snyk code test

```
(.venv) PS F:\Projects\jhu_software_concepts\module_5> snyk code test

Testing F:\Projects\jhu_software_concepts\module_5 ...

Open Issues

 ✗ [MEDIUM] Path Traversal
   Finding ID: bb659755-c2ec-42ab-b105-339b36c93b07
   Path: src/subprocess/llm_hosting/app.py, line 297
   Info: Unsanitized input from a command line argument flows into open, where it is used as a pat
h. This may result in a Path Traversal vulnerability and allow an attacker to read arbitrary files
.

 ✗ [MEDIUM] Path Traversal
   Finding ID: 0e6ce5bf-73bc-485b-b1e1-310fca70a279
   Path: src/subprocess/llm_hosting/app.py, line 305
   Info: Unsanitized input from a command line argument flows into open, where it is used as a pat
h. This may result in a Path Traversal vulnerability and allow an attacker to write arbitrary file
s.

 ✗ [MEDIUM] Path Traversal
   Finding ID: 19db025e-babf-4ae2-8912-6c794e1da8a1
   Path: src/subprocess/llm_hosting/app.py, line 318
   Info: Unsanitized input from a command line argument flows into json.dump, where it is used as
a path. This may result in a Path Traversal vulnerability and allow an attacker to write arbitrary
 files.

 ✗ [MEDIUM] Debug Mode Enabled
   Finding ID: 50e8d914-b75e-4e8d-a8d1-508698e3c8f0
   Path: src/app.py, line 193
   Info: Running the application in debug mode (debug flag is set to True in run) is a security ri
sk if the application is accessible by untrusted parties.


Test Summary

  Organization:      sivag1
  Test type:         Static code analysis
  Project path:      F:\Projects\jhu_software_concepts\module_5

  Total issues:   4
  Ignored issues: 0 [ 0 HIGH  0 MEDIUM  0 LOW ]
  Open issues:    4 [ 0 HIGH  4 MEDIUM  0 LOW ]
```

3 errors coming from the llm_hosting/app.py (provided file):

This calls out the potential vulnerability in passing of JSON. An attacker could write malicious files.

1 error from our app.py:

This is because I have the app getting launched with Debug flag True which is expected as we are still in development.