Supabash Audit (Readiness) Report

Target: localhost **Assessment Type:** Supabash Audit (Readiness) **Run Type:** ai-audit **Compliance Profile:** BSI IT-Grundschutz **Compliance Focus:** Baseline security controls with evidence of secure configuration and vulnerability management.

Run Info

- started_at: 2026-02-06 08:11:36 UTC
- finished_at: 2026-02-06 08:16:12 UTC

Table of Contents

Summary

The localhost assessment identified multiple open application and database ports but no explicit vulnerabilities or misconfigurations were detected by the automated tools. The primary risk is increased attack surface from numerous exposed services rather than specific known CVEs.

Notes

- ffuf fallback (after gobuster failure) ran and found 0 paths across 1 target(s): http://localhost:33425 (0).

LLM Usage

- total_tokens=4888
- cost_usd=0.013329

Findings

- **MEDIUM** Multiple application services exposed on non-standard HTTP ports
- Evidence: Nmap detected HTTP services on ports 19090, 33425, 3947, 42901, 8080, 9090, and 9840 (Golang net/http and Node.js Express frameworks, plus an HTTP proxy).
- Recommendation: Restrict access to these ports using host-based firewalls or network ACLs, expose only necessary services to untrusted networks, and ensure each web service is hardened (authentication, TLS where applicable, up-to-date frameworks, and minimal enabled endpoints).
- **MEDIUM** Database and cache services exposed on network-accessible ports
- Evidence: Nmap identified PostgreSQL on 5432/tcp (version 9.6.0 or later) and Redis 6.2.11 on 6379/tcp as open.
- Recommendation: Bind PostgreSQL and Redis to localhost or internal interfaces only, enforce strong authentication and access controls, and restrict access via firewall rules. Verify that no default or weak credentials are in use and that encryption in transit is enabled where supported.
- **LOW** Additional non-standard services increasing attack surface
- Evidence: Open ports with non-HTTP services: 3000/tcp (ppp), 4000/tcp (remoteanything), 5050/tcp (mmcc), 9100/tcp (jetdirect), 34403/tcp and 52550/tcp (unknown services).
- Recommendation: Review the necessity of each exposed service, disable or uninstall unused daemons, and document business justification for required ports. Where services must remain exposed, ensure they are updated, authenticated, and restricted to trusted source networks.
- **LOW** Lack of TLS on detected web services
- Evidence: SSL/TLS scans were skipped because no TLS ports (443/8443) were detected; all identified web targets use plain HTTP (e.g., http://localhost:33425, http://localhost:19090, etc.).
- Recommendation: For any service accessible beyond the local host or development environment, enable HTTPS with modern TLS configurations and valid certificates, and redirect HTTP to HTTPS to protect credentials and sensitive data in transit.

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: compliance_bsi
- Compliance focus: Baseline security controls with evidence of secure configuration and vulnerability management.

Agentic Expansion

- phase: baseline+agentic
- baseline_finished_at: 2026-02-06 08:16:06 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	2
LOW	2
INFO	0

Detailed (Tools)

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

Findings (Detailed)

Note: 10 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, X-Powered-By
- **INFO** Wappalyzer Technology Detection (nuclei)
- Evidence: http://localhost:33425
- Compliance Impact: NON-COMPLIANT: BSI IT-Grundschutz: Vulnerability Management
- **INFO** HTTP Missing Security Headers (nuclei)
- Evidence: http://localhost:33425
- Compliance Impact: NON-COMPLIANT: BSI IT-Grundschutz: Vulnerability Management
- **INFO** CAA Record (nuclei)
- Evidence: localhost
- Compliance Impact: NON-COMPLIANT: BSI IT-Grundschutz: Vulnerability Management

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-k2hfr855/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
whatweb	success	`whatweb http://localhost:33425 --log-json -`
wpscan	skipped	
- **wpscan**: □ skipped — WordPress not detected by whatweb		
nuclei	success	`nuclei -u http://localhost:33425 -jsonl -rate-limit 100`
gobuster	failed	`gobuster dir -u http://localhost:33425 -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:33425/1bf2854c-59b8-4cfe-9149-5249e42f7944 => 401 (Length: 12). To		

Tool	Status	Command
continue please exclude the status code or the length		
ffuf	success	`ffuf -u http://localhost:33425/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 — 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	
- **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 --script ssl-enum-ciphers -p-`
- **httpx**: `/usr/local/bin/httpx -silent -json -l /tmp/supabash-httpx-k2hfr855/targets.txt -threads 50 -timeout 5 -retries 1 -status-code -title -web-server -tech-detect -follow-redirects`
- **whatweb**: `whatweb http://localhost:33425 --log-json -`
- **nuclei**: `nuclei -u http://localhost:33425 -jsonl -rate-limit 100`
- **gobuster**: `gobuster dir -u http://localhost:33425 -w /home/devcore24/projects/supabash/src/supabash/data/wordlists/common.txt -t 10 -q -z --no-error`
- **ffuf**: `ffuf -u http://localhost:33425/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`
- **dnsenum**: `dnsenum localhost`
- **supabase_audit**: `supabase_audit`