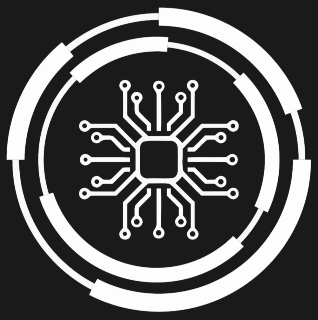
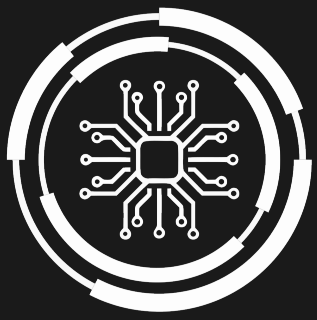


Manual & Security Audit for Train

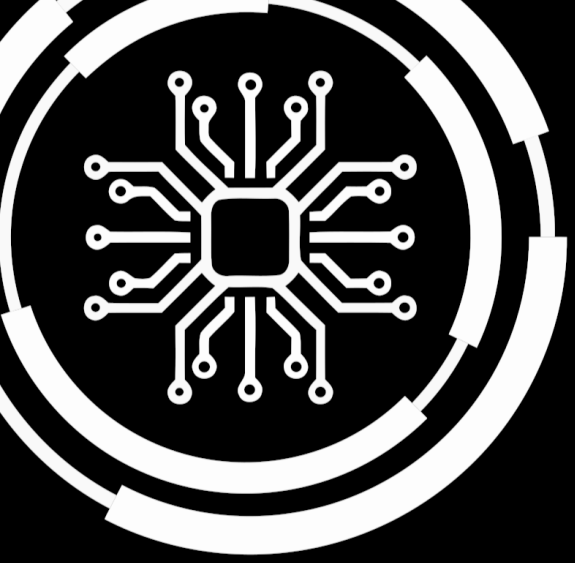
PickleDetection

Sascha Martin Welten



PADME-ANALYTICS.DE

First printing, February 1, 2024



Contents

1. Train Summary

1.1 Overview

- **Train name:** PickleDetection
- **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=PickleDetection`

1.2 Image Building File

Listing 1.1: Image building file

```
FROM python:3.11.7-slim


WORKDIR /usr/src/app

# LABEL
LABEL "envs"="[{\"name\": \"DB_NAME\",\"type\": \"text\",\"
   required\": true},{\"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}]"

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

```
import pickle

with open("data.pickle", "rb") as f:
    data = pickle.load(f)
```

Listing 1.2: main.py

```
Error:  Cannot visualize code file:data.pickle
```

1.5 Connection Parameters

Overall, 6 connection parameters have been found in the train:

Name	Type	Required?
DB_NAME	text	True
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:** 223783
- **Vulnerabilities per Line:** 8e-06
- **Analysis Score:** 1.0

Total

Summary: Low: 0 Medium: 1 High: 1

2.1 SAST

Summary: Low: 0 Medium: 1 High: 1

Detailed Vulnerabilities:

Vulnerability 2.1

Test-specific ID: 9e15de46d165d9a55a6f89ccc7db81168ba16792a28d93253c645eb8cd16f784
Severity: Info
Identifiers:

- **semgrep_id:** bandit.B403
- **cwe:** 502
- **owasp:** A8
- **bandit_test_id:** B403

Message:Deserialization of Untrusted Data
File:PickleDetection/main.py **Start line**: 1

Vulnerability 2.2

Test-specific ID: 8be33333009f919201729e79b05edecef42a74e6b21f57cdbddfca3f05fa0bf9
Severity: Medium
Identifiers:

- **semgrep_id:** bandit.B301-1
- **cwe:** 502
- **owasp:** A8
- **bandit_test_id:** B301-1

Message:Deserialization of Untrusted Data
File:PickleDetection/main.py **Start line**: 4

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: 45 Medium: 0 High: 0 Critical: 1

Detailed Vulnerabilities:

Critical:

Vulnerability 3.1

Test-specific ID: SNYK-DEBIAN12-ZLIB-6008963 **Severity:** critical
Identifiers: **Message**:Integer Overflow or Wraparound

High:

Medium:

Low:

Vulnerability 3.2

Test-specific ID: SNYK-DEBIAN12-APT-1541449 **Severity:** low
Identifiers: **Message**:Improper Verification of Cryptographic Signature

Vulnerability 3.3

Test-specific ID: SNYK-DEBIAN12-COREUTILS-1543939 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.4

Test-specific ID: SNYK-DEBIAN12-COREUTILS-1543947 **Severity:** low
Identifiers: **Message**:Race Condition

Vulnerability 3.5

Test-specific ID: SNYK-DEBIAN12-GCC12-2606941 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.6

Test-specific ID: SNYK-DEBIAN12-GCC12-5901316 **Severity:** low
Identifiers: **Message**:CVE-2023-4039

Vulnerability 3.7

Test-specific ID: SNYK-DEBIAN12-GLIBC-1546991 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.8

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547039 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.9

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547069 **Severity:** low
Identifiers: **Message**:Uncontrolled Recursion

Vulnerability 3.10

Test-specific ID: SNYK-DEBIAN12-GLIBC-1547135 **Severity:** low
Identifiers: **Message**:Use of Insufficiently Random Values

Vulnerability 3.11
Test-specific ID: SNYK-DEBIAN12-GLIBC-1547196 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.12
Test-specific ID: SNYK-DEBIAN12-GLIBC-1547293 **Severity:** low
Identifiers: **Message**:Resource Management Errors

Vulnerability 3.13
Test-specific ID: SNYK-DEBIAN12-GLIBC-1547373 **Severity:** low
Identifiers: **Message**:CVE-2019-1010023

Vulnerability 3.14
Test-specific ID: SNYK-DEBIAN12-GNUPG2-3330747 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.15
Test-specific ID: SNYK-DEBIAN12-GNUTLS28-1547121 **Severity:** low
Identifiers: **Message**:Improper Input Validation

Vulnerability 3.16
Test-specific ID: SNYK-DEBIAN12-GNUTLS28-6159410 **Severity:** low
Identifiers: **Message**:Improper Verification of Cryptographic Signature

Vulnerability 3.17
Test-specific ID: SNYK-DEBIAN12-GNUTLS28-6159418 **Severity:** low
Identifiers: **Message**:Information Exposure

Vulnerability 3.18
Test-specific ID: SNYK-DEBIAN12-KRB5-1549480 **Severity:** low
Identifiers: **Message**:Integer Overflow or Wraparound

Vulnerability 3.19
Test-specific ID: SNYK-DEBIAN12-LIBGCRYPT20-1550206 **Severity:** low
Identifiers: **Message**:Use of a Broken or Risky Cryptographic Algorithm

Vulnerability 3.20
Test-specific ID: SNYK-DEBIAN12-NCURSES-6123823 **Severity:** low
Identifiers: **Message**:CVE-2023-50495

Vulnerability 3.21
Test-specific ID: SNYK-DEBIAN12-OPENSSL-1555825 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.22
Test-specific ID: SNYK-DEBIAN12-OPENSSL-1555907 **Severity:** low
Identifiers: **Message**:Cryptographic Issues

Vulnerability 3.23
Test-specific ID: SNYK-DEBIAN12-OPENSSL-6048820 **Severity:** low
Identifiers: **Message**:Improper Check for Unusual or Exceptional Conditions

Vulnerability 3.24
Test-specific ID: SNYK-DEBIAN12-OPENSSL-6148845 **Severity:** low
Identifiers: **Message**:Out-of-bounds Write

Vulnerability 3.25
Test-specific ID: SNYK-DEBIAN12-OPENSSL-6157243 **Severity:** low
Identifiers: **Message**:CVE-2023-6237

Vulnerability 3.26
Test-specific ID: SNYK-DEBIAN12-OPENSSL-6190223 **Severity:** low
Identifiers: **Message**:CVE-2024-0727

Vulnerability 3.27
Test-specific ID: SNYK-DEBIAN12-PAM-6178914 **Severity:** low
Identifiers: **Message**:CVE-2024-22365

Vulnerability 3.28
Test-specific ID: SNYK-DEBIAN12-PERL-1556505 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.29
Test-specific ID: SNYK-DEBIAN12-PERL-5489184 **Severity:** low
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.30
Test-specific ID: SNYK-DEBIAN12-PERL-5489190 **Severity:** low
Identifiers: **Message**:Improper Certificate Validation

Vulnerability 3.31
Test-specific ID: SNYK-DEBIAN12-SHADOW-1559391 **Severity:** low
Identifiers: **Message**:Access Restriction Bypass

Vulnerability 3.32
Test-specific ID: SNYK-DEBIAN12-SHADOW-1559403 **Severity:** low
Identifiers: **Message**:Incorrect Permission Assignment for Critical Resource

Vulnerability 3.33
Test-specific ID: SNYK-DEBIAN12-SHADOW-5423923 **Severity:** low
Identifiers: **Message**:Arbitrary Code Injection

Vulnerability 3.34
Test-specific ID: SNYK-DEBIAN12-SHADOW-5879156 **Severity:** low
Identifiers: **Message**:Improper Authentication

Vulnerability 3.35
Test-specific ID: SNYK-DEBIAN12-SQLITE3-2407042 **Severity:** low
Identifiers: **Message**:Memory Leak

Vulnerability 3.36
Test-specific ID: SNYK-DEBIAN12-SQLITE3-6139924 **Severity:** low
Identifiers: **Message**:Out-of-Bounds

Vulnerability 3.37
Test-specific ID: SNYK-DEBIAN12-SQLITE3-6155400 **Severity:** low
Identifiers: **Message**:Use After Free

Vulnerability 3.38
Test-specific ID: SNYK-DEBIAN12-SYSTEMD-1560739 **Severity:** low
Identifiers: **Message**:Link Following

Vulnerability 3.39
Test-specific ID: SNYK-DEBIAN12-SYSTEMD-5733385 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.40
Test-specific ID: SNYK-DEBIAN12-SYSTEMD-5733390 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.41
Test-specific ID: SNYK-DEBIAN12-SYSTEMD-5733398 **Severity:** low
Identifiers: **Message**:Improper Validation of Integrity Check Value

Vulnerability 3.42
Test-specific ID: SNYK-DEBIAN12-SYSTEMD-6137714 **Severity:** low
Identifiers: **Message**:CVE-2023-7008

Vulnerability 3.43
Test-specific ID: SNYK-DEBIAN12-TAR-1560620 **Severity:** low
Identifiers: **Message**:CVE-2005-2541

Vulnerability 3.44
Test-specific ID: SNYK-DEBIAN12-TAR-3253526 **Severity:** low
Identifiers: **Message**:Out-of-bounds Read

Vulnerability 3.45
Test-specific ID: SNYK-DEBIAN12-TAR-6120422 **Severity:** low
Identifiers: **Message**:CVE-2023-39804

Vulnerability 3.46

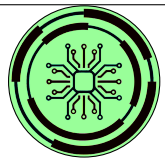
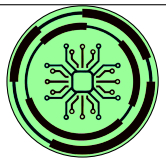
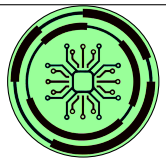
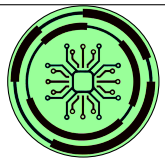
Test-specific ID: SNYK-DEBIAN12-UTILLINUX-2401083 **Severity:** low
Identifiers: **Message**:Information Exposure

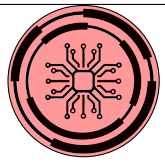
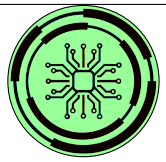
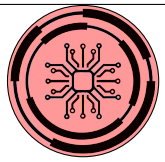
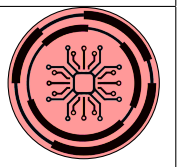
4. Dynamic Train Analysis

No Dynamic Report Available

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]).
- The reports dynamic_report.json are missing. Acceptance threshold increased from 0.5 to 0.75.

Audit Result

Train Rejected

February 1, 2024