SAST/SCA Report

Scan Identifier:	3f7a1c9e-8b42-4d61-9c05-27ae1f6b3d80
Report ID:	b64d05f2-1ac7-4e9a-8f13-6d20c9b47e55
Artifact ID:	e1c8a730-5f96-42bb-b0d4-9a7351ec2f18
Technology:	SAST, SCA
Project:	SampleRepository
Version:	v2.4.0 (commit 9f3c2ab1d4e7)
Report Created:	Wednesday, September 16, 2026
Manufacturer:	Firma XY welche den Code besitzt

True issues by severity

Critical severity issues	3
High severity issues	73
Medium severity issues	28
Low severity issues	11
Total true issues	**115**

CipherCellScan Information

Scan started at:	Wednesday, September 16, 2026 05:43:14 (UTC)
Scan duration:	07:30:38
Scan completed at:	Wednesday, September 16, 2026 13:13:52 (UTC)
Pipeline Steps:	Preanalysis, SAST, SBOM Dependency Tracking, SBOM Reachability, AI FP Detection, AI Ranking
Errors Detected:	None (2 warnings, see SBOM Reachability)

Pre-Analysis Settings

Selected Tools:	Propylon v0.9.4
Profile:	deterministic
Errors Detected:	None

SAST Settings

Selected Tools:	ruff v0.14.4, bandit v1.8.6, cppcheck v2.18.0, semgrep v1.145.0
Language Coverage:	C (cppcheck, semgrep), Python (ruff, bandit, semgrep), JavaScript (semgrep)
Rule Profile:	security — ruleset `ciphercell-sec-2026.03`, sha256 `8f2b41c6…d97a`
Deduplication Method:	Deterministic
Created Artifacts:	`sast_combined.sarif`
Errors Detected:	None

SBOM Dependency Tracking Settings

Selected Tools:	syft v1.33.0, cdxgen v11.10.0, deptrace v0.7.2
Profile:	Standard SBOM
SBOM Format:	CycloneDX 1.6
Advisory Sources:	NVD, OSV.dev, GitHub Advisory Database, Sonatype OSS Index, VulnDB
Created Artifacts:	`sbom.cdx.json, sbom.vdr.json`
Errors Detected:	None

SBOM Reachability

Selected Tools:	CodeQL v2.24.1, Joern v4.0.312
Profile:	Default Taint Analysis
Created Artifacts:	`sbom_annotated.vdr.json`
Errors Detected:	2 warnings

ID	Stage	Warning
W-01	Joern, JavaScript	2 of 148 entry points could not be resolved (dynamic `require()` in `server/plugins/loader.js:41`). The 6 findings depending on these entry points were escalated and are reported conservatively as true issues.
W-02	CodeQL, C	Database build skipped for vendored sources under `third_party/`; excluded by scan scope, no reachability verdict is claimed for those paths.

AI FP Detection

Selected Tools:	Polygraph v1.6.2
Profile:	static and escalation agent
AI Model:	Qwen3-32B, digest `sha256:4ab1…c70f`
Inference:	On-premise, CipherCell inference cluster
Reasoning Effort:	Default (classification), Default (escalation)
Response Cache:	Enabled
Context Enrichment:	Static (50 lines before, 50 lines after)
Errors Detected:	None

Ranking

Selected Tools:	Prism v0.4.1
Effort:	Standard
Context Size:	Minimal
Errors Detected:	None

Project Information

Project:	SampleRepository
Version:	v2.4.0 (commit `9f3c2ab1d4e7`)
Analysed lines of code:	184,920

Languages

C	40.2 %
Python	39.6 %
JavaScript	20.2 %
Total	**100.0 %**

Summary

Raw findings:	210
Filtered:	95 (82 SAST, 13 SCA)
True issues:	115 (86 SAST, 29 SCA)
Distinct issue types (true):	8 SAST CWEs, 12 affected components

True SAST issues by CWE (86)

CWE-22: Improper Limitation of a Pathname to a Restricted Directory	3	
CWE-78: Improper Neutralization of Special Elements used in an OS Command	2	
CWE-327: Use of a Broken or Risky Cryptographic Algorithm	3	
CWE-674: Uncontrolled Recursion	50	
CWE-770: Allocation of Resources Without Limits or Throttling	10	
CWE-798: Use of Hard-coded Credentials	4	
CWE-918: Server-Side Request Forgery	2	
CWE-1333: Inefficient Regular Expression Complexity	12	

Low (9) Medium (20) High (55) Critical (2) — bar length is proportional to the issue count (100 % = 50).

Most affected components, true SCA issues (top 4 of 12)

`next@16.3.2`	4	
`glibc@2.36-9+deb12u7`	3	
`nanoid@3.3.14`	2	
`lodash@4.17.21`	2	

Low Medium High Critical — 11 of 29 true SCA issues shown; 100 % = 4.

Most Critical Vulnerabilities

Type	Severity	CVE/CWE	Affected File / Component	Description
SAST	Critical	CWE-78	`src/tools/exporter.py:57`	User-controlled argument passed to `subprocess.run(…, shell=True)`.
SCA	Critical	GHSA-2xp9-vwfh-vxw4	`next@16.3.2`	Heap buffer overflow in libheif, reached through sharp during AVIF image optimization; allows unauthenticated remote code execution.
SAST	High	CWE-22	`src/storage/paths.py:114`	Non-literal path component passed to `os.path.join()`.
SAST	High	CWE-918	`src/utils.js:68`	Non-literal URL passed to `fetch()`.

SAST Vulnerabilities

True Issues by CWEs

CWE-22: Improper Limitation of a Pathname to a Restricted Directory (3 issues)	
Severity	High
Description	A path component that is not a string literal is passed to a file system API. Where the component originates from a request parameter, an attacker can traverse outside the intended directory.

CWE-22 #1 — `sast-9f3c2ab-0001`	
Location	`src/storage/paths.py:114`
Description	Non-literal path component passed to `os.path.join()`. The value originates from `request.args["file"]` and is not normalised before use.
Reported By	bandit v1.8.6 (B108), semgrep v1.145.0
Reachability	Reachable — taint path from entry point `api/upload.py:31 (upload_handler)`, 4 hops (Joern)
Evidence	Deterministic, no LLM escalation

CWE-918 #1 — `sast-9f3c2ab-0042`	
Location	`src/utils.js:68`
Description	Non-literal URL passed to `fetch()`. The host part is taken from the request body and is not validated against an allow list.
Reported By	semgrep v1.145.0
Reachability	Reachable — taint path from entry point `server/routes/webhook.js:31`, 3 hops (Joern)
Evidence	Deterministic, no LLM escalation

Filtered Issues by CWEs

The following findings were reported by the scanners but assessed as not exploitable in this artifact. Each entry carries the filtering reason together with the VEX justification that is written to `sbom_annotated.vdr.json`. Filtered issues are not counted in the severity summary.

CWE-1333: Inefficient Regular Expression Complexity (18 issues filtered)	
Reported Severity	Low
Description	Regular expressions with super-linear worst-case runtime that can be abused for algorithmic denial of service if reachable with attacker-controlled input.

CWE-1333 #1 — `sast-9f3c2ab-0113`	
Location	`server/lib/llm.js:68`
Description	Backtracking regular expression in the log line parser `parseLogLine()`.
Reported By	semgrep v1.145.0
Filtering Reason	`code_not_reachable` — no call path from any of the 148 resolved entry points to `parseLogLine()`; the only caller is the debug CLI, which is excluded from the production build. Deterministic (Joern), no LLM escalation. Decided 2026-09-16 by Polygraph v1.6.2.

CWE-674 #1 — `sast-9f3c2ab-0207`	
Location	`parser/expr.c:412`
Description	Uncontrolled recursion in the expression parser; deeply nested input could exhaust the stack.
Reported By	cppcheck v2.18.0
Filtering Reason	`protected_by_mitigating_control` — recursion depth is bounded at the call site (`parser/limits.c:88`, `MAX_DEPTH = 64`); the guard dominates every path into `parse_expr()` (CodeQL). Escalated to the LLM stage, confirmed by A. Braml on 2026-09-16.

Filtered SAST issues by CWE (82)

CWE	Filtered	Dominant VEX justification
CWE-674: Uncontrolled Recursion	41	`protected_by_mitigating_control`
CWE-1333: Inefficient Regular Expression Complexity	18	`code_not_reachable`
CWE-327: Use of a Broken or Risky Cryptographic Algorithm	9	`code_not_reachable`
CWE-798: Use of Hard-coded Credentials	8	`code_not_present`
CWE-89: SQL Injection	6	`code_not_reachable`
Total	**82**	

SBOM / SCA Vulnerabilities

True Issues by CVEs

GHSA-2xp9-vwfh-vxw4	
Affected component	`next@16.3.2 (via sharp → libheif@1.23.1)`
CVE	None assigned
Severity	**Critical**
Description	A heap buffer overflow in the libheif library used by sharp, which Next.js uses for image optimization, can lead to remote code execution when AVIF files are optimized.
CVSS	9.5 / 10 (CVSS v4.0) — `CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H`
Impact	Confidentiality (High), Integrity (High), Availability (High)
Upstream reference	`GHSA-g89c-p67h-r497 (strukturag/libheif, ≤ v1.23.1)`
Fixed in	`next 16.3.3 / 15.5.24`
Reachability	Reachable — AVIF output is enabled in `next.config.js:22` (`images.formats` contains `image/avif`)
Evidence	Deterministic (configuration and call path), no LLM escalation
Known for	22 days (advisory published 2026-08-25)

Filtered Issues by CVEs

Vulnerabilities present in the SBOM whose vulnerable code path is not exploitable in this artifact. The filtering reason is carried into `sbom.vdr.json` as a CycloneDX VEX statement.

CVE-2026-75604 (GHSA-p293-qw3h-jr36)	
Affected component	`next@16.3.2`
Reported Severity	**Critical**
Description	Path traversal (CWE-22) in Next.js applications served from a Windows filesystem, leading to unauthenticated remote code execution.
CVSS	9.0 / 10 (CVSS v3.1) — `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H`
Fixed in	`next 16.3.3 / 15.5.24`
Filtering Reason	`requires_environment` — the vulnerable code path only executes on a Windows filesystem. The deployment target of this artifact is `linux/amd64` (base image `debian:12-slim`, see `sbom.cdx.json`). Deterministic, no LLM escalation. Decided 2026-09-16 by Polygraph v1.6.2.
Known for	22 days (advisory published 2026-08-25)

CVE-2025-7338	
Affected component	`multer@1.4.5-lts.2`
Reported Severity	**High**
Description	Multer allows an attacker to trigger a denial of service by sending a malformed multipart upload request, which raises an unhandled exception and crashes the process.
CVSS	7.5 / 10 (CVSS v3.1) — `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H`
CWE	CWE-248: Uncaught Exception
Fixed in	`multer 2.0.2`
Filtering Reason	`code_not_reachable` — multer is declared with scope `development` in `sbom.cdx.json` and is imported only by the integration test fixture server; no production entry point reaches it. Deterministic (Joern), no LLM escalation. Decided 2026-09-16 by Polygraph v1.6.2.
Known for	426 days (advisory published 2025-07-17)

Filtered SCA issues by justification (13)

VEX justification	Filtered	Typical case in this artifact
`code_not_reachable`	7	Development-scoped dependencies and unused transitive packages
`requires_environment`	3	Windows-only or macOS-only code paths
`requires_configuration`	2	Feature flags not enabled in the shipped configuration
`code_not_present`	1	Vulnerable function removed by the build-time tree shaker
Total	**13**	