from reaching port 6379. Rotate any data or credentials that may have been exposed.
- **MEDIUM** Sensitive services listening on wildcard interfaces
- Evidence: ss -lnt shows 0.0.0.0 listeners on ports 5432 (PostgreSQL), 6379 (Redis), 8080 (HTTP proxy/app), 9090 (Prometheus), 9100 (likely node_exporter) (readiness_probe).
- Recommendation: Reconfigure these services to bind only to required interfaces (e.g., 127.0.0.1 or internal VLAN) and enforce host-based firewalls or security groups to restrict inbound access. For databases and monitoring exporters, allow connections only from explicitly authorized application or monitoring hosts.
- **LOW** Go pprof debug endpoint exposed
- Evidence: Go pprof heap debug page is accessible without authentication: http://localhost:9090/debug/pprof/heap?debug=1 (detected by nuclei).
- Recommendation: Disable pprof in production or restrict /debug/pprof/* to trusted operators via network controls and/or authentication. If debugging is required, expose pprof only temporarily or on a separate, access-controlled interface.

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:42567, http://localhost:19090, http://localhost:41175, http://localhost:9923, http://localhost:4876, 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.
- 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, gobuster, ffuf	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`
- manifest: `evidence/manifest.json`
- artifact_count: 25

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: 2026-02-08 14:22:53 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	1
MEDIUM	3
LOW	1
INFO	0

Detailed (Tools)

Severity	Count
CRITICAL	0
HIGH	2
MEDIUM	6
LOW	1
INFO	29

Risk Normalization

- Reduced in summary risk synthesis: HIGH-1, MEDIUM-3, INFO-29
- Basis: LLM summary may aggregate multiple low-signal findings into higher-level operational risk statements.

Normalization Details

- HIGH Prometheus configuration API exposed without authentication
- Derived via: rule:web_surface_aggregation (ports: 4876, 8080, 9090, 9923, 19090, 41175, 42567)
- MEDIUM Prometheus metrics endpoints exposed without authentication
- Derived via: rule:web_surface_aggregation (ports: 4876, 8080, 9090, 9923, 19090, 41175, 42567)

- MEDIUM Redis service reachable without authentication
- Derived via: rule:data_store_exposure_aggregation (ports: 5432, 6379)
- LOW Go pprof debug endpoint exposed
- Derived via: rule:web_surface_aggregation (ports: 4876, 8080, 9090, 9923, 19090, 41175, 42567)

Findings (Detailed)

Note: 32 repeated INFO findings were deduplicated for readability.

- **INFO** Open port 3000/tcp (nmap)
- Evidence: ppp
- **INFO** Open port 4000/tcp (nmap)
- Evidence: remoteanything
- **INFO** Open port 4876/tcp (nmap)
- Evidence: http Node.js Express framework
- **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 9923/tcp (nmap)
- Evidence: http Node.js Express framework
- **INFO** Open port 19090/tcp (nmap)
- Evidence: http Golang net/http server
- **INFO** Open port 25835/tcp (nmap)
- Evidence: unknown
- **INFO** Open port 34155/tcp (nmap)
- Evidence: unknown
- **INFO** Open port 41175/tcp (nmap)
- Evidence: http Node.js Express framework
- **INFO** Open port 42567/tcp (nmap)
- Evidence: http Node.js Express framework
- **INFO** Tech stack detected (whatweb)
- Evidence: Country, HTML5, IP, Title, UncommonHeaders, X-Powered-By
- **INFO** Tech stack detected (whatweb)
- Evidence: Country, IP
- **INFO** Tech stack detected (whatweb)
- Evidence: Country, IP, RedirectLocation
- **INFO** Tech stack detected (whatweb)
- Evidence: Bootstrap, Country, HTML5, IP, JQuery, Script, Title
- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:4876
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:4876
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **INFO** CAA Record (nuclei)
- Evidence: localhost
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **MEDIUM** Prometheus Metrics - Detect (nuclei)
- Evidence: http://localhost:8080/metrics
- Compliance Mapping: Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: high)
- **INFO** Allowed Options Method (nuclei)

- Evidence: http://localhost:8080
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **INFO** FingerprintHub Technology Fingerprint (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **INFO** Allowed Options Method (nuclei)
- Evidence: http://localhost:9090
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **INFO** Prometheus flags API endpoint (nuclei)
- Evidence: http://localhost:9090/api/v1/status/flags
- **LOW** Go pprof Debug Page (nuclei)
- Evidence: http://localhost:9090/debug/pprof/heap?debug=1
- **HIGH** Prometheus Monitoring System - Unauthenticated (nuclei)
- Evidence: http://localhost:9090/api/v1/status/config
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high)
- **MEDIUM** Prometheus Metrics - Detect (nuclei)
- Evidence: http://localhost:9090/metrics
- Compliance Mapping: Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: high)
- **MEDIUM** Sensitive services listening on wildcard interfaces (readiness_probe)
- Evidence: ss -lnt shows wildcard listeners on ports: 5432, 6379, 8080, 9090, 9100
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **MEDIUM** Unauthenticated metrics endpoint accessible (readiness_probe)
- Evidence: http://localhost:8080/metrics (HTTP 200)
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: medium); Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **MEDIUM** Unauthenticated metrics endpoint accessible (readiness_probe)
- Evidence: http://localhost:9090/metrics (HTTP 200)
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: medium); Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **HIGH** Prometheus config endpoint accessible without authentication (readiness_probe)
- Evidence: http://localhost:9090/api/v1/status/config (HTTP 200)
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high); Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **MEDIUM** Redis reachable without authentication (readiness_probe)
- Evidence: redis-cli PING returned PONG for localhost:6379
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high)

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-r5_bq6o3/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
whatweb	success	`whatweb http://localhost:4876 --log-json -`
whatweb	success	`whatweb http://localhost:8080 --log-json -`
whatweb	success	`whatweb http://localhost:9090 --log-json -`
wpscan	skipped	

Tool	Status	Command
wpscan	skipped	
wpscan	skipped	
nuclei	success	`nuclei -u http://localhost:4876 -jsonl -rate-limit 100`
nuclei	success	`nuclei -u http://localhost:8080 -jsonl -rate-limit 100`
nuclei	success	`nuclei -u http://localhost:9090 -jsonl -rate-limit 100`
gobuster	success	`gobuster dir -u http://localhost:4876 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
gobuster	success	`gobuster dir -u http://localhost:9090 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
gobuster	failed	`gobuster dir -u http://localhost:8080 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
ffuf	success	`ffuf -u http://localhost:8080/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	
katana	skipped	
katana	skipped	
dnsenum	skipped	
sslscan	skipped	
enum4linux-ng	skipped	
sqlmap	skipped	
searchsploit	skipped	
supabase_audit	success	`supabase_audit`
readiness_probe	success	`internal readiness probes`

Tool Notes

- **wpscan**: SKIPPED - WordPress not detected by whatweb
- **wpscan**: SKIPPED - WordPress not detected by whatweb
- **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:8080/abc094d1-0411-4eef-a46f-546530464f4a => 501 (Length: 191). To continue please exclude the status code or the length
- **katana**: SKIPPED - Disabled by config (tools..enabled=false)
- **katana**: SKIPPED - Disabled by config (tools..enabled=false)
- **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-r5_bq6o3/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
- **whatweb**: `whatweb http://localhost:4876 --log-json -`

- **whatweb**: `whatweb http://localhost:8080 --log-json -`
- **whatweb**: `whatweb http://localhost:9090 --log-json -`
- **nuclei**: `nuclei -u http://localhost:4876 -jsonl -rate-limit 100`
- **nuclei**: `nuclei -u http://localhost:8080 -jsonl -rate-limit 100`
- **nuclei**: `nuclei -u http://localhost:9090 -jsonl -rate-limit 100`
- **gobuster**: `gobuster dir -u http://localhost:4876 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
- **gobuster**: `gobuster dir -u http://localhost:9090 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
- **gobuster**: `gobuster dir -u http://localhost:8080 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
- **ffuf**: `ffuf -u http://localhost:8080/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`
- **readiness_probe**: `internal readiness probes`