■ HYBRIDSCAN SECURITY AUDIT REPORT

REPORT INFORMATION	
Scan Type:	HYBRID
Target:	SAST:54 + DAST:55
Generated:	2025-12-03 01:57:03
Timestamp:	2025-12-03T06:55:03.038776

VULNERABILITY SUMMARY

Metric	Count	Percentage
■ CRITICAL	1	7.1%
■ HIGH	2	14.3%
■ MEDIUM	5	35.7%
■ LOW	6	42.9%
TOTAL	**14**	**100%**

HYBRID CORRELATION METRICS

Metric	Value
Total SAST Findings	12
Total DAST Findings	2
False Positive Reduction	0.0%

DETAILED FINDINGS

1. blacklist [SAST] [LOW]

Description: Consider possible security implications associated with pickle module.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:7

CWE: 502

Remediation: https://bandit.readthedocs.io/en/1.8.0/blacklists/blacklist_imports.html#b403-import-pickle

Detected by: bandit

2. blacklist [SAST] [LOW]

Description: Consider possible security implications associated with the subprocess module.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:8

CWE: 78

Remediation: https://bandit.readthedocs.io/en/1.8.0/blacklists/blacklist_imports.html#b404-import-subprocess

Detected by: bandit

3. hardcoded_password_string [SAST] [LOW]

Description: Possible hardcoded password: 'admin123password'

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:15

CWE: 259

Remediation: https://bandit.readthedocs.io/en/1.8.0/plugins/b105_hardcoded_password_string.html

Detected by: bandit

4. hardcoded_password_string [SAST] [LOW]

Description: Possible hardcoded password: 'root_password_123'

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:16

CWE: 259

Remediation: https://bandit.readthedocs.io/en/1.8.0/plugins/b105_hardcoded_password_string.html

Detected by: bandit

5. hardcoded_sql_expressions [SAST] [MEDIUM]

Description: Possible SQL injection vector through string-based query construction.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:25

CWE: 89

Remediation: https://bandit.readthedocs.io/en/1.8.0/plugins/b608_hardcoded_sql_expressions.html

Detected by: bandit

6. start_process_with_a_shell [SAST] [HIGH]

Description: Starting a process with a shell, possible injection detected, security issue.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:34

CWE: 78

Remediation: https://bandit.readthedocs.io/en/1.8.0/plugins/b605_start_process_with_a_shell.html

Detected by: bandit

7. blacklist [SAST] [MEDIUM]

Description: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:42

CWE: 502

Remediation: https://bandit.readthedocs.io/en/1.8.0/blacklists/blacklist_calls.html#b301-pickle

Detected by: bandit

8. blacklist [SAST] [MEDIUM]

Description: Use of insecure and deprecated function (mktemp).

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:57

CWE: 377

Remediation: https://bandit.readthedocs.io/en/1.8.0/blacklists/blacklist_calls.html#b306-mktemp-q

Detected by: bandit

9. assert_used [SAST] [LOW]

Description: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:67

CWE: 703

Remediation: https://bandit.readthedocs.io/en/1.8.0/plugins/b101_assert_used.html

Detected by: bandit

10. blacklist [SAST] [LOW]

Description: Standard pseudo-random generators are not suitable for security/cryptographic purposes.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:76

CWE: 330

Remediation: https://bandit.readthedocs.io/en/1.8.0/blacklists/blacklist_calls.html#b311-random

Detected by: bandit

11. flask_debug_true [SAST] [HIGH]

Description: A Flask app appears to be run with debug=True, which exposes the Werkzeug debugger and allows the execution of arbitrary code.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:81

CWE: 94

Remediation: https://bandit.readthedocs.io/en/1.8.0/plugins/b201_flask_debug_true.html

Detected by: bandit

12. hardcoded_bind_all_interfaces [SAST] [MEDIUM]

Description: Possible binding to all interfaces.

Location: C:\Users\oscar\AppData\Local\Temp\hybridscan_secure\scan_20251203_011521_112f763b\vulnerable_app.py:81

CWE: 605

Remediation: https://bandit.readthedocs.io/en/1.8.0/plugins/b104_hardcoded_bind_all_interfaces.html

Detected by: bandit

13. SQL Injection [DAST] [CRITICAL]

Description: No description

URL: https://api.ejemplo.com/v1/users/user

Detected by: OWASP ZAP

14. Insecure Direct Object Reference (IDOR) [DAST] [MEDIUM]

Description: No description

URL: https://api.ejemplo.com/v1/users/profile

Detected by: OWASP ZAP