Exchange Security Audit Report

Table Of Contents

1 Executive Summary

On 2025.07.30, the SlowMist security team received the Minara team's security audit application for Minara AI, 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 lead, grey box assists" 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 application includes two steps:

- The applications are scanned/tested for commonly known and more specific vulnerabilities using automated analysis tools.
- Manual audit of the applications for security issues. The applications are 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	Deposit/Transfer security audit	Passed
2	WHOIS information collection	Passed
3	Real IP discovery	Passed
4	Subdomain detection	Passed
5	Mail service detection	Passed
6	Certificate information collection	Passed
7	Web services component fingerprint collection	Passed
8	Port service component fingerprint collection	Passed
9	Segment C service acquisition	Passed
10	Personnel structure collection	Passed
11	GitHub source code leak detection	Passed
12	Google Hack detection	Passed
13	Privacy data leak detection	Passed
14	CDN service detection	Passed
15	Network infrastructure configuration test	Passed

NO.	Audit Items	Result
16	Application platform configuration management test	Passed
17	File extension resolution test	Passed
18	Backup, unlinked file test	Passed
19	Enumerate management interface test	Passed
20	HTTP method test	Passed
21	HTTP strict transmission test	Passed
22	Web front-end cross-domain policy test	Passed
23	Web security response header test	Passed
24	Weak password and default password detection	Passed
25	Role definition test	Passed
26	User registration process test	Passed
27	Account rights change test	Passed
28	Account enumeration test	Passed
29	Weak username strategy testing	Passed
30	Password information encrypted transmission test	Passed
31	Default password test	Passed
32	Account lockout mechanism test	Passed
33	Certification bypass test	Passed
34	Password memory function test	Passed
35	Browser cache test	Passed
36	Password strategy test	Passed
37	Security quiz test	Passed

NO.	Audit Items	Result
38	Password reset test	Passed
39	OAuth authentication model test	Passed
40	Privilege escalation test	Passed
41	Authorization bypass test	Passed
42	Two-factor authentication bypass test	Passed
43	Hash robustness test	Passed
44	Session management bypass test	Passed
45	Cookies property test	Passed
46	Session fixation test	Passed
47	Session token leak test	Passed
48	Cross Site Request Forgery (CSRF) test	Passed
49	Logout function test	Passed
50	Session timeout test	Passed
51	Session token overload test	Passed
52	Cross Site Scripting (XSS) test	Passed
53	Template injection test	Passed
54	Third-party component vulnerability test	Passed
55	HTTP parameter pollution test	Passed
56	SQL injection test	Passed
57	XXE entity injection test	Passed
58	Deserialization vulnerability test	Passed
59	SSRF vulnerability test	Passed

NO.	Audit Items	Result
60	Code injection test	Passed
61	Local file contains test	Passed
62	Remote file contains test	Passed
63	Command execution injection test	Passed
64	Buffer overflow test	Passed
65	Formatted string test	Passed
66	Interface security test	Passed
67	Request forgery test	Passed
68	Integrity test	Passed
69	Overtime detection	Passed
70	Interface frequency limit test	Passed
71	Workflow bypass test	Passed
72	Application misuse protection test	Passed
73	Unexpected file type upload test	Passed
74	Malicious file upload test	Passed
75	Weak SSL/TLS encryption, insecure transport layer protection test	Passed
76	SSL pinning security deployment test	Passed
77	Non-encrypted channel transmission of sensitive data test	Passed
78	Others	Passed

3 Project Overview

3.1 Project Introduction

Audit Scope

https://minara.ai/

Code Version

https://github.com/Minara-AI/minara-core-for-audit

Commit: f31bab713289177fb2c138c375c871f0e9ca1642

Note: The project team did not provide the fixed version of the code for verification, all fixed issues were verified using the black-box method.

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Email Code Sending and Verification Use GET Requests	Interface security test	Low	Fixed
N2	Missing Human Verification	Interface frequency limit test	Low	Fixed
N3	Verification Code Can Be Brute-Forced	Interface frequency limit test	High	Fixed
N4	Missing Two-Factor Authentication	Others	Low	Fixed
N5	Manual Logout Does Not Invalidate Token Server-Side	Logout function test	Low	Fixed
N6	API Error Response Exposes Server-Side Library Details	Interface security test	Low	Fixed
N7	Missing Withdrawal Fee Information	Others	Suggestion	Fixed
N8	Fake Deposit Testing	Deposit/Transfer security audit	Low	Fixed
N9	Transaction System Error	Others	Critical	Fixed
N10	Token Display Does Not Match Actual	Others	Low	Fixed

NO	Title	Category	Level	Status
	Chain			
N11	Token Display Error in Chat Mention	Others	Low	Fixed
N12	Incomplete Transaction Information Display	Others	Suggestion	Fixed
N13	Slippage Setting Is Too High	Others	High	Fixed
N14	API Does Not Check Account Balance	Interface security test	Suggestion	Acknowledged
N15	Missing Anti-Phishing Strategy	Others	Suggestion	Acknowledged
N16	Missing AML Strategy	Others	Suggestion	Acknowledged
N17	DNSSEC Not Configured	Network infrastructure configuration test	Suggestion	Acknowledged
N18	Low TLS Versions Allowed	Network infrastructure configuration test	Suggestion	Fixed
N19	Missing X-Frame-Options Header	Web security response header test	Suggestion	Acknowledged
N20	Missing X-Content-Type-Options Header	Web security response header test	Suggestion	Acknowledged
N21	Missing Strict-Transport-Security Header	Web security response header test	Suggestion	Acknowledged
N22	Missing Content-Security-Policy Header	Web security response header test	Suggestion	Acknowledged
N23	CORS Configuration Is Insecure	Web front-end cross-domain policy test	Suggestion	Acknowledged

3.3 Vulnerability Summary

[N1] [Low] Email Code Sending and Verification Use GET Requests

Category: Interface security test

Content

Requests for sending and verifying the email code are implemented via GET, for example:

- https://api.minara.ai/auth/email/code?email=ac002@dapptest.space
- https://api.minara.ai/auth/email/verify?email=ac002@dapptest.space&code=123456

Using GET exposes the user email address and the verification code in URLs and various logs.

Solution

It is recommended to send and verify the email code via POST requests to avoid leaking sensitive data in URLs and logs.

Status

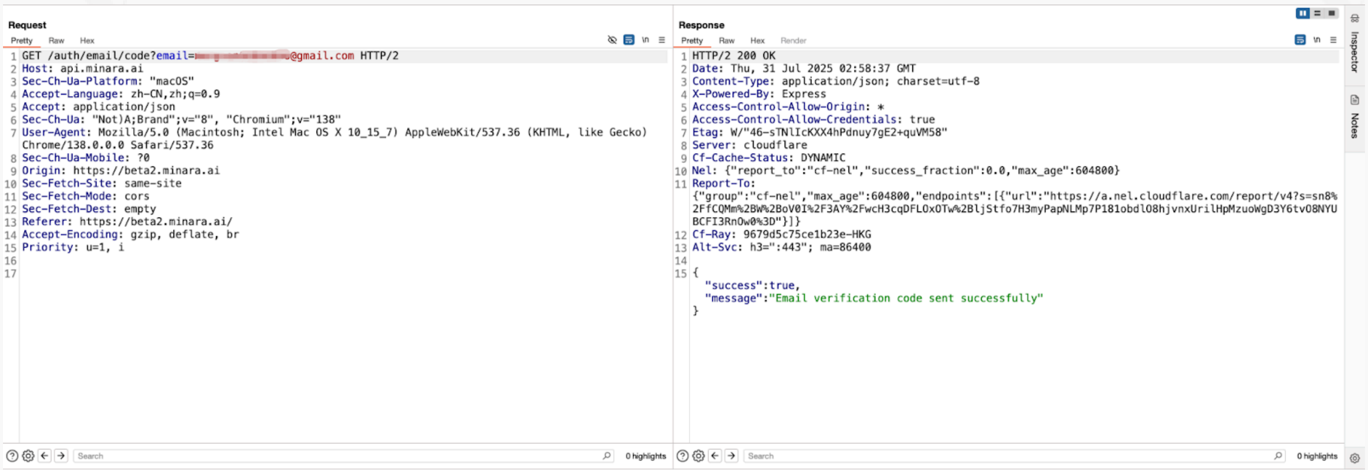
Fixed

[N2] [Low] Missing Human Verification

Category: Interface frequency limit test

Content

When logging in via email, the system needs to send a verification code to the user's email. However, the current flow for sending email codes does not include a human verification step, which allows attackers to send unlimited verification codes to target addresses, potentially causing email verification code bombing.



```
GET /auth/email/code?email=[redacted]@gmail.com HTTP/2
Host: api.minara.ai
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: zh-CN,zh;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Origin: https://beta2.minara.ai
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://beta2.minara.ai/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

```
HTTP/2 200 OK
Date: Thu, 31 Jul 2025 02:58:37 GMT
Content-Type: application/json; charset=utf-8
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Etag: W/"46-sTNlIcKXX4hPdnuy7gE2+quVM58"
Server: cloudflare
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=sn8%
2FfCQMm%2BW%2BoV0I%2F3AY%2FwcH3cqDFLOxOTw%2BljStfo7H3myPapNLMp7P181obdlO8hjvnxUrilHpMzuoWgD3Y6tvO8NYU
BCFI3RnOw0%3D"}]}
Cf-Ray: 9679d5c75ce1b23e-HKG
Alt-Svc: h3=":443"; ma=86400

{
  "success":true,
  "message":"Email verification code sent successfully"
}
```

Solution

It is recommended to add a human verification step to the verification code sending flow.

Status

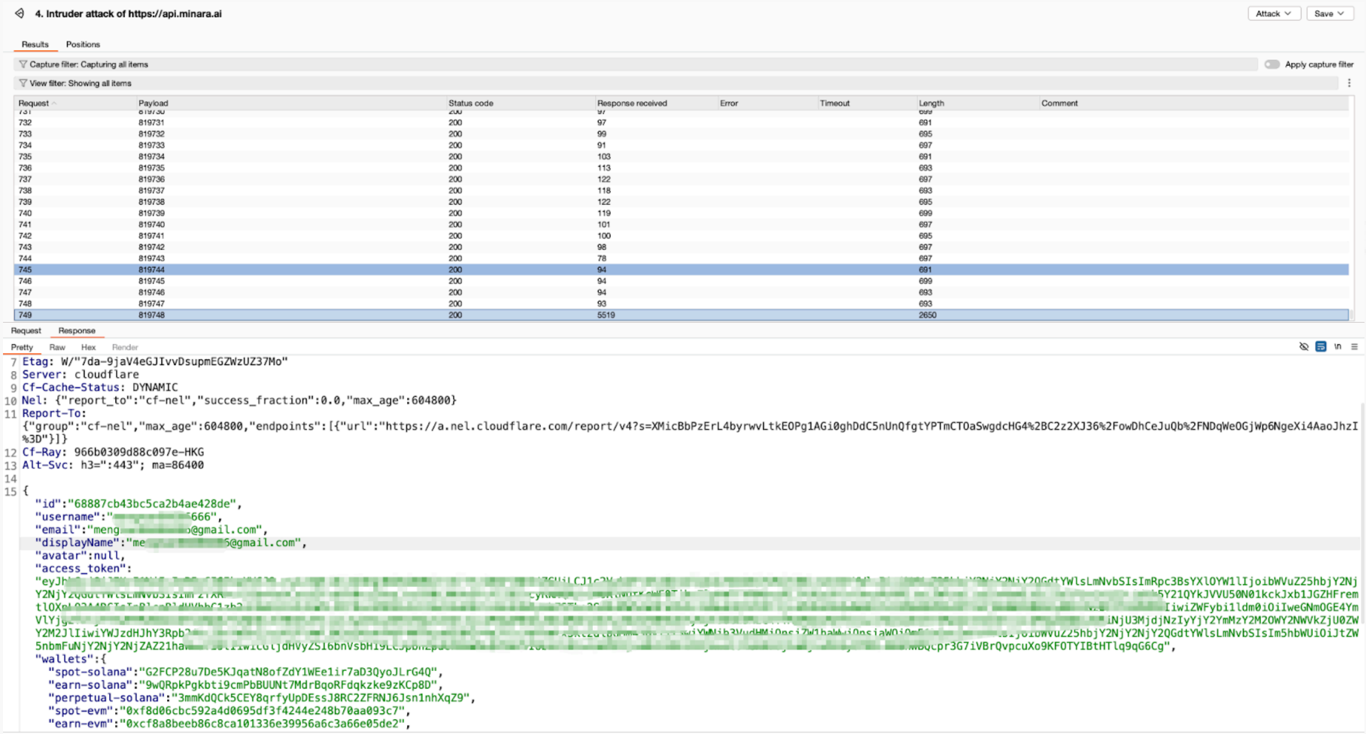
Fixed

[N3] [High] Verification Code Can Be Brute-Forced

Category: Interface frequency limit test

Content

The site relies solely on email verification codes for authentication without any form of secondary verification. The current verification flow has risks: there is no limit on failed attempts; the code is a 6-digit number; and the code expiration is set to five minutes. These conditions together allow practical brute-force attacks on login verification codes. If successful, an attacker can gain control of the victim's account.



4. Intruder attack of https://api.minara.ai

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
731	819730	200	97			699	
732	819731	200	97			691	
733	819732	200	99			695	
734	819733	200	91			697	
735	819734	200	103			691	
736	819735	200	113			693	
737	819736	200	122			697	
738	819737	200	118			693	
739	819738	200	122			695	
740	819739	200	119			699	
741	819740	200	101			697	
742	819741	200	100			695	
743	819742	200	98			697	
744	819743	200	78			697	
745	819744	200	94			691	
746	819745	200	94			699	
747	819746	200	94			693	
748	819747	200	93			693	
749	819748	200	5519			2650	

```
Etag: W/"7da-9jaV4eGJIvvDsupmEGZWzUZ37Mo"
Server: cloudflare
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=XMicBbPzErL4byrwvLtkEOPg1AGi0ghDdC5nUnQfgtYPTmCTOaSwgdcHG4%2BC2z2XJ36%2FowDhCeJuQb%2FNDqWeOGjWp6NgeXi4AaoJhzI
%3D"}]}
Cf-Ray: 966b0309d88c097e-HKG
Alt-Svc: h3=":443"; ma=86400

{
  "id":"68887cb43bc5ca2b4ae428de",
  "username":"[redacted]666",
  "email":"meng[redacted]o@gmail.com",
  "displayName":"me[redacted]5@gmail.com",
  "avatar":null,
  "access_token":
  "eyJh[redacted]YWlsLmNvbSIsImRpc3BsYXlOYW1lIjoibWVuZ25hbjY2Nj
  Y2NjY[redacted]5Y21QYkJVVU50N01kckJxb1JGZHFrem
  tlOX[redacted]IiwiZWFybi1ldm0iOiIweGNmOGE4Ym
  VlYj[redacted]iNjU3MjdjNzIyYjY2YmMzY2M2OWY2NWVkZjU0ZW
  Y2M2JlIiwiYWJzdHJhY3Rpb[redacted]bWVuZ25hbjY2NjY2NjY2QGdtYWlsLmNvbSIsIm5hbWUiOiJtZW
  5nbmFuNjY2NjY2NjZAZ21ha[redacted]cpr3G7iVBrQvpcuXo9KFOTYIBtHTlq9qG6Cg",
  "wallets":{
    "spot-solana":"G2FCP28u7De5KJqatN8ofZdY1WEe1ir7aD3QyoJLrG4Q",
    "earn-solana":"9wQRpkPgkbti9cmPbBUUNt7MdrBqoRFdqkzke9zKCp8D",
    "perpetual-solana":"3mmKdQCk5CEY8qrfyUpDEssJ8RC2ZFRNJ6Jsn1nhXqZ9",
    "spot-evm":"0xf8d06cbc592a4d0695df3f4244e248b70aa093c7",
    "earn-evm":"0xcf8a8beeb86c8ca101336e39956a6c3a66e05de2",
```

Relevant code excerpts:

1.Verification code complexity and expiry settings

Code location: xneuro-core-for-audit/src/auth/auth.service.ts #L287-288

```
const code = Math.floor(100000 + Math.random() * 900000).toString();
await this.redisService.set(this.emailPrefix + email, code, 60 * 5);
```

2.Verification code validation logic

Code location: xneuro-core-for-audit/src/auth/auth.service.ts #L302-317

```
async verifyEmailCode(email: string, code: string, userId?: string) {
  const storedCode = await this.redisService.get(this.emailPrefix + email);
  if (storedCode !== code) {
    return {
      statusCode: HttpStatus.BAD_REQUEST,
      message: 'Invalid verification code',
    };
  }

  await this.redisService.del(this.emailPrefix + email);
  return this.handleThirdPartyAuth(userId, 'email', {
    email: email,
    name: email,
  });
}
```

Solution

1. It is recommended to enforce limits on consecutive verification failures and temporarily lock after repeated failures.
2. It is recommended to shorten the verification code validity period to 2–3 minutes.
3. It is recommended to increase verification code complexity (e.g., alphanumeric combinations).

Status

Fixed

[N4] [Low] Missing Two-Factor Authentication

Category: Others

Content

- Login security is low: login relies solely on email codes without password, SMS OTP, or authenticator-based second factors. Compromise of email or interception of the code allows direct account access.
- Sensitive operations (e.g., trading and withdrawals) lack a dedicated verification step (e.g., transaction password or 2FA). If the account is compromised, an attacker can directly transfer funds.

Solution

It is recommended to guide users to enable 2FA after the first login, and to require 2FA for login and sensitive actions such as trading and withdrawals to protect user assets.

Status

Fixed

[N5] [Low] Manual Logout Does Not Invalidate Token Server-Side

Category: Logout function test

Content

The platform allows multi-terminal logins; a user can obtain multiple JWTs. When clicking “Log Out,” only frontend storage is cleared, and no logout request is sent to the server. The current JWT remains valid until it expires and cannot be proactively invalidated server-side.

Solution

It is recommended to send a server-side logout request on “Log Out,” and mark the current JWT as invalid on the server.

Status

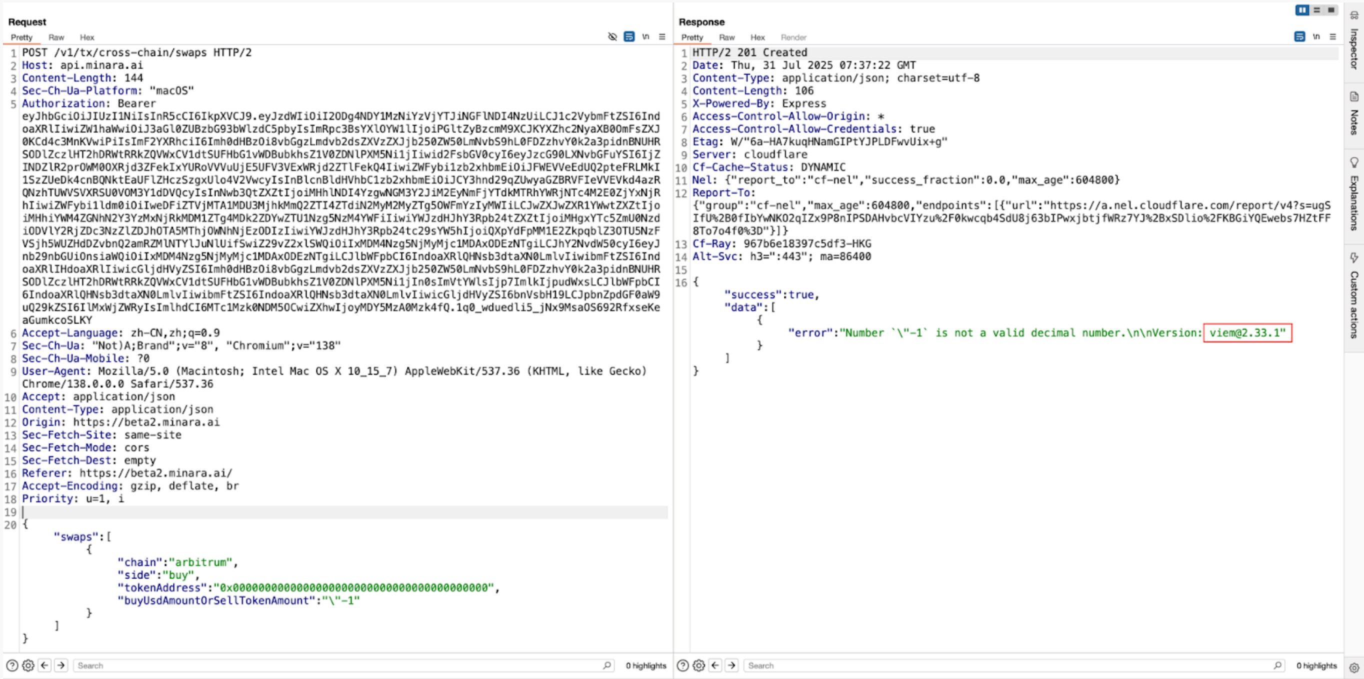
Fixed

[N6] [Low] API Error Response Exposes Server-Side Library Details

Category: Interface security test

Content

Server error responses disclose the names and versions of backend libraries. For example, the transaction API’s error reveals the use of the TypeScript library “viem,” version 2.33.1.



```
POST /v1/tx/cross-chain/swaps HTTP/2
Host: api.minara.ai
Content-Length: 144
Sec-Ch-Ua-Platform: "macOS"
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI2ODg4NDY1MzNiYzVjYTJiNGFlNDI4NzUiLCJ1c2VybmFtZSI6Ind
oaXRlIiwiZW1haWwiOiJ3aGl0ZUBzbG93bWlzdC5pbyIsImRpc3BsYXlOYW1lIjoiPGltZyBzcmM9XCJKYXZhc2NyaXB0OmFsZXJ
0KCd4c3MnKVwiPiIsImF2YXRhciI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0k2a3pidnBNUHR
SODlZczlHT2hDRWtRRkZQVWxCV1dtSUFHbG1vWDBubkhsZ1V0ZDNlPXM5Ni1jIiwid2FsbGV0cyI6eyJzcG90LXNvbGFuYSI6IjZ
INDZlR2prOWM0OXRjd3ZFekIxYURoVVVuUjE5UFV3VExWRjd2ZTlFekQ4IiwiZWFybi1zb2xhbmEiOiJFWEVVeEdUQ2pteFRLMkI
1SzZUeDk4cnBQNktEaUFlZHczSzgxUlo4V2VwcyIsInBlcnBldHVhbC1zb2xhbmEiOiJCY3hnd29qZUwyaGZBRVFIeVVEVkd4azR
QNzhTUWVSVXRSU0VOM3Y1dDVQcyIsInNwb3QtZXZtIjoiMHhlNDI4YzgwNGM3Y2JiM2EyNmFjYTdkMTRhYWRjNTc4M2E0ZjYxNjR
hIiwiZWFybi1ldm0iOiIweDFiZTVjMTA1MDU3MjhkMmQ2ZTI4ZTdiN2MyM2MyZTg5OWFmYzIyMWIiLCJwZXJwZXR1YWwtZXZtIjo
iMHhiYWM4ZGNhN2Y3YzMxNjRkMDM1ZTg4MDk2ZDYwZTU1Nzg5NzM4YWFiIiwiYWJzdHJhY3Rpb24tZXZtIjoiMHgxYTc5ZmU0Nzd
iODVlY2RjZDc3NzZlZDJhOTA5MThjOWNhNjEzODIzIiwiYWJzdHJhY3Rpb24tc29sYW5hIjoiQXpYdFpMM1E2ZkpqblZ3OTU5NzF
VSjh5WUZHdDZvbnQ2amRZMlNTYlJuNlUifSwiZ29vZ2xlSWQiOiIxMDM4Nzg5NjMyMjc1MDAxODEzNTgiLCJhY2NvdW50cyI6eyJ
nb29nbGUiOnsiaWQiOiIxMDM4Nzg5NjMyMjc1MDAxODEzNTgiLCJlbWFpbCI6IndoaXRlQHNsb3dtaXN0LmlvIiwibmFtZSI6Ind
oaXRlIHdoaXRlIiwicGljdHVyZSI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0k2a3pidnBNUHR
SODlZczlHT2hDRWtRRkZQVWxCV1dtSUFHbG1vWDBubkhsZ1V0ZDNlPXM5Ni1jIn0sImVtYWlsIjp7ImlkIjpudWxsLCJlbWFpbCI
6IndoaXRlQHNsb3dtaXN0LmlvIiwibmFtZSI6IndoaXRlQHNsb3dtaXN0LmlvIiwicGljdHVyZSI6bnVsbH19LCJpbnZpdGF0aW9
uQ29kZSI6IlMxWjZWRyIsImlhdCI6MTc1Mzk0NDM5OCwiZXhwIjoyMDY5MzA0Mzk4fQ.1q0_wduedli5_jNx9MsaOS692RfxseKe
aGumkcoSLKY
Accept-Language: zh-CN,zh;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Accept: application/json
Content-Type: application/json
Origin: https://beta2.minara.ai
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://beta2.minara.ai/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "swaps":[
        {
            "chain":"arbitrum",
            "side":"buy",
            "tokenAddress":"0x0000000000000000000000000000000000000000",
            "buyUsdAmountOrSellTokenAmount":"\"-1"
        }
    ]
}
```

```
HTTP/2 201 Created
Date: Thu, 31 Jul 2025 07:37:22 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 106
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Etag: W/"6a-HA7kuqHNamGIPtYJPLDFwvUix+g"
Server: cloudflare
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=ugS
IfU%2B0fIbYwNKO2qIZx9P8nIPSDAHvbcVIYzu%2F0kwcqb4SdU8j63bIPwxjbtjfWRz7YJ%2BxSDlio%2FKBGiYQEwebs7HZtFF
8To7o4f0%3D"}]}
Cf-Ray: 967b6e18397c5df3-HKG
Alt-Svc: h3=":443"; ma=86400

{
    "success":true,
    "data":[
        {
            "error":"Number `\"-1` is not a valid decimal number.\n\nVersion: viem@2.33.1"
        }
    ]
}
```

Solution

It is recommended to standardize server error responses and avoid disclosing framework or library details.

Status

Fixed

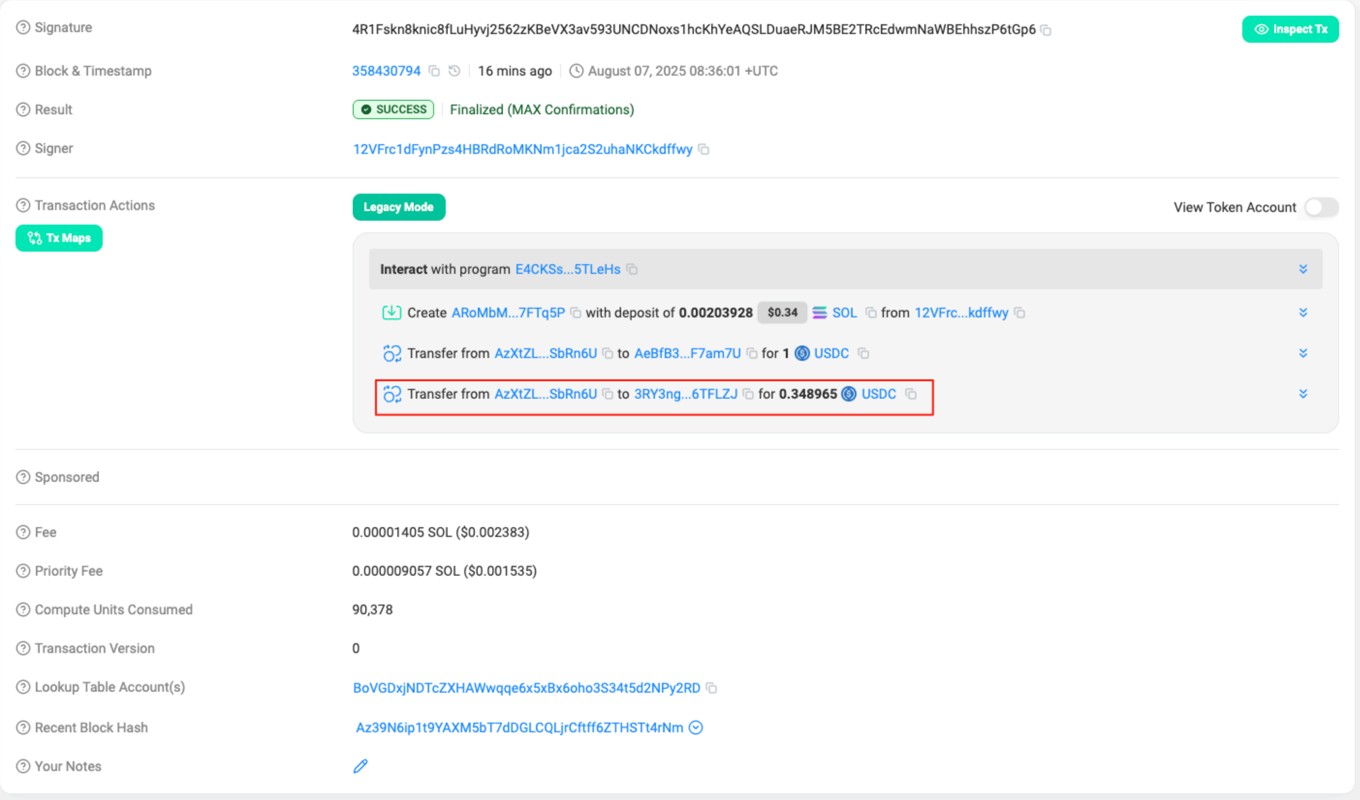
[N7] [Suggestion] Missing Withdrawal Fee Information

Category: Others

Content

The system does not inform users that a fee will be charged for withdrawals.

Reviewing transaction details shows that a fee is deducted.



Signature	4R1Fskn8knic8fLuHyvj2562zKBeVX3av593UNCDNoxs1hcKhYeAQSLDuaeRJM5BE2TRcEdwmNaWBEhhszP6tGp6
Block & Timestamp	358430794 | 16 mins ago | August 07, 2025 08:36:01 +UTC
Result	SUCCESS | Finalized (MAX Confirmations)
Signer	12VFrc1dFynPzs4HBRdRoMKNm1jca2S2uhaNKCkdffwy
Transaction Actions	Legacy Mode **Interact** with program E4CKSs...5TLeHs Create ARoMbM...7FTq5P with deposit of **0.00203928** $0.34 SOL from 12VFrc...kdffwy Transfer from AzXtZL...SbRn6U to AeBfB3...F7am7U for **1** USDC Transfer from AzXtZL...SbRn6U to 3RY3ng...6TFLZJ for **0.348965** USDC
Sponsored	
Fee	0.00001405 SOL ($0.002383)
Priority Fee	0.000009057 SOL ($0.001535)
Compute Units Consumed	90,378
Transaction Version	0
Lookup Table Account(s)	BoVGDxjNDTcZXHAWwqqe6x5xBx6oho3S34t5d2NPy2RD
Recent Block Hash	Az39N6ip1t9YAXM5bT7dDGLCQLjrCftff6ZTHSTt4rNm
Your Notes	

Solution

It is recommended to clearly display the exact withdrawal fee amount in the withdrawal dialog.

Status

Fixed

[N8] [Low] Fake Deposit Testing

Category: Deposit/Transfer security audit

Content

Test transactions were conducted as follows:

- Chain: Ethereum | Coin: ETH

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://etherscan.io/tx/0xe35f5e076f9379e62ac764b33e2a3afae576b50b7a09e98ece2948314ba49551

  TX Hash (USDC):

  https://etherscan.io/tx/0xfe0291b083ef6f7000de945820b8cab24b0f85d5c7e2eee227a652921e86ba5d

- Chain: BNB Chain | Coin: BNB

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://bscscan.com/tx/0xa8547c81d189ff4b48b7d1fe8ab87722b11fa9c7962e3d3cb7fd48128058df37

  TX Hash (USDC):

  https://bscscan.com/tx/0x767f73bad21cc0776081c926810a20e0338a81eae0307d3f0bcefc0bd8cf70cc

- Chain: Polygon | Coin: POL

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://polygonscan.com/tx/0xebdf0a5b62497ea87f8b21691fa8e263184eb752bf65f3fe8570b04e34f5994c

  TX Hash (USDC):

  https://polygonscan.com/tx/0x80acae0e1d0ab5b8a3b2eeedd202e1d0cb00f64885688f456a91db2b54d86938

- Chain: Arbitrum One | Coin: ARB_ETH

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://arbiscan.io/tx/0x3f97e14aadc03b2c68b746e1d375936fa6a6c26e67cf1e3bb221854c17a6dc16

  TX Hash (USDC):

  https://arbiscan.io/tx/0x1320f46c2c8ed121de3e2df65ed9e53116e5eec41d41a90d020957e54a1ac0ee

- Chain: Optimism | Coin: OP_ETH

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://optimistic.etherscan.io/tx/0x9184258e19a5b4892078fa87fbbcec305ba12aa7b072a4a4945fa43750b75b07

  TX Hash (USDC):

  https://optimistic.etherscan.io/tx/0xe9e43f4e69dcaae0bad5f13f9ccc40027495a138a847cc26bdad79c5a9a3f34d

- Chain: Avalanche C-Chain | Coin: AVAX

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://snowtrace.io/tx/0xfdceeafd809ed603a5e6dfbc03d50aa249cb5c11cd8bd2aed6a7abc03edd57e0

  TX Hash (USDC):

  https://snowtrace.io/tx/0x58cec53a90ee1f1534b04570ecc52277457e5812fd8b63a78915f6dbc8a32400

- Chain: Fantom | Coin: FTM

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://explorer.fantom.network/tx/0x8059aecce712d33c17eea524ef0aea16f4df979ebfa6fa939ace272f3ecca5c2

- Chain: zkSync Era | Coin: ERA_ETH

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://explorer.zksync.io/tx/0xe8b953900b9f25f3d576ed597d5a1f8db06b72be99f33f9ab1ce98eb00ee3a7a

  TX Hash (USDC):

  https://explorer.zksync.io/tx/0x3900139126365ba1b09eead0dc3203feb3ffe838e01bcbcecb21aa990338d9c3

- Chain: Base | Coin: BASE_ETH

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://basescan.org/tx/0x13e65a41014c4915178d0805eb469814d3db3fad570d6e1778fdeebd5cf0c09d

  TX Hash (USDC):

  https://basescan.org/tx/0xb7073ecf190afbd934b5be41d317b823a81bda09d0867009c3b8181bb036864c

- Chain: Linea | Coin: LINEA_ETH

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://lineascan.build/tx/0xe7049f049227e20fd30ef73231ce1d8a9733b2e8bbb6e7f5244923659a33f34f

  TX Hash (USDC):

  https://lineascan.build/tx/0xdc600daf23f2838a144c1ae88ad60437acc32a7fe68127ebf2f7c4dbafe7ac11

- Chain: Ethereum Classic | Coin: ETC

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://etc.blockscout.com/tx/0x2505be1873821d8699cdf6486aaba26dabd2a0c13195699e53c0bfe6e9b5cd4d

- Chain: Sei | Coin: SEI

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://seistream.app/transactions/0x6424ca870b26d2e84e6c3ead6e0dba75862c259c4353938aab2ae117f5e5c695

- Chain: Kaia | Coin: KAIA

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://kaiascan.io/tx/0x071d217c2f1efa6214a85375db92e0e000a61498e84fb7e88536fad8db8c298c

- Chain: Cronos | Coin: CRO

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

  TX Hash (NativeToken):

  https://cronoscan.com/tx/0xd097ee9d04a13ddf8ca1570207f98aec7379d87a9e31553d7d1408f8c5f9c10f

- Chain: Flare | Coin: FLR

  Deposit Address: 0x1a79fe477b85ecdcd7776ed2a90918c9ca613823

TX Hash (NativeToken): https://flare-explorer.flare.network/tx/0xcc83382f25056a84ee6ec1d841edb85e81fff724d8d2eb568e95f5868aa26e57

- Chain: Solana | Coin: SOL

  Deposit Address: AzXtZL3Q6fJjnVw95971UJ8yYFGt6ont6jdY2SSbRn6U

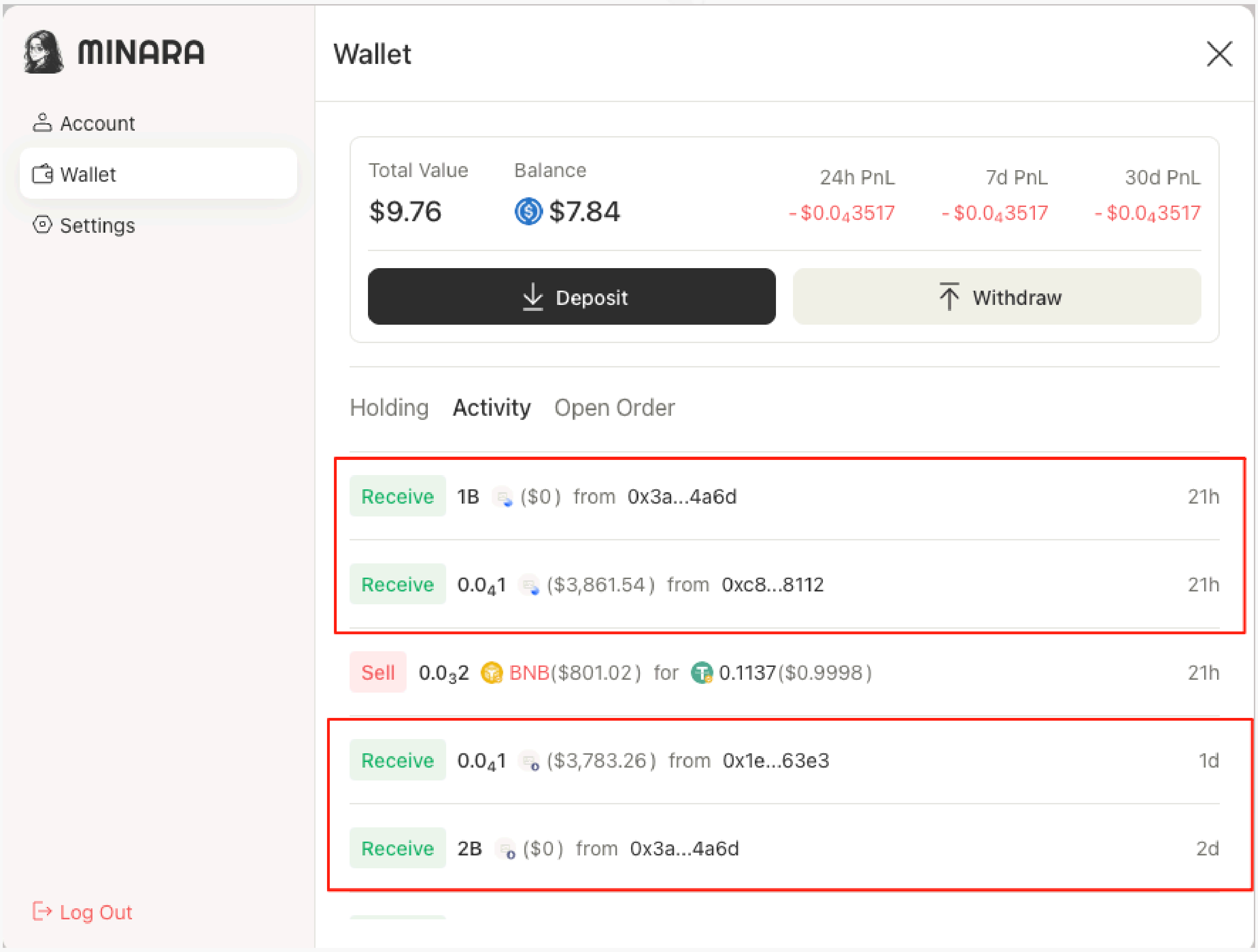
  TX Hash (NativeToken):

  https://solscan.io/tx/2uQJGjeJFcbu5sAjJFr6scc2hqetybUkfqD7CCG9Yd4SjGe5zS7xT5KLQesb3MRizCmp1BXzNDZHupza119RYQeF

  TX Hash (USDC):

  https://solscan.io/tx/2Fpd6x9d8FgP3ufvtDtnPfpKCVdJDZseGyST3Zy1XH7FKYhs9N5MUVg1U2TZBosCeUkqMDbt79JvyBQh5pZYf7et

After inspecting deposit records, on EVM chains both tokens and native coins appear in Activity, while only actual native coin deposits reflect value; some tokens appear as “fake deposits” without value. Native coin deposits show corresponding value correctly.



Total Value	Balance	24h PnL	7d PnL	30d PnL
$9.76	$7.84	- $\$0.0_{4}3517$	- $\$0.0_{4}3517$	- $\$0.0_{4}3517$

Receive 1B ($0) from 0x3a...4a6d 21h

Receive $0.0_{4}1$ ($3,861.54) from 0xc8...8112 21h

Sell $0.0_{3}2$ BNB($801.02) for 0.1137($0.9998) 21h

Receive $0.0_{4}1$ ($3,783.26) from 0x1e...63e3 1d

Receive 2B ($0) from 0x3a...4a6d 2d

Solution

1. It is recommended to whitelist legitimate token contract addresses and hide deposits for tokens outside the whitelist.
2. It is recommended to verify whether native coin deposits are actually credited, and only show successful credits in records.
3. It is recommended to display transaction hashes in wallet activity records so users can inspect details.

Status

Fixed

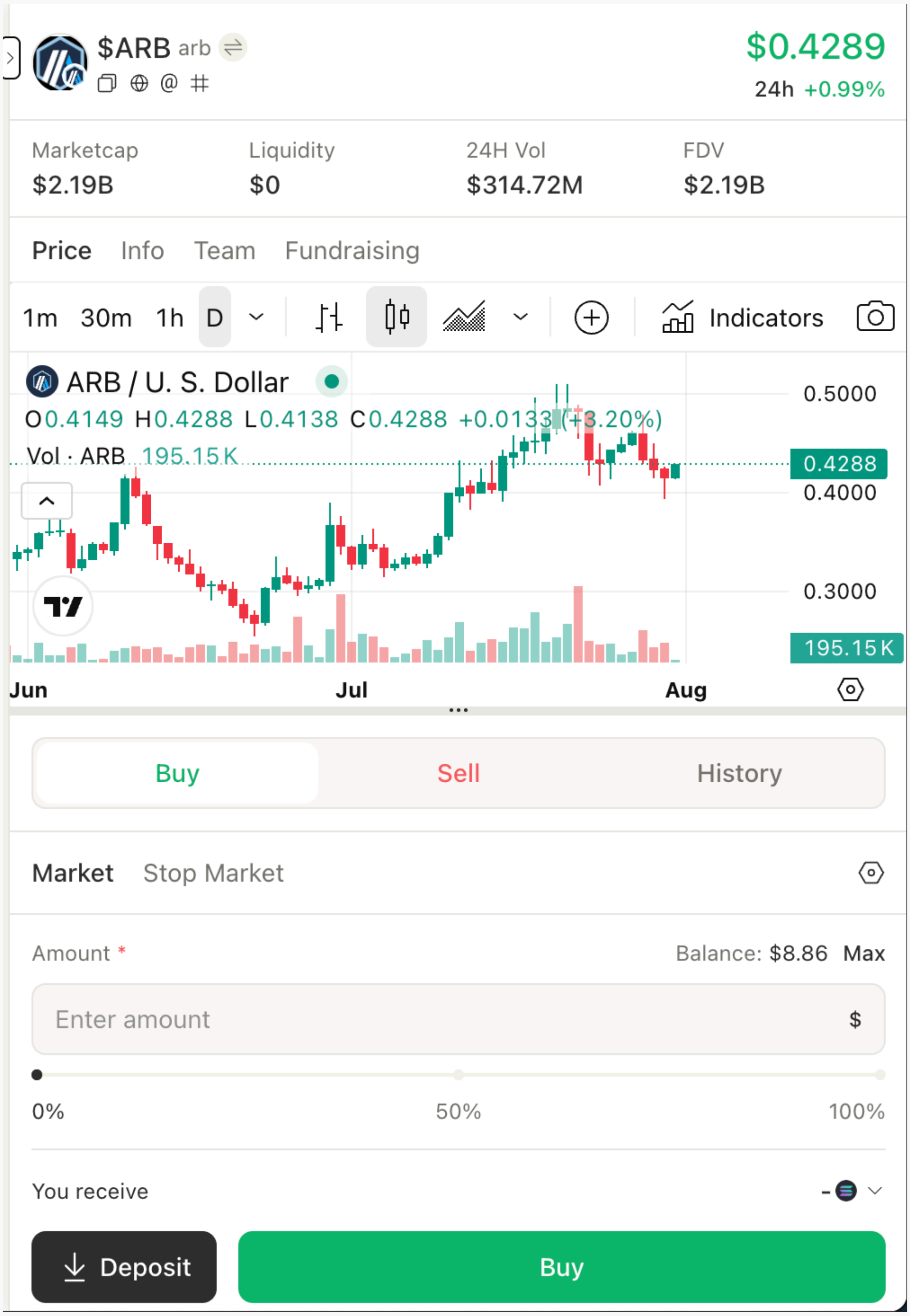
[N9] [Critical] Transaction System Error

Category: Others

Content

After completing a token purchase through the AI-recommended dialog, the purchased asset does not match the asset displayed in the dialog.

AI presented an ARB purchase quote on Arbitrum:



$ARB arb

$0.4289

24h +0.99%

Marketcap $2.19B

Liquidity $0

24H Vol $314.72M

FDV $2.19B

ARB / U. S. Dollar

O0.4149 H0.4288 L0.4138 C0.4288 +0.0133 (+3.20%)

Vol · ARB 195.15K

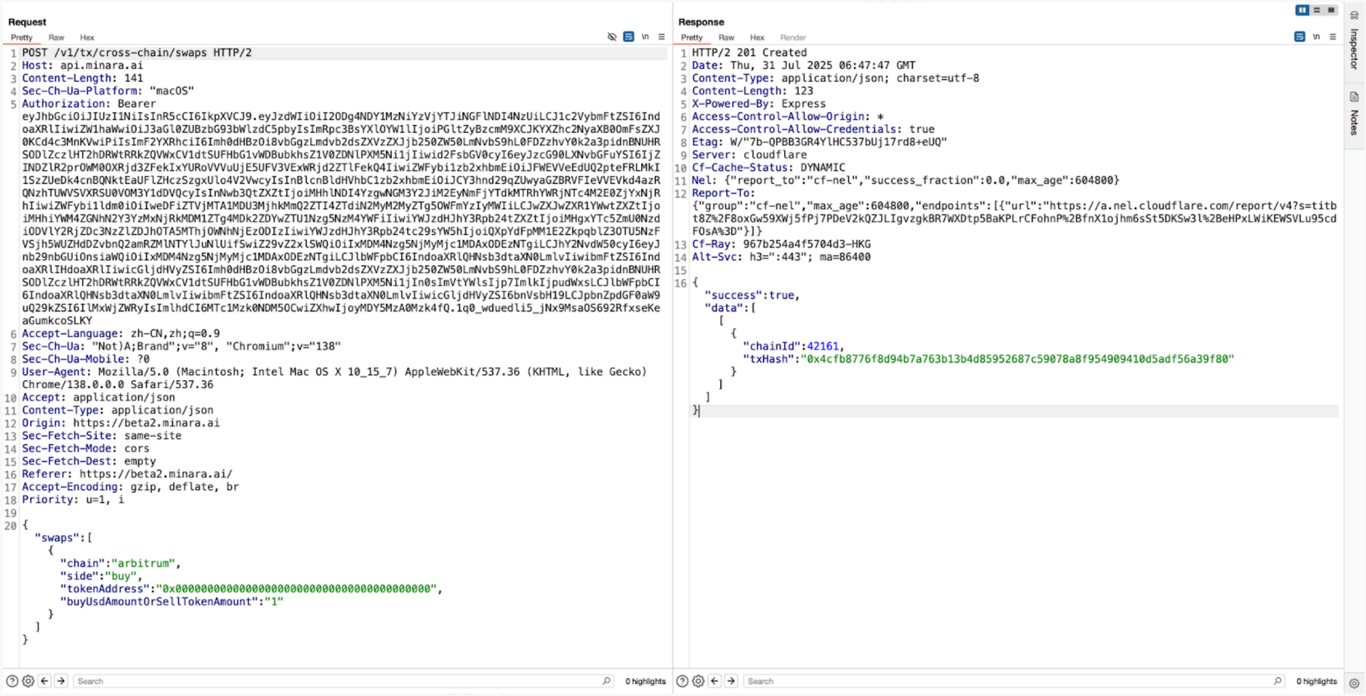
Amount *

Balance: $8.86 Max

Enter amount $

You receive -

After clicking Buy and issuing the swap request, the returned transaction hash shows the purchased asset is not ARB:



Request

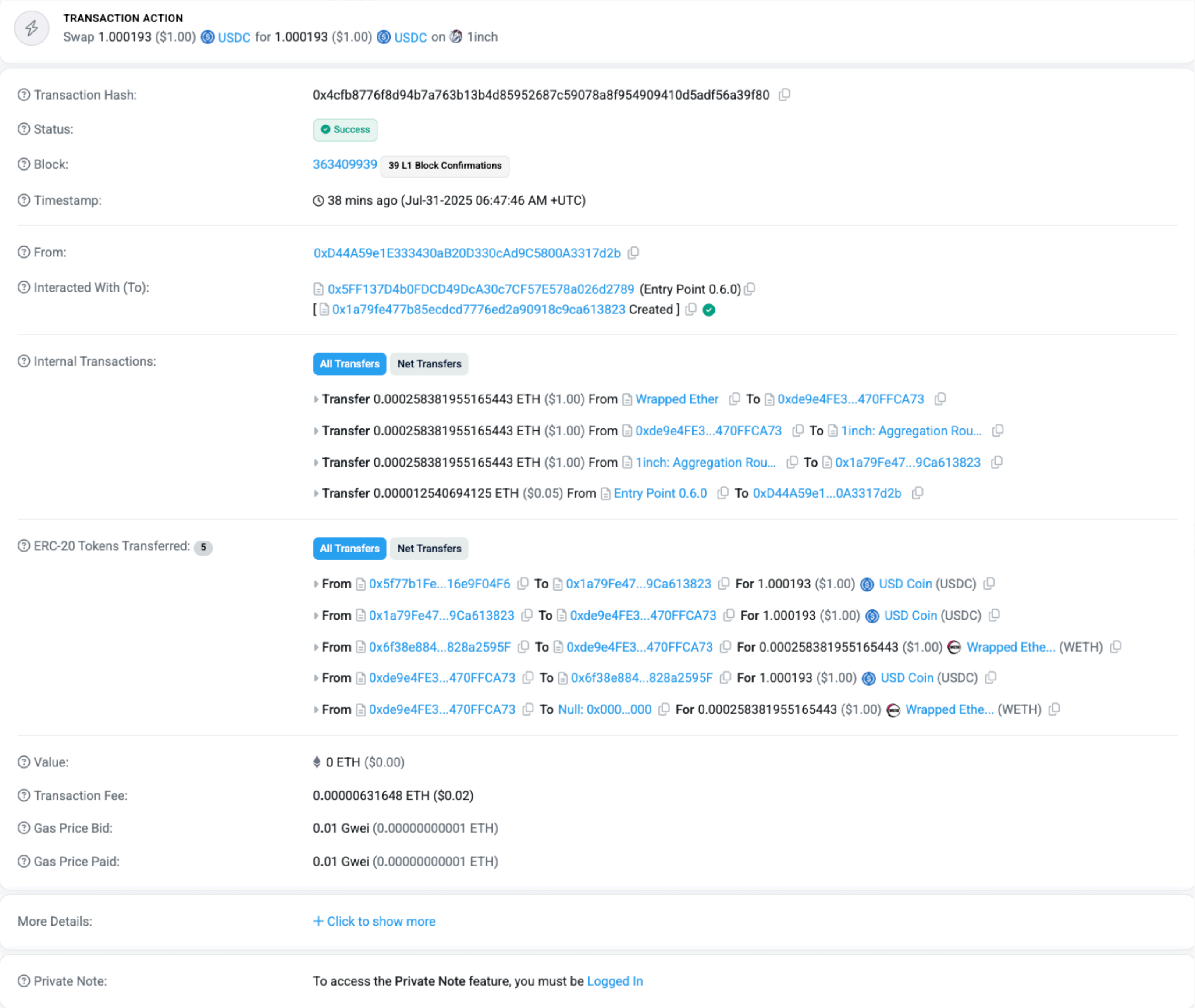
```
POST /v1/tx/cross-chain/swaps HTTP/2
Host: api.minara.ai
Content-Length: 141
Sec-Ch-Ua-Platform: "macOS"
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI2ODg4NDY1MzNiYzVjYTJiNGFlNDI4NzUiLCJ1c2VybmFtZSI6Ind
oaXRlIiwiZW1haWwiOiJ3aGl0ZUBzbG93bWlzdC5pbyIsImRpc3BsYXlOYW1lIjoiPGltZyBzcmM9XCJKYXZhc2NyaXB0OmFsZXJ
0KCd4c3MnKVwiPiIsImF2YXRhciI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0k2a3pidnBNUHR
SODlZczlHT2hDRWtRRkZQVWxCV1dtSUFHbG1vWDBubkhsZ1V0ZDNlPXM5Ni1jIiwid2FsbGV0cyI6eyJzcG90LXNvbGFuYSI6IjZ
INDZlR2prOWM0OXRjd3ZFekIxYURoVVVuUjE5UFV3VExWRjd2ZTlFekQ4IiwiZWFybi1zb2xhbmEiOiJFWEVVeEdUQ2pteFRLMkI
1SzZUeDk4cnBQNktEaUFlZHczSzgxUlo4V2VwcyIsInBlcnBldHVhbC1zb2xhbmEiOiJCY3hnd29qZUwyaGZBRVFIeVVEVkd4azR
QNzhTUWVSVXRSU0VOM3Y1dDVQcyIsInNwb3QtZXZtIjoiMHhlNDI4YzgwNGM3Y2JiM2EyNmFjYTdkMTRhYWRjNTc4M2E0ZjYxNjR
hIiwiZWFybi1ldm0iOiIweDFiZTVjMTA1MDU3MjhkMmQ2ZTI4ZTdiN2MyM2MyZTg5OWFmYzIyMWIiLCJwZXJwZXR1YWwtZXZtIjo
iMHhiYWM4ZGNhN2Y3YzMxNjRkMDM1ZTg4MDk2ZDYwZTU1Nzg5NzM4YWFiIiwiYWJzdHJhY3Rpb24tZXZtIjoiMHgxYTc5ZmU0Nzd
iODVlY2RjZDc3NzZlZDJhOTA5MThjOWNhNjEzODIzIiwiYWJzdHJhY3Rpb24tc29sYW5hIjoiQXpYdFpMM1E2ZkpqblZ3OTU5NzF
VSjh5WUZHdDZvbnQ2amRZMlNTYlJuNlUifSwiZ29vZ2xlSWQiOiIxMDM4Nzg5NjMyMjc1MDAxODEzNTgiLCJhY2NvdW50cyI6eyJ
nb29nbGUiOnsiaWQiOiIxMDM4Nzg5NjMyMjc1MDAxODEzNTgiLCJlbWFpbCI6IndoaXRlQHNsb3dtaXN0LmlvIiwibmFtZSI6Ind
oaXRlIHdoaXRlIiwicGljdHVyZSI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0k2a3pidnBNUHR
SODlZczlHT2hDRWtRRkZQVWxCV1dtSUFHbG1vWDBubkhsZ1V0ZDNlPXM5Ni1jIn0sImVtYWlsIjp7ImlkIjpudWxsLCJlbWFpbCI
6IndoaXRlQHNsb3dtaXN0LmlvIiwibmFtZSI6IndoaXRlQHNsb3dtaXN0LmlvIiwicGljdHVyZSI6bnVsbH19LCJpbnZpdGF0aW9
uQ29kZSI6IlMxWjZWRyIsImlhdCI6MTc1Mzk0NDM5OCwiZXhwIjoyMDY5MzA0Mzk4fQ.1q0_wduedli5_jNx9MsaOS692RfxseKe
aGumkcoSLKY
Accept-Language: zh-CN,zh;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Accept: application/json
Content-Type: application/json
Origin: https://beta2.minara.ai
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://beta2.minara.ai/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
  "swaps":[
    {
      "chain":"arbitrum",
      "side":"buy",
      "tokenAddress":"0x0000000000000000000000000000000000000000",
      "buyUsdAmountOrSellTokenAmount":"1"
    }
  ]
}
```

Response

```
HTTP/2 201 Created
Date: Thu, 31 Jul 2025 06:47:47 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 123
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Etag: W/"7b-QPBB3GR4YlHC537bUj17rd8+eUQ"
Server: cloudflare
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=titb
t8Z%2F8oxGw59XWj5fPj7PDeV2kQZJLIgvzgkBR7WXDtp5BaKPLrCFohnP%2BfnX1ojhm6sSt5DKSw3l%2BeHPxLWiKEWSVLu95cd
FOsA%3D"}]}
Cf-Ray: 967b254a4f5704d3-HKG
Alt-Svc: h3=":443"; ma=86400

{
  "success":true,
  "data":[
    [
      {
        "chainId":42161,
        "txHash":"0x4cfb8776f8d94b7a763b13b4d85952687c59078a8f954909410d5adf56a39f80"
      }
    ]
  ]
}
```



TRANSACTION ACTION

Swap 1.000193 ($1.00) USDC for 1.000193 ($1.00) USDC on 1inch

Transaction Hash:	0x4cfb8776f8d94b7a763b13b4d85952687c59078a8f954909410d5adf56a39f80
Status:	✓ Success
Block:	363409939 39 L1 Block Confirmations
Timestamp:	38 mins ago (Jul-31-2025 06:47:46 AM +UTC)
From:	0xD44A59e1E333430aB20D330cAd9C5800A3317d2b
Interacted With (To):	0x5FF137D4b0FDCD49DcA30c7CF57E578a026d2789 (Entry Point 0.6.0) [0x1a79fe477b85ecdcd7776ed2a90918c9ca613823 Created] ✓
Internal Transactions:	Transfer 0.000258381955165443 ETH ($1.00) From Wrapped Ether To 0xde9e4FE3...470FFCA73 Transfer 0.000258381955165443 ETH ($1.00) From 0xde9e4FE3...470FFCA73 To 1inch: Aggregation Rou... Transfer 0.000258381955165443 ETH ($1.00) From 1inch: Aggregation Rou... To 0x1a79Fe47...9Ca613823 Transfer 0.000012540694125 ETH ($0.05) From Entry Point 0.6.0 To 0xD44A59e1...0A3317d2b
ERC-20 Tokens Transferred: 5	From 0x5f77b1Fe...16e9F04F6 To 0x1a79Fe47...9Ca613823 For 1.000193 ($1.00) USD Coin (USDC) From 0x1a79Fe47...9Ca613823 To 0xde9e4FE3...470FFCA73 For 1.000193 ($1.00) USD Coin (USDC) From 0x6f38e884...828a2595F To 0xde9e4FE3...470FFCA73 For 0.000258381955165443 ($1.00) Wrapped Ethe... (WETH) From 0xde9e4FE3...470FFCA73 To 0x6f38e884...828a2595F For 1.000193 ($1.00) USD Coin (USDC) From 0xde9e4FE3...470FFCA73 To Null: 0x000...000 For 0.000258381955165443 ($1.00) Wrapped Ethe... (WETH)
Value:	0 ETH ($0.00)
Transaction Fee:	0.00000631648 ETH ($0.02)
Gas Price Bid:	0.01 Gwei (0.00000000001 ETH)
Gas Price Paid:	0.01 Gwei (0.00000000001 ETH)
More Details:	+ Click to show more
Private Note:	To access the **Private Note** feature, you must be Logged In

Solution

It is recommended to investigate and fix the root cause to ensure the actual purchased token always matches what is displayed to the user.

Status

Fixed

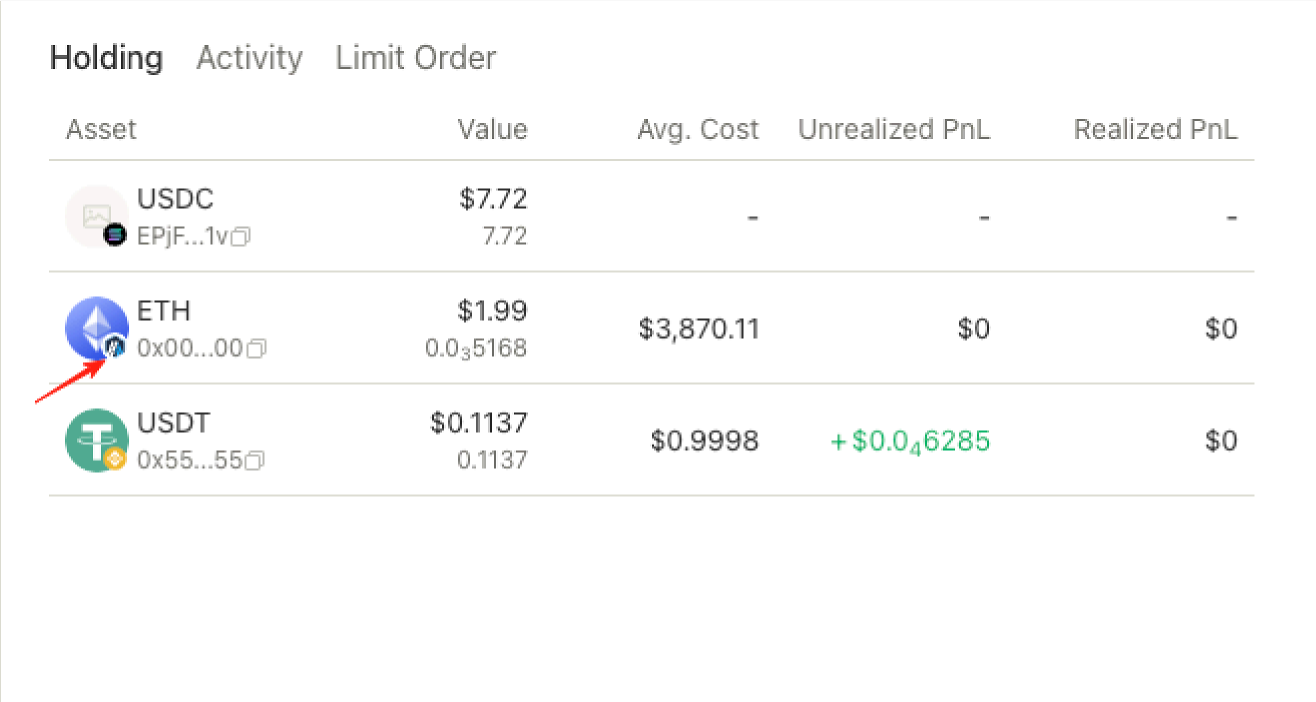
[N10] [Low] Token Display Does Not Match Actual Chain

Category: Others

Content

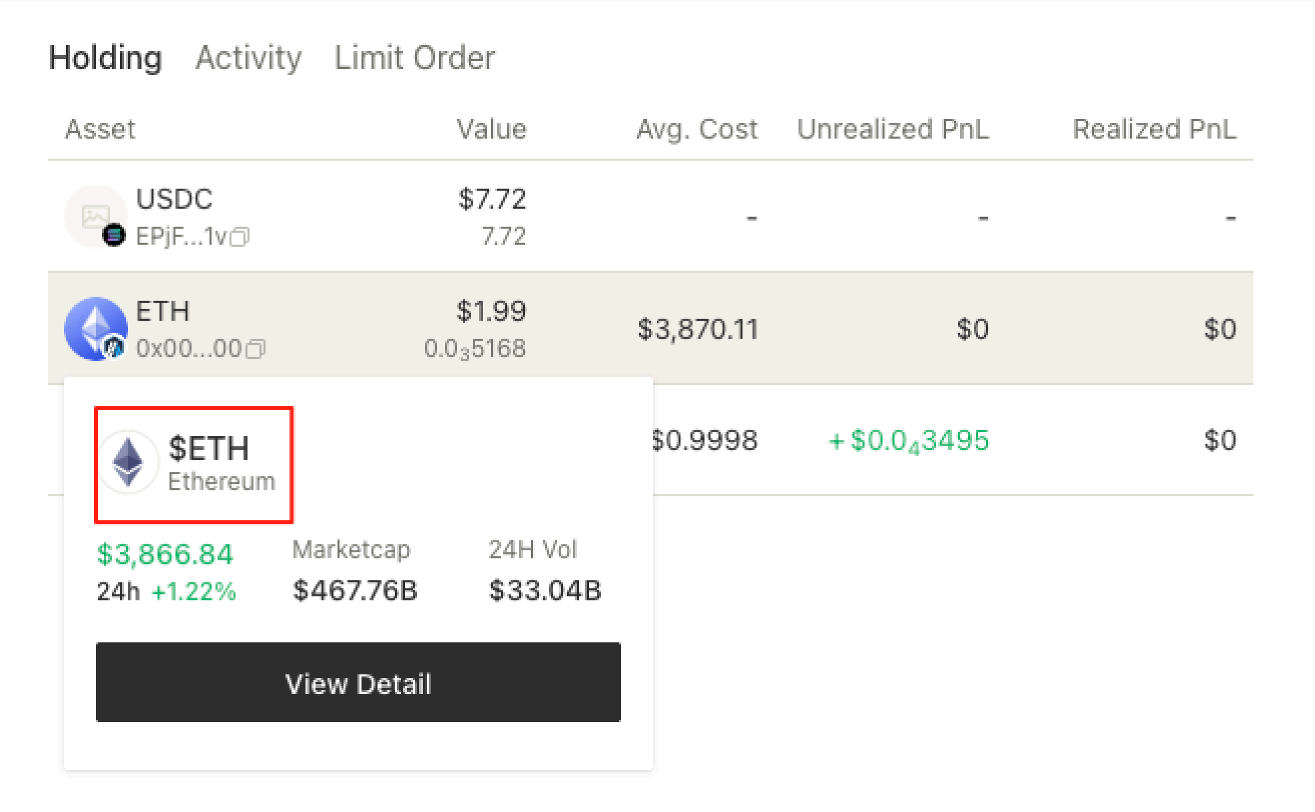
On the Wallet Holding page, the displayed chain for a token deviates from reality, which may mislead users.

The page shows ETH on Arbitrum:



Asset	Value	Avg. Cost	Unrealized PnL	Realized PnL
USDC EPjF...1v	$7.72 7.72	-	-	-
ETH 0x00...00	$1.99 $0.0_{3}5168$	$3,870.11	$0	$0
USDT 0x55...55	$0.1137 0.1137	$0.9998	+$\$0.0_{4}6285$	$0

Hovering reveals ETH on Ethereum mainnet:



Asset	Value	Avg. Cost	Unrealized PnL	Realized PnL
USDC EPjF...1v	$7.72 7.72	-	-	-
ETH 0x00...00	$1.99 $0.0_{3}5168$	$3,870.11	$0	$0
		$0.9998	+$0.0_{4}3495$	$0

$ETH
Ethereum

	Marketcap	24H Vol
$3,866.84 24h +1.22%	$467.76B	$33.04B

Solution

It is recommended to fix the data source or mapping so the Wallet Holding page reflects the true chain for each asset.

Status

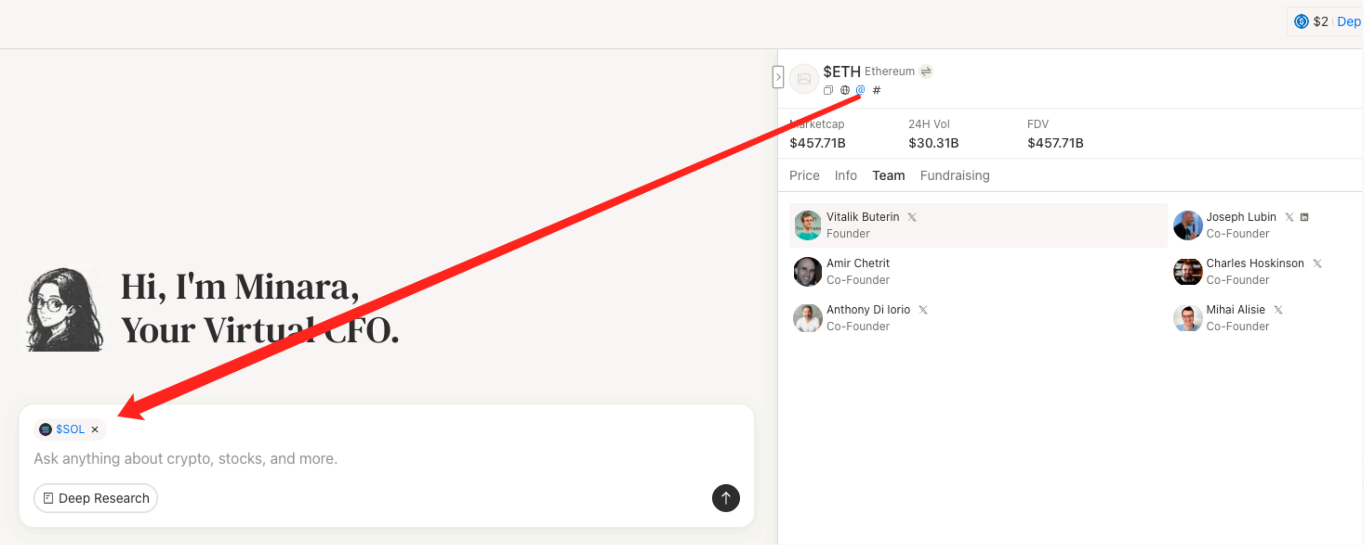
Fixed

[N11] [Low] Token Display Error in Chat Mention

Category: Others

Content

On the ETH trading interface, clicking “Mention in next chat” shows the token as SOL in the chat window.



$2 Dep

$ETH Ethereum

arketcap $457.71B

24H Vol $30.31B

FDV $457.71B

Price Info Team Fundraising

Vitalik Buterin Founder	Joseph Lubin Co-Founder
Amir Chetrit Co-Founder	Charles Hoskinson Co-Founder
Anthony Di Iorio Co-Founder	Mihai Alisie Co-Founder

Hi, I'm Minara,
Your Virtual CFO.

$SOL ×

Ask anything about crypto, stocks, and more.

Deep Research

Solution

It is recommended to correct the token reference passed to chat so it matches the user’s context.

Status

Fixed

[N12] [Suggestion] Incomplete Transaction Information Display

Category: Others

Content

After initiating a transaction, the pop-up shows only the token and total fee, without the full counterparty, slippage, and detailed fee breakdown.

Solution

It is recommended to show a secondary confirmation dialog detailing the counterparty, exact token amounts, and a complete fee breakdown before final confirmation.

Status

Fixed

[N13] [High] Slippage Setting Is Too High

Category: Others

Content

Default slippage is 25% and cannot be changed, exposing users to sandwich attacks.

Solution

It is recommended to dynamically adapt slippage to market conditions and allow user overrides.

Status

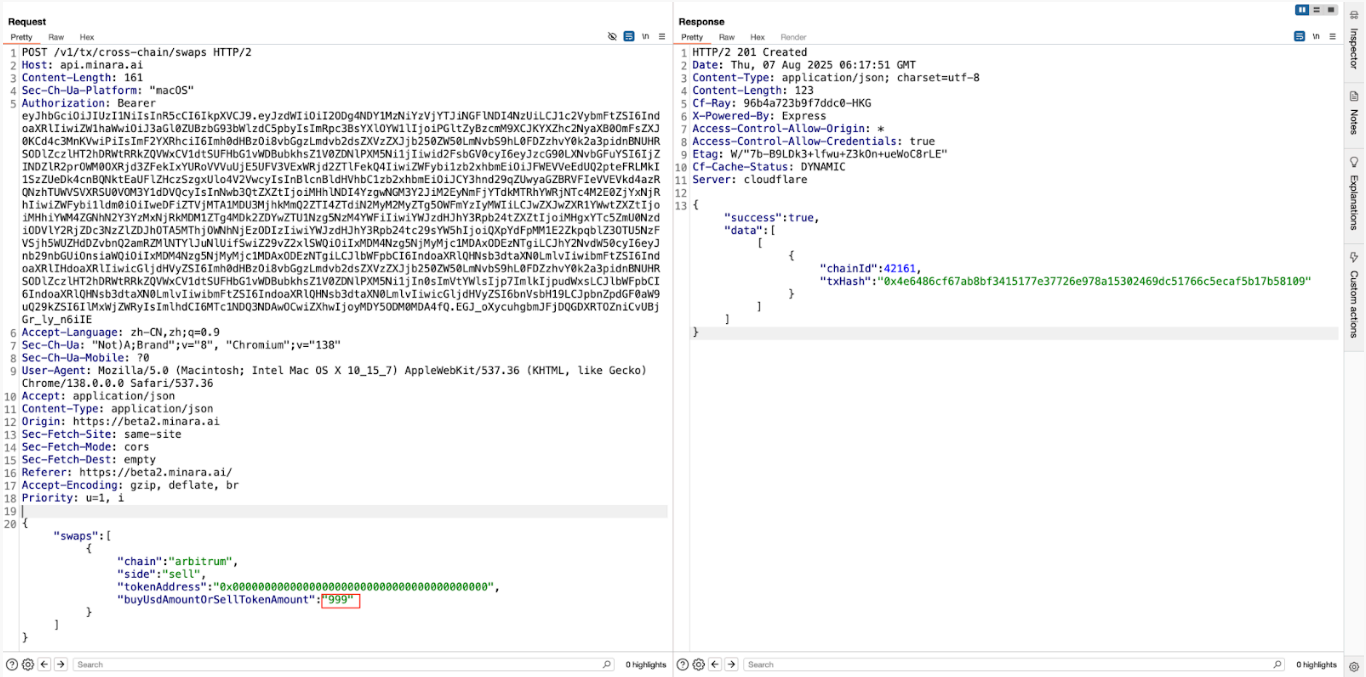
Fixed

[N14] [Suggestion] API Does Not Check Account Balance

Category: Interface security test

Content

During a Swap, setting the amount to 999 does not trigger a balance check; instead, the API attempts to spend the entire available balance of the selected token.



```
POST /v1/tx/cross-chain/swaps HTTP/2
Host: api.minara.ai
Content-Length: 161
Sec-Ch-Ua-Platform: "macOS"
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiI2ODg4NDY1MzNiYzVjYTJiNGFlNDI4NzUiLCJ1c2VybmFtZSI6Ind
oaXRlIiwiZW1haWwiOiJ3aGl0ZUBzbG93bWlzdC5pbyIsImRpc3BsYXlOYW1lIjoiPGltZyBzcmM9XCJKYXZhc2NyaXB0OmFsZXJ
0KCd4c3MnKVwiPiIsImF2YXRhciI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0k2a3pidnBNUHR
SODlZczlHT2hDRWtRRkZQVWxCV1dtSUFHbG1vWDBubkhsZ1V0ZDNlPXM5Ni1jIiwid2FsbGV0cyI6eyJzcG90LXNvbGFuYSI6IjZ
INDZlR2prOWM0OXRjd3ZFekIxYURoVVVuUjE5UFV3VExWRjd2ZTlFekQ4IiwiZWFybi1zb2xhbmEiOiJFWEVVeEdUQ2pteFRLMkI
1SzZUeDk4cnBQNktEaUFlZHczSzgxUlo4V2VwcyIsInBlcnBldHVhbC1zb2xhbmEiOiJCY3hnd29qZUwyaGZBRVFIeVVEVkd4azR
QNzhTUWVSVXRSU0VOM3Y1dDVQcyIsInNwb3QtZXZtIjoiMHhlNDI4YzgwNGM3Y2JiM2EyNmFjYTdkMTRhYWRjNTc4M2E0ZjYxNjR
hIiwiZWFybi1ldm0iOiIweDFiZTVjMTA1MDU3MjhkMmQ2ZTI4ZTdiN2MyM2MyZTg5OWFmYzIyMWIiLCJwZXJwZXR1YWwtZXZtIjo
iMHhiYWM4ZGNhN2Y3YzMxNjRkMDM1ZTg4MDk2ZDYwZTU1Nzg5NzM4YWFiIiwiYWJzdHJhY3Rpb24tZXZtIjoiMHgxYTc5ZmU0Nzd
iODVlY2RjZDc3NzZlZDJhOTA5MThjOWNhNjEzODIzIiwiYWJzdHJhY3Rpb24tc29sYW5hIjoiQXpYdFpMM1E2ZkpqblZ3OTU5NzF
VSjh5WUZHdDZvbnQ2amRZMlNTYlJuNlUifSwiZ29vZ2xlSWQiOiIxMDM4Nzg5NjMyMjc1MDAxODEzNTgiLCJhY2NvdW50cyI6eyJ
nb29nbGUiOnsiaWQiOiIxMDM4Nzg5NjMyMjc1MDAxODEzNTgiLCJlbWFpbCI6IndoaXRlQHNsb3dtaXN0LmlvIiwibmFtZSI6Ind
oaXRlIHdoaXRlIiwicGljdHVyZSI6Imh0dHBzOi8vbGgzLmdvb2dsZXVzZXJjb250ZW50LmNvbS9hL0FDZzhvY0k2a3pidnBNUHR
SODlZczlHT2hDRWtRRkZQVWxCV1dtSUFHbG1vWDBubkhsZ1V0ZDNlPXM5Ni1jIn0sImVtYWlsIjp7ImlkIjpudWxsLCJlbWFpbCI
6IndoaXRlQHNsb3dtaXN0LmlvIiwibmFtZSI6IndoaXRlQHNsb3dtaXN0LmlvIiwicGljdHVyZSI6bnVsbH19LCJpbnZpdGF0aW9
uQ29kZSI6IlMxWjZWRyIsImlhdCI6MTc1NDQ3NDAwOCwiZXhwIjoyMDY5ODM0MDA4fQ.EGJ_oXycuhgbmJFjDQGDXRTOZniCvUBj
Gr_ly_n6iIE
Accept-Language: zh-CN,zh;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Accept: application/json
Content-Type: application/json
Origin: https://beta2.minara.ai
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://beta2.minara.ai/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "swaps":[
        {
            "chain":"arbitrum",
            "side":"sell",
            "tokenAddress":"0x0000000000000000000000000000000000000000",
            "buyUsdAmountOrSellTokenAmount":"999"
        }
    ]
}
```

```
HTTP/2 201 Created
Date: Thu, 07 Aug 2025 06:17:51 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 123
Cf-Ray: 96b4a723b9f7ddc0-HKG
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Etag: W/"7b-B9LDk3+lfwu+Z3kOn+ueWoC8rLE"
Cf-Cache-Status: DYNAMIC
Server: cloudflare

{
    "success":true,
    "data":[
        [
            {
                "chainId":42161,
                "txHash":"0x4e6486cf67ab8bf3415177e37726e978a15302469dc51766c5ecaf5b17b58109"
            }
        ]
    ]
}
```

Solution

It is recommended to validate the available balance at the API layer before constructing the transaction.

Status

Acknowledged

[N15] [Suggestion] Missing Anti-Phishing Strategy

Category: Others

Content

No anti-phishing protections were found.

Solution

It is recommended to implement anti-phishing controls.

Status

Acknowledged

[N16] [Suggestion] Missing AML Strategy

Category: Others

Content

An AML security strategy is missing. AML policies are intended to prevent, monitor, and combat money laundering via KYC, transaction monitoring, risk assessment, and compliance audits. Without these, the platform faces regulatory and financial security risks.

Solution

It is recommended to establish AML policies to prevent interactions with sanctioned entities and malicious addresses, reducing the risk of fund freezes.

Status

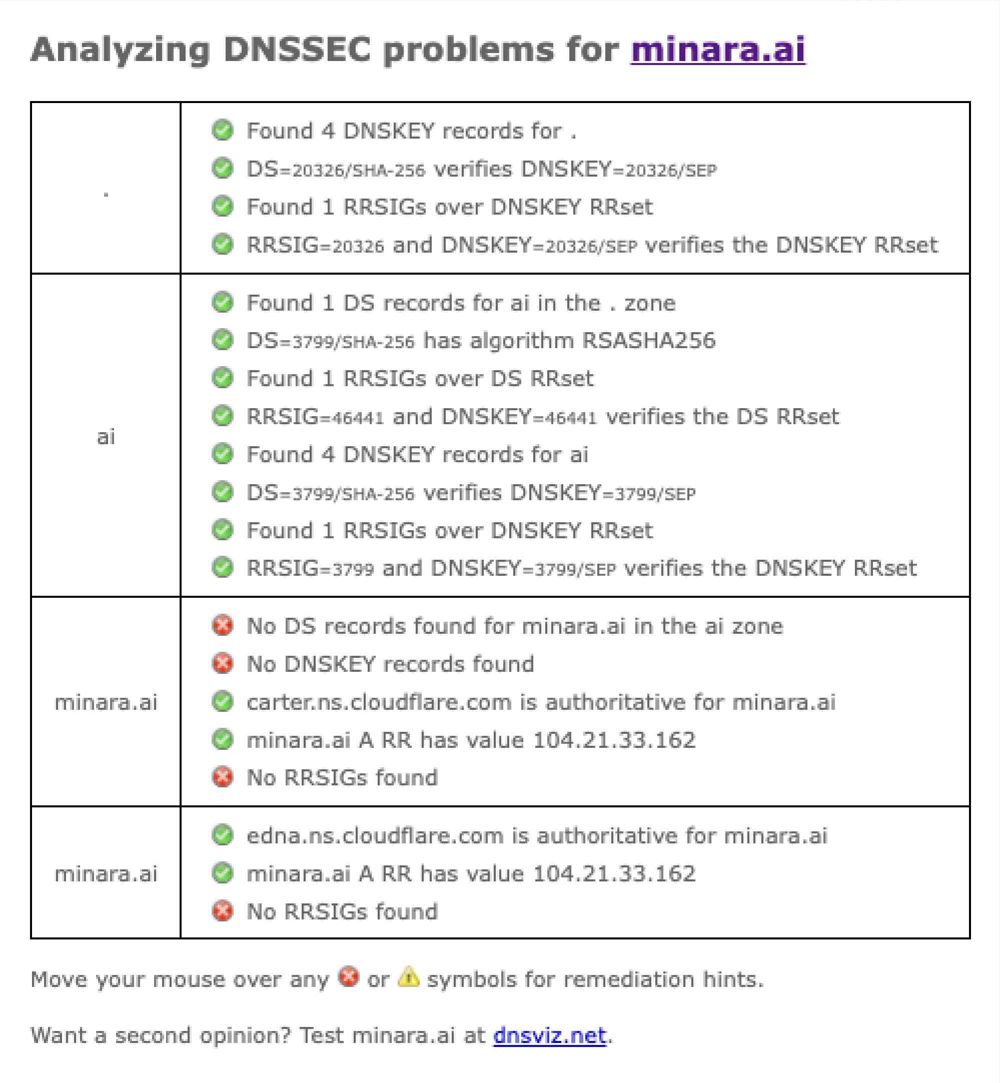
Acknowledged

[N17] [Suggestion] DNSSEC Not Configured

Category: Network infrastructure configuration test

Content

The domain is not configured with DNSSEC.



Analyzing DNSSEC problems for minara.ai

.	✓ Found 4 DNSKEY records for . ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
ai	✓ Found 1 DS records for ai in the . zone ✓ DS=3799/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=46441 and DNSKEY=46441 verifies the DS RRset ✓ Found 4 DNSKEY records for ai ✓ DS=3799/SHA-256 verifies DNSKEY=3799/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=3799 and DNSKEY=3799/SEP verifies the DNSKEY RRset
minara.ai	✗ No DS records found for minara.ai in the ai zone ✗ No DNSKEY records found ✓ carter.ns.cloudflare.com is authoritative for minara.ai ✓ minara.ai A RR has value 104.21.33.162 ✗ No RRSIGs found
minara.ai	✓ edna.ns.cloudflare.com is authoritative for minara.ai ✓ minara.ai A RR has value 104.21.33.162 ✗ No RRSIGs found

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

Want a second opinion? Test minara.ai at dnsviz.net.

Solution

It is recommended to correctly configure DNSSEC for the domain.

Status

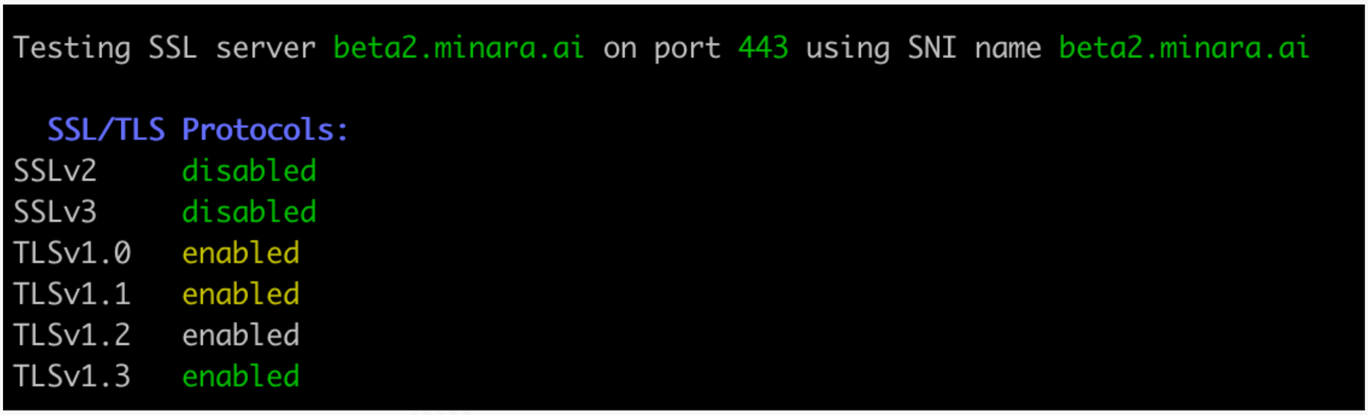
Acknowledged

[N18] [Suggestion] Low TLS Versions Allowed

Category: Network infrastructure configuration test

Content

The site supports legacy TLS versions with known vulnerabilities, which can enable eavesdropping or tampering and do not meet modern security standards.



```
Testing SSL server beta2.minara.ai on port 443 using SNI name beta2.minara.ai

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled
```

Solution

It is recommended to only support TLS 1.2 and above to improve transport security.

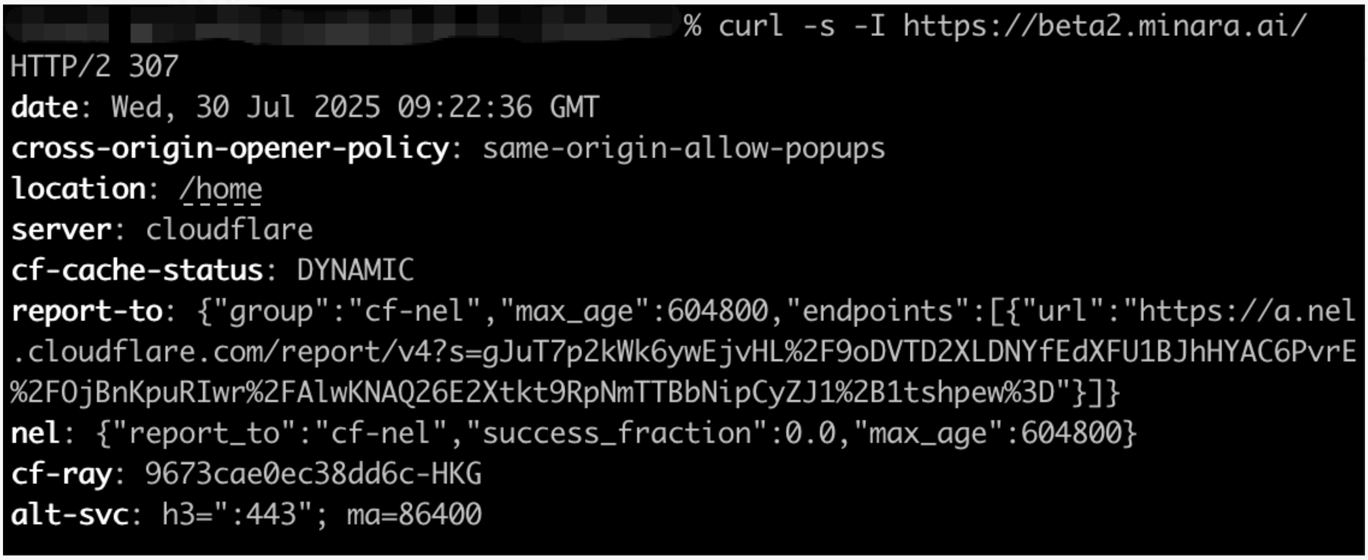
Status

Fixed

[N19] [Suggestion] Missing X-Frame-Options Header

Category: Web security response header test

Content



```
[redacted] % curl -s -I https://beta2.minara.ai/
HTTP/2 307
date: Wed, 30 Jul 2025 09:22:36 GMT
cross-origin-opener-policy: same-origin-allow-popups
location: /home
server: cloudflare
cf-cache-status: DYNAMIC
report-to: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel
.cloudflare.com/report/v4?s=gJuT7p2kWk6ywEjvHL%2F9oDVTD2XLDNYfEdXFU1BJhHYAC6PvrE
%2FOjBnKpuRIwr%2FAlwKNAQ26E2Xtkt9RpNmTTBbNipCyZJ1%2B1tshpew%3D"}]}
nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
cf-ray: 9673cae0ec38dd6c-HKG
alt-svc: h3=":443"; ma=86400
```

X-Frame-Options is an HTTP response header used to defend against clickjacking attacks. Its main function is to control whether the current web page is allowed to be embedded in frame, iframe, embed, or object. By setting appropriate values such as DENY (prohibiting any web page embedding), SAMEORIGIN (allowing only same-origin web page embedding), or ALLOW-FROM uri (allowing web page embedding from a specified source), it can effectively prevent attackers from using nested frames to induce users to perform operations on seemingly normal pages, thereby stealing sensitive information or executing unintended operations. If this response header is missing, the website is at risk of clickjacking attacks where it is embedded in frames by malicious websites.

Solution

It is recommended to add the X-Frame-Options configuration item in the HTTP response header. You can choose an appropriate value according to actual needs. For example, X-Frame-Options: DENY, X-Frame-Options: SAMEORIGIN, or X-Frame-Options: ALLOW-FROM https://example.com (need to replace https://example.com with the actual allowed source).

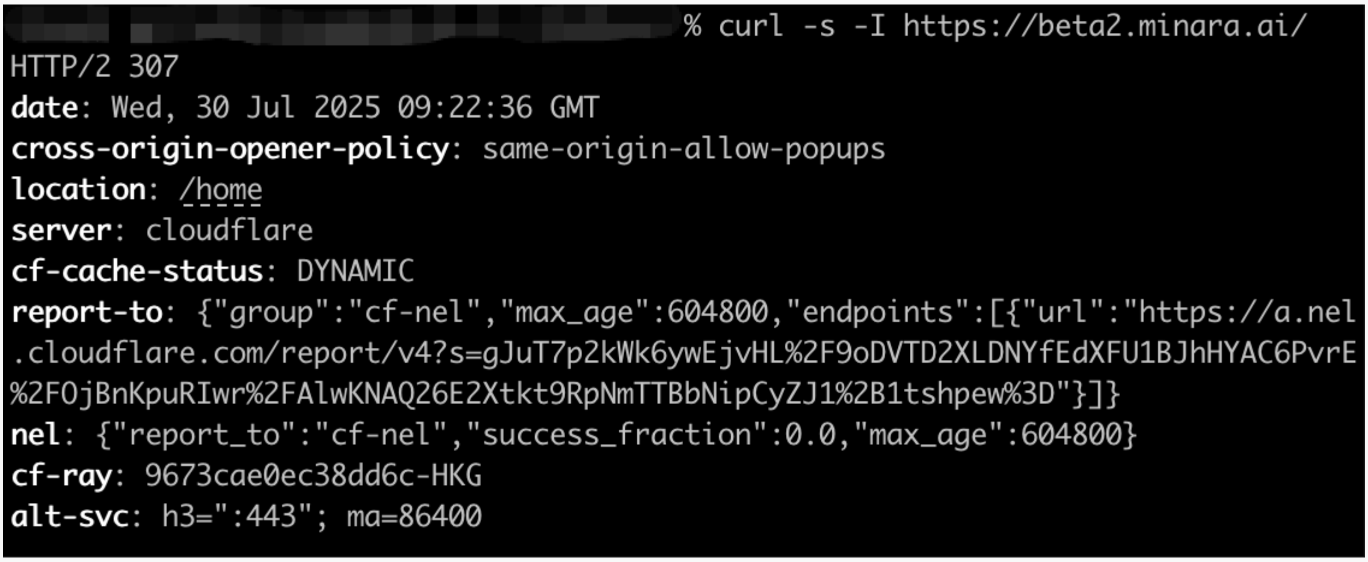
Status

Acknowledged

[N20] [Suggestion] Missing X-Content-Type-Options Header

Category: Web security response header test

Content



```
[redacted] % curl -s -I https://beta2.minara.ai/
HTTP/2 307
date: Wed, 30 Jul 2025 09:22:36 GMT
cross-origin-opener-policy: same-origin-allow-popups
location: /home
server: cloudflare
cf-cache-status: DYNAMIC
report-to: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel
.cloudflare.com/report/v4?s=gJuT7p2kWk6ywEjvHL%2F9oDVTD2XLDNYfEdXFU1BJhHYAC6PvrE
%2FOjBnKpuRIwr%2FAlwKNAQ26E2Xtkt9RpNmTTBbNipCyZJ1%2B1tshpew%3D"}]}
nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
cf-ray: 9673cae0ec38dd6c-HKG
alt-svc: h3=":443"; ma=86400
```

The `X-Content-Type-Options` header field is not included in the HTTP response headers returned by the server. The core function of this response header is to prevent browsers from performing 'sniffing' on the MIME type of resources. The so-called 'sniffing' refers to the behavior where browsers attempt to guess the file format of files whose types are not explicitly declared. When the value of this header field is set to `nosniff`, the browser will process the relevant resources strictly in accordance with the Content-Type declared by the server. This can effectively prevent malicious scripts that are originally text from being incorrectly identified as executable files, thereby significantly reducing the risks posed by attacks such as cross-site scripting (XSS). If this response header is missing, there will be potential security vulnerabilities on the website, which are likely to be exploited by attackers to bypass the browser's security restriction mechanisms.

Solution

It is recommended to add the configuration item X-Content-Type-Options: nosniff to the HTTP response header.

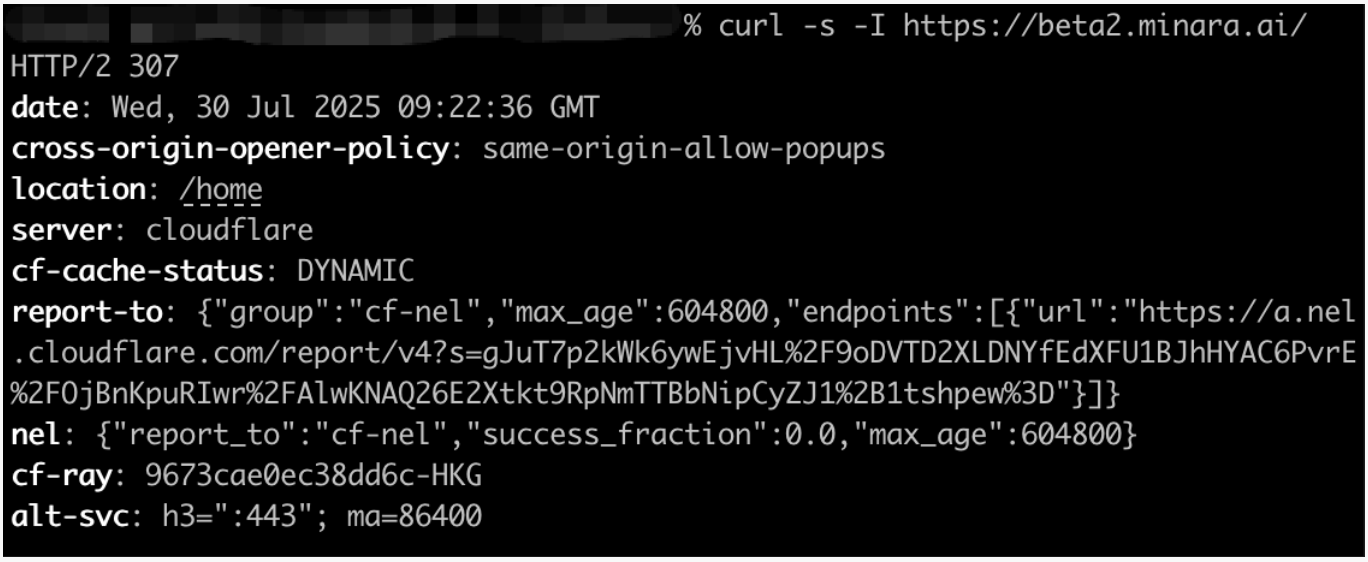
Status

Acknowledged

[N21] [Suggestion] Missing Strict-Transport-Security Header

Category: Web security response header test

Content



```
[redacted] % curl -s -I https://beta2.minara.ai/
HTTP/2 307
date: Wed, 30 Jul 2025 09:22:36 GMT
cross-origin-opener-policy: same-origin-allow-popups
location: /home
server: cloudflare
cf-cache-status: DYNAMIC
report-to: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel
.cloudflare.com/report/v4?s=gJuT7p2kWk6ywEjvHL%2F9oDVTD2XLDNYfEdXFU1BJhHYAC6PvrE
%2FOjBnKpuRIwr%2FAlwKNAQ26E2Xtkt9RpNmTTBbNipCyZJ1%2B1tshpew%3D"}]}
nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
cf-ray: 9673cae0ec38dd6c-HKG
alt-svc: h3=":443"; ma=86400
```

Strict-Transport-Security (referred to as HSTS) is an important HTTP response header. Its core function is to force browsers to always access websites via the HTTPS protocol instead of HTTP. Even if a user manually enters an HTTP address or clicks on an HTTP link, the browser will automatically redirect to the HTTPS version. This mechanism can effectively avoid security risks such as man-in-the-middle attacks, eavesdropping and tampering during data transmission that may occur when using the HTTP protocol, providing more reliable security guarantees for website communications. If this response header is missing, the website may face the risk of being downgraded to HTTP protocol access, thereby increasing the possibility of various security attacks.

Solution

It is recommended to add the configuration item Strict-Transport-Security: max-age=31536000; includeSubDomains; preload to the HTTP response header (specific parameters can be adjusted according to actual conditions. It is recommended that max-age be at least 6 months. includeSubDomains requires ensuring that subdomains have deployed HTTPS. preload is an optional parameter used to apply for inclusion in the browser's HSTS preload list).

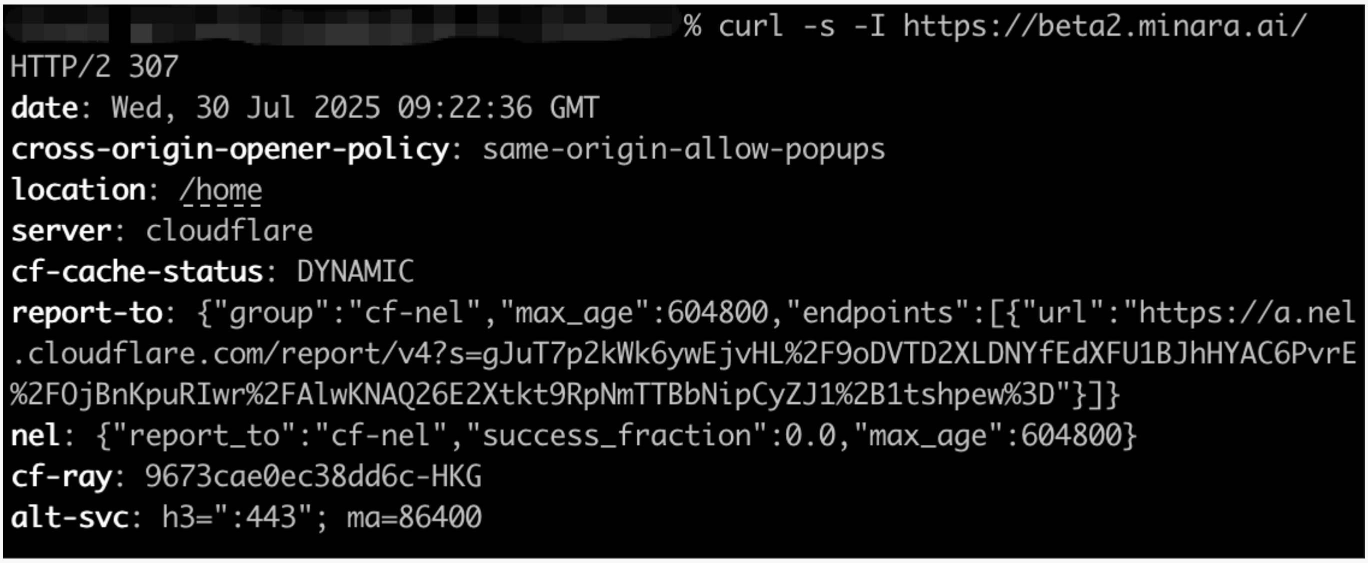
Status

Acknowledged

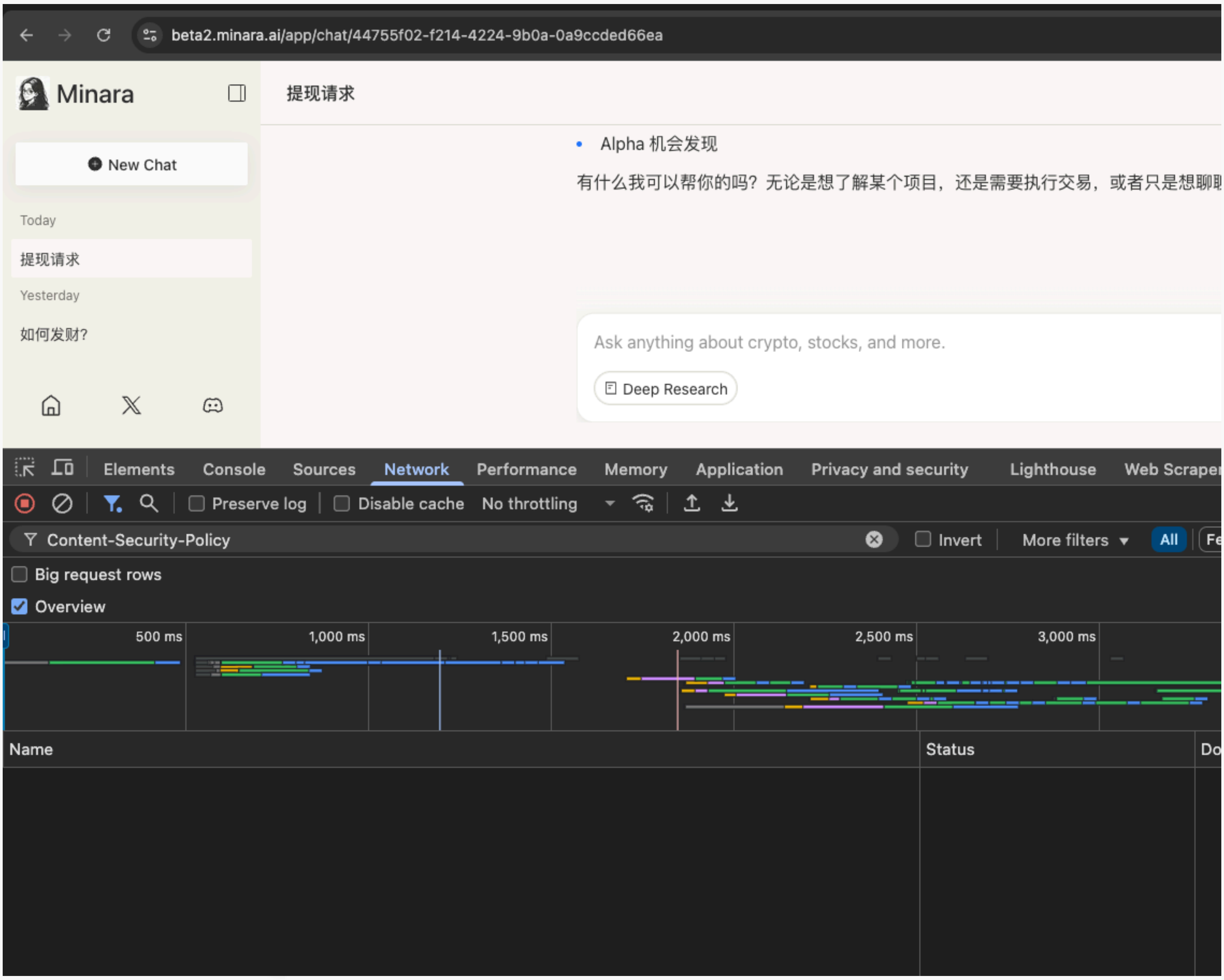
[N22] [Suggestion] Missing Content-Security-Policy Header

Category: Web security response header test

Content



```
[redacted] % curl -s -I https://beta2.minara.ai/
HTTP/2 307
date: Wed, 30 Jul 2025 09:22:36 GMT
cross-origin-opener-policy: same-origin-allow-popups
location: /home
server: cloudflare
cf-cache-status: DYNAMIC
report-to: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel
.cloudflare.com/report/v4?s=gJuT7p2kWk6ywEjvHL%2F9oDVTD2XLDNYfEdXFU1BJhHYAC6PvrE
%2FOjBnKpuRIwr%2FAlwKNAQ26E2Xtkt9RpNmTTBbNipCyZJ1%2B1tshpew%3D"}]}
nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
cf-ray: 9673cae0ec38dd6c-HKG
alt-svc: h3=":443"; ma=86400
```



beta2.minara.ai/app/chat/44755f02-f214-4224-9b0a-0a9ccded66ea

提现请求

- Alpha 机会发现

有什么我可以帮你的吗？无论是想了解某个项目，还是需要执行交易，或者只是想聊聊

Ask anything about crypto, stocks, and more.

Content-Security-Policy

Content-Security-Policy (referred to as CSP) is an important security response header used to defend against various code injection attacks such as cross-site scripting (XSS) and clickjacking. It restricts browsers to load resources only from trusted sources by explicitly specifying the sources from which resources (such as scripts, style sheets, images, audio, video, fonts, etc.) are allowed to be loaded, thereby preventing the execution of malicious code. For example, scripts can be restricted to load only from the own domain name or specific trusted domain names to prevent the injection of external malicious scripts. If this response header is missing, the website cannot effectively restrict resource loading, making it vulnerable to various code injection attacks, which may lead to security issues such as user data leakage and website tampering.

Solution

It is recommended to add the Content-Security-Policy configuration item to the HTTP response header and set a reasonable policy according to the actual situation of the website. For example, Content-Security-Policy: default-src 'self'; script-src 'self' https://trusted-cdn.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:;. Among them, default-src 'self' means that by default, only resources from the same origin are allowed to be loaded; script-src specifies the trusted sources of scripts; style-src specifies the trusted sources of style sheets, etc. (Specific policies need to be adjusted according to the website's resource loading requirements, and 'unsafe-inline' and the like should be used with caution).

Status

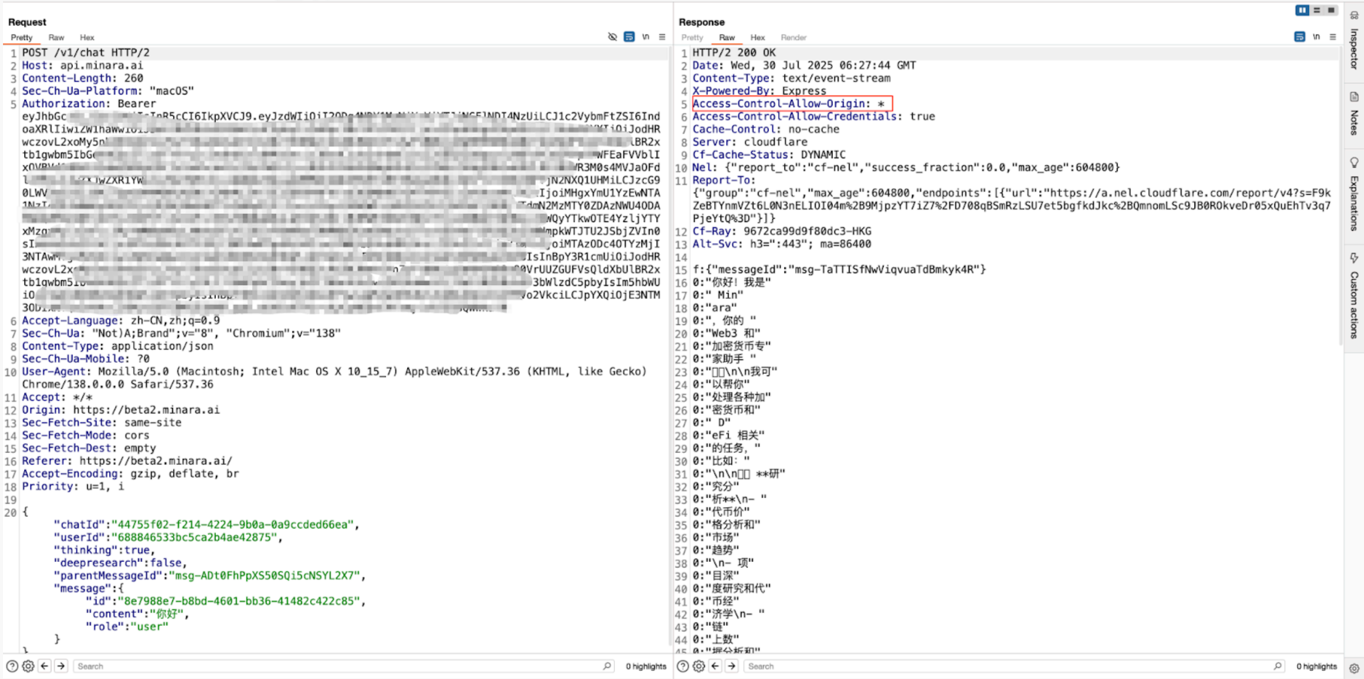
Acknowledged

[N23] [Suggestion] CORS Configuration Is Insecure

Category: Web front-end cross-domain policy test

Content

The site sets Access-Control-Allow-Origin to “*”, allowing requests from any origin to access the resource.



```
POST /v1/chat HTTP/2
Host: api.minara.ai
Content-Length: 260
Sec-Ch-Ua-Platform: "macOS"
Authorization: Bearer
[redacted]
Accept-Language: zh-CN,zh;q=0.9
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
Accept: */*
Origin: https://beta2.minara.ai
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://beta2.minara.ai/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "chatId":"44755f02-f214-4224-9b0a-0a9ccded66ea",
    "userId":"688846533bc5ca2b4ae42875",
    "thinking":true,
    "deepresearch":false,
    "parentMessageId":"msg-ADt0FhPpXS50SQi5cNSYL2X7",
    "message":{
        "id":"8e7988e7-b8bd-4601-bb36-41482c422c85",
        "content":"你好",
        "role":"user"
    }
}
```

```
HTTP/2 200 OK
Date: Wed, 30 Jul 2025 06:27:44 GMT
Content-Type: text/event-stream
X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Cache-Control: no-cache
Server: cloudflare
Cf-Cache-Status: DYNAMIC
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=F9k
ZeBTYnmVZt6L0N3nELIOI04m%2B9MjpzYT7iZ7%2FD708qBSmRzLSU7et5bgfkdJkc%2BQmnomLSc9JB0ROkveDr05xQuEhTv3q7
PjeYtQ%3D"}]}
Cf-Ray: 9672ca99d9f80dc3-HKG
Alt-Svc: h3=":443"; ma=86400

f:{"messageId":"msg-TaTTISfNwViqvuaTdBmkyk4R"}
0:"你好！我是"
0:" Min"
0:"ara"
0:"，你的 "
0:"Web3 和"
0:"加密货币专"
0:"家助手 "
0:"��\n\n我可"
0:"以帮你"
0:"处理各种加"
0:"密货币和"
0:" D"
0:"eFi 相关"
0:"的任务，"
0:"比如："
0:"\n\n�� **研"
0:"究分"
0:"析**\n- "
0:"代币价"
0:"格分析和"
0:"市场"
0:"趋势"
0:"\n- 项"
0:"目深"
0:"度研究和代"
0:"币经"
0:"济学\n- "
0:"链"
0:"上数"
0:"据分析和"
```

Solution

It is recommended to configure Access-Control-Allow-Origin with specific trusted origins based on actual business requirements.

Status

Acknowledged

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002508190001	SlowMist Security Team	2025.07.30 - 2025.08.19	Passed

Summary conclusion: The SlowMist security team undertakes an audit of the project through manual inspection and the utilisation of the analysis tool developed by the SlowMist team. During the audit, nine suggestions were acknowledged. All the other findings have been fixed.

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.

SLOWMIST

Official Website

www.slowmist.com

✉

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist