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 10:33:11 UTC
- finished_at: 2026-02-08 10:37:41 UTC

Table of Contents

Summary

No critical, high, medium, or low-severity vulnerabilities were identified on localhost; the assessment primarily observed multiple open application and database service ports. These exposures are informational in this context but would require hardening and access controls in a production or internet-exposed environment.

Notes

- ffuf fallback (after gobuster failure) ran and found 0 paths across 1 target(s): http://localhost:42567 (0).

LLM Usage

- total_tokens=5002
- cost_usd=0.014635
- provider=openai
- model=gpt-5.1

Findings

- **LOW** Multiple application services exposed on non-standard HTTP ports
- Evidence: Open HTTP services detected on ports 19090 (Golang net/http), 41175 (Node.js Express), 42567 (Node.js Express), 4876 (Node.js Express), 8080 (http-proxy), 9090 (Golang net/http), and 9923 (Node.js Express) via nmap service detection.
- Recommendation: Restrict access to these application ports using host-based firewalls or network security groups, exposing only required ports to untrusted networks. Ensure each service enforces authentication, TLS (where applicable), and least-privilege access, and avoid leaving development or admin interfaces reachable from broader networks.
- **LOW** Database service PostgreSQL exposed on default port
- Evidence: nmap identified port 5432/tcp open running "postgresql PostgreSQL DB 9.6.0 or later".
- Recommendation: Limit PostgreSQL exposure to trusted subnets or localhost only, enforce strong authentication and TLS, and ensure pg_hba.conf is configured to restrict client sources. In production, avoid exposing 5432 directly to the internet and place the database behind an application or VPN layer.
- **LOW** Redis key-value store exposed on default port
- Evidence: nmap identified port 6379/tcp open running "redis Redis key-value store 6.2.11".

- Recommendation: Bind Redis to localhost or a private network interface only, and protect access with network controls (firewall, security groups, or VPN). Enable Redis AUTH (or equivalent access control), disable dangerous commands where possible, and avoid exposing port 6379 to untrusted networks.
- **LOW** Unidentified TCP services on high ports
- Evidence: nmap reported open ports 25835/tcp and 34155/tcp with service "unknown".
- Recommendation: Review host configuration to identify which applications listen on these ports and confirm they are required. If not needed, disable the services or close the ports via firewall; if required, restrict access to trusted sources and ensure the services are patched and authenticated.
- **INFO** Additional non-HTTP services exposed on localhost
- Evidence: nmap detected open ports: 3000/tcp (ppp), 4000/tcp (remoteanything), 5050/tcp (mmcc), 9100/tcp (jetdirect).
- Recommendation: Validate that each exposed service is necessary for the environment. For any non-essential service, stop the service and close the port. For required services, document their purpose, apply vendor hardening guidance, and restrict access to trusted networks only.

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:4876, http://localhost:8080, http://localhost:41175, http://localhost:9923, 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`
- manifest: `evidence/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: 2026-02-08 10:37:36 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	4
INFO	1

Detailed (Tools)

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

Risk Normalization

- Promoted in summary risk synthesis: LOW+4
- 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 services exposed on non-standard HTTP ports
- Derived via: rule:web_surface_aggregation (ports: 4876, 8080, 9090, 9923, 19090, 41175, 42567); rule:unclassified_service_aggregation (ports: 25835, 34155)
- LOW Database service PostgreSQL exposed on default port
- Derived via: rule:data_store_exposure_aggregation (ports: 5432, 6379)
- LOW Redis key-value store exposed on default port

- Derived via: rule:data_store_exposure_aggregation (ports: 5432, 6379)
- LOW Unidentified TCP services on high ports
- Derived via: rule:unclassified_service_aggregation (ports: 25835, 34155)

Findings (Detailed)

Note: 10 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, IP, X-Powered-By
- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:42567
- **INFO** CAA Record (nuclei)
- Evidence: localhost
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:42567
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)

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-h9e0dez4/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
whatweb	success	`whatweb http://localhost:42567 --log-json -`
wpscan	skipped	
nuclei	success	`nuclei -u http://localhost:42567 -jsonl -rate-limit 100`

Tool	Status	Command
gobuster	failed	`gobuster dir -u http://localhost:42567 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
ffuf	success	`ffuf -u http://localhost:42567/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:42567/a520b89d-207d-4e34-af65-14962e30831f => 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-h9e0dez4/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
- **whatweb**: `whatweb http://localhost:42567 --log-json -`
- **nuclei**: `nuclei -u http://localhost:42567 -jsonl -rate-limit 100`
- **gobuster**: `gobuster dir -u http://localhost:42567 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
- **ffuf**: `ffuf -u http://localhost:42567/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`