Vulnora AI Security Report

Scan Summary

Project Path	**/Users/dharanisham/Developer/Github-Repositories/Vulnora-AI/test_project**
Scan Date	**2025-12-01 09:51:44**
Smell Score	**17.00 / 100**
Files Scanned	**2**
Total Issues	**3**

Detailed Findings

#1 [Critical] Command Injection

File: /Users/dharanisham/Developer/Github-Repositories/Vulnora-AI/test_project/vulnerable.py:6

Description: User input is directly concatenated into a system command, allowing an attacker to inject arbitrary commands.

Suggested Fix: subprocess.run(['ls', user_input], check=True)

Vulnerable Code:

```
os.system("ls " + user_input)
```

--

#2 [High] Hardcoded Secret

File: /Users/dharanisham/Developer/Github-Repositories/Vulnora-AI/test_project/vulnerable.py:8

Description: A sensitive API key is hardcoded in plain text, allowing an attacker to access the API without authentication.

Suggested Fix: import os; api_key = os.environ.get('API_KEY')

Vulnerable Code:

```
api_key = "12345678901234567890123456789012345"
```

--

#3 [Medium] Taint Flow

File: /Users/dharanisham/Developer/Github-Repositories/Vulnora-AI/test_project/vulnerable.py:10

Description: User input is echoed to the console without proper sanitization, potentially leading to information disclosure.

Suggested Fix: print(user_input)

Vulnerable Code:

```
subprocess.Popen("echo " + user_input, shell=True)
```

--