



# Wallet Application Security Audit Report



# Table Of Contents

<b>1 Executive Summary</b>	_____
<b>2 Audit Methodology</b>	_____
<b>3 Project Overview</b>	_____
3.1 Project Introduction	_____
3.2 Vulnerability Information	_____
3.3 Vulnerability Summary	_____
<b>4 Audit Result</b>	_____
<b>5 Statement</b>	_____

# 1 Executive Summary

On 2024.08.22, the SlowMist security team received the kucoin team's security audit application for KuCoin Web3 Wallet Security Audit(iOS), developed the audit plan according to the agreement of both parties and the characteristics of the project, and finally issued the security audit report.

The SlowMist security team adopts the strategy of "black-box and grey-box lead" to conduct a complete security test on the project in the way closest to the real attack.

The test method information:

Test method	Description
Black box testing	Conduct security tests from an attacker's perspective externally.
Grey box testing	Conduct security testing on code modules through the scripting tool, observing the internal running status, mining weaknesses.
White box testing	Based on the open source code, non-open source code, to detect whether there are vulnerabilities in programs such as nodes, SDK, etc.

The vulnerability severity level information:

Level	Description
Critical	Critical severity vulnerabilities will have a significant impact on the security of the project, and it is strongly recommended to fix the critical vulnerabilities.
High	High severity vulnerabilities will affect the normal operation of the project. It is strongly recommended to fix high-risk vulnerabilities.
Medium	Medium severity vulnerability will affect the operation of the project. It is recommended to fix medium-risk vulnerabilities.
Low	Low severity vulnerabilities may affect the operation of the project in certain scenarios. It is suggested that the project team should evaluate and consider whether these vulnerabilities need to be fixed.
Weakness	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.
Suggestion	There are better practices for coding or architecture.

## 2 Audit Methodology

The security audit process of SlowMist security team for wallet application includes two steps:

The codes are scanned/tested for commonly known and more specific vulnerabilities using automated analysis tools.

Manual audit of the codes for security issues. The wallet application is manually analyzed to look for any potential issues.

The following is a list of security audit items considered during an audit:

NO.	Audit Items	Result
1	App runtime environment detection	Passed
2	Code decompilation detection	Passed
3	App permissions detection	Passed
4	File storage security audit	Passed
5	Communication encryption security audit	Passed
6	Interface security audit	Passed
7	Business security audit	Passed
8	WebKit security audit	Passed
9	App cache security audit	Passed
10	WebView DOM security audit	Passed
11	SQLite storage security audit	Passed
12	Deeplinks security audit	Passed
13	Client-Based Authentication Security audit	Passed
14	Signature security audit	Passed
15	Deposit/Transfer security audit	Passed
16	Transaction broadcast security audit	Passed

NO.	Audit Items	Result
17	Secret key generation security audit	Passed
18	Secret key storage security audit	Passed
19	Secret key usage security audit	Passed
20	Secret key backup security audit	Passed
21	Secret key destruction security audit	Passed
22	Screenshot/screen recording detection	Passed
23	Paste copy detection	Passed
24	Keyboard keystroke cache detection	Passed
25	Insecure entropy source audit	Passed
26	Background obfuscation detection	Passed
27	Suspend evoke security audit	Passed
28	AML anti-money laundering security policy detection	Passed
29	Others	Passed
30	User interaction security	Passed

## 3 Project Overview

### 3.1 Project Introduction

#### Audit Version

iOS

Version: 3.115.0

Sha256Sum: 6f37e286017c6bd2eec91e1da5e1a80b7199683082d40881805e906e2b90dfba

#### Fixed Version

## iOS

Version: 1.0.0

Sha256Sum: 5cba061243106e504543c283c51889618c9209c6344d88ea38ecbf4e204b5e78

## 3.2 Vulnerability Information

The following is the status of the vulnerabilities found in this audit:

NO	Title	Category	Level	Status
N1	App runtime environment issue	App runtime environment detection	Suggestion	Acknowledged
N2	Code decompilation issue	Code decompilation detection	Suggestion	Acknowledged
N3	Communication encryption security issue	Communication encryption security audit	Suggestion	Acknowledged
N4	Business security issue	Business security audit	Suggestion	Acknowledged
N5	WebView DOM security issue	WebView DOM security audit	Low	Fixed
N6	Client-Based authentication security issue	Client-Based Authentication Security audit	Suggestion	Acknowledged
N7	Signature security issue	Signature security audit	Suggestion	Acknowledged
N8	Secret key generation security issue	Secret key generation security audit	Low	Fixed
N9	Secret key backup security issue	Secret key backup security audit	Suggestion	Acknowledged
N10	Screenshot/screen recording issue	Screenshot/screen recording detection	Suggestion	Acknowledged
N11	Paste copy issue	Paste copy detection	Suggestion	Acknowledged
N12	Keyboard keystroke cache issue	Keyboard keystroke cache detection	Suggestion	Acknowledged

NO	Title	Category	Level	Status
N13	Suspend evoke security issue	Suspend evoke security audit	Suggestion	Acknowledged
N14	AML anti-money laundering security policy issue	AML anti-money laundering security policy detection	Suggestion	Acknowledged
N15	User interaction security issue	User interaction security	Suggestion	Acknowledged

### 3.3 Vulnerability Summary

#### [N1] [Suggestion] App runtime environment issue

**Category: App runtime environment detection**

##### Content

1. Jailbreak detection is not exists.
2. The detection of Frida hooks is missing.
3. Debug mode is not enabled.

```
% frida -U -f com.gesan.bmark.com -l ./hook\ iOS.js

----
/_ _ |  Frida 16.2.1 - A world-class dynamic instrumentation toolkit
|(_| |
> _ |  Commands:
/_/ |_ |  help      -> Displays the help system
. . . .  object?   -> Display information about 'object'
. . . .  exit/quit -> Exit
. . . .
. . . .  More info at https://frida.re/docs/home/
. . . .
. . . .  Connected to iPhone (id=7c02e8b3a284dcdf36a0a077d9ede249abdd5263)
Spawning `com.gesan.bmark.com`...
isDebuggerPresent function not found
Debug mode is not enabled.
Spawned `com.gesan.bmark.com`. Resuming main thread!
[iPhone::com.gesan.bmark.com ]-> █
```

##### Solution

It is recommended to add Frida hook detection.

##### Status

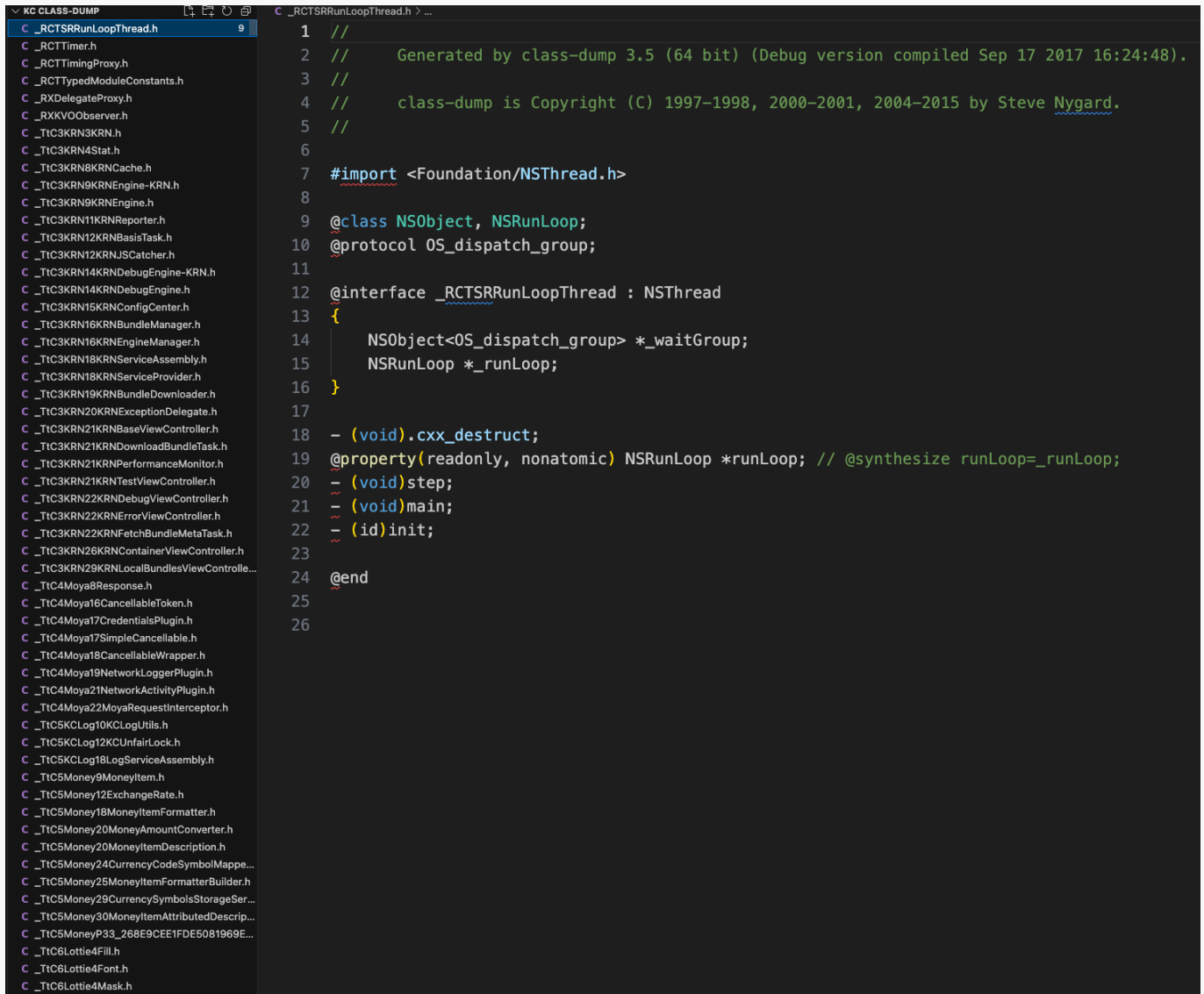
Acknowledged

## [N2] [Suggestion] Code decompilation issue

### Category: Code decompilation detection

#### Content

The header files of the iOS APP are not obfuscated. The function names and parameter passing rules can be seen through decompilation.



```

KC CLASS-DUMP
C _RCTSRRunLoopThread.h
C _RCTTimer.h
C _RCTTimingProxy.h
C _RCTTypedModuleConstants.h
C _RXDelegateProxy.h
C _RXKVOObserver.h
C _TtC3KRN3KRN.h
C _TtC3KRN4Stat.h
C _TtC3KRN8KRNCache.h
C _TtC3KRN9KRNEngine-KRN.h
C _TtC3KRN9KRNEngine.h
C _TtC3KRN11KRNReporter.h
C _TtC3KRN12KRNBasicTask.h
C _TtC3KRN12KRNJSCatcher.h
C _TtC3KRN14KRNDebugEngine-KRN.h
C _TtC3KRN14KRNDebugEngine.h
C _TtC3KRN15KRNConfigCenter.h
C _TtC3KRN16KRNBundleManager.h
C _TtC3KRN16KRNEngineManager.h
C _TtC3KRN18KRNServiceAssembly.h
C _TtC3KRN18KRNServiceProvider.h
C _TtC3KRN19KRNBundleDownloader.h
C _TtC3KRN20KRNExceptionDelegate.h
C _TtC3KRN21KRNBaseViewController.h
C _TtC3KRN21KRNDownloadBundleTask.h
C _TtC3KRN21KRNPerformanceMonitor.h
C _TtC3KRN21KRNTestViewController.h
C _TtC3KRN22KRNDebugViewController.h
C _TtC3KRN22KRNErrorViewController.h
C _TtC3KRN22KRNFetchBundleMetaTask.h
C _TtC3KRN26KRNContainerViewController.h
C _TtC3KRN29KRNLocalBundlesViewControll...
C _TtC4Moya8Response.h
C _TtC4Moya16CancellableToken.h
C _TtC4Moya17CredentialsPlugin.h
C _TtC4Moya17SimpleCancellable.h
C _TtC4Moya18CancellableWrapper.h
C _TtC4Moya19NetworkLoggerPlugin.h
C _TtC4Moya21NetworkActivityPlugin.h
C _TtC4Moya22MoyaRequestInterceptor.h
C _TtC5KLog10KLogUtils.h
C _TtC5KLog12KUnfairLock.h
C _TtC5KLog18LogServiceAssembly.h
C _TtC5Money9MoneyItem.h
C _TtC5Money12ExchangeRate.h
C _TtC5Money18MoneyItemFormatter.h
C _TtC5Money20MoneyAmountConverter.h
C _TtC5Money20MoneyItemDescription.h
C _TtC5Money24CurrencyCodeSymbolMappe...
C _TtC5Money25MoneyItemFormatterBuilder.h
C _TtC5Money29CurrencySymbolsStorageSer...
C _TtC5Money30MoneyItemAttributedDescrip...
C _TtC5MoneyP33_268E9CEE1FDE5081969E...
C _TtC6Lottie4Fill.h
C _TtC6Lottie4Font.h
C _TtC6Lottie4Mask.h
  
```

```

1 //
2 //   Generated by class-dump 3.5 (64 bit) (Debug version compiled Sep 17 2017 16:24:48).
3 //
4 //   class-dump is Copyright (C) 1997-1998, 2000-2001, 2004-2015 by Steve Nygard.
5 //
6
7 #import <Foundation/NSThread.h>
8
9 @class NSObject, NSRunLoop;
10 @protocol OS_dispatch_group;
11
12 @interface _RCTSRRunLoopThread : NSThread
13 {
14     NSObject<OS_dispatch_group> *_waitGroup;
15     NSRunLoop *_runLoop;
16 }
17
18 - (void).cxx_destruct;
19 @property(readonly, nonatomic) NSRunLoop *runLoop; // @synthesize runLoop=_runLoop;
20 - (void)step;
21 - (void)main;
22 - (id)init;
23
24 @end
25
26
  
```

#### Solution

It is recommended to confuse the header files to improve the threshold of decompilation and reverse engineering.

You can refer to: <https://github.com/pjebs/Obfuscator-iOS>

#### Status

Acknowledged

## [N3] [Suggestion] Communication encryption security issue



**Category: Communication encryption security audit****Content**

Apps do not have SSL Pinning mechanism, but all use HTTPS for communication.

**Solution**

It is recommended to use SSL Pinning to enhance the security of communication.

You can refer to: [https://cheatsheetseries.owasp.org/cheatsheets/Pinning\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Pinning_Cheat_Sheet.html)

**Status**

Acknowledged

**[N4] [Suggestion] Business security issue****Category: Business security audit****Content**

When adding an address to the address book, the user is not reminded to double-check whether the address is correct.

**Solution**

It is recommended that users be reminded to reconfirm whether the added address is correct when adding an address in the address book to prevent financial losses due to adding an incorrect address.

**Status**

Acknowledged

**[N5] [Low] WebView DOM security issue****Category: WebView DOM security audit****Content**

1. When a user opens a DApp, the wallet will automatically connect to the DApp without the user having to manually click to connect. If the user opens a malicious DApp, the automatic connection of the wallet may cause security risks.
2. The wallet's signature requests on the DApp page are not scoped, allowing them to be received under other tabs like the Wallet, which poses a phishing risk.

**Solution**

1. It is recommended that users do not connect automatically after opening the DApp, but let users click to connect manually.
2. It is recommended to restrict the scope of DApps by defaulting to disconnect and stop receiving requests when leaving the DApp page.

**Status**

Fixed; 1. As the wallet signature requires password verification, the risk level for accessing the DApp's automatic connection has been reduced to "Suggestion."

2. The project team has established a range limit for wallet signature requests on the DApp page, and the signature cannot be invoked once the user leaves the DApp page.

**[N6] [Suggestion] Client-Based authentication security issue****Category: Client-Based Authentication Security audit****Content**

When the wallet is set up with fingerprint or password authentication, you do not need to verify your fingerprint or password when you switch the app to the background and wake it up again or completely exit it and open it again.

**Solution**

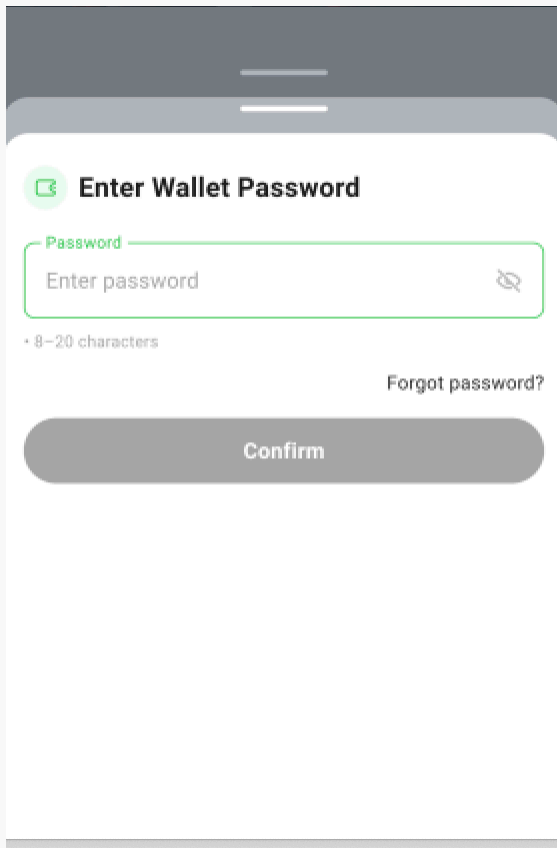
It is recommended to verify fingerprint or password when switching the app to the background and then waking it up, or when completely exiting the app and then reopening it.

**Status**

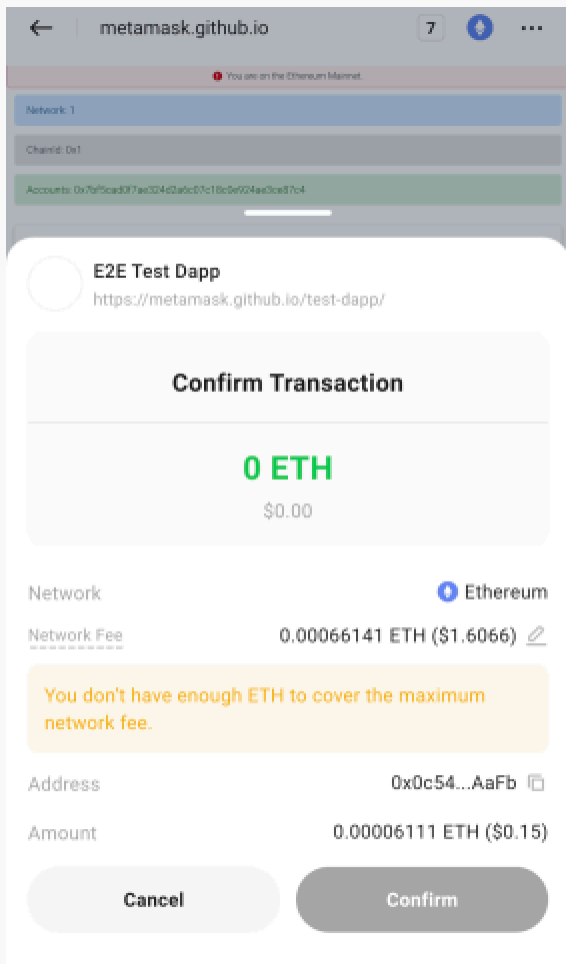
Acknowledged

**[N7] [Suggestion] Signature security issue****Category: Signature security audit****Content**

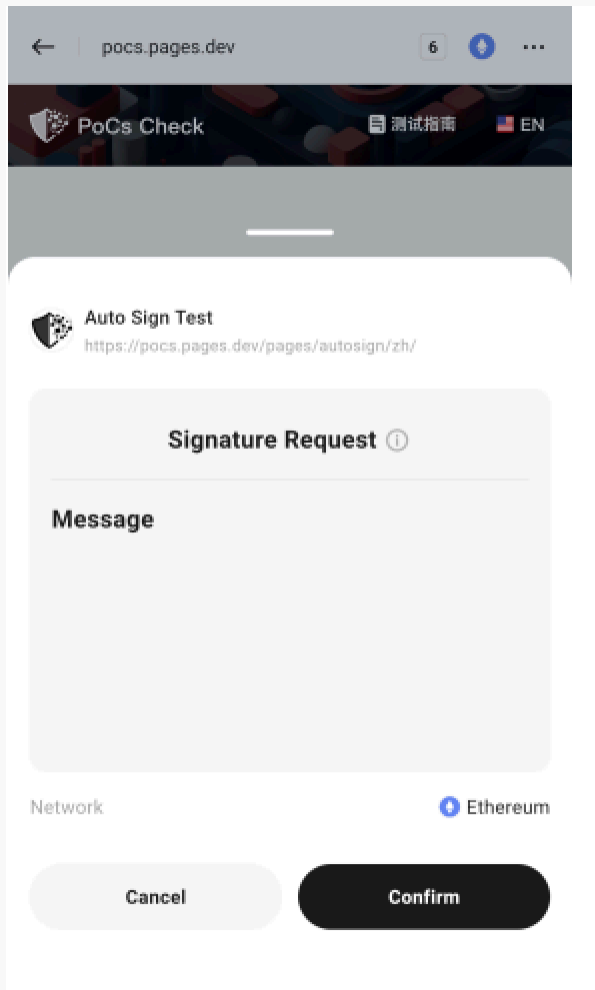
Signing requires a verification password.



The complete payment address is not displayed when signing the transfer.



Allow the use of eth\_sign blind signing service.



### Solution

1. It is recommended to display the complete payment address when signing and remind users to carefully check the transfer details.
2. It is recommended to disable the eth\_sign blind signing service.

### Status

Acknowledged; The eth\_sign blind signing service is no longer supported.

### [N8] [Low] Secret key generation security issue

**Category:** Secret key generation security audit

### Content

When the mnemonic is generated, it will be recorded in the log.

```
delta_in/delta_out: 213/448, Cell in/out: 0/0, Cell delta_in/delta_out: 0/0, RNF: 0, subscriber tag: 0
9396 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8787 DR=64.7743 factor=0.1322
9397 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8785 DR=64.7802 factor=0.1322
9398 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore[23334] <Notice>: | JGP | I - [JPCOREConnectManager] Action - closeConection
9399 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8783 DR=64.7861 factor=0.1321
9400 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8782 DR=64.7920 factor=0.1321
9401 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8780 DR=64.7979 factor=0.1321
9402 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8778 DR=64.8038 factor=0.1321
9403 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8777 DR=64.8097 factor=0.1321
9404 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8775 DR=64.8156 factor=0.1321
9405 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8773 DR=64.8216 factor=0.1321
9406 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8771 DR=64.8275 factor=0.1320
9407 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8770 DR=64.8334 factor=0.1320
9408 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8768 DR=64.8392 factor=0.1320
9409 Sep 19 15:02:14 iPhone-2 backboardd(CoreBrightness) [622] <Notice>: Lcurrent=121.6901 Lr=1.8766 DR=64.8451 factor=0.1320
9410 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(Flutter) [23334] <Notice>: flutter: flutter/channel_security:send: [channel = keychain, method = put, arguments =
[kc_exchange_wallet, 0x2BF0B4DcD03024C19c970627be2D43fa2b02a573_mnemonic, canyon split rabbit track rent total drive earth wall behave coin lamp, Biometric, ]]
9411 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(LocalAuthentication) [23334] <Notice>: Creating LAContext new cid:6
9412 Sep 19 15:02:14 iPhone-2 kernel(AppleSEPcredentialManager) [0] <Notice>: AppleCredentialManager: sendSEPCommand: SEP cmd(36) took 0 ms -> ioErr=0x0 acmErr=0.
9413 Sep 19 15:02:14 iPhone-2 coreauthd [1187] <Notice>: Context [237:2344] created
9414 Sep 19 15:02:14 iPhone-2 coreauthd [1187] <Notice>: ContextProxy [261:237:2344] created for Context [237:2344] pid:23334 uid:501
9415 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(LocalAuthentication) [23334] <Notice>: LAContext [23334:4] created new cid:6
9416 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(LocalAuthentication) [23334] <Notice>: LAContext [23334:1] deallocated
9417 Sep 19 15:02:14 iPhone-2 coreauthd [1187] <Notice>: ContextProxy [258:234:2340] deallocated
9418 Sep 19 15:02:14 iPhone-2 coreauthd [1187] <Notice>: Context [234:2340] deallocated
9419 Sep 19 15:02:14 iPhone-2 kernel(AppleSEPcredentialManager) [0] <Notice>: AppleCredentialManager: sendSEPCommand: SEP cmd(2) took 0 ms -> ioErr=0x0 acmErr=0.
9420 Sep 19 15:02:14 iPhone-2 coreauthd [1187] <Notice>: externalizedContextWithReply on ContextProxy [261:237:2344] rid:264
9421 Sep 19 15:02:14 iPhone-2 kernel(AppleSEPcredentialManager) [0] <Notice>: AppleCredentialManager: sendSEPCommand: SEP cmd(19) took 0 ms -> ioErr=0x0 acmErr=0.
9422 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(LocalAuthentication) [23334] <Notice>: externalizedContext on LAContext [23334:4] cid:7 returned be7a9a1
9423 Sep 19 15:02:14 iPhone-2 kernel(AppleSEPKeyStore) [0] <Notice>: AppleSEPKeyStore:10708:695: operation failed (sel: 43 ret: e007c008)
9424 Sep 19 15:02:14 iPhone-2 securityd [695] <Notice>: Authentication is needed for genp,rowid=8612 (-25330): Error Domain=NSOSSStatusErrorDomain Code=-25330 "(null)"
UserInfo={-25330=}
9425 Sep 19 15:02:14 iPhone-2 securityd [695] <Notice>: Authentication is needed KuCoin-Appstore[23334]/1#9 LF=0 copy_matching Error Domain=NSOSSStatusErrorDomain
Code=-25330 "(null)" UserInfo={-25330=}
9426 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(LocalAuthentication) [23334] <Notice>: Creating LAContext with externalized context be7a9a1 cid:8
9427 Sep 19 15:02:14 iPhone-2 coreauthd [1187] <Notice>: ContextProxy [262:237:2344] created for Context [237:2344] pid:23334 uid:501
9428 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(LocalAuthentication) [23334] <Notice>: LAContext [23334:5] created with externalized context be7a9a1 cid:8
9429 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(Security) [23334] <Notice>: LAEvaluateAndUpdateACL(<private>, <private>, <private>)
9430 Sep 19 15:02:14 iPhone-2 KuCoin-Appstore(LocalAuthentication) [23334] <Notice>: evaluateAccessControl:<SecAccessControlRef: aku;od(cpo
(DeviceOwnerAuthentication))>odel(true);oe(true)> options:{
9431 Sep 19 15:02:14 iPhone-2 coreauthd [1187] <Notice>: evaluateACL:dabca89 operation:od options:{
9432 Sep 19 15:02:14 iPhone-2 coreauthd(DaemonUtils) [1187] <Notice>: Determined bundle ID com.gesam.bmark.com for pid 23334
```

## Solution

It is recommended to block all user-related sensitive information in the log.

## Status

Fixed

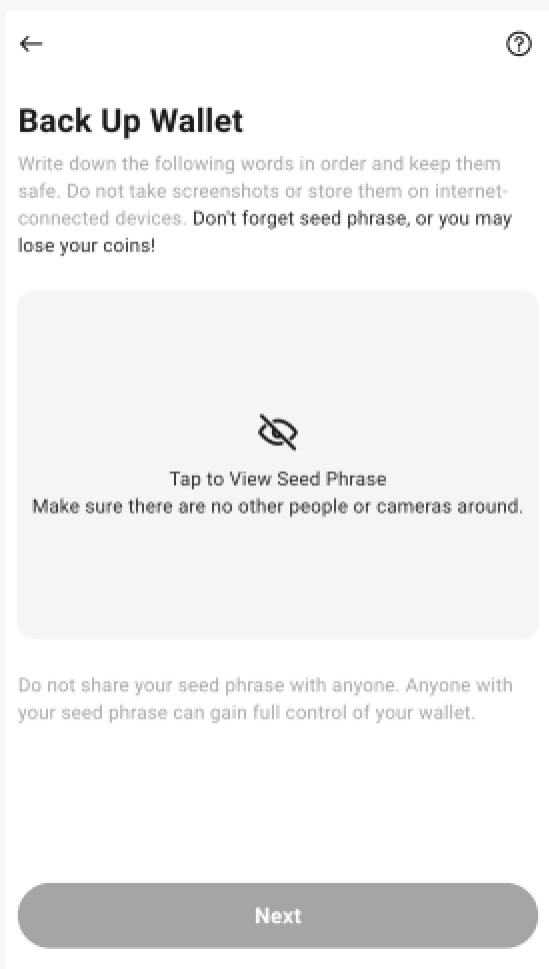
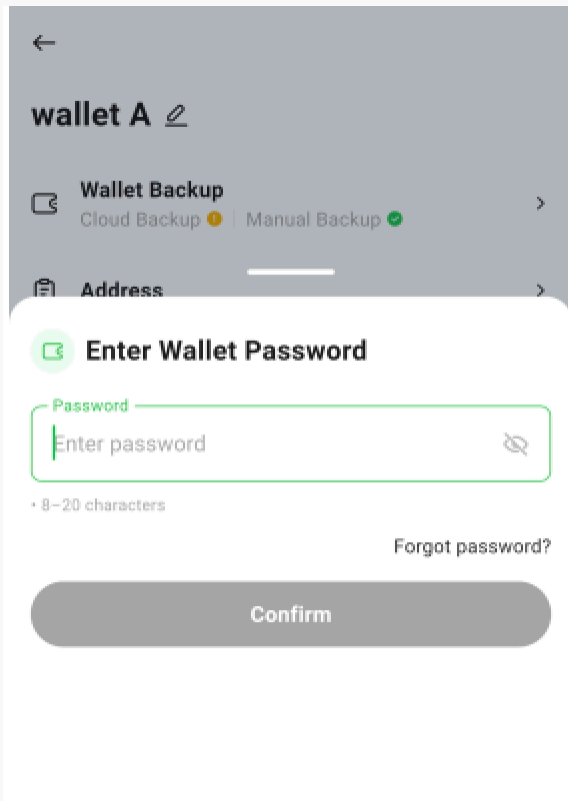
## [N9] [Suggestion] Secret key backup security issue

Category: Secret key backup security audit

## Content

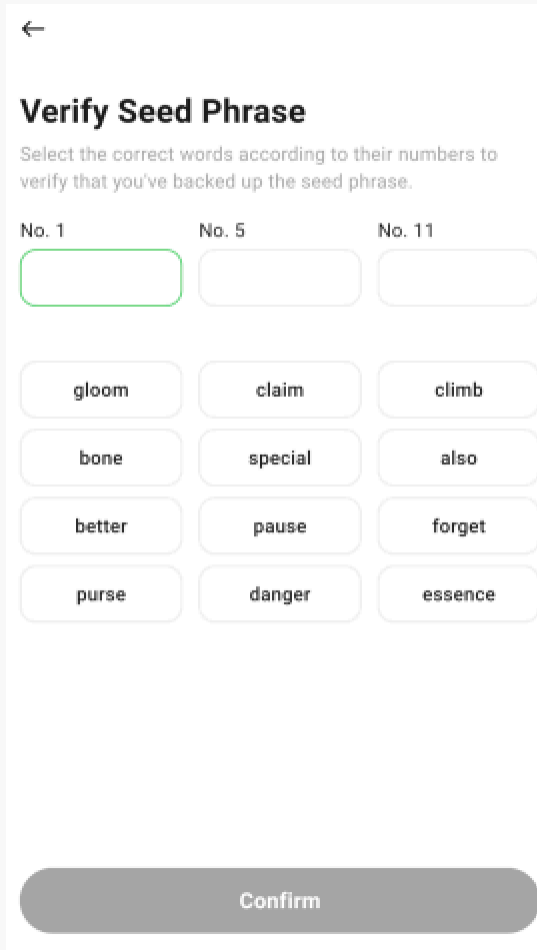
When backing up the mnemonic, verify the password first, and remind the user to ensure they are in a secure environment before displaying the mnemonic.

Only after the user confirms that the environment is secure should the plaintext information be shown.



There's a problem with only randomly verifying 3 words when backing up the mnemonic.

It doesn't provide enough validation.



←

### Verify Seed Phrase

Select the correct words according to their numbers to verify that you've backed up the seed phrase.

No. 1      No. 5      No. 11

gloom	claim	climb
bone	special	also
better	pause	forget
purse	danger	essence

Confirm

#### Solution

It is recommended to verify the full mnemonic phrase list when backing up.

#### Status

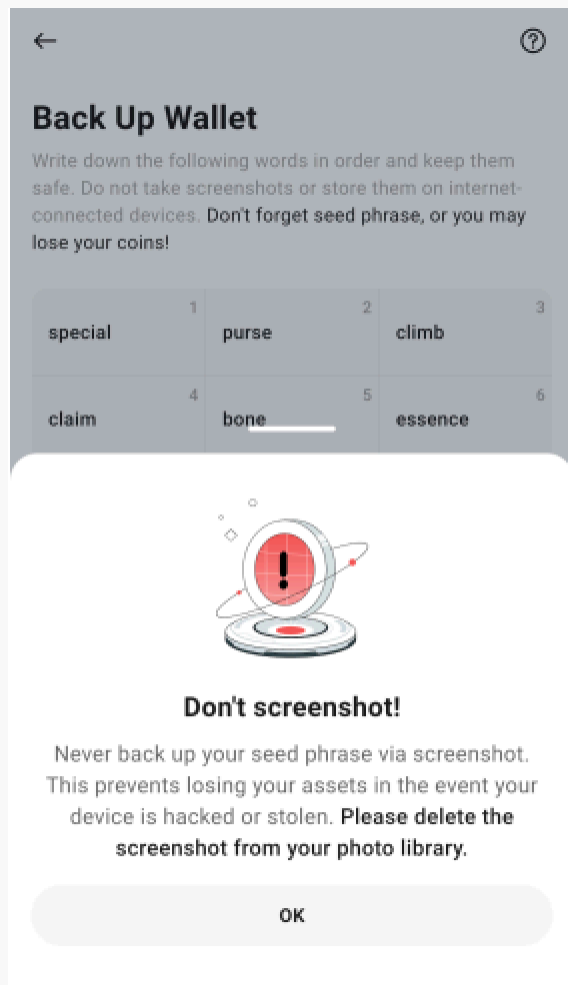
Acknowledged

#### [N10] [Suggestion] Screenshot/screen recording issue

**Category:** Screenshot/screen recording detection

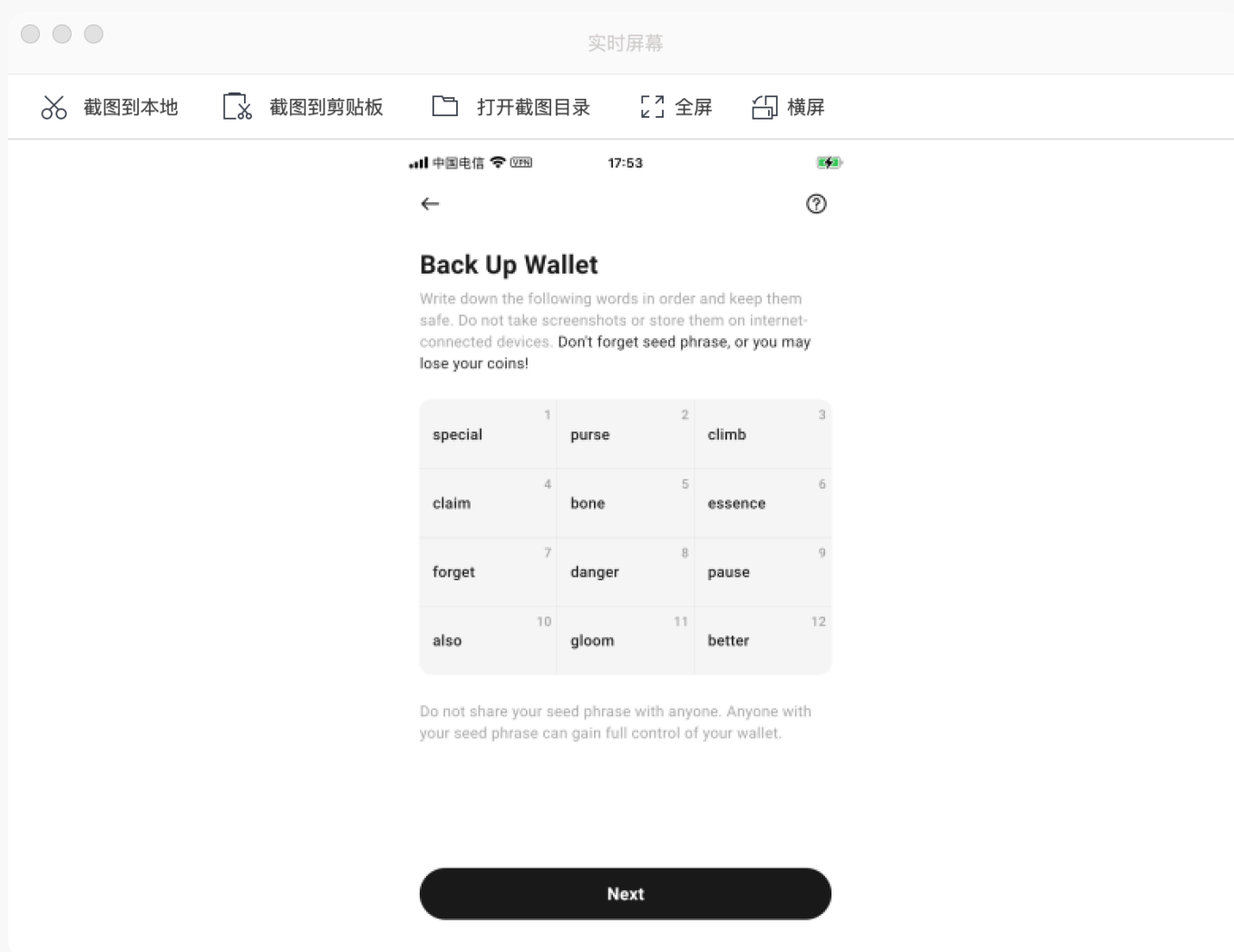
#### Content

Screen capture detection exists.



Lack of screen recording detection.





### Solution

It is recommended to add screen recording detection.

### Status

Acknowledged

### [N11] [Suggestion] Paste copy issue

#### Category: Paste copy detection

#### Content

After using the clipboard to import the mnemonics, the APP did not clear the contents of the clipboard or remind the user that the clipboard may leak sensitive data.

### Solution

It is recommended that after using the clipboard to import mnemonics, you should help users clear the data in the clipboard to prevent the mnemonics in the clipboard from being read by other applications, which may lead to mnemonics leakage.

**Status**

Acknowledged

**[N12] [Suggestion] Keyboard keystroke cache issue**

**Category:** Keyboard keystroke cache detection

**Content**

The phone's system keyboard is used when importing mnemonics.

**Solution**

It is recommended to use the built-in keyboard of the APP when entering sensitive data such as mnemonics to avoid sensitive information being uploaded to the cloud by third-party keyboards, which may lead to data leakage.

**Status**

Acknowledged

**[N13] [Suggestion] Suspend evoke security issue**

**Category:** Suspend evoke security audit

**Content**

The wallet app lacks a timeout mechanism and does not require password verification when resuming from suspension.

**Solution**

It is recommended to implement a timeout mechanism in the wallet app and introduce password verification upon resuming from suspension.

**Status**

Acknowledged

**[N14] [Suggestion] AML anti-money laundering security policy issue**

**Category:** AML anti-money laundering security policy detection

**Content**

The app does not have access to the AML security policy and cannot synchronize malicious addresses to users in a timely manner.

**Solution**

It is recommended to access the AML security policy to remind users to avoid interacting with malicious addresses.

### Status

Acknowledged

## [N15] [Suggestion] User interaction security issue

Category: User interaction security

### Content

Functionality	Support	Notes
<a href="#">WYSIWYS</a>	•	Allow the use of eth_sign blind signing service.
AML	✗	AML strategy is not supported.
Anti-phishing	✗	Phishing detect warning is not supported.
Pre-execution	✗	Pre-execution result display is not supported.
Contact whitelisting	✓	The contact whitelisting is supported, causing similar address attacks.
Password complexity requirements	•	Only the password length is limited, there is no complexity limit.

Tip: ✓ Full support, • Partial support, ✗ No support

### Solution

It is recommended to optimize relevant user interactions.

### Status

Acknowledged

## 4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002409040001	SlowMist Security Team	2024.08.22 - 2024.09.04	Passed

Summary conclusion: The SlowMist security team conducted an audit of the project utilizing both manual methods and the team's analytical tools. During the audit, we identified two low-risk vulnerabilities and thirteen suggested improvements. The two low-risk issues have been verified and fixed, while all other findings have also been acknowledged. We would like to express our gratitude to the KuCoin wallet team for their recognition of SlowMist and for the hard work and support of the relevant staff.

## 5 Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility based on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.



**Official Website**  
[www.slowmist.com](http://www.slowmist.com)



**E-mail**  
[team@slowmist.com](mailto:team@slowmist.com)



**Twitter**  
[@SlowMist\\_Team](https://twitter.com/SlowMist_Team)



**Github**  
<https://github.com/slowmist>