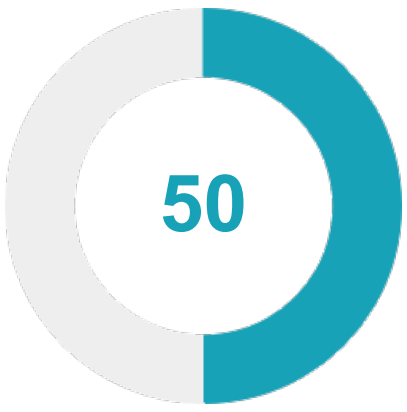
Security Score



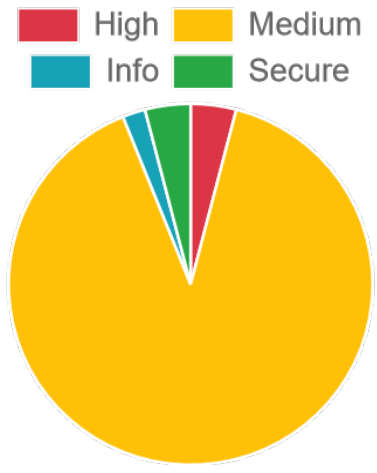
Security Score 50/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

3

User/Device Trackers

Findings

High	Medium	Info
2	43	1

Secure	Hotspot
2	2

high The file or SharedPreference is World Readable. Any App can read from the file	CODE
high Remote WebView debugging is enabled.	CODE
medium App can be installed on a vulnerable Android version	MANIFEST
medium Application Data can be Backed up	MANIFEST
medium Activity (com.pt.bark.phone.PhoneSetupActivity) is not Protected.	MANIFEST
medium TaskAffinity is set for activity	MANIFEST
medium TaskAffinity is set for activity	MANIFEST
medium Activity (com.pt.bark.uninstall.UninstallActivity) is not Protected.	MANIFEST
medium Broadcast Receiver (com.pt.bark.receivers.ExplicitMediaMonitoringReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.pt.bark.receivers.AppUpdateReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.pt.bark.receivers.RebootReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.pt.bark.receivers.WakeUpReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.pt.bark.phone.BootstrapReceiver) is not Protected.	MANIFEST
medium Broadcast Receiver (com.pt.bark.receivers.DetectNetwork) is not Protected.	MANIFEST

medium	Service (com.pt.bark.services.ObserversStartService) is not Protected.	MANIFEST
medium	Service (com.pt.bark.services.accessibility.BarkAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.pt.bark.services.BarkJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.pt.bark.observer.browser.v2.ChromeObserverV2) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.pt.bark.observer.browser.v2.DefaultBrowserObserverV2) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.pt.bark.observer.browser.v2.SamsungBrowserObserverV2) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.pt.bark.observer.message.v2.SmsObserverV2) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.pt.bark.vpn.BarkVpnService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) is not Protected.	MANIFEST
medium	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) is not Protected.	MANIFEST
medium	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	High Intent Priority (999)	MANIFEST
medium	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	CODE
medium	MD5 is a weak hash known to have hash collisions.	CODE

medium 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.	CODE
medium The App uses an insecure Random Number Generator.	CODE
medium IP Address disclosure	CODE
medium App creates temp file. Sensitive information should never be written into a temp file.	CODE
medium SHA-1 is a weak hash known to have hash collisions.	CODE
medium App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium This App may request root (Super User) privileges.	CODE
medium Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	CODE

medium Application contains Privacy Trackers	TRACKERS
medium This app may contain hardcoded secrets	SECRETS
info The App logs information. Sensitive information should never be logged.	CODE
secure This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
secure This App may have root detection capabilities.	CODE
hotspot Found 14 critical permission(s)	PERMISSIONS
hotspot Found 1 certificate/key file(s)	FILES

MobSF Application Security Scorecard generated for No icon (Bark 6.28.0)