QuillAudits

Audit Report
November, 2024

For

BRAHMA

Table of Content

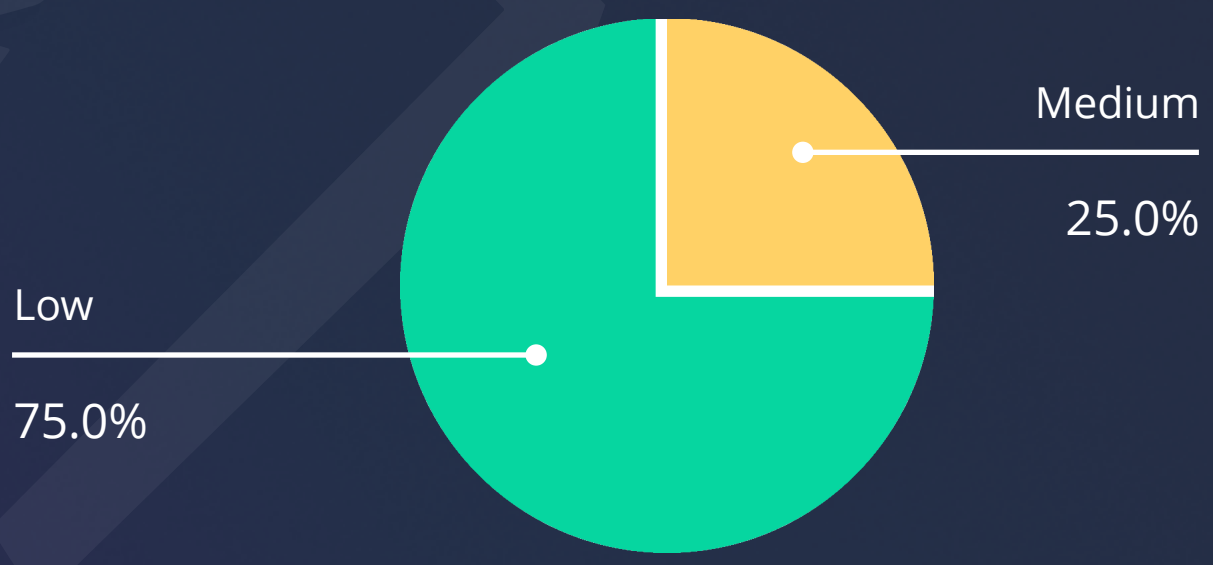
Overview

Project Name	Brahma Fi
Project URL	https://brahma.fi/
Overview	Brahma Console is a unified, non-custodial crypto account that makes managing and executing crypto transactions seamless and effortless. From setting up account to executing a range of actions like swapping, lending, or bridging assets directly in-app, Console supports entire on-chain journey. User can also connect easily to external dApps, all from the same platform.
Scope of Audit	The scope of this pentest was to analyze the Brahma Fi Web App for quality, security, and correctness. https://dev.console.brahma.fi
Method	Manual Analysis, Functional Testing, Automated Testing
Review 1	14th October 2024 - 26th October 2024
Updated Code Received	21st November 2024
Review 2	21st November 2024 - 25th November 2024

Number of Issues per Severity

	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	0	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	1	3	0

Security Issues



Checked Vulnerabilities

We scanned the application for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Improper Authentication
- Improper Resource Usage
- Improper Authorization
- Insecure File Uploads
- Insecure Direct Object References
- Client-Side Validation Issues
- Rate Limit
- Input Validation
- Injection Attacks
- Cross-Site Request Forgery
- Broken Authentication and Session Management
- Insufficient Transport Layer Protection
- Broken Access Controls
- Insecure Cryptographic Storage
- Insufficient Cryptography
- Insufficient Session Expiration
- Information Leakage
- Third-Party Components
- Malware
- Denial of Service (DoS) Attacks
- Cross-Site Scripting (XSS)
- Security Misconfiguration
- Unvalidated Redirects and Forwards

And more...

Techniques and Methods

Throughout the pentest of application, care was taken to ensure:

- Information gathering – Using OSINT tools information concerning the web architecture, information leakage, web service integration, and gathering other associated information related to web server & web services.
- Using Automated tools approach for Pentest like Nessus, Acunetix etc.
- Platform testing and configuration
- Error handling and data validation testing
- Encryption-related protection testing
- Client-side and business logic testing

Tools and Platforms used for Pentest:

- Burp Suite
- DNSenum
- Dirbuster
- SQLMap
- Acunetix
- Neucli
- Nabbu
- Turbo Intruder
- Nmap
- Metasploit
- Horusec
- Postman
- Netcat
- Nessus and many more.

Issue Categories

Every issue in this report has been assigned with a severity level. There are four levels of severity, and each of them has been explained below.

High Severity Issues

A high severity issue or vulnerability means that your web app can be exploited. Issues on this level are critical to the web app's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the web app code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are four issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Medium Severity Issues

1. Broken Access Control

Description

Certain API Endpoints in the application are not parsing JWT tokens and have no mechanism to check who is executing the request. This allows attacker to send victim parameters in the body and accordingly the API updates victim's data.

Some API endpoints are parsing JWT tokens but not checking if the data in the body of the request belongs to the same person.
Since the API endpoint relies on client-provided addresses without verifying the ownership of the address via authentication or authorization, this creates a critical flaw where users can access data and perform actions on behalf of other users.

Vulnerable Endpoint

https://gtw.dev.brahma.fi/v1/accounts/user

https://gtw.dev.brahma.fi/v1/console-referrals/user/:address

https://gtw.dev.brahma.fi/v1/deployer/deploy/relay

https://gtw.dev.brahma.fi/v1/karma/:address/score

POC

Request

Pretty Raw Hex

```
PATCH /v1/accounts/user HTTP/2
Host: gtw.dev.brahma.fi
Content-Length: 391
Trackingid: ba14bbc0-0daf-415a-9404-8f5c88ca4233
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IjY3RDNDRjJSUVI1TUVFTVZPT0RVVjdYWkJIVEVDM1ZMRlJMRE1L
QlYiLCJ0eXAiOiJKV1QifQ.eyJjaGFpbnMiOnsiNDIxNjEiOlsiMHgzNDk0NjIxMzlhMmFiZDg1NGQ1Y
2VhNmZlMjA1ZTFkMDUwYTM0MzgwIl0sIjg0NTMiOlsiMHgzNDk0NjIxMzlhMmFiZDg1NGQ1Y2VhNmZlM
jA1ZTFkMDUwYTM0MzgwIl19LCJjb25zb2xlcyI6eyIweDM0OTQ2MjEzOWEyYWJkODU0ZDVjZWE2ZmUyM
DVlMWQwNTBhMzQzODAiOls4NDUzLDQyMTYxXX0sImV4cCI6MTcyOTg3Njc3OCwiaWF0IjoxNzI5ODY5N
Tc4LCJpc3MiOiJjb25zb2xlLWF1dGgiLCJqdGkiOiI3YTNiMDZkOC1kYWM0LTRmZGEtYjdiNS0zNjllO
GVkYTM3ZmYiLCJzdWIiOiIweGQ3MzcxMjgzM0M5OWJiYmY4QzMwOWMzNURjNTY1MTBjMmYwZjQ3NEUiL
CJzdWJBY2NvdW50cyI6e30sInR5cGUiOiJhY2Nlc3MifQ.ltQacDDKAnwpa3Y-7Hf6d65mF9A2hD6X-H
luseIXoR9m3HD4LJikZ3jOyTNzqHNQHrI5nlim_OdmAtG634J5fLDggLjBeKOd_81yg7Z54T5qkmznzc
oSmEvSxnxs5S2xQruYx7eGWgcwyg9GzPuSoWvHXidTRikzLXCFOEj5PonqAKMNbgUAK2Ol9QBB4yGd-l
z-LjcXNglUm-AQjDFp5FkC23NRUGcOSesGIwCffz4NfF_FL8q6HPPQQW4BLCmF25Yh2YXKyA3G4k_0YE
6NUI9_ssdU02VsYZTImE5gKMD3Go2uiJh5rA1LGnCv3mrKeIRfKkfdgo5Lf0QmAow_6w
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/json
Origin: https://dev.console.brahma.fi
Referer: https://dev.console.brahma.fi/
```

UserA token

```
{
  "signer":"0x3d768f0F2D482EcC17f5162666909AD276E411F6",
  "signature":
  "0xcca2fa710abbaee684845d91a0f5d145c2e8a8b9a4888678dfefbd2d5f13b09b676cfd352cc
  a4b38a8909b9bcca279bd33d16f00141c3ddae329c277982f09c51c",
  "request":{
    "domain":{
      "name":"Brahma-Console",
      "chainId":42161
    },
    "message":{
      "consoleAddress":"0xd287c97f40b34c7d92696b10c9361590ac997abe",
```

UserB details

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Date: Fri, 25 Oct 2024 15:22:35 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 261
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length, Content-Type
Content-Security-Policy: default-src 'self';
Referrer-Policy: same-origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Origin
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Krakend: Version undefined
X-Krakend-Completed: true
X-Xss-Protection: 1; mode=block
```

```
{
  "data":{
    "accountName":"cybersecurity01_1",
    "consoleAddress":
    "0xD287C97F40b34c7d92696b10C9361590aC997ABE",
    "consoleType":"lite",
    "owners":[
      "0x3d768f0f2d482ecc17f5162666909ad276e411f6"
    ],
    "setting":{
      "42161":{
        "feeToken":"ETH",
        "gasPreference":"NORMAL"
      }
    },
    "threshold":1
  }
}
```

userB data updated

Request

Pretty Raw Hex

```
POST /v1/deployer/deploy/relay HTTP/2
Host: gtw.dev.brahma.fi
Content-Length: 89
Sec-Ch-Ua: "Chromium";v="125", "Not.A/Brand";v="24"
Accept: application/json, text/plain, */*
Content-Type: application/json
Trackingid: e45a8766-2255-423c-87e9-fda66d64c003
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://dev.console.brahma.fi
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://dev.console.brahma.fi/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=4, i

{
  "owner":"0x3d768f0F2D482EcC17f5162666909AD276E411F6",
  "accountName":"cybersecurity03333"
}
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Date: Fri, 25 Oct 2024 15:29:37 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 197
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length, Content-Type
Content-Security-Policy: default-src 'self';
Referrer-Policy: same-origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Origin
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Krakend: Version undefined
X-Krakend-Completed: true
X-Xss-Protection: 1; mode=block

{
  "data":{
    "chainID":42161,
    "createdAt":1729870177,
    "eoa":"0x3d768f0F2D482EcC17f5162666909AD276E411F6",
    "status":"running",
    "taskID":
    "0xbe077714d8296e86e5738956d4cff575fbd9d64032a6d9969346e59e3a50fcd1"
  }
}
```

Recommendation

Implement JWT token throughout the application. If JWT is not possible, implement a temporary cookie or token to identify the user. Validate who is executing requests for whom.

Impact

Unauthorized Access to Sensitive Data.

Privilege Escalation.

Modification in other users' account

Status

Resolved

Low Severity Issues

2. ENS not accessible

Description

Adding contacts require you to add an address or an ENS name for the address and also a name for the contact. But it throws error in the end stating an error.

Recommendation

Resolve ENS name properly and then allow users to save contact with ENS as well.

POC

Request

Pretty Raw Hex

```
POST /v1/accounts/addresses/0x6103a9d2ce8be9803df4dbe6a311d531efcdae22/42161 HTTP/2
Host: gtw.dev.brahma.fi
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:131.0) Gecko/20100101
Firefox/131.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 98
Referer: https://dev.console.brahma.fi/
Trackingid: 82e778f6-65a3-4d95-b9d5-9afc0a8e38a1
Origin: https://dev.console.brahma.fi
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IjY3RDNDRjJSUVI1TUVFTVZPT0RVVjdYWkJIVEVDM1ZMRlJMRE1LQlYiLCJ0eX
AiOiJKV1QifQ.eyJjaGFpbnMiOnsiNDIxNjEiOlsiMHg2MTAzYTlkMmNlOGJlOTgwM2RmNGRiZTZhMzExZDUzMWVmY
2RhZTIyIl0sIjg0NTMiOlsiMHg2MTAzYTlkMmNlOGJlOTgwM2RmNGRiZTZhMzExZDUzMWVmY2RhZTIyIl19LCJjb25
zb2xlcyI6eyIweDYxMDNhOWQyY2U4YmU5ODAzZGY0ZGJlNmEzMTFkNTMxZWZjZGFlMjIiOls4NDUzLDQyMTYxXX0sI
mV4cCI6MTcyOTkyNjIwNCwiaWF0IjoxNzI5OTE5MDA0LCJpc3MiOiJjb25zb2xlLWF1dGgiLCJqdGkiOiJlODQwNDU
zZC0yY2I2LTRjOGUtODViNy1hNTY0MzE2OTkwYWMiLCJzdWIiOiIweGY1MjkzZUEzN0Y0MTAzQTE2MDcyQ0ExMGUyY
jQ0NTVkMTFDOGMwOWEiLCJzdWJBY2NvdW50cyI6eyIweDY2Yzg4Y2YwN2Q2NWYwYzY5MmYzOWUxYWJmMTJjZjNhMzJ
lY2UyN2MiOls0MjE2MV19LCJ0eXBlIjoiYWNjZXNzIn0.eqQ5_rqQO6FCNemgkMxEtyEeraoMRpCqBnhh8Zh_QYatt
BydDlBRPhk-HWGZdcuQB6j_PORUTtygp-9TQPl0WGhYEU1ibpJYYC-xQHGF8-jQOgw2yoDYyrQMWhnUiWptg6jMgHw
A8ct_ToLMs8r8keEoYnSO9pTfqa0ikkq5Iqzfv4OJjyFA2A2A4vRuL3-ezip5Ew6HoNwOadcZ3DQNvfeF2_mjgQv1l
sUJH6Ge8KWBww9ng826xbj02SfGrJ9kt1UztsDqhC6TfJNZxgb94Ts-E2cqzr154GDYiZ4oOWaXgKCeZl8jzM-27b5
uVtBDUY5PZdnX4NduTdgayc39tQ
Priority: u=0
Te: trailers

{
  "addressBooks":[
    {
      "address":"allhack.eth",
      "name":"allhack",
      "sharedWith":[
      ],
      "isMultiChain":false
    }
```

Response

Pretty Raw Hex Render

```
HTTP/2 500 Internal Server Error
Date: Sat, 26 Oct 2024 05:06:50 GMT
Content-Type: application/json
Content-Length: 161
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length, Content-Type
Content-Security-Policy: default-src 'self';
Referrer-Policy: same-origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Origin
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Krakend: Version undefined
X-Krakend-Completed: false
X-Xss-Protection: 1; mode=block

{
  "data":{
    "error":"An unexpected error occurred. Please try again or summon support",
    "module":"/v1/accounts/addresses/:consoleAddress/:chainId",
    "requestId":"-"
  }
}
```

Status

Resolved

Brahma Fi team's Comment

ENS support has been removed because of unsatisfactory support on L2s.

3. Delete Confirmation Of Contacts

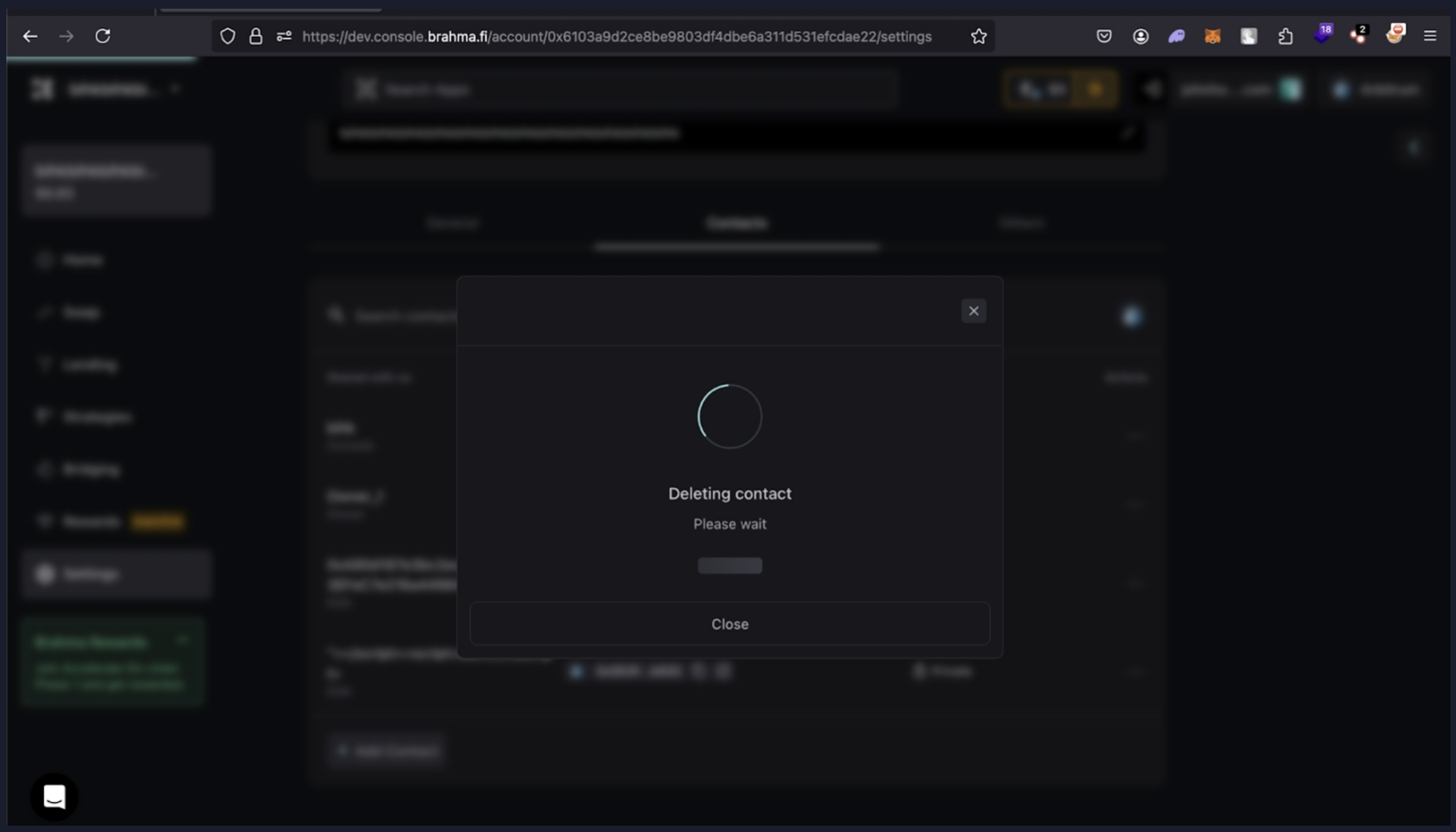
Description

After you add a Contact, you can delete the contacts except the first two in contacts, but if you delete any other it directly deletes the account without any confirmation for deleting the contact.

Recommendation

Add a confirmation for deleting so users can confirm without clicking on delete by mistake.

POC



Status

Resolved

4. Username character limit bypass on the backend

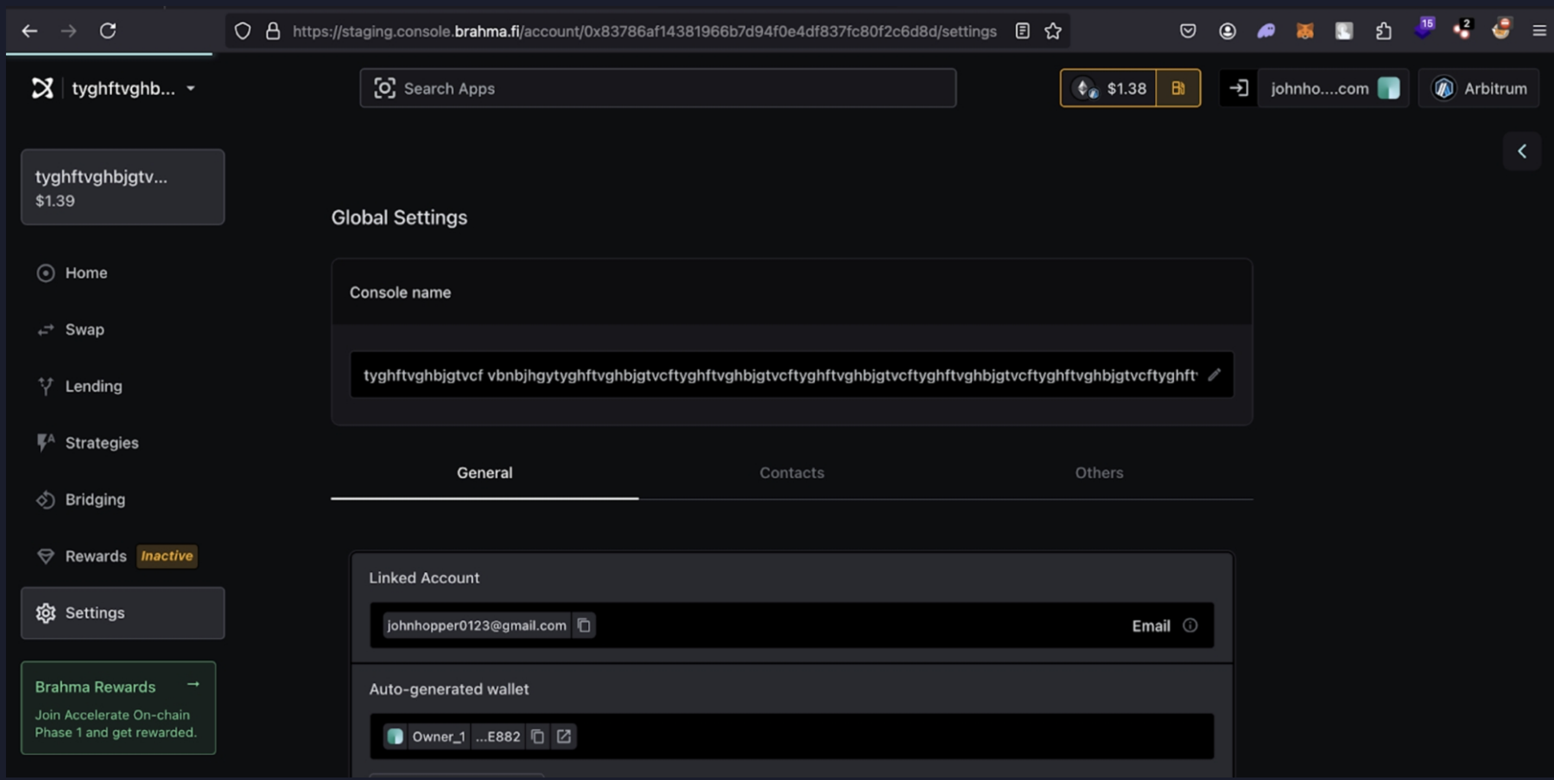
Description

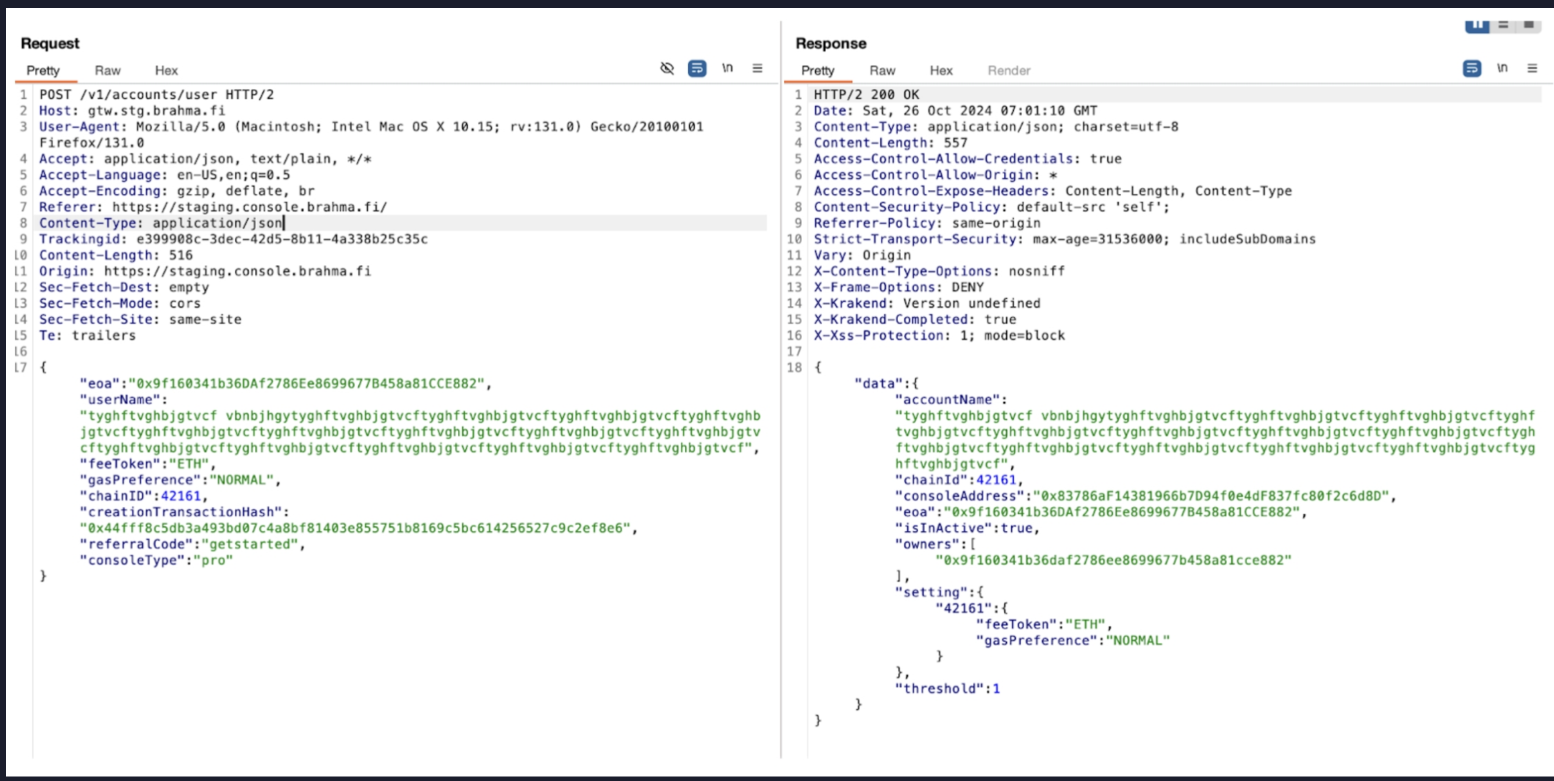
On the front end, you can only add a few characters in the username but you can manipulate the request to bypass the character limit to create a huge username.

Recommendation

Add a backend test as well for the character limit in the username

POC





Status

Resolved

Closing Summary

In this report, we have considered the security of the Brahma Finance Web App. We performed our audit according to the procedure described above.

Some issues of medium and low severity were found; some suggestions and best practices are also provided to improve the code quality and security posture. In the End, Brahma Fi team, Resolved all Issues.

Disclaimer

QuillAudits Dapp security audit provides services to help identify and mitigate potential security risks in the Brahma Fi Platform. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of Brahma Fi . One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the Brahma Fi Team to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a leading name in Web3 security, offering top-notch solutions to safeguard projects across DeFi, GameFi, NFT gaming, and all blockchain layers. With six years of expertise, we've secured over 1000 projects globally, averting over $30 billion in losses. Our specialists rigorously audit smart contracts and ensure DApp safety on major platforms like Ethereum, BSC, Arbitrum, Algorand, Tron, Polygon, Polkadot, Fantom, NEAR, Solana, and others, guaranteeing your project's security with cutting-edge practices.

1000+
Audits Completed

$30B
Secured

1M+
Lines of Code Audited

Follow Our Journey

Audit Report
November, 2024

For

BRAHMA

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com