Supabash Audit Report

Target: localhost
Assessment Type: Supabash Audit
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: 2026-02-14 19:05:38 UTC
- finished_at: 2026-02-14 19:10:41 UTC

Table of Contents

Summary

The localhost environment exposes multiple unauthenticated administrative/metrics endpoints and Supabase secrets, including a service role key, creating immediate risk of full database access, user enumeration, and sensitive configuration disclosure. Several data services (Postgres/Redis/metrics) are reachable and some listen on wildcard interfaces, increasing the attack surface.

Notes

- ffuf fallback (after gobuster failure) ran and found 0 paths across 1 target(s): http://localhost:8080 (0).
- agentic ffuf action(s) ran and found 0 paths across 1 target(s): http://localhost:3001 (0).

LLM Usage

- total_tokens=8211
- cost_usd=0.029976
- provider=openai
- model=gpt-5.2

Findings

- **CRITICAL** Supabase service role key exposed (credential/secrets leakage)
- Evidence: Supabase audit detected service role JWT in content: key=eyJhbG....sig, source=http://localhost:4001
- Recommendation: Rotate the service role key immediately, remove it from any client-accessible responses/assets, and restrict usage to trusted server-side components only.
- **HIGH** Prometheus accessible without authentication (config exposure)
- Evidence: Prometheus config endpoint reachable: http://localhost:9090/api/v1/status/config (HTTP 200); nuclei also flagged unauth Prometheus at the same endpoint
- Recommendation: Require authentication/authorization for Prometheus UI and APIs, and restrict access via firewall/allowlist (bind to localhost or internal network only).

- **HIGH** Supabase REST API accessible without authentication / potential missing RLS
- Evidence: REST endpoint reachable without auth: http://localhost:4001/rest/v1/ (HTTP 200); tool notes 'RLS may be disabled'
- Recommendation: Enable and verify Row Level Security (RLS) on all tables, ensure policies are least-privilege, and require appropriate API keys/JWT auth for data access.
- **HIGH** Unauthenticated Supabase RPC allows user enumeration
- Evidence: RPC callable without auth: http://localhost:4001/rest/v1/rpc/list_users (HTTP 200)
- Recommendation: Restrict RPC execution to authenticated roles, add explicit role checks within functions, and ensure underlying tables/views are protected by RLS/policies.
- **MEDIUM** Unauthenticated metrics endpoints exposed
- Evidence: Metrics accessible: http://localhost:8080/metrics (HTTP 200) and http://localhost:9090/metrics (HTTP 200); nuclei detected Prometheus metrics endpoints
- Recommendation: Protect metrics with authentication and/or network segmentation; avoid exposing metrics publicly as they can leak internal topology, versions, and operational data.
- **MEDIUM** Redis reachable without authentication
- Evidence: readiness_probe: redis-cli PING returned PONG for localhost:6379
- Recommendation: Enable Redis AUTH/ACLs, bind to localhost/internal interfaces, and enforce firewall rules to prevent untrusted network access.
- Compliance Mapping:
    - Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high)
- Mapping Basis: corroborated by readiness_probe findings
- Evidence Artifacts: `evidence/results/025-readiness_probe.json`
- Manifest Reference: `evidence/manifest.json`
- **MEDIUM** Sensitive services listening on wildcard interfaces (increased exposure)
- Evidence: ss -lnt shows wildcard listeners on ports: 5432, 6379, 8080, 9090, 9100
- Recommendation: Bind services to localhost/internal interfaces where possible and enforce host/network firewall policies to limit access to trusted sources only.
- **MEDIUM** Directory listing / sensitive configuration path detected
- Evidence: nuclei: Sensitive Configuration Files Listing - Detect at http://localhost:3001/config/
- Recommendation: Disable directory listing, remove sensitive files from web roots, and restrict access to configuration endpoints/paths.
- **LOW** Go pprof debug endpoint exposed
- Evidence: nuclei: http://localhost:9090/debug/pprof/heap?debug=1
- Recommendation: Disable pprof in production or restrict it to localhost/admin networks with authentication to prevent information leakage and potential DoS vectors.
- **LOW** Supabase anon key exposed in client content
- Evidence:
    - Supabase audit detected anon JWT in content: key=eyJhbG….sig, source=http://localhost:4001
    - supabase_audit: key=eyJhbG….sig, source=http://localhost:4001
- Recommendation: Treat anon keys as public but ensure RLS and policies prevent data exposure; rotate if mistakenly granted elevated privileges and minimize scope/permissions.
- Compliance Mapping:
    - Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: medium)
- Mapping Basis: corroborated by supabase_audit findings
- Evidence Artifacts: `evidence/results/024-supabase_audit.json`
- Manifest Reference: `evidence/manifest.json`

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:19090, http://localhost:44427, http://localhost:5670, http://localhost:4001, http://localhost:44717, http://localhost:9417, http://localhost:8080 ...
- 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	basis=corroborated_findings; based on successful tool runs
Vulnerability & Misconfiguration Checks	Partial	nuclei, gobuster, ffuf	basis=corroborated_findings; skipped: sqlmap (No parameterized URL provided (include '?' in target URL))
Encryption/Transport Control Review	Partial	nmap	basis=corroborated_findings; skipped: sslscan (No TLS candidate ports detected from discovery)
Access Control Exposure Review	Partial	readiness_probe, nuclei, supabase_audit	basis=corroborated_findings; based on successful tool runs

- Status legend: `Covered` = mapped checks succeeded with corroborating evidence, `Partial` = some mapped checks/evidence present, `Not Assessed` = no successful mapped checks or signal was inconclusive.

Not Assessable Automatically

- The following areas require manual validation, process evidence, or third-party assessment:
- Policy design/effectiveness over the audit period (not point-in-time scan evidence).
- Access review governance (JML workflow approvals and periodic recertifications).
- Change management control operation evidence (tickets, approvals, segregation).
- Incident response process effectiveness and tabletop/drill execution records.

Evidence Pack

- directory: `evidence`
- manifest: `evidence/manifest.json`
- artifact_count: 26

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-5.2

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

Reproducibility Trace

- file: `ai-audit-soc2-20260214-200538-replay.json`
- markdown_file: `ai-audit-soc2-20260214-200538-replay.md`
- step_count: 1

- version: 1

LLM Reasoning Trace

- json_file: `ai-audit-soc2-20260214-200538-llm-trace.json`
- markdown_file: `ai-audit-soc2-20260214-200538-llm-trace.md`
- llm_event_count: 5
- decision_steps: 1
- llm_calls: 2
- version: 1
- note: captures explicit planner rationale/messages and decisions; hidden model internals are not included.

Agentic Expansion

- phase: baseline+agentic
- baseline_finished_at: 2026-02-14 19:10:34 UTC
- max_actions: 1
- notes: Only one action proposed (remaining_actions=1). Note: gobuster and nuclei/httpx/whatweb for this target/profile were already run; ffuf provides complementary fuzzing-based discovery not excluded for :3001 in constraints.
- decision_steps: 1
- planner: tool_calling

Decision Trace Highlights

- step 1: executed
- initial_candidate: tool=ffuf target=http://localhost:3001 priority=10
- selected_action: ffuf target=http://localhost:3001

Actions

- ffuf target=http://localhost:3001 profile=compliance_soc2: success
- Rationale: SOC 2 evidence goal: demonstrate ongoing vulnerability assessment and exposure management by validating whether previously identified sensitive areas (e.g., /config/, /README.md, /robots.txt) extend to additional undiscovered unauthenticated endpoints on the primary app. A focused content discovery run on the main web app can uncover admin panels, backups, or configuration artifacts that materially change risk posture and remediation scope.

Findings Overview

Summary (LLM)

Severity	Count
CRITICAL	1
HIGH	3
MEDIUM	4
LOW	2
INFO	0

Detailed (Tools)

Severity	Count
CRITICAL	1
HIGH	5
MEDIUM	8
LOW	2

Severity	Count
INFO	43

Risk Normalization

- Reduced in summary risk synthesis: HIGH-2, MEDIUM-4, INFO-43
- Basis: LLM summary may aggregate multiple low-signal findings into higher-level operational risk statements.

Normalization Details

- CRITICAL Supabase service role key exposed (credential/secrets leakage)
- Derived via: rule:web_surface_aggregation (ports: 3001, 4001, 5670, 8080, 9090, 9417, 19090, 44427)
- HIGH Prometheus accessible without authentication (config exposure)
- Derived via: rule:web_surface_aggregation (ports: 3001, 4001, 5670, 8080, 9090, 9417, 19090, 44427)
- HIGH Supabase REST API accessible without authentication / potential missing RLS
- Derived via: rule:web_surface_aggregation (ports: 3001, 4001, 5670, 8080, 9090, 9417, 19090, 44427)
- HIGH Unauthenticated Supabase RPC allows user enumeration
- Derived via: rule:web_surface_aggregation (ports: 3001, 4001, 5670, 8080, 9090, 9417, 19090, 44427)
- MEDIUM Unauthenticated metrics endpoints exposed
- Derived via: rule:web_surface_aggregation (ports: 3001, 4001, 5670, 8080, 9090, 9417, 19090, 44427)
- MEDIUM Sensitive services listening on wildcard interfaces (increased exposure)
- Derived via: rule:llm_risk_synthesis (aggregated from 59 tool findings)
- MEDIUM Directory listing / sensitive configuration path detected
- Derived via: rule:web_surface_aggregation (ports: 3001, 4001, 5670, 8080, 9090, 9417, 19090, 44427)
- LOW Go pprof debug endpoint exposed
- Derived via: rule:web_surface_aggregation (ports: 3001, 4001, 5670, 8080, 9090, 9417, 19090, 44427)

Findings (Detailed)

Note: 34 repeated INFO findings were deduplicated for readability.

Correlated Signals

- **MEDIUM** Prometheus Metrics - Detect: 2 correlated observations across 2 distinct evidence entries; tools=nuclei.
- **MEDIUM** Unauthenticated metrics endpoint accessible: 2 correlated observations across 2 distinct evidence entries; tools=readiness_probe.
- **INFO** Allowed Options Method: 2 correlated observations across 2 distinct evidence entries; tools=nuclei.
- **INFO** FingerprintHub Technology Fingerprint: 2 correlated observations across 2 distinct evidence entries; tools=nuclei.
- **INFO** HTTP Missing Security Headers: 3 correlated observations across 3 distinct evidence entries; tools=nuclei.
- **INFO** Missing Cookie SameSite Strict: 2 correlated observations across 2 distinct evidence entries; tools=nuclei.
- **INFO** Tech stack detected: 5 correlated observations across 5 distinct evidence entries; tools=whatweb.
- **INFO** Wappalyzer Technology Detection: 3 correlated observations across 3 distinct evidence entries; tools=nuclei.
- **INFO** Open port 3000/tcp (nmap)
- Evidence: ppp
- **INFO** Open port 3001/tcp (nmap)
- Evidence: http Apache httpd 2.4.25
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 3002/tcp (nmap)
- Evidence: exlm-agent
- **INFO** Open port 4000/tcp (nmap)
- Evidence: tcpwrapped
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 4001/tcp (nmap)
- Evidence: http nginx 1.29.4
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 5050/tcp (nmap)
- Evidence: mmcc

- **INFO** Open port 5432/tcp (nmap)
- Evidence: postgresql PostgreSQL DB 9.6.0 or later
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: medium); Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: medium)
- **INFO** Open port 5670/tcp (nmap)
- Evidence: http Node.js Express framework
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 6379/tcp (nmap)
- Evidence: redis Redis key-value store 6.2.11
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: medium); Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: medium)
- **INFO** Open port 8080/tcp (nmap)
- Evidence: http-proxy
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 9090/tcp (nmap)
- Evidence: http Golang net/http server
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 9100/tcp (nmap)
- Evidence: jetdirect
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 9417/tcp (nmap)
- Evidence: http Node.js Express framework
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 19090/tcp (nmap)
- Evidence: http Golang net/http server
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 34547/tcp (nmap)
- Evidence: unknown
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 44427/tcp (nmap)
- Evidence: http Node.js Express framework
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 44717/tcp (nmap)
- Evidence: http Node.js Express framework
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Open port 51414/tcp (nmap)
- Evidence: unknown
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Tech stack detected (whatweb)
- Evidence: Apache, Cookies, Country, HTTPServer, IP, RedirectLocation
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low)
- **INFO** Tech stack detected (whatweb)
- Evidence: Apache, Cookies, Country, DVWA, HTTPServer, IP, PasswordField, Title
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: low); Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: low)
- **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** FingerprintHub Technology Fingerprint (nuclei)
- Evidence: http://localhost:3001/login.php
- **INFO** Missing Cookie SameSite Strict (nuclei)
- Evidence: http://localhost:3001/login.php
- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:3001/login.php
- **INFO** Missing Cookie SameSite Strict (nuclei)
- Evidence: http://localhost:3001
- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:3001
- **INFO** Gitignore Config - Detect (nuclei)
- Evidence: http://localhost:3001/.gitignore

- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:3001/login.php
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **INFO** CAA Record (nuclei)
- Evidence: localhost
- **INFO** README.md file disclosure (nuclei)
- Evidence: http://localhost:3001/README.md
- **INFO** WAF Detection (nuclei)
- Evidence: http://localhost:3001/
- **INFO** robots.txt endpoint prober (nuclei)
- Evidence: http://localhost:3001/robots.txt
- **MEDIUM** Sensitive Configuration Files Listing - Detect (nuclei)
- Evidence: http://localhost:3001/config/
- Compliance Mapping: Potential Gap: SOC 2 CC7.1 (Vulnerability Management) (mapping confidence: medium)
- **INFO** robots.txt file (nuclei)
- Evidence: http://localhost:3001/robots.txt
- **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** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** FingerprintHub Technology Fingerprint (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)
- **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)
- **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
- **MEDIUM** Prometheus Metrics - Detect (nuclei)
- Evidence: http://localhost:9090/metrics
- Compliance Mapping: Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: high)
- **INFO** Discovered path (gobuster)
- Evidence: [2K/robots.txt (Status: 200) [Size: 26]
- Compliance Mapping: Potential Gap: SOC 2 CC8.1 (Configuration Management) (mapping confidence: medium)
- **LOW** Supabase anon key exposed in client content (supabase_audit)
- Evidence: key=eyJhbG….sig, source=http://localhost:4001
- Recommendation: Verify RLS policies and limit anon key usage to least privilege.
- Compliance Mapping: Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: medium)
- **CRITICAL** Supabase service role key exposed (supabase_audit)
- Evidence: key=eyJhbG….sig, source=http://localhost:4001

- Recommendation: Rotate the service role key immediately and remove it from client-side code.
- Compliance Mapping: Potential Gap: SOC 2 CC7.1 (Vulnerability Management) (mapping confidence: medium); Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high); Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: high)
- **HIGH** Supabase REST API accessible without authentication (supabase_audit)
- Evidence: http://localhost:4001/rest/v1/ (HTTP 200)
- Recommendation: Enforce RLS and require API keys/auth for REST endpoints.
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high); Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: medium)
- **MEDIUM** Supabase RPC endpoint exposed without authentication (supabase_audit)
- Evidence: http://localhost:4001/rest/v1/rpc/ (HTTP 200)
- Recommendation: Restrict RPC access with policies and authentication.
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high); Potential Gap: SOC 2 CC7.1 (Vulnerability Management) (mapping confidence: medium); Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: medium)
- **HIGH** Supabase RLS may be disabled (supabase_audit)
- Evidence: http://localhost:4001/rest/v1/ (HTTP 200)
- Recommendation: Enable RLS and verify policies for affected tables/views.
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high); Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: medium)
- **HIGH** Supabase RPC 'list_users' callable without authentication (supabase_audit)
- Evidence: http://localhost:4001/rest/v1/rpc/list_users (HTTP 200)
- Recommendation: Require authentication for RPCs and enforce RLS or role checks.
- Compliance Mapping: Potential Gap: SOC 2 CC6.1 (Logical Access) (mapping confidence: high); Potential Gap: SOC 2 CC6.8 (Data Classification & Protection) (mapping confidence: medium)
- **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)

Recommended Next Actions

1. Restrict monitoring/debug endpoints to trusted admin or monitoring networks only; add authentication/authorization controls where supported.
2. Reduce attack surface by closing unused listeners and rebinding critical services from wildcard interfaces to least-privilege network zones.
3. Limit PostgreSQL exposure to required application hosts and enforce strong auth/TLS policies for database connectivity.
4. Harden Redis: require authentication/ACLs, bind to localhost or private interfaces, and block untrusted network access at the firewall.
5. Collect SOC 2 control-operation evidence not assessable by scanning (JML/access reviews, change approvals, incident response drills, and policy governance records).
6. After remediation, rerun the readiness assessment and compare deltas in findings severity, exposed services, and evidence artifacts.

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-cnlo8rqf/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
whatweb	success	`whatweb http://localhost:3001 --log-json -`
whatweb	success	`whatweb http://localhost:8080 --log-json -`
whatweb	success	`whatweb http://localhost:9090 --log-json -`
wpscan	skipped	
wpscan	skipped	
wpscan	skipped	
nuclei	success	`nuclei -u http://localhost:3001 -jsonl -rate-limit 300`
nuclei	success	`nuclei -u http://localhost:8080 -jsonl -rate-limit 300`
nuclei	success	`nuclei -u http://localhost:9090 -jsonl -rate-limit 300`
gobuster	success	`gobuster dir -u http://localhost:3001 -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:3001/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`
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 (x3)

- **gobuster**: FAILED - Error: the server returns a status code that matches the provided options for non existing urls. http://localhost:8080/50e1cf62-9c8a-430d-868e-76a414dee544 => 501 (Length: 191). To continue please exclude the status code or the length
- **katana**: SKIPPED - Disabled by config (tools..enabled=false) (x3)
- **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-cnlo8rqf/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
- **whatweb**: `whatweb http://localhost:3001 --log-json -`
- **whatweb**: `whatweb http://localhost:8080 --log-json -`
- **whatweb**: `whatweb http://localhost:9090 --log-json -`
- **nuclei**: `nuclei -u http://localhost:3001 -jsonl -rate-limit 300`
- **nuclei**: `nuclei -u http://localhost:8080 -jsonl -rate-limit 300`
- **nuclei**: `nuclei -u http://localhost:9090 -jsonl -rate-limit 300`
- **gobuster**: `gobuster dir -u http://localhost:3001 -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:3001/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`
- **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`