MOBSF

ANDROID STATIC ANALYSIS REPORT

BloodPressure (0.1.19)

File Name:	com.bluefish.bloodpressure_19.apk
Package Name:	com.bluefish.bloodpressure
Scan Date:	Aug. 29, 2025, 8:21 p.m.
App Security Score:	43/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	1	0	0

FILE INFORMATION

File Name: com.bluefish.bloodpressure_19.apk
Size: 8.24MB
MD5: 859a5a9db6f0d50f81377703081745b6
SHA1: 1fbcc0a255b01fd64c8a9bb2fdb99ebff6d3e1a4
SHA256: df40c785710a6050d1518a3a75139f0fc59f76a053b878df5f0c29eb38abc23b

APP INFORMATION

App Name: BloodPressure
Package Name: com.bluefish.bloodpressure
Main Activity: com.bluefish.bloodpressure.MainActivity
Target SDK: 33
Min SDK: 21
Max SDK:
Android Version Name: 0.1.19

Android Version Code: 19

APP COMPONENTS

Activities: 5
Services: 5
Receivers: 8
Providers: 3
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, CN=Bluefish
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-08-17 06:53:47+00:00
Valid To: 2043-08-11 06:53:47+00:00
Issuer: C=US, CN=Bluefish
Serial Number: 0x6552057c
Hash Algorithm: sha256
md5: 068f3bff417a9367501230d643fca195
sha1: 49e423f56684b9d850b30c5aa842fdee8a858268
sha256: 9639710fdc6e287835a16d6a0cca0c2a01d72c4c5db92d091a2e124f0c973a78
sha512: e75218be4fd1062f88d8117768b9b19d94e4a789e9e4fa25c093bd0a76d22319155059f82e2f16ac362ef018d17d6c23448f93baaadb64392552dc97c55fcf0c
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: fbb964361151b5c325399a86c6fff32d44175ff504af461743655fff724b1a93
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.bluefish.bloodpressure.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.DEVICE check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	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 protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bluefish/bloodpressure/BottomNavigationViewHelper.java com/bluefish/bloodpressure/DBTuple.java com/bluefish/bloodpressure/Utility.java com/bluefish/bloodpressure/calendar/CalendarProvider.java com/db/chart/view/ChartView.java
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/bluefish/bloodpressure/DBHelper.java com/bluefish/bloodpressure/DBUtil.java com/bluefish/bloodpressure/calendar/CalendarProvider.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/bluefish/bloodpressure/FragmentSetting.java com/bluefish/bloodpressure/Utility.java com/bluefish/bloodpressure/alertdialog/rateAlertDialog.java com/bluefish/bloodpressure/alertdialog/rateAlertDialog2.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/bluefish/bloodpressure/FragmentSetting.java
00036	Get resource file from res/raw directory	reflection	com/bluefish/bloodpressure/FragmentSetting.java com/bluefish/bloodpressure/Utility.java com/bluefish/bloodpressure/alertdialog/rateAlertDialog.java com/bluefish/bloodpressure/alertdialog/rateAlertDialog2.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.VIBRATE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	2/44	com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.68.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
bluefish12390@gmail.com	com/bluefish/bloodpressure/alertdialog/helpAlertDialog.java
bluefish12390@gmail.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
9mv9Ihk+HlE8P3WJWSjhrxWrdB7cEu1gaxdteA5kBJ6DKumpWYk1Q5Vf8aocVg4i
gL88T2vBvJS+jBemUvhPpVS5IeaU7cU4wFVgyT6PJl7pFldWXOd3mZxVZlQUSll5

POSSIBLE SECRETS
Jz2tk/JKeGJKcc4wwXH5Pf6ZM64fYgV4wWxByPOgNQE=
s1ejGoWFNJedDDJqGqL3B22F5ZMvy0oaymBcWJepS9Hv4/6KtsHBpmbtFfwgqqen
I5l5b06e/m6OPcJVryww5aceHDWuWNMRDm4mYVrBvJQ=
NOrE2caDXO4nkFR2Fjy7NgGPKtPlIg1WAorknI/US68=
Q+fOnDUQnIPH75lusFutOgWOI4DeJ6z7X13oo1pZ5m19Kfyi56UOJglWSBqO3AzA
aC7c3pDenGsdb0eFildzKOBrhobw8fKkmd52rTlBEKM=
sK9i540XcONymgaiZVMKYXr1VbNcwMhjwo2LFhhSCFg=
1ZhioNexfONxLbr8oNixHPTbX/qv3RsJiyYoeeb0m+g=
8UC+BMIoCN+KAKrN9TZmuJsGMmo3RUHS+FjVMSp9QfgjxjGZ10kqO/oSdOn5Rw29
A3EfeXObjqx38Tdc4wdTZSQNpfpw6YVck+944M4A/m0=
qUEdP6yfmpdCkPVqoE8EyrX/MPjGh4YKRo5g3kOeMoc=
7qOZVP58PfP3kLkbSBo98onihlohkIEpZC40FvE5nnCJ8ryn0NERK9JAnlww55zq
tfuuP59pzWN+H8zv1geT3jADiBKBGMQRjmCPoIvL5f45Lvl5qgJ0PgBqZF4WPnQj
ae2044fb577e65ee8bb576ca48a2f06e
1OxyLDHu2cwu0U7XKtDO3q+DghLeQ8xcTgpGCDWDuEeCcfs+HPxSt8kldIfiq1K0

POSSIBLE SECRETS
Ee4p/yPQz67p3LoSNbpt1G8K9rDuoWxBYT8E4CbWyr8=
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233333133333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
bObXLZFRWAdU6+me08AeNX2ciqxi45ddv3QSqAplzos=
RSyr2AK130nKbepDTsaNV0Uv17TWUb4O6ebIiV3GgVs=
MIrDuKB7N0O22daoYjLtFOJg5TtVRHK1+0ktwmGNtdU=
SMfJnKfhfLLyTw7dzHC+3CXVRNFLWK4N2mQHKB3gm/o=
nIX5dAPvXYWFIvHlyxyLt0TnZ91UnAjFxZwf2qcoWSGcs+p5B5p88VCOzepPfMpE
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
gzR6fJL0MpYPfJ/UkFL9UHjS7jlytQ+eyVRsQJTsxzK4yqDaskM4UtldyBDUp+Z9

POSSIBLE SECRETS
B3EEABB8EE11C2BE770B684D95219ECB
zahwJ4oRFMB+Gn9BGkfZDZ8TzDEfKTB8Y6I4bT4vlwkVFXvqlnkWd7htbiUzWQyR
s7rU1m4XsqJ83s2reIjdkboWJYkg+gYouDrDcn3Ghpw=
1eWk7vHD3Ee+FybzKEoWLH07Pvdxo5flYR768ntLvpJZNSFjE7xgNzi+al9tiZC4
Y0trGqGVEUAa7A3LYgSQFKe4N9h1BuTC7OKFYCHfLSg=
xLOAO7msIR4UFUyldUn5stL2wwbLdISu2CSlTLg4f6Q=
e694eb0f451250a160502658293f575d5b1df0579ba735ad0f54ee9a7cac42a1
3PwoDnm3HnsskB+3ZnJHoZ7BzV0InxUqaAwJBlSwKFs=
ttuIHg/yfWDxJlotLoMLf9WBnVTbWFFKY03C8KHR8FAhIQHccw4LaDLJatYkpo23
BkxOKZDOMH8NUFJEmpCq1X+PtIP0kLI1Ua0ujwsrkUE=
ZVHCdOeJUA1S4bCrFb9VMsUCP8Sf65wDnbBE+q4M36k=
5181942b9ebc31ce68dacb56c16fd79f
XCj6cS5OVeEeObzd394PGDbjTuQh+vSye2UT6221ugsKtO2/oznWOSes2cnebrVR
MbAcGuLi+XGl3MsgqAiQYLikemL120ZFxn+dIhaD+rHWJuTeO/M8+1c58cczHjCs
ZHFOx+FjaOsul7gEkIcfA8auDnyRWXmT0qbiHVEO6U1RLulNSOFK3tPEgm+pvQxr

POSSIBLE SECRETS
Eg2eC3eNesWzbAUINzxj1mXRcYgmzS654CxZFoVQbAM=
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b13 07416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613 616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930 3130323333363536 5a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406 03550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060 355040b1307416e64726f69643110300e06035504031307416e64726f6964312 2302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a 864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa 0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0 b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869 d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185 eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e6 20c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef32 98cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c6 1863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03 f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f 726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b13 07416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613 616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff 300d06092a864886f70d01010405000382010010019d30cf105fb78923f4c0d7dd223233d40967acfce0008 1d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc 95a5e3a010036f49248d5109bbf2e1e6181 86673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f 1939759733afd8aa160f4296c2d0163e8182859c6643e9c196 2fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fb a484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb 21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
w5tjCRfZfXWJzckDvIkXwf5aGJEVejLzfxhnwyqJH5E=
zmLnsak1Fo/LHy30EeWswBCxcOoFKuH08l3DkSTUgzb476o6nI+C8ZUC+d8tLJwZ
y+BEEb1lYOUGwTehZ9VIg/2gibmtEOjDZzKXHhs5BV0=
beFEMZ/YBSUug4MSXb2BKymKiM6ZxOOlxExWa37jMlM=
fxU2A2MjpZ4aJWGzXeMNURilSCaKosw3oXImrqnhSVmXB+tMi32JakdNlHCV3t0c
KHu8Xbxzr2mu9S25CNgKE5zXBf18Zj2waiAPYoFRjyhOXCyg+mYLv2x/JjCH7GjX

POSSIBLE SECRETS
hMVcCX1S6+m7rVEDNdCHhVgXRFILMOQ9RgLSmTdPHeNgAU8CbmBsymKBuqLQcQaU
iibTgWRTbrwM2W7HZGJP5cjM0DLiCyA9TVVy1genRaa4nvgE3+CiRN/Fx87DVDsO
r6m9xWOlfK6iHuNH3QiJQf71aQCKDM6NhABQId+yaKg=

PLAYSTORE INFORMATION

Title: Blood Pressure Diary

Score: 4.7214575 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.bluefish.bloodpressure

Developer Details: Health & Fitness AI Lab, Health+%26+Fitness+AI+Lab, None, https://smartailab.blogspot.com/, bluefish12390@gmail.com,

Release Date: Nov 29, 2018 **Privacy Policy:** Privacy link

Description:

Note that this app DOES NOT measure the blood pressure. Please use FDA-approved blood pressure monitor (i.e., BP monitor) to measure BP reliably Control high blood pressure (i.e., Hypertension) with our app! Simple and Easy to use blood pressure app 1. You can easily log and track systolic, diastolic and pulse by just swiping your finger 2. You can easily add your tags (e.g., irregular heartbeat, cuff location like left/right arms, seated/reclined) 3. You can easily search your data (e.g., by date, tags, and bloodpressure zones) Fully integrate with blood pressure zones 1. Automatically calculate bloodpressure zone 2. Support all blood pressure zones (i.e., Stage 1 and 2 Hypertension, Prehypertension, Normal, Hypotension) 3. Helpful to monitor and control your blood pressure and health 4. Easy-to-use for BP monitoring and tracking app It’s ALL FREE 1. No restrictive feature (e.g., unlimited csv export) Beautiful material UIs 1. Statistics with graphs and charts (e.g., average, minimum, maximum) 2. Interactive UI for blood pressure zones 3. Simple, but very effective UI Support auto backup (> Android 6.0) and free csv export 1. Send your bloodpressure data to your physician or doctor 2. Also record heartrate and heartbeat * Blood pressure (BP) monitoring/tracking and heart rate are very important for health. You can start managing your bloodpressure and heartrate now by using our blood pressure app, especially high bloodpressure or low blood pressure patients. * According to American Heart Association (AHA), normal range of blood pressure are Systolic 91 ~ 120 mmHg and Diastolic 61 ~ 80 mmHg. Please enjoy our blood pressure (BP) log and tracker app. * We'd appreciate your valuable feedback. Please, report bugs or request features to bluefish12390@gmail.com.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:21:31	Generating Hashes	OK
2025-08-29 20:21:31	Extracting APK	OK
2025-08-29 20:21:31	Unzipping	OK
2025-08-29 20:21:31	Parsing APK with androguard	OK
2025-08-29 20:21:31	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:21:31	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:21:34	Parsing AndroidManifest.xml	OK
2025-08-29 20:21:34	Extracting Manifest Data	OK
2025-08-29 20:21:34	Manifest Analysis Started	OK
2025-08-29 20:21:34	Performing Static Analysis on: BloodPressure (com.bluefish.bloodpressure)	OK

2025-08-29 20:21:34	Fetching Details from Play Store: com.bluefish.bloodpressure	OK
2025-08-29 20:21:35	Checking for Malware Permissions	OK
2025-08-29 20:21:35	Fetching icon path	OK
2025-08-29 20:21:35	Library Binary Analysis Started	OK
2025-08-29 20:21:35	Reading Code Signing Certificate	OK
2025-08-29 20:21:36	Running APKiD 2.1.5	OK
2025-08-29 20:21:39	Detecting Trackers	OK
2025-08-29 20:21:41	Decompiling APK to Java with JADX	OK
2025-08-29 20:21:57	Converting DEX to Smali	OK
2025-08-29 20:21:57	Code Analysis Started on - java_source	OK
2025-08-29 20:21:58	Android SBOM Analysis Completed	OK

2025-08-29 20:22:06	Android SAST Completed	OK
2025-08-29 20:22:06	Android API Analysis Started	OK
2025-08-29 20:22:13	Android API Analysis Completed	OK
2025-08-29 20:22:13	Android Permission Mapping Started	OK
2025-08-29 20:22:20	Android Permission Mapping Completed	OK
2025-08-29 20:22:20	Android Behaviour Analysis Started	OK
2025-08-29 20:22:27	Android Behaviour Analysis Completed	OK
2025-08-29 20:22:27	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:22:28	Email and URL Extraction Completed	OK
2025-08-29 20:22:28	Extracting String data from APK	OK
2025-08-29 20:22:28	Extracting String data from Code	OK

2025-08-29 20:22:28	Extracting String values and entropies from Code	OK
2025-08-29 20:22:30	Performing Malware check on extracted domains	OK
2025-08-29 20:22:34	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.