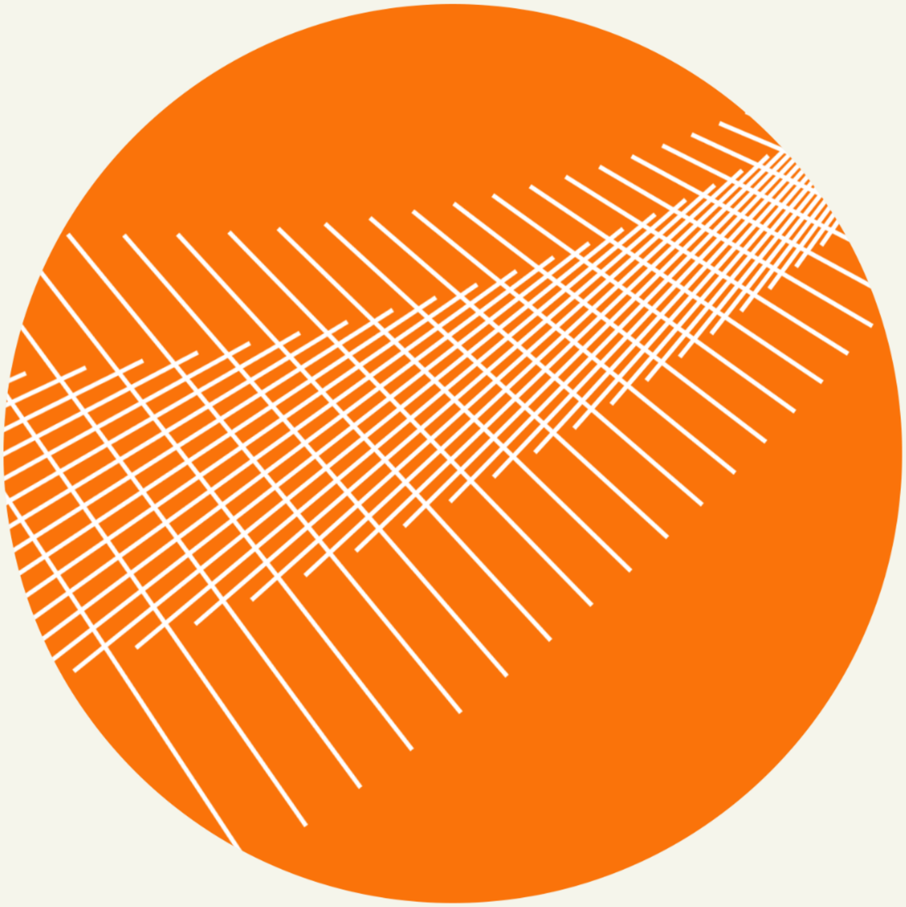
# CTDSEC

## YOU ARE PROTECTED



## TERMS

# Penetration Testing Android Bitrock Wallet [PASS✅]

# 1.0 Introduction

## 1.1 Project engagement

During January of 2024, Bitrock Wallet engaged CTDSec to audit apk that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the android application.

## 1.2 Disclaimer

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the application, rather limited to an assessment of the logic and implementation. In order to ensure a secure application that’s able to withstand the network’s fast-paced and rapidly changing environment, we at CTDSec recommend that bitrock wallet team put in place a bug bounty program to encourage further and active analysis of the wallet and always use multisignature/cold wallets if the user tries to manage a critical amount of funds for it. Hot wallets are used to make infrequent and small transfers.

# 3.0 Security Issues

Performing the attacks, we were able to run the application in rooted or emulated environments, use instrumentation tools to modify the application behavior and read the apk non encrypted.

The attack exercises carried out have been through black box pentests.

During the audit, 7 vulnerabilities were identified, 2 critical, 3 medium and 2 low.

All vulnerabilities were resolved and mitigated, except for one of them which is partially mitigated.

# 4.0 Summary of the audit

The bitrock wallet application **has passed the pentest control**, we recommend completely mitigating the medium reported vulnerability and having a bug bounty program. **We recommend that users use hot wallets for only sporadic and small transfers and for the secure use of funds use multi signature wallets and cold wallets**.