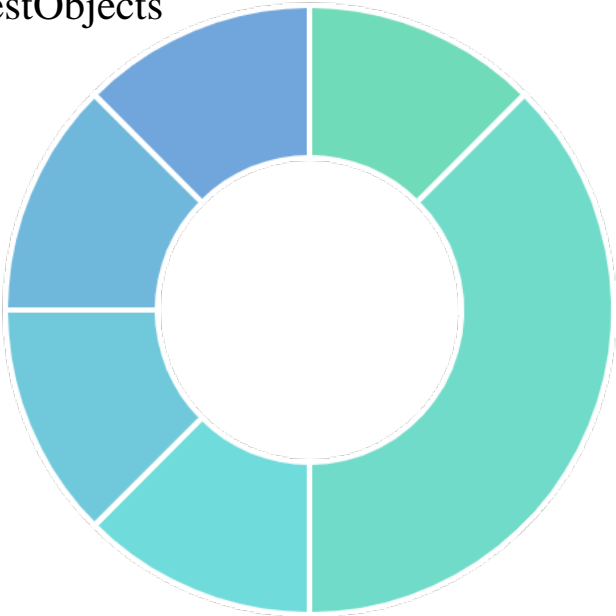


# DevSecode Security Report

## Findings by Type:

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

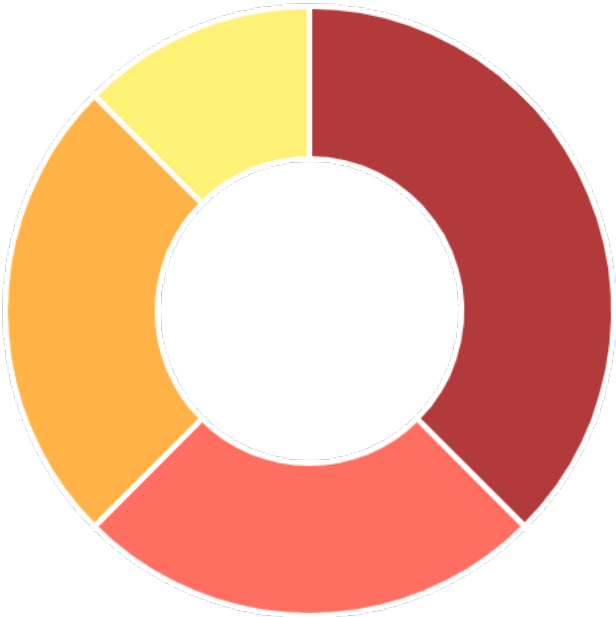
Project: TestObjects



## Secret Detection

## 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)

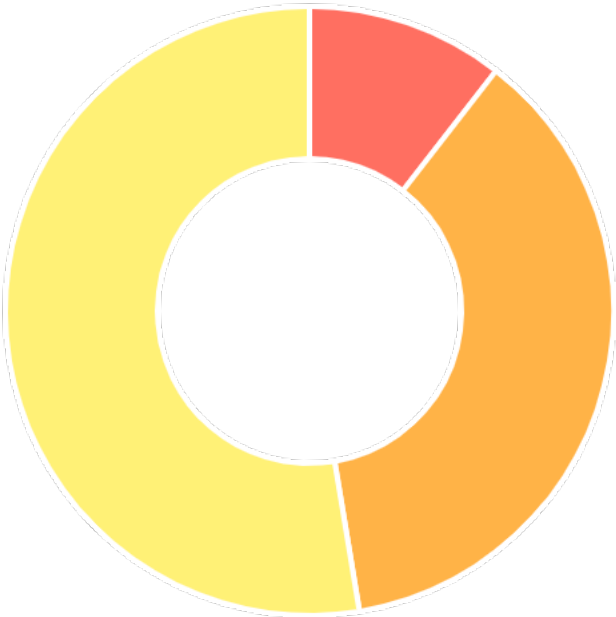
## Findings by Type:

- 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: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/sast\_test.py

**Line:** 3

**Rule:** B101

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

**Recommendation:** It is recommended to review uses of 'B101', follow secure coding practices, and replace any exposed secrets with secure storage methods.

## Severity: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 5

**Rule:** B105

**Description:** Possible hardcoded password: 'wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY'

**Recommendation:** It is recommended to review uses of 'B105', 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:** 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:** 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: 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: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 11

**Rule:** B105

**Description:** Possible hardcoded password: 'glpat-12345678abcdefgHijKLMNOPqrstu'

**Recommendation:** It is recommended to review uses of 'B105', 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: Low

**Tool:** Gitleaks

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 14

**Rule:** slack-webhook-url

**Description:** Discovered a Slack Webhook, which could lead to unauthorized message posting and data leakage in Slack channels.

**Snippet:** REDACTED

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

## Severity: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/sast\_test.py

**Line:** 15

**Rule:** B105

**Description:** Possible hardcoded password: 'SuperSecret123!'

**Recommendation:** It is recommended to review uses of 'B105', 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: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 19

**Rule:** B105

**Description:** Possible hardcoded password: 'ddf'

**Recommendation:** It is recommended to review uses of 'B105', 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: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/sast\_test.py

**Line:** 24

**Rule:** B110

**Description:** Try, Except, Pass detected.

**Recommendation:** It is recommended to review uses of 'B110', follow secure coding practices, and replace any exposed secrets with secure storage methods.

## Severity: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 24

**Rule:** B105

**Description:** Possible hardcoded password: 'sk\_test\_4eC39HqLyjWDarjtT1zdp7dc'

**Recommendation:** It is recommended to review uses of 'B105', follow secure coding practices, and replace any exposed secrets with secure storage methods.

## Severity: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 25

**Rule:** B105

**Description:** Possible hardcoded password: 'EAFakeClientSecret1234567890'

**Recommendation:** It is recommended to review uses of 'B105', 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: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 29

**Rule:** B105

**Description:** Possible hardcoded password: '1234567890abcdef1234567890abcdef'

**Recommendation:** It is recommended to review uses of 'B105', 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: High

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/sast\_test.py

**Line:** 30

**Rule:** B201

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

**Recommendation:** It is recommended to review uses of 'B201', follow secure coding practices, and replace any exposed secrets with secure storage methods.

## Severity: High

**Tool:** Gitleaks

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 33

**Rule:** generic-api-key

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

**Snippet:** jwt\_secret = "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: Low

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 33

**Rule:** B105

**Description:** Possible hardcoded password: 'myjwtsecret1234567890'

**Recommendation:** It is recommended to review uses of 'B105', follow secure coding practices, and replace any exposed secrets with secure storage methods.

## Severity: High

**Tool:** Bandit

**File:** /Users/macbook/DevSecode/TestObjects/sast\_test.py

**Line:** 34

**Rule:** B324

**Description:** Use of weak MD4 hash for security. Consider usedforsecurity=False

**Recommendation:** It is recommended to review uses of 'B324', follow secure coding practices, and replace any exposed secrets with secure storage methods.

## Severity: High

**Tool:** Gitleaks

**File:** /Users/macbook/DevSecode/TestObjects/secretDetection\_test.py

**Line:** 35

**Rule:** private-key

**Description:** Identified a Private Key, which may compromise cryptographic security and sensitive data encryption.

**Snippet:** REDACTED

**Recommendation:** It is recommended to review uses of 'private-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.