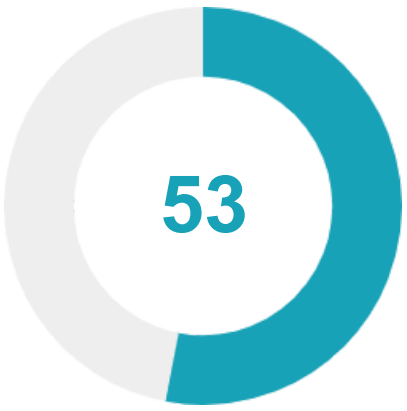
## Security Score

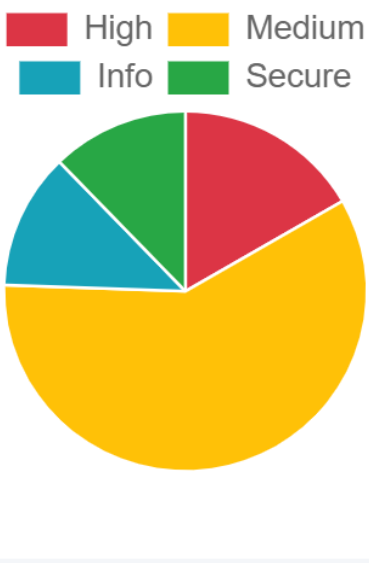



Security Score 53/100

## Risk Rating


Grade


## Severity Distribution (%)




## Privacy Risk


User/Device Trackers

## Findings

| High | Medium | Info | Secure | Hotspot |
|---|---|---|---|---|
| 2 | 7 | 2 | 2 | 1 |

| | |
|---|---|
| high Content Provider (.providers.TheftOverwriteProvider) is not Protected. | MANIFEST |
| high Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext. | CODE |
| medium Application Data can be Backed up | MANIFEST |
| medium Activity (.activities.DeeplinkActivity) is not Protected. | MANIFEST |
| medium Activity (.activities.LoginActivity) is not Protected. | MANIFEST |
| medium Activity (.activities.MainActivity) is not Protected. | MANIFEST |
| medium Service (.services.InsecureLoggerService) is not Protected. | MANIFEST |
| medium Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | CODE |
| medium App can read/write to External Storage. Any App can read data written to External Storage. | CODE |
| info App can write to App Directory. Sensitive Information should be encrypted. | CODE |
| 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 application has no privacy trackers | TRACKERS |
| hotspot Found 2 critical permission(s) | PERMISSIONS |

MobSF Application Security Scorecard generated for ( Oversecured Vulnerable Android App )



Version v3.5.2 Beta