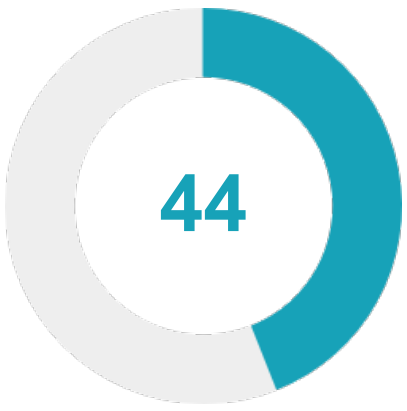
Security Score



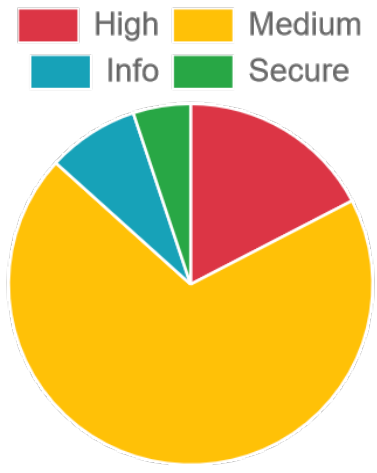
Security Score 44/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
6	24	3	2	1

high Base config is insecurely configured to permit clear text traffic to all domains	NETWORK
high Base config is configured to trust user installed certificates	NETWORK
high Domain config is insecurely configured to permit clear text traffic to these domains in scope	NETWORK
high App can be installed on a vulnerable upatched Android version	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 Base config is configured to trust system certificates	NETWORK
medium Activity (com.as.monitoringapp.Activity.TrialPage) is not Protected.	MANIFEST
medium High Intent Priority (2147483647)	MANIFEST
medium High Intent Priority (2147483605)	MANIFEST
medium High Intent Priority (2147483605)	MANIFEST
medium High Intent Priority (2147483645)	MANIFEST
medium High Intent Priority (2147483644)	MANIFEST

medium	High Intent Priority (2147483643)	MANIFEST
medium	High Intent Priority (2147483642)	MANIFEST
medium	High Intent Priority (2147483647)	MANIFEST
medium	High Intent Priority (2147483647)	MANIFEST
medium	High Intent Priority (2147483647)	MANIFEST
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	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	App creates temp file. Sensitive information should never be written into a temp file.	CODE
medium	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	CODE
medium	This App may request root (Super User) privileges.	CODE
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.	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	App can write to App Directory. Sensitive Information should be encrypted.	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 26 critical permission(s)	PERMISSIONS