SLOWMIST

Web Application Security Audit

Table Of Contents

1 Executive Summary

On 2025.01.08, the SlowMist security team received the Safeheron team's security audit application for Safeheron Console, 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	WHOIS information collection	Passed
2	Real IP discovery	Passed
3	Subdomain detection	Passed
4	Mail service detection	Passed
5	Certificate information collection	Passed
6	Web services component fingerprint collection	Passed
7	Port service component fingerprint collection	Passed
8	Segment C service acquisition	Passed
9	Personnel structure collection	Passed
10	GitHub source code leak detection	Passed
11	Google Hack detection	Passed
12	Privacy data leak detection	Passed
13	CDN service detection	Passed
14	Network infrastructure configuration test	Passed
15	Application platform configuration management test	Passed

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

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

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

3 Project Overview

3.1 Project Introduction

Audit Version

Web Console

https://console.safeheron.com

API

API List

https://docs.safeheron.com/api/zh.html#API%20%E5%88%97%E8%A1%A8

Web3 API

https://docs.safeheron.com/api/zh.html#Web3%20API

MPC Sign

https://docs.safeheron.com/api/zh.html#MPC%20Sign

Webhook

https://docs.safeheron.com/api/zh.html#Webhook

3.2 Vulnerability Information

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

NO	Title	Category	Level	Status
N1	Session storage Issue	Session timeout test	Suggestion	Acknowledged
N2	HTTP Parameter Pollution Issue	HTTP parameter pollution test	Suggestion	Acknowledged
N3	Anti-phishing strategies	Others	Suggestion	Acknowledged
N4	DNSSEC Security Issue	Network infrastructure configuration test	Suggestion	Fixed
N5	HTTP Header Security Issue	Web security response header test	Suggestion	Fixed

3.3 Vulnerability Summary

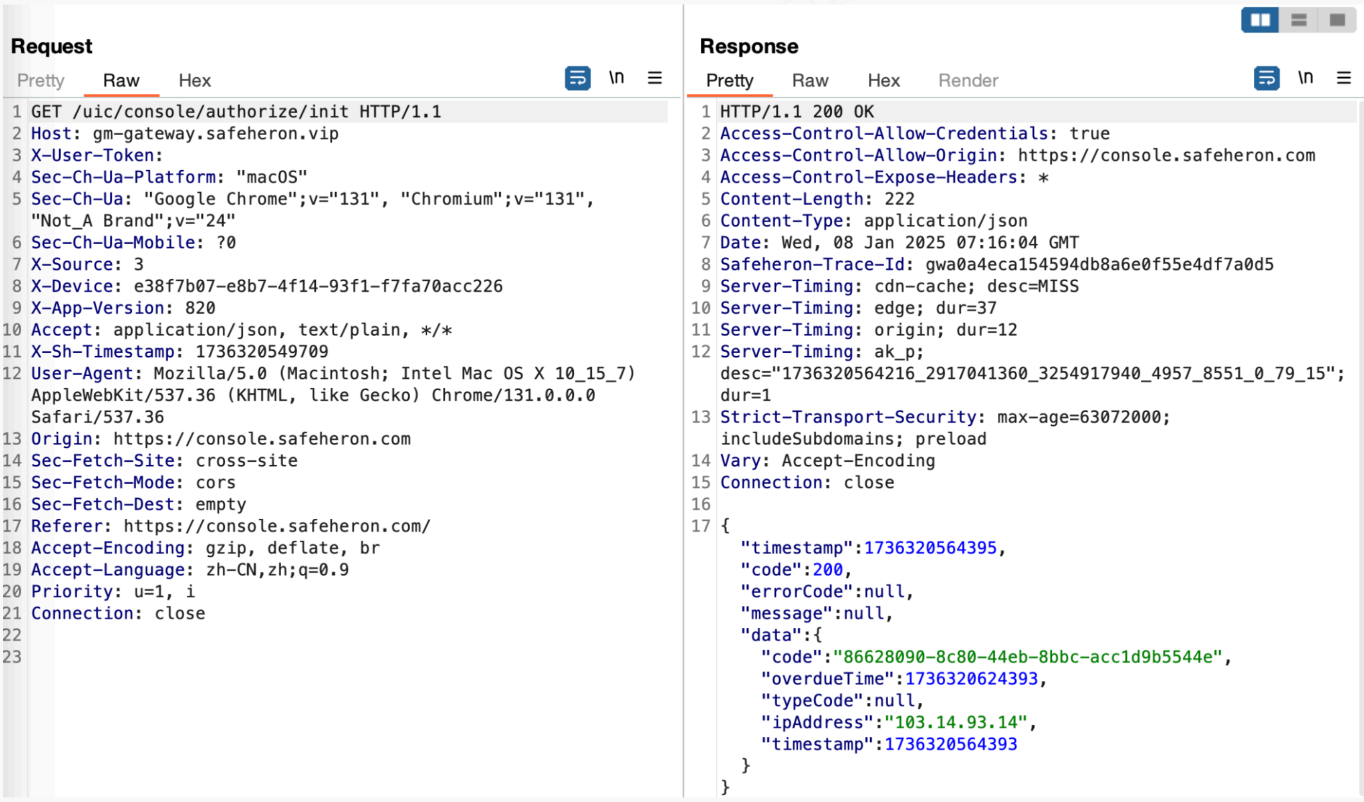
[N1] [Suggestion] Session storage Issue

Category: Session timeout test

Content

Get the code and other information through the "/uic/console/authorize/init" interface and display it through a QR code.

https://gm-gateway.safeheron.vip/uic/console/authorize/init

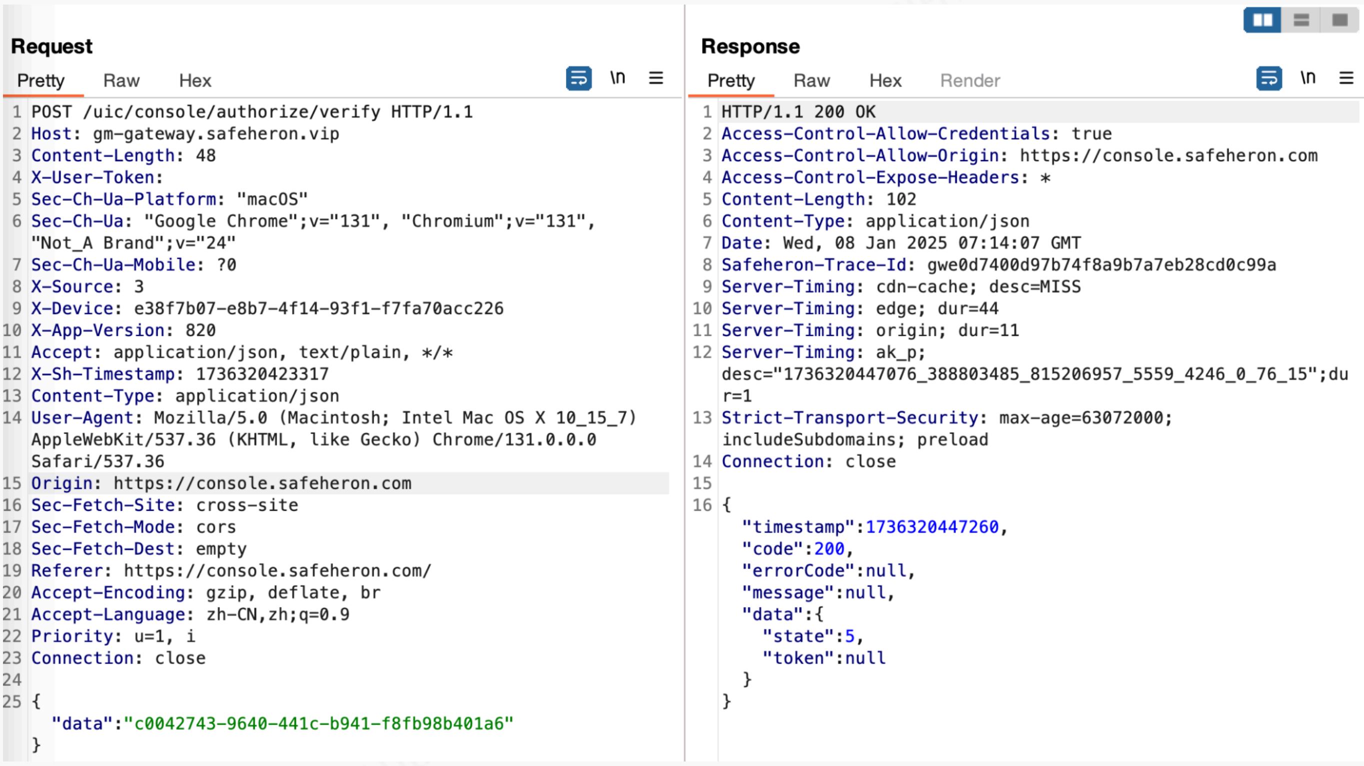


```
GET /uic/console/authorize/init HTTP/1.1
Host: gm-gateway.safeheron.vip
X-User-Token:
Sec-Ch-Ua-Platform: "macOS"
Sec-Ch-Ua: "Google Chrome";v="131", "Chromium";v="131",
"Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: e38f7b07-e8b7-4f14-93f1-f7fa70acc226
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736320549709
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Priority: u=1, i
Connection: close


```

```
HTTP/1.1 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Expose-Headers: *
Content-Length: 222
Content-Type: application/json
Date: Wed, 08 Jan 2025 07:16:04 GMT
Safeheron-Trace-Id: gwa0a4eca154594db8a6e0f55e4df7a0d5
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=37
Server-Timing: origin; dur=12
Server-Timing: ak_p;
desc="1736320564216_2917041360_3254917940_4957_8551_0_79_15";
dur=1
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Vary: Accept-Encoding
Connection: close

{
  "timestamp":1736320564395,
  "code":200,
  "errorCode":null,
  "message":null,
  "data":{
    "code":"86628090-8c80-44eb-8bbc-acc1d9b5544e",
    "overdueTime":1736320624393,
    "typeCode":null,
    "ipAddress":"103.14.93.14",
    "timestamp":1736320564393
  }
}
```

Request the above code through "/uic/console/authorize/verify" POST to verify whether the code is scanned to confirm the login.

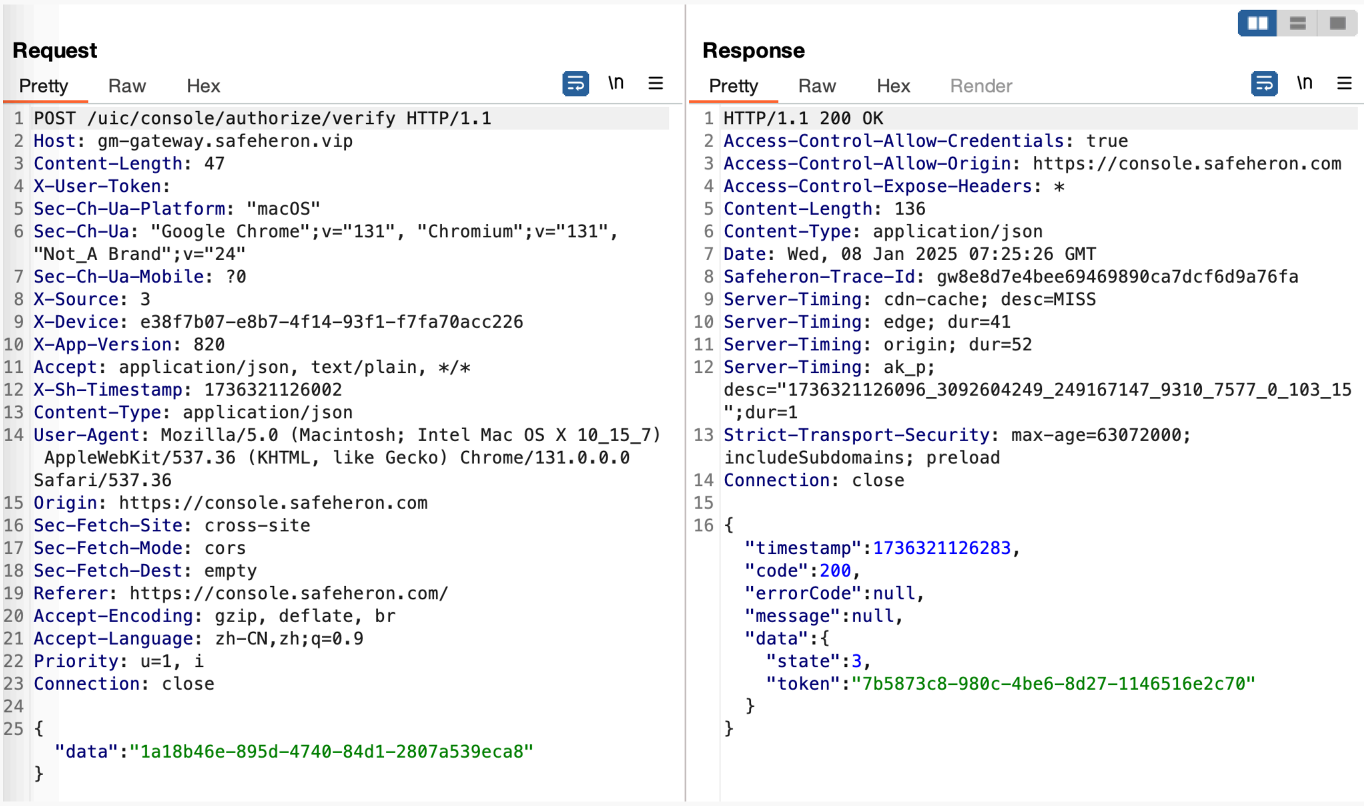
https://gm-gateway.safeheron.vip/uic/console/authorize/verify



```
POST /uic/console/authorize/verify HTTP/1.1
Host: gm-gateway.safeheron.vip
Content-Length: 48
X-User-Token:
Sec-Ch-Ua-Platform: "macOS"
Sec-Ch-Ua: "Google Chrome";v="131", "Chromium";v="131",
"Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: e38f7b07-e8b7-4f14-93f1-f7fa70acc226
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736320423317
Content-Type: application/json
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Priority: u=1, i
Connection: close

{
  "data":"c0042743-9640-441c-b941-f8fb98b401a6"
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Expose-Headers: *
Content-Length: 102
Content-Type: application/json
Date: Wed, 08 Jan 2025 07:14:07 GMT
Safeheron-Trace-Id: gwe0d7400d97b74f8a9b7a7eb28cd0c99a
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=44
Server-Timing: origin; dur=11
Server-Timing: ak_p;
desc="1736320447076_388803485_815206957_5559_4246_0_76_15";du
r=1
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Connection: close

{
  "timestamp":1736320447260,
  "code":200,
  "errorCode":null,
  "message":null,
  "data":{
    "state":5,
    "token":null
  }
}
```

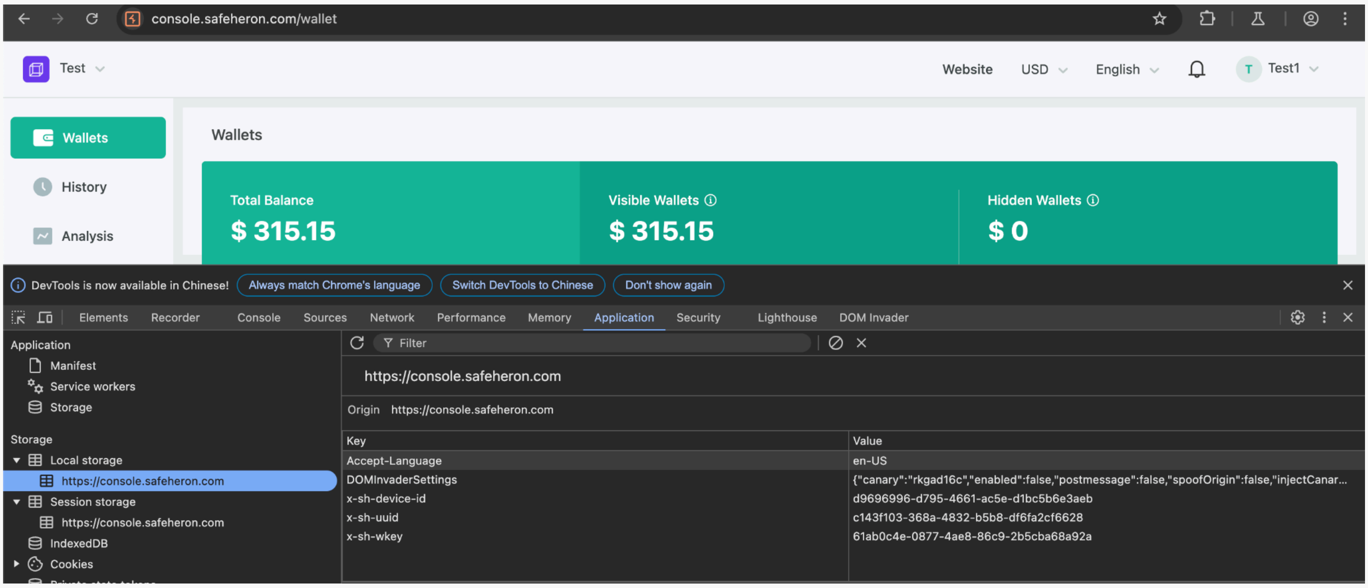
The App scans the code successfully and returns a Token on the interface.



```
POST /uic/console/authorize/verify HTTP/1.1
Host: gm-gateway.safeheron.vip
Content-Length: 47
X-User-Token:
Sec-Ch-Ua-Platform: "macOS"
Sec-Ch-Ua: "Google Chrome";v="131", "Chromium";v="131",
"Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: e38f7b07-e8b7-4f14-93f1-f7fa70acc226
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736321126002
Content-Type: application/json
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Priority: u=1, i
Connection: close

{
  "data":"1a18b46e-895d-4740-84d1-2807a539eca8"
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Expose-Headers: *
Content-Length: 136
Content-Type: application/json
Date: Wed, 08 Jan 2025 07:25:26 GMT
Safeheron-Trace-Id: gw8e8d7e4bee69469890ca7dcf6d9a76fa
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=41
Server-Timing: origin; dur=52
Server-Timing: ak_p;
desc="1736321126096_3092604249_249167147_9310_7577_0_103_15
";dur=1
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Connection: close

{
  "timestamp":1736321126283,
  "code":200,
  "errorCode":null,
  "message":null,
  "data":{
    "state":3,
    "token":"7b5873c8-980c-4be6-8d27-1146516e2c70"
  }
}
```

All identity verification information is stored in Local storage and will not become invalid after closing the browser.



https://console.safeheron.com

Origin https://console.safeheron.com

Key	Value
Accept-Language	en-US
DOMInvaderSettings	{"canary":"rkgad16c","enabled":false,"postmessage":false,"spoofOrigin":false,"injectCanar...
x-sh-device-id	d9696996-d795-4661-ac5e-d1bc5b6e3aeb
x-sh-uuid	c143f103-368a-4832-b5b8-df6fa2cf6628
x-sh-wkey	61ab0c4e-0877-4ae8-86c9-2b5cba68a92a

Solution

It is recommended that all authentication-related information be stored in session storage, which will become invalid once the browser is closed.

Status

Acknowledged

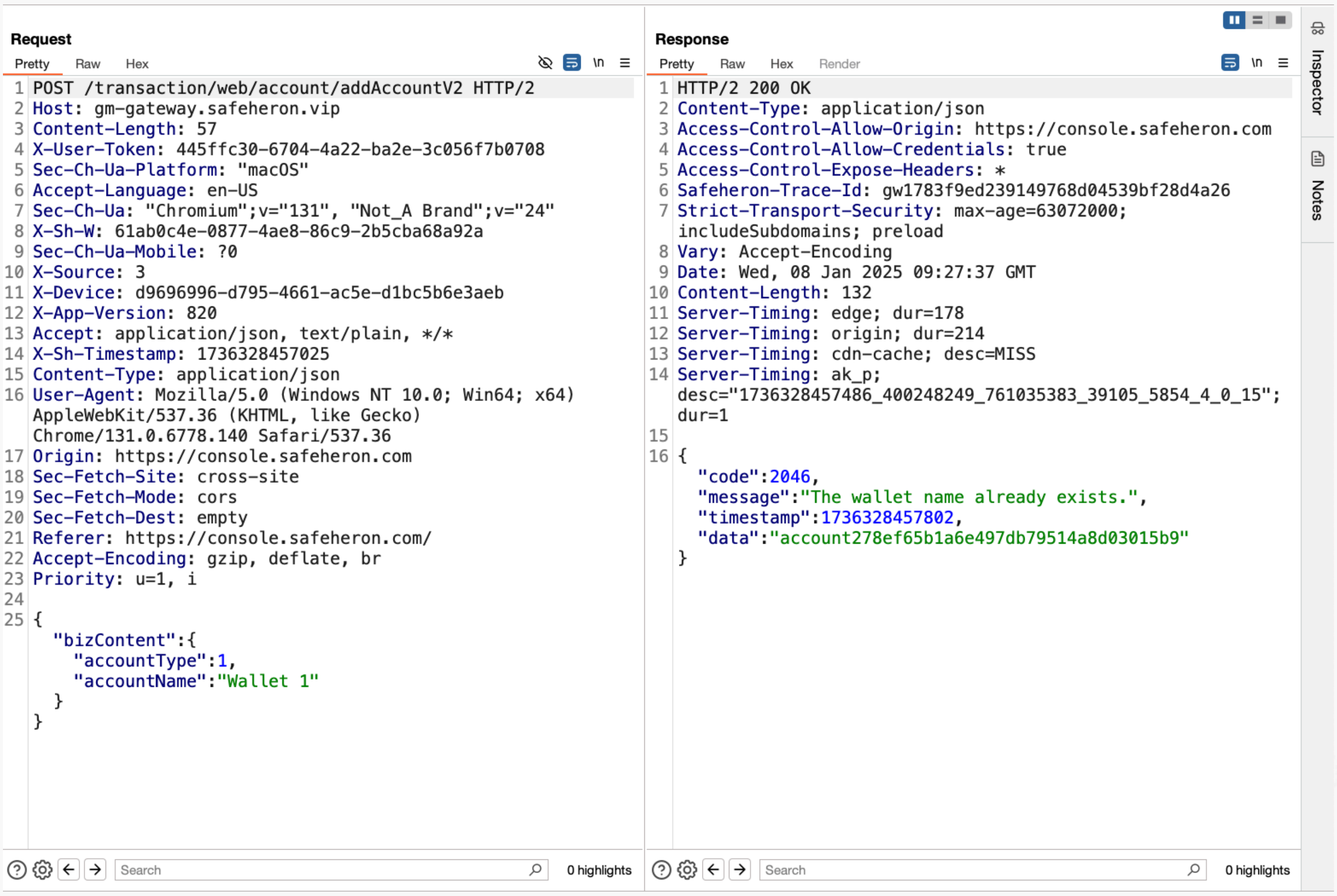
[N2] [Suggestion] HTTP Parameter Pollution Issue

Category: HTTP parameter pollution test

Content

1.Create Wallet

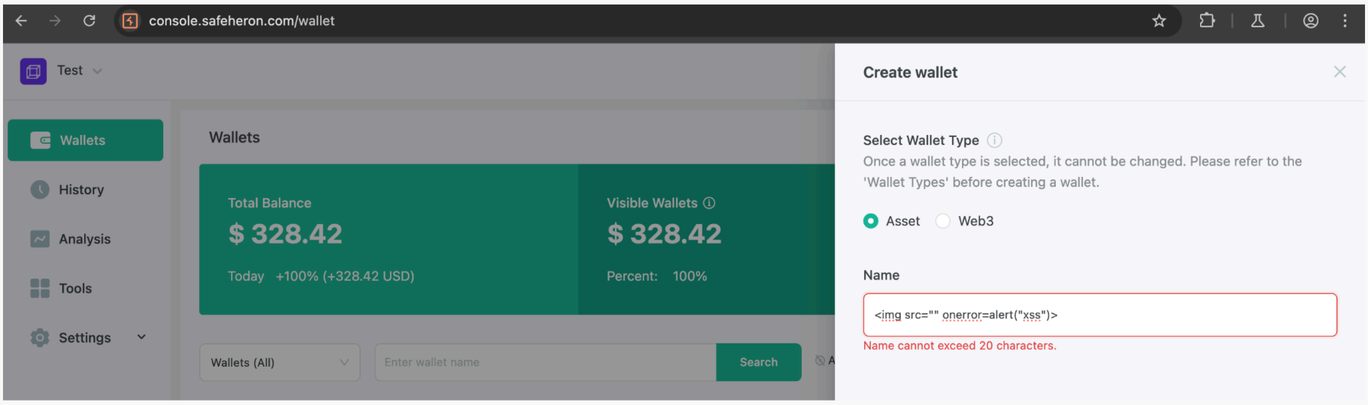
Trying to create a wallet with the same name returns "wallet name already exists".



```
POST /transaction/web/account/addAccountV2 HTTP/2
Host: gm-gateway.safeheron.vip
Content-Length: 57
X-User-Token: 445ffc30-6704-4a22-ba2e-3c056f7b0708
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
X-Sh-W: 61ab0c4e-0877-4ae8-86c9-2b5cba68a92a
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: d9696996-d795-4661-ac5e-d1bc5b6e3aeb
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736328457025
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
  "bizContent":{
    "accountType":1,
    "accountName":"Wallet 1"
  }
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gw1783f9ed239149768d04539bf28d4a26
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Vary: Accept-Encoding
Date: Wed, 08 Jan 2025 09:27:37 GMT
Content-Length: 132
Server-Timing: edge; dur=178
Server-Timing: origin; dur=214
Server-Timing: cdn-cache; desc=MISS
Server-Timing: ak_p;
desc="1736328457486_400248249_761035383_39105_5854_4_0_15";
dur=1

{
  "code":2046,
  "message":"The wallet name already exists.",
  "timestamp":1736328457802,
  "data":"account278ef65b1a6e497db79514a8d03015b9"
}
```

There is a length limit for wallet names, which cannot exceed 20 characters.



Create wallet

Select Wallet Type

Once a wallet type is selected, it cannot be changed. Please refer to the 'Wallet Types' before creating a wallet.

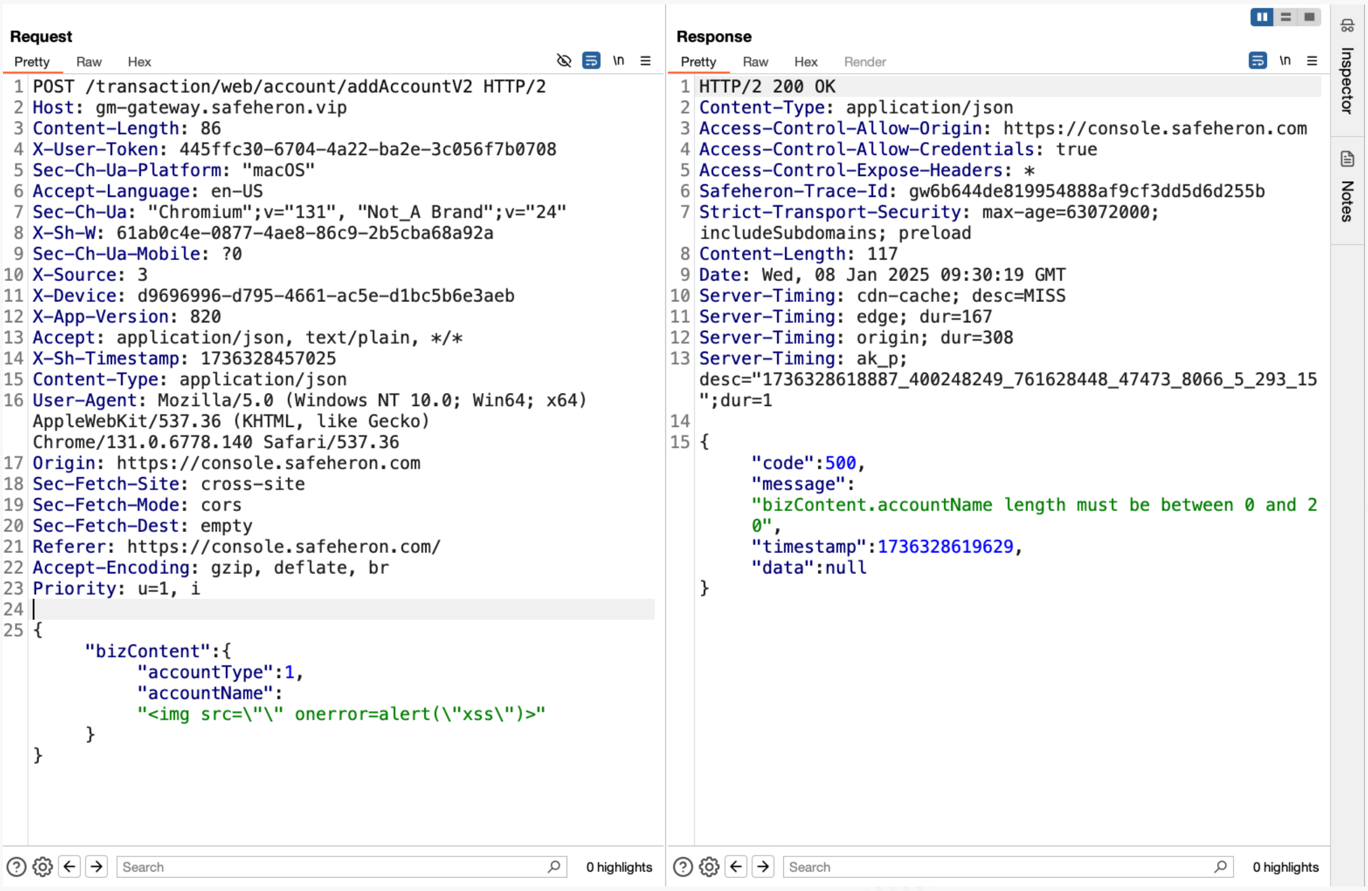
● Asset ○ Web3

Name

<img src="" onerror=alert("xss")>

Name cannot exceed 20 characters.

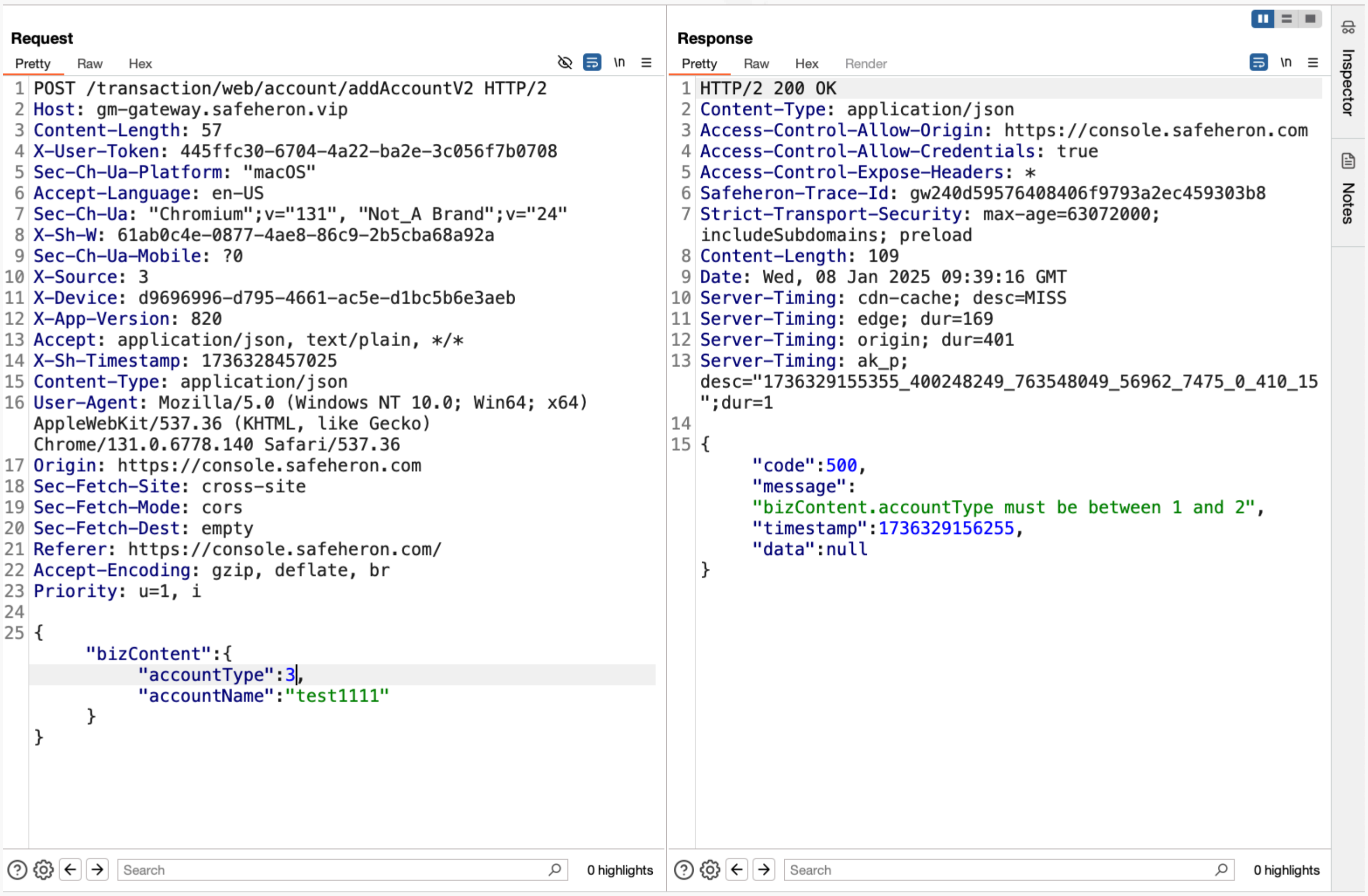
There are also length restrictions at the interface level.



```
POST /transaction/web/account/addAccountV2 HTTP/2
Host: gm-gateway.safeheron.vip
Content-Length: 86
X-User-Token: 445ffc30-6704-4a22-ba2e-3c056f7b0708
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
X-Sh-W: 61ab0c4e-0877-4ae8-86c9-2b5cba68a92a
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: d9696996-d795-4661-ac5e-d1bc5b6e3aeb
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736328457025
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "bizContent":{
        "accountType":1,
        "accountName":
        "<img src=\"\" onerror=alert(\"xss\")>"
    }
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gw6b644de819954888af9cf3dd5d6d255b
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Content-Length: 117
Date: Wed, 08 Jan 2025 09:30:19 GMT
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=167
Server-Timing: origin; dur=308
Server-Timing: ak_p;
desc="1736328618887_400248249_761628448_47473_8066_5_293_15
";dur=1

{
    "code":500,
    "message":
    "bizContent.accountName length must be between 0 and 2
    0",
    "timestamp":1736328619629,
    "data":null
}
```

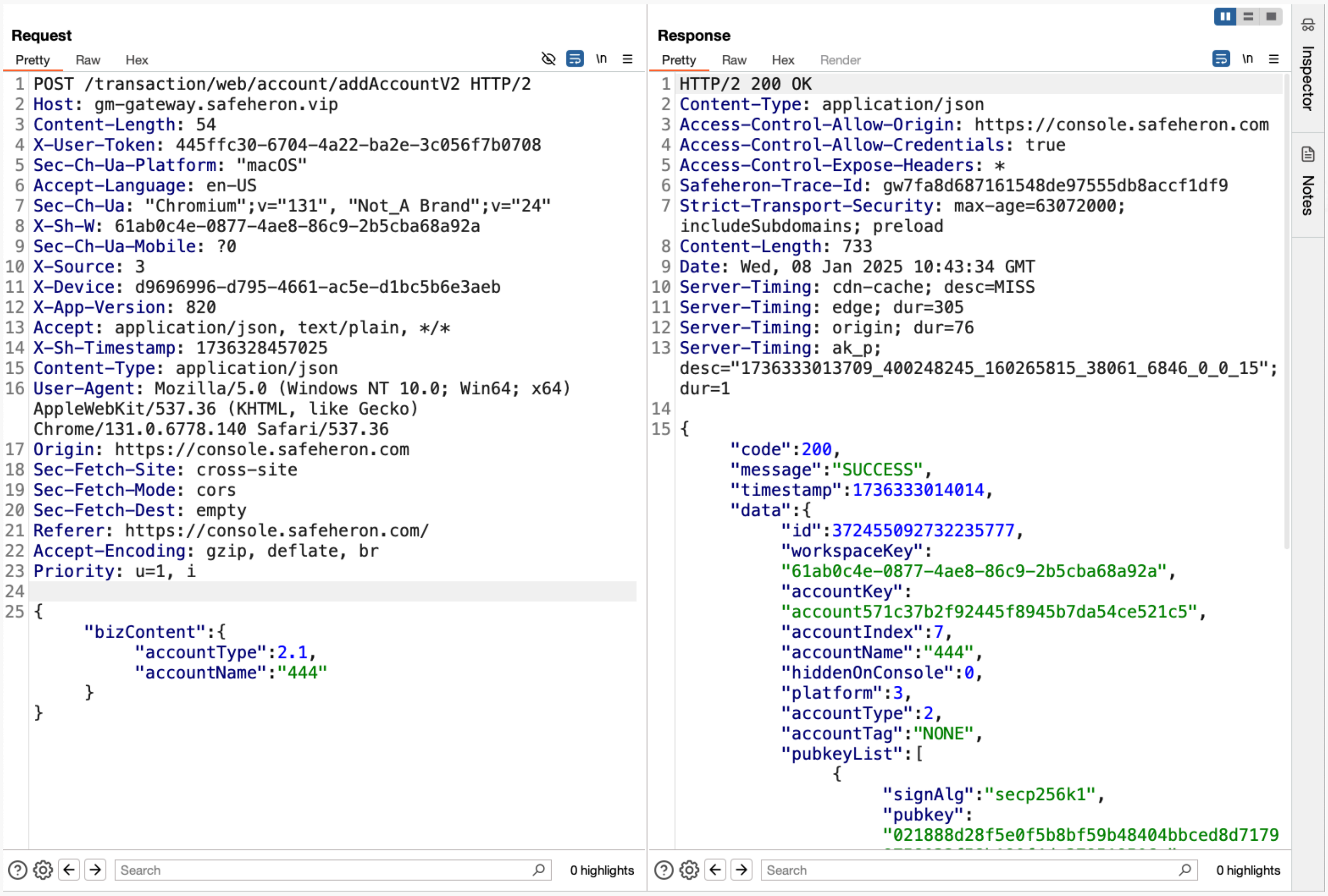
Creating a wallet with the wrong "accountType" returns "bizContent.accountType must be between 1 and 2".



```
POST /transaction/web/account/addAccountV2 HTTP/2
Host: gm-gateway.safeheron.vip
Content-Length: 57
X-User-Token: 445ffc30-6704-4a22-ba2e-3c056f7b0708
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
X-Sh-W: 61ab0c4e-0877-4ae8-86c9-2b5cba68a92a
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: d9696996-d795-4661-ac5e-d1bc5b6e3aeb
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736328457025
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "bizContent":{
        "accountType":3,
        "accountName":"test1111"
    }
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gw240d59576408406f9793a2ec459303b8
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Content-Length: 109
Date: Wed, 08 Jan 2025 09:39:16 GMT
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=169
Server-Timing: origin; dur=401
Server-Timing: ak_p;
desc="1736329155355_400248249_763548049_56962_7475_0_410_15
";dur=1

{
    "code":500,
    "message":
    "bizContent.accountType must be between 1 and 2",
    "timestamp":1736329156255,
    "data":null
}
```

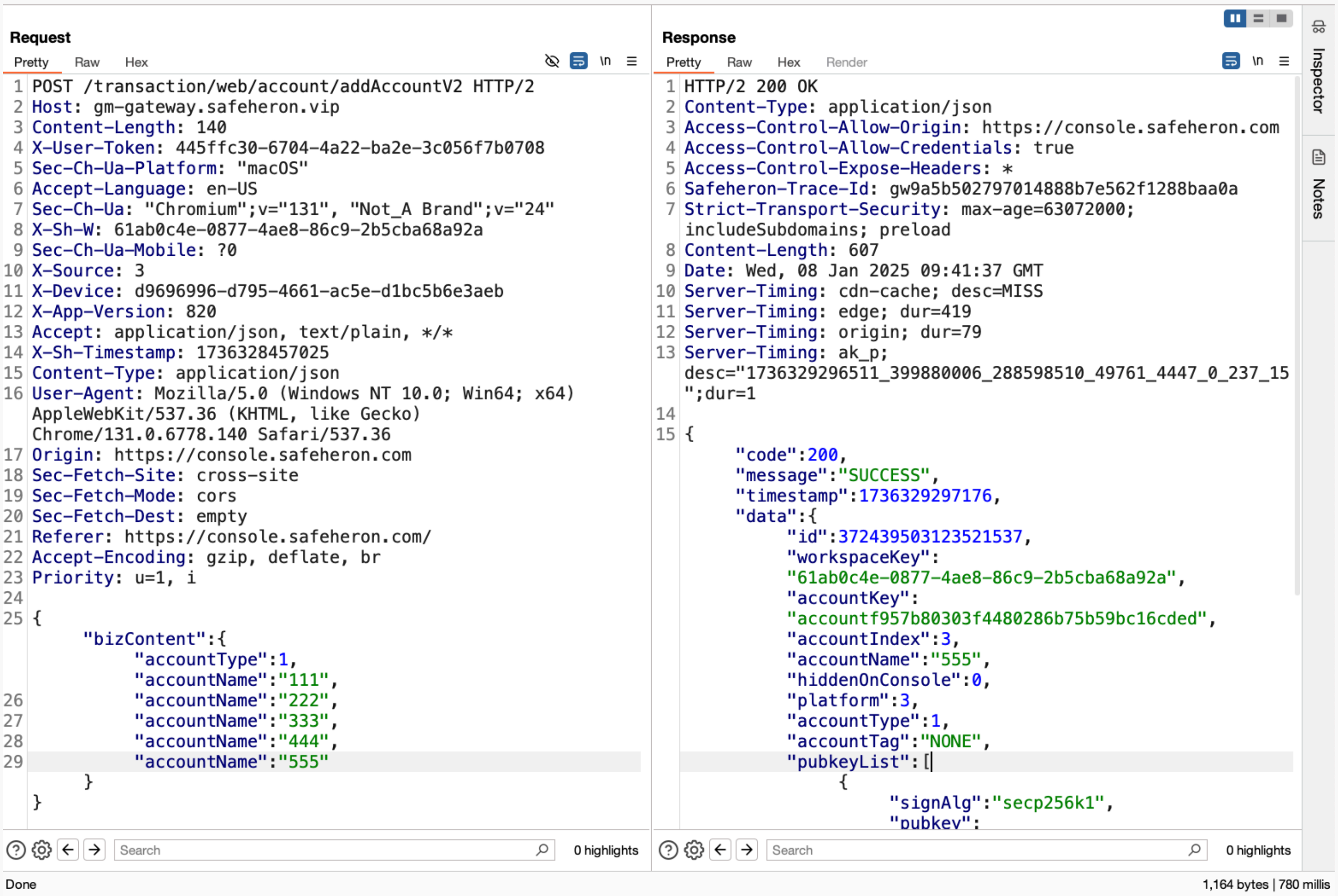
"accountType" is rounded by default and will not be rounded.



```
POST /transaction/web/account/addAccountV2 HTTP/2
Host: gm-gateway.safeheron.vip
Content-Length: 54
X-User-Token: 445ffc30-6704-4a22-ba2e-3c056f7b0708
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
X-Sh-W: 61ab0c4e-0877-4ae8-86c9-2b5cba68a92a
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: d9696996-d795-4661-ac5e-d1bc5b6e3aeb
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736328457025
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "bizContent":{
        "accountType":2.1,
        "accountName":"444"
    }
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gw7fa8d687161548de97555db8accf1df9
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Content-Length: 733
Date: Wed, 08 Jan 2025 10:43:34 GMT
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=305
Server-Timing: origin; dur=76
Server-Timing: ak_p;
desc="1736333013709_400248245_160265815_38061_6846_0_0_15";
dur=1

{
    "code":200,
    "message":"SUCCESS",
    "timestamp":1736333014014,
    "data":{
        "id":372455092732235777,
        "workspaceKey":
        "61ab0c4e-0877-4ae8-86c9-2b5cba68a92a",
        "accountKey":
        "account571c37b2f92445f8945b7da54ce521c5",
        "accountIndex":7,
        "accountName":"444",
        "hiddenOnConsole":0,
        "platform":3,
        "accountType":2,
        "accountTag":"NONE",
        "pubkeyList":[
            {
                "signAlg":"secp256k1",
                "pubkey":
                "021888d28f5e0f5b8bf59b48404bbced8d7179
```

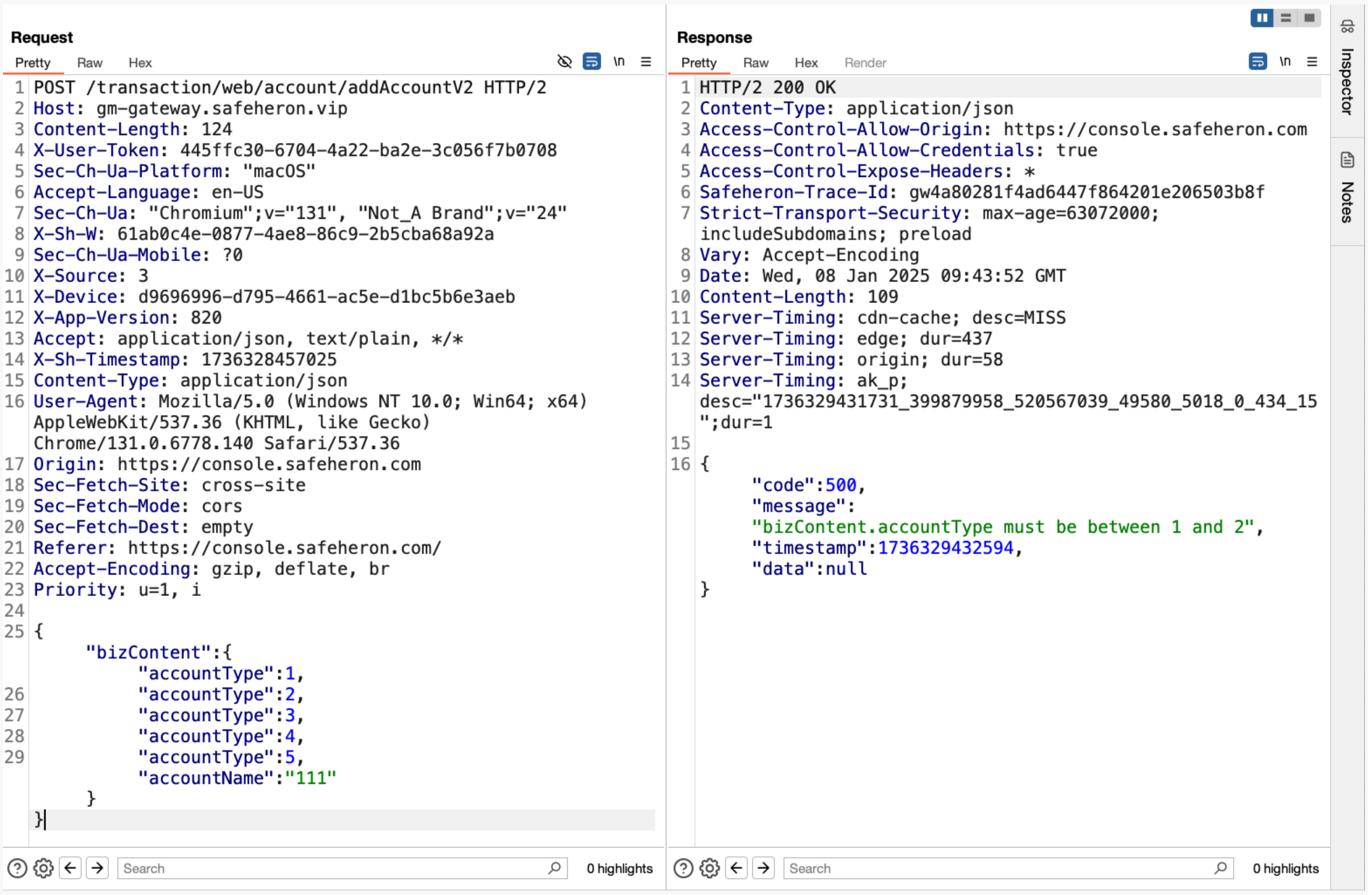
When multiple "accountName" exist, the last one is used by default.



```
POST /transaction/web/account/addAccountV2 HTTP/2
Host: gm-gateway.safeheron.vip
Content-Length: 140
X-User-Token: 445ffc30-6704-4a22-ba2e-3c056f7b0708
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
X-Sh-W: 61ab0c4e-0877-4ae8-86c9-2b5cba68a92a
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: d9696996-d795-4661-ac5e-d1bc5b6e3aeb
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736328457025
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "bizContent":{
        "accountType":1,
        "accountName":"111",
        "accountName":"222",
        "accountName":"333",
        "accountName":"444",
        "accountName":"555"
    }
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gw9a5b502797014888b7e562f1288baa0a
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Content-Length: 607
Date: Wed, 08 Jan 2025 09:41:37 GMT
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=419
Server-Timing: origin; dur=79
Server-Timing: ak_p;
desc="1736329296511_399880006_288598510_49761_4447_0_237_15
";dur=1

{
    "code":200,
    "message":"SUCCESS",
    "timestamp":1736329297176,
    "data":{
        "id":372439503123521537,
        "workspaceKey":
        "61ab0c4e-0877-4ae8-86c9-2b5cba68a92a",
        "accountKey":
        "accountf957b80303f4480286b75b59bc16cded",
        "accountIndex":3,
        "accountName":"555",
        "hiddenOnConsole":0,
        "platform":3,
        "accountType":1,
        "accountTag":"NONE",
        "pubkeyList":[
            {
                "signAlg":"secp256k1",
                "pubkey":
```

When multiple "accountType" exist, the last one is used by default.

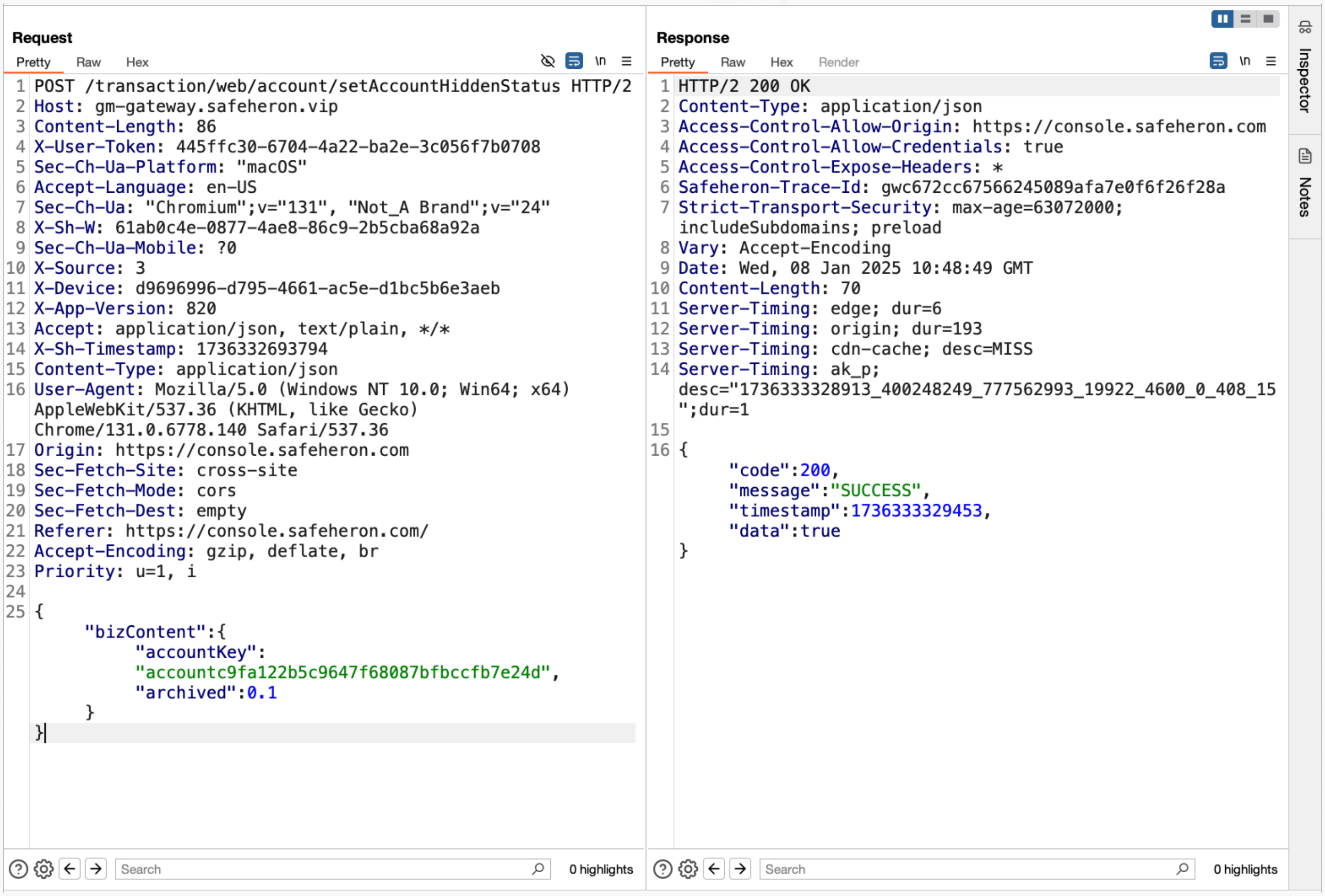


```
POST /transaction/web/account/addAccountV2 HTTP/2
Host: gm-gateway.safeheron.vip
Content-Length: 124
X-User-Token: 445ffc30-6704-4a22-ba2e-3c056f7b0708
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
X-Sh-W: 61ab0c4e-0877-4ae8-86c9-2b5cba68a92a
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: d9696996-d795-4661-ac5e-d1bc5b6e3aeb
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736328457025
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "bizContent":{
        "accountType":1,
        "accountType":2,
        "accountType":3,
        "accountType":4,
        "accountType":5,
        "accountName":"111"
    }
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gw4a80281f4ad6447f864201e206503b8f
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Vary: Accept-Encoding
Date: Wed, 08 Jan 2025 09:43:52 GMT
Content-Length: 109
Server-Timing: cdn-cache; desc=MISS
Server-Timing: edge; dur=437
Server-Timing: origin; dur=58
Server-Timing: ak_p;
desc="1736329431731_399879958_520567039_49580_5018_0_434_15
";dur=1

{
    "code":500,
    "message":
    "bizContent.accountType must be between 1 and 2",
    "timestamp":1736329432594,
    "data":null
}
```

2.setAccountHiddenStatus

The "archived" parameter is restricted to values between 0 and 1. When setting "archived" to 0.1 and sending the request, it returns "SUCCESS," but the wallet status does not change.



```
POST /transaction/web/account/setAccountHiddenStatus HTTP/2
Host: gm-gateway.safeheron.vip
Content-Length: 86
X-User-Token: 445ffc30-6704-4a22-ba2e-3c056f7b0708
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
X-Sh-W: 61ab0c4e-0877-4ae8-86c9-2b5cba68a92a
Sec-Ch-Ua-Mobile: ?0
X-Source: 3
X-Device: d9696996-d795-4661-ac5e-d1bc5b6e3aeb
X-App-Version: 820
Accept: application/json, text/plain, */*
X-Sh-Timestamp: 1736332693794
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Origin: https://console.safeheron.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://console.safeheron.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
    "bizContent":{
        "accountKey":
        "accountc9fa122b5c9647f68087bfbccfb7e24d",
        "archived":0.1
    }
}
```

```
HTTP/2 200 OK
Content-Type: application/json
Access-Control-Allow-Origin: https://console.safeheron.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: *
Safeheron-Trace-Id: gwc672cc67566245089afa7e0f6f26f28a
Strict-Transport-Security: max-age=63072000;
includeSubdomains; preload
Vary: Accept-Encoding
Date: Wed, 08 Jan 2025 10:48:49 GMT
Content-Length: 70
Server-Timing: edge; dur=6
Server-Timing: origin; dur=193
Server-Timing: cdn-cache; desc=MISS
Server-Timing: ak_p;
desc="1736333328913_400248249_777562993_19922_4600_0_408_15
";dur=1

{
    "code":200,
    "message":"SUCCESS",
    "timestamp":1736333329453,
    "data":true
}
```

Solution

1. If "accountType" only accepts values 1 and 2, it is recommended that the interface be restricted to only these two parameters.
2. If "accountType" only accepts values 0 and 1, it is recommended that the interface be restricted to only these two parameters.

Status

Acknowledged

[N3] [Suggestion] Anti-phishing strategies

Category: Others

Content

No anti-phishing strategy was found.

Solution

It is recommended to add anti-phishing strategies.

Status

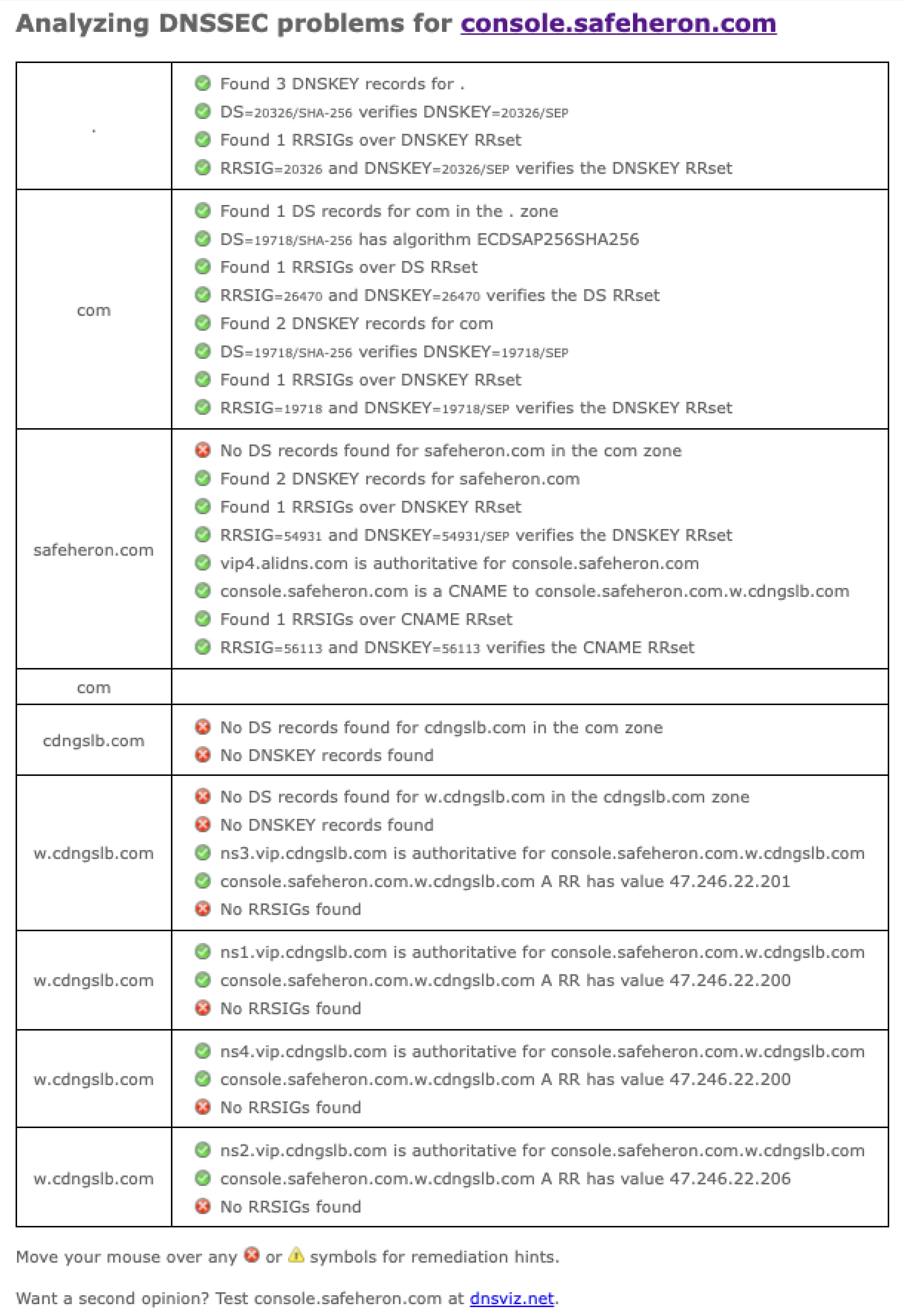
Acknowledged

[N4] [Suggestion] DNSSEC Security Issue

Category: Network infrastructure configuration test

Content

console.safeheron.com does not configure the DNSSEC policy.



Analyzing DNSSEC problems for console.safeheron.com

.	✓ Found 3 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
com	✓ Found 1 DS records for com in the . zone ✓ DS=19718/SHA-256 has algorithm ECDSAP256SHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=26470 and DNSKEY=26470 verifies the DS RRset ✓ Found 2 DNSKEY records for com ✓ DS=19718/SHA-256 verifies DNSKEY=19718/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=19718 and DNSKEY=19718/SEP verifies the DNSKEY RRset
safeheron.com	✗ No DS records found for safeheron.com in the com zone ✓ Found 2 DNSKEY records for safeheron.com ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=54931 and DNSKEY=54931/SEP verifies the DNSKEY RRset ✓ vip4.alidns.com is authoritative for console.safeheron.com ✓ console.safeheron.com is a CNAME to console.safeheron.com.w.cdngslb.com ✓ Found 1 RRSIGs over CNAME RRset ✓ RRSIG=56113 and DNSKEY=56113 verifies the CNAME RRset
com	
cdngslb.com	✗ No DS records found for cdngslb.com in the com zone ✗ No DNSKEY records found
w.cdngslb.com	✗ No DS records found for w.cdngslb.com in the cdngslb.com zone ✗ No DNSKEY records found ✓ ns3.vip.cdngslb.com is authoritative for console.safeheron.com.w.cdngslb.com ✓ console.safeheron.com.w.cdngslb.com A RR has value 47.246.22.201 ✗ No RRSIGs found
w.cdngslb.com	✓ ns1.vip.cdngslb.com is authoritative for console.safeheron.com.w.cdngslb.com ✓ console.safeheron.com.w.cdngslb.com A RR has value 47.246.22.200 ✗ No RRSIGs found
w.cdngslb.com	✓ ns4.vip.cdngslb.com is authoritative for console.safeheron.com.w.cdngslb.com ✓ console.safeheron.com.w.cdngslb.com A RR has value 47.246.22.200 ✗ No RRSIGs found
w.cdngslb.com	✓ ns2.vip.cdngslb.com is authoritative for console.safeheron.com.w.cdngslb.com ✓ console.safeheron.com.w.cdngslb.com A RR has value 47.246.22.206 ✗ No RRSIGs found

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

Want a second opinion? Test console.safeheron.com at dnsviz.net.

Solution

It is recommended to configure the DNSSEC policy.

Status

Fixed

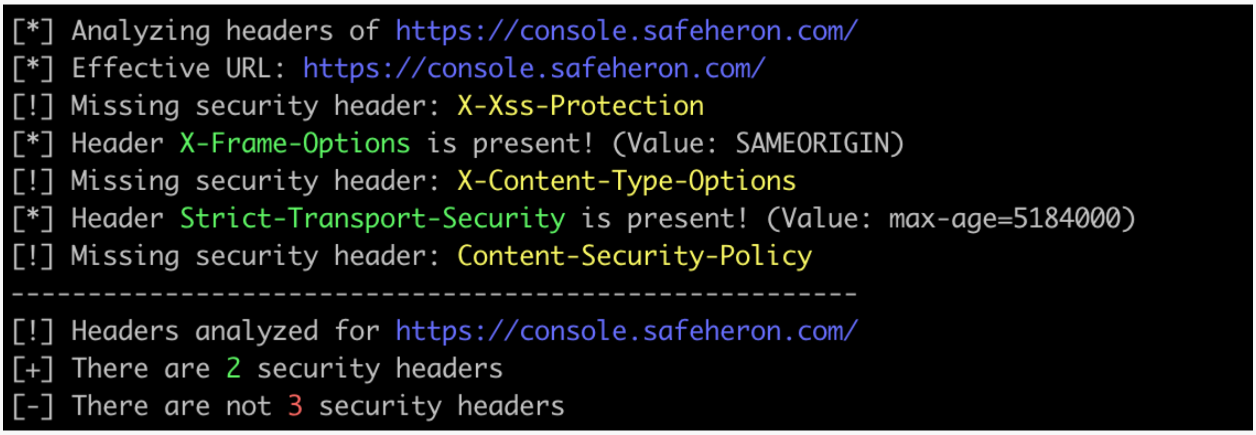
[N5] [Suggestion] HTTP Header Security Issue

Category: Web security response header test

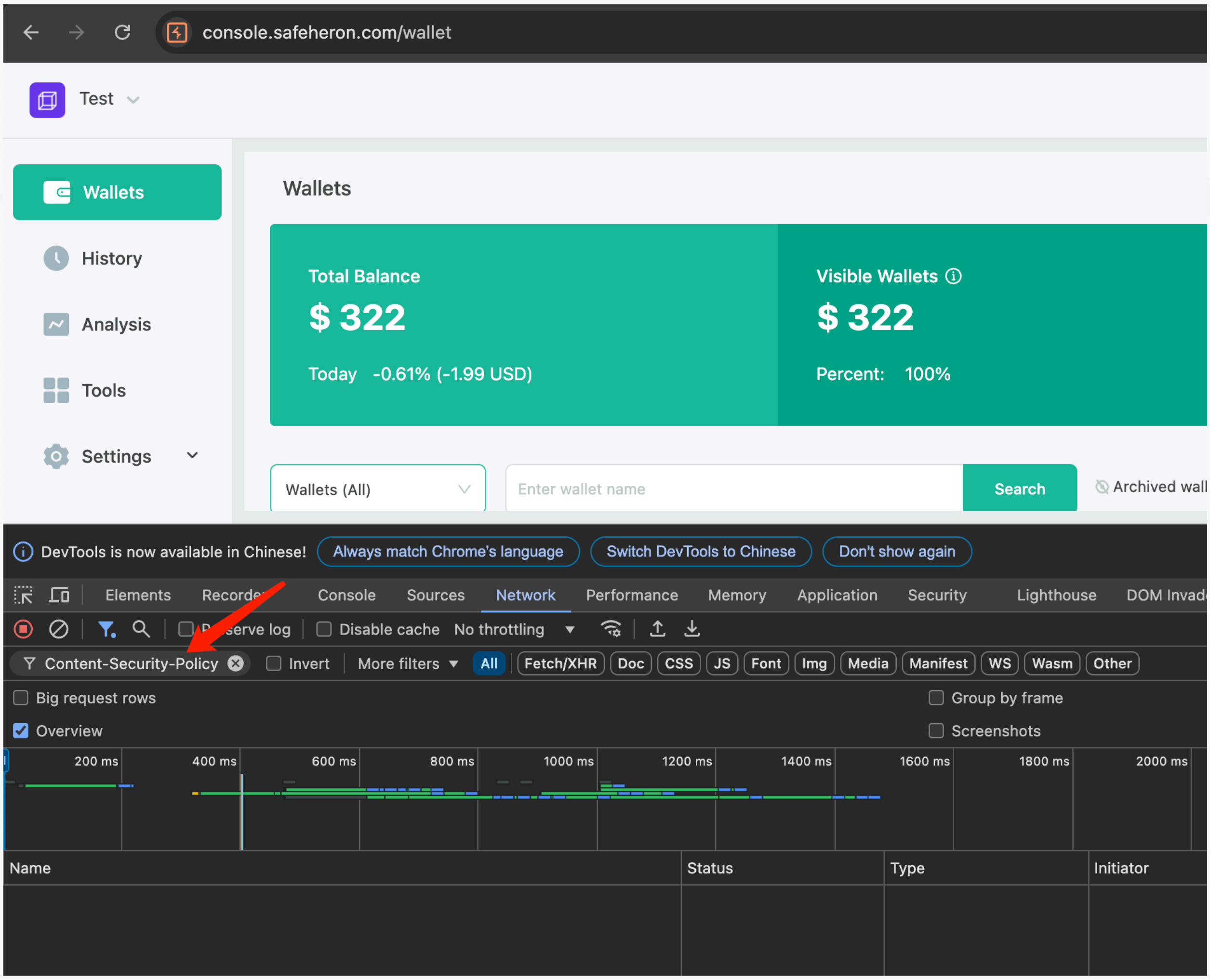
Content

The following security headers are missing:

1. X-XSS-Protection
2. X-Content-Type-Options
3. Content-Security-Policy



```
[*] Analyzing headers of https://console.safeheron.com/
[*] Effective URL: https://console.safeheron.com/
[!] Missing security header: X-Xss-Protection
[*] Header X-Frame-Options is present! (Value: SAMEORIGIN)
[!] Missing security header: X-Content-Type-Options
[*] Header Strict-Transport-Security is present! (Value: max-age=5184000)
[!] Missing security header: Content-Security-Policy
-------------------------------------------------------
[!] Headers analyzed for https://console.safeheron.com/
[+] There are 2 security headers
[-] There are not 3 security headers
```



Solution

It is recommended to adding missing security response headers.

Status

Fixed

4 Audit Result

Audit Number	Audit Team	Audit Date	Audit Result
0X002501210005	SlowMist Security Team	2025.01.08 - 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, five suggestions were identified. Three of these suggestions have been acknowledged, and 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