

QuranCaption

github.com/zonetecde/QuranCaption

Scanned 18 August 2026 at 09:38 · Report generated 29 October 2026 · TypeScript · 240 stars

OVERALL ASSESSMENT

Medium

Combined score 45 · 139 findings after filtering

Summary

This repository shows signs of potential malicious activity rather than just standard insecure coding, as it was flagged by multiple security tools for dangerous patterns like downloading and executing remote files or using credential-harvesting techniques. The most concerning issue is that two YARA rules detected code attempting to download a resource and execute it directly, which could allow an attacker to run arbitrary commands on your system if the code is ever shared publicly. Additionally, there are several medium-level vulnerabilities, including weak hashing methods, unsafe file operations, and potential SQL injection risks, but these appear to be common mistakes in application development rather than intentional attempts to harm others. While some dependencies have loose version constraints that could theoretically be exploited by attackers pushing malicious updates, the overall risk remains low because the codebase does not contain obvious malware or exploits designed specifically to damage your 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

Medium (35)

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

MALICIOUS PATTERN

Low (10)

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
bandit	Insecure coding patterns in Python source	0	34	32	66
dep_checker	Vulnerable, unpinned or typosquatted dependencies	0	0	60	60
yara	Signatures of malicious behaviour in source files	7	0	6	13

0 of 139 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	yara	YARA rule matched: detect_credential_harvester — References credential/secret material by name AND a deliberate outbound-send API in the same file - narrower than 'reads any env var', which large legitimate codebases do constantly regardless of intent. Still not proof the two are connected (YARA c	2	/src-tauri/python/local_multi_aligner_segmenter.py
HIGH	yara	YARA rule matched: detect_anti_analysis — Checks for a debugger, VM, or sandbox before continuing - a common malware evasion technique, essentially never present in ordinary application code	1	/src-tauri/python/quran-multi-aligner/src/pipeline.py
HIGH	yara	YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed	2	/src-tauri/python/quran-multi-aligner/src/core/worker_pool.py
HIGH	yara	YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone	2	/src-tauri/python/quran_recite_to_text/src/core/updater.py

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	bandit	Use of weak MD5 hash for security. Consider usedforsecurity=False	1	/src-tauri/python/quran-multi-aligner/src/api/session_api.py:107
MEDIUM	bandit	Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.	6	/src-tauri/python/quran_recite_to_text/src/core/updater.py:53
MEDIUM	bandit	Possible SQL injection vector through string-based query construction.	1	/src-tauri/python/quran-multi-aligner/src/ui/styles.py:14
MEDIUM	bandit	Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.	6	/src-tauri/python/quran-multi-aligner/src/api/session_api.py:162
MEDIUM	bandit	Possible binding to all interfaces.	1	/src-tauri/python/quran-multi-aligner/app.py:169
MEDIUM	bandit	Probable insecure usage of temp file/directory.	5	/src-tauri/python/quran-multi-aligner/config.py:32
MEDIUM	bandit	Unsafe Hugging Face Hub download without revision pinning in load_dataset()	4	/src-tauri/python/quran-multi-aligner/src/ui/dev_tools.py:289
MEDIUM	bandit	Unsafe Hugging Face Hub download without revision pinning in hf_hub_download()	1	/src-tauri/python/quran-multi-aligner/src/segmenter/segmenter_aoti.py:69

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	bandit	Unsafe Hugging Face Hub download without revision pinning in snapshot_download()	1	/src-tauri/python/surah-splitter/src/surah_splitter/services/transcription_service.py:86
MEDIUM	bandit	Unsafe Hugging Face Hub download without revision pinning in from_pretrained()	8	/src-tauri/python/quran-multi-aligner/src/alignment/phoneme_asr.py:91
LOW	bandit	Possible hardcoded password: "	1	/src-tauri/python/quran-multi-aligner/src/api/session_api.py:1406
LOW	bandit	Starting a process without a shell.	2	/src-tauri/python/quran_recite_to_text/run.py:35
LOW	bandit	Try, Except, Continue detected.	3	/src-tauri/python/segment_core/segment_processor.py:352
LOW	bandit	Consider possible security implications associated with the subprocess module.	8	/src-tauri/python/quran-multi-aligner/app.py:25
LOW	bandit	Starting a process with a partial executable path	6	/src-tauri/python/quran-multi-aligner/src/core/usage_logger.py:447
LOW	dep_checker	Loose version constraint: '@tauri-apps/api^2.6.0' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	bandit	subprocess call - check for execution of untrusted input.	12	/src-tauri/python/quran_recite_to_text/src/core/updater.py:72
LOW	dep_checker	Loose version constraint: 'qrcode^1.5.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'prettier^3.4.12' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'prettier-plugin-tailwindcss^0.6.11' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'prettier-plugin-svelte^3.3.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'posthog-js^1.318.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'markdown-it-deflist^3.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'plyr^3.7.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'playwright^1.53.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'modern-screenshot^4.6.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'material-icons^1.13.14' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'markdown-it^14.1.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'markdown-it-task-lists^2.1.1' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'markdown-it-footnote^4.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'dom-to-image^2.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'reflect-metadata^0.2.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'sharp^0.34.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'svelte-5-french-toast^2.0.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'svelte-check^4.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'svelte-contextmenu^1.0.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'svelte^5.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'tailwindcss^4.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'typesafe-i18n^5.27.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'typescript-eslint^8.20.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'typescript^5.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vite^6.2.6' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'vitest-browser-svelte^0.1.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vitest^3.2.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'wavesurfer.js^7.10.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'howler^2.2.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@eslint/compat^1.2.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@eslint/js^9.18.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@sveltejs/adapters-auto^6.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@sveltejs/adapters-static^3.0.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@sveltejs/kit^2.16.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@sveltejs/vite-plugin-svelte^5.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tailwindcss/forms^0.5.9' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tailwindcss/typography^0.5.16' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@tailwindcss/vite^4.0.0' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@tauri-apps/cli^2.6.0' — attacker could push malicious update	1	package.json

Showing the 60 most significant of 81 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 18 August 2026.