

easy-dataset

github.com/ConardLi/easy-dataset

Scanned 24 September 2026 at 06:52 · Report generated 29 October 2026 · JavaScript · 14,947 stars

OVERALL ASSESSMENT

High

Combined score 276 · 348 findings after filtering

Summary

This repository has a high vulnerability score of 275.0, which means there are many insecure coding patterns that an attacker could easily exploit to break into your system. While the malicious-pattern risk is very low at 1.0, this suggests the code itself does not appear to be intentionally harmful, but rather just poorly written or outdated. The most serious issues involve using unencrypted HTTP servers instead of HTTPS and allowing Docker containers to run as root users, which could let attackers control sensitive data. Additionally, there are several loose version constraints in your dependencies that might allow malicious updates to slip through if you don't update them regularly. Overall, the code is not malicious but is unsafe enough that it needs immediate attention before being used in a production environment.

Written by a language model running locally on the scanning machine, from the findings in this report. The risk levels above and below were decided by the scoring model, not by this summary.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

High (275)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Low (1)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
semgrep	Insecure coding patterns across many languages	2	213	79	294

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
dep_checker	Vulnerable, unpinned or typosquatted dependencies	0	0	53	53
yara	Signatures of malicious behaviour in source files	1	0	0	1

9 of 348 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	semgrep	By not specifying a USER, a program in the container may run as 'root'. This is a security hazard. If an attacker can control a process running as root, they may have control over the container. Ensure that the last USER in a Dockerfile is a USER other than 'root'.	2	/ Dockerfile:86
HIGH	yara	YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed	1	/lib/util/file.js
MEDIUM	semgrep	Possible writing outside of the destination, make sure that the target path is nested in the intended destination	1	/app/api/projects/[projectId]/files/route.js:203
MEDIUM	semgrep	This .npmrc does not set a minimum release age or sets it too low. Newly published packages can be malicious or unstable. Add `min-release-age = 7` to wait 7 days before resolving newly published package versions. Added in: v11.10 Reference: https://github.blog/changelog/2026-02-18-npm-bulk-trusted-	1	/.npmrc:1
MEDIUM	semgrep	GitHub Actions step uses a mutable tag or branch reference. Tags and branch names can be silently repointed by the action owner, enabling supply-chain attacks — as seen in the trivy-action and kics-github-action compromises. Pin the reference to a full 40-character commit SHA instead, e.g. `uses: ac	5	/.github/workflows/docker-build.yml:18

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Checks for any usage of http servers instead of https servers. Encourages the usage of https protocol instead of http, which does not have TLS and is therefore unencrypted. Using http can lead to man-in-the-middle attacks in which the attacker is able to read sensitive information.	2	/electron/modules/server.js:132
MEDIUM	semgrep	Detected possible user input going into a `path.join` or `path.resolve` function. This could possibly lead to a path traversal vulnerability, where the attacker can access arbitrary files stored in the file system. Instead, be sure to sanitize or validate user input first.	204	/lib/file/text-splitter.js:280
LOW	semgrep	Detected string concatenation with a non-literal variable in a util.format / console.log function. If an attacker injects a format specifier in the string, it will forge the log message. Try to use constant values for the format string.	79	/app/projects/[projectId]/distill/autoDistillservice.js:601
LOW	dep_checker	Loose version constraint: '@huggingface/hub^2.0.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'react-markdown^10.0.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'nanoid^5.1.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'react-i18next^15.4.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'react-dom^18.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'prisma^6.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'pkg^5.8.1' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'opener^1.5.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'ollama-ai-provider^1.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'next^14.2.29' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'next-themes^0.2.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'langchain^0.3.24' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'react^18.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'recharts^3.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'remark-gfm^4.0.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'sharp^0.33.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'sonner^2.0.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'turndown^7.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'wait-on^7.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'xlsx^0.18.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'xmldom^0.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'zhipu-ai-provider^0.1.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'zod^3.25.76' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'electron-build^0.0.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@commitlint/cli^19.8.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@commitlint/config-conventional^19.8.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@emotion/react^11.11.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@emotion/styled^11.11.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@fontsource/inter^5.0.16' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@fontsource/jetbrains-mono^5.0.18' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@lobehub/icons^1.96.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@opendocsg/pdf2md^0.2.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@openrouter/ai-sdk-provider^0.4.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@prisma/client^6.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'adm-zip^0.5.16' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'ai^4.3.4' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'axios^1.8.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'concurrently^8.2.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'mammoth^1.9.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'electron-builder^24.13.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'electron-updater^6.3.9' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'electron^35.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'formidable^3.5.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'framer-motion^12.4.10' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'github-markdown-css^5.8.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'husky^9.1.7' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'i18next-browser-languagedetector^8.0.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'i18next^24.2.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'image-size^2.0.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'jotai^2.12.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'jsonrepair^3.13.1' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'jszip^3.10.1' — attacker could push malicious update	1	package.json

Showing the 60 most significant of 61 distinct findings. The counts in the previous section cover all of them.

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 24 September 2026.