DevSecode Security Report

Project: TestObject

Generated on: 22.8.2025, 14:56:38

Severity: Medium

Tool: Trivy

File: requirements.txt

Line: 1

Rule: CVE-2020-28493

Description: python-jinja2: ReDoS vulnerability in the urlize filter

Snippet: jinja2

Recommendation: It is recommended to review uses of 'CVE-2020-28493', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Trivy

File: requirements.txt

Line: 1

Rule: CVE-2024-22195

Description: jinja2: HTML attribute injection when passing user input as keys to xmlattr filter

Snippet: jinja2

Recommendation: It is recommended to review uses of 'CVE-2024-22195', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Trivy

File: requirements.txt

Line: 1

Rule: CVE-2024-34064

Description: jinja2: accepts keys containing non-attribute characters

Snippet: jinja2

Recommendation: It is recommended to review uses of 'CVE-2024-34064', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Trivy

File: requirements.txt

Line: 1

Rule: CVE-2024-56326

Description: jinja2: Jinja has a sandbox breakout through indirect reference to format method

Snippet: jinja2

Recommendation: It is recommended to review uses of 'CVE-2024-56326', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Trivy

File: requirements.txt

Line: 1

Rule: CVE-2025-27516

Description: jinja2: Jinja sandbox breakout through attr filter selecting format method

Snippet: jinja2

Recommendation: It is recommended to review uses of 'CVE-2025-27516', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Trivy

File: requirements.txt

Line: 1

Rule: CVE-2023-32681

Description: python-requests: Unintended leak of Proxy-Authorization header

Snippet: requests

Recommendation: It is recommended to review uses of 'CVE-2023-32681', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Trivy

File: requirements.txt

Line: 1

Rule: CVE-2024-35195

Description: requests: subsequent requests to the same host ignore cert verification

Snippet: requests

Recommendation: It is recommended to review uses of 'CVE-2024-35195', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Trivy

File: requirements.txt

Line: 1

Rule: CVE-2024-47081

Description: requests: Requests vulnerable to .netrc credentials leak via malicious URLs

Snippet: requests

Recommendation: It is recommended to review uses of 'CVE-2024-47081', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Bandit

File: /Users/bardavidi/Desktop/DevSecode/TestObject/secretDetection_test.py

Line: 17

Rule: B307

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

Recommendation: It is recommended to review uses of 'B307', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Bandit

File: /Users/bardavidi/Desktop/DevSecode/TestObject/secretDetection_test.py

Line: 31

Rule: B301

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

Recommendation: It is recommended to review uses of 'B301', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Bandit

File: /Users/bardavidi/Desktop/DevSecode/TestObject/secretDetection_test.py

Line: 41

Rule: B108

Description: Probable insecure usage of temp file/directory.

Recommendation: It is recommended to review uses of 'B108', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Bandit

File: /Users/bardavidi/Desktop/DevSecode/TestObject/secretDetection_test.py

Line: 58

Rule: B113

Description: Call to requests without timeout

Recommendation: It is recommended to review uses of 'B113', follow secure coding practices, and replace any exposed secrets with secure storage methods.