

■■ Security Scan Report

Generated on: 2024-11-15 11:56:24

■ Bandit Findings

Severity	Issue	File	Line
LOW	Consider possible security implications associated with pickle module	app_vulnerable.py	4
LOW	Possible hardcoded password: 'supersecretkey'	./app_vulnerable.py	9
MEDIUM	Possible SQL injection vector through string-based query construction	app_vulnerable.py	62
MEDIUM	Possible SQL injection vector through string-based query construction	app_vulnerable.py	73
HIGH	Starting a process with a shell, possible injection detected	app_vulnerable.py	118
MEDIUM	Pickle and modules that wrap it can be unsafe when used to process untrusted data, possible security issue	app_vulnerable.py	127

■ Semgrep Findings

Severity	Message	File	Line
WARNING	N/A	app_vulnerable.py	8
ERROR	N/A	app_vulnerable.py	9
WARNING	N/A	app_vulnerable.py	40
WARNING	N/A	app_vulnerable.py	57
WARNING	N/A	app_vulnerable.py	58
WARNING	N/A	app_vulnerable.py	62
ERROR	N/A	app_vulnerable.py	62
ERROR	N/A	app_vulnerable.py	62
ERROR	N/A	app_vulnerable.py	62
WARNING	N/A	app_vulnerable.py	69
WARNING	N/A	app_vulnerable.py	73
ERROR	N/A	app_vulnerable.py	73
ERROR	N/A	app_vulnerable.py	73
ERROR	N/A	app_vulnerable.py	73
WARNING	N/A	app_vulnerable.py	77
ERROR	N/A	app_vulnerable.py	116
ERROR	N/A	app_vulnerable.py	118
ERROR	N/A	app_vulnerable.py	118
ERROR	N/A	app_vulnerable.py	127
WARNING	N/A	app_vulnerable.py	127
WARNING	N/A	app_vulnerable.py	128

■ Pylint Findings

Type	Message	Module	Line
------	---------	--------	------

convention	Final newline missing	tempCodeRunnerFile	2
convention	Missing module docstring	tempCodeRunnerFile	1
convention	Module name "tempCodeRunnerFile" doesn't conform to snake_case naming style	tempCodeRunnerFile	1
convention	standard import "sqlite3" should be placed before third party imports like "Flask"	tempCodeRunnerFile	2
warning	Unused Flask imported from flask	tempCodeRunnerFile	1
warning	Unused request imported from flask	tempCodeRunnerFile	1
warning	Unused render_template_string imported from flask	tempCodeRunnerFile	1
warning	Unused import sqlite3	tempCodeRunnerFile	2
convention	Missing module docstring	app_vulnerable	1
convention	Missing function or method docstring	app_vulnerable	15
convention	Missing function or method docstring	app_vulnerable	20
convention	Missing function or method docstring	app_vulnerable	34
convention	Missing function or method docstring	app_vulnerable	56
convention	Missing function or method docstring	app_vulnerable	68
convention	Missing function or method docstring	app_vulnerable	87
convention	Missing function or method docstring	app_vulnerable	107
convention	Missing function or method docstring	app_vulnerable	115
convention	Missing function or method docstring	app_vulnerable	122
convention	standard import "sqlite3" should be placed before third party imports like "Flask"	app_vulnerable	2
convention	standard import "os" should be placed before third party imports like "Flask"	app_vulnerable	3
convention	standard import "pickle" should be placed before third party imports like "Flask"	app_vulnerable	4
warning	Unused secure_filename imported from werkzeug.utils	app_vulnerable	5