Bandit Analysis Report

Analysis Results:

File: .\temp_code.py
Issue: Consider possible security implications associated with the subprocess module.
Severity: LOW
Confidence: HIGH
Line Number: 7

File: .\temp_code.py
Issue: Probable insecure usage of temp file/directory.
Severity: MEDIUM
Confidence: MEDIUM
Line Number: 21

File: .\temp_code.py
Issue: subprocess call with shell=True identified, security issue.
Severity: HIGH
Confidence: HIGH
Line Number: 33

File: .\temp_code.py
Issue: Possible SQL injection vector through string-based query construction.
Severity: MEDIUM
Confidence: LOW
Line Number: 45

File: .\temp_code.py
Issue: Possible hardcoded password: 'password123'
Severity: LOW
Confidence: MEDIUM
Line Number: 71

File: .\temp_code.py

Issue: Possible hardcoded password: 'This is sensitive information!'

Severity: LOW

Confidence: MEDIUM

Line Number: 79

File: .\temp_code.py

Issue: Use of weak MD5 hash for security. Consider usedforsecurity=False

Severity: HIGH

Confidence: HIGH

Line Number: 109

File: .\temp_code.py

Issue: Use of possibly insecure function - consider using safer ast.literal_eval.

Severity: MEDIUM

Confidence: HIGH

Line Number: 125
