Semgrep Report

Category	python.sqlalchemy.security.sqlalchemy-execute-raw-query.sqlalchemy-execute-raw-query
Description	Avoiding SQL string concatenation: untrusted input concatenated with raw SQL query can result in SQ
Severity Level	High
Reference	https://sg.run/2b1L
Affected Lines	29 cursor.execute(query)

Category	python.lang.security.audit.formatted-sql-query.formatted-sql-query
Description	Detected possible formatted SQL query. Use parameterized queries instead.
Severity Level	Medium
Reference	https://sg.run/EkWw
Affected Lines	29 cursor.execute(query)

Category	python.flask.security.audit.render-template-string.render-template-string
Description	Found a template created with string formatting. This is susceptible to server-side template injection ar
Severity Level	Medium
Reference	https://sg.run/8yjE
Affected Lines	42 return render_template_string(f"<h1>Hello, {user_name}!</h1>")

Category	python.django.security.injection.raw-html-format.raw-html-format
Description	Detected user input flowing into a manually constructed HTML string. You may be accidentally bypass
Severity Level	Medium

Reference	https://sg.run/oYj1
Affected Lines	42 return render_template_string(f"<h1>Hello, {user_name}!</h1>")

Category	python.flask.security.injection.raw-html-concat.raw-html-format
Description	Detected user input flowing into a manually constructed HTML string. You may be accidentally bypass
Severity Level	Medium
Reference	https://sg.run/Pb7e
Affected Lines	42 return render_template_string(f"<h1>Hello, {user_name}!</h1>")

Category	python.flask.security.audit.debug-enabled.debug-enabled
Description	Detected Flask app with debug=True. Do not deploy to production with this flag enabled as it will leak
Severity Level	Medium
Reference	https://sg.run/dKrd
Affected Lines	60 app.run(debug=True) # Start Flask app for XSS demo

Category	python.flask.debug.debug-flask.active-debug-code-flask
Description	The application is running debug code or has debug mode enabled. This may expose sensitive inform
Severity Level	Low
Reference	https://sg.run/lBbpB
Affected Lines	60 app.run(debug=True) # Start Flask app for XSS demo