# SECURITY AUDIT REPORT

## 1. APPLICATION OVERVIEW

**App Name:** vuln_demo_app_secure
**Package:** com.example.vuln_demo_app
**Size:** 41.31MB
**Target SDK:** 36
**Scan Date:** 2/22/2026

## 2. EXECUTIVE SUMMARY

## SECURITY SCORE: 0/100

**Risk Category: High Risk**
Analysis: App is critically vulnerable. Do not deploy.

## 3. VULNERABILITY METRICS

• Embedded Trackers Detected:

• Signature Analysis: Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Androi...

### A. HIGH SEVERITY ISSUES

**1. App can be installed on a vulnerable unpatched Android version 7.0, [minSdk=24]**
This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable sec...

**2. Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]**
A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is...

### B. CRITICAL PERMISSIONS GRANTED

No notoriously dangerous permissions were requested by this application.

### C. SOURCE CODE VULNERABILITIES

No critical source code vulnerabilities or injection flaws detected.

### D. HARDCODED SECRETS & TOKENS

WARNING: 4 potential hardcoded secrets/API keys were discovered in the source code.
*1. Pattern Match: VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIE...*

*2. Pattern Match: VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy...*
*3. Pattern Match: VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYW...*

## 4. PRE-PRODUCTION SECURITY CHECKLIST

**[ PASS ]** Debug/Test Flags Disabled?

**[ PASS ]** Cleartext (HTTP) Traffic Disabled?

**[ FAIL ]** App signed with Valid Production Certificate?

**[ FAIL ]** No Critical Hardcoded Secrets?

**[ PASS ]** High Severity Code Issues Remediated?