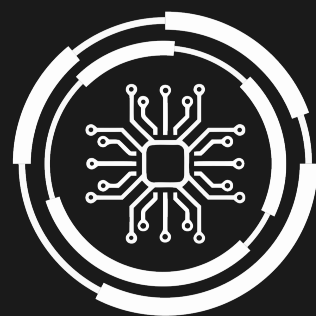


PADME

Manual & Security Audit for Train

SQLInjection

Sascha Martin Welten



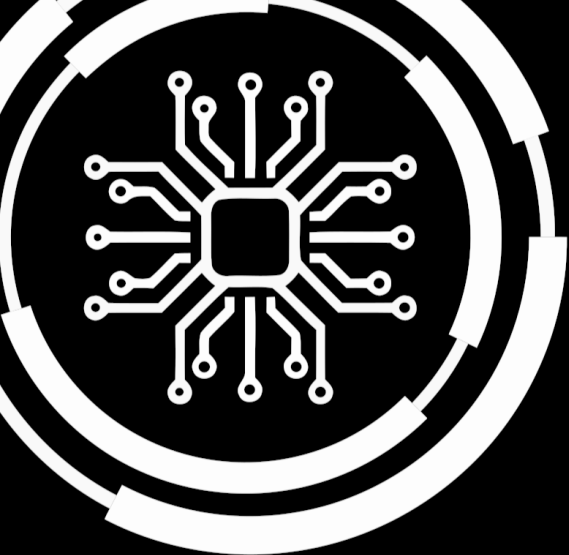
PADME

Copyright © 2023 PADME

PADME-ANALYTICS.DE

Licensed under the Creative Commons Attribution-NonCommercial 3.0 Unported License (the “License”). You may not use this file except in compliance with the License. You may obtain a copy of the License at <http://creativecommons.org/licenses/by-nc/3.0>. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

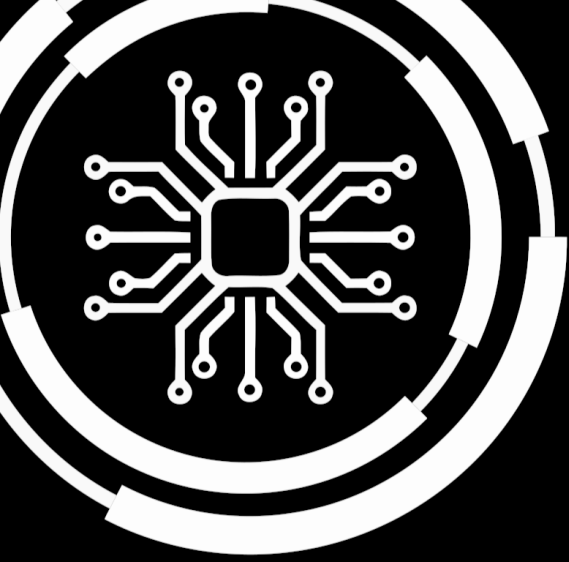
First printing, February 2, 2024



Contents

1	Train Summary	5
1.1	Overview	5
1.2	Image Building File	5
1.3	Requirements & Dependencies	6
1.4	Code Base	6
1.5	Connection Parameters	6
2	Static Train Analysis	9
2.1	SAST	9
2.2	Secret Detection	10
2.3	Dependency Analysis	10
2.4	Blacklist Detection	10
3	Train Image Analysis	11
3.1	Vulnerabilities	11
4	Dynamic Train Analysis	39
4.1	Image size differences after simulation:	39
4.1.1	Simulated route:	39
4.1.2	Directory Overview of changed files:	39
4.1.3	./simulationResults/result.txt	39
4.2	Execution metrics:	39
4.3	Network I/O:	39

5	Conclusion	41
----------	-------------------------	-----------



1. Train Summary

1.1 Overview

- **Train name:** SQLInjection
- **Creator of the train:** Sascha Martin Welten
- **Location:** <https://git.rwth-aachen.de/padme-development/padme-train-depot/-/archive/main/padme-train-depot-main.zip?path=SQLInjection>

1.2 Image Building File

Listing 1.1: Image building file

```
FROM python:3.8

WORKDIR /usr/src/app

# LABEL
LABEL "envs"="[{"name": "DATA_SOURCE_USERNAME","type":
  "text","required": true},{"name": "DATA_SOURCE_HOST
  ","type": "text","required": true},{"name": "
  DATA_SOURCE_PORT","type": "number","required": true
  },{"name": "DATA_SOURCE_PASSWORD","type": "password
  ","required": true},{"name": "STATION_NAME","type
  ":"text","required": true}]"

#Dependencies
RUN pip install --no-cache-dir psycopg2

COPY . .
```

```
CMD [ "python", "main.py" ]
```

1.3 Requirements & Dependencies

No requirements.txt found

1.4 Code Base

Legend: env query retrieve_previous_results execute_analysis save log

```

1 import psycpg2
2 import os
3
4 print("Welcome to the PADME Playground Eval!")
5 print(os.environ["STATION_NAME"])
6
7 conn = psycpg2.connect(dbname="patientdb",
8                        user=os.environ["DATA_SOURCE_USERNAME"],
9                        host=os.environ["DATA_SOURCE_HOST"],
10                       password=os.environ["DATA_SOURCE_PASSWORD"],
11                       port=os.environ["DATA_SOURCE_PORT"])
12
13 cursor = conn.cursor()
14
15 cursor.execute(f"SELECT * FROM {'patient_info' if os.environ['STATION_NAME']
16                  ']' == 'Bruegel' else 'patients'} WHERE age >= 50")
17 result = cursor.fetchall()
18 nPatientsOver50 = len(result)
19
20 # emulate SQL injection
21 age = f"50; UPDATE {'patient_info' if os.environ['STATION_NAME'] == '
22    Bruegel' else 'patients'} SET age = 999 WHERE age >= 50"
23 cursor.execute(f"SELECT * FROM {'patient_info' if os.environ['STATION_NAME']
24                  ']' == 'Bruegel' else 'patients'} WHERE age >= {age}")
25
26 print(f"Number of rows affected: {nPatientsOver50}")
27
28 nPatientsOver50 = len(result)
29
30 # Write Dummy File
31 f = open("result.txt", "a")
32 f.write(f"{nPatientsOver50}\n")
33 f.close()

```

Listing 1.2: main.py

```

1 {"resources": [{"id": "d7b0a9a7-07fd-4a31-b93a-3c946dc82667", "datasets": [{"id":
2    "34680662-1e34-11ed-861d-0242ac120002"}]}],
3    {"id": "5bce186a-5005-4ca8-878e-9d8d4e0747c0", "datasets": [{"id": "3466461a
4    -1e34-11ed-861d-0242ac120002"}]}],
5    "route": [{"id": "d7b0a9a7-07fd-4a31-b93a-3c946dc82667",
6    "ownEnvs": [{"name": "STATION_NAME", "value": "Bruegel"}]},
7    {"id": "5bce186a-5005-4ca8-878e-9d8d4e0747c0", "ownEnvs": [{"name": "
8    STATION_NAME", "value": "Klee"}]}]}

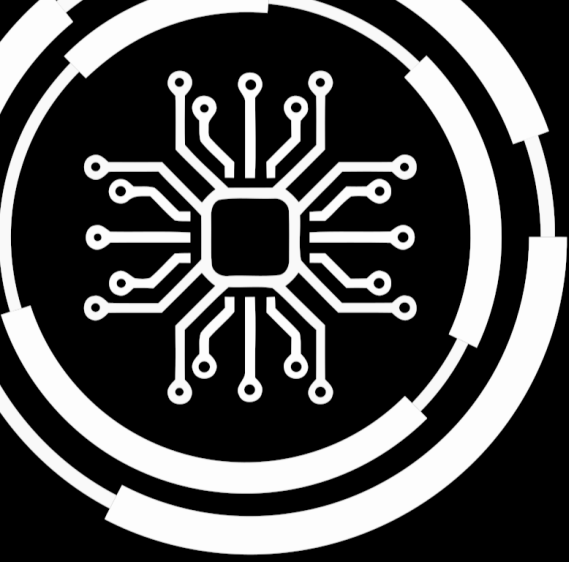
```

Listing 1.3: route.json

1.5 Connection Parameters

Overall, 5 connection parameters have been found in the train:

Name	Type	Required?
DATA_SOURCE_USERNAME	text	True
DATA_SOURCE_HOST	text	True
DATA_SOURCE_PORT	number	True
DATA_SOURCE_PASSWORD	password	True
STATION_NAME	text	True



2. Static Train Analysis

Summary 2.1

- **Number of Lines:** 223929
- **Vulnerabilities per Line:** 1.7e-05
- **Analysis Score:** 1.0

Total

Summary: Low: 0 Medium: 2 High: 2

2.1 SAST

Summary: Low: 0 Medium: 2 High: 2

Detailed Vulnerabilities:

Vulnerability 2.1

Test-specific ID: dc30536032fb7ff53e20606cd68ce292999acdba323b6a9ef5b908fee30b1f2f

Severity: Medium

Identifiers:

- **semgrep_id:** bandit.B608
- **cwe:** 89
- **owasp:** A1
- **bandit_test_id:** B608

Message: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

File: SQLInjection/main.py

Start line: 15

Vulnerability 2.2

Test-specific ID: fba7d9dfb2337c2e05f9a6d3687c391b318b984e2b7a106ea06e772c75e74128

Severity: Medium

Identifiers:

- **semgrep_id:** bandit.B608
- **cwe:** 89
- **owasp:** A1
- **bandit_test_id:** B608

Message: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

File: SQLInjection/main.py

Start line: 21

2.2 Secret Detection

Summary: Low: 0 Medium: 0 High: 0

Detailed Secret Detection:

2.3 Dependency Analysis

Summary: Low: 0 Medium: 0 High: 0

Detailed Dependency Analysis:

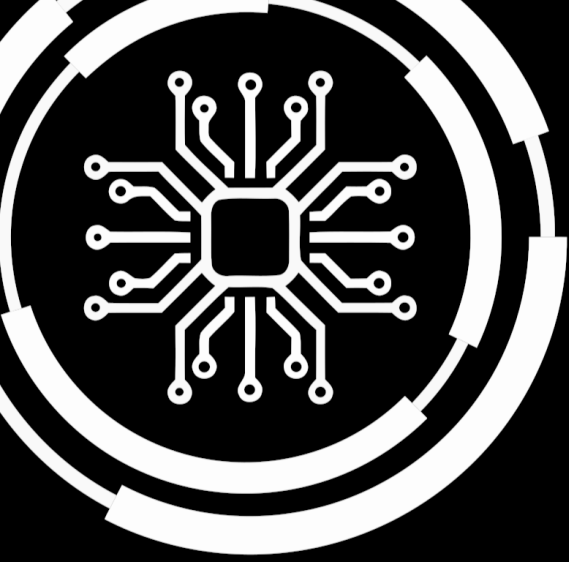
2.4 Blacklist Detection

The following patterns have been configured:

\bPOST\b

The following matches have been found:

None



3. Train Image Analysis

3.1 Vulnerabilities

Summary: **Low:** 179 **Medium:** 2 **High:** 1 **Critical:** 1

Detailed Vulnerabilities:

Critical:

Vulnerability 3.1

Test-specific ID: SNYK-DEBIAN12-ZLIB-6008963 **Severity:** critical

Identifiers: **Message:**Integer Overflow or Wraparound

High:

Vulnerability 3.2

Test-specific ID: SNYK-DEBIAN12-OPENSSSH-6139205 **Severity:** high

Identifiers: **Message:**CVE-2023-51767

Medium:

Vulnerability 3.3

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-5746982 **Severity:** medium

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.4

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-5933304 **Severity:** medium

Identifiers: **Message:**Use After Free

Low:

Vulnerability 3.5

Test-specific ID: SNYK-DEBIAN12-AOM-5878995 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.6

Test-specific ID: SNYK-DEBIAN12-AOM-6140324 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.7

Test-specific ID: SNYK-DEBIAN12-APT-1541449 **Severity:** low

Identifiers: **Message:**Improper Verification of Cryptographic Signature

Vulnerability 3.8

Test-specific ID: SNYK-DEBIAN12-BINUTILS-1542107 **Severity:** low

Identifiers: **Message:**Integer Overflow or Wraparound

Vulnerability 3.9

Test-specific ID: SNYK-DEBIAN12-BINUTILS-1542119 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.10

Test-specific ID: SNYK-DEBIAN12-BINUTILS-1542166 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.11

Test-specific ID: SNYK-DEBIAN12-BINUTILS-1542259 **Severity:** low

Identifiers: **Message:**Uncontrolled Recursion

Vulnerability 3.12

Test-specific ID: SNYK-DEBIAN12-BINUTILS-1542441 **Severity:** low

Identifiers: **Message:**Allocation of Resources Without Limits or Throttling

Vulnerability 3.13

Test-specific ID: SNYK-DEBIAN12-BINUTILS-5422222 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.14

Test-specific ID: SNYK-DEBIAN12-BINUTILS-5803143 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.15

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542206 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.16

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542243 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.17

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542258 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.18

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542269 **Severity:** low

Identifiers: **Message:** Out-of-Bounds

Vulnerability 3.19

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542283 **Severity:** low

Identifiers: **Message:** Out-of-Bounds

Vulnerability 3.20

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542377 **Severity:** low

Identifiers: **Message:** Out-of-Bounds

Vulnerability 3.21

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542408 **Severity:** low

Identifiers: **Message:** Out-of-Bounds

Vulnerability 3.22

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542413 **Severity:** low

Identifiers: **Message:** Out-of-Bounds

Vulnerability 3.23

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542489 **Severity:** low

Identifiers: **Message:** Use After Free

Vulnerability 3.24

Test-specific ID: SNYK-DEBIAN12-BLUEZ-1542671 **Severity:** low

Identifiers: **Message:** Out-of-Bounds

Vulnerability 3.25

Test-specific ID: SNYK-DEBIAN12-CAIRO-1542506 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.26

Test-specific ID: SNYK-DEBIAN12-CAIRO-1542635 **Severity:** low

Identifiers: **Message:**Reachable Assertion

Vulnerability 3.27

Test-specific ID: SNYK-DEBIAN12-CAIRO-1542674 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.28

Test-specific ID: SNYK-DEBIAN12-CAIRO-1542729 **Severity:** low

Identifiers: **Message:**Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability 3.29

Test-specific ID: SNYK-DEBIAN12-COREUTILS-1543939 **Severity:** low

Identifiers: **Message:**Improper Input Validation

Vulnerability 3.30

Test-specific ID: SNYK-DEBIAN12-COREUTILS-1543947 **Severity:** low

Identifiers: **Message:**Race Condition

Vulnerability 3.31

Test-specific ID: SNYK-DEBIAN12-DAV1D-5518047 **Severity:** low

Identifiers: **Message:**Race Condition

Vulnerability 3.32

Test-specific ID: SNYK-DEBIAN12-DJVULIBRE-5858453 **Severity:** low

Identifiers: **Message:** Divide By Zero

Vulnerability 3.33

Test-specific ID: SNYK-DEBIAN12-DJVULIBRE-5858454 **Severity:** low

Identifiers: **Message:** Divide By Zero

Vulnerability 3.34

Test-specific ID: SNYK-DEBIAN12-GCC12-2606941 **Severity:** low

Identifiers: **Message:** Uncontrolled Recursion

Vulnerability 3.35

Test-specific ID: SNYK-DEBIAN12-GCC12-5901316 **Severity:** low

Identifiers: **Message:** CVE-2023-4039

Vulnerability 3.36

Test-specific ID: SNYK-DEBIAN12-GDKPIXBUF-6207393 **Severity:** low

Identifiers: **Message:** CVE-2022-48622

Vulnerability 3.37

Test-specific ID: SNYK-DEBIAN12-GIT-1547086 **Severity:** low

Identifiers: **Message:** Improper Input Validation

Vulnerability 3.38

Test-specific ID: SNYK-DEBIAN12-GIT-2399902 **Severity:** low

Identifiers: **Message:** Exposure of Resource to Wrong Sphere

Vulnerability 3.39

Test-specific ID: SNYK-DEBIAN12-GIT-5461948 **Severity:** low

Identifiers: **Message:**Use of Externally-Controlled Format String

Vulnerability 3.40

Test-specific ID: SNYK-DEBIAN12-GIT-5461953 **Severity:** low

Identifiers: **Message:**Directory Traversal

Vulnerability 3.41

Test-specific ID: SNYK-DEBIAN12-GIT-5461954 **Severity:** low

Identifiers: **Message:**Arbitrary Code Injection

Vulnerability 3.42

Test-specific ID: SNYK-DEBIAN12-GLIB20-1547042 **Severity:** low

Identifiers: **Message:**Cryptographic Issues

Vulnerability 3.43

Test-specific ID: SNYK-DEBIAN12-GLIBC-1546991 **Severity:** low

Identifiers: **Message:**Information Exposure

Vulnerability 3.44

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547039 **Severity:** low

Identifiers: **Message:**Uncontrolled Recursion

Vulnerability 3.45

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547069 **Severity:** low

Identifiers: **Message:**Uncontrolled Recursion

Vulnerability 3.46

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547135 **Severity:** low

Identifiers: **Message:**Use of Insufficiently Random Values

Vulnerability 3.47

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547196 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.48

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547293 **Severity:** low

Identifiers: **Message:**Resource Management Errors

Vulnerability 3.49

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547373 **Severity:** low

Identifiers: **Message:**CVE-2019-1010023

Vulnerability 3.50

Test-specific ID: SNYK-DEBIAN12-GNUPG2-3330747 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.51

Test-specific ID: SNYK-DEBIAN12-GNUTLS28-1547121 **Severity:** low

Identifiers: **Message:**Improper Input Validation

Vulnerability 3.52

Test-specific ID: SNYK-DEBIAN12-GNUTLS28-6159410 **Severity:** low

Identifiers: **Message:**Improper Verification of Cryptographic Signature

Vulnerability 3.53

Test-specific ID: SNYK-DEBIAN12-GNUTLS28-6159418 **Severity:** low

Identifiers: **Message:**Information Exposure

Vulnerability 3.54

Test-specific ID: SNYK-DEBIAN12-HARFBUZZ-3311294 **Severity:** low

Identifiers: **Message:**Allocation of Resources Without Limits or Throttling

Vulnerability 3.55

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548360 **Severity:** low

Identifiers: **Message:**Missing Release of Resource after Effective Lifetime

Vulnerability 3.56

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548383 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.57

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548409 **Severity:** low

Identifiers: **Message:**Missing Release of Resource after Effective Lifetime

Vulnerability 3.58

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548461 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.59

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548464 **Severity:** low

Identifiers: **Message:**CVE-2005-0406

Vulnerability 3.60

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548490 **Severity:** low

Identifiers: **Message:**Resource Management Errors

Vulnerability 3.61

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548733 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.62

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548737 **Severity:** low

Identifiers: **Message:**Resource Exhaustion

Vulnerability 3.63

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-1548871 **Severity:** low

Identifiers: **Message:**Divide By Zero

Vulnerability 3.64

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-2441368 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.65

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-3027312 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.66

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-3358958 **Severity:** low

Identifiers: **Message:**Improper Input Validation

Vulnerability 3.67

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-5421094 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.68

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-5591136 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.69

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-5660573 **Severity:** low

Identifiers: **Message:**OS Command Injection

Vulnerability 3.70

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-5660608 **Severity:** low

Identifiers: **Message:**Integer Overflow or Wraparound

Vulnerability 3.71

Test-specific ID: SNYK-DEBIAN12-IMAGEMAGICK-5707518 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.72

Test-specific ID: SNYK-DEBIAN12-JANSSON-1548880 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.73

Test-specific ID: SNYK-DEBIAN12-JBIGKIT-1549085 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.74

Test-specific ID: SNYK-DEBIAN12-KRB5-1549480 **Severity:** low

Identifiers: **Message:**Integer Overflow or Wraparound

Vulnerability 3.75

Test-specific ID: SNYK-DEBIAN12-LIBDE265-6105348 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.76

Test-specific ID: SNYK-DEBIAN12-LIBDE265-6105349 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.77

Test-specific ID: SNYK-DEBIAN12-LIBDE265-6105361 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.78

Test-specific ID: SNYK-DEBIAN12-LIBGCRYPT20-1550206 **Severity:** low

Identifiers: **Message:**Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.79

Test-specific ID: SNYK-DEBIAN12-LIBHEIF-5498469 **Severity:** low

Identifiers: **Message:**Divide By Zero

Vulnerability 3.80

Test-specific ID: SNYK-DEBIAN12-LIBHEIF-6105360 **Severity:** low

Identifiers: **Message:**CVE-2023-49462

Vulnerability 3.81

Test-specific ID: SNYK-DEBIAN12-LIBHEIF-6105367 **Severity:** low

Identifiers: **Message:**CVE-2023-49460

Vulnerability 3.82

Test-specific ID: SNYK-DEBIAN12-LIBHEIF-6105368 **Severity:** low

Identifiers: **Message:**CVE-2023-49464

Vulnerability 3.83

Test-specific ID: SNYK-DEBIAN12-LIBHEIF-6105378 **Severity:** low

Identifiers: **Message:**CVE-2023-49463

Vulnerability 3.84

Test-specific ID: SNYK-DEBIAN12-LIBPNG16-2363910 **Severity:** low

Identifiers: **Message:**Buffer Overflow

Vulnerability 3.85

Test-specific ID: SNYK-DEBIAN12-LIBWMF-1551191 **Severity:** low

Identifiers: **Message:**Resource Management Errors

Vulnerability 3.86

Test-specific ID: SNYK-DEBIAN12-LIBWMF-1551196 **Severity:** low

Identifiers: **Message:**Numeric Errors

Vulnerability 3.87

Test-specific ID: SNYK-DEBIAN12-LIBWMF-1551197 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.88

Test-specific ID: SNYK-DEBIAN12-LIBWMF-1551447 **Severity:** low

Identifiers: **Message:**Numeric Errors

Vulnerability 3.89

Test-specific ID: SNYK-DEBIAN12-LIBXML2-5871333 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.90

Test-specific ID: SNYK-DEBIAN12-LIBXML2-5947663 **Severity:** low

Identifiers: **Message:**Use After Free

Vulnerability 3.91

Test-specific ID: SNYK-DEBIAN12-LIBXSLT-1551290 **Severity:** low

Identifiers: **Message:**Use of Insufficiently Random Values

Vulnerability 3.92

Test-specific ID: SNYK-DEBIAN12-M4-1553360 **Severity:** low

Identifiers: **Message:**CVE-2008-1688

Vulnerability 3.93

Test-specific ID: SNYK-DEBIAN12-M4-1553473 **Severity:** low

Identifiers: **Message:**CVE-2008-1687

Vulnerability 3.94

Test-specific ID: SNYK-DEBIAN12-MARIADB-6091687 **Severity:** low

Identifiers: **Message:**CVE-2023-22084

Vulnerability 3.95

Test-specific ID: SNYK-DEBIAN12-NCURSES-6123823 **Severity:** low

Identifiers: **Message:**CVE-2023-50495

Vulnerability 3.96

Test-specific ID: SNYK-DEBIAN12-OPENEXR-1555478 **Severity:** low

Identifiers: **Message:**Resource Exhaustion

Vulnerability 3.97

Test-specific ID: SNYK-DEBIAN12-OPENEXR-1555810 **Severity:** low

Identifiers: **Message:**Integer Underflow

Vulnerability 3.98

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555599 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.99

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555605 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.100

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555606 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.101

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555618 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.102

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555638 **Severity:** low

Identifiers: **Message:**Improper Input Validation

Vulnerability 3.103

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555659 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.104

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555684 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.105

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555859 **Severity:** low

Identifiers: **Message:**Divide By Zero

Vulnerability 3.106

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555862 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.107

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555866 **Severity:** low

Identifiers: **Message:**Integer Overflow or Wraparound

Vulnerability 3.108

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555892 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.109

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555911 **Severity:** low

Identifiers: **Message:**Allocation of Resources Without Limits or Throttling

Vulnerability 3.110

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1555936 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.111

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1556010 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.112

Test-specific ID: SNYK-DEBIAN12-OPENJPEG2-1556013 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.113

Test-specific ID: SNYK-DEBIAN12-OPENLDAP-1555631 **Severity:** low

Identifiers: **Message:**Improper Initialization

Vulnerability 3.114

Test-specific ID: SNYK-DEBIAN12-OPENLDAP-1555724 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.115

Test-specific ID: SNYK-DEBIAN12-OPENLDAP-1555918 **Severity:** low

Identifiers: **Message:**Improper Certificate Validation

Vulnerability 3.116

Test-specific ID: SNYK-DEBIAN12-OPENLDAP-1555941 **Severity:** low

Identifiers: **Message:**Cryptographic Issues

Vulnerability 3.117

Test-specific ID: SNYK-DEBIAN12-OPENLDAP-5660620 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.118

Test-specific ID: SNYK-DEBIAN12-OPENSSH-1555751 **Severity:** low

Identifiers: **Message:**Information Exposure

Vulnerability 3.119

Test-specific ID: SNYK-DEBIAN12-OPENSSH-1555766 **Severity:** low

Identifiers: **Message:**Access Restriction Bypass

Vulnerability 3.120

Test-specific ID: SNYK-DEBIAN12-OPENSSH-1556004 **Severity:** low

Identifiers: **Message:**Improper Authentication

Vulnerability 3.121

Test-specific ID: SNYK-DEBIAN12-OPENSSH-1556046 **Severity:** low

Identifiers: **Message:**Information Exposure

Vulnerability 3.122

Test-specific ID: SNYK-DEBIAN12-OPENSSH-1556049 **Severity:** low

Identifiers: **Message:**Information Exposure

Vulnerability 3.123

Test-specific ID: SNYK-DEBIAN12-OPENSSH-1556053 **Severity:** low

Identifiers: **Message:**Inappropriate Encoding for Output Context

Vulnerability 3.124

Test-specific ID: SNYK-DEBIAN12-OPENSSH-1556262 **Severity:** low

Identifiers: **Message:**OS Command Injection

Vulnerability 3.125

Test-specific ID: SNYK-DEBIAN12-OPENSSH-1585651 **Severity:** low

Identifiers: **Message:**CVE-2016-20012

Vulnerability 3.126

Test-specific ID: SNYK-DEBIAN12-OPENSSL-1555825 **Severity:** low

Identifiers: **Message:**Cryptographic Issues

Vulnerability 3.127

Test-specific ID: SNYK-DEBIAN12-OPENSSL-1555907 **Severity:** low

Identifiers: **Message:**Cryptographic Issues

Vulnerability 3.128

Test-specific ID: SNYK-DEBIAN12-OPENSSL-6048820 **Severity:** low

Identifiers: **Message:**Improper Check for Unusual or Exceptional Conditions

Vulnerability 3.129

Test-specific ID: SNYK-DEBIAN12-OPENSSL-6148845 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.130

Test-specific ID: SNYK-DEBIAN12-OPENSSL-6157243 **Severity:** low

Identifiers: **Message:**CVE-2023-6237

Vulnerability 3.131

Test-specific ID: SNYK-DEBIAN12-OPENSSL-6190223 **Severity:** low

Identifiers: **Message:**CVE-2024-0727

Vulnerability 3.132

Test-specific ID: SNYK-DEBIAN12-PAM-6178914 **Severity:** low

Identifiers: **Message:**CVE-2024-22365

Vulnerability 3.133

Test-specific ID: SNYK-DEBIAN12-PATCH-1556285 **Severity:** low

Identifiers: **Message:**Directory Traversal

Vulnerability 3.134

Test-specific ID: SNYK-DEBIAN12-PATCH-1556552 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.135

Test-specific ID: SNYK-DEBIAN12-PATCH-1556555 **Severity:** low

Identifiers: **Message:**Double Free

Vulnerability 3.136

Test-specific ID: SNYK-DEBIAN12-PATCH-2324793 **Severity:** low

Identifiers: **Message:**Release of Invalid Pointer or Reference

Vulnerability 3.137

Test-specific ID: SNYK-DEBIAN12-PERL-1556505 **Severity:** low

Identifiers: **Message:**Link Following

Vulnerability 3.138

Test-specific ID: SNYK-DEBIAN12-PERL-5489184 **Severity:** low

Identifiers: **Message:**Improper Certificate Validation

Vulnerability 3.139

Test-specific ID: SNYK-DEBIAN12-PERL-5489190 **Severity:** low

Identifiers: **Message:**Improper Certificate Validation

Vulnerability 3.140

Test-specific ID: SNYK-DEBIAN12-PIXMAN-5803155 **Severity:** low

Identifiers: **Message:**Divide By Zero

Vulnerability 3.141

Test-specific ID: SNYK-DEBIAN12-PROCPS-5816466 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.142

Test-specific ID: SNYK-DEBIAN12-PYTHON311-3325304 **Severity:** low

Identifiers: **Message:**Improper Input Validation

Vulnerability 3.143

Test-specific ID: SNYK-DEBIAN12-PYTHON311-5430932 **Severity:** low

Identifiers: **Message:**Improper Input Validation

Vulnerability 3.144

Test-specific ID: SNYK-DEBIAN12-PYTHON311-5754614 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.145

Test-specific ID: SNYK-DEBIAN12-PYTHON311-5853785 **Severity:** low

Identifiers: **Message:**Untrusted Search Path

Vulnerability 3.146

Test-specific ID: SNYK-DEBIAN12-PYTHON311-5861799 **Severity:** low

Identifiers: **Message:**CVE-2023-40217

Vulnerability 3.147

Test-specific ID: SNYK-DEBIAN12-SHADOW-1559391 **Severity:** low

Identifiers: **Message:**Access Restriction Bypass

Vulnerability 3.148

Test-specific ID: SNYK-DEBIAN12-SHADOW-1559403 **Severity:** low

Identifiers: **Message:**Incorrect Permission Assignment for Critical Resource

Vulnerability 3.149

Test-specific ID: SNYK-DEBIAN12-SHADOW-5423923 **Severity:** low

Identifiers: **Message:**Arbitrary Code Injection

Vulnerability 3.150

Test-specific ID: SNYK-DEBIAN12-SHADOW-5879156 **Severity:** low

Identifiers: **Message:**Improper Authentication

Vulnerability 3.151

Test-specific ID: SNYK-DEBIAN12-SQLITE3-2407042 **Severity:** low

Identifiers: **Message:**Memory Leak

Vulnerability 3.152

Test-specific ID: SNYK-DEBIAN12-SQLITE3-6139924 **Severity:** low

Identifiers: **Message:**Out-of-Bounds

Vulnerability 3.153

Test-specific ID: SNYK-DEBIAN12-SQLITE3-6155400 **Severity:** low

Identifiers: **Message:**Use After Free

Vulnerability 3.154

Test-specific ID: SNYK-DEBIAN12-SYSTEMD-1560739 **Severity:** low

Identifiers: **Message:**Link Following

Vulnerability 3.155

Test-specific ID: SNYK-DEBIAN12-SYSTEMD-5733385 **Severity:** low

Identifiers: **Message:**Improper Validation of Integrity Check Value

Vulnerability 3.156

Test-specific ID: SNYK-DEBIAN12-SYSTEMD-5733390 **Severity:** low

Identifiers: **Message:**Improper Validation of Integrity Check Value

Vulnerability 3.157

Test-specific ID: SNYK-DEBIAN12-SYSTEMD-5733398 **Severity:** low

Identifiers: **Message:**Improper Validation of Integrity Check Value

Vulnerability 3.158

Test-specific ID: SNYK-DEBIAN12-SYSTEMD-6137714 **Severity:** low

Identifiers: **Message:**CVE-2023-7008

Vulnerability 3.159

Test-specific ID: SNYK-DEBIAN12-TAR-1560620 **Severity:** low

Identifiers: **Message:**CVE-2005-2541

Vulnerability 3.160

Test-specific ID: SNYK-DEBIAN12-TAR-3253526 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.161

Test-specific ID: SNYK-DEBIAN12-TAR-6120422 **Severity:** low

Identifiers: **Message:**CVE-2023-39804

Vulnerability 3.162

Test-specific ID: SNYK-DEBIAN12-TCL86-1560164 **Severity:** low

Identifiers: **Message:**Use of Externally-Controlled Format String

Vulnerability 3.163

Test-specific ID: SNYK-DEBIAN12-TIFF-1560922 **Severity:** low

Identifiers: **Message:**Missing Release of Resource after Effective Lifetime

Vulnerability 3.164

Test-specific ID: SNYK-DEBIAN12-TIFF-1561093 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.165

Test-specific ID: SNYK-DEBIAN12-TIFF-1561130 **Severity:** low

Identifiers: **Message:**Use After Free

Vulnerability 3.166

Test-specific ID: SNYK-DEBIAN12-TIFF-1561402 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.167

Test-specific ID: SNYK-DEBIAN12-TIFF-1561632 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.168

Test-specific ID: SNYK-DEBIAN12-TIFF-2440572 **Severity:** low

Identifiers: **Message:**Improper Resource Shutdown or Release

Vulnerability 3.169

Test-specific ID: SNYK-DEBIAN12-TIFF-5416364 **Severity:** low

Identifiers: **Message:**Out-of-bounds Read

Vulnerability 3.170

Test-specific ID: SNYK-DEBIAN12-TIFF-5673710 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.171

Test-specific ID: SNYK-DEBIAN12-TIFF-5724640 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.172

Test-specific ID: SNYK-DEBIAN12-TIFF-5747599 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.173

Test-specific ID: SNYK-DEBIAN12-TIFF-5749338 **Severity:** low

Identifiers: **Message:**Buffer Overflow

Vulnerability 3.174

Test-specific ID: SNYK-DEBIAN12-TIFF-5750144 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.175

Test-specific ID: SNYK-DEBIAN12-TIFF-5767899 **Severity:** low

Identifiers: **Message:**Buffer Overflow

Vulnerability 3.176

Test-specific ID: SNYK-DEBIAN12-TIFF-5773187 **Severity:** low

Identifiers: **Message:**Buffer Overflow

Vulnerability 3.177

Test-specific ID: SNYK-DEBIAN12-TIFF-6079922 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.178

Test-specific ID: SNYK-DEBIAN12-TIFF-6084514 **Severity:** low

Identifiers: **Message:**Resource Exhaustion

Vulnerability 3.179

Test-specific ID: SNYK-DEBIAN12-TIFF-6190608 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.180

Test-specific ID: SNYK-DEBIAN12-TIFF-6190785 **Severity:** low

Identifiers: **Message:**Out-of-bounds Write

Vulnerability 3.181

Test-specific ID: SNYK-DEBIAN12-UNZIP-2387294 **Severity:** low

Identifiers: **Message:**NULL Pointer Dereference

Vulnerability 3.182

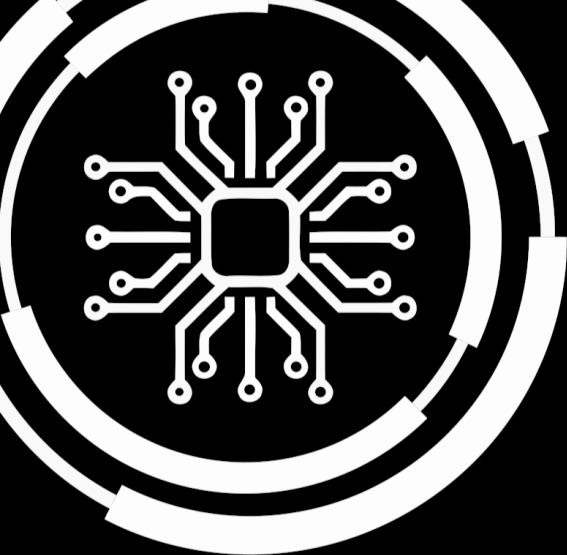
Test-specific ID: SNYK-DEBIAN12-UTILLINUX-2401083 **Severity:** low

Identifiers: **Message:**Information Exposure

Vulnerability 3.183

Test-specific ID: SNYK-DEBIAN12-WGET-1562497 **Severity:** low

Identifiers: **Message:**Open Redirect



4. Dynamic Train Analysis

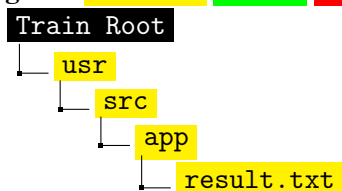
4.1 Image size differences after simulation:

4.1.1 Simulated route:

- Station d7b0a9a7-07fd-4a31-b93a-3c946dc82667: 2
- Station 5bce186a-5005-4ca8-878e-9d8d4e0747c0: 4

4.1.2 Directory Overview of changed files:

Legend: Modified Added Deleted



4.1.3 `./simulationResults/result.txt`

Listing 4.1: result.txt

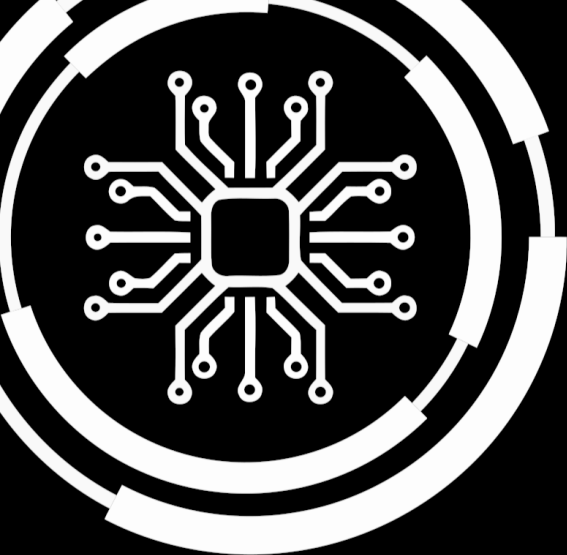
4
5

4.2 Execution metrics:

- Maximum CPU Usage:0
- Maximum Memory Usage:0
- Maximum Number of PIDS:0

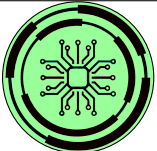

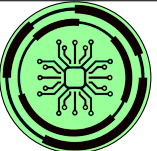
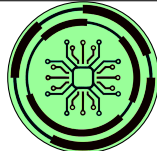
4.3 Network I/O:

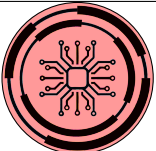
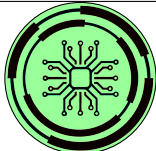
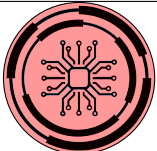
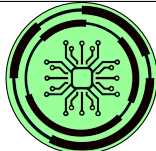
- RX (Reading):0
- TX (Transmitting):0



5. Conclusion

The PADME Security Audit has come to the following conclusion:

Static Complete	SAST	Dependencies	Secret Detection
			

Standard Compliant	Blacklist	Train Image Analysis	DAST
			

Warnings

- Found 1 critical vulnerability in the image.
- Couldn't detect compliance with standards (usage of the python module `padme_conductor` [<https://pypi.org/project/padme-conductor/>]).

Audit Result

Train Approved

February 2, 2024

