

DevSecode Security Report

Project: TestObjects

Generated on: 19.6.2025, 14:10:36

Secret Detection

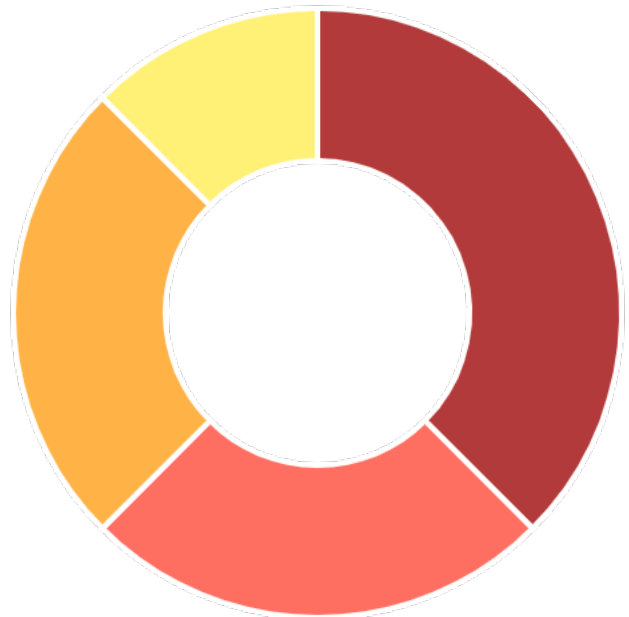
Findings by Type:

- gitlab-pat
- stripe-access-token
- algolia-api-key
- private-key
- slack-webhook-url
- generic-api-key



Findings by Severity:



- Critical
- High
- Medium
- Low



Software Composition Analysis (SCA)

Findings by Type:

Findings by Severity:

-  Critical
-  High
-  Medium
-  Low

Static Application Security Testing (SAST)

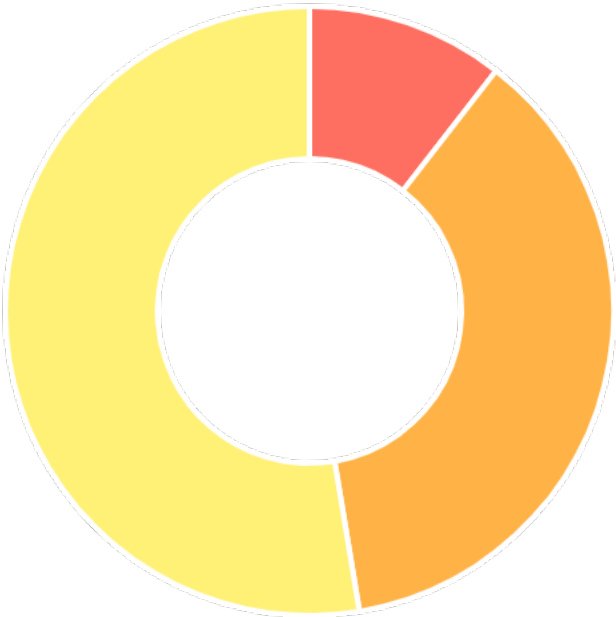
Findings by Type:

- hardcoded_bind_all_interfaces
- assert_used
- exec_used
- hardcoded_password_string
- hardcoded_tmp_directory
- try_except_pass
- flask_debug_true
- hashlib
- markupsafe_markup_xss
- request_without_timeout
- yaml_load



Findings by Severity:

- Critical
- High
- Medium
- Low



Severity: Medium

Tool: Bandit

File: /Users/macbook/DevSecode/TestObjects/sca_test.py

Line: 6

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.

Severity: Medium

Tool: Bandit

File: /Users/macbook/DevSecode/TestObjects/sast_test.py

Line: 7

Rule: B102

Description: Use of exec detected.

Recommendation: It is recommended to review uses of 'B102', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Bandit

File: /Users/macbook/DevSecode/TestObjects/sca_test.py

Line: 7

Rule: B506

Description: Use of unsafe yaml load. Allows instantiation of arbitrary objects. Consider `yaml.safe_load()`.

Recommendation: It is recommended to review uses of 'B506', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Bandit

File: /Users/macbook/DevSecode/TestObjects/dast_test.py

Line: 10

Rule: B104

Description: Possible binding to all interfaces.

Recommendation: It is recommended to review uses of 'B104', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Critical

Tool: Gitleaks

File: /Users/macbook/DevSecode/TestObjects/secretDetection_test.py

Line: 11

Rule: gitlab-pat

Description: Identified a GitLab Personal Access Token, risking unauthorized access to GitLab repositories and codebase exposure.

Snippet: REDACTED

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

Severity: Critical

Tool: Gitleaks

File: /Users/macbook/DevSecode/TestObjects/secretDetection_test.py

Line: 11

Rule: generic-api-key

Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.

Snippet: gitlab_token = "REDACTED"

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

Severity: Medium

Tool: Bandit

File: /Users/macbook/DevSecode/TestObjects/sast_test.py

Line: 12

Rule: B104

Description: Possible binding to all interfaces.

Recommendation: It is recommended to review uses of 'B104', follow secure coding practices, and replace any exposed secrets with secure storage methods.

Severity: Medium

Tool: Bandit

File: /Users/macbook/DevSecode/TestObjects/sast_test.py

Line: 19

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: Critical

Tool: Gitleaks

File: /Users/macbook/DevSecode/TestObjects/secretDetection_test.py

Line: 24

Rule: stripe-access-token

Description: Found a Stripe Access Token, posing a risk to payment processing services and sensitive financial data.

Snippet: REDACTED"

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

Severity: Medium

Tool: Gitleaks

File: /Users/macbook/DevSecode/TestObjects/secretDetection_test.py

Line: 29

Rule: generic-api-key

Description: Detected a Generic API Key, potentially exposing access to various services and sensitive operations.

Snippet: twilio_auth_token = "REDACTED"

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

Severity: Medium

Tool: Gitleaks

File: /Users/macbook/DevSecode/TestObjects/secretDetection_test.py

Line: 30

Rule: algolia-api-key

Description: Identified an Algolia API Key, which could result in unauthorized search operations and data exposure on Algolia-managed platforms.

Snippet: algolia_api_key = "REDACTED"

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

Severity: Medium

Tool: Bandit

File: /Users/macbook/DevSecode/TestObjects/sast_test.py

Line: 38

Rule: B704

Description: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.

Recommendation: It is recommended to review uses of 'B704', follow secure coding practices, and replace any exposed secrets with secure storage methods.