Dante HackTheBox

PEN-DOC-202212121341

Pentest company, https://github.com/1modm/petereport

12-12-2022

QU35T Reports

Contents

QU35T Reports

1 Project Overview

1.1 Description

My personal reports

QU35T Reports

2 Executive Summary

This is the Dante lab.

2.1 Summary of Findings Identified

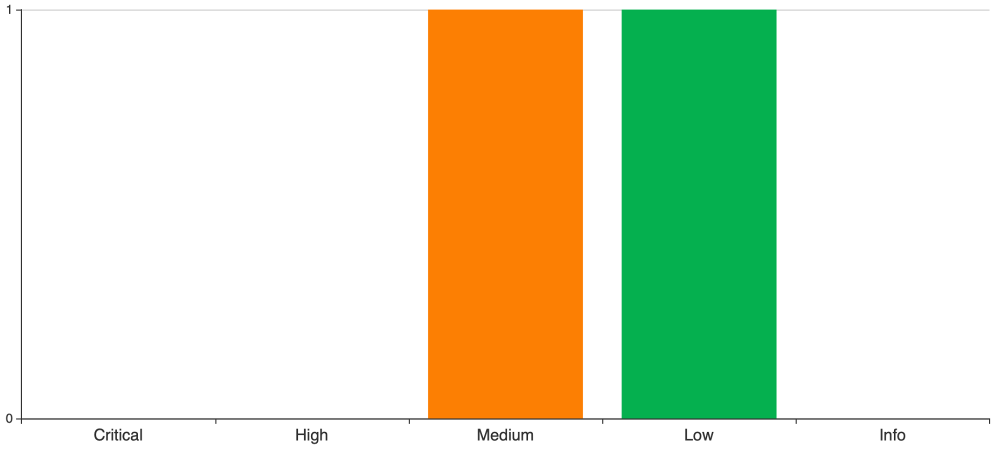

Figure 1: Executive Summary

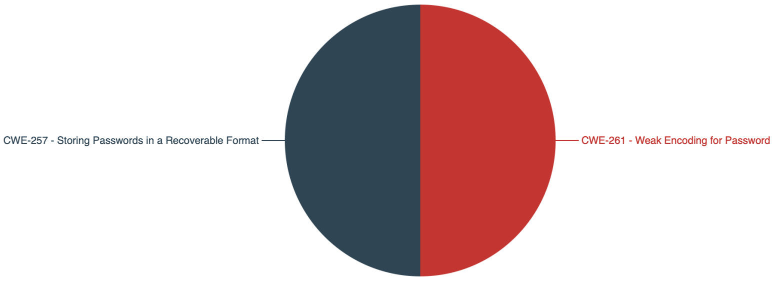

Figure 2: Breakdown by Categories

# 1 Medium Weak Credentials

# 2 Low Hardcoded passwords

QU35T Reports

2.2 Scope

2.2.1 In Scope

The scope is :

- 10.10.10.0/24

2.2.2 Out of Scope

Out Of scope :

- 10.10.10.2

QU35T Reports

2.3 Methodology

The methodologie

QU35T Reports

2.4 Recommendations

The recommandation general

QU35T Reports

3 Findings and Risk Analysis

3.1 Weak Credentials

Severity: Medium
CVSS Score: 6.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:H)

CWE

261 - Weak Encoding for Password

Description

This password is weak : "jdjskdjk"

Location

Admin Panel

Impact

Account takeover omg

Recommendation

Change password

References

portswigger.com/passwords

QU35T Reports

3.2 Hardcoded passwords

⚠ **Severity:** Low
CVSS Score: 3.5 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:N)

CWE

257 - Storing Passwords in a Recoverable Format

Description

Omg

Location

Leak

Impact

Boum

Recommendation

reco

References

Ref

QU35T Reports

4 Additional Notes

QU35T Reports