Supabash Audit Report

Target: localhost **Run Type:** ai-audit

Run Info

- started_at: 2026-01-29 19:52:01 UTC
- finished_at: 2026-01-29 20:02:32 UTC

Table of Contents

Summary

The localhost environment exposes an unauthenticated Prometheus instance and multiple metrics/debug endpoints, increasing the risk of information disclosure and potential lateral movement, alongside several open services that should be access-controlled. No critical remote-code execution issues were identified in this scan.

LLM Usage

- total_tokens=12660
- cost_usd=0.029580

Findings

- **HIGH** Unauthenticated Prometheus monitoring interface exposed
- Evidence: Nuclei detected accessible Prometheus configuration API at http://localhost:9090/api/v1/status/config from an unauthenticated context.
- Recommendation: Restrict access to the Prometheus UI and APIs (e.g., bind to localhost only, place behind VPN/reverse proxy with authentication, or use network ACLs/firewall rules). Disable or limit sensitive endpoints (config, flags) where possible and avoid exposing Prometheus directly to untrusted networks.
- **MEDIUM** Prometheus metrics endpoint exposed on application port 8080
- Evidence: Nuclei identified a Prometheus /metrics endpoint at http://localhost:8080/metrics.

- Recommendation: Limit access to /metrics to trusted monitoring infrastructure only (IP allowlist, mTLS, or authenticated reverse proxy). Review exported metrics for sensitive data (user identifiers, internal hostnames, tokens) and remove or redact as needed.
- **MEDIUM** Prometheus metrics endpoint exposed on Prometheus port 9090
- Evidence: Nuclei identified a Prometheus /metrics endpoint at http://localhost:9090/metrics.
- Recommendation: Restrict network access to the metrics endpoint to monitoring systems or internal networks only, and ensure no secrets or sensitive identifiers are present in metric labels or values.
- **LOW** Go pprof debug endpoint exposed
- Evidence: Nuclei detected an accessible Go pprof heap debug page at http://localhost:9090/debug/pprof/heap?debug=1.
- Recommendation: Disable pprof in production or restrict it to localhost/admin-only networks. If needed for operations, protect it behind authentication and ensure it is not reachable from untrusted clients, as profiles can leak memory contents and internal implementation details.
- **LOW** Multiple open TCP services without documented access controls
- Evidence: Nmap reported open ports: 3000/tcp (ppp), 4000/tcp (remoteanything), 5050/tcp (mmcc), 5432/tcp (PostgreSQL 9.6.0+), 8080/tcp (http-proxy), 9090/tcp (Golang net/http server), 9100/tcp (jetdirect).
- Recommendation: Harden network exposure by closing unused ports, binding services to localhost where possible, and enforcing firewall rules to limit access to required internal ranges only. For PostgreSQL and other stateful services, ensure strong authentication, TLS (if applicable), and least-privilege accounts.

Methodology

- Baseline: deterministic evidence collection with scope controls and safe defaults.
- Agentic expansion: tool-calling planner proposes additional evidence collection within allowed scope.

Agentic Expansion

- phase: baseline+agentic
- baseline_finished_at: 2026-01-29 19:56:10 UTC
- max_actions: 10
- notes: Prior scans already identified Prometheus on 9090 and metrics on 8080; this final action concentrates on structured HTTP vulnerability evidence for the main application endpoint to close the audit loop.
- planner: tool_calling

Actions

- gobuster target=http://localhost:8080 profile=standard: failed

- Rationale: Baseline web enumeration on primary HTTP proxy (8080) to identify hidden paths that may expose sensitive data or admin interfaces, supporting vulnerability management controls for all compliance profiles.
- Error: Error: the server returns a status code that matches the provided options for non existing urls. http://localhost:8080/132cb166-b432-4ee1-b8ed-9573bca5da50 => 501 (Length: 191). To continue please exclude the status code or the length
- gobuster target=http://localhost:9090 profile=standard: success
- Rationale: Directory and file brute-forcing on secondary Golang HTTP service (9090) to discover additional attack surface and potential misconfigurations, complementing earlier tech stack and header findings.
- nuclei target=http://localhost:9090 profile=standard: success
- Rationale: Template-based vulnerability scan on the 9090 Golang service to mirror coverage already obtained on 8080, checking for missing security headers, exposed metrics, and common misconfigurations for audit evidence.
- httpx target=http://localhost:8080 profile=compliance_soc2: success
- Rationale: Run HTTPX against the primary web target to confirm service availability, HTTP methods, and response metadata as supporting evidence for SOC 2 vulnerability management and service inventory controls. Baseline tech and status info also helps contextualize existing nuclei findings.
- httpx target=http://localhost:9090 profile=compliance_soc2: skipped
- Rationale: Profile the Prometheus endpoint with HTTPX to capture headers, status codes, and supported methods as evidence for exposure of monitoring interfaces, supporting SOC 2 controls around secure configuration and restricted management access.
- Reason: Target not in allowed web targets
- nuclei target=http://localhost:9090 profile=compliance_soc2: skipped
- Rationale: A focused follow-up nuclei run on the Prometheus endpoint to ensure coverage of authentication, access control, and debug/metrics exposures, deepening evidence for the previously detected unauthenticated Prometheus instance in line with SOC 2 vulnerability assessment requirements.
- Reason: Already completed in agentic phase
- whatweb target=http://localhost:8080 profile=standard: success
- Rationale: Identify web stack and technologies on the primary web target to correlate with existing Prometheus/pprof findings and support technology-specific control checks (headers, frameworks, versions).
- httpx target=http://localhost:8080 profile=standard: skipped
- Rationale: Collect HTTP response metadata (status codes, redirects, TLS/HTTP options) for the main web target to validate exposure, methods, and header behavior as supporting evidence for configuration and hardening controls.
- Reason: Already completed in agentic phase
- nuclei target=http://localhost:8080 profile=standard: success
- Rationale: Run a focused vulnerability and misconfiguration scan against the main web target to complement existing nuclei results on port 9090 and check for similar unauthenticated or missing-control issues on the application entry point.

Findings Overview

Summary (LLM)

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

Detailed (Tools)

Severity	Count
CRITICAL	0
HIGH	1
MEDIUM	3
LOW	1
INFO	53

Findings (Detailed)

- **INFO** Open port 3000/tcp (nmap)
- Evidence: ppp
- **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 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** Tech stack detected (whatweb)
- Evidence: Country, IP
- **INFO** Tech stack detected (whatweb)
- Evidence: Country, IP
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)

- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **MEDIUM** Prometheus Metrics - Detect (nuclei)
- Evidence: http://localhost:8080/metrics
- **INFO** Allowed Options Method (nuclei)
- Evidence: http://localhost:8080
- **INFO** CAA Record (nuclei)
- Evidence: localhost
- **INFO** Allowed Options Method (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:8080
- **MEDIUM** Prometheus Metrics - Detect (nuclei)
- Evidence: http://localhost:8080/metrics
- **INFO** CAA Record (nuclei)
- Evidence: localhost
- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:9090/classic/graph

- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **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
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:9090/classic/graph
- **MEDIUM** Prometheus Metrics - Detect (nuclei)
- Evidence: http://localhost:9090/metrics
- **LOW** Go pprof Debug Page (nuclei)
- Evidence: http://localhost:9090/debug/pprof/heap?debug=1
- **INFO** Prometheus flags API endpoint (nuclei)
- Evidence: http://localhost:9090/api/v1/status/flags
- **HIGH** Prometheus Monitoring System - Unauthenticated (nuclei)
- Evidence: http://localhost:9090/api/v1/status/config
- **INFO** Allowed Options Method (nuclei)
- Evidence: http://localhost:9090
- **INFO** CAA Record (nuclei)
- Evidence: localhost

Tools Run

Tool	Status	Command
nmap	success	`nmap localhost -oX - -sV -O`
httpx	success	`/usr/local/bin/httpx -silent -json -l /tmp/supabash-httpx-1ztkltwj/`

Tool	Status	Command
		targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects
httpx	success	/usr/local/bin/httpx -silent -json -l /tmp/supabash-httpx-khg2m_hd/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects
httpx	skipped	
- **httpx**: ⏭ skipped — Target not in allowed web targets		
httpx	skipped	
- **httpx**: ⏭ skipped — Already completed in agentic phase		
whatweb	success	whatweb http://localhost:8080 --log-json -
whatweb	success	whatweb http://localhost:8080 --log-json -
wpscan	skipped	
- **wpscan**: ⏭ skipped — WordPress not detected by whatweb		
nuclei	success	nuclei -u http://localhost:8080 -jsonl -rate-limit 100
nuclei	success	nuclei -u http://localhost:8080 -jsonl -rate-limit 50
nuclei	success	nuclei -u http://localhost:9090 -jsonl -rate-limit 50
nuclei	skipped	
- **nuclei**: ⏭ skipped — Already completed in agentic phase		
gobuster	success	gobuster dir -u http://localhost:9090 -w /home/devcore24/projects/supabash/src/supabash/data/

Tool	Status	Command
		wordlists/common.txt -t 20 -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
- **gobuster**: × failed — Error: the server returns a status code that matches the provided options for non existing urls. http://localhost:8080/d44b344f-9405-4de5-8809-ae34e5865c23 => 501 (Length: 191). To continue please exclude the status code or the length		
gobuster	failed	gobuster dir -u http://localhost:8080 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 20 -q -z --no-error
- **gobuster**: × failed — Error: the server returns a status code that matches the provided options for non existing urls. http://localhost:8080/132cb166-b432-4ee1-b8ed-9573bca5da50 => 501 (Length: 191). To continue please exclude the status code or the length		
katana	skipped	
- **katana**: skipped — Disabled by config (tools..enabled=false)		
dnsenum	failed	dnsenum localhost
- **dnsenum**: × failed — localhost NS record query failed: NXDOMAIN		
sslscan	skipped	
- **sslscan**: skipped — No TLS ports detected (443/8443)		
enum4linux-ng	skipped	
- **enum4linux-ng**: skipped — No SMB ports detected (139/445)		
sqlmap	skipped	

Tool	Status	Command
- **sqlmap**: ⏭ skipped — No parameterized URL provided (include '?' in target URL)		
searchsploit	skipped	
- **searchsploit**: ⏭ skipped — Disabled by config (tools..enabled=false)		
supabase_audit	success	`supabase_audit`

Commands Executed

- **nmap**: `nmap localhost -oX - -sV -O`
- **httpx**: `/usr/local/bin/httpx -silent -json -l /tmp/supabash-httpx-1ztkltwj/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
- **httpx**: `/usr/local/bin/httpx -silent -json -l /tmp/supabash-httpx-khg2m_hd/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
- **whatweb**: `whatweb http://localhost:8080 --log-json -`
- **whatweb**: `whatweb http://localhost:8080 --log-json -`
- **nuclei**: `nuclei -u http://localhost:8080 -jsonl -rate-limit 100`
- **nuclei**: `nuclei -u http://localhost:8080 -jsonl -rate-limit 50`
- **nuclei**: `nuclei -u http://localhost:9090 -jsonl -rate-limit 50`
- **gobuster**: `gobuster dir -u http://localhost:9090 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 20 -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`
- **gobuster**: `gobuster dir -u http://localhost:8080 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 20 -q -z --no-error`
- **dnsenum**: `dnsenum localhost`
- **supabase_audit**: `supabase_audit`