Snyk code test found 5 medium-severity issues:

1. Path Traversal (scrape.py) – The –output CLI argument was passed directly to open(), allowing attacker to write files outside the intended directory via ../../ paths. Fixed by stripping to basename and writing only within cwd.
2. Debug Mode Enabled (app.py) – Flask was running with debug=True, which exposes an interactive debugger to anyone who can reach the server. Fixed by setting debug=False
3. Server Information Exposure (3 instances in app.py) – Exception details ({e}) were included in JSON error responses returned to the client, potentially leaking stack traces, database internals or network topology. Fixed by replacing with generic error messages while keeping the details in server-side logs only.