Security Score

49

Security Score 49/100

Risk Rating

Medium Risk

Grade

A **B** C F

Severity Distribution (%)

High Medium
Info Secure

Privacy Risk

2

User/Device Trackers

📄 Findings

🐛 High **4**	⚠️ Medium **65**	ℹ️ Info **2**	✔️ Secure **2**	🔍 Hotspot **1**

`high` App can be installed on a vulnerable upatched Android version   **MANIFEST**

`high` Clear text traffic is Enabled For App   **MANIFEST**

`high` Weak Encryption algorithm used   **CODE**

`high` The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.   **CODE**

`medium` Application vulnerable to Janus Vulnerability   **CERTIFICATE**

`medium` Service (com.app.parentalcontrol.Activity.floating_wizard_view.FloatingBall_Wizard) is not Protected.   **MANIFEST**

`medium` Service (com.app.parentalcontrol.Activity.floating_wizard_view.FloatingActivity_Service) is not Protected.   **MANIFEST**

`medium` Service (com.app.parentalcontrol.logging.ShowFloatWdnService) is not Protected.   **MANIFEST**

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.Get10ClpInfoReceiver) is not Protected.   **MANIFEST**

`medium` Broadcast Receiver (.MyDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked.   **MANIFEST**

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.FloatActivity) is not standard.   **MANIFEST**

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.SplashScreen) is not standard.   **MANIFEST**

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.Home) is not standard.   **MANIFEST**

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.Logging) is not standard.   **MANIFEST**

MANIFEST

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.ImagePagerActivity) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.KeyloggingOption) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.timelimit.WarningBlockedActivity) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.AppSecurityActivity) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.ChangePin) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.LanguageActivity) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.ChangePassword) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.LoginPage) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.TrialPage) is not standard.

`medium` Activity (com.app.parentalcontrol.Activity.TrialPage) is not Protected.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.ResetPasswordActivity) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.ImageGridActivity) is not standard.

`medium` Activity (com.android.inputmethod.latin.settings.SettingsActivity) is not Protected.

`medium` Activity (com.android.inputmethod.latin.spellcheck.SpellCheckerSettingsActivity) is not Protected.

`medium` Activity (com.android.inputmethod.dictionarypack.DictionarySettingsActivity) is not Protected.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.SettingsActivityNew) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.root.PermissionsActivity) is not standard.

`medium` Launch Mode of activity (com.app.parentalcontrol.Activity.DebugActivity) is not standard.

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.BkgroundWork) is not Protected.

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.StartupReceiver) is not Protected.

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.OutgoingCallObserver) is not Protected.

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.screenshot.ScreenShotsReceiver) is not Protected.

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.LicenseReceiver) is not Protected.

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.RestartReceiver) is not Protected.

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.GpsHandler) is not Protected.

`medium` Broadcast Receiver (com.app.parentalcontrol.logging.Receivers.NetworkChangeReceiver) is not Protected.

`medium` Broadcast Receiver (com.android.inputmethod.dictionarypack.EventHandler) is not Protected.

`medium` Service (com.app.parentalcontrol.logging.BackService) is not Protected.

`medium` Service (com.app.parentalcontrol.logging.iKClipboardService) is not Protected.

`medium` Service (com.app.parentalcontrol.logging.CallingRecordService) is not Protected.

`medium` Service (com.android.internet.Stenographer_Service) is Protected by a permission, but the protection level of the permission should be checked.

`medium` Service (com.android.inputmethod.latin.LatinIME) is Protected by a permission, but the protection level of the permission should be checked.

`medium` Service (com.android.inputmethod.latin.spellcheck.AndroidSpellCheckerService) is Protected by a permission, but the protection level of the permission should be checked.

`medium` Service (com.app.parentalcontrol.logging.LocationUpdatesService) is not Protected.

`medium` Service (com.app.parentalcontrol.logging.MyNotificationListenService) is Protected by a permission, but the protection level of the permission should be checked.

`medium` High Intent Priority (2147483647)

`medium` High Intent Priority (2147483605)

`medium` High Intent Priority (2147483645)

`medium` High Intent Priority (2147483644)

`medium` High Intent Priority (2147483643)

`medium` High Intent Priority (2147483642)

`medium` High Intent Priority (2147483647)

`medium` High Intent Priority (2147483647)

`medium` High Intent Priority (2147483647)

`medium` Files may contain hardcoded sensitive information like usernames, passwords, keys etc.

`medium` Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.

| 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 | 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 | App creates temp file. Sensitive information should never be written into a temp file. | CODE |

| medium | The App uses an insecure Random Number Generator. | CODE |

| medium | MD5 is a weak hash known to have hash collisions. | CODE |

| medium | SHA-1 is a weak hash known to have hash collisions. | 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 |

| info | This app listens to Clipboard changes. Some malware also listen to Clipboard changes. | 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 24 critical permission(s) | PERMISSIONS |

MobSF Application Security Scorecard generated for (Settings 3.0.1)