/code Endpoint Audit Report

Audit Date: 2025-09-07 23:02:53

Executive Summary

The `/code` endpoint is stable for standard operations (`run`, `lint`, `format`, `fix`, `test`). However, input sanitization and structured error responses for malformed CLI arguments need urgent improvement. Bulk endpoint support for code actions is non-functional.

Successes

- Executed standard operations correctly.
- Maintained file and execution safety.
- Correctly rejected unsupported languages.

Failures & Gaps

- 500 errors from malformed CLI arguments.
- Inconsistent error schema (500 instead of 400).
- `/batch` fails with `/code` due to structure issues.
- Argument sanitization is weak.

Structured Results

| Action | Status Code | Output/Observation |

|----------|-------------|---------------------------|

| run | 0 | Area: 78.54 |

| lint | 0 | Clean |

| format | 0 | No changes |

| fix | 0 | No fixes |

| test | 5 | No test functions detected |

Recommendations

Priority	Recommendation
High	Add strong CLI argument sanitization
Medium	Improve error messaging structure and transparency
Medium	Fix `/batch` compatibility with `/code`
Low	Add better context and chaining awareness