



# 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 2025.01.15, the SlowMist security team received the Safeheron team's security audit application for Safeheron Crypto MPC Wallet (Android), 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" 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

Android

DownLink: <https://play.google.com/store/apps/details?id=com.safeheron.app.sg>

Version: 1.5.1

Shasum: 3c64b554cf1bec2ecf155127fe9849617c6e590d97f3bdb5cea2743346ec93a9

## 3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	App Permissions Detection Issue	App permissions detection	Suggestion	Acknowledged
N2	File Upload Issue	Business security audit	Suggestion	Acknowledged
N3	Client-Based Authentication Security Issue	Client-Based Authentication Security audit	Suggestion	Acknowledged
N4	Screenshot/Screen Recording Issue	Screenshot/screen recording detection	Suggestion	Acknowledged
N5	Copy And Paste Issue	Paste copy detection	Suggestion	Acknowledged
N6	Keyboard Keystroke Cache Issue	Keyboard keystroke cache detection	Suggestion	Acknowledged
N7	Background Obfuscation Issue	Background obfuscation detection	Suggestion	Acknowledged
N8	Suspend Evoke Security Issue	Suspend evoke security audit	Suggestion	Acknowledged
N9	User Interaction Security Issue	User interaction security	Suggestion	Acknowledged

## 3.3 Vulnerability Summary

### [N1] [Suggestion] App Permissions Detection Issue

**Category:** App permissions detection

#### Content

Review the permissions the APK has.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.POST_NOTIFICATIONS	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.htyap.mcs.permission.RECIEVE_MCS_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.hihonor.android.launcher.permission.CHANGE_BADGE	unknown	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.meizu.flyme.permission.PUSH	unknown	Unknown permission	Unknown permission from android reference
com.safheron.app.sg.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.safheron.app.sg.permission.JPUSH_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.safheron.app.sg.permission.MIPUSH_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	unknown	Unknown permission	Unknown permission from android reference

## Solution

According to the actual business needs, follow the principle of permission design minimization, and reasonably set the use of App permissions.

## Status

Acknowledged

## [N2] [Suggestion] File Upload Issue

**Category: Business security audit**

## Content

Removing "X - Sh - W - Sig" and "X - Sh - W" from the file upload interface request package allows for bypassing the signature check.

The upload interface will check the file extension.

Request

Pretty Raw Hex

1 POST /uic/app/user/portrait/update HTTP/2

2 Host: gm-gateway.safeheron.vip

3 Accept: application/json

4 Accept-Language: en-US

5 X-Source: 1

6 X-Device: 8da261e0b0109c08

7 User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Android SDK built for arm64 Build/OSM1.180201.044.D2; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.98 Mobile Safari/537.36 Safeheron/1.5.1

8 X-App-Version: 10501

9 X-User-Token: b4ff9cd5-f14d-4fbd-a023-8f9e2105e053

10 X-Sh-Timestamp: 1737019354669

11 X-Wallet-Member-Id: app-99b99ba4-b979-4c79-b5e7-0a41e15f18a3

12 Content-Type: multipart/form-data; boundary=62300449-5fde-4c59-9d19-139090fa47f2

13 Content-Length: 342864

14 Accept-Encoding: gzip, deflate, br

15

16 --62300449-5fde-4c59-9d19-139090fa47f2

17 content-disposition: form-data; name="file"; filename="photo.png"; filename\*=utf-8''photo.js

18 Content-Type: image/png

19 Content-Length: 342635

20

21 ŷøÿàJFIFÿÜÿÄÄ"ŷÄ

22 ŷÄ !1A"Qaq ð2Bi±ÄÑ#3Ráñ

23 \$CSb4crs 8DTv£³%57dtw 'µ¶·ÄEue ¢=Ô&'6Fu ÄÖäVW

24 Gf¥!²Öó(g \$ÄÄ× ÖÖäääöŷÄ

25 ŷÄX1!AQa iÑ"2q ±ÄðáñBb#34CR r²\$5Ss¢³ÄDcÔTt Uu £'â%'

26 Ä7F ŷÜ? w@Hø\$Tø µ

27 KÖ P7é T) µ,İØ Æ + ¥5,,{ðä¼!Öà"ø Rg1 7g,Azİäöœ ¼

28 "cø Ê Æz·ØJñ ;bk €p: E:HÄ

29 «ÄØt ²ð¿L÷Ä{EQ€ LPâ=i, )ÉZ

30 ÉÄfâÿ ÄÄÄ±vF1äpÆ(è µ M<l|ÜdÄä,g,ÄäÄ~ «&Ü#Ääæ~ d6K@È

31 ò%Ø ³JøjëgØÄ V!ò K<<G6ÜøgİêL³}İüö D R( È{ixx °

32 !t%|f&p#cRlZµ³|xÖ·á\¹&D Wº:ýİJen

33 ÜY [ò B; ² 8.ì .qsûíİÆe&-³/ ,òj

34 Ä±÷>ðIUøB6 ² +i ÆKê\$' ¼Yò·Mì

35 ©WjÄE|OGÈ8ö |Gk^= ²ª&äö÷è'Ö@!²5+ [g[4éu DÄyEtý(¼ è'Ç

36 FÉF-\$ ,è¹L ÜÄP! :,i#

37 r ² \*Ê 8!·2} \$ .µ£Ö¢(ð«&.èBda<Üç¼L

38 %/Lö äÄ!€İEK|tÖ7¥!ÜY A@) " ¥'Ä×]lŸt ± . %X·! äÜ°=p

39 ÜëİYDE~\_HN¼-¹€#²89YÄÄÄ(äİ €Ä)·MİÜ€"%/¼ñ ¼Rg¥

Response

Pretty Raw Hex Render

1 HTTP/2 200 OK

2 Content-Type: application/json

3 Access-Control-Allow-Credentials: true

4 Access-Control-Expose-Headers: \*

5 Safeheron-Trace-Id: gw3a0a4d5accacae41a6a64d46b878a0b6ab

6 Strict-Transport-Security: max-age=63072000; includeSubdomains; preload

7 Vary: Accept-Encoding

8 Date: Thu, 16 Jan 2025 10:00:36 GMT

9 Content-Length: 106

10 Server-Timing: edge; dur=10

11 Server-Timing: origin; dur=152

12 Server-Timing: cdn-cache; desc=MISS

13 Server-Timing: ak\_p; desc="1737021636771\_399123221\_43136329\_16240\_3852\_4\_0\_15"; dur=1

14

15 {

16 "timestamp":1737021636928,

17 "code":405,

18 "errorCode":101009,

19 "message":"[101009]File type error.",

20 "data":null

21 }

Inspector

Notes

Search

0 highlights

Search

0 highlights

The upload interface will check the file size.



The image displays a web browser window with a REST client interface. The interface is split into two main panels: 'Request' on the left and 'Response' on the right. The 'Request' panel shows a POST request to the endpoint `/uic/app/user/portrait/update` with a `Host: gm-gateway.safeheron.vip` and various headers including `Accept: application/json`, `Accept-Language: en-US`, `X-Source: 1`, `X-Device: 8da261e0b0109c08`, `User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Android SDK built for arm64 Build/OSM1.180201.044.D2; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.98 Mobile Safari/537.36 Safeheron/1.5.1`, `X-App-Version: 10501`, `X-User-Token: b4ff9cd5-f14d-4fbd-a023-8f9e2105e053`, `X-Sh-Timestamp: 1737019354669`, `X-Wallet-Member-Id: app-99b99ba4-b979-4c79-b5e7-0a41e15f18a3`, `Content-Type: multipart/form-data; boundary=62300449-5fde-4c59-9d19-139090fa47f2`, `Content-Length: 13419463`, and `Accept-Encoding: gzip, deflate, br`. The body is a multipart form data with a `content-disposition: form-data; name="file"; filename="photo.png"` and `Content-Type: image/png`. The 'Response' panel shows a 200 OK response with `Content-Type: application/json`, `Access-Control-Allow-Credentials: true`, `Access-Control-Expose-Headers: *`, `Safeheron-Trace-Id: gwfed9fe750897435faabda88cc5898542`, `Strict-Transport-Security: max-age=63072000; includeSubdomains; preload`, `Vary: Accept-Encoding`, `Date: Thu, 16 Jan 2025 09:55:40 GMT`, `Content-Length: 122`, `Server-Timing: edge; dur=35`, `Server-Timing: origin; dur=6104`, `Server-Timing: cdn-cache; desc=MISS`, and `Server-Timing: ak_p; desc="1737021334624_399123413_23098799_613927_3015_1_52_15";dur=1`. The response body is a JSON object: `{ "timestamp": 1737021340813, "code": 405, "errorCode": 101013, "message": "[101013]The file size exceeds the limit.", "data": null }`. The browser's address bar shows the URL `http://gm-gateway.safeheron.vip/uic/app/user/portrait/update` and the status bar at the bottom indicates '0 highlights'.

The upload interface checks the Content-Type field.

Request

Pretty

Raw

Hex

🔍

📄

🔍

🔍

🔍

1 POST /uic/app/user/portrait/update HTTP/2

2 Host: gm-gateway.safeheron.vip

3 Accept: application/json

4 Accept-Language: en-US

5 X-Source: 1

6 X-Device: 8da261e0b0109c08

7 User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Android SDK built for arm64 Build/OSM1.180201.044.D2; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.98 Mobile Safari/537.36 Safeheron/1.5.1

8 X-App-Version: 10501

9 X-User-Token: b4ff9cd5-f14d-4fbd-a023-8f9e2105e053

10 X-Sh-Timestamp: 1737019354669

11 X-Wallet-Member-Id: app-99b99ba4-b979-4c79-b5e7-0a41e15f18a3

12 Content-Type: multipart/form-data; boundary=62300449-5fde-4c59-9d19-139090fa47f2

13 Content-Length: 342880

14 Accept-Encoding: gzip, deflate, br

15

16 --62300449-5fde-4c59-9d19-139090fa47f2

17 content-disposition: form-data; name="file"; filename="photo.png"; filename\*=utf-8''photo.png

18 Content-Type: application/x-javascript

19 Content-Length: 342635

20

21 ŷøÿàJFIFÿÜCÿÜCÿÄÄ"ÿÄ

22 ŷÄ !1A"Qaq ð2Bi±ÄÑ#3Ráñ

23 \$CSb4crs 8DTv£³57dtw ´µ¶·ÄEUE ¢=Ô&'6Fu ÄÖäVW

24 Gf¥!²Óó(g \$ÄÄx ÖÖääöÿÄ

25 ŷÄX1!AQa iN"2q ±ÄðáñBb#34CR r²\$5Ss¢³ÄDcÔTt Uu £´â%

26 Ä7F ŷÜ? w@Hø\$Tø µ

27 KÖ P7é T) µ,İØ Æ + ¥5,,{ðä½!Öà"ø Rg1 7g,Azİäö€ç ¼

28 "cø Ê Æz·ØJñ ;bk €p: E:HÄ

29 «Äøt ²ð¿L÷Ä{EQ€ LPâ=i, )ÉZ

30 ÉÄfäy ÄÄ4Æ±vF1äpÆ(è µ M<l`|ÜdÄä,g,ÄäÄ~ «&Ü#Ääæ~ d6K@Ë

31 ò%Ø ³JojëgØÄ V!ð K<<G6ÜÜøgİêL³}İÜö D R( Ê[ixx °

32 !t%|f&p#cRlZµ³|xÖ·á\`&D Wº:ýİJen

33 ÜY [ò B; º 8.1 .qsÜíİÆe&-³/ ,òj

34 Ä±±>ðIUöB6 º +i ÆKê\$´ ½Yð·Mì

35 ©WjÄE|OG£8ö\_|Gk^= ¨ª&äö÷è`Ö@!`5+ [g[4éu DÄyEtý(¼ è´C

36 FÉF-\$ ,è¹L ÜÄP! :,i#

37 r º \*É 8!,2} \$ .µ£Ö¢(ð«&.èBda<Üç¾L

38 %/Lö äÄ!€iEK)tÖ7¥!ÜY A@) " ¥'Äx]lŸt ± . %X·! äÜ°=p

39 ÜëiYDE~\_HN¾-¹€#ä²89YÄÄÄ(äİ €Ä·MİÜ©"%/¾ñ ½Rg¥

40

21 HTTP/2 200 OK

2 Content-Type: application/json

3 Access-Control-Allow-Credentials: true

4 Access-Control-Expose-Headers: \*

5 Safeheron-Trace-Id: gw8b79ef57085b45408f92e7ff5591e977

6 Strict-Transport-Security: max-age=63072000; includeSubdomains; preload

7 Vary: Accept-Encoding

8 Date: Thu, 16 Jan 2025 10:02:49 GMT

9 Content-Length: 106

10 Server-Timing: edge; dur=43

11 Server-Timing: origin; dur=196

12 Server-Timing: cdn-cache; desc=MISS

13 Server-Timing: ak\_p; desc="1737021769285\_386011158\_199068936\_23965\_5079\_3\_45\_15";dur=1

14

15 {

16 "timestamp":1737021769570,

17 "code":405,

18 "errorCode":101009,

19 "message":"[101009]File type error.",

20 "data":null

21 }

🔍

🔍

🔍

🔍

🔍

Search

0 highlights

🔍

🔍

🔍

🔍

🔍

Search

0 highlights

Special characters are not allowed in the file name.

**Request**

Pretty Raw Hex

```
1 POST /uic/app/user/portrait/update HTTP/2
2 Host: gm-gateway.safeheron.vip
3 Accept: application/json
4 Accept-Language: en-US
5 X-Source: 1
6 X-Device: 8da261e0b0109c08
7 User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Android
  SDK built for arm64 Build/OSM1.180201.044.D2; wv)
  AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
  Chrome/61.0.3163.98 Mobile Safari/537.36 Safeheron/1.5.1
8 X-App-Version: 10501
9 X-User-Token: b4ff9cd5-f14d-4fbd-a023-8f9e2105e053
10 X-Sh-Timestamp: 1737019354669
11 X-Wallet-Member-Id:
  app-99b99ba4-b979-4c79-b5e7-0a41e15f18a3
12 Content-Type: multipart/form-data;
  boundary=62300449-5fde-4c59-9d19-139090fa47f2
13 Content-Length: 342875
14 Accept-Encoding: gzip, deflate, br
15
16 --62300449-5fde-4c59-9d19-139090fa47f2
17 content-disposition: form-data; name="file"; filename="
  !@#%^&*().png"; filename*=utf-8'!'!@#%^&*().png
18 Content-Type: image/png
19 Content-Length: 342635
20
21 y0yàJFIFÿÜCÿÜCÿÄÄ"ÿÄ
22 ÿÄ !1A"Oaq 02Bi±ÄÑ#3Ráñ
  $CSb4csrc 8DTv£%57dtw 'µµ·ÄEue ¢=0&'6Fu Ä0äVW
  Gf¥!²06(g $ÄÄ× 00ääääöÿÄ
23 ÿÄX1!Aqa iN"2q ±Ä0áñBb#34CR r²$5Ss¢³ÄDc0Tt Uu £'â% '
  Ä7F ÿÜ? w@H0$T0 µ
24 KÓ P7é T) µ.Ï0 Æ + ¥5. {ðä½!0à"0 Rg1 7g.Ai.Ïä0Ec ½
  "c0 É Æz.0Jñ !bk ¢p: E:HÄ
25 «Ä0t ²0¿L+Ä{EQ0 LPâ=i. )ÉZ
26 ÉÄfây ÄÄ4±tvF1äpÆ(è µ M<L`|ÜdÄä,g,ÄäÄ- «ðÜ#Ääæ- d6K@É
  0%0 #Jojëg0Ä V!ð K<<G60ü0gïèL³}Iú0 D R( É!ixx .°
  !t%|fðp#cRLZµ³|x0.á:ð0 W0:ýIjen
  ÜY [0 B; 0 8.i .qsúííÆe&-³/ ,òj
  Ä±+>ðÏÜ0B6 0 +i ÆKè$ ½Yð·M1
  ©WjÄE|0G£80_ |Gk^= ±#ðä0+è'0@!²5+ [g[4éu DÄyEtý(¼ è´C
  FÉF-$ ,è¹L ÜÄp! :.i#
  r # *É 8!|.2} $ .µ£0¢(ð«&.ÉBda<Üc¾L
27 %/L0 äÄ!èiEK|t07¥!ÜY A@) " ¥'Äx|Ünt ± . %X·| äÜ·#p
  ÜèiYDE_-HN¾-¹¢#ä²89YÄÄÄ(äi €Ä»·MIÜ0"µ/¾ñ ½Rg¥
  28
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: application/json
3 Access-Control-Allow-Credentials: true
4 Access-Control-Expose-Headers: *
5 Safeheron-Trace-Id: gwa524530594b64168b2b06ebb617c20d8
6 Strict-Transport-Security: max-age=63072000;
  includeSubdomains; preload
7 Vary: Accept-Encoding
8 Date: Thu, 16 Jan 2025 10:06:35 GMT
9 Content-Length: 98
10 Server-Timing: edge; dur=11
11 Server-Timing: origin; dur=183
12 Server-Timing: cdn-cache; desc=MISS
13 Server-Timing: ak_p;
  desc="1737021995228_386011158_199334609_19456_5465_2_0_15"
  ;dur=1
14
15 {
  "timestamp":1737021995427,
  "code":500,
  "errorCode":null,
  "message":"[500]System error.",
  "data":null
}
```

Inspector Notes

0 highlights

No directory traversal issues were found.

The screenshot displays the Burp Suite interface with two main panels: Request and Response.

**Request Panel:**

- Method: POST
- URL: /uic/app/user/portrait/update HTTP/2
- Host: gm-gateway.safeheron.vip
- Accept: application/json
- Accept-Language: en-US
- X-Source: 1
- X-Device: 8da261e0b0109c08
- User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Android SDK built for arm64 Build/OSM1.180201.044.D2; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.98 Mobile Safari/537.36 Safeheron/1.5.1
- X-App-Version: 10501
- X-User-Token: b4ff9cd5-f14d-4fbd-a023-8f9e2105e053
- X-Sh-Timestamp: 1737019354669
- X-Wallet-Member-Id: app-99b99ba4-b979-4c79-b5e7-0a41e15f18a3
- Content-Type: multipart/form-data; boundary=62300449-5fde-4c59-9d19-139090fa47f2
- Content-Length: 342879
- Accept-Encoding: gzip, deflate, br
- 62300449-5fde-4c59-9d19-139090fa47f2
- content-disposition: form-data; name="file"; filename="../../../../.png"; filename\*=utf-8'../../../../.png
- Content-Type: image/png
- Content-Length: 342635

**Response Panel:**

- Status: 200 OK
- Content-Type: application/json
- Access-Control-Allow-Credentials: true
- Access-Control-Expose-Headers: \*
- Safeheron-Trace-Id: gw614fb50ddbcb04ef492c59c81c48be929
- Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
- Vary: Accept-Encoding
- Date: Thu, 16 Jan 2025 10:08:05 GMT
- Content-Length: 98
- Server-Timing: edge; dur=13
- Server-Timing: origin; dur=179
- Server-Timing: cdn-cache; desc=MISS
- Server-Timing: ak\_p; desc="1737022085614\_386011158\_199437585\_19225\_6875\_2\_0\_15";dur=1

**Error Message:**

```
{
  "timestamp":1737022085811,
  "code":500,
  "errorCode":null,
  "message":"[500]System error.",
  "data":null
}
```

The file upload interface has permission control.

The image shows a web browser's developer tools with the 'Network' tab selected. A single network request is visible, and its details are expanded. The 'Request' pane on the left shows the raw HTTP request, and the 'Response' pane on the right shows the raw HTTP response.

**Request:**

```
1 POST /uic/app/user/portrait/update HTTP/2
2 Host: gm-gateway.safeheron.vip
3 Accept: application/json
4 Accept-Language: en-US
5 X-Source: 1
6 X-Device: 8da261e0b0109c08
7 User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Android
  SDK built for arm64 Build/OSM1.180201.044.D2; wv)
  AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
  Chrome/61.0.3163.98 Mobile Safari/537.36 Safeheron/1.5.1
8 X-App-Version: 10501
9 X-Sh-Timestamp: 1737019354669
10 X-Wallet-Member-Id:
  app-99b99ba4-b979-4c79-b5e7-0a41e15f18a3
11 Content-Type: multipart/form-data;
  boundary=62300449-5fde-4c59-9d19-139090fa47f2
12 Content-Length: 342865
13 Accept-Encoding: gzip, deflate, br
14
15 --62300449-5fde-4c59-9d19-139090fa47f2
16 content-disposition: form-data; name="file"; filename="
  photo.png"; filename*=utf-8''photo.png
17 Content-Type: image/png
18 Content-Length: 342635
19
20 ŸŸäJFIFŸÜCŸÜCŸÄÄ"ŸÄ
21 ŸÄ !1A"Qaq 02Bi±ÄÑ#3Ráñ
  $CSb4crs 8DTvf%57dtw 'µñ!·ÄEUe ¢=0&'6Fu Ä0äVW
  Gf¥!²0ó(g $ÄÄ× 00äää0ŸÄ
22 ŸÄX1!Aqa iN"2q ±Ä0áñBb#34CR r²$5Sst³ÄDC0Tt Uu £'â%'
  Ä7F ŸÜ? w@H0ST0 µ
23 KÓ P7é T) µ,İ0 Æ + ¥5,_{äâ¼!Öà"Ø Rg1 7g,Azİäöeç ¼
  "c0 É Æz·0Jñ !bk €p: E:HÄ
24 <Ä0t ²0L+Ä{(EQE LPâ=i, )EZ
25 ÉÄfay ÄÄ4±vF1äpÆ(è µ M<l`İÜDÄâ,g,ÄÄÄ- «&Ü#Ääæ- d6K0É
  0%0 ªJojëg0Ä V!ò K<«G6Ü0@giÉL³}İü0 D R( É[ixx ·°
  !t%!f&þ#cRLZµ³|x0·á¹&D W0:ŸİJen
  ÜY [ò B; ° 8.ì .qsúìİÆe&-³/ ,òj
  Ä±±>DİÜ086 ° +i ÆKè$´ ¼Yò·Mì
  ¢WJÄE|0Gf8ö_|Gk^= º*äö+è°@;"5+ [g4éu DÄyEtÿ(¼ ë'Ç
  FÉF-$ ,è¹L ÜÄP! :,i#
  r º *É 8!,2} $ ,µfÖ¢(ò«&,èBda<Ü¼³L
26 %/L0 äÄ!€iEK!t07¥!ÜY A@) " ¥'Ä×]Lñt ± . %X·! äÜ°>þ
  ÜëiYDE-_HN³-¹€ä²89YÄÄÄ(äİ €Ä·MİÜc"%/¾ñ ¼Rg¥
27 h +xİ a h kùµfCV±TL Ÿİ
```

**Response:**

```
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 Content-Length: 55
4 Access-Control-Allow-Credentials: true
5 Access-Control-Expose-Headers: *
6 Safeheron-Trace-Id: dff67599-6b0f-4ade-aabd-067e4e425ac0
7 Strict-Transport-Security: max-age=63072000;
  includeSubdomains; preload
8 Date: Thu, 16 Jan 2025 10:09:11 GMT
9 Server-Timing: edge; dur=31
10 Server-Timing: origin; dur=158
11 Server-Timing: cdn-cache; desc=MISS
12 Server-Timing: ak_p;
  desc="1737022151193_399123221_43768672_18963_4636_2_41_15"
  ;dur=1
13
14 {
  "errMsg":"Not Logged in",
  "isSuccess":false,
  "code":400
}
```

### Solution

It is recommended that the interface checks for the existence of the signature.

## Status

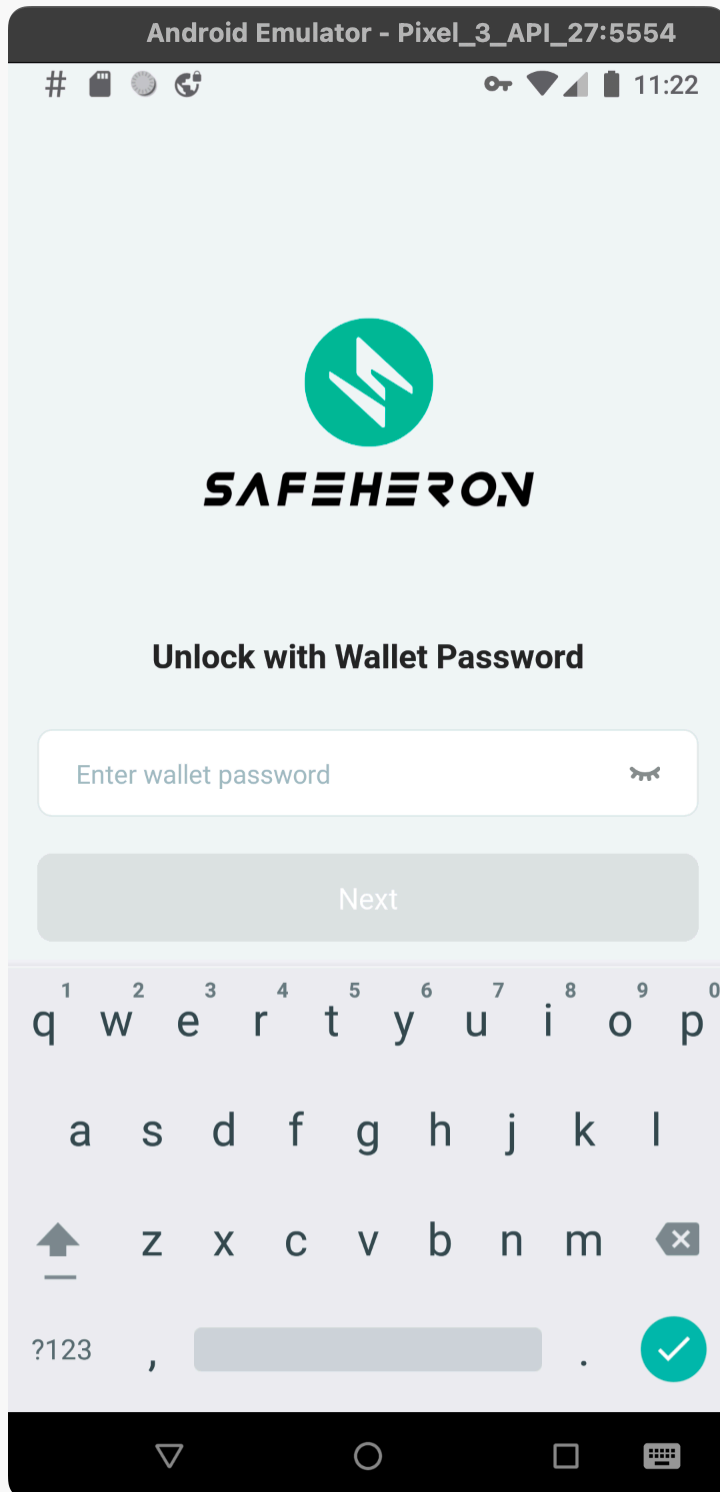
## Acknowledged

### [N3] [Suggestion] Client-Based Authentication Security Issue

**Category: Client-Based Authentication Security audit**

## Content

When the App Lock function is turned on, you need to verify your wallet password to completely exit the app.



The wallet password needs to be verified when the background is called up again after being suspended for a while.

The user is not guided to set the wallet password when logging into the App for the first time.

### Solution

It is recommended that the user be guided to set the wallet password when logging into the App for the first time.

### Status

Acknowledged

**[N4] [Suggestion] Screenshot/Screen Recording Issue****Category: Screenshot/screen recording detection****Content**

There are no safety alerts when performing screenshots/recording operations.

**Solution**

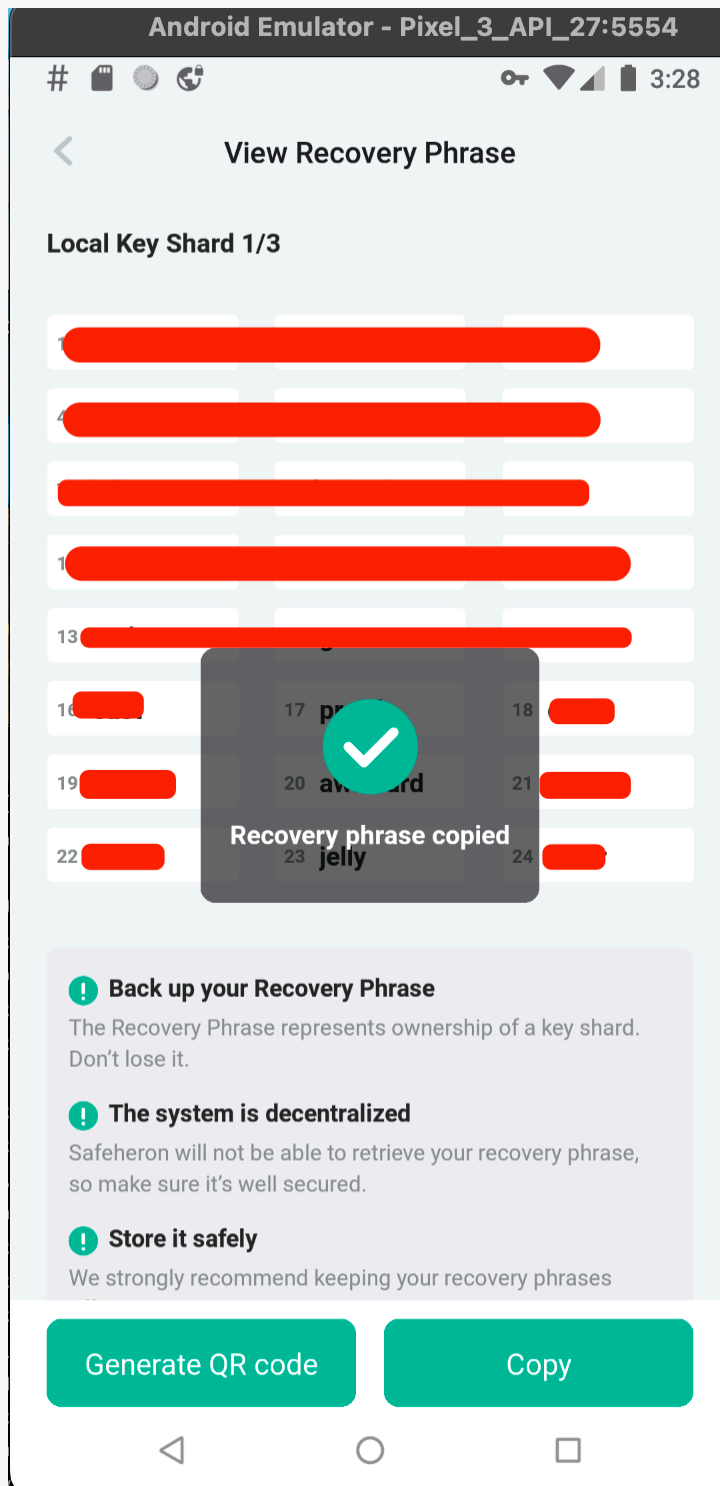
It is recommended that a reminder be popped up when the application detects screenshots/recordings.

**Status**

Acknowledged

**[N5] [Suggestion] Copy And Paste Issue****Category: Paste copy detection****Content**




There is no security prompt when copying the mnemonic.



When adding a whitelist, pasting the address into the input box does not prompt the user to double-check the address, which may pose a risk of attacks such as clipboard hijacking.



Android Emulator - Pixel\_3\_API\_27:5554

#



3:30

<
Add whitelist

Address Name

Type

☒ EVM
☐ Bitcoin
☐ Bitcoin Cash
☐ Dash

☐ TRON
☐ NEAR
☐ Filecoin
☐ Sui

☐ Aptos
☐ Solana
☐ Bitcoin Testnet

☐ TON
☐ TON Testnet


Public blockchains like Ethereum,Optimism,Arbitrum, AVAX C-Chain, BNB Smart Chain, Ploygon, ETC and other public blockchain networks or L2 that are compatible with Ethereum EVM. The addresses are common and can receive mainnet coins and tokens.

Address

Scan

Paste

Save



## Solution

It is recommended to pop up a security reminder when copying the mnemonic.

It is recommended to remind users to double-check when pasting the whitelist address.

## Status

Acknowledged

**[N6] [Suggestion] Keyboard Keystroke Cache Issue**

**Category: Keyboard keystroke cache detection****Content**

No safety keyboard found, third-party keyboard allowed. Third-party input methods collect user input, which may lead to the disclosure of passwords and mnemonics.

**Solution**

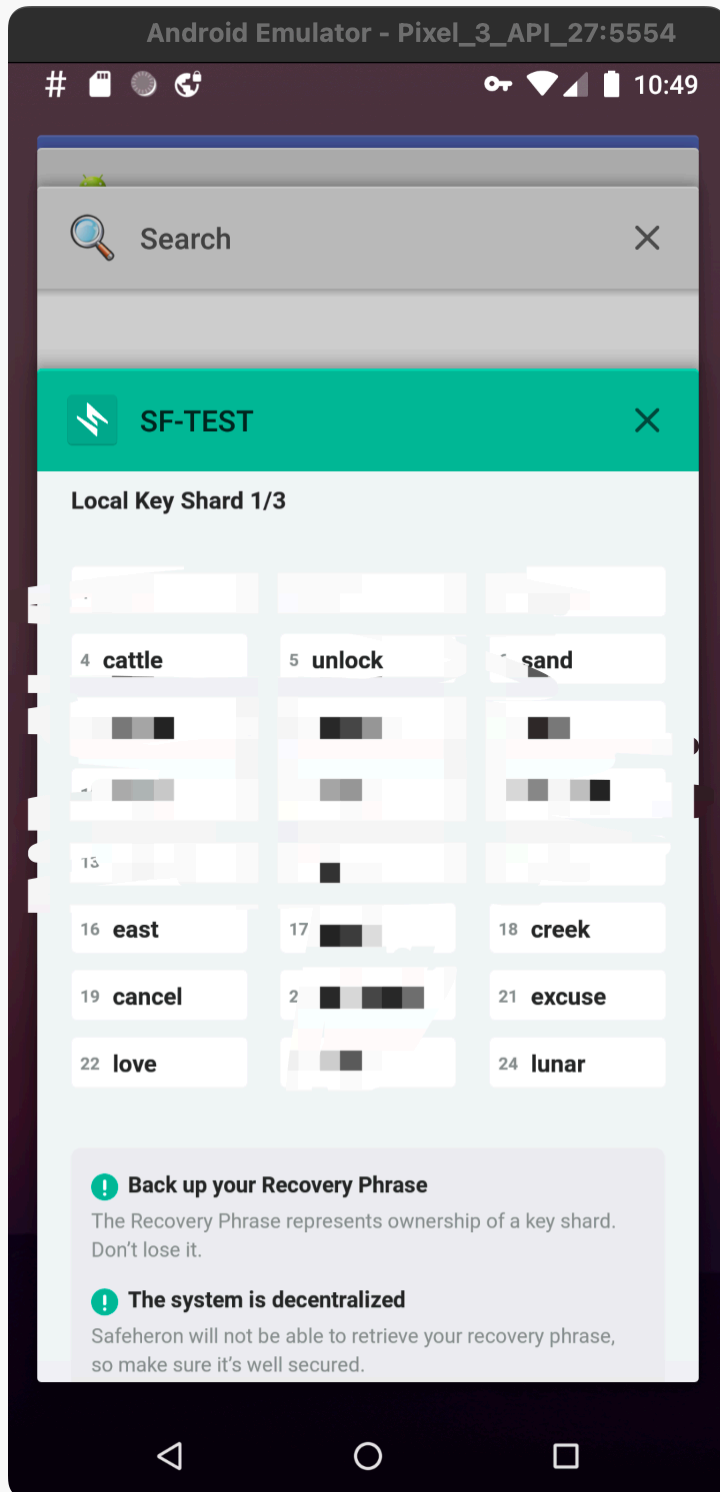
It is recommended that the App integrate a secure keyboard to shuffle the keyboard order when entering a password.

**Status**

Acknowledged

**[N7] [Suggestion] Background Obfuscation Issue****Category: Background obfuscation detection****Content**

No obfuscation was done on the background hang.



## Solution

The process of viewing private key shards, approving, and viewing mnemonics may involve some aspects of user privacy. Such as transfer address, initiator information, etc., it is recommended to fuzzy process the App background running after the App is suspended to protect private information.

## Status

Acknowledged

## [N8] [Suggestion] Suspend Evoke Security Issue

**Category:** Suspend evoke security audit

### Content

The app does not have an automatic lock feature.

### Solution

It is recommended that the wallet is automatically locked if there is no operation for a long time.

### Status

Acknowledged

## [N9] [Suggestion] User Interaction Security Issue

**Category:** User interaction security

### Content

Functionality	Support	Notes
<a href="#">WYSIWYS</a>	✓	Approving a transaction will display the complete transaction details.
AML	✓	AML strategy is 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.
Password complexity requirements	✓	The password complexity limit is supported.

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

### Solution

1. It is recommended to add a phishing page detection function.
2. It is recommended to add a transaction pre-execution function.

### Status

Acknowledged

## 4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002501210004	SlowMist Security Team	2025.01.15 - 2025.01.21	Passed

Summary conclusion: The SlowMist security team employs a manual approach along with the SlowMist team's analysis tool to conduct an audit of the project. During the audit process, we discovered nine suggestions. All the findings have been acknowledged.

## 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>